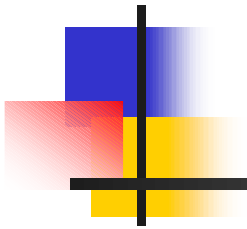
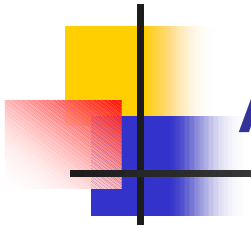


Meccanismi di autenticazione sicura

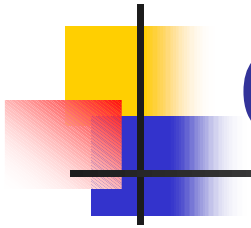
Paolo Amendola

GARR-CERT



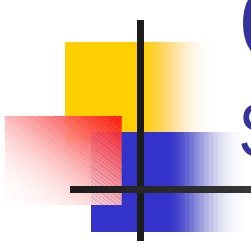
Argomenti

- Crittografazione del traffico
- Identita’ digitali
- One-time passwords
- Kerberos



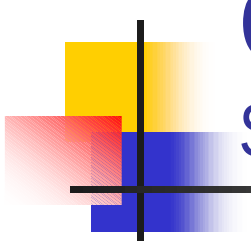
Crittografazione del traffico

- Secure Shell
- SASL
- SRP
- sftp
- SDSC/GT secure ftp



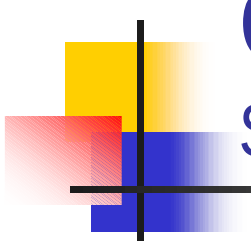
Crittografazione del traffico
Secure Shell

- Due versioni: ssh1 (piu' vecchia) e ssh2 (piu' recente e piu' sicura).
- Nella configurazione standard, viene negoziata tra client e server una chiave comune con la quale crittografare la sessione, dopodiche' viene richiesta la password dell'account.
- Possibilita' di effettuare una sessione interattiva attraverso i comandi *ssh/slogin* e trasferimento files attraverso *scp* (non interattivo) e *sftp* (interattivo, solo ssh2).
- Piattaforme:
  - Server: Unix, OpenVMS, Windows 32 bit
  - Client: Unix, OpenVMS, Windows 16/32 bit e CE, Mac, Java, PalmOS
- URL:
  - http://www.ssh.com/products/ssh/download.html
  - http://www.employees.org/~satch/ssh/faq/ssh-faq.html
  - http://www.cert.garr.it/incontri/na/ssh.html
  - http://security.fi.infn.it/tools/ssh-applet/



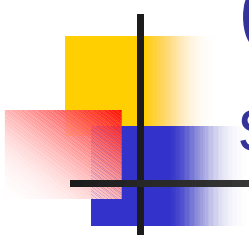
Crittografazione del traffico
SRP

- Protocollo sviluppato dalla Stanford University per lo scambio sicuro di chiavi tra client e server. Resiste agli attacchi di “forza bruta” contro le passwords, anche se si utilizzano passwords relativamente semplici da indovinare.
- Il protocollo e’ una RFC (2945).
- Esistono versioni di *telnet* e *ftp* che supportano questo protocollo.
- L’installazione e’ molto semplice: basta sostituire gli eseguibili di client e server.
- Piattaforme:
  - Server: Unix
  - Client: Unix, Windows 32 bit, Java
- URL:
  - http://srp.stanford.edu



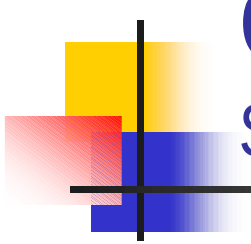
Crittografazione del traffico
SASL

- Simple Authentication and Security Layer: sviluppato dalla Carnegie Mellon University. L'idea e' quella di estendere i protocolli gia' esistenti aggiungendo il supporto per la scelta del tipo di autenticazione.
- C'e' una fase iniziale durante la quale viene negoziato il tipo di autenticazione tra quelli supportati dal client e dal server, dopodiche', svolta questa fase con successo, la sessione continua utilizzando il tipo di sicurezza negoziato.
- Il protocollo e' una RFC (2222).
- Tipi di autenticazione attualmente supportati:
  - Kerberos V4, S/KEY, GSSAPI
- Piattaforme:
  - Viene distribuito sotto forma di librerie da inserire all'interno dei propri programmi.
  - Attualmente supportano SASL: sendmail >8.10, Netscape >4.x, Outlook Express >4.x, Cyrus IMAP server.
- URL:
  - http://asg.web.cmu.edu/sasl/



Crittografazione del traffico
sftp

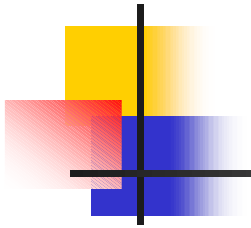
- E’ un sostituto per ftp che utilizza un tunnel ssh per la connessione. Implementa una interfaccia utente a caratteri. Consiste di una parte client e una parte server.
- Ne esiste una versione per X11, *gftp*, che utilizza le librerie gtk+.
- Funziona sia con il protocollo ssh1 che ssh2.
- Piattaforme:
  - Server: Unix
  - Client: Unix, Windows 32bit
- URL:
  - http://www.xbill.org/sftp/ (sftp)
  - http://gftp.seul.org/ (gftp)



Crittografazione del traffico

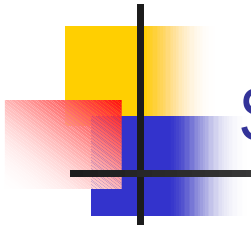
SDSC/GT secure ftp

- Client ftp in java che effettua connessioni attraverso il protocollo SSL. Effettua la crittografazione del solo canale di controllo.
- Piattaforme:
  - Tutte le piattaforme che supportano Java 2.
- URL:
  - http://www.glub.com



Identita’ digitali

- Secure Shell
- SSL



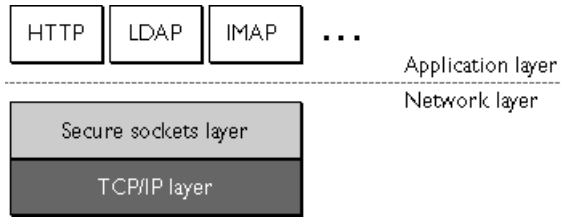
Identita' digitali

Secure Shell

- E' possibile configurare Secure Shell in modo da permettere l'autenticazione di un utente attraverso la sua chiave privata o attraverso la sua chiave PGP (solo ssh2).
- L'utente deposita una copia della chiave pubblica sul server, che verra' utilizzata per effettuare l'autenticazione; solo lui, che e' in possesso della corrispondente chiave privata, puo' continuare la sessione.
- Autenticazione fortemente sicura: c'e' uno stretto legame tra la chiave privata e l'identita' del suo possessore.

Identita’ digitali
SSL (1)

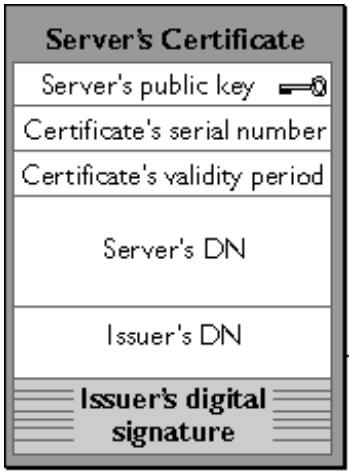
- SSL: Secure Socket Layer. E’ un protocollo che si pone tra il livello TCP e il livello delle applicazioni.



- Permette la mutua autenticazione tra un client che richiede un servizio e il server che lo fornisce.

Identita’ digitali
SSL (2)

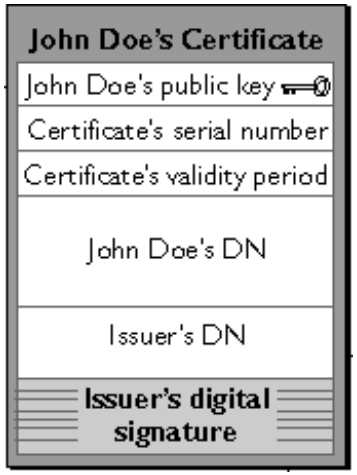
- Autenticazione effettuata attraverso i “*certificati*”, unita’ di informazione che vengono emessi da entita’ chiamate **Certification Authorities (CA)**. Un certificato contiene informazioni sul proprietario del certificato, sia esso una persona o un computer, sulla scadenza e sulla CA che lo ha emesso.



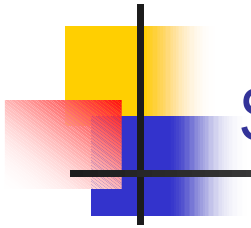
- All’atto della connessione, il server presenta al client il suo certificato. Se il certificato e’ valido e il client “si fida” della CA che lo ha emesso, la sessione puo’ continuare.

Identita’ digitali
SSL (3)

- Opzionalmente, il server puo’ richiedere che anche il client dimostri la propria identita’.



- In questo caso, il server effettua dei controlli analoghi a quelli effettuati dal client.

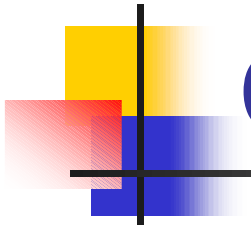


Identita' digitali

SSL (4) - stunnel

- Stunnel e' un programma per la creazione di canali crittografati attraverso il protocollo SSL. Normalmente viene utilizzato per aggiungere funzionalita' SSL ad applicazioni che non supportano tale protocollo nativamente.
- Puo' funzionare sia in modalita' *daemon* (cioe' come processo autonomo) che in modalita' *inetd* (cioe' fatto partire dal demone inetd).
- Richiede l'installazione di librerie a parte per il supporto SSL.

- Piattaforme:
  - stunnel esiste sia per Unix che per Windows 32bit.
  - Client: Netscape >4.x, Outlook Express >4.x (IMAPS, POP3S, HTTPS).
- URL:
  - http://www.stunnel.org (stunnel)
  - http://www.openssl.org (OpenSSL)

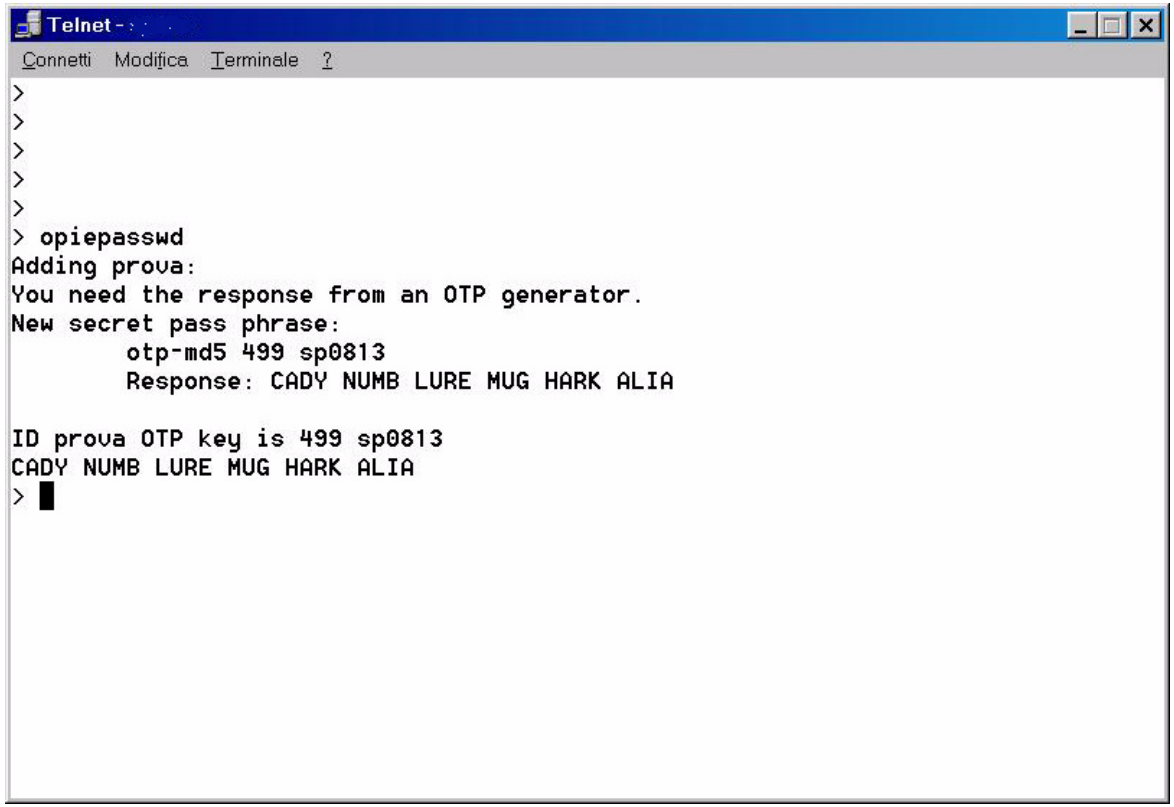


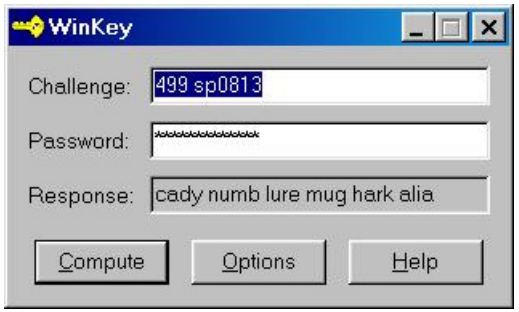
One Time Passwords

- Le one-time passwords sono passwords che possono essere utilizzate una sola volta per sessione.
- L'utente, attraverso un opportuno comando e utilizzando una "*secret password*", inizializza sul server un numero a scelta di passwords.
- All'atto di ogni login, all'utente viene presentata una *"challenge"* costituita da un valore numerico variabile e da un valore alfanumerico fisso.
- L'utente utilizzera' queste informazioni, unite alla *"secret password",* per generare **sulla macchina locale** un *"response"* da fornire al server.
- Il *"response"* viene calcolato attraverso un algoritmo di checksum crittografico: il risultato, un valore di 64 bit, viene trasformato per praticita' in una sequenza di 6 parole di lunghezza variabile da 1 a 4 caratteri, prese da un vocabolario noto di 2048 parole.
- Una volta autenticato correttamente, al prossimo login il valore numerico sara' decrementato di una unita'.

One Time Passwords

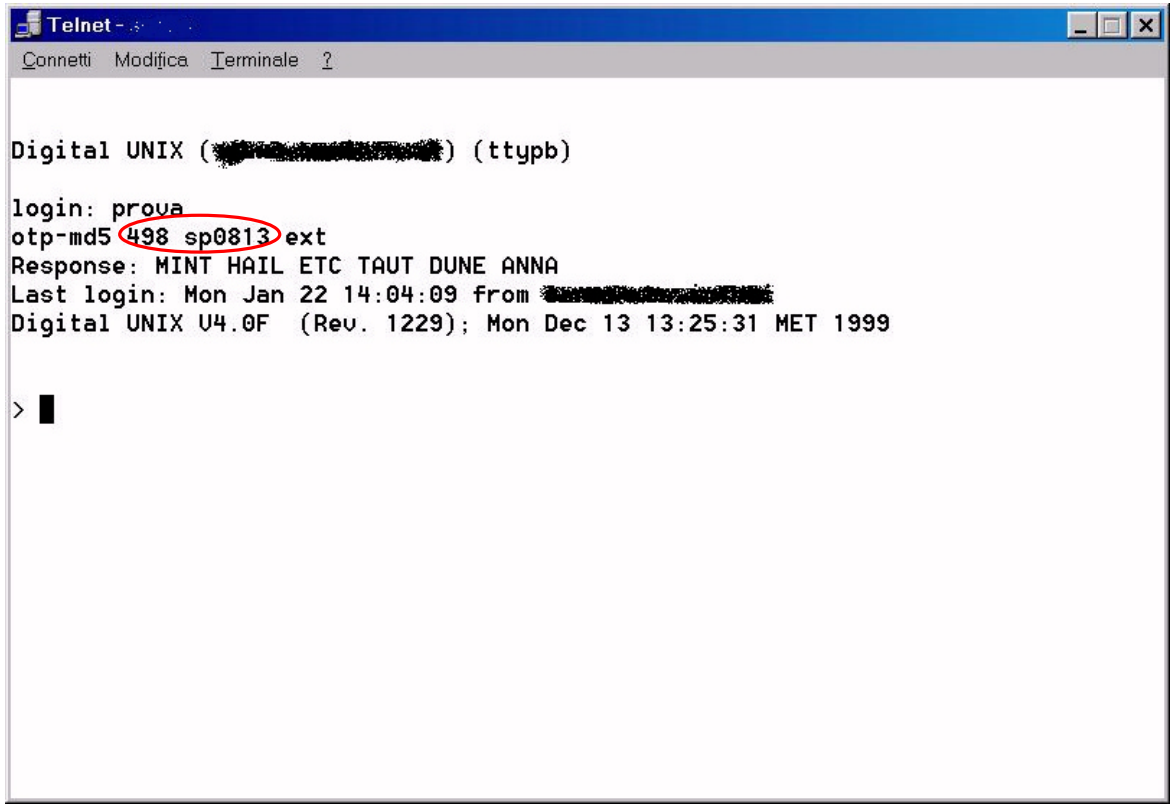
Esempio – inizializzazione database

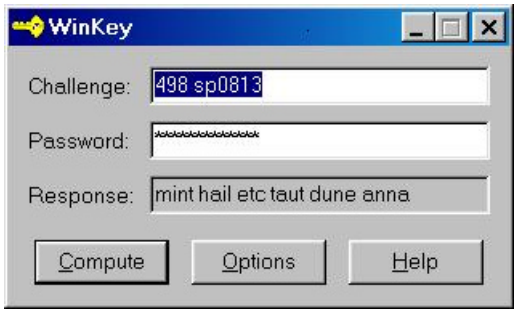


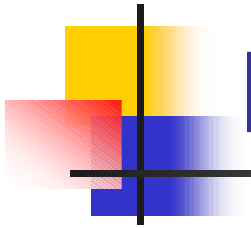


One Time Passwords

Esempio - login





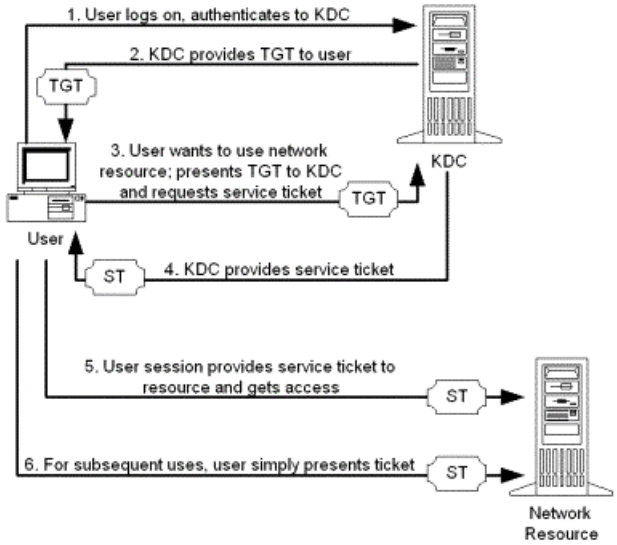


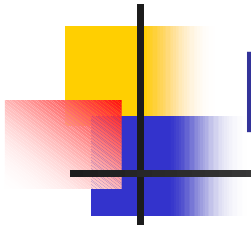
Kerberos (1)

- Sistema di autenticazione sicura sviluppato dal MIT. Permette agli utenti ed ai servizi di cui vogliono usufruire di autenticarsi mutuamente in maniera sicura.
- Si basa sulla fiducia che hanno sia i servizi che gli utenti su una “terza parte”, il KDC (Key Distribution Center).
- Sia gli utenti che i servizi (denominati “*principal*”) possiedono una chiave che deve essere conosciuta dal KDC.

Kerberos (2)

- **1.** All' atto dell'autenticazione, il client chiede al KDC un "Ticket Granting Ticket" (TGT).
- **2.** Il ticket viene concesso, crittografato con la chiave dell'utente.
- **3.** Ogni volta che l'utente deve utilizzare un servizio, presenta il TGT al KDC, specificando il servizio che vuole utilizzare.
- **4.** Il KDC rilascia al client un "Service Ticket" (ST), crittografato con la chiave del servizio scelto.
- **5.** Questo ST viene presentato al servizio e serve per ottenere l'accesso.
- **6.** Ad ogni uso successivo, al client basta presentare l'ST.





Kerberos (3)

- Piattaforme:
  - KDC: Unix, Windows 2000
  - Client: Unix, Windows 9x/NT/2000, Mac
- URL:
  - http://web.mit.edu/kerberos/www/
  - http://www.crypto-publish.org/