



# Laboratorio di sicurezza dei protocolli di rete - lab\_001

2 Febbraio 2007

**Master in progettazione e gestione di  
sistemi di rete - III edizione**



Dipartimento di  
Informatica



# Agenda lab 001

LAB\_001 Sicurezza dei Protocolli



Dipartimento di  
Informatica

# Agenda lab 001

LAB\_001 Sicurezza dei Protocolli

- La posta elettronica
  - servizi in plain-text
  - servizi con SSL



Dipartimento di  
Informatica

# Agenda lab 001

- ❑ La posta elettronica
  - ❑ servizi in plain-text
  - ❑ servizi con SSL
  
- ❑ Crittografia Personale
  - ❑ GPG
  - ❑ S/MIME



# Agenda lab 001

- La posta elettronica
  - servizi in plain-text
  - servizi con SSL
  
- Crittografia Personale
  - GPG
  - S/MIME



# SMTP

Simple Mail Transfer Protocol è utilizzato dai diversi server di posta per parlare tra loro.

Utilizza la porta 25/TCP e viene definito dall'RFC 2821.



# SMTP con telnet

```
coniglio:~ mayhem$ telnet mail.tin.it 25
```

```
Trying 62.211.72.20...
```

```
Connected to mail.tin.it.
```

```
Escape character is '^]'.  
220 vsmtplib3.tin.it ESMTP Service (7.2.072.1) ready
```

```
helo alba.st
```

```
250 vsmtplib3.tin.it
```

```
mail from: <alessio@alba.st>
```

```
250 MAIL FROM:<alessio@alba.st> OK
```

```
rcpt to: <mayhem@recursiva.org>
```

```
250 RCPT TO:<mayhem@recursiva.org> OK
```



# SMTP con telnet [2]

data

354 Start mail input; end with <CRLF>.<CRLF>

Subject: Test invio mail...

questo è il corpo della mail ...

.

250 <4589478001439900> Mail accepted

quit

221 vsmtplib3.tin.it QUIT

Connection closed by foreign host.

coniglio:~ mayhem\$

# MX record

Un server SMTP viene associato ad un dominio tramite il campo MX nel DNS.

Posso avere più MX, con diverse priorità, così da poter gestire enormi moli di posta.





# MX e dig

```
coniglio:~ mayhem$ dig mx recursiva.org
```

```
[...]
```

```
:: ANSWER SECTION:
```

```
recursiva.org.      67626  IN     MX     20 smtp.recursiva.org.
```

```
[...]
```

```
:: ADDITIONAL SECTION:
```

```
smtp.recursiva.org. 67626  IN     A      85.42.100.222
```

# Prelevare la posta

Il servizio che gestisce SMTP riceve la posta e la immagazzina su disco (formati mbox, maildir) o in un database.

Gli utenti poi accederanno alla propria mailbox attraverso un servizio POP o IMAP.

Post Office Protocol usa la porta 110/TCP e viene definito dalla RFC 1939.

L'utilizzo di default prevede lo spostamento delle mail dallo spool del server al client stesso.



# IMAP

Internet Message Access Protocol  
usa la porta 143/TCP ed è definito  
dalla RFC 3501.

L'accesso via IMAP conserva invece  
le mail sul server.



Dsniff è una suite di programmi per intercettare password, file e per portare attacchi di tipo MITM.



# Configuriamo il DNS

Per ogni PC creeremo:

- ➔ un dominio gammaXX.it
- ➔ un campo A smtp.
- ➔ un campo MX
- ➔ creare un CNAME pop.





- ➔ Avviare VMware
- ➔ Eseguire la macchina virtuale “Linux”
- ➔ Installare postfix, dovecot, dsniff
- ➔ creare un account
- ➔ configurare l’infrastruttura di gestione della posta
- ➔ Eseguire la macchina virtuale “Windows”
- ➔ Installare thunderbird
- ➔ Configurare un account per scaricare la posta
- ➔ Intercettare le password con dsniff

```
# dsniff -m
```

# Agenda lab 001

- La posta elettronica
  - servizi in plain-text
  - servizi con SSL
  
- Crittografia Personale
  - GPG
  - S/MIME



# SSL, TLS

Gli stessi servizi possono utilizzare Secure Socket Layer o Transport Layer Security per proteggere la comunicazione.

Le porte diventano 465/TCP per SMTPS, 995/TCP per POP3S e 993/TCP per IMAPS.



# Generare un certificato

Tramite le librerie openssl è possibile generare un certificato self-signed.

Tale certificato proteggerà adeguatamente la connessione, ma non sarà riconosciuto dal client come “fidato”.





creare il certificato per il server smtp:

```
# openssl req -new -newkey rsa:1024 \  
-days 365 -nodes -x509 -keyout \  
smtp.gammaXX.it.pem \  
-out smtp.gammaXX.it.pem
```

creare il certificato per il server pop3.

# Verificare il traffico

- Verificare con wireshark la possibilità di leggere il corpo della mail
- Riconfigurare thunderbird per usare SSL.
- Verificare con dsniff la non intercettabilità delle password.
- Verificare con wireshark l'impossibilità di visualizzare le mail durante il flusso SMTP.



