



Progetto:

**Sicurezza della posta elettronica:
MIME & S/MIME**

Università degli studi di Catania

Facoltà: Scienze Matematiche Fisiche Naturali

Corso: Informatica Applicata

Insegnamento: Sicurezza dei Sistemi Informatici I

Docente: Giuseppe Scollo

Anno Accademico 2007/2008

Realizzato da:

Zelinda Trovato

Matricola A40/000140

SICUREZZA DELLA POSTA ELETTRONICA PROTOCOLLI MIME & S/MIME



Indice

◆ Premessa	4
◆ 1. Cos'è la posta elettronica	5
1.1 . Come funziona	6
◆ 2. Il protocollo SMTP	8
2.1. Esempio i comunicazione SMTP	8
◆ 3. Il protocollo POP3	9
3.1. Esempio di comunicazione POP3	9
◆ 4. L'algoritmo MD5	10
4.1. Storia e analisi della crittografia	12
4.2 Applicazione dell'MD5	13
◆ 5. Introduzione	14
5.1. Evoluzione di S/MIME	14
5.2. Servizi offerti da S/MIME	15
5.2.1 Le firme digitali	16
5.2.1.1. Autenticazione	16
5.2.1.2 Non ripudio	16
5.2.1.3. Integrità dei dati	17
5.2.1.4. Applicazione di una firma digitale e verifica	18
5.2.2. Crittografia dei messaggi	20
5.2.2.1. Riservatezza	20
5.2.2.2. Integrità dei dati	20
5.2.2.3. Operazioni di crittografia e decrittografia	21
◆ 6. Interazioni	23
6.1 applicazioni	23
◆ 7. Messaggio con tripla crittografia	25
◆ 8. Conclusioni	26
◆ 9. Riferimenti	27

Premessa

Oggi giorno tutti posseggono un computer con un collegamento a internet e spesso di ha anche una piccola rete LAN a cui connettersi (casalinga o aziendale che sia), per condividere un documento, navigare sulla rete alla ricerca di offerte e nuovi software e ricevere anche comunicazioni nella propria casella di posta elettronica.

Tutte queste sono ormai diventate azioni comuni grazie all'utilizzo sempre più crescente del pc, sia in casa propria che in ambiente di lavoro.

Se siamo in attesa di qualche risposta, lettera e così via, non stiamo più in attesa che arrivi il postino e suona il campanello e ci consegna la posta, ma bensì stiamo davanti al pc in attesa che sullo schermo ci lampeggi una "bustina".

D'altra parte al di là degli innegabili vantaggi che l'era telematica ha apportato alle nostre abitudini di vita e lavorative, esistono anche altri aspetti da considerare, ed in particolar modo quelli legati all'esistenza di una serie di "rischi":

La posta elettronica è oggi una delle vittime.

Infatti il mio progetto relativo al corso di Sicurezza 1 approfondisce il problema dei rischi della posta elettronica, partendo dalla nascita di questo servizio che con l'evolversi del tempo, delle esigenze e delle problematiche, si arriva allo studio dei protocolli standard che permettono la sicurezza della posta elettronica.

Z. Trovato

1. Cos'è la posta elettronica

Oggi giorno uno dei mezzi più diffusi per la comunicazione è quello della posta elettronica. L' e-mail (Electronica Mail), è un servizio internet grazie al quale ogni utente può inviare e ricevere messaggi ed è l'applicazione internet più conosciuta e più utilizzata attualmente.

La sua nascita risale al 1972, quando Ray Tomlison installò su ARPANET un sistema in grado di scambiare messaggi tra le varie università ma chi ne ha definito veramente il funzionamento si chiamava Jon Postel.

In pratica l' e-mail è la controparte digitale ed elettronica della posta ordinaria e cartacea. A differenza di quest'ultima il ritardo con cui arriva dal mittente al destinatario è di pochi secondi o minuti.



Ray Tomlison



dal postino --> all'e.mail



1.1 Come funziona

Quando un provider concede ad un utente l'accesso ad internet, gli assegna un identificativo che lo individua in modo univoco nella rete e in genere gli mette a disposizione anche una casella di posta elettronica, cioè uno spazio fisico nel server dove verranno automaticamente depositati i messaggi a lui diretti. Per usufruire del servizio di posta elettronica abbiamo quindi bisogno:

- Un computer o altri apparecchi predisposti come palmari e cellulari
- Una casella di posta attiva da un Internet Service Provider (ISP) col suo indirizzo
- Un interfaccia di posta elettronica Client o Browser

Il sistema di funzionamento della posta elettronica è abbastanza complesso, ma semplificando in modo banale, possiamo dire che un messaggio di posta elettronica può essere considerato come un file che viene scambiato tra mittente e destinatario, tramite server appositi.

