



# Sicurezza delle reti<sup>1</sup>

Mattia Monga

Dip. di Informatica e Comunicazione  
Università degli Studi di Milano, Italia  
[mattia.monga@unimi.it](mailto:mattia.monga@unimi.it)

a.a. 2010/11

<sup>1</sup> © 2011 M. Monga. Creative Commons Attribuzione-Condividi allo stesso modo 2.5 Italia License.  
<http://creativecommons.org/licenses/by-sa/2.5/it/>. Materiale derivato da © 2010 M. Cremonini.



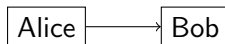
# Lezione XIX: L'autenticazione in rete



# Autenticazione

## Autenticazione

Autenticare significa verificare l'identità di un soggetto (non necessariamente umano)



Tre modalità di base per l'autenticazione (di Alice) in rete:

- tramite una password (ossia la conoscenza di un segreto)
- basata sulla locazione (logica o fisica) da cui proviene la richiesta di autenticazione
- per mezzo di operazioni crittografiche su dati forniti dall'autenticatore (Bob).



# Pericoli

Alcune vulnerabilità sono intrinseche:

- Le password possono essere indovinate
- Le locazioni possono essere millantate
- I dati crittografici possono essere intercettati e riutilizzati (replay attack)

Queste minacce possono essere mitigate

- Aumentando la cardinalità delle password possibili
- Controlli di coerenza
- Crittografia a chiave pubblica e protocolli articolati

L'autorizzazione conseguita con l'autenticazione dura un intervallo temporale detto sessione.

## Password guessing



- Una password può essere scelta in maniera prevedibile (anziché **del tutto casuale**) nell'insieme possibile.
  - *Online guessing*: l'attaccante prova tutte le password possibili (**brute force**); si limitano i tentativi e/o si rallenta il feedback
  - *Offline guessing*: l'attaccante accede all'elenco dei segreti (generalmente crittati con hash) e prova elenchi di parole (**dictionary attack**); si **salano** gli hash
- | Utente | salt | stored password                     |
|--------|------|-------------------------------------|
| Alice  | 42   | hash(42 password <sub>Alice</sub> ) |
- Le password possono essere **intercettate**
  - Una password può essere utilizzata in occasioni differenti
  - Un problema classico è anche la **distribuzione iniziale delle credenziali**; si fanno scadere al primo accesso

235

Sicurezza delle reti  
Monga  
L'autenticazione in rete  
Password  
Altre credenziali  
OTP  
Metodi crittografici

## Credenziali generalizzate



Alice può provare la sua identità mostrando

- qualcosa che **sa** (password tradizionale)
- qualcosa che **ha** (authentication token)
- qualcosa che **è** (biometria)

È naturalmente possibile (e spesso desiderabile) avere autenticazioni **a più fattori**.

236

Sicurezza delle reti  
Monga  
L'autenticazione in rete  
Password  
Altre credenziali  
OTP  
Metodi crittografici

## Client inaffidabili



La diffusione del malware ha reso spesso inaffidabili i client  
Chi garantisce che la schermata di login non sia un  *cavallo di Troia*  capace di memorizzare/rubare le credenziali?  
(Si noti che la protezione del "tastierino" che cambia ad ogni login è puramente apparente. Un esempio di falsa sicurezza, che tra l'altro impedisce all'utente di utilizzare meccanismi automatici di memorizzazione delle password)

Login

Numero carta:

Codice cliente:

PIN: 

0	4	2	1	8
5	6	7	3	9

Inserisci i tuoi codici d'accesso.  
Please insert your access codes.  
Geben Sie Ihre Zugangscodes ein.