# Agenda lab 001

- La posta elettronica
  - servizi in plain-text
  - servizi con SSL
  
- Crittografia Personale
  - GPG
  - S/MIME



# Riservatezza delle mail

Abbiamo verificato che attraverso SSL è possibile proteggere il traffico. Tuttavia le mail, una volta sul server, vengono conservate in chiaro.





- Leggere lo spool di mail da command line.

# Agenda lab 001

- La posta elettronica
  - servizi in plain-text
  - servizi con SSL
  
- Crittografia Personale
  - GPG
  - S/MIME



# Gnu Privacy Guard

GPG è un programma OpenSource, multiplatforma, gratuito il cui scopo è creare una coppia di chiavi crittografiche atte a proteggere le nostre e-mail ed i nostri file.

OpenPGP RFC 2440



# Chiave Privata

Permette a noi di “firmare” le mail inviate, così da rendere certo il destinatario sull’integrità del messaggio e sull’identità del mittente.

Il destinatario potrà verificare il messaggio utilizzando la nostra chiave pubblica.



# Chiave Pubblica

Permette ad uno sconosciuto di inviare un messaggio criptato diretto a noi.

Solo noi, con la chiave privata, potremo decriptare il contenuto della mail.



# Signature

Viene creato il digest del messaggio, con un algoritmo one way, che poi viene criptato con la chiave privata.

Il digest ha lunghezza costante indipendentemente dalla quantità di input.

Dal digest è impossibile ricostruire l'input che lo ha generato.



# Singnature #2

Una modifica microscopica al messaggio provoca una modifica macroscopica del digest.

Tutti possono decriptare il digest con la chiave pubblica. Tutti possono calcolare il digest del messaggio.

Di conseguenza tutti possono verificare il messaggio.



# Keyserver

Dopo avere creato le proprie chiavi le si pubblica su un keyserver, al fine di permettere agli altri di scaricare la nostra chiave pubblica.



# Identità del mittente

Non vi è modo di essere certi che la chiave GPG associata ad una mail sia effettivamente quella generata dal proprietario della mail.



# Key-signing party

Per questa ragione ci si firma reciprocamente le chiavi pubbliche al fine di creare un network di “fiducia”.

Per firmare una chiave altrui è necessario incontrarsi di persona e scambiarsi il fingerprint della chiave.





- ➔ installare GPG
- ➔ creare le chiavi
- ➔ configurare thunderbird per usare GPG
- ➔ scambiare email criptate
- ➔ verificare lo spool del server
- ➔ verificare i dettagli delle mail criptate

# Agenda lab 001

- La posta elettronica
  - servizi in plain-text
  - servizi con SSL
  
- Crittografia Personale
  - GPG
  - S/MIME



# S/MIME

E' uno standard largamente diffuso e presente nativamente in quasi tutti i client di posta.

Non è necessario installare software aggiuntivo per utilizzarlo.

S/MIME Version 3.1 Message Specification (RFC 3851)

S/MIME Version 3.1 Certificate Handling (RFC 3850)



# Trust Model

Mentre GPG utilizza un *trust model* basato sul *web of trust*.

S/MIME invece ha una gestione gerarchica delle chiavi, è cioè la CA stessa a garantire la corrispondenza chiave-mittente.



# La CA ha la mia private key?

Quando chiedo alla CA di generare la mia coppia di chiavi esse vengono generate il locale sul browser.

La CA prende una copia della mia chiave pubblica, la firma e la pubblica.





- ➔ creare un account Thawte
- ➔ abilitare un indirizzo mail
- ➔ richiedere il certificato
- ➔ configurare thunderbird per utilizzarlo
- ➔ scambiarsi email criptate
- ➔ [visualizzarle nello spool]
- ➔ visualizzare le proprietà delle mail

# Conclusioni

- ✓ Tutto il traffico può essere intercettato
- ✓ SSL protegge la nostra riservatezza
- ✓ GPG, S/MIME proteggono il singolo messaggio
- ✓ GPG richiede un client che lo supporti
- ✓ GPG richiede l'installazione del programma
- ✓ S/MIME è nativo su molti client di posta
- ✓ GPG stabilisce una rete di trust
- ✓ S/MIME si basa sulla fiducia in una CA
- ✓ “Per fare crittografia bisogna essere in due...”



# Bibliografia

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

<http://tools.ietf.org/html/rfc2821>

[http://it.wikipedia.org/wiki/Post\\_Office\\_Protocol](http://it.wikipedia.org/wiki/Post_Office_Protocol)

<http://www.rfc-editor.org/rfc/rfc1939.txt>

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

<http://www.rfc-editor.org/rfc/rfc3501.txt>

<http://monkey.org/~dugsong/dsniff/>



# Grazie!

Queste slide sono disponibili su  
<http://www.scienze.univr.it/fol/main?ent=avvisoin&cs=105>

Per domande od approfondimenti:  
[alessio@alba.st](mailto:alessio@alba.st)



Dipartimento di  
Informatica

These slides written by  
Alessio L.R. Pennasilico  
aka mayhem. They are  
subjected to Creative  
Commons Attribution-  
ShareAlike 2.5 version;  
you can copy, modify,  
sell. "Please" cite your  
source and use the same  
licence :)