Sicurezza

Guarantire sicurezza significa proteggere i dati e le risorse garantendo

- Segretezza (*Confidenzialità*) L'informazione può essere rilasciata – direttamente o indirettamente – solo a utenti autorizzati a conoscerla.

  Privacy: diritto di un individuo di stabilire se, come, quando e a chi l'informazione che lo riguarda può essere rilasciata.

- Integrità Le informazioni (e le risorse) non devono essere modificate, cancellate o distrutte in modo non autorizzato o *improprio*.

- Disponibilità (*Availability* –no *denials-of-service*) Non deve essere impedito agli utenti gli accessi propri e per i quali hanno la autorizzazione necessaria.

Servizi di sicurezza

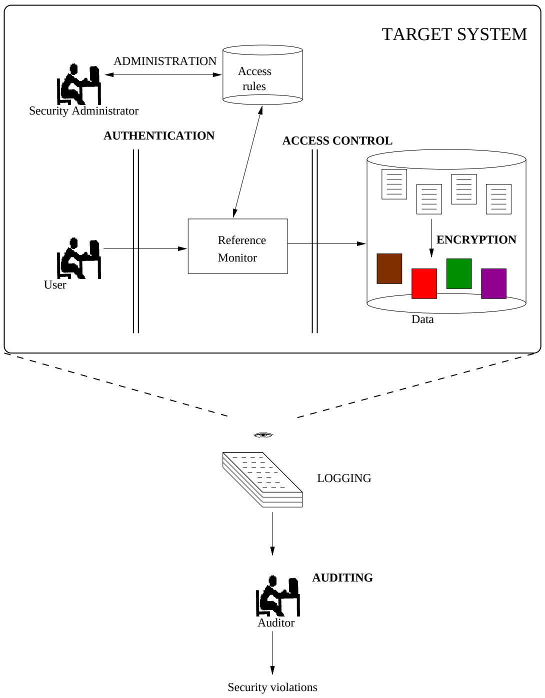
- Identificazione e Autenticazione Fornisce al sistema la abilità di identificare gli utenti e verificarne l'identità.

- Controllo dell'accesso valuta le richieste di accesso alle risorse fatte da utenti autenticati e, sulla base di regole definite, determina se permettere o negare l'accesso.
  - controlla solo gli accessi *diretti*. Può essere arricchito con controlli *di flusso*, *inferenza* e *non-interferenza*

- Audit permette una valutazione a posteriori delle richieste e degli accessi avvenuti per determinare se ci sono state (o sono state tentate) violazioni.

- Crittografia assicura che i dati memorizzati nel sistema o spediti lungo la rete possano essere decifrati solo dal legittimo ricevente.
  Nella comunicazione su rete può anche essere utilizzata per stabilire l'autenticità delle informazioni trasmesse o delle parti coinvolte.

Security services - The global picture



Autenticazione

- Stabilisce l'identità di una "parte" ad una altra "parte".
- Le parti possono essere utenti o computer.
- Spesso richiesta autenticazione bi-direzionale (es., comunicazione peer-to-peer). Autenticazione di un computer ad un utente per prevenire attacchi di spoofing in cui un computer pretende di essere un altro computer (per acquisire la password degli utenti).
- Spesso necessaria la combinazione di autenticazione "utente-a-computer" e "computer-a-computer".
- È per molti aspetti il servizio di sicurezza primario.
  - La correttezza del controllo degli accessi si basa su una corretta autenticazione.
  - La correttezza del controllo delle intrusioni degli accessi si basa su una corretta autenticazione.

Autenticazione e crittografia

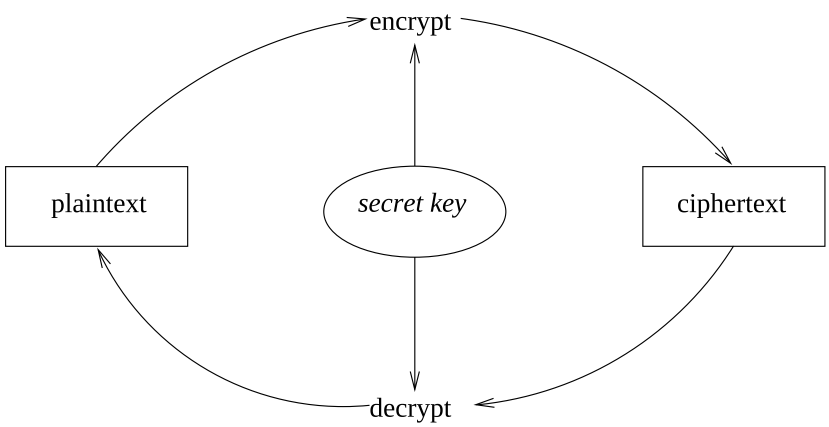
L'autenticazione può fare uso di misure crittografiche.

Crittografia: dato un testo in chiaro produce una versione non intelligibile (testo crittato) e viceversa. Utilizza una chiave per crittare e decrittare.

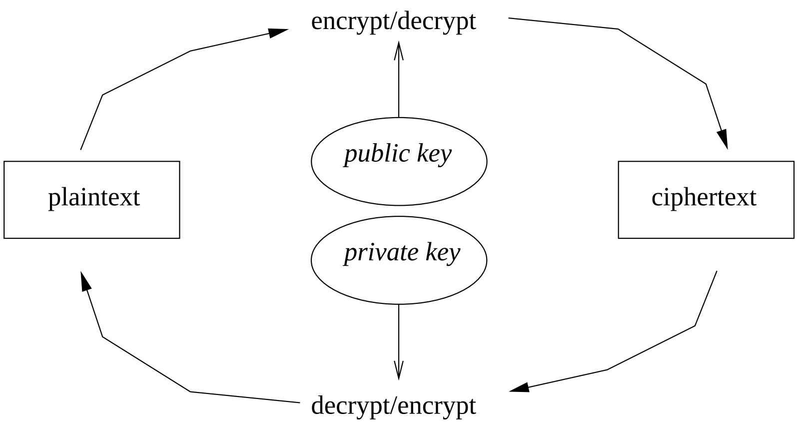
Distinguiamo crittografia a

- chiave privata (o simmetrica) La stessa chiave è utilizzata per crittare e decrittare
- chiave pubblica (o asimmetrica) Utilizza una coppia di chiavi (⟨pubblica,privata⟩): una per crittare e l'altra per decrittare

Crittografia simmetrica



Crittografia asimmetrica



Autenticazione utente a computer

Può essere basata su:

- qualcosa che l'utente conosce (es., password)
- qualcosa che l'utente possiede (es., tesserina magnetica)
- qualcosa che l'utente è, stabilito sulla base di caratteristiche biometriche (es., impronte digitali, impronta della voce).

o una combinazione di queste.

Autenticazione basata su password

- Basata su coppia:
  - login: l'utente si identifica
  - password: l'utente fornisce prova della sua identità.
- Metodo di autenticazione più antico e più diffuso (e lo sarà ancora nel breve futuro).
  - è il più semplice
  - è il più economico
  - è di facile implementabilità

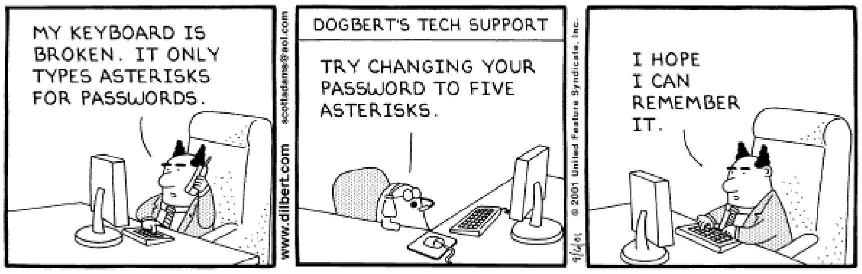
    però ....
  - è anche il più debole

Vulnerabilità delle password

- Spesso le password possono:
  - essere facilmente indovinate (guessing)
  - osservate da persone che osservano l'utente legittimo mentre la scrive (snooping)
  - acquisite da terze parti nella comunicazione lungo la rete (sniffed)
  - acquisite da terze parti che impersonano l'interfaccia di login (spoofing)
- Chiunque riesca a conoscere la password di un utente può impersonare (masquerading) l'utente nell'accesso al sistema.

Vulnerabilità delle password

Una delle maggiori cause della vulnerabilità delle password è rappresentata dagli utenti che non le scelgono o gestiscono propriamente.



Cause di vulnerabilità delle password

Il primo passo per limitare la vulnerabilità delle password è una buona gestione delle password.
Spesso le password sono vulnerabili perchè gli utenti non pongono abbastanza cura:

- non cambiano la password per molto tempo
- condividono la password con colleghi o amici
- scelgono password “deboli” perchè facili da ricordare (e.g., nome o date di nascita di parenti o animali domestici)
- usano la stessa password su più computer
- scrivono le password su pezzi di carta per essere sicuri di non dimenticarla.

Scelta delle password

Una buona gestione richiede che gli utenti

- cambino spesso la propria password
- mantengano le loro password private
- scelgano password che non siano facili da indovinare.
  Una buona password dovrebbe
  - essere di almeno 8 caratteri e utilizzare un insieme di caratteri abbastanza largo (sia caratteri alfanumerici sia caratteri speciali).
  - non essere facilmente intuibile e non corrispondere a parole di dizionari (o leggere variazioni di queste).
  - facile da ricordare, altrimenti
    - gli utenti la scrivono
    - gli utenti la dimenticano (denials-of-service)

...... Sfortunatamente spesso questi principi di base non sono seguiti.

Controlli su password

Molti sistemi utilizzano controlli automatici per evitare grosse debolezze nelle password.

- restrizioni su lunghezza e sul minimo numero di caratteri, richiedendo combinazione di caratteri numerici o alfanumerici.
- controllo rispetto a dizionari e rifiuto di parole del linguaggio naturale (per prevenire dictionary attacks).
- massimo tempo di validità di password (gli utenti sono obbligati a cambiare la password quando "scade").
  - mantenimento della storia recente delle password
  - mantenimento di tempo minimo di validità

Controlli su password

In alternativa

- la password può essere scelta dal sistema.
  - non sempre ben accetto (password difficili da ricordare)
  - problema di distribuzione delle password.
- utilizzo di sequenze one-time-password (spesso gli utenti le scrivono per ricordarsele).

Distribuzione iniziale di password

- L'utente si reca fisicamemte dall'amministratore e si autentica tramite metodi tradizionali (es., carta di identità). L'amministratore prepara l'account e l'utente digita la password.
  - scomodità per l'utente
  - pericolo per il sistema (l'utente accede al sistema in modalità superuser, mentre l'amministratore non guarda!!!!!).
    A volte la password è digitata da una tastiera speciale (es., ATM)
- L'amministratore prepara l'account con una password iniziale e la comunica all'utente che dovrà cambiarla al primo utilizzo (pre-expired password).
  - la password dovrebbe essere abbastanza forte (e.g., scelta casualmente).
  - spesso password iniziale molto debole per convenienza (es., matricola studente).

Autenticazione basata su possesso

- Basata su possesso da parte degli utenti di token (oggetto della dimensione di una carta di credito).
- Ogni token ha una chiave crittografica (memorizzata nel token) che può essere utilizzata per dimostrare l'identità del token a un computer.
- Token sono più sicuri delle password
  - mantenendo controllo sul token l'utente mantiene controllo sull'utilizzo della sua identità

Vulnerabilità dei token

- L'autenticazione basata sul token dimostra solo l'identità del token, non quella dell'utente
  - I token possono essere persi, rubati o falsificati
  - chiunque acquisisca un token può impersonare l'utente
- spesso autenticazione basata su token è combinata con autenticazione basata su conoscenza.
  - Per compiere violazioni, terze parti necessitano sia di token sia di sapere la password.
  - Es., Bancomat richiede: Tessera bancomat + PIN (Personal Identification Number).

Autenticazione basata su token

Due tipi di token:

- memory card: hanno memoria ma non hanno capacità di processo.
  - non possono controllare il PIN o crittografarlo per la trasmissione.
  - il PIN è trasmesso in chiaro
    - vulnerabile a attacchi di sniffing
    - richiede fiducia nel server di autenticazione
- smart token: hanno capacità di processo.
  - Es. il Bancomat può controllare il PIN o crittografarlo per la trasmissione.

Smart token

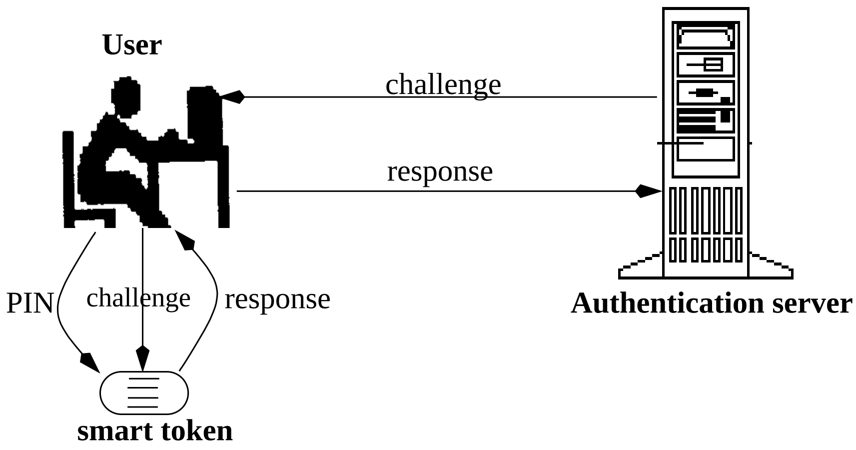
Smart token possono utilizzare differenti protocolli di autenticazione

- scambio statico di password: l'utente si autentica al token e il token si autentica al sistema.
- generazione dinamica di password: il token genera periodicamente nuove chiavi. Per autenticare il token al sistema l'utente deve leggere la chiave corrente e scriverla nel sistema (la chiave può anche essere comunicata direttamente dal token).
- challenge-response: basato su un challenge-response handshake.
  - La comunicazione fra token e sistema può avvenire direttamente o tramite utente.

Challenge response handshake

- il server di autenticazione stabilisce una sfida (challenge). Es., numero casuale.
- il token genera la risposta alla sfida utilizzando la chiave privata del token.
- l'autenticazione ha successo se la risposta è corretta.
- Esempio: smart card
  - Ogni smart card ha una unica chiave privata (nota al server di autenticazione).
  - Per autenticare l'utente al sistema la smart card verifica il PIN.
  - Codifica l'identificatore dell'utente, il PIN e informazione addizionale (es., data e ora), e manda il testo crittato al server.
  - La autenticazione ha successo se il server può decodificare correttamente.

Esempio di challenge-response handshake



Autenticazione basata su caratteristiche dell'utente

- Basata su caratteristiche biometriche dell'utente:
  - caratteristiche fisiche: impronte digitali, forma della mano, impronta della retina o del viso, ...
  - caratteristiche comportamentali: firma, timbro di voce, scrittura, "keystroke dynamic"....
- Richiede una fase iniziale (enrollment phase)
  - esecuzione di più misurazioni sulla caratteristica di interesse
  - definizione di un template

Autenticazione basata su caratteristiche dell'utente

- Autenticazione: confronto fra caratteristica misurata per l'utente sotto controllo rispetto al template memorizzato.
- L'autenticazione ha successo se la misura e il template corrispondono (a meno di un intervallo di tolleranza)
- Non si può richiede perfetta uguaglianza.
- Importante definire la soglia di tolleranza in modo da massimizzare i successi (autenticazione corretta di utenti legittimi e rifiuto di intrusi) e minimizzare gli insuccessi.

Autenticazione biometrica

- Anche se meno accurate sono la forma di autenticazione più forte
  - eliminano vulnerabilità dovute a impersonificazioni.
- Ancora poco utilizzate
  - troppo costose (necessitano di hardware costoso)
  - intrusive (non sempre accettate dagli utenti)
    - Gli scanner della retina sono una tra le misure più accurate ma si teme per pericoli agli occhi causati dal laser.
  - dibattiti politici e sociali per potenziale mancanza di privacy.

Quale tecnica di autenticazione?

- Esiste metodo di autenticazione "più forte", non "migliore"
  - Trade-off fra costi e benefici: metodi più deboli possono andare bene in certi casi
  - Le password sono (e saranno ancora nel breve futuro) il meccanismo di autenticazione più utilizzato.
- Da un punto di vista prettamente tecnico il miglior metodo di autenticazione è costituito dalla combinazione di:
  - autenticazione biometrica fra utente e token
  - mutua autenticazione basata su crittografia fra token e sistema.

....l'autenticazione non finisce qui ... (continuamo quando trattiamo crittografia)