237

Sicurezza delle reti  
Monga  
L'autenticazione in rete  
Password  
Altre credenziali  
OTP  
Metodi crittografici

## Anti-malware



Contro client alterati è difficile proteggersi, ma protezioni più efficaci sono:

- In ogni sessione viene comunicata solo parte della password
- Two-factor authentication (2FA)
- One-time password (OTP)

Nessuna di queste misure protegge da:

- **Man in the Browser** il client alterato non si limita ad intercettare le credenziali, ma è in grado di manipolare i dati della transazione
- **Session hijacking** l'attaccante è in grado di manipolare una sessione già in corso

238

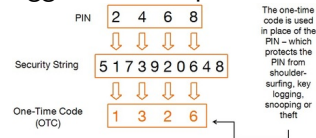
Sicurezza delle reti  
Monga  
L'autenticazione in rete  
Password  
Altre credenziali  
OTP  
Metodi crittografici



Sicurezza delle  
reti  
Monga

L'autenticazione  
in rete  
Password  
Altre credenziali  
OTP  
Metodi  
crittografici

L'idea è quello di utilizzare **due** (o più) meccanismi di autenticazione: tipicamente una password e il possesso di un oggetto fisico: p.es. un security token o un telefono cellulare.



È importante che i due fattori siano effettivamente indipendenti: web browsing con uno smart-phone e sms?

239



Sicurezza delle  
reti  
Monga

L'autenticazione  
in rete  
Password  
Altre credenziali  
OTP  
Metodi  
crittografici

I più diffusi si basano su **synchronous dynamic password**: la password cambia ad intervalli regolari, per esempio ogni minuto.



La sincronizzazione per periodi lunghi è critica (e intervalli di accettazione più lunghi introducono una vulnerabilità): alcuni permettono la risincronizzazione tramite collegamento fisico.

240



Sicurezza delle  
reti  
Monga

L'autenticazione  
in rete  
Password  
Altre credenziali  
OTP  
Metodi  
crittografici

In generale si tratta di password **utilizzate una volta soltanto** e pertanto non riutilizzabili da un eventuale intercettore. L'effettivo possesso di un security token è generalmente verificato tramite una one time password generata dal token stesso o richiesta *out of band*.

241



Sicurezza delle  
reti  
Monga

L'autenticazione  
in rete  
Password  
Altre credenziali  
OTP  
Metodi  
crittografici

Leslie Lamport nel 1981 ha proposto uno schema per autenticazione tramite OTP che non prevede la necessità di sincronizzazione temporale.

Si basa sull'esistenza di una **funzione di hash  $H$**  sicura (non invertibile).

- 1 Alice e Bob concordano un segreto  $W$
- 2 Bob conserva  $H(\dots H(H(W))\dots) = H^n(W)$  e  $n$
- 3 Autenticazione
  - 1 Alice comunica la propria *username*
  - 2 Bob risponde con il numero  $n$
  - 3 Alice comunica  $x = H^{n-1}(W)$
  - 4 Bob verifica che  $H(x) = H^n(W)$  e decrementa  $n$

Lo schema funziona  $n$  volte, poi bisogna cambiare  $W$ .

242



Sturezza delle reti  
Monga

Lo schema di Lamport è stato implementato da Neil Haller Phil Karn e John Walden in S/KEY.

Usa numeri a 64 bit + 2 bit di parità. Poiché stringhe casuali di 8 caratteri potrebbero essere difficili da utilizzare per un utente umano, è prevista una mappatura su 2048 parole da 1 a 4 caratteri: i 66 bit diventano una sequenza di 6 parole (TAG SLOW NOV MIN WOOL KENO ↔ 0x3F3BF4B4145FD74B).

{	"A"	"ABE"	"ACE"	"ACT"	"AD"	"ADA"	"ADD"
"AGO"	"AID"	"AIM"	"AIR"	"ALL"	"ALP"	"AM"	"AMY"
"AN"	"ANA"	"AND"	"ANN"	"ANT"	"ANY"	"APE"	"APS"
"APT"	"ARC"	"ARE"	"ARK"	"ARM"	"ART"	"AS"	"ASH"
"ASK"	"AT"	"ATE"	"AUG"	"AUK"	"AVE"	"AME"	"AMK"
"AML"	"AMN"	"AX"	"AYE"	"BAD"	"BAG"	"BAH"	"BAM"
"BAN"	"BAR"	"BAT"	"BAY"	"BE"	"BED"	"BEE"	"BEG"
"BEN"	"BET"	"BEV"	"BIB"	"BID"	"BIG"	"BIN"	"BITT"
"BOB"	"BOG"	"BON"	"BOO"	"BOP"	"BOM"	"BOY"	"BUB"
"BUD"	"BUG"	"BUM"	"BUN"	"BUS"	"BUT"	"BUY"	"BY"
"BYE"	"CAB"	"CAL"	"CAM"	"CAN"	"CAP"	"CAR"	"CAT"
"CAM"	"COD"	"COG"	"COL"	"COM"	"COO"	"COP"	"COT"
"COY"	"COY"	"CRY"	"CUB"	"CUE"	"CUR"	"CUT"	"CUT"
"DAB"	"DAD"	"DAM"	"DAN"	"DAR"	"DAY"	"DEE"	"DEL"
"DEN"	"DES"	"DEW"	"DID"	"DIE"	"DIG"	"DIN"	"DIP"
"DO"	"DOE"	"DOG"	"DON"	"DOT"	"DOW"	"DRY"	"DUB"
"DUD"	"DUE"	"DUG"	"DUN"	"EAR"	"EAT"	"ED"	"EEL"
"EGG"	"EGO"	"ELI"	"ELK"	"ELM"	"ELY"	"EM"	"END"
"EST"	"ETC"	"EVA"	"EVE"	"EWA"	"EVE"	"EAD"	"EAM"
"FAR"	"FAT"	"FAY"	"FED"	"FEE"	"FEM"	"FIB"	"FIG"
"FIN"	"FIR"	"FIT"	"FLO"	"FLY"	"FOE"	"FOG"	"FOR"
"FRY"	"FOW"	"FOW"	"FUR"	"FLY"	"GAB"	"GAD"	"GAG"
"GAM"	"GAP"	"GAS"	"GAY"	"GEE"	"GEL"	"GEM"	"GET"
"GIG"	"GIL"	"GIN"	"GO"	"GOT"	"GUM"	"GUN"	"GUS"
"GUT"	"GUY"	"GYM"	"GYF"	"HA"	"HAD"	"HAL"	"HAM"
"HAN"	"HAP"	"HAS"	"HAT"	"HAM"	"HAY"	"HE"	"HEM"
"HEN"	"HER"	"HEM"	"HEY"	"HI"	"HID"	"HIM"	"HIP"
"HIS"	"HIT"	"HO"	"HOB"	"HOC"	"HOE"	"HOG"	"HOP"
"HOT"	"HOB"	"HUB"	"HUE"	"HUG"	"HUM"	"HUN"	"HUT"
"I"	"ICV"	"IDA"	"IFE"	"IKE"	"INK"	"INN"	"INN"
"IO"	"ION"	"IO"	"IRA"	"IRE"	"IRK"	"IS"	"IT"
"ITS"	"IYV"	"JAB"	"JAG"	"JAM"	"JAR"	"JAM"	"JAM"
"JAY"	"JET"	"JIG"	"JIM"	"JOY"	"JOB"	"JOE"	"JOG"
"JOT"	"JOY"	"JUG"	"JUT"	"KAY"	"KEG"	"KEN"	"KEY"
"KID"	"KIM"	"KIN"	"KIT"	"LA"	"LAB"	"LAC"	"LAD"
"LAG"	"LAM"	"LAP"	"LAW"	"LAY"	"LEA"	"LED"	"LEE"
"LEG"	"LEM"	"LEN"	"LET"	"LEW"	"LEO"	"LIE"	"LID"
"LIP"	"LIT"	"LO"	"LOB"	"LOG"	"LOP"	"LOS"	"LOT"
"LOU"	"LOW"	"LOY"	"LUG"	"LYE"	"MA"	"MAC"	"MAD"
"MAE"	"MAN"	"MAO"	"MAP"	"MAT"	"MAW"	"MAY"	"ME"



Sturezza delle reti  
Monga

Anche questo schema non protegge da Man in the Browser o Session Hijacking. Un problema ancora più grave è l'attacco con  $n$  piccolo

- 1 Bob conserva il numero  $n$
- 2 Mallory impersona Bob e manda ad Alice un  $n' < n$
- 3 Alice risponde con  $H^{n'}(W)$
- 4 Mallory potrà usare  $H^{n'}(W)$  per sostituirsi ad Alice quando Bob arriverà a conservare  $n'$

Il pericolo può essere mitigato rendendo Alice edotta su  $n$  attuale, in modo che possa insospettirsi per eventuali  $n' \ll n$



Sturezza delle reti  
Monga

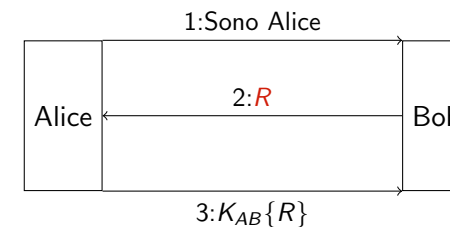
Lo schema di Lamport però funziona bene con modalità "carta e penna".

- Alice conserva una lista cartacea di password ( $H^n(W), H^{n-1}(W), \dots$ )
- Una volta usata la prima della lista la cancella

Questo schema non è suscettibile all'attacco di  $n$  piccolo, ma la lista è naturalmente un punto critico.



Sturezza delle reti  
Monga



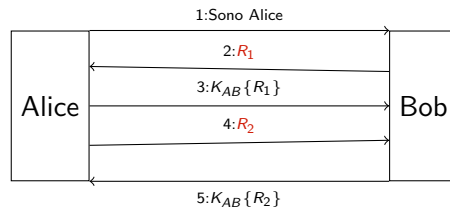
- L'autenticazione non è reciproca: qualcuno potrebbe sostituirsi a Bob.
- Offline-guessing di  $K_{AB}$  è possibile intercettando  $R$  e  $K_{AB}\{R\}$

## Challenge/Response con mutua autenticazione



Sturezza delle reti  
Monga

L'autenticazione in rete  
Password  
Altre credenziali  
OTP  
Metodi crittografici



Sono necessari ben 5 scambi: si può rendere piú efficiente?

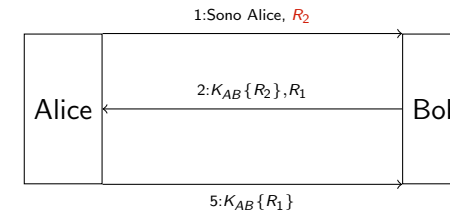
247

## Challenge/Response con mutua autenticazione

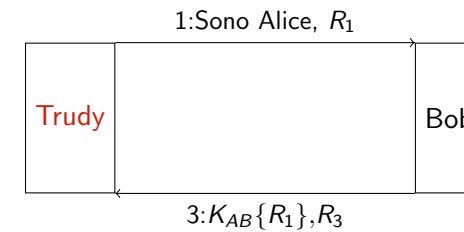
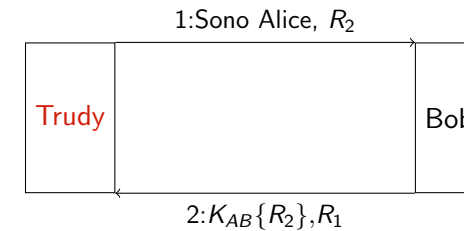


Sturezza delle reti  
Monga

L'autenticazione in rete  
Password  
Altre credenziali  
OTP  
Metodi crittografici



Purtroppo cosí si presta ad un reflection attack



248

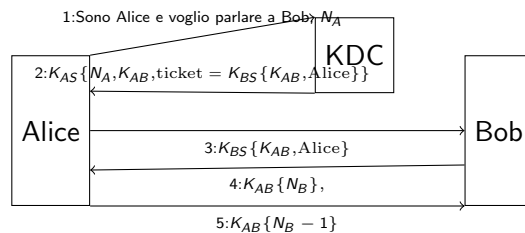
## Needham-Schroeder



Sturezza delle reti  
Monga

L'autenticazione in rete  
Password  
Altre credenziali  
OTP  
Metodi crittografici

Per semplificare la gestione dei segreti condivisi, possono essere introdotti dei Key Distribution Center (KDC). Uno dei protocolli classici è Needham-Schroeder [1978]



Qualora  $K_{AB}$  sia compromesso (p.es. accedendo alla macchina di Alice) è possibile un replay attack del *ticket*, quindi occorre complicarlo ulteriormente introducendo dei timestamp, in modo che i ticket non possano essere riutilizzati. I numeri  $N$  sono detti nonce.

249

Inoltre si presta all'offline guessing (anche senza intercettazione!).

Cosí va meglio:

