

Public-Key Infrastructure (PKI)

Protocolli come HTTPS danno all'utente evidenza del sito che questo visita. In presenza di HTTPS l'utente può autenticare l'URL e avere certezza dei contenuti visualizzati (nota bene, non degli indirizzi).

Sebbene il protocollo DNS sia **insicuro**, avere HTTPS rende i contenuti abbinati alla URL attendibili. Alternativa per mettere in sicurezza il DNS è il DNS Sec. Ovviamente se si va su una URL malevola (appositamente) questo discorso non vale.

Il web server interessato attraverso HTTPS espone il proprio certificato al browser. Il browser verifica il certificato del sito e trasmette l'informazione all'utente. Tipicamente il browser detiene una lista di certificati di root validi build-in ad esso e li usa per risolvere la catena di fiducia.

Lo store dei certificati può anche essere uno store del sistema operativo e non strettamente del browser. Nel caso sia appannaggio del browser lo store dei certificati i browser possono avere diversi store tra loro che differiscono.

Tipicamente un sito ha più certificati, espone al browser quello che quest'ultimo riconosce.

Lo store dei certificati di root, anche detta **root of trust**, è uno degli oggetti a cui prestare attenzione dal punto di vista della sicurezza. L'aggiunta di un certificato "malevolo" allo store è quindi compromettente.

Struttura di un attacco allo store dei certificati

1. Generati k_a e k_a^{-1}
2. Generati k_{RCA_a} e $k_{RCA_a}^{-1}$
3. Costruito certificato $\{a, k_a\}_{k_{RCA_a}}$
4. Costruito certificato $\{RCA_a, k_{RCA_a}\}_{K_{RCA_a}^{-1}}$
5. Importo il certificato di root costruito al punto 4 nello store del browser
6. utente accede al sito
7. utente ottiene padlock (lucchetto chiuso)

All'utente è permesso vedere e aggiungere alla lista dei certificati. È possibile inoltre vedere la gerarchia di certificazione analizzando il certificato.

Tipi di certificati

I certificati possono essere:

- **DV Domain Validated:** è un certificato spicciolo, ottenibile tramite protocolli che non richiedono particolari procedure. Mandata una mail alla casella indicata, in caso di risposta, viene concesso il certificato.
- **EV Extended Validated:** dalla procedura più articolata ed invasiva, costoso e maggiormente degno di trustworthyness.

Quindi anche per un attaccante è possibile ottenere un certificato DV. Dobbiamo fare un passo indietro, e andare all'acquisizione dei domini. Non c'è un singolo ente che, in maniera centralizzata, gestisca l'acquisizione dei domini.

Tipicamente i grandi enti comprano i domini anche dei nomi simili a quelli del proprio sito.

 **Domanda d'esame:** Cos'è PKI?

Certificati self-issued

Sono molti i motivi per cui i browser danno errore sul certificato foglia.

- unknown CA
- expired certificate
- notifica di revoca da parte della CA

E altri ancora.

Si hanno due possibilità quando si ottiene un errore relativo al certificato da parte del browser:


- accettarlo in via permanente
- accettarlo per la sessione in corso

Accettare temporaneamente un certificato, di volta in volta, si ha la possibilità di sbagliare o indovinare. Di fatto significa dare più opportunità ad un'attaccante di spacciare un certificato farlocco. Nella scelta definitiva invece la possibilità è unica. Ovviamente farlo in ambiente circoscritto in via definitiva è meno rischioso (ma comunque problematico).

Non si ha una soluzione assoluta a questo problema.

Certificate pinning

Il certificato non deve cambiare. È un ulteriore vincolo nello scambio dei certificati e fa in modo che l'attaccante non propini un certificato valido fatto da lui ma diverso dal precedente.

 **Domanda d'esame:** differenza tra certificato pinnato e certificato valido?

Risposta: se è pinnato è valido, ma se è valido non è necessariamente pinnato.

Vedi anche: **certificate transparency**, iniziativa per i certificati trasparenti.

Segretezza vs Trust

La perdita di segretezza **non si propaga**, la **perdita di trust sì**, si propaga ai livelli inferiori. Se un'autorità perde la chiave privata con cui ha firmato il certificato le altre non sono compromesse.

 **Domanda d'esame:** come influisce sulla catena la perdita di segretezza? E la perdita di trust?

Certificate Revocation List (CRL)

Perché avviene la revoca di un certificato:

- viene smarrita la chiave privata
- cambio di subject identifier

Le CRL vengono firmate dall'autorità di certificazione che ha fornito il certificato che si vuole revocare. La revoca di un certificato è a sua volta un certificato firmato e presuppone l'autorità pari al certificare. La revoca di un certificato prevede a sua volta un protocollo (**OCSP**). Il browser dovrebbe avere le CRL recenti ma non c'è uno standard. La revoca di un certificato è un problema assai articolato quindi.

 **Domanda d'esame:** cos'è OCSP?

Ad oggi la gestione della revoca è nascosta e non configurabile

Elenco di lettura

- Attributes-based authentication
- [Certificate root store](#)
- [Have i been pwned](#)
- [Certificate pinning](#)
- [Let's Encrypt](#)
- [Certificate transparency](#)
- [Certificate transparency in Chromium](#)
- [Certificate transparency Github](#)
- [How well do current browser handle certificate revocation](#)
- [OCSP](#)