

# **Esperti nella gestione dei sistemi informativi e tecnologie informatiche**

---

## **Analisi del rischio e Sicurezza delle attività**

**Docente:** Eduard Roccatello  
**Email:** eduard@roccatello.it  
**Sito:** <http://www.roccatello.it/teaching/gsi/>

# Controllo degli accessi

- Controllo degli accessi
  - È la limitazione, imposta da decisioni politiche, all'accesso al sistema e ai dati
    - Se l'attaccante non può accedere ai dati sensibili, certamente non può rubarli
  - Prevenire che attaccanti possano guadagnare accessi
    - Fermandoli appena tentano di farlo

## □ Innanzitutto

### 1. Enumerazione delle risorse

1. Ogni risorsa importante-sensibile deve essere opportunamente enumerata
  1. Risorse umane
  2. File dei server con importanti informazioni dell'azienda
2. Molto difficile da fare bene

### 2. Sensibilità di ogni risorsa

1. Deve essere valutata la sensibilità di ogni risorsa
  1. In particolare le risorse ***mission-critical***, senza le quali il centro non può continuare a funzionare
  2. Altre potrebbe non essere così sensibili da bloccare il centro

## □ Chi dovrebbe avere accesso

1. Deve essere presa una decisione su chi dovrebbe avere accesso a **ciascuna** risorsa
2. Può essere fatta individuo per individuo
3. Ma è più efficiente definire dei ruoli (che sono in numero minore rispetto agli individui)
  1. Utenti logged-in
  2. Amministratori di sistema
  3. Membri del team di progetto

## □ Quali permessi di accesso (autorizzazioni) devono avere

1. I permessi di accesso (autorizzazioni) definiscono **per tutti** se un ruolo (o un individuo) può avere un certo accesso
  1. Se sì, definiscono **esattamente** cosa può essere fatto (o può essere permesso fare) delle risorse con quel ruolo
  2. Usualmente si presentano sotto forma di una lista di permessi per cose concesse agli utenti per ogni risorsa
    1. Leggere
    2. Cambiare
    3. Eseguire
  3. Ogni tipo di risorsa dovrebbe avere una politica di controllo degli accessi

## □ Come dovrebbe essere implementato il controllo degli accessi

1. Per ogni risorsa, occorre una pianificazione di accesso protetto
  1. Per come deve essere implementata la protezione
  2. Secondo la politica di controllo scelta
2. Per un file in un server
  1. Limitare le autorizzazioni al più piccolo gruppo
  2. Irrobustire il server contro gli attacchi
  3. Usare firewall per fermare gli attacchi
3. Le decisioni dovrebbero essere documentate in un ***access protection policy*** per ogni risorsa

## □ **Controllo degli accessi e protezione** *policy-based*

1. Si deve specificare una politica di controllo e una politica di protezione degli accessi per ogni risorsa
2. Questo permette di
  1. Focalizzare l'attenzione su ogni risorsa
  2. Guidare la selezione e la configurazione degli firewall e similari
  3. Guidare l'auditing e i testing periodici

## □ **Sicurezza del sito**

1. Se è vero che la maggior parte degli attacchi viene da Internet
2. Alcuni degli attacchi più devastanti vengono dall'interno
  1. Attenzione alle reti wireless
  2. L'intercettazione può essere effettuata anche al di fuori dell'edificio

## □ Password riutilizzabili

- Una stessa password può essere per accedere più volte a delle risorse in diverse occasioni
- **Pericolosità**
  - un attaccante potrebbe avere il tempo di impararla e poi usarla

## □ Difficoltà di crackare password mediante tentativi remoti

- Se il sistema è ben configurato
  - dopo alcuni tentativi normalmente l'attaccante viene buttato fuori
- **Attenzione**
  - Possibilità di scaricare il file delle password e crackarle su un proprio computer con calma off line

