Servizi Applicativi su Internet

SMTP/POP/IMAP

La posta elettronica

Pierluigi Gallo, Domenico Garlisi, Fabrizio Giuliano

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

E-mail - Indice

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

- Introduzione
- Formato del messaggio
- Server
- Protocolli
- Comandi SMTP
- MIME
- Sicurezza

E-mail - Introduzione

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Che cos'è l'e-mail?
  - Tramite la posta elettronica è possibile scambiarsi in tempi estremamente ridotti sia messaggi di puro testo contenente allegati in vario formato
  - Avere un account di posta elettronica vuol dire avere un nome e un indirizzo a cui farvi inviare e da cui spedire posta.
  - Ci sono due principali modi per inviare e ricevere un e-mail: guardarla via web attraverso il vostro browser (Firefox, …) o scaricarla sulla propria postazione remota attraverso un client di posta elettronica (Thunderbird, …) in grado di parlare con il server e di recapitarvi le mail sul vostro pc.

E-mail – Formato messaggio

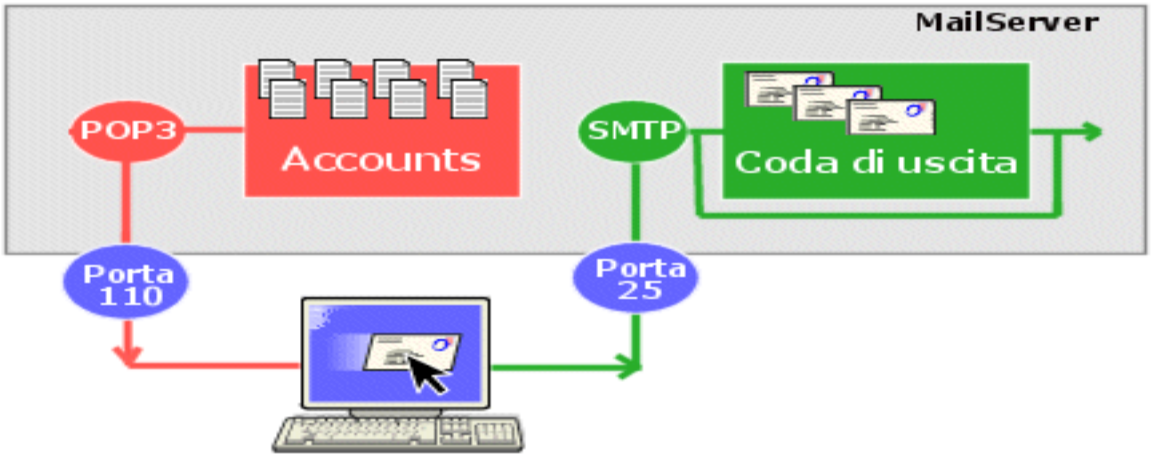
- E' necessario che il documento venga opportunamente codificato in caratteri ASCII, a 7 bit

- I messaggi sono costituiti da diverse parti:
  - il mittente
    - Per individuare mittenti e destinatari dei messaggi, si utilizzano gli indirizzi E-mail, che hanno l'aspetto seguente: mario.rossi@libero.it, dove mario.rossi è il nome che identifica l'utente, mentre libero.it identifica l'indirizzo del fornitore del servizio sul quale si trovano le mailbox.
  - Il destinatario
  - La data
  - L'oggetto
  - Il corpo del messaggio

UNIVERSITÀ DEGLI STUDI DI PALERMO

E-mail - Server

- Il sistema di posta elettronica e' basato su due server/protocolli
  - SMTP Server (Simple Mail Tranfer Protocol)
    - Gestisce le e-mail da spedire.
  - POP3 Server (Post Office Protocol)
    - Gestisce le e-mail in ricezione.
  - Per convenzione, ognuno dei protocolli usati usa una porta specifica:
    - SMTP usa la porta 25
    - POP3 usa la porta 110



E-mail - Passaggi necessari per l'invio

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Elementi e funzioni coinvolte nello scambio di un messaggio
  - Connessione al server SMTP usando la porta 25.
  - Trasferimento dell'indirizzo del mittente e di quello del destinatario nonchè il titolo del messaggio e il suo contenuto.
  - Il server SMTP prende l'indirizzo del destinatario jsmith@mindspring.com e lo scompone nel nome della mail box jsmith e nel nome del dominio mindspring.com.
  - Se il nome del dominio corrisponde a quello del mittente, il server SMTP trasferisce direttamente il messaggio al POP3 locale usando un piccolo programma chiamato delivery agent.
  - Per risolvere il nome del dominio e stabilire quale sia l'indirizzo IP corrispondente al nome mindspring.com il server deve rivolgersi al server DNS.
  - Nel caso più semplice il server SMTP locale si connetterà direttamente al server SMTP di mindspring.com, altrimenti si connetterà ad un altro SMTP.
  - Alla fine il messaggio verrà recapitato al server POP3 che lo depositerà nella mailbox di jsmith.