Per far sì che il messaggio arrivi a destinazione, questo ha dei campi fissi da compilare:

- Mittente : l'indirizzo e-mail o il nome da visualizzare come mittente del messaggio di posta elettronica
- Destinatario: l'indirizzo e-mail di destinazione
- Oggetto: (facoltativo) descrizione del messaggio

Infatti come ogni protocollo che preveda un servizio di posta elettronica. TCP/IP utilizza un formato che suddivide il messaggio in due parti:

intestazione --> header

testo --> body

In particolare il protocollo mentre lascia ampia libertà da dare al testo del messaggio , impone regole ben precise per quando riguarda l'intestazione, dalla quale non possono assolutamente mancare l'indirizzo del mittente e del destinatario.

Per quanto riguarda l'indirizzo di posta elettronica, questo prevede che sia formato da una parte che individua in modo inequivocabile l'utente e dall'altra, ben più importante, che consente di identificare il dominio di appartenenza:

`id_utente@id_dominio`

Il protocollo utilizzato per gestire la comunicazione tra l'utente e il server di posta elettronica è SMTP (Simple Mail Transfer Protocol) è molto semplice e prevede che il client, inviata una richiesta di collegamento, si ponga in attesa di un messaggio di conferma (Ready for Mail) da parte del server.

Dopo uno scambio di messaggi per l'attivazione della connessione, l'utente può inviare messaggi per la spedizione, catturare i messaggi giunti alla propria casella postale (mail box) finché non decide di interrompere la connessione. Naturalmente anche il server può procedere alla chiusura della connessione qualora non vengono inseriti comandi per un certo tempo, in modo da non tenere occupate inutilmente delle linee di collegamento.

2. Il protocollo SMTP

Il Simple Mail Transfer Protocol (SMTP) è il protocollo standard per la trasmissione via internet delle e-mail.

È un protocollo semplice, testuale nel quale vengono specificati uno o più destinatari di un messaggio, verifica la loro esistenza ed il messaggio viene trasferito. È abbastanza facile verificare come funziona un server di trasmissione SMTP mediante un cliente telnet.

SMTP usa il protocollo di trasmissione TCP, e per associare il server SMTP a un dato nome di dominio (DNS) si usa un record denominato MX (Mail Exchange).

L'SMTP iniziò a diffondersi nei primi anni '80, a quel tempo era un'alternativa all'UUCP (Unix to Unix Copy), che era più adatto a gestire il trasferimento mail tra computer la cui connessione era intermittente. L'SMTP funziona meglio se i computer sono collegati sempre alla rete.

“Sendmail” fu uno dei primi Mail Transfer Agent ad implementare il protocollo SMTP. Fino al 2001 sono stati scritti almeno 50 programmi che implementano il protocollo come client (mittente del messaggio) o server (destinatario del messaggio)

2.1 Esempio di comunicazione SMTP

Quella che segue è una transazione SMTP:

Le righe inviate dal cliente sono precedute da C; Le righe inviate dal server sono precedute da S;

```
S: 220 www.example.com ESMTP Postfix
C: HELO mydomain.com
S: 250 Hello mydomain.com
C: MAIL FROM: <sender@mydomain.com>
S: 250 Ok
C: RCPT TO: <friend@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: messaggio di prova
C: From: sender@mydomain.com
C: To: friend@example.com
C:
C: Ciao,
C: questa è una prova.
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```

poiché SMTP è un protocollo testuale basato sulla codifica ASCII, non è permesso trasmettere direttamente testo composto con un diverso set di caratteri e tanto meno file binari, e la lunghezza massima di una riga impediscono la spedizione di file binari senza transcodifica. SMTP è un protocollo che permette soltanto di inviare messaggi di posta, ma non richiederli ad un server.

Per ricevere messaggi di posta, il client di posta ha bisogno di altri protocolli: POP3 e IMAP.

3. Il protocollo POP3

Il Pop (Post Office Protocol) è un protocollo che ha il compito di permettere tramite autenticazione, l'accesso ad un account di posta elettronica, presente su un host per scaricare le e-mail del relativo account. Il demone POP3 rimane in attesa della porta 110 dell'host per una connessione TCP da parte di un client. I messaggi di posta elettronica per essere letti devono essere scaricati sul computer, anche se è possibile lasciare una copia sull'host. Il protocollo POP3 non prevede alcun tipo di cifratura, quindi le password di autenticazione fra server e client passano in chiaro. Per risolvere questo problema è stata sviluppata l'estensione APOP che utilizza MD5.

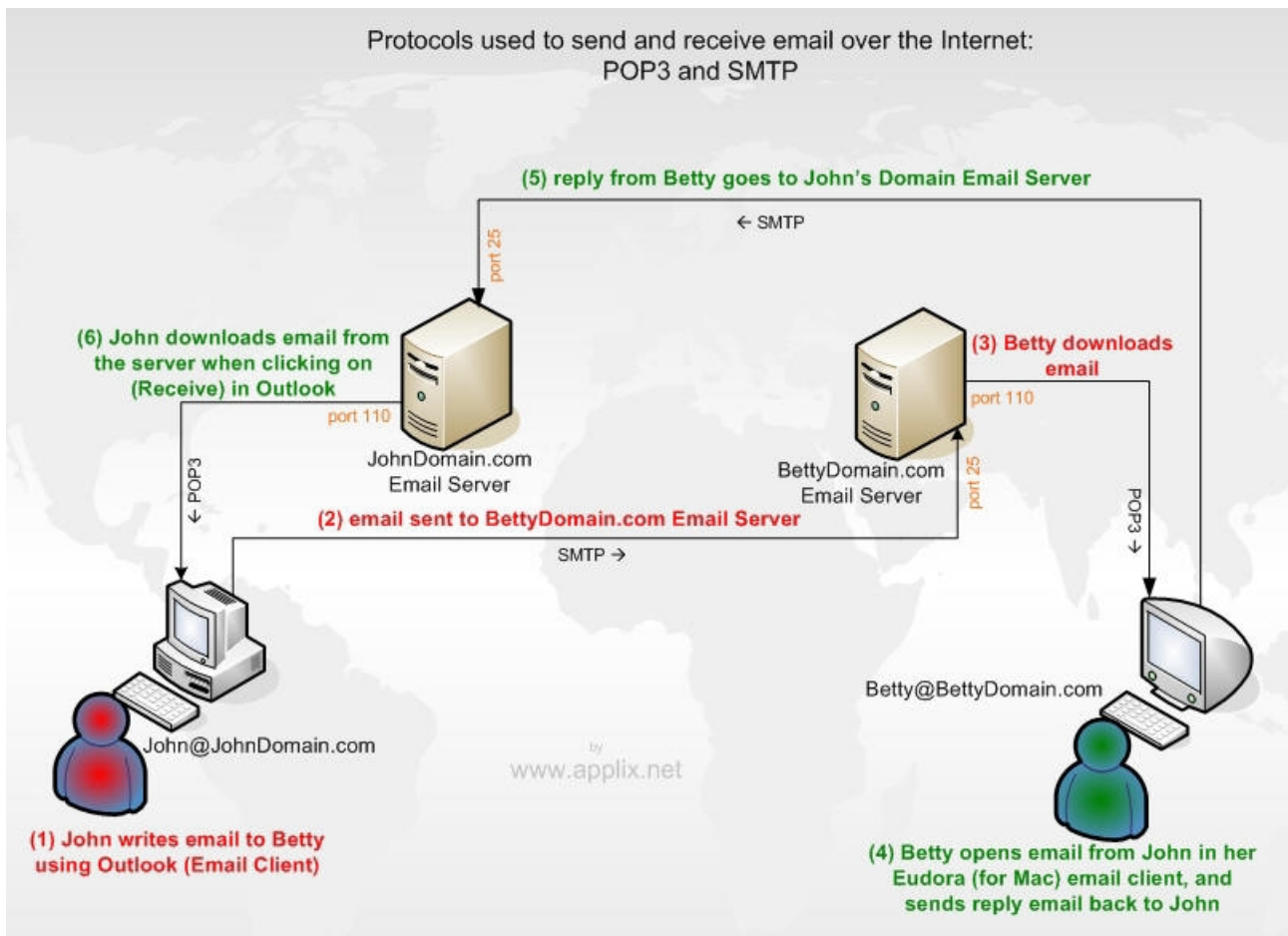
3.1 Esempio di comunicazione POP3:

Quella che segue è una transazione POP3:

Le righe inviate dal client sono precedute da C; le righe inviate dal server sono precedute da S;

```
S:+OK <22593.1129980067@example.com>
C:USER pippo
S:+OK
C:PASS pluto
S:+OK
C:LIST
S:+OK
  1 817
  2 124
  .
C:RETR 1
S:+OK
  Return-Path: <pippo@example.org>
  Delivered-To: pippo@example.org
  Date: Sat, 22 Oct 2005 13:24:54 +0200
  From: Mario Rossi <mario@rossi.org>
  Subject: xxxx
  Content-Type: text/plain; charset=ISO-8859-1
```

```
testo messaggio  
.  
C:DELE 1  
S:+OK  
C:QUIT  
S:+OK
```



Esempio di comunicazione, con invio e ricezione E-mail tra due utenti.

4. L'algoritmo MD5

L'MD5 (acronimo di Mesate Digest Algorithm) è un algoritmo per la crittografia dei dati a senso unico Realizzato da Ronald Rivest nel 1991 e standardizzato con RFC 1321.

Questo tipo di codifica prende in input una stringa di lunghezza arbitraria e ne produce un'altra a 128 bit (con lunghezza fissa di 32 valori esadecimali, indipendentemente dalla stringa di input), che può essere usata per calcolare la firma digitale dell'input.

La codifica avviene velocemente e si presuppone che l'output restituito sia univoco e che non ci siano possibilità, se non per tentativi, per risalire alla stringa di input (formata da due diverse stringhe) partendo dalla stringa di output (i cui possibili valori sono pari a 16 alla 32esima potenza).

La stringa di output è nota come MD5 Checksum o MD5 Hash.



Ronal Rivest

4.1 Storia e analisi della crittografia

I Message Digest sono una serie di algoritmi progettati dal prof. Ronald Rivest al MIT.

- Nel 1991, quando Had Dobbertin provò la debolezza dell'MD4, fu progettato da Ronald Rivest l'MD5, che rimpiazzò il suo predecessore in ambito di sicurezza.
- Nel 1993 Der Boer e Bosselaers ottennero un primo risultato trovando una pseudo-collisione dell'algoritmo MD5: cioè due diversi vettori di inizializzazione "i" e "j" con 4 bit di differenza tali che:
$$\text{MD5 compress}(i,x) = \text{MD5 compress}(j,x)$$
- Nel 1996 Dobbertin annunciò una collisione nella funzione di collisione MD5, ma anche se non presentava un attacco alla funzione hash MD5 completa, per molti crittografi fu sufficiente per andarlo subito a sostituire con il WHIRLPOOL, SHA-1 o RIPEMD-160. La cui dimensione dell'hash di 128 bit era abbastanza piccola per completare un Birthday -attack.
- Nel marzo 2004 iniziò il progetto distribuito da MD5CRK, con lo scopo di dimostrare che l'MD5 era un algoritmo insicuro, trovando una collisione e usando un birthday attack.
- Nell'agosto 2004 ebbe fine l'MD5CRK, quando fu trovata una collisione annunciata da Xiaoyun Wang.
- Nel marzo 2005 Arjen Lenstra, Xiaoyun Wang e Benne de Weger, dimostrarono la costruzione di due certificati X509 con differenti chiavi pubbliche, e lo stesso MD5 hash dimostrando una collisione nella pratica.
- Nel 18 marzo 2006 Vlastimil Klima pubblicò un algoritmo che riusciva a trovare una collisione in un minuto su un singolo computer, usando un metodo che chiamò "calls tunneling".

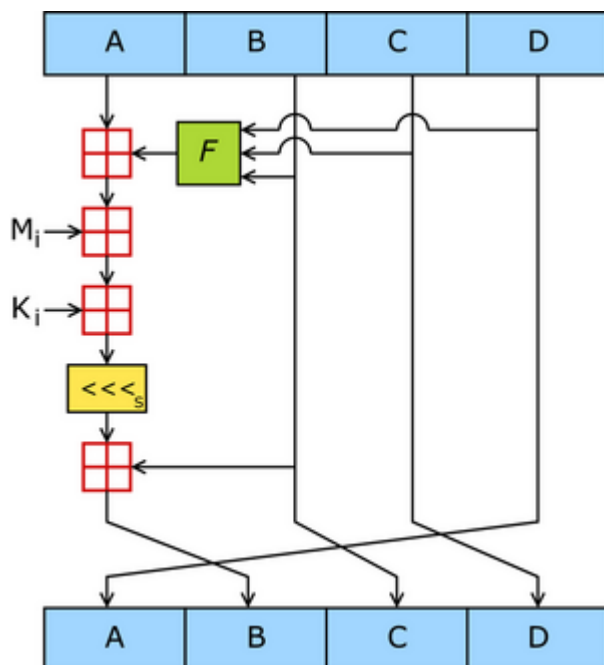
4. 2 Applicazione dell'MD5

La crittografia tramite l'algoritmo MD5 viene applicata in tutti i settori dell'informatica che lavorano con il supporto delle firme digitali, o che comunque trattano dati sensibili.

Ad esempio viene utilizzata per controllare che uno scambio di dati sia avvenuto senza perdite, semplicemente con il confronto tra la stringa prodotta dal file inviato e la stringa prodotta dal file ricevuto. Con lo stesso metodo si può anche verificare se il contenuto del file è cambiato.

E' diffuso anche come supporto per l'autenticazione degli utenti attraverso i linguaggi di scripting web server-side:

Durante la registrazione di un utente su un portale internet, la password scelta durante il processo verrà codificata tramite MD5 e la sua firma digitale verrà memorizzata nel database. Successivamente durante il login, la password immessa dell'utente, subirà lo stesso trattamento descritto precedentemente e verrà confrontata con la copia di possesso del server, per avere la certezza dell'autenticità.



qui è illustrato il funzionamento dell'MD5

5. Introduzione

Dopo SMTP (Simple Mail Transfer Protocol), un protocollo per la posta elettronica accettato a livello globale, che tuttavia presentava un limite intrinseco dal punto di vista della protezione, e la scelta dell'amministratore doveva necessariamente privilegiare o la protezione o la connettività, non potendo includere entrambe le caratteristiche, venne introdotto un nuovo protocollo: S/MIME.

Con l'introduzione di S/MIME, gli amministratori hanno potuto adottare una soluzione di posta elettronica più protetta e allo stesso tempo a livello globale. Caratterizzato a un livello di diffusione paragonabile a SMTP. Lo standard S/MIME presenta funzionalità più avanzate rispetto al protocollo precedente, poiché consente un'ampia connettività per la posta elettronica senza compromettere la protezione.

5.1 Evoluzione di S/MIME

Per comprendere lo standard S/MIME (Secure Multipurpose Internet Mail Extensions) è utile conoscere prima la sua evoluzione.

La prima versione di S/MIME viene sviluppata nel 1995 da un gruppo di fornitori di soluzioni di protezione. Inizialmente si trattava di una delle tante specifiche per la protezione dei messaggi, al pari di GPG (Pretty Good Privasi).

Ai tempi della prima versione di S/MIME non esisteva un unico standard riconosciuto per i messaggi protetti, ma più standard concorrenti.

Nel 1998 con la seconda versione di S/MIME, la situazione ha cominciato a cambiare. Infatti questa versione fu sottoposta all'ente IETF (Internet Engineering Task Force) per l'accettazione come standard internet. E in questo modo S/MIME è diventato uno degli standard più accreditati per la protezione dei messaggi. Questa utilizzava due specifiche RFC di IETF:

l'RFC 2311 che stabiliva lo standard per i messaggi

l'RFC 2312 che stabiliva lo standard per la gestione dei certificati

Queste due specifiche RFC costituivano il primo framework basato su standard

internet disponibile per la realizzazione di soluzioni integrate per la protezione di messaggi. E così è diventato lo standard per la protezione dei messaggi.

Nel 1999 per potenziare le funzionalità di S/MIME l'ente IETF ha proposto l'introduzione della terza versione di S/MIME, che comprende le seguenti specifiche:

l'RFC 2632 che si basava sull'RFC 2311 per definire ulteriori standard per i messaggi S/MIME

l'RFC 2633 che potenzia la specifica RFC 2312 per la gestione dei certificati

l'RFC 2634 che estende le funzionalità dello standard S/MIME mediante la funzione di servizi aggiuntivi quali le conferme e le etichette di protezione, nonché la tripla crittografia.

Con la terza versione il protocollo S/MIME ha ottenuto un riconoscimento a livello globale come standard della protezione dei messaggi, ed è supportato dai seguenti software della microsoft:

Microsoft Outlook 2000 (con SR-1) e versioni successive

Microsoft Outlook Express 5.01 e versioni successive

Microsoft Exchange 5.5 e versioni successive

5.2 Servizi offerti da S/MIME

S/MIME fornisce due servizi di protezione:

- Firme digitali
- Crittografia dei messaggi

Questi due servizi sono alla base della protezione dei messaggi S/MIME.

Ad essi sono correlati tutti gli altri concetti relativi alla protezione. Benché apparentemente complessa, la protezione dei messaggi è basata sulle firme digitali e sulla crittografia dei messaggi.

5.2.1 Firme Digitali

Le firme digitali sono il servizio più utilizzato da S/MIME. Come indicato dal nome, queste sono il corrispondente digitale delle firme tradizionali, con effetto legale, apposte ai documenti cartacei. Analogamente a quelle tradizionali, le firme digitali presentano le seguenti caratteristiche di protezione:

5.2.1.1 Autenticazione

Una firma ha la funzione di convalidare un'identità, consentendo ad ogni singola identità di distinguersi da tutte le altre e di provare la propria univocità. poiché nella posta elettronica basata su SMTP non è prevista l'autenticazione, non è possibile conoscere l'effettivo mittente di un messaggio. Per ovviare a questo problema è disponibile l'autenticazione tramite firma digitale, che consente al destinatario di un messaggio di verificare se quest'ultimo è stato effettivamente inviato dal presunto mittente.

5.2.1.2 Non ripudio

Il carattere di unicità di una firma impedisce al relativo proprietario di disconoscerla. Questa caratteristica è definita "non ripudio". l'autenticazione tramite firma consente di avvalersi della garanzia di non ripudio. Questo concetto è particolarmente diffuso nell'ambito dei contratti scritti. Un contratto firmato è un documento legalmente vincolante ed è quindi possibile disconoscere una firma autenticata. Le firme digitali svolgono questa stessa funzione, e soprattutto in determinati settori, sono sempre più riconosciuti come legalmente vincolanti, proprio come una firma su carta. poiché la posta elettronica basata su SMTP non fornisce alcun mezzo di autenticazione, non è in grado di garantire il non ripudio. Qualsiasi mittente può disconoscere la proprietà di un messaggio di posta elettronica SMTP.

5.2.1.3 Integrità dei dati

E' un servizio di protezione aggiuntivo risultante dalle operazioni che consentono l'utilizzo delle firme digitali. Con questo servizio, quando il destinatario di un messaggio di posta elettronica con firma digitale esegue la convalida della firma, ha la sicurezza che il messaggio ricevuto non sia stato modificato durante il trasferimento. Se dopo la firma il messaggio viene modificato, la firma non sarà più valida. In questo modo, le firme digitali forniscono un tipo di garanzia che le firme su carta non sono in grado di offrire, poiché un documento cartaceo può essere modificato anche dopo la firma.

Le firme digitali garantiscono l'integrità dei dati ma non la riservatezza. I messaggi con firma digitale vengono inviati come testo non crittografato analogamente ai messaggi SMTP, e possono essere letti da altri utenti. I messaggi con firma crittografata sono caratterizzati da un determinato livello di protezione in quanto sono codificati in base allo standard base 64 pur non essendo inviati come testo non crittografato.

Per proteggere quindi il contenuto della posta elettronica è necessario utilizzare la crittografia.

L'autenticazione, il non ripudio e l'autenticità dei dati sono le caratteristiche digitali delle firme digitali. Queste tre funzioni garantiscono al destinatario di un messaggio che questo è stato inviato dal mittente specificato e che non è stato modificato durante il trasferimento.

L'utilizzo della firma digitale comporta l'applicazione della firma al testo del messaggio di posta elettronica al momento dell'invio e la verifica di tale firma alla lettura del messaggio ricevuto.

5.2.1.4 Applicazione di una firma digitale e verifica della firma su un messaggio di posta elettronica



Per l'applicazione della firma al momento dell'invio del messaggio sono richieste informazioni che possono essere fornite solo dal mittente. Durante l'operazione di firma le informazioni fornite dal mittente vengono utilizzate per l'acquisizione del messaggio di posta elettronica e l'applicazione della firma digitale. Al termine dell'operazione viene generata la firma digitale effettiva, che viene quindi inclusa ed aggiunta nel messaggio al momento dell'invio.

applicazione di una firma digitale ad un messaggio di posta elettronica

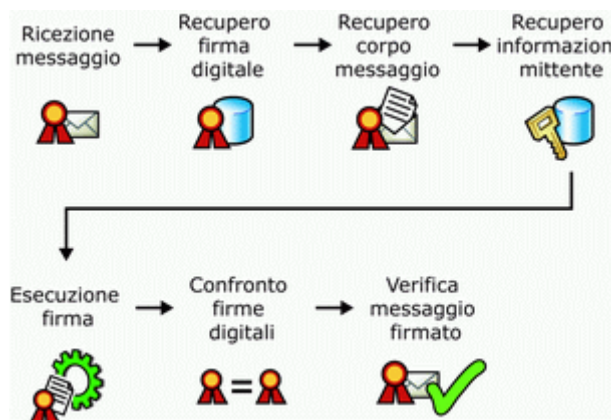


1. acquisizione del messaggio
2. recupero delle informazioni che identificano il mittente in maniera univoca
3. Applicazione al messaggio di una firma digitale generata in base alle informazioni univoche del mittente
4. Aggiunta della firma digitale al messaggio
5. Invio del messaggio

poiché quest'operazione richiede l'inserimento di informazioni univoche da parte del mittente, le firme digitali forniscono sia l'autenticazione che il non ripudio. Queste informazioni provano che il messaggio può essere inviato solo dal mittente. Però nessun meccanismo di protezione è perfetto. E' possibile che le informazioni univoche utilizzate dal mittente per l'applicazione delle firme digitali vengano acquisite da utenti non autorizzati, che possono così simulare l'identità del mittente. Tuttavia lo standard S/MIME è in grado di gestire questa situazione mostrando come non valide le firme non autorizzate.

Quando il messaggio di posta elettronica con firma digitale viene aperto dal destinatario, viene eseguita la procedura di verifica della firma. Questa procedura consiste nel recupero della firma digitale, del messaggio originale e nell'esecuzione di un'altra operazione di firma. Con conseguente generazione di un'altra firma digitale. Le due firme vengono poi confrontate. Se corrispondono si ha certezza che il messaggio proviene effettivamente dal mittente, altrimenti il messaggio viene contrassegnato come non valido.

Verifica di una firma digitale di un messaggio di posta elettronica



1. ricezione del messaggio
2. recupero della firma digitale del messaggio
3. recupero del messaggio
4. recupero delle informazioni identificative del mittente
5. operazioni di firma sul messaggio
6. confronto della firma digitale inclusa nel messaggio con quella generata al momento della ricezione
7. se le firme corrispondono il messaggio è valido

Le informazioni del mittente utilizzate per la verifica della firma, non corrispondono a quelle fornite dal mittente al momento della firma del messaggio. Le informazioni utilizzate dal destinatario sono correlate in modo da consentire a quest'ultimo di verificare l'autenticità delle informazioni univoche del mittente senza effettivamente conoscere il contenuto, garantendone così la riservatezza. Il processo di applicazione e verifica della firma digitale, consiste sostanzialmente nell'autenticare il mittente di un messaggio di posta elettronica e di determinare l'integrità dei dati all'interno del messaggio firmato.

L'autenticazione dei mittenti fornisce funzionalità aggiuntive di non ripudio che impedisce ai mittenti autenticati di disconoscere la proprietà di un messaggio inviato. Le firme digitali forniscono una soluzione ai problemi di identità e manomissione dei dati, che possono verificarsi con la posta elettronica internet basata su SMTP.

5.2.2 Crittografia dei messaggi

La crittografia dei messaggi offre una soluzione per la riservatezza delle informazioni. I messaggi di posta elettronica internet basati su SMTP, non sono protetti. Possono essere intercettati e letti da qualsiasi utente durante la fase di trasferimento o nell'area stessa in cui sono archiviati.

Questi problemi non si verificano se si utilizza lo standard S/MIME.

La crittografia fornisce il metodo per modificare le informazioni in modo da impedire la lettura e la comprensione finché non viene ripristinato il formato originale, quindi ad uno dei punti più deboli della posta elettronica su internet.

La crittografia dei messaggi fornisce due servizi di protezione specifici:

5.2.2.1 riservatezza

La crittografia consente di proteggere il contenuto di un messaggio di posta elettronica, rendendolo accessibile solo al destinatario specificato. In questo modo viene garantita la massima riservatezza del messaggio durante il trasferimento o nell'area di archiviazione.

5.2.2.2 Integrità dei dati

Analogamente alle firme digitali, anche le operazioni di crittografia dei messaggi, garantiscono l'integrità dei dati.

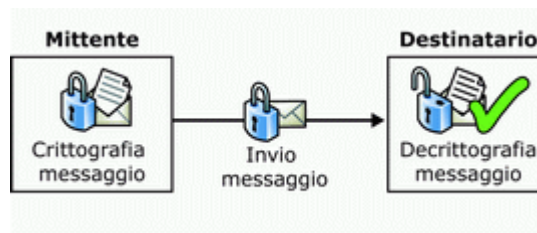
La crittografia dei messaggi garantisce invece la riservatezza dei dati ma non esegue l'autenticazione del mittente. Un messaggio crittografato senza firma digitale può essere soggetto a problemi di sostituzione di identità, come un messaggio non crittografato. Allo stesso modo la crittografia non garantisce il non ripudio, poiché questa caratteristica è il risultato diretto dell'autenticazione.

Inoltre l'integrità dei dati di un messaggio crittografato è garantito solo dal momento dell'invio. Non sono quindi disponibili informazioni riguardanti il mittente del messaggio e per provare l'identità del mittente, al messaggio deve essere applicata una firma digitale.

La riservatezza e l'integrità dei dati costituiscono le caratteristiche principali della crittografia dei messaggi . Queste due funzioni specificano infatti, che solo il destinatario specificato sarà in grado di visualizzare il messaggio , e che il messaggio ricevuto corrisponde esattamente a quello inviato.

La crittografia ha lo scopo di rendere illeggibile il testo dei messaggi prima che questi vengano inviati attraverso la rete. Al termine della ricezione il testo viene reso nuovamente leggibile tramite un'operazione di decrittografia.

5.2.2.3 operazioni di crittografia e decrittografia di un messaggio di posta elettronica



L'operazione di crittografia eseguita al momento dell'invio acquisisce il messaggio di posta elettronica e lo rende illeggibile, utilizzando le informazioni relative al destinatario specificato. Il messaggio crittografato sostituisce quello originale e viene poi inviato al destinatario.

Crittografia di un messaggio di posta elettronica



1. acquisizione del messaggio
2. . recupero delle informazioni che identificano il messaggio in maniera univoca
3. Crittografia del messaggio in base alle informazioni relative al destinatario
4. sostituzione del testo originale del messaggio con quello crittografato
5. Invio del messaggio

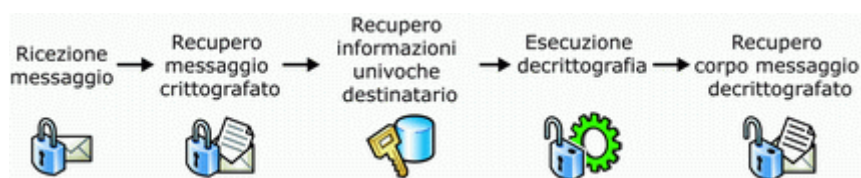
poiché richiede l'utilizzo di informazioni univoche relative al destinatario, la crittografia dei messaggi garantisce la riservatezza dei dati. Solo il destinatario specificato dispone delle informazioni necessarie per decrittografare il messaggio, e quindi solo questo utente è in grado di visualizzarlo.

Le informazioni del destinatario utilizzate per la crittografia del messaggio non corrispondono a quelle fornite dal destinatario per l'operazione di decrittografia. Le informazioni visualizzate dal mittente sono correlate in modo da consentire a quest'ultimo di verificare l'autenticità delle informazioni univoche del destinatario, senza effettivamente conoscere il contenuto garantendone così la riservatezza.

Quando il destinatario apre un messaggio crittografato viene eseguita un'operazione di decrittografia: vengono recuperati sia il messaggio crittografato che le informazioni univoche del destinatario, da utilizzare per la decrittografia del messaggio. Per effetto di quest'operazione, viene restituito il messaggio decrittografato, che risulta quindi visibile al destinatario.

Se il messaggio non è stato modificato durante il trasferimento, l'operazione di crittografia non riuscirà.

Decrittografia di un messaggio di posta elettronica



1. ricezione del messaggio
2. recupero del messaggio crittografato
3. recupero delle informazioni che identificano il destinatario in maniera univoca
4. decrittografia del messaggio crittografato in modo da generare un messaggio decrittografato in base alle informazioni univoche del destinatario
5. recapito del messaggio non crittografato al destinatario

Il processo di crittografia e decrittografia garantisce la riservatezza dei messaggi di posta elettronica, e anche questo processo consente di risolvere uno dei problemi più deboli della posta elettronica internet.

6. Interazione delle firme digitali con la crittografia dei messaggi

Le firme digitali e la crittografia dei messaggi non si escludono reciprocamente. Ciascuno di questi servizi consente di risolvere problemi specifici di protezione. Le firme digitali forniscono il supporto per l'autenticazione e il non ripudio, mentre la crittografia garantisce la riservatezza dei messaggi.

In considerazione dei diversi ruoli svolti, entrambi i servizi sono normalmente richiesti nell'ambito di una stessa strategia di protezione dei messaggi.

L'integrità di questi due servizi è importante poiché ciascuno si interessa di un diverso aspetto della relazione mittente destinatario.

Le firme affrontano le problematiche relative ai mittenti, mentre la crittografia le problematiche relative ai destinatari.

Quando le firme digitali e la crittografia dei messaggi vengono utilizzati insieme, gli utenti possono beneficiare di entrambi i servizi, e la modalità di gestione e di elaborazione dei due servizi rimane invariata.

6.1 Applicazione di una firma digitale e crittografia di un messaggio di posta elettronica



1. acquisizione del messaggio
2. recupero delle informazioni che identificano il mittente in maniera univoca
3. recupero delle informazioni che identificano il destinatario in maniera univoca
4. applicazione al messaggio di una firma generata in base alle informazioni univoche del mittente
5. aggiunta della firma digitale al messaggio
6. crittografia del messaggio in base alle informazioni relative al destinatario
7. sostituzione del messaggio originario con quello crittografato
8. invio del messaggio

Decrittografia del messaggio di posta elettronica e verifica di una firma digitale



1. ricezione del messaggio
2. recupero del messaggio crittografato
3. recupero delle informazioni che identificano il destinatario in maniera univoca
4. decrittografia del messaggio decrittografato in modo da generare un messaggio non crittografato in base alle informazioni univoche del destinatario
5. restituzione del messaggio non crittografato
6. recapito del messaggio non crittografato al destinatario
7. recupero della firma digitale dal messaggio non crittografato
8. recupero delle informazioni identificative del mittente
9. applicazione al messaggio non crittografato di una firma generata in base alle informazioni del mittente

10. confronto della firma digitale inclusa nel messaggio con quella generata al momento della ricezione
11. se le firme corrispondono il messaggio è valido

7. Messaggi con tripla crittografia

Uno dei miglioramenti apportati nella terza edizione dello standard S/MIME, è rappresentato dalla tripla crittografia.

Un messaggio S/MIME con tripla crittografia è un messaggio firmato, crittografato, quindi nuovamente firmato. Questo ulteriore livello di crittografia fornisce una protezione avanzata dei messaggi.

Le firme digitali e la crittografia dei messaggi sono due servizi complementari in grado di fornire una protezione completa ai problemi di protezione che interessano la posta elettronica Internet basata su SMTP.

8. Conclusioni

Questo progetto mi ha messo a conoscenza di tante cose che non sapevo.

Spesso noi studenti per la fretta di darci le materie e finire prima il corso di laurea non approfondiamo gli argomenti, tranne se è oggetto d'esami come in questo caso, e mi sono accorta invece che è una cosa abbastanza utile.

Adesso sono a conoscenza del vero mondo della posta elettronica che prima vedevo come un semplice scambio di messaggi via internet, senza naturalmente sapere tutto quello che c'è dietro.

Infatti un normale utente vede proprio questo, una semplice interfaccia grafica di un editor di testo dove scrivere per poi inviare un messaggio e allo stesso modo riceverlo.

Così come tutti sembrerebbe una banalità, e invece ci sono dietro un sacco di controlli, algoritmi e protocolli che ne permettono il funzionamento e la sicurezza.

9. Riferimenti

http://it.wikipedia.org/wiki/Posta_elettronica

<http://it.wikipedia.org/wiki/SMTP>

http://it.wikipedia.org/wiki/Post_Office_Protocol

<http://it.wikipedia.org/wiki/MD5>

<http://www.skrenta.com/2007/08/>

<http://www.tech-faq.com/lang/it/s-mime.shtml>

<http://security.fi.infn.it/documenti/cripmail.html>

[http://technet.microsoft.com/it-it/library/aa995740\(EXCHG.65\).aspx](http://technet.microsoft.com/it-it/library/aa995740(EXCHG.65).aspx)