UNIVERSITA' DEGLI STUDI DI PERUGIA

Facoltà di Scienze Matematiche, Fisiche e Naturali

Corso di Laurea Triennale in Matematica

Seminario di Sicurezza Informatica

Il protocollo SMTP e lo sniffer SPYD

Studente

Raffaela Sarlo

Azzurra Virgulti

Docente

Stefano Bistarelli

INDICE

INTRODUZIONE

La posta elettronica è oggi d'importanza vitale perché potente mezzo di comunicazioni tra utenti comuni. Tuttavia, la sicurezza delle informazioni personali di un soggetto che interagisce in una rete di computer è di frequente molto labile. Difatti le e-mail transitano, durante il loro tragitto, da un mittente ad un destinatario attraverso una tipologia di reti denominate Ethernet e la conoscenza di un particolare protocollo, chiamato SMPT, e con l'utilizzo di particolari programmi, detti sniffer, è possibile l'intercettazione e la lettura delle informazioni inviate.

Cenni storici

Nel 1970 il Network Working Group, nato dalla collaborazione tra le università legate ad Arpanet, definisce il NCP (Network Control Protocol), in altre parole l'insieme delle regole necessarie per far parlare tra loro due host, computer collegati alla rete.
Nel 1971 Ray Tomlinson, ricercatore della BBN, spedisce il primo messaggio di posta elettronica della storia. Lo standard ufficiale dell'e-mail viene elaborato nel corso degli anni attraverso varie tappe, l'ultima delle quali è la RFC 821 (Request For Comment) del 1982, con la quale si definisce il SMTP, il protocollo di trasmissione dei messaggi e-mail tuttora in uso.

Descrizione del funzionamento

Il sistema di posta elettronica è diviso in tre fasi:

- Consegna dei messaggi (protocollo SMTP)
- Mantenimento dei messaggi nella casella di posta del server e presentazione, a richiesta, al proprietario della mailbox (protocolli POP3 ed IMAP)

- Programma, sul computer dell'utente, che si occupa della spedizione e della lettura della posta dalla casella di posta elettronica (client).

Per fare un'analogia con la posta ordinaria, il client di posta, che a seconda dei casi corrisponde al mittente o al destinatario, se deve spedire qualcosa cerca una buca delle lettere (server SMTP), v'infila la corrispondenza che sarà prelevata e portata a destinazione dal sistema postale.
Dal punto di vista del destinatario, l'unica cosa da fare è controllare periodicamente la propria cassetta delle lettere (mailbox POP3 o IMAP) per vedere se vi è stato inserito qualcosa.
Esattamente come la posta ordinaria, la corrispondenza viene smistata in base all'indirizzo. L'indirizzo di posta elettronica ha una sua particolare struttura: nomecognome@server.dominio.

IL PROTOCOLLO SMPT

Cos'è?

Simple Mail Transfer Protocol (SMTP) è il protocollo utilizzato per la trasmissione dei messaggi di posta elettronica tra due host. SMTP utilizza il protocollo di trasporto TCP. Il server SMPT si occupa poi di trasferire i messaggi nelle mailbox dei destinatari oppure, qualora non fosse il diretto responsabile di queste, di inoltrarli al server che provvederà a farlo.
Il protocollo è descritto nella RFC 821, ma lavora in stretta collaborazione con altri standard poiché ha diversi limiti, come per esempio le dimensioni dei messaggi oppure la trasmissione di e-mail non in inglese.

