

CONCETTI GENERALI SULLA SICUREZZA INFORMATICA

E le reti informatiche

COMPETENZE

- Acquisire familiarità con il concetto di sicurezza informatica, sicurezza delle informazioni e protezione dei sistemi informativi

CONTENUTI

- Concetti di base
- Autenticazione e controllo degli accessi
- Aspetti pratici
- Gestione del rischio
- Organizzazione della sicurezza
- Le norme sul sistema di gestione della sicurezza

CONCETTI DI BASE

CONCETTI DI BASE

Obiettivi

Sapere quali sono i
principali aspetti della
sicurezza delle informazioni:

Disponibilità

Riservatezza

Integrità

CONCETTI DI BASE

- La sicurezza delle informazioni è un'esigenza che ha accompagnato la storia dell'uomo fin dalle antiche civiltà.
- Ci preoccupiamo di mantenere riservate le informazioni personali, militari e d'affari.

CONCETTI DI BASE

- Nel V secolo a.C. gli spartani inviavano gli ordini ai capi militari tramite messaggi scritti su una striscia di cuoio che, avvolta su un bastone (lo scitale) di un diametro ben preciso, permetteva di leggere il testo in chiaro lungo il bastone.
- Giulio Cesare cifrava i messaggi sostituendo ogni lettera con quella che nell'alfabeto segue di qualche posizione.

CONCETTI DI BASE

La crittografia, cioè la scienza della scrittura segreta, ha avuto una progressiva evoluzione nel corso dei secoli, fino ai rapidi sviluppi teorici e tecnologici impressi dalla seconda guerra mondiale, che permisero la decifrazione dei codici giapponesi e tedeschi da parte degli alleati.

CONCETTI DI BASE



Oggi buona parte del pianeta vive nella *società dell'informazione*, basata cioè sull'uso delle informazioni come parte integrante delle attività umane.



Pertanto, la sicurezza delle informazioni è diventata una componente della sicurezza dei beni in generale, o *security*, e non si limita alle tecniche per nascondere il contenuto dei messaggi.

CONCETTI DI BASE

Qualunque programma che si occupi di preservare la sicurezza delle informazioni, persegue, in qualche misura, tre obiettivi fondamentali:

- **la disponibilità**
- **l'integrità e la**
- **riservatezza delle informazioni.**

DISPONIBILITÀ

- La **disponibilità** è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono.

DISPONIBILITÀ

- Questo significa che sistemi, reti e applicazioni hanno le capacità necessarie a fornire il livello di servizio e le prestazioni richieste e che, in caso di guasto o di eventi distruttivi, sono pronti gli strumenti e le procedure per ripristinare l'attività in tempi accettabili.

DISPONIBILITÀ

Per impedire
l'*inaccessibilità* delle
informazioni, si deve
preservare la disponibilità

1 delle risorse hardware e
software a fronte sia di
problemi interni (guasti,
errori, blackout, disastri e
altro),

2 sia di precise condizioni
ambientali (energia,
temperatura, umidità,
atmosfera, etc.)

3 Prevenire attacchi esterni,
per esempio provenienti da
Internet, volti a impedire o
a ridurre l'accessibilità ai
sistemi e alle informazioni.

DISPONIBILITÀ

- **Strumenti che servono per mantenere la disponibilità**
- Sistemi di backup locale e remoto
- ridondanza dell'hardware e degli archivi,
- firewall e router configurati per neutralizzare attacchi DoS (Denial of Service),
- sistemi di climatizzazione,
- gruppi di continuità,
- controllo dell'accesso fisico
- monitoraggio delle prestazioni

L'INTEGRITÀ

1 - è il grado di
correttezza, coerenza
e affidabilità delle
informazioni

2 - e anche il grado di
completezza,
coerenza e condizioni
di funzionamento delle
risorse informatiche.

INTEGRITÀ

- Per l'hardware e i sistemi di comunicazione, **l'integrità** consiste di fattori come elaborazione corretta dei dati, livello adeguato di prestazioni e corretto instradamento dei dati
- Per l'hardware e i sistemi di comunicazione, **l'integrità** consiste di fattori come elaborazione corretta dei dati, livello adeguato di prestazioni e corretto instradamento dei dati.
- L'integrità del software riguarda fattori come la completezza e coerenza dei moduli del sistema operativo e delle applicazioni e la correttezza dei file critici di sistema e di configurazione

INTEGRITÀ

- Per le informazioni, l'integrità viene meno quando i dati sono alterati, cancellati o anche inventati, per errore o per dolo, e quando si perde, per esempio in un database, la coerenza tra dati in relazione tra loro (per esempio i record coinvolti in una transazione).

INTEGRITÀ

Strumenti utili a preservare l'integrità delle informazioni e delle risorse

- Procedure di manutenzione
- diagnosi preventiva, hardware e software per la rilevazione e prevenzione di
 - accessi illeciti
 - attacchi virali e intrusioni
 - applicazioni che minimizzano errori logici e formali di data entry
- accesso ristretto alle risorse critiche
- controllo degli accessi

INTEGRITÀ

- Anche le tecniche di hashing (calcolo di un numero di lunghezza fissa a partire da un qualsiasi messaggio o documento) sono usate per verificare che le informazioni non vengano alterate per dolo o per errore (anche di trasmissione)

RISERVATEZZA

- La riservatezza consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate, e si applica sia all'archiviazione sia alla comunicazione delle informazioni

RISERVATEZZA

- Un'informazione è composta generalmente di più dati in relazione tra di loro, ciascuno dei quali non necessariamente costituisce un'informazione.
- Il nome e il numero di conto corrente di una persona, separati, non sono informazioni;
- È la combinazione dei due dati che costituisce l'informazione.

RISERVATEZZA

- La riservatezza dell'informazione può essere quindi garantita
- sia nascondendo l'intera informazione (per esempio con tecniche di crittografia)
- sia nascondendo la relazione tra i dati che la compongono

RISERVATEZZA

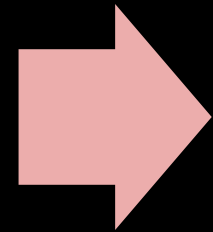
La riservatezza non dipende solo da strumenti hardware e software.

Il fattore umano gioca un ruolo chiave quando vengono ignorate le elementari regole di comportamento:

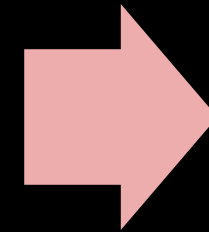
- tenere le password segrete,
- controllare gli accessi a reti e sistemi,
- Rifiutare informazioni a sconosciuti (anche quando affermano di essere tecnici della manutenzione)
- cifrare i documenti e i messaggi riservati e così via

ALTRI OBIETTIVI

Altri due obiettivi di sicurezza possono essere considerati un'estensione dell'integrità delle informazioni, applicate a eventi più complessi come l'invio di un messaggio o una transazione



l'autenticità garantisce che eventi documenti e Messaggi vengano attribuiti con certezza al legittimo autore e a nessun altro



il non ripudio impedisce che un evento o documento possa essere disconosciuto dal suo autore

ALTRI OBIETTIVI

Queste due caratteristiche trovano applicazione nella firma digitale, che utilizza tecniche di *hashing* e crittografia per garantire che un documento resti integro e provenga da un autore univocamente identificato

AUTENTICAZIONE E CONTROLLO DEGLI ACCESSI

AUTENTICAZIONE E AUTORIZZAZIONE

- Autenticazione (authentication) = processo mediante il quale si verifica **l'identità** di un'entità (utente, processo, computer, messaggio)

AUTENTICAZIONE E AUTORIZZAZIONE

- Nessun computer, software o utente può confermare con **certezza l'identità di un utente**: si possono solo eseguire test che, se superati, forniscono una garanzia sufficiente sull'identità dell'interlocutore

AUTENTICAZIONE E AUTORIZZAZIONE

- L'entità che deve essere autenticata presenta alcune **credenziali** (password, certificato digitale) come prova della propria identità: se sono ritenute valide e sufficienti, l'entità è ritenuta autentica

AUTENTICAZIONE E AUTORIZZAZIONE

- L'autenticazione verifica solo che un'entità sia quella che dichiara di essere, senza entrare nel merito dell'accesso al sistema

AUTENTICAZIONE E AUTORIZZAZIONE

- Una volta che un'entità è stata autenticata, il passo successivo è assicurare che possa accedere solo alle risorse per cui è autorizzata (ad es. mediante controlli di accesso, permessi, privilegi)

AUTENTICAZIONE E AUTORIZZAZIONE

- L'autorizzazione viene talvolta confusa con l'autenticazione, ma è un concetto ben distinto...

AUTENTICAZIONE E AUTORIZZAZIONE

- Autorizzazione è il **diritto** accordato ad un'entità (hardware, software, individuo) di accedere ad un sistema e alle sue risorse secondo un profilo di permessi ben definito

AUTENTICAZIONE E AUTORIZZAZIONE

Il controllo del passaporto di un Viaggiatore è un esempio di autenticazione, nella quale la foto viene confrontata con l'aspetto della persona ed il documento viene validato rispetto all'Ente che lo ha rilasciato...

AUTENTICAZIONE E AUTORIZZAZIONE

Il successo dell'autenticazione non implica che il viaggiatore possa varcare la frontiera: la persona potrebbe risultare priva di qualche requisito od essere indesiderata (*accesso negato per mancata autorizzazione*).

AUTENTICAZIONE E AUTORIZZAZIONE

Su una rete (e quindi Internet)
l'autenticazione è più complessa
sia perché eseguita da macchine
sia perché le entità della rete di
solito non hanno accesso fisico
alle entità da autenticare

AUTENTICAZIONE E AUTORIZZAZIONE

Se un individuo riesce ad impersonare un utente valido, non ci sono limiti al danno potenziale per la riservatezza e integrità delle informazioni, oltre agli eventuali danni economici.

In qualche caso può persino essere compromessa la futura capacità di autenticazione degli utenti

AUTENTICAZIONE E AUTORIZZAZIONE

Metodi di autenticazione più diffusi:

- password
- certificati digitali
- dispositivi biometrici
- token fisici
- smart card

ma nessuno è perfettamente sicuro!

AUTENTICAZIONE E AUTORIZZAZIONE

Per impieghi di autenticazione medio - elevati può essere idonea una combinazione di requisiti: ad es. un PDA con capacità crittografiche e biometriche (*riconoscimento dell'impronta digitale, della firma e della voce*)

MODELLI DI AUTENTICAZIONE

I modelli a cui si fa riferimento per progettare un sistema di autenticazione dipendono da:

- *tipo di utenti*
- *distribuzione fisica delle risorse*
- *valore delle informazioni da proteggere*
- *altri fattori...*

MODELLI DI AUTENTICAZIONE

1) Autenticazione locale: è quella utilizzata su un computer desktop o portatile.

L'intero sistema, inclusi i meccanismi di autenticazione e controllo degli accessi, risiede all'interno di un singolo perimetro di sicurezza, all'interno del quale l'utente definisce e tiene aggiornate le informazioni di autenticazione

MODELLI DI AUTENTICAZIONE

2) Autenticazione diretta: usata in passato dai server LAN e dai sistemi time-sharing.

Il sistema è usato da molti utenti, anche remoti; autenticazione e controllo degli accessi risiedono in un singolo perimetro fisico; è “diretto” perché centralizzato: un singolo sistema prende le decisioni e contiene il database dei profili utente. Le password sono crittografate

MODELLI DI AUTENTICAZIONE

3) Autenticazione indiretta: usata nei moderni sistemi distribuiti per consentire agli utenti di accedere a più sistemi in rete.

Quando un sistema riceve una richiesta di autenticazione, la inoltra ad un server di autenticazione centralizzato che verifica e conferma l'identità dell'utente (vengono usati i protocolli RADIUS e Kerberos o Active Directory Windows)

MODELLI DI AUTENTICAZIONE

4) Autenticazione off-line: usata nei sistemi che sfruttano l'infrastruttura a chiave pubblica (PKI).

Diversi componenti autonomi prendono decisioni sull'autenticazione degli utenti. È una combinazione dei tre precedenti: autenticazione e controllo accessi risiedono sullo stesso dispositivo, mentre il titolare della sicurezza (la CA, non necessariamente online) mantiene un *db* centralizzato degli utenti autorizzati.

MODELLI DI AUTENTICAZIONE

Esempio: il funzionamento del protocollo SSL

- un browser si procura il certificato con la chiave pubblica dal server da autenticare (ad es. il sito di una banca)
- lo autentica con un'altra chiave pubblica prestabilita (nota al browser - "CA attendibili")
- quindi utilizza la chiave pubblica del server nella fase di scambio dati per la costruzione di una chiave di sessione con cui cifrare le comunicazioni.

GLI SCHEMI DI AUTENTICAZIONE

Elementi comuni dei sistemi di autenticazione

- l'entità da autenticare
- le caratteristiche distintive su cui si basa l'autenticazione
- un proprietario o amministratore del sistema di sicurezza
- un meccanismo di autenticazione che verifica le caratteristiche distintive.

GLI SCHEMI DI AUTENTICAZIONE

- Il meccanismo di controllo dell'accesso è una funzione successiva all'autenticazione, invocato se quest'ultima ha avuto successo

GLI SCHEMI DI AUTENTICAZIONE

Esempio: Bancomat

Entità da autenticare: l'utente.

Caratteristiche distintive: la tessera ed il PIN. Amministratore sistema di sicurezza: la Banca.

Meccanismo di autenticazione: software di validazione delle informazioni fornite dalla scheda e dall'utente.

Se l'autenticazione ha successo e l'utente ha il credito necessario, il meccanismo di controllo dell'accesso autorizza il prelievo

GLI SCHEMI DI AUTENTICAZIONE

Esempio: e-commerce

Entità da autenticare: il proprietario del sito.

Caratteristiche distintive: chiave pubblica in un certificato digitale.

Amministratore sistema di sicurezza: la CA emittente il certificato digitale.

Meccanismo di autenticazione: il software, nel browser dell'utente, di convalida del certificato del sito (protocollo SSL)

GLI SCHEMI DI AUTENTICAZIONE

Fattori di autenticazione di un utente(*)

- qualcosa che sai (password, PIN, ...);
- qualcosa che hai (token, smartcard, ...);
- qualcosa che sei (impronta digitale, retina, iride, volto, voce, ...
(Attenzione: corpo vs. individuo!).

() Carlton et al., “Alternate Authentication Mechanisms”, 1988)*

GLI SCHEMI DI AUTENTICAZIONE

Fattori di autenticazione di un utente(*)

- qualcosa che sai (password, PIN, ...);
- qualcosa che hai (token, smartcard, ...);
- qualcosa che sei (impronta digitale, retina, iride, volto, voce, ...
(Attenzione: corpo vs. individuo!).

() Carlton et al., “Alternate Authentication Mechanisms”, 1988)*

GLI SCHEMI DI AUTENTICAZIONE

Qualcosa che sai

- È uno dei metodi di autenticazione più antichi. Comprende: parole d'ordine (password), frasi (passphrase), PIN (combinazione numerica) ed in genere informazioni note solo al possessore, da usare in risposta a specifiche domande personali.
- L'autenticazione tramite un dato segreto noto solo al possessore è vulnerabile sia per motivi tecnici che per comportamenti insicuri degli utenti: tende ad essere sostituita da combinazioni di più fattori (ad es. scheda + PIN).
- *Il grado di sicurezza peggiora rapidamente quando l'utente scrive le password su carta o le conserva in file non cifrati!*

GLI SCHEMI DI AUTENTICAZIONE

Qualcosa che hai

- Il termine **chiave** in informatica deriva in effetti dalle chiavi di casa, ma può essere semplicemente un file, in passato incorporato in un dispositivo fisico (token).
- L'autenticazione tramite token è la più difficile da violare, poiché l'oggetto fisico deve essere posseduto al momento dell'autenticazione e dell'accesso al sistema.
- L'utente sa se il token gli è stato rubato o è stato smarrito; il token non può essere "condiviso" con altri, costa di più, si può guastare, ma soddisfa le esigenze di sicurezza di un ampio spettro di applicazioni

GLI SCHEMI DI AUTENTICAZIONE

Qualcosa che sei

- Si basa su caratteristiche del corpo umano e, secondariamente, anche su comportamenti unici della persona.
- Queste caratteristiche prima includevano un ritratto, la firma, una descrizione scritta, le impronte digitali;
- oggi i computer permettono di confrontare rapidamente un attributo fisico (caratteristiche biometriche, firma autografa, ...) con una registrazione in un database.



GLI SCHEMI DI AUTENTICAZIONE

Qualcosa che sei: punti deboli

- maggiore costo;
- possibilità di intercettazione;
- identificazione non certa (falsi positivi e falsi negativi);
- variabilità nel tempo;
- trafugamento da parte di terzi con definitiva compromissione dell'autenticazione!

GLI SCHEMI DI AUTENTICAZIONE

Esiste un metodo di autenticazione perfetto?

- Non esiste - almeno per ora - un metodo di autenticazione perfetto: la scelta dipende dai rischi, dai costi e da altri fattori.
- Poiché tutti i metodi presentano inconvenienti e spesso non offrono il livello di protezione richiesto, è sempre più comune utilizzare meccanismi di protezione multipli: essi offrono la cosiddetta **autenticazione forte** perché, **usando più fattori**, ciascuno di essi contribuisce a neutralizzare i punti deboli degli altri.

GLI SCHEMI DI AUTENTICAZIONE

Autenticazione in rete?

- quando si passa dall'autenticazione locale a quella in rete **le cose si complicano**.
- Le tre categorie (qualcosa che sai, hai, sei) si basano su caratteristiche distintive della persona o entità, ma quando tali caratteristiche si traducono in bit che attraversano la rete **nessun meccanismo può fornire la certezza assoluta** che una password o una lettura biometrica siano fornite dal titolare anziché da altri.

GLI SCHEMI DI AUTENTICAZIONE

Autenticazione in rete?

- In rete assieme ai fattori di autenticazione forniti dagli utenti, sono necessarie tecniche che identifichino univocamente i messaggi scambiati e impediscano agli estranei di inserirsi nel dialogo (spoofing)

LE PASSWORD

- Le password sono uno dei più antichi sistemi di autenticazione; i primi computer le conservavano in chiaro in un file.
- Nel 1967 fu introdotto l'hashing delle password, tuttora utilizzato. Il sistema conserva in un file i nomi utente e l'hash delle relative password; durante l'autenticazione, l'hash calcolato in base alla password digitata viene confrontato con quello registrato: se coincidono, l'utente è autenticato.

LE PASSWORD

- Poiché dall'hash è impossibile ricostruire la password, il sistema è relativamente sicuro (a meno di attacchi brute force o dictionary based).
- L'hash delle password può essere aggirato dai programmi di keystroke sniffing.
- L'evoluzione degli attacchi ha portato al network sniffing (analisi del traffico di rete per carpire password, chiavi di cifratura e altre informazioni).

LE PASSWORD

Social engineering

- Un metodo usato per conquistare l'accesso ad un sistema è il social engineering: l'attaccante si fa aiutare da un dipendente, inconsapevole, convincendolo a rivelare le informazioni (come username e password) necessarie ad entrare nel sistema

LE PASSWORD

Social engineering

Uno dei modi più usati consiste nel presentarsi come un tecnico di assistenza, che ad es. ha urgente bisogno del nome utente e password dell'interlocutore allo scopo dichiarato di evitargli la perdita dei dati.

L'attaccante può anche ordinare, con una falsa email apparentemente inviata dal system administrator (vedi phishing), di cambiare provvisoriamente la password - come specificato - per lavori di manutenzione.

LE PASSWORD

Password criteri di scelta

1) Lunghezza

Più la password è lunga, più è difficile da scoprire; la lunghezza minima è di sei caratteri o più, secondo le dimensioni del set di caratteri

LE PASSWORD

Password criteri di scelta

2) Caratteri

Idealmente una password dovrebbe contenere minuscole, maiuscole, cifre ed altri segni, in modo da aumentare il numero di combinazioni (a parità di lunghezza) e di eludere gli attacchi tramite dizionario

LE PASSWORD

Password criteri di scelta

3) Contenuto

Dovrebbero essere esclusi nomi di persone, luoghi, aziende, animali, prodotti, targhe automobilistiche, date, parole del dizionario ed altri nomi o simboli riconducibili all'utente

LE PASSWORD

Password criteri di scelta

4) Assegnazione

Per diversi prodotti hw/sw non è obbligatorio, ma consigliabile, specificare username e password (molte reti WiFi sono ancora installate senza alcuna protezione!)

LE PASSWORD

Password criteri di scelta

5) Periodo di validità

Più frequente è la modifica della password, minore è la probabilità che venga scoperta

LE PASSWORD

Password criteri di scelta

6) Cambiamento

Ogni password assegnata o scelta da un utente dovrebbe essere nuova e differente

LE PASSWORD

Password criteri di scelta

7) Valore di default

Molti dispositivi sono posti in commercio con nome utente e password preimpostati, da modificare all'atto dell'installazione

LE PASSWORD

Password criteri di scelta

8) Conservazione

Se una password dev'essere annotata o registrata, va conservata al sicuro (in cassaforte, cifrata adeguatamente).

LE PASSWORD

Password criteri di scelta

9) Memorizzazione

In teoria una password dovrebbe essere lunga, complicata e memorizzata dall'utente senza lasciarne traccia: ma una password troppo lunga e complicata è meno sicura perché induce l'utente a registrarla (con pericolo di visibilità; meglio una "passphrase")

PASSWORD
INTERNE
ED
ESTERNE

L'uso consigliato delle password varia a seconda che gli utenti siano interni (personale dell'azienda) o esterni (come i clienti che si collegano via Internet)

PASSWORD INTERNE ED ESTERNE

Password interne

Le password interne servono all'autenticazione dei dipendenti e di solito non forniscono un alto livello di protezione, visto che gli utenti hanno accesso fisico al sistema. È superfluo imporre agli utenti interni password complicate

PASSWORD
INTERNE
ED
ESTERNE

Password interne criteri di scelta

1-Usare password mnemoniche

(affinché non vengano scritte), ma difficili da indovinare anche per amici e colleghi

PASSWORD
INTERNE
ED
ESTERNE

Password interne criteri di scelta

2-Disabilitare la scadenza della
password

che induce gli utenti ad
annotare le password

PASSWORD
INTERNE
ED
ESTERNE

Password interne criteri di scelta

3-Incoraggiare gli utenti a
cambiare password

in occasione dei cambiamenti di
configurazione del computer

PASSWORD
INTERNE
ED
ESTERNE

Password interne criteri di scelta

4 - Server

Tenere i server e i dispositivi di
rete sotto chiave

PASSWORD
INTERNE
ED
ESTERNE

Password interne criteri di scelta

5-I posti di lavoro dedicati ad applicazioni critiche

(come paghe e stipendi)
dovrebbero essere situati in
stanze separate chiuse a chiave e
non restare mai incustoditi

PASSWORD
INTERNE
ED
ESTERNE

Password interne criteri di scelta

6-Accesso ai Sistemi

I sistemi cui si accede tramite
single sign-on non usano password
"interne", solo ma "esterne"

PASSWORD
INTERNE
ED
ESTERNE

Password interne criteri di scelta

7-Amministratori

Le password degli amministratori devono essere più forti di quelle degli utenti interni

PASSWORD
INTERNE
ED
ESTERNE

Password interne criteri di scelta

Conclusione

In pratica, all'interno dell'azienda si cerca di mediare tra usabilità e sicurezza: una password troppo complicata per essere usabile diventa una minaccia alla sicurezza quando è scritta su un post-it!

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Una password esterna,
deve essere più complessa
di una interna, protetta con
metodi crittografici e
modificata di frequente

PASSWORD INTERNE ED ESTERNE

Password esterne

In un'azienda, le connessioni remote dovrebbero ricevere un trattamento diverso rispetto alle connessioni interne ed essere filtrate da un dispositivo di sicurezza (firewall, VPN).

Ecco alcune raccomandazioni

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Raccomandazioni

1) Se il sistema gestisce informazioni di particolare valore, anziché normali password si dovrebbero usare token con password single-use, smartcard, token USB e simili

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Raccomandazioni

2) Le connessioni esterne dovrebbero usare protocolli che impediscano il *re-routing* (instradamento verso destinazione diversa) della connessione

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Raccomandazioni

3) Le password esterne dovrebbero resistere agli attacchi di tipo dizionario

4) Le password esterne dovrebbero essere cambiate periodicamente

PASSWORD INTERNE ED ESTERNE

Password esterne

Raccomandazioni

- 5) Le password esterne dovrebbero essere fisicamente protette dagli attacchi interni.
- 6) Le password esterne usate su computer portatili non devono essere conservate sul computer

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Come scegliere una password
esterna

memorizzabile e che resista ai
dizionari?

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Come scegliere una password esterna

1) Scegliere una password a caso, secondo i criteri visti per le password interne

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Come scegliere una password esterna

- 1) Scegliere una password a caso, secondo i criteri visti per le password interne
- 2) Scegliere una seconda password a caso, non avente alcuna relazione con la prima

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Come scegliere una password esterna

- 1) Scegliere una password a caso, secondo i criteri visti per le password interne
- 2) Scegliere una seconda password a caso, non avente alcuna relazione con la prima

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Come scegliere una password
esterna

3) Scegliere a caso una cifra
o segno di punteggiatura
come carattere intermedio

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Come scegliere una password
esterna

4) Costruire la password forte concatenando la prima password debole, il carattere intermedio e la seconda password debole

PASSWORD
INTERNE
ED
ESTERNE

Password esterne

Come scegliere una password esterna

5) Esaminare il risultato e trovare qualche modello strutturale, ritmo, ripetizioni o qualsiasi significato che permetta di memorizzarlo senza doverlo scrivere.

Ad es. “casale9ferrato” è una password resistente, ma abbastanza facile da ricordare.



AUTENTICAZIONE TRAMITE TOKEN

- Token: oggetto della categoria “qualcosa che hai” utilizzato da un utente (o gruppo di utenti) per pagare qualcosa o per un impiego specifico

AUTENTICAZIONE TRAMITE TOKEN

Proprietà fondamentali: il titolare dev'essere in possesso fisico del token per poterlo usare

un buon token è molto difficile da duplicare

una persona può smarrire un token e con esso

perdere l'accesso a risorse critiche

AUTENTICAZIONE TRAMITE TOKEN

Rispetto ad una password, un token offre notevoli benefici:

Elimina l'onere di dover ricordare password complicate;

può contenere un dato segreto molto più complesso di quanto sia memorizzabile da una persona;

è spesso associato ad un secondo fattore di autenticazione, come ad es. un PIN;

un token attivo può generare un output diverso in diverse circostanze oppure ad ogni utilizzo

- Un token può assumere i formati e le dimensioni più svariate: una carta di credito, una chiave, una calcolatrice, un anello ed altro ancora.
- Da un punto di vista funzionale, la principale distinzione è tra token passivi (che si limitano a memorizzare i dati, come ad es. una tessera Bancomat o un dispositivo RFID) e token attivi (dotati di capacità di elaborazione, come ad es. una smartcard con coprocessore crittografico).

AUTENTICAZIONE
TRAMITE TOKEN

CHALLENGE/RESPONSE



Una variante di token di autenticazione utilizza il cosiddetto Challenge/Response



Nella sicurezza informatica, l'autenticazione challenge-response è una famiglia di protocolli in cui una parte presenta una domanda e un'altra parte deve fornire una risposta valida per essere autenticata

BIOMETRIA

La biometria (bios=vita e metron=misura) è la scienza e tecnologia dell'autenticazione misurando le caratteristiche fisiologiche o comportamentali di una persona.

Le caratteristiche fisiche utilizzate per l'autenticazione biometrica sono diverse:

SCHEMI DI AUTENTICAZIONE BIOMETRICA



1) Impronte digitali.

Usate da un secolo e mezzo, mantengono la loro reputazione di unicità per ogni individuo, gemelli inclusi.



Gli scanner di impronte digitali

sono molto diffusi ed hanno un basso costo, molto inferiore a quello degli altri dispositivi biometrici.



SCHEMI DI AUTENTICAZIONE BIOMETRICA

2) Geometria delle mani.

Rispetto alle impronte digitali, che richiedono mani pulite, ha il vantaggio di poter essere usata anche in condizioni ambientali difficili, come fabbriche e cantieri



SCHEMI DI AUTENTICAZIONE BIOMETRICA

3) Retina.

La sua scansione è utilizzata in installazioni militari e governative.

Il modello dei vasi sanguigni della retina è unico e stabile, sebbene siano possibili variazioni (come durante la gravidanza).

La fotografia della retina richiede un'esposizione prolungata a bassa intensità luminosa ed è vista come una procedura intrusiva, sebbene non rechi danno agli occhi.



SCHEMI DI AUTENTICAZIONE BIOMETRICA

4) **Iride.**

Come per la retina, la sua scansione fornisce un modello unico e stabile ed è oggi una delle tecnologie in rapida ascesa per l'adozione in aeroporti e controlli dell'immigrazione.

La foto è ripresa da una certa distanza e presenta difficoltà simili a quelle della retina.

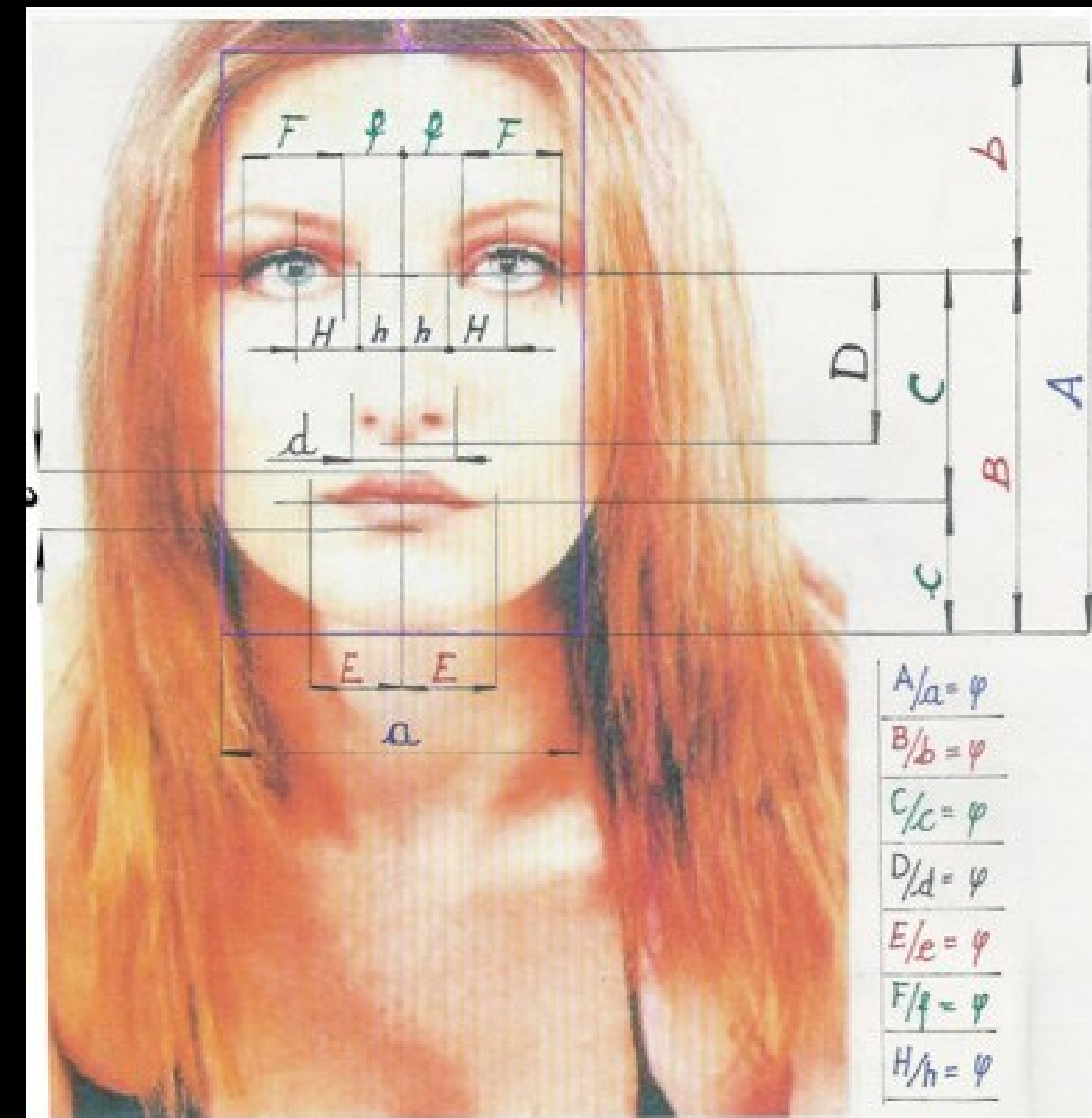


SCHEMI DI AUTENTICAZIONE BIOMETRICA

5) **Riconoscimento del volto.**

È un metodo particolarmente flessibile e può essere utilizzato all'insaputa della persona oggetto della scansione (con i relativi pro e contro).

Può essere usato per cercare un individuo nella folla, a patto che si raggiunga la necessaria precisione di riconoscimento.



SCHEMI DI AUTENTICAZIONE BIOMETRICA



6) **Impronta vocale.**

Come il riconoscimento del volto, l'analisi della voce può essere usata all'insaputa dell'interessato.

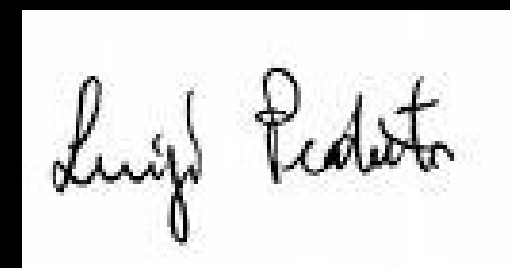
È possibile falsificarla manipolando una registrazione, ma una voce imitata non trae in inganno un analista esperto.

Questa caratteristica a volte è elencata nella categoria dei tratti comportamentali, dato che non si basa sull'osservazione di una parte del corpo.

SCHEMI DI AUTENTICAZIONE BIOMETRICA

Altre caratteristiche comportamentali sono:

Firma autografa. I sistemi di riconoscimento affidabili la confrontano con una registrazione che comprende la dinamica del movimento della penna da parte dell'utente.



Dinamica della digitazione su tastiera.

Esistono alcuni sistemi che riconoscono i comportamenti dell'utente durante la battitura, come il ritardo tra la pressione di varie coppie di tasti. Un vantaggio è che non occorre hardware aggiuntivo



SCHEMI DI AUTENTICAZIONE BIOMETRICA

La diffusione dei dispositivi biometrici ha subito un forte impulso (ad esempio dati biometrici nei passaporti dal settembre 2001) da quando è iniziato un processo di progressivo spostamento del punto di equilibrio tra esigenze di sicurezza e garanzie personali (privacy).

Oggi sono già installati in varie nazioni dispositivi biometrici per il controllo delle frontiere che sono basati sulla scansione delle impronte digitali o della retina

SCHEMI DI AUTENTICAZIONE BIOMETRICA

Per autenticare un soggetto (utente o processo) in un contesto di rete occorre trovare un compromesso fra

- 1-modalità operative ragionevolmente semplici
- 2-un onere amministrativo non eccessivo per i sistemisti
- 3-e un livello di sicurezza accettabile