Informatica

Dipartimento di Economia

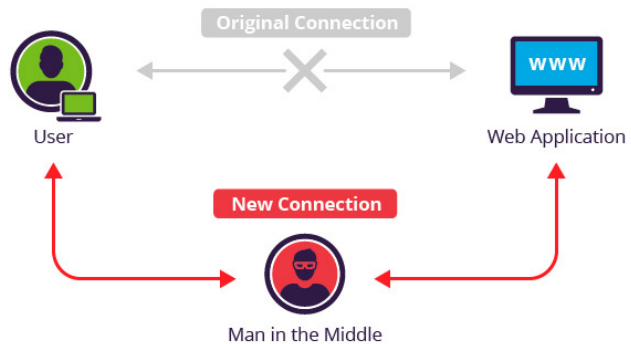
Ing. Cristiano Gregnanin

Corso di laurea in Economia

19 novembre 2016

Man in the middle

qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro. L'attaccante crea connessioni indipendenti con le vittime e ritrasmette i messaggi per far credere loro che stiano comunicando direttamente tramite una connessione privata, mentre in realtà l'intera conversazione è controllata dall'attaccante. Il malintenzionato deve essere in grado di intercettare tutti i messaggi importanti che passano tra le due vittime e iniettarne di nuovi.



Man in the middle - esempio

Alice vuole comunicare con Bob e che Mallory voglia spiare la conversazione e, se possibile, consegnare a Bob dei falsi messaggi.
Per iniziare, Alice deve chiedere a Bob la sua chiave pubblica. Se Bob invia la sua chiave pubblica ad Alice, ma Mallory è in grado di intercettarla, può iniziare un attacco Man in the middle.
Mallory può semplicemente inviare ad Alice una chiave pubblica della quale possiede la corrispondente chiave privata. Alice poi, credendo che questa sia la chiave pubblica di Bob, cifra i suoi messaggi con la chiave di Mallory ed invia i suoi messaggi cifrati a Bob.
Mallory quindi li intercetta, li decifra, ne tiene una copia per sé, e li re-cifra (dopo averli alterati se lo desidera) usando la chiave pubblica che Bob aveva originariamente inviato ad Alice. Quando Bob riceverà il messaggio cifrato, crederà che questo provenga direttamente da Alice.

Man in the middle - esempio

- Alice invia un messaggio a Bob, il quale viene intercettato da Mallory
- Mallory ritrasmette il messaggio a Bob. Bob non può sapere che non si tratta realmente di Alice
- Bob risponde con la propria chiave
- Mallory sostituisce la chiave di Bob con la propria e la ritrasmette ad Alice, sostenendo sia la chiave di Bob
- Alice cripta un messaggio con quella che crede essere la chiave di Bob, pensando che solo Bob potrà leggerlo
- Ora Mallory può decriptare il messaggio, essendo stata usata la sua chiave, leggerlo, modificarlo se lo desidera, criptarlo con la chiave di Bob e infine inviarlo a Bob
- Bob crede che questo messaggio provenga da una comunicazione sicura con Alice.

Man in the middle - esempio

Questo esempio mostra la necessità per Alice e Bob di avere un modo per garantire che essi stiano utilizzando le rispettive chiavi pubbliche, piuttosto che quella di un attaccante. Tali attacchi sono generalmente possibili contro ogni comunicazione che utilizzi la tecnologia a chiave pubblica. Fortunatamente, esistono una varietà di tecniche per difendersi contro gli attacchi MITM.

Sql injection

SQL injection è una tecnica, usata per **attaccare database**, con la quale vengono inseriti delle stringhe di codice SQL all'interno di campi di input in modo che vengano eseguiti.
Sfrutta le vulnerabilità di sicurezza del codice di un'applicazione, ad esempio quando l'input dell'utente non è correttamente filtrato da 'caratteri di escape' contenuti nelle stringhe SQL. L'SQL injection è più conosciuto come attacco per i siti web, ma è anche usato per attaccare qualsiasi tipo di database SQL.

Session hijacking

Consiste nello sfruttamento di una normale sessione di lavoro per raggiungere un accesso non autorizzato alle informazioni o ai servizi di un computer. In particolare, si tratta di un furto dei cookies usati per autenticare un utente su un sistema remoto. Sono rilevanti soprattutto per gli sviluppatori Web i cookie, essi possono essere rubati facilmente da un attacker per mezzo di un calcolatore intermedio o con l'accesso ai cookies conservati sul calcolatore della vittima.

Session hijacking

Molti siti Web permettono che gli utenti generino e controllino i loro utenti, usando un username e parola d'accesso (che può essere cifrata durante il transito). Affinché l'utente non abbia bisogno di re-inserire il proprio username e password in ogni pagina per mantenere la sua sessione, molti siti web utilizzano i cookies di sessione: una parte delle informazioni sono rilasciate dal server e restituite dal browser dell'utente per confermare la sua identità. Se un attacker è in grado di rubare questo cookie, può fare egli stesso le richieste come se fosse l'utente vero, accedendo alle informazioni e ai dati personali. Se il cookie è persistente, lo scambio d'identità può continuare per un periodo di tempo considerevole.