Email – Protocollo di comunicazione

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Il protocollo di comunicazione per inviare una email e' specificato nella RFC
- in figura si ha una transazione SMTP valida. Le righe inviate dal client sono precedute da "C:", mentre quelle inviate dal server da "S:“

```
S: 220 www.example.com ESMTP Postfix
C: HELO mydomain.com
S: 250 Hello mydomain.com, pleased to meet you
C: MAIL FROM: <sender@mydomain.com>
S: 250 sender@mydomain.com ... Sender ok
C: RCPT TO: <friend@example.com>
S: 250 friend@example.com ... Recipient Ok
C: DATA
S: 354 End data with "." on a line by itself
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
```

Inviare una mail da telnet


```
telnet smtp.tiscali.it 25
Trying 213.205.33.13...
Connected to smtp.tiscali.it.
Escape character is '^]'.
220 joe.mail.tiscali.it ESMTP Service ready
250 joe.mail.tiscali.it
250 MAIL FROM:<mittente@tiscali.it> OK
250 RCPT TO:<destinatario@gmail.com> OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Subject: mail di prova da telnet

Questo e' il corpo della mail
altra riga
termino la mail inviando un punto su una nuova riga
.
250 <4D08E71A007ED204> Mail accepted
```

E-mail – Comandi SMTP

- HELO provider.it
  Questo comando serve per salutare il server SMTP il quali ci riconoscerà dal nostro IP

- MAIL FROM: <nick_proprio@provider.it>
  Questo comando serve per indicare l'indirizzo email del mittente.

- RCPT TO: <nick_destinatario@provider.it>
  Questo comando serve per indicare l'indirizzo email del destinatario.

- DATA
  A questo comando segue una riga vuota che va riempita con la prima riga del nostro messaggio

- Per ulteriori informazioni sul protocollo SMTP e su quello POP3, la cosa migliore è fare riferimento ai documenti RFC che spiegano in dettaglio i protocolli, ad esempio:
  - Per SMTP : RFC 5321 (la RFC 2821 e' obsoleta)
    - http://www.ietf.org/rfc/rfc5321.txt
  - Per POP3 : RFC 1939 (Standard) Updated byRFC 1957, RFC 2449
    - http://www.ietf.org/rfc/rfc1939.txt
    -

E-mail – IMAP

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Il protocollo IMAP (Internet Message Access Protocol) è un protocollo alternativo al protocollo POP3 ma che offre molte più possibilità :
  - IMAP permette di gestire più accessi simultanei
  - IMAP permette di gestire più caselle postali
  - IMAP permette di smistare la posta secondo più criteri

E-mail - MIME

UNIVERSITÀ DEGLI STUDI DI PALERMO

- MIME (Multipurpose Internet Mail Extensions) è uno standard generico per il formato dei documenti scambiati sulla rete Internet tramite posta elettronica, che rappresenta una estensione del protocollo SMTP.
  - Una delle più importanti RFC di riferimento è la numero 2045
    - http://www.faqs.org/rfcs/rfc2045.html

E-mail - MIME

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Specifica un nuovo modo di codifica dei dati accessorio a quello principale, utilizzato per permettere loro di passare attraverso tutti i meccanismi di trasporto della posta elettronica, e di supportare alfabeti relativi a più lingue.
  - La codifica viene definita attraverso un opportuno campo del protocollo e secondo le seguenti tipologie:
    - 7bit, 8bit, binary, quoted-printable, Base64, x-token

- MIME permette di includere molti tipi di file e documenti nei messaggi email.
  - Nello specifico, i messaggio MIME possono contenere
    - testo
    - immaggini
    - audio
    - video
    - altro

E-mail - MIME

- Un documento MIME contiene una testata in cui si trovano i seguenti campi:
  - MIME version
    - Identifica la versione
  - Content-Type
    - Specifica il tipo ed il sottotipo di dati contenuti nel messaggio
  - Content-Transfer-Encoding
    - Specifica un modo di codifica dei dati
  - Content-ID
    - Identifica il messaggio in modo univoco
  - Content-Description
    - Descrizione testuale del contenuto del messaggio

