UNIVERSITÀ
DEGLI STUDI
DI PALERMO

Prova Finale

Riccardo Li Pira Mat. 0714123

21 Febbrraio 2024

1 Attacchi MiTM

Un attacco di tipo Man-in-the-middle è un attacco informatico che permette al cybercriminale (d'ora in poi indicato come attaccante) di interporsi tra il sorgente e il destinatario. Lo scopo di questi attacchi può variare in base all'obbiettivo dell'attaccante. Questi potrebbe voler esclusivamente monitorare il traffico di rete senza modificarne il contenuto (il cosiddetto spoofing) oppure cambiare elementi della richiesta o risposta così da ingannare la controparte. La minaccia di questi attacchi deriva dal fatto che , sul mezzo di trasmissione, i dati possono essere letti da chiunque.

- DEMO ATTACCO MiTM usando tool mitmproxy

1.1 Come possiamo preventire un attacco MITM?

la crittografia è , per definizione, la garanzia che su un canale di comunicazione aperto (dove tutti possono ascoltare) gli unici ad essere in grado di comprendere il messaggio siano i diretti interessati (sorgente e destinatario). esistono diversi metodi di crittografia, che hanno proprietà diverse fra loro (simmetrici e asimmetrici) , tuttavia questi condividono delle similarità: la presenza di chiavi e algoritmi. alcuni di questi questi prevedono l'esistenza di 2 chiavi: una di queste nota a tutti i partecipanti alla comunicazione detta "chiave pubblica", e l'altra nota solo al proprietario detta per l'appunto "chiave privata". La chiave pubblica viene utilizzata per decrittare un messaggio crittato con la chiave privata , questo permette di garantire che il messaggio sia stato scritto proprio dal possessore della chiave privata e quindi oltre a garantire la "confidenzialità" del messaggio viene garantita anche la cosiddetta "autenticità". la sicurezza nell'utilizzo delle chiavi è basata sulla difficoltà computazionale della fattorizzazione in numeri primi di un numero n abbastanza lungo (esempio RSA-2048 almeno 300 cifre). questi algoritmi vengono poi utilizzati dai protocolli di sicurezza per le comunicazioni sul web.

1.2 HSTS

HTTP Strict Transport Security è una procedura che implementa una politica di sicurezza per le comunicazioni web, e che garantisce un canale sicuro e affidabile tra sorgente e destinatario utilizzando (tra le altre cose) dei certificati.

1.3 Certificati

Abbiamo parlato di certificati, ma che cosa è un certificato? un certificato è un elemento che racchiude al suo interno la chiave pubblica di cui abbbiamo discusso e le informazioni relative a chi ha emesso il certificato (nome, indirizzo di fatturazione, etc.).

2 Certificate Autority

Abbiamo parlato di autenticità di messaggi realizzata attraverso dei certificati, ma adesso ci chiediamo di chi dobbiamo fidarci nel ricevere dei certificati apparentemente autentici? (chiunque abbia delle conoscenze necessarie può effettivamente emettere un certificato self-signed, ovvero autofirmato).Ecco che qui entrano in gioco le Certificate Autority, ovvero degli enti che rendono "fidate" solo alcuni di tutti i certificati resi pubblici, così da garantirci che coloro con cui stiamo comunicando siano effettivamente chi dicano di essere.

3 Firewall

Un Firewall (tradotto Muro di fuoco) è un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi. per fare ciò i firewall storicamente, analizzano i pacchetti che transitano sulla rete e applicano una delle seguenti azioni in base a dei criteri che vengono impostati in fase di configurazioni:

- allow: il firewall lascia passare il pacchetto;
- deny: il firewall blocca il pacchetto e lo rimanda al mittente;
- drop: il firewall blocca il pacchetto e lo scarta senza inviare alcuna segnalazione al mittente

3.1 Firewall di livello Applicativo

Un altra tipologia è quella dei firewall a livello di applicazione: si tratta di dispositivi che "vedono" il traffico passante non come una sequenza di pacchetti ma come un flusso di dati e verificano la legittimità delle connessioni prima di effettuare delle azioni. Queste tipologie di applicazioni solitamente analizzano il traffico prima di reindirizzarlo (a differenza dei proxy che reindirizzano e basta, anche se oggigiorno la linea tra i prodotti sul mercato è molto sottile se non inesistente). una delle operazioni che si può fare con firewall di livello applicativo (che è anche il fulcro della attuale presentazione) è l'operazione di TLS inspection

4 Protocollo TLS

Il protocollo TLS è un protocollo di livello applicativo che sfrutta i concetti prima descritti di crittografia e di Certificate Autority per creare un canale di comunicazione sicuro con l'host di destinazione avendo la certezza di ricevere ed inviare dei messaggi ad un ente conosciuto e ritenuto sicuro dalla CA. Il funzionamento del protocollo TLS può essere suddiviso in tre fasi principali:

- Negoziazione fra le parti dell'algoritmo da utilizzare
- Scambio delle chiavi e autenticazione (RSA, PSK, algoritmi di crittografia suddescritti)
- Cifratura simmetrica e autenticazione dei messaggi

Nella prima fase, il client e il server negoziano il protocollo di cifratura che sarà utilizzato nella comunicazione sicura, il protocollo per lo scambio delle chiavi e l'algoritmo di autenticazione nonché il Message authentication code (MAC). L'algoritmo per lo scambio delle chiavi e quello per l'autenticazione normalmente sono algoritmi a chiave pubblica o, come nel caso di TLS-PSK, fanno uso di una chiave precondivisa (Pre-Shared Key). L'integrità dei messaggi è garantita da una funzione di hash che usa un costrutto HMAC per il protocollo TLS o una funzione pseudorandom non standard per il protocollo SSL.

5 TLS inspection

Tornando a noi, l'operazione di TLS inspection consiste in: decrittare il traffico TLS in modo tale da permetterci di analizzare i contenuti che transitano (così da poterli bloccare in caso di eventuali minacce). In generale possiamo utilizzare l'ispezione TLS per proteggere sia il client che il server, protezione lato client perchè vengono analizzate le trasmissioni iniziate (outgoing) dai client nella rete protetta, protezione lato server perche vengono

analizzate le trasmissioni in ingresso (ingoing) ai server nella rete protetta. Nota, i firewall che sfruttano le ispezioni TLS accettano comunicazioni solo dalle fonti i quali certificati sono preinstallati delle macchine (e non è possibile modificarli e/o eliminarli) quindi garantendo la sicurezza nelle comunicazioni e prevenendo completamente gli attacchi di tipo MITM (quantomeno non da fonti sconosciute).

- DEMO TLS INSPECTION CON MITMPROXY usando tool mitmproxy

6 Conclusioni

In definitiva, la protezione delle comunicazioni lato web è un problema che ci tocca in prima persona ogni volta che ci colleghiamo su internet anche per fare una semplice ricerca o per postare una foto sui social.

6.1 Riflessioni su scambio dei contenuti

Come abbiamo visto è facile scambiare i contenuti di una pagina se si è in grado di gestire il traffico in ingresso e in uscita da un host in rete : sia che questo sia fatto legalmente (come ad esempio l'utilizzo di un proxy aziendale per monitorare l'efficienza dei dipendenti) o che sia fatto illegalmente , come al posto di scambiare la foto del gatto con quella di un cane, si scambia il form di login ufficiale di una pagina, con uno fatto dal malintenzionato per rubare le informazioni di autenticazione.

6.2 Raccomandazioni

E' sempre raccomandabile, per evitare situazioni sgradevoli come queste, aggiornare frequentemente le applicazioni web e i browser (oltre che i sistemi operativi) in modo tale da ricevere le ultime patch di sicurezza, e se si vuole essere ancora più sicuri, si potrebbe controllare il certificato utilizzato dal sito, così da essere certi che questi rientrino nella lista degli enti fidati. Alcuni sistemi di autenticazione oggigiorno propongono come soluzione anche l'ausilio di sistemi two-factor-autentication (2FA), ma questi sono facilmente bypassabili con tecniche di social-engineering oppure da attacchi MiTM (con algoritmi un pò più avanzati di quelli descritti in precedenza).

6.3 Casi improbabili ma possibili

tutto questo non elimina completamente la probabilità che un attacco si verifichi lo stesso, se si riuscisse ad esempio a manomettere un certificato globale questi potrebbe rendere nulle tutte le procedure descritte in precedenza, tuttavia le probabilità che questo sia un caso reale sono molto basse. considerando che l'unico modo ad oggi conosciuto per ricavare le chiavi RSA è sostanzialmente il brute-force e le capacità computazionali necessarie ad una tale operazioni sono aldilà dei nostri attuali calcolatori : anche un supercomputer impiegherebbe anni per effettuare la fattorizzazione di , ad esempio, una chiave RSA a "soli" 2048.

6.4 Q-Day

le situazioni suddescritte cambierebbero drasticamente con il giorno l'avvento dei computer quantistici (il cosiddetto Q-day) dove gli attuali algoritmi di crittografia verranno superati dalle capacità computazionali di questi ultimi.