## □ Hacking della password di root

1. In tutti i sistemi esistono dei super account che permettono di compiere qualunque azione in qualunque directory
2. **Hacking della password**
  1. Di root in sistemi LINUX/UNIX
  2. Di administrator in sistemi Windows
  3. Supervisor in sistemi Novell Netware
3. **L'hacking della root è piuttosto rara**
  1. Possono essere hackerate solo ordinarie password utente
4. C'è la possibilità di hacker capaci di **aumentare i propri privilegi** di utente per intraprendere azioni tipiche della root

## □ Cracking fisico delle password

### 1. **Ingenua**, ma non comune pratica:

1. Il sistemista batte la password e poi se ne dimentica

### 2. **L0phtrack**

1. Programma di cracking
  1. Deve girare sul server
    1. Necessita di accesso fisico
  2. O avere una copia del file delle password
    1. Allora può girare su qualunque altra macchina

### 3. Tentativo a forza bruta (***brute-force***)

1. Tentare tutte le possibili combinazioni di caratteri
2. Ovviamente password più lunghe sono più robuste

### **3. Usando più caratteri la password diviene più robusta**

1. Lettere alfabetiche senza maiuscole (26 possibilità)
2. Lettere alfabetiche con maiuscole (52 possibilità)
3. Caratteri alfanumerici (62)
4. Tutte le lettera della tastiera (~ 80)
5. Attenzione
  1. L'attaccante deve provare in media metà delle possibili combinazioni

# Dipendenza dalla lunghezza della password

Lunghezza Password	Alfabetica (N=26)	Alfabetica con maiuscole (N=52)	Alfanumerica: lettere e numeri (N=62)	Tutta i caratteri della tastiera (N=~80)
1	26	52	62	80
2 (N <sup>2</sup> )	676	2,704	3,844	6,400
4 (N <sup>4</sup> )	456,976	7,311,616	14,776,336	40,960,000
6	308,915,776	19,770,609,664	56,800,235,584	2.62144E+11
8	2.08827E+11	5.34597E+13	2.1834E+14	1.67772E+15
10	1.41167E+14	1.44555E+17	8.39299E+17	1.07374E+19

## 4. Gli attacchi a forza brutta sono sufficientemente lenti e inefficienti

## 5. **Attacchi a dizionario**

1. Vengono tentate le parole comuni
2. Survey della Pentasafe Secrity Technologies
  1. 25% usa parole comuni di dizionario (es. banana)
  2. 50 % basa le password sui nomi dei familiari, amici, favoriti (pets)
  3. 30 % usa nomi di idoli dello sport o dello spettacolo
  4. 10 % basa le password su nomi fantastici
  5. Solo 10 % usa password complesse, difficili da crackare
3. Ce ne sono solo qualche migliaio
  - **Cracking veramente rapido**

## 6. Attacchi ibridi

1. Molti utenti tentano (invano) di irrobustire le password, ad esempio
  1. Aggiungendo una cifra all'inizio o alla fine della parola
  2. Sostituendo la lettera "o" con la cifra "0"  
Sostituendo la lettera "l" con la cifra "1"
2. Gli attacchi ibridi tentano tutte le semplici modifiche delle parole comuni

## 7. Efficacia del cracking delle password

1. Password lunghe e non-parole sono ancora molto difficile da crackare con gli ordinari computer
2. Per particolari scopi vengono usate delle macchine costruite ad hoc o cluster di pc
  1. Non vengono usati contro normali aziende

# □ Politiche per le password

## 1. Buone password

1. Ogni azienda dovrebbe avere una politica che richieda password robuste
2. Esempio di buona politica per le password
  1. Lunghezza di almeno 8 caratteri
  2. Avere almeno un cambio di minuscolo/maiuscolo, ma non all'inizio
  3. Avere almeno una cifra, ma non alla fine
  4. Avere almeno un carattere non alfanumerico, ma non alla fine
  5. Esempio: cor6#Rere
    1. Variante di una parola per questioni di memorizzazione
    2. Meglio che scriverla su un foglietto

## 2. Testing e rinforzo delle password

1. Far girare dei programmi di cracking sul proprio server per testare il rispetto della politica
2. Forzare la scelta – richiesta di approvazione

## 3. Durata delle password

1. Una password dovrebbe essere cambiata almeno ogni 3 mesi
2. Password critiche devono essere cambiate molto più spesso

## 4. Password condivise (*shared*)

1. Dovrebbero essere proibite
  1. Usare piuttosto politiche di privilegi di gruppo
2. Non possono essere cambiate facilmente
  1. Devono essere comunicate a tutti
3. In caso di incidente non si riesce ad individuare facilmente il possibile colpevole

## 5. Disabilitare le password non più valide

1. Cancellare la password
  1. Appena un dipendente lascia il centro
  2. Appena un consulente e un appaltatore finisce il rapporto di lavoro
  3. In molti centri, una larga percentuale (30-60 %) di tutti gli account sono assegnati a persone che non sono più nel centro

## 6. Password perse

1. Password reset: occorre fornire nuove password per l'account
2. Costituiscono una buona opportunità per attacchi **social engineering**
3. Evitare di lasciare la password cambiata nella segreteria telefonica

## 5. Reset automatico delle password

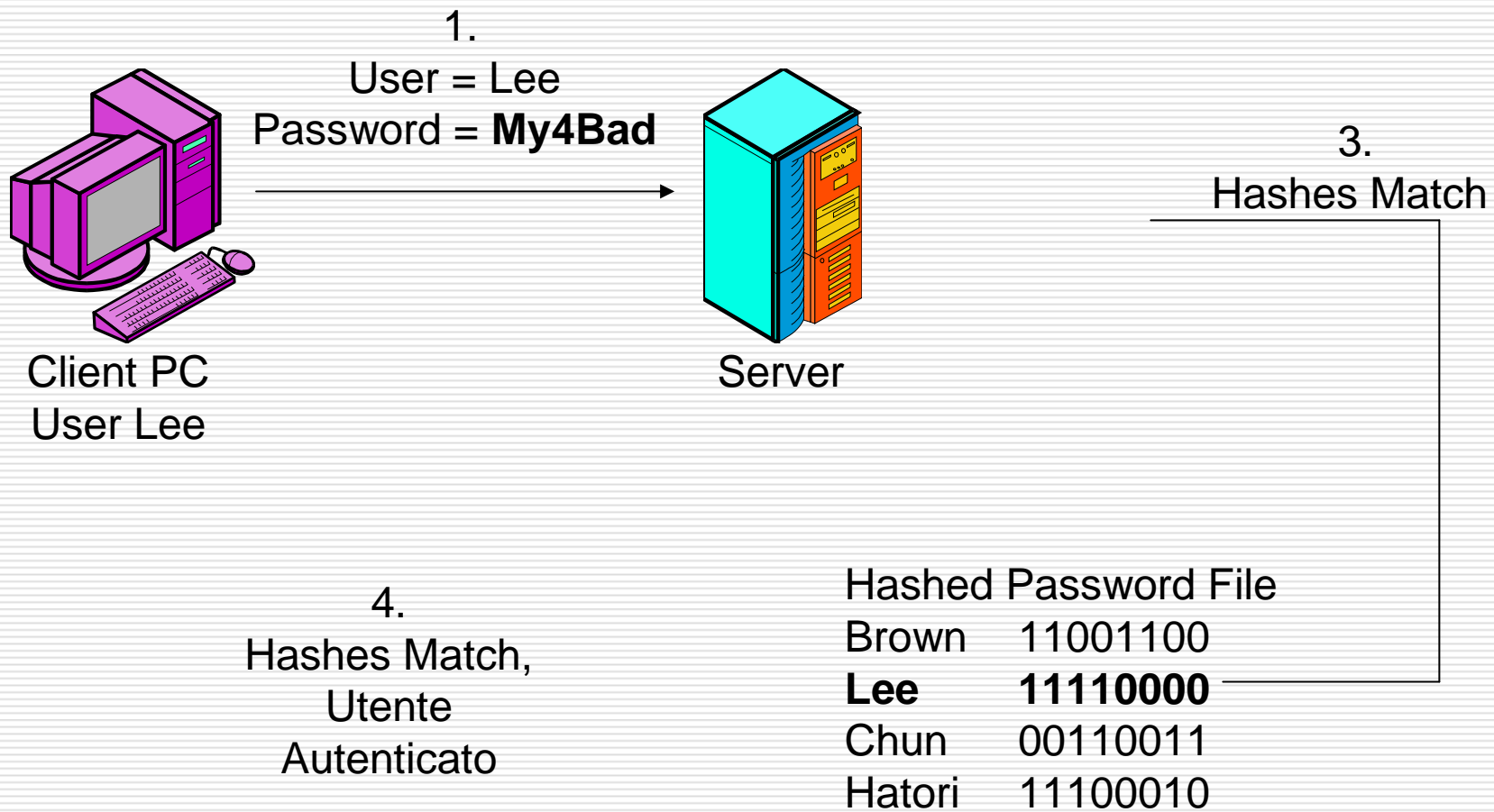
1. I dipendenti si collegano via WEB
2. Devono rispondere a delle domande personali, del tipo "qual è il nome da nubile di tua madre"
3. Attenzione alle domande semplici: le risposte potrebbero essere state precedentemente raccolte facilmente con una ricerca su quella persona

## □ Files per password crittografate

1. Per rendere le cose più difficili per i cracker, i Sistemi Operativi crittografano i file delle password
  1. Viene usato il DES o una sua variante
  2. O l'hashing mediante MD5
    1. Per aumentare la difficoltà vengono crittografate la password più due lettere (**salt**)

## 2. UNIX / LINUX

1. La cifratura delle password in UNIX è una funzione non invertibile
2. Quando un utente batte la password
  1. Il server cripta la password
  2. La password criptata viene confrontata con quella memorizzata



### **3. Le password cifrate offrono una considerevole sicurezza**

1. Non sono conosciute neanche dall'amministratore
2. Il file contiene la password criptata
3. E questa non è invertibile

### **4. Attenzione**

#### **1. Se l'attaccante riesce a prendere il file delle password ha tutto il tempo per crackarle**

1. Vengono generate delle password
2. Vengono criptate e poi confrontate con quelle del file

# 1. La maggior parte dei sistemi UNIX ha un file **/etc/passwd** che ha diversi campi

*Senza file Shadow Password*

<u>User Name</u>	<u>User ID</u>	<u>GCOS</u>	<u>Shell</u>
<b>plee</b>	<b>6babc345d7256</b>	<b>47:3</b>	<b>Pat Lee:/usr/plee:/bin/csh</b>
	Password	Group ID	Home Directory

## 4. File di password con shadow

1. Il file delle password è visibile da tutti i processi
  1. Può essere copiato
  2. Decriptato con calma
2. Le reali password sono memorizzate in un'area accessibile solo da root
  1. La vera password è sostituita da una x
3. Attenzione:
  1. Alcuni software girano con privilegi di root
  2. Un attaccante può impossessarsi del controllo di tali programmi
  3. Può avere accesso al file shadow delle password

`plee:6babc345d7256:47:3:Pat Lee:/usr/plee:/bin/csh`

`plee:x:47:3:Pat Lee:/usr/plee:/bin/csh`

## 5. Password di Windows Server LAN Manager

1. Ha diversi punti di debolezza e quindi non dovrebbe essere utilizzata
2. Le password sono **effettivamente** limitate a soli 7 caratteri
  1. Possono essere create password di 14 caratteri
  2. Ma sono divise in due parti da 7 caratteri
    1. Piccolocane ↔↔ Piccolo + cane
    2. cane (solo 4 caratteri) può essere facilmente crackata
    3. Da questa e dal contesto generale si può risalire alla password integrale

## **6. Password di Windows Server NT LAN Manager (NTLM)**

### 1. Versione 1

1. Vengono permesse password più lunghe
2. Case sensitive
3. Divise in due stringhe

### 2. Versione 2

1. NTLMv2 è anche più forte

### 3. NTLM può imporre che le password siano forti

1. Ma attenzione: non è di default

## **7. Disabilitare delle password LAN Manager**

1. La maggior parte delle versioni di Windows Server permettono le password LAN Manager per compatibilