PUBLIC KEY INFRASTRUCTURE

In tutti i protocolli visti finora rimane sempre un problema da affrontare per garantire la sicurezza, ovvero la distribuzione sicura delle chiavi pubbliche. Non esiste una soluzione univoca a questo problema, esistono diversi approcci che si adattano a scenari diversi e nessuno di essi è esente da difetti.

Alcuni approcci più diffusi per diffondere CHIAVI PUBBLICHE AUTENTICATE (gli end-point si devono fidare del fatto che tutti gli altri siano lealmente parte della rete di comunicazione):

I) TRUST ON FIRST USE (TOFU)
II) OUT-OF-BOUNDS COMMUNICATION
III) DELEGATED APPROACH
IV) AUTOMATIC VERIFICATION APPROACH

↓ complessità di impiego

TRUST ON FIRST USE: La prima comunicazione con un end-point avviene in modo non autenticato, senza chiave pubblica che viene offerta durante la prima comunicazione. Si assume quindi di NON ESSERE ATTACCATI durante la PRIMA COMUNICAZIONE

OUT-OF-BOUNDS COMMUNICATION: La chiave pubblica viene condivisa usando un canale di comunicazione diverso da quello da proteggere (assunto sicuro rispetto all'attaccante).

DELEGATED APPROACH: Deleghiamo un'altra entità per autenticare le chiavi pubbliche. È molto scalabile ma bisogna fidarsi delle CERTIFICATION AUTHORITIES e bisogna mantenere una infrastruttura complessa.

AUTOMATIC VERIFICATION APPROACH: Si usano protocolli speciali per verificare l'autenticità di chiavi pubbliche associate ad entità particolari che hanno un ruolo nella comunicazione che vogliamo fare.

Per esempio se vogliamo autenticare un HOSTNAME che passa tramite DNS è possibile autenticare le chiavi pubbliche sfruttando il fatto che l'hostname non è una semplice stringa di testo.

ESEMPI E CASI D'USO

I) Trust on first use:

Visto che un attaccante passivo non può ottenere informazioni grazie alla scambio di chiavi segreto, assumiamo che non vi siano attacchi attivi durante la prima comunicazione.

Viene impiegato per esempio nell'SSH

Questo approccio è vulnerabile al man in the middle durante il PRIMO UTILIZZO

II) Out of band:

Si utilizza un canale diverso in grado di garantire INFORMAZIONI AUTENTICATE, per ricevere la chiave pubblica con certezza.

Le info scambiate sull'altro canale sono molto poche quindi è anche possibile usare per esempio il telefono, un SMS, una mail, ecc.

Per esempio WHATSAPP scambia le chiavi pubbliche per la crittografia end-to-end tramite QR code, usando quindi la fotocamera come canale di comunicazione (di default non sono autenticate).

III) Delegated Approach:

Ci sono alcune entità pubbliche di cui gli utenti si fidano, dette CERTIFICATION AUTHORITIES, che si occupano di autenticare tramite firma digitale le chiavi di altre entità.

Si delega il processo di fase verifica alle CA, bisogna quindi fidarsi delle CA.

Ci sono 2 approcci per realizzare questo:

I) APPROCCIO CENTRALIZZATO: Alcune quindi autorità ben note dette TRUSTED THIRD PARTY (PKI)

II) APPROCCIO DISTRIBUITO: Molteplici soggetti possono garantire l'autenticità, ad esempio nel protocollo OPENPGP WEB OF TRUST ogni nodo garantisce per altri nodi quindi non c'è un'autorità che verifica tutti.

Il protocollo PKI è alla base del funzionamento di moltissimi protocolli WEB.

IV) Automatic Verification approach

Questo paradigma è il più complesso ma offre garanzie maggiori.
Si basa sul fatto che l'identità da verificare è esterna da un info che ho un modo rilevante e ben preciso all'interno del protocollo di comunicazione che stiamo usando (ad esempio hostname per DNS)

Il protocollo ACME/LETSENCRYPT permette di rilasciare certificati WEB utilizzando un protocollo PROOF OF CONTROL che consiste ogni nel "dimostrare" il possesso del server su cui per cui si rilascia il certificato.

Un'altra applicazione è KEYBASE che consente di collegare diverse identità virtuali degli utenti tra vari popolari servizi fornisce un protocollo PROOF OF INTEGRATION. L'utente quindi dimostra la sua identità dimostrando il controllo di account di altri servizi.

METADATI NELLA CRITTOGRAFIA ASIMMETRICA

I Key pair hanno bisogno di METADATI per svolgere correttamente il loro lavoro. I metadati sono una serie di informazioni aggiuntive che descrivono il "contesto", come per esempio

- Protocolli impiegati
- Quando è stata generata il Key pair
- Quando scade
- Chi è il proprietario delle chiavi
- ...

Le PUBLIC KEY INFRASTRUCTURES si basano sull'utilizzo di CERTIFICATI che sono DOCUMENTI FIRMATI contenenti tutti i metadati LEGATI alle chiavi e/o a dati crittografici.

Lo standard per i certificati è il X509

L'uso più diffuso dei certificati è nel protocollo HTTPS, servono per autenticare i server con cui si comunica per confermare l'autenticità del server stesso (evitare man in the middle).

Nei servizi CLIENT-TO-BUSINESS (per esempio un utente che visita un sito WEB) solo il server viene autenticato tramite certificato.

In altre parole al server non importa autenticare il client ma al

client impone essere certo di parlare con il server corretto.

In uno scenario BUSINESS-TO-BUSINESS invece, dove 2 SERVER dialogano tra loro senza coinvolgere gli utenti, è spesso necessario autenticare entrambi. Questo è possibile perché entrambi gli end point hanno un hostname pubblico (quindi certificabile).

Le PKI sono impiegate anche per comunicazioni EMAIL con protocollo S/MIME. In questo caso i certificati autenticano indirizzi e-mail.

Lo scopo è utilizzare correttamente protocolli di cifratura per trasmettere in modo sicuro e autenticato i messaggi.

Quelli descritti sopra sono i 3 scenari tipici per l'uso di PKI.

PROTOCOLLO HTTPS (comunicazione client - server)

Lo USER AGENT (browser web del client) invia una richiesta DNS per tradurre l'hostname in indirizzo IP. Il server DNS risponde con la traduzione. Durante questa fase tutto il traffico è in chiaro e non autenticato (esistono versioni sicure del DNS).

Se la connessione non fosse sicura lo user-agent farebbe un hand-shake TCP con il server e procede poi con una richiesta HTTP.

Nella versione cifrata si fa invece l'handshake TLS che oltre all'handshake TCP fa anche uno scambio di chiavi D-H con il server. Il server inoltre manda la FIRMA DI g^b (contributo D-H del server) e manda anche la PROPRIA CHIAVE PUBBLICA.

Il client può autenticare la chiave pubblica grazie al CERTIFICATO che il server manda e che contiene un riferimento all'hostname che lo user-agent ha richiesto al DNS.

Se il dominio contenuto nel certificato non combacia con quello della richiesta lo user-agent considera la chiave pubblica non valida (connessione non sicura).

Per poter considerare "ATTENDIBILE" il certificato ed usarlo quindi per autenticare il server si usa la TRUSTED THIRD PARTY. Questa entità fidata GARANTISCE che il certificato è autentico FIRMANDO il certificato con la propria chiave privata. Lo user agent accetta il certificato solo se RICONOSCE COME AFFIDABILE LA TTP. Esistono elenchi standard di autorità attendibili ma ogni user-agent è libero di aggiungere CA alla propria lista fidata.

Le CA vengono riconosciute come tali grazie alle policy che implementano per garantire l'autenticità di quello che certificano.

La serie di certificazioni ed il gruppo delle CA si dice CERTIFICATE CHAIN.

In definitiva quindi lo user-agent si fida della certificate-chain.

Questa architettura è anche EFFICIENTE dal punto di vista delle PRESTAZIONI poiché le CA vengono consultate solo per operazioni di RILASCIO, RINNOVO o REVOCA delle certificazioni. Lo user agent inoltre per verificare il certificato deve provare un numero di chiavi MINORE O UGUALE al numero di CA nella sua CERTIFICATE CHAIN.

I certificati hanno un PERIODO DI VALIDITÀ che definisce l'intervallo temporale entro cui il certificato è valido. Questo serve a combattere i furti e le falsificazioni. Al momento la policy mondiale è di rilasciare certificati con durata massima 1 anno. Questo è fatto per ridurre le esigenze di revoca, operazione complessa e dispendiosa.