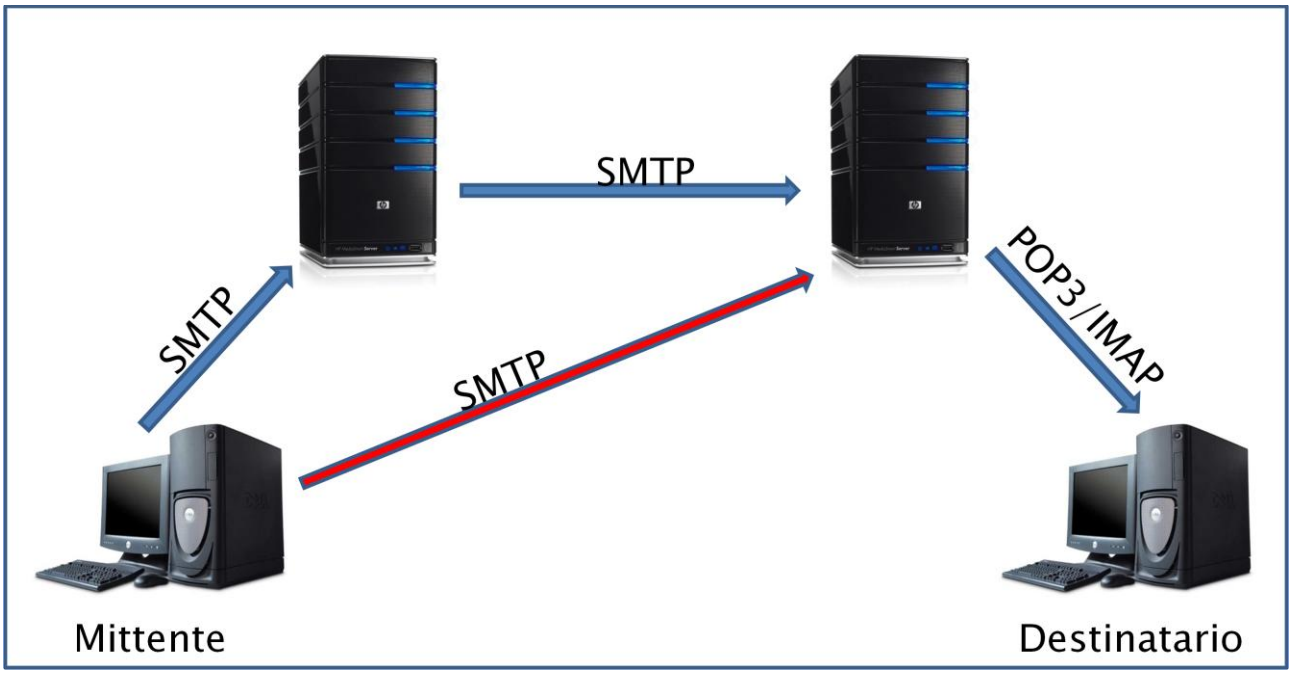
Uso del protocollo SMTP

Lo scambio dei messaggi avviene tra un mittente (M) ed un server destinatario (D) attraverso una connessione di rete.

L'invio avviene in due passi:

- **Il programma di posta elettronica usato dall'utente invia il messaggio al proprio server, usando il protocollo SMTP.**
- **Il server trasferisce il messaggio al server del destinatario utilizzando lo stesso protocollo.**

È possibile che il programma di posta elettronica usato dall'utente effettui direttamente il collegamento con il serve del destinatario, senza utilizzare il proprio server.



Il protocollo SMTP non può essere usato per il trasferimento "finale", poiché la macchina destinataria è di solito offline ed è

connessa solo per brevi periodi. Perciò il server SMTP trasferisce la posta al server POP (Post Office Protocol), dove viene accodato. Il destinatario per recuperare l'e-mail usa il protocollo POP.

Procedura del trasferimento del messaggio dal punto di vista del server destinatario:

- M, sulla base dell'indirizzo e-mail del destinatario, identifica il server D ed apre una connessione.
- D identifica il suo indirizzo IP ed accetta la connessione. Inoltre, memorizza tale identificazione come parte iniziale del messaggio da ricevere.
- M comunica lo username del destinatario.
- D verifica la validità dell'indirizzo ed autorizza la trasmissione del messaggio.
- D memorizza il messaggio in attesa che il reale destinatario si colleghi e ritiri il messaggio utilizzando un apposito protocollo (POP3 o IMAP).

È importante sottolineare che gli unici elementi che non possono essere arbitrari, quindi contraffatti, sono l'indirizzo IP di M e lo username del destinatario. Quest'ultimo però è quello dell'utente che effettivamente riceve il messaggio, mentre l'indicazione "TO: nomecognome@server.dominio" contenuta nel testo è quella trasmessa la M, quindi può essere totalmente arbitraria. Il server del destinatario, inoltre, non ha modo di sapere se il messaggio proviene da un server ben configurato e correttamente gestito, oppure da un generico PC, magari controllato da un programma installato da un virus.