XSS (Cross-site scripting)

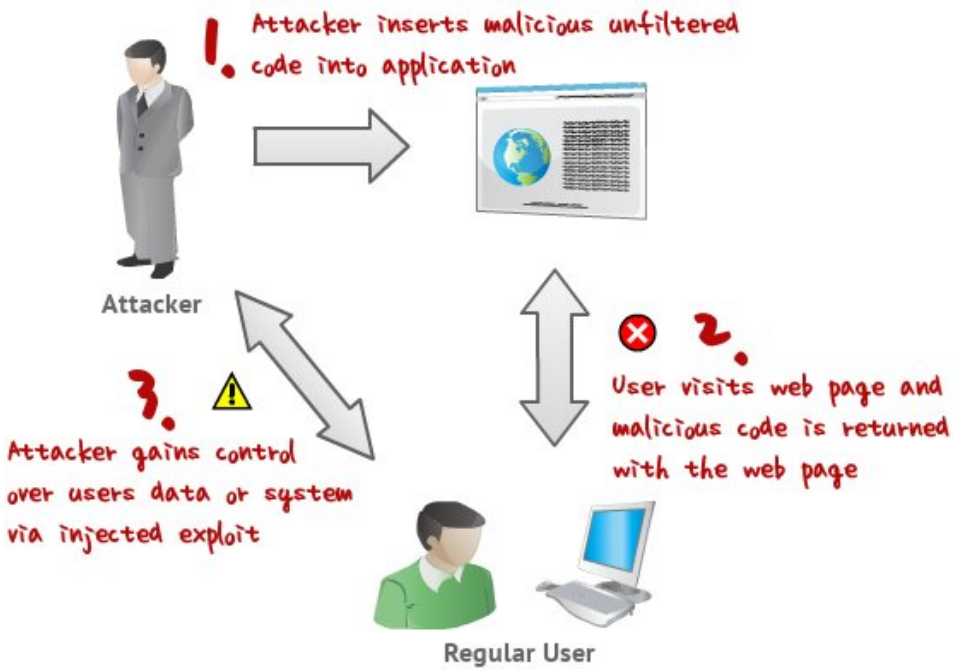
è una vulnerabilità che affligge **siti web dinamici** che impiegano un insufficiente controllo dell'input nei form. Un XSS permette a un Cracker di inserire o eseguire codice lato client (tipicamente js) La sicurezza nel web dipende da una varietà di meccanismi incluso il concetto di fiducia noto come Same origin policy. Questo afferma in sostanza che se al contenuto del primo sito viene concessa l'autorizzazione di accedere alle risorse di un sistema, allora qualsiasi contenuto da quel sito condividerà queste autorizzazioni, mentre il contenuto di un altro sito deve avere delle autorizzazioni a parte.

XSS (Cross-site scripting)

Gli attacchi Cross-site scripting usano vulnerabilità note delle applicazioni web, nei loro server o dei plugin su cui si basano. Sfruttando una di queste vulnerabilità, gli aggressori iniettano contenuto malevolo nel contenuto che fornisce il sito compromesso. Quando il contenuto arriva nel web browser lato client risulta inviato dalla fonte attendibile, perciò opera sotto le autorizzazioni concesse a quel sistema. Trovando il modo di iniettare script malevoli, l'utente malintenzionato può ottenere privilegi di accesso al contenuto di pagine sensibili, ai cookie di sessione e a una varietà da altre informazioni gestite dal browser per conto dell'utente.

XSS (Cross-site scripting)

Vulnerabilità XSS sono state segnalate e sfruttate dal 1990. Siti noti sono stati compromessi nel passato, inclusi siti di social-network come Twitter, Facebook, MySpace, YouTube e Orkut. Negli anni successivi, i problemi di cross-site scripting hanno superato quelli di buffer overflows diventando la vulnerabilità di sicurezza più comunemente segnalata.



Esempi di attacchi informatici - Sony

Nel 2011 furono ben 77 milioni gli account online di **Sony** del network ad essere colpiti, e fra i dati sensibili vi furono carte di credito e di debito degli ignari utenti. L'attacco fu lanciato da uno sconosciuto gruppo di hacker informatici, portando ad un danno stimato fra 1 e 2 miliardi di dollari. La cosa più incredibili è che l'attacco andò avanti per 24 giorni, nonostante gli sforzi della società per impedire la continuazione della frode. Solo dopo 24 giorni la falla era chiusa, e gli account nuovamente al sicuro, almeno per un po'.

Esempi di attacchi informatici - Giochi olimpici

Gli attacchi erano indirizzati all'impianto nucleare di Natanz, motivo per cui la faccenda destò parecchia preoccupazione, essendo interessato un impianto del genere. Il virus responsabile era il Stuxnet, un worm risultato del lavoro congiunto di Israele e Stati Uniti, che aveva come obiettivo quello di intromettersi nella gestione della velocità di rotazione delle turbine nucleari. Il worm arrivò a distruggere un numero di 1.000 centrifughe nucleari di Teheran, arretrando il programma atomico del paese ad almeno due anni prima.