E-mail - Sicurezza

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Tutte le comunicazioni relative ai protocolli precedentemente visti normalmente avvengono in chiaro, attraverso tutti i nodi che attraversano, e senza alcuna protezione, la criticità del servizio di posta elettronica è dovuta a:
  - Protocolli di trasmissione/ricezione
  - Passaggio per diversi server

E-mail - Sicura

UNIVERSITÀ DEGLI STUDI DI PALERMO

- IN TRASMISSIONE (SMTP)
- NON prevede NESSUNA forma di autenticazione

- IN RICEZIONE (POP3 e IMAP)
- Sebbene prevede l'autenticazione lo scambio dei messaggi avviene IN CHIARO
  - Facile leggere sia la password che i dati.

E-mail - Sicurezza

- Per risolvere questo problema, si può optare per
  - Scaricare e inviare la posta in maniera cifrata
    - connessioni protette con l'ISP tramite SMTP+SSL e POP+SSL
- Utilizzare protocolli opportuni come:
  - S/MIME
    - Necessita di una Certification Authority
  - PGP
    - Usa un sistema web of trust

E-mail - S/MIME (1)

- Sviluppato da RSA nel 1996, S/MIME (Secure/ Multipurpose Internet Mail Extensions) è ampiamente riconosciuto e utilizzato per la messaggistica.

- La tecnologia si basa sul Public Key Cryptographic Standard (PKCS), che offre interoperabilità per quanto riguarda l'utilizzo della crittografia.
- Due caratteristiche chiave di S/MIME sono:
  - la firma digitale
  - la busta digitale (integrità del messaggio e riservatezza del messaggio).

E-mail - S/MIME (2)

UNIVERSITÀ DEGLI STUDI DI PALERMO

- PKCS public key cryptography standards è un insieme di standard per l'implementazione di crittografia a chiave pubblica, abbiamo:
  - PKCS #1: RSA Encryption
  - PKCS #7: Cryptographic Message Syntax
  - PKCS #10 : Certification Request Syntax

- S/MIME v3 utilizza CMS (Cryptographic Message Syntax) che è derivato da PKCS #7

E-mail - S/MIME - SERVIZI

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

- S/MIME offre i seguenti servizi:

- Compressione
- Autenticazione
- Confidenzialità

E-mail - S/MIME - SERVIZI

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Compressione
  - Si attua al fine di risparmiare tempo e spazio per la firma
  - La compressione è effettuata facendo l'hash del messaggio (message digest) utilizzando gli algoritmi : SHA-1 e MD5. Entrambi gli algoritmi prendono in input un messaggio di lunghezza arbitraria e restituiscono in output un messaggio di 128 bit (MD5) oppure 160 bit (SHA-1).

E-mail - S/MIME - SERVIZI

- Autenticazione
  - Il messaggio viene compresso con una funzione hash e fornisce un message digest di lunghezza costante
    - Algoritmi usati: SHA-1 (160) o MD5 (128)
  - Il message digest viene firmato con la chiave privata del mittente
    - Schema di firma usato:
      - RSA per S/MIME v2
      - DSS per S/MIME v3
  - Per poter firmare un messaggio, il mittente deve avere un certificato digitale che stabilisce il legame tra la chiave pubblica e l'identità dell'utente (standard X.509)

E-mail - S/MIME - SERVIZI

- Confidenzialità
  - Il messaggio è cifrato con un algoritmo a chiave privata
  - Algoritmi usati: RC2, DES, EDE-DES
  - La chiave (session key) è generata dal mittente per ogni messaggio
  - La session key è poi cifrata con la chiave pubblica del destinatari
  - Algoritmo usato:
    - RSA per S/MIME v2
    - Diffie-Hellman per S/MIME v3

E-mail - S/MIME compatibilità v2 e v3

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Gli agenti S/MIME v3 dovrebbero cercare di avere la più grande interoperabilità possibile con gli agenti S/MIME v2

- S/MIME v3 prevede tutti gli algoritmi supportati da S/MIME versione 2

E-mail - S/MIME MESSAGGIO

- I messaggi S/MIME sono una combinazione di corpi MIME ed oggetti PKCS
- I dati che devono essere resi sicuri sono sempre entità MIME canoniche
  - Rappresentazione unica e non ambigua dell'entità
- S/MIME fornisce un formato per i dati solo imbustati (solo cifrati), diversi formati per dati solo firmati, e diversi formati per dati firmati e imbustati

S/MIME - Codifica di Trasferimento

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Le implementazioni S/MIME devono essere capaci di trattare con oggetti MIME binari

- I dati trasmessi sull'infrastruttura internet standard SMTP o un altro trasporto che è vincolato a testo a 7-bit deve avere una codifica di trasferimento applicata in modo da essere rappresentata come testo a 7-bit

- Le entità come testo ad 8-bit e dati binari possono essere codificati con codifica di trasferimento quoted-printable o base-64

S/MIME - Quoted-printable e Base64

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Quoted-printable
  - Questo valore significa che un'operazione di codifica è stata applicata ai dati in modo da trasformare il messaggio in una sequenza di caratteri ASCII

- base-64
  - Con questa operazione il messaggio viene trasformato in una sequenza di caratteri appartenenti ad un sottogruppo del set di caratteri ASCII (le lettere maiuscole da "A" a "Z", quelle minuscole da "a" a "z", i numeri da "0" a "9", il carattere "+" ed il carattere "\“)

S/MIME - Tipi di contenuto PKCS#7

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Il formato del messaggio PKCS #7 permette una grossa varietà di opzioni sia per il contenuto e che per il supporto degli algoritmi

- PKCS #7 definisce sei tipi di contenuto distinti:
  - signedData
  - envelopedData
  - signedAndEnvelopedData
  - digestedData
  - encryptedData

S/MIME Il messaggio in ricezione

- Quando un messaggio S/MIME è ricevuto i servizi di sicurezza sul messaggio sono rimossi e il risultato è l'entità MIME

- L'entità MIME è tipicamente passata ad un agente MIME, essa è decodificata e presentata all'utente o all'applicazione ricevente

E-mail - PGP

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Pretty Good Privacy (PGP) è un programma di crittografia a chiave pubblica che utilizza dei cifrati con licenza open source per firmare e crittografare i messaggi come:
  - RSA
  - IDEA
  - MD5

- Anche in questo caso vengono garantiti I servizi di:
  - Compressione
  - Autenticazione
  - Confidenzialità

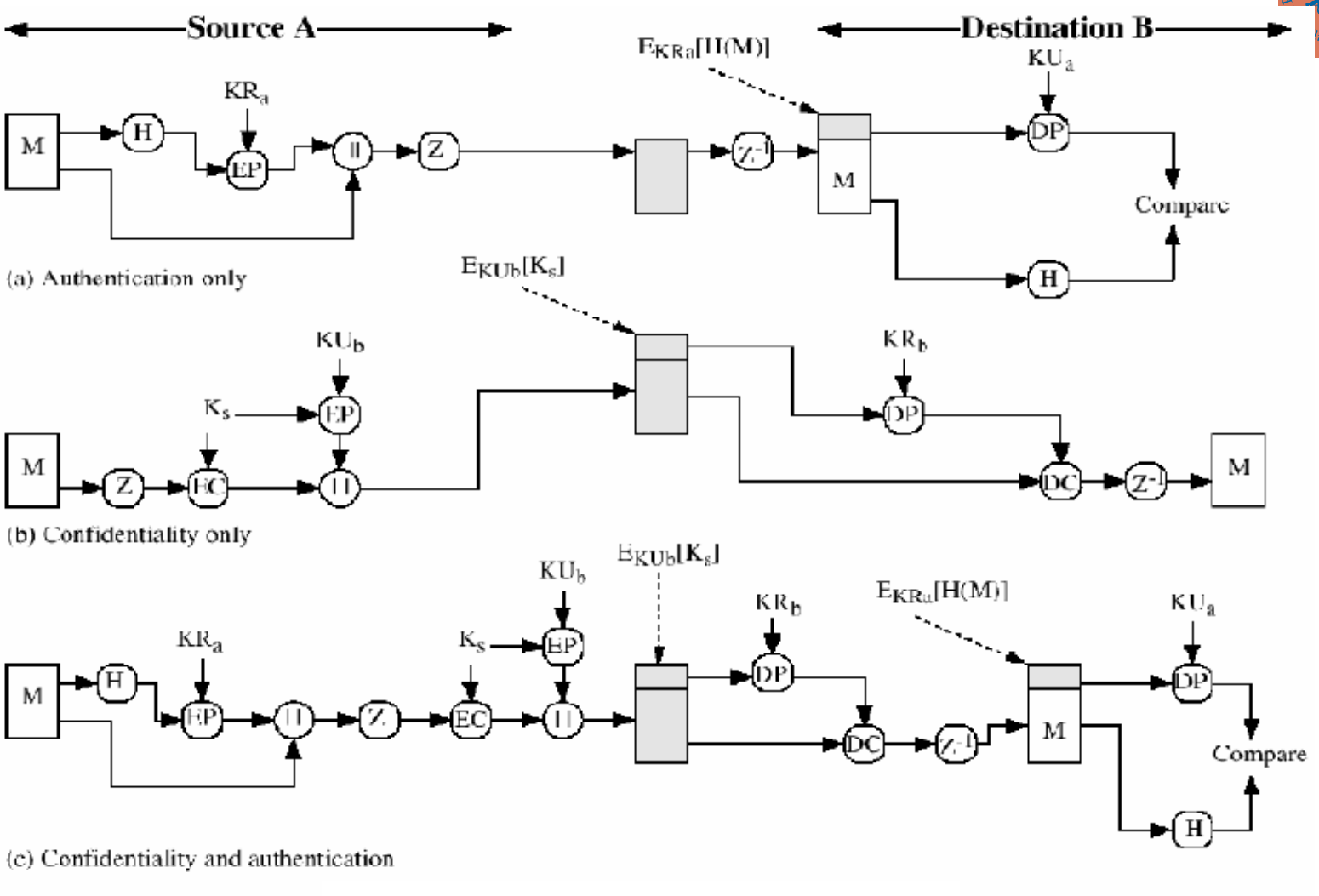
E-mail - PGP

- Autenticazione
- Il sender crea il messaggio
  - Viene usato SHA-1 per generare un hash a 160 bit del messaggio
  - Il messaggio viene firmato con RSA usando la chiave privata del sender e la firma è aggiunta al messaggio
- Il receiver usa RSA con la chiave pubblica del sender per decriptare e recuperare l'hash
- Il receiver verifica il messaggio ricevuto calcolando
- il suo hash e confrontandolo con quello ricevuto

E-mail - PGP

- Confidenzialità
- Il sender genera il messaggio nonché un numero random di dimensione adatta da usare come chiave di sessione
- Il sender cripta il messaggio con la chiave di sessione
- Il sender cripta, RSA, la chiave di sessione con la chiave pubblica del recipient e la aggiunge al messaggio
- Il receiver, usando RSA e la sua chiave privata, recupera la chaive di sessione
- Il receiver decripta il messaggio usando la chiave di sessione

E-mail - PGP


Source A
Destination B
M
H
EP
Z
KRa
EKRa[H(M)]
Z-1
KUa
DP
Compare
(a) Authentication only
EKUb[Ks]
KUb
Ks
EC
KRb
DC
(b) Confidentiality only
(c) Confidentiality and authentication

Email – PGP – Key management

UNIVERSITÀ DEGLI STUDI DI PALERMO

- PGP, piuttosto che basarsi sulle CA, fa sì che ogni utilizzatore sia la CA di se stesso
- Può firmare le chiavi di utilizzatori che conosce direttamente
- PGP ha diffuso il concetto di "web of trust"
- Possibile avere fiducia alle chiavi firmate da altri se si dispone di una catena di firme fino a questi
- Le raccolte di chiavi (key ring) includono i trust indicators

E-mail S/MIME vs PGP

UNIVERSITÀ DEGLI STUDI DI PALERMO

- Sono funzionalmente equivalenti tranne per un aspetto rilevante: il modello di fiducia
  - La differenza fondamentale tra i due sistemi è che mentre PGP utilizza una gestione "utente-centrica" delle chiavi pubbliche (il cosiddetto web of trust), S/MIME impiega una struttura gerarchica di certificazione (le Certification Authorities o CA)
- S/MIME ha un modello di fiducia gerarchico in cui delle "autorità di certificazione" certificano l'identità degli utenti
- PGP adotta un sistema a rete in cui gli utenti si certificano a vicenda

E-mail S/MIME vs PGP

- S/MIME e PGP non sono specifiche compatibili fra di loro

- La maggior parte dei prodotti di posta elettronica supporta l'uno o l'altro, ma c'è la tendenza di supportarli entrambi :
  - Si parla anche di unificare i due prodotti in uno standard unico