Limiti del protocollo SMTP e sicurezza

SMTP è un protocollo testuale basato sulla codifica ASCII, non è permesso trasmettere direttamente testo composto con un diverso set di caratteri e tantomeno file binari.
Una delle limitazioni del protocollo SMTP originario è che non gestisce l'autenticazione del mittente. Oltre al rischio di spam, esiste la possibilità di inviare e-mail facendo apparire come mittente l'indirizzo corrispondente ad un altro account. Per ovviare a questi problemi è stata sviluppata un'estensione chiamata SMTP-AUTH. Nonostante questo, lo spam rimane ancora oggi un grave problema. Per questo motivo sono stati proposti diversi protocolli ausiliari per assistere le transazioni SMTP. Infatti, si sta lavorando su varie proposte di autenticazione e-mail.

SNIFFER

Cos'è lo sniffer e perché si "sniffa"

In una rete con tecnologia ethernet tutti gli host sono in grado di leggere le informazioni trasmesse nella rete stessa. Infatti, la parola "ether" deriva da "etere" ed ogni scheda di rete con tale tecnologia si comporta come una persona che vuol parlare ad un'altra in una stessa stanza, ma alla presenza di tante altre persone non interessate al discorso, le quali, onestamente, possono ignorare la conversazione oppure, disonestamente, ascoltare e venire a conoscenza delle informazioni.

Le informazioni che due reti ethernet si scambiano "nella stanza" alla presenza delle altre schede sono racchiuse, come in un gioco

di scatole cinesi, in pacchetti ethernet, i quali contengono pacchetti di protocolli IP, che contiene a sua volta pacchetti del protocollo TCP, che può contenere a sua volta pacchetti del protocollo SMTP.

In genere, le informazioni che una "scheda disonesta" spia, appartengono ai pacchetti del protocollo SMTP. Un utente malintenzionato può ascoltare illegalmente, o sniffare, una sessione di posta in uscita tra un utente ed il suo server di posta utilizzando proprio la caratteristica di tali schede con tecnologia ethernet che "gridano ai quattro venti" le loro informazioni. In zone in cui è richiesta sicurezza, la rete ethernet non dovrebbe mai essere scelta come tecnologia portante.

Lo sniffer SPYD

Cos'è?

Il programma demone SPYD ha proprio il compito di dimostrare quanto insicura possa essere una rete con tecnologia ethernet. Il nome, SPYD, sta per "The Spy Daemon", cioè il demone spia, poiché la posta intercettata può essere letta senza permesso alcuno del mittente o del destinatario.

Chi l'ha creato?

Il programma SPYD è stato realizzato da Giovanni Bembo, Mara Chirichiello, Iolanda Viscito, Aniello Viviano, ed è distribuito come "freewear" o "Open Source Software".
Tale programma ha come scopo unico quello di mettere in evidenza le debolezze di una rete con tecnologia ethernet e deve essere utilizzato per fini educativi.

Funzionamento

Possiamo descrivere l'attività del demone in tre fasi:

1. Girando su di un host X esso cattura ogni singolo pacchetto ethernet, lo apre e ne estrae il pacchetto IP.

2. Tenendo memoria di tutti i pacchetti IP che ha catturato, li analizza e li raggruppa per sessioni. Scartando tutti i pacchetti IP in cui sia la sorgente che la destinazione non comprendono la porta 25, SPYD ricostruisce tutti i pacchetti IP al fine di assemblare un pacchetto TCP.

3. Una volta ricostruito un pacchetto TCP lo analizza e si informa se debba aspettarsi o meno altri pacchetti TCP per ricostruire una sessione SMTP. Nel primo caso mette da parte il pacchetto TCP assemblato e aspetta di assemblare i rimanenti per poi estrarne la sessione SMTP; nel secondo caso estrae direttamente la sessione SMPT. Alla fine, isolata la sessione, SPYD la scrive in un file di testo nel file system e l'utente malintenzionato può comodamente andarla a leggere.

SPYD, infatti, può sniffare più sessioni di posta in uscita simultaneamente.

SPYD è stato realizzato per essere compilato ed eseguito su sistemi Linux. I requisiti di sistema sono minimi. Per eseguire al meglio il programma c'è bisogno di:

- Un sistema linux con un'interfaccia alla rete ethernet dalla quale si vuole "sniffare" il traffico di posta elettronica.
- Un compilatore C per compilare il demone.
- Privilegi di superutente (root) per eseguire lo stesso.

Il demone, una volta in memoria, cattura tutte le e-mail in entrata ed in uscita che passano per quella rete e memorizza ciascuna e-mail in un file diverso; ai file contenenti le lettere verrà assegnato un nome corrispondente alla data e all'ora della cattura delle e-mail relative, saranno posti nella stessa directory da dove il programma è stato eseguito e avranno come estensione la parola ".spied".

Protezione dagli sniffer

Il modo più semplice ed efficace per avere garantita la propria sicurezza durante l'invio di e-mail è quello di non far capire a chiunque avesse utilizzato uno sniffer cosa c'è scritto nelle stesse e-mail.
Mediante l'utilizzo di programmi di crittografia è possibile codificare il testo in chiaro di una e-mail secondo opportuni algoritmi che implementano la codifica e la decodifica di dati utilizzando dei cifrari, i quali tramite l'utilizzo di parole chiave sono in grado di trasformare l'e-mail in testo incomprensibile ed in testo in chiaro.
Bisogna dire che i più recenti client di posta forniscono degli strumenti di cifratura interni piuttosto efficienti e versatili. Grazie ad essi, programmi come Outlook ed Outlook Express, sono in grado sia di cifrare il contenuto dei messaggi sia di certificare la provenienza di un messaggio.

GLOSSARIO

Algoritmo : insieme di calcoli che, svolti ripetutamente e sempre nella stessa sequenza, conducono ad un obiettivo.

Codifica ASCII : American Standard Code for Information Interchange, codice standard americano per lo scambio di informazioni. E' un sistema di codifica a 7bit comunemente utilizzato nei compilatori. Negli anni sono state proposte varie estensioni con lo scopo di raddoppiare il numero di caratteri rappresentabili.

Compilatore : programma che rende eseguibile direttamente un codice sorgente. Il file viene tradotto dalla forma testuale del linguaggio di programmazione alla forma binaria. Il file diventa così di tipo EXE.

Crittografia : è il metodo di codifica dei dati che impedisce l'accesso, senza autorizzazione, ad estranei. Garantisce la privacy nelle comunicazioni via rete.

Directory : è una specifica entità del file system che elenca altre entità, quali file e altre directory, permettendo così una struttura ad albero.

Ethernet : regole e standard per connettere un computer a LAN.

IMAP : Internet Messagging Access Protocol, protocollo per la posta elettronica in internet, più evoluto del POP. Consente di

lavorare offline come il POP e di ricevere/spedire messaggi tutti insieme. Consente, anche, di selezionare i messaggi da scaricare, di archiviare i messaggi sul computer e sul server.

LAN : Local Area Network. Rete di computer limitata ad un'area circoscritta, come un ufficio o un edificio.

Linux : sistema operativo multimediale, simile e derivato da Unix, ma più compatto e semplice.

POP3 : Post Office Protocol versione 3, protocollo che regola la connessione ad un sistema per gestire la posta elettronica e trasferisce i messaggi di un utente.

Porta 25 : porta universalmente dedicata al protocollo di posta in uscita.

Rete : sistema o particolare tipo di rete di telecomunicazioni che permette la condivisione di dati informativi e risorse tra diversi calcolatori. Tale servizio fornito dal sistema ricopre un'area più o meno ampia.

RFC : Request For Comments. Si tratta di documenti redatti dalla Internet Engineering TaskForce, organismo che definisce gli Internet Standard, ovvero di approvare quelle che sono le regole che governano la comunicazione nella rete. Ad ogni RFC viene associato un numero intero, una volta che il documento è stato pubblicato il suo numero non può più cambiare ed eventuali modifiche all'origine comportano l'introduzione di nuovi numeri.

Root : nei sistemi operativi di tipo Unix, è l'utente dotato di massimi privilegi, l'amministratore di sistema o anche detto superutente.

Scheda di rete : interfaccia digitale solitamente inserita all' interno di PC, server, stampanti, router, per svolgere tutte le elaborazioni o funzioni necessarie così da consentire la connessione ad una rete informatica.

TCP/IP : Trasmission Control Protocol/Internet Protocol. L'insieme delle regole che rendono possibile il dialogo tra più computer e la connessione ad internet. L'insieme di trasmissione dei protocolli è usato per l'interscambio di dati su internet.

UNIX : sistema operativo usato dai grandi mainframe e da molti computer collegati ad internet.