PROTOCOLLI PER EMAIL SICURE

Le email sono storicamente il primo protocollo di comunicazione tra utenti e vengono molto utilizzate in ambiente lavorativo.

Poiché sono usate da personale NON TECNICO ci sono forti rischi per la sicurezza.

Oltre agli attacchi basati su software malevolo uno degli attacchi più diffusi è il SENDER SPOOFING (camuffare il mittente per essere qualcun'altro).

Il protocollo email nasce SENZA sicurezza.

Gli attacchi possono essere:

- NON TECNICI: phishing, malware ... (sfruttano le mail x la loro diffusione). Spingono gli utenti ignari a fare qualcosa per compromettere le credenziali o i dispositivi degli utenti.
- TECNICI: sfruttano delle vulnerabilità del protocollo.

Esistono dei protocolli appositamente sviluppati per combattere il phishing lato client, bloccando le azioni degli utenti in caso si abbia la non autenticità del sito web.

Inoltre alcuni provider implementano programmi di sicurezza che hanno gli utenti ad utilizzare procedure di autenticazione e sicurezza più forti (per esempio escludendo la possibilità di usare password per autenticarsi).

In caso del malware è analogo, ci sono dei software che fanno da blocco i danni.

ADDRESS SPOOFING

L'address spoofing consiste nel fingersi qualcun'altro. Storicamente questo è un problema perché le mail non hanno sistemi di cifratura/autenticazione nativi.

In genere le email funzionano come SISTEMA DISTRIBUITO in cui ogni PROVIDER consente agli utenti di inviare e ricevere mail occupandosi poi di dialogare con gli altri provider. Non esiste quindi una AUTORITÀ CENTRALE in grado di autenticare gli utenti. In particolare un client (detto MAIL USER AGENT) non possono verificare che un altro utente sia effettivamente un utente di un altro dominio.

Lo scambio di mail avviene tramite SMPT (invio) e POP/IMAP (ricezione). Tutti questi protocolli possono essere eseguiti su TLS per bloccare gli ATTACCHI ESTERNI ma non garantisce autenticità né sicurezza end-to-end.

Nelle mail L'IDENTITÀ DEL MITTENTE viene inserita tra gli header della mail stessa, quindi non c'è garanzia perché i messaggi SMTP auto-definiscono il mittente.

PROTOCOLLI DI SICUREZZA PER E-MAIL

Nel tempo sono stati ideati dei protocolli volti a risolvere il problema dello spoofing, aggiungendo una infrastruttura di sicurezza parallela e complementare a SMTP.

Alcuni di questi protocolli sono:

- MISURE DI SICUREZZA LATO PROVIDER (trasparenti per l'utente):
  - SENDER POLICY FRAMEWORK (SPF)
  - DOMAIN KEYS IDENTIFIED MAIL (DKIM)
  - DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE (DMARC)
  - BRAND INDICATORS FOR MESSAGE IDENTIFICATION (BIMI)
  - AUTHENTICATED RECEIVED CHAIN (ARC)
- MISURE DI SICUREZZA END-TO-END (prese dagli utenti)
  - S/MIME
  - PGP
- PROTOCOLLI LEGALI MISTI (diversi per ogni paese)
  - PEC (in Italia)

Dettaglio sulle misure lato server:

La fase critica per combattere lo spoofing è la comunicazione SMTP tramite tra provider diversi perché, di base, non vengono ad autenticarsi tra loro.

Tutti i protocolli di sicurezza vengono gestiti dal RECEIVING SERVICE.

I protocolli principali sono SPF e DKIM. Entrambi lavorano con il servizio DNS.

Il protocollo SPF verifica sul server DNS relativo al provider di provenienza della mail, richiedendo dei record DNS TXT (record non specializzati per controllare che l'IP del server mittente compaia nell'elenco di IP AUTORIZZATI A INVIARE

dell'indirizzo del provider MITTENTE presso il server DNS stesso.

Questo meccanismo permette ai provider di pubblicare l'elenco dei server autorizzati ad inviare mail per conto loro. Il problema è che questo controllo non si occupa di proteggere le query DNS da attacchi MITM che però non sono un grosso problema per i provider di grandi dimensioni poiché non è facile fare l'attacco.

Il protocollo DKIM invece si basa sul fatto che il SENDING SERVICE firmi gli header della mail (quindi anche il mittente). Il RECEIVING SERVICE invece va a recuperare le chiavi pubbliche del provider dal record TXT DNS per verificare la firma. Questo controllo è solo per gli scambi tra provider.

Tutti questi protocolli sono FACOLTATIVI ed il loro utilizzo è a totale discrezione dei provider. La maggior parte dei provider accetta messaggi anche da providers che non usano misure di sicurezza ma segnalano il messaggio come spam.

MISURE DI SICUREZZA END-TO-END (LATO CLIENT)

Anche con le misure lato server sopra descritte NON VIENE GARANTITA LA CONFIDENZIALITÀ ed inoltre gli utenti non possono avere la certezza che il mittente sia realmente lui (si può solo garantire che venga dal provider giusto).

Confidenzialità: S/MIME: questo standard si appoggia alla infrastruttura PKI e certificati x509 per firmare e cifrare le email

PGP: non si appoggia ad infrastrutture terze ma garantisce comunque confidenzialità e autenticità.

S/MIME: SECURE MIME

Nasce come standard proprietario ma poi viene standardizzato.

Il mittente firma la mail con un certificato x509 che poi allega (con la propria certificate chain) per permettere al destinatario di verificare la mail.

Esistono alcuni provider (CA) che erogano certificati S/MIME gratuiti.

La PEC (POSTA ELETTRONICA CERTIFICATA) tecnicamente si basa su S/MIME ma utilizza come CA ROOT non quelle garantite da mozilla nel WEB ma un insieme di CA accreditate presso lo stato italiano.

Queste CA si occupano di accertare l'identità del proprietario della mail, per garantire il principio di NON RIPUDIABILITÀ per dare VALORE LEGALE alla mail.

La PEC non si occupa di di crittografare il contenuto.

La PEC fornisce anche una "RICEVUTA" di avvenuta ricezione della mail, per equiparare il protocollo alla raccomandata A/R.

La ricevuta di ritorno è firmata ed inoltrata dal receiving server.

A livello legale inoltre l'utente è OBBLIGATO a controllare la casella PEC quindi se non la legge la mail risulta comunque consegnata al destinatario.

L'obbligo di controllare la PEC serve a garantire a livello legale qualcosa che tecnicamente non sarebbe garantito.

Il difetto attuale della PEC è che ha validità legale solo in Italia

PGP: PRETTY GOOD PRIVACY

Protocollo usato per firmare in generale comunicazioni ASINCRONE (anche cifrare il contenuto). Viene sfruttato un paradigma di cifratura asimmetrica ibrida.

L'implementazione dello standard più diffuso è il protocollo OPEN PGP.

Svolge le stesse funzioni di S/MIME ma non si basa su PKI bensì sfrutta un approccio fortemente DECENTRALIZZATO, sfruttando protocolli propri per gestire e distribuire le chiavi pubbliche (quindi i certificati).

Nell'architettura PKI la gerarchia delle CA garantisce maggiore resistenza contro gli attacchi. In PGP non ci sono certificatori esterni ma ogni utente sfrutta una chiave proprietaria per svolgere tutte le funzioni crittografiche.

Per aumentare la sicurezza è possibile DERIVARE dalla chiave MASTER diverse ~~SOTTOCHIAVI~~ SOTTOCHIAVI SPECIALIZZATE per ogni funzione e di poterle anche REVOCARE. Si genera quindi una gerarchia di chiavi, detta KEYRING, permettendo di gestire in modo migliore la sicurezza delle chiavi (soprattutto la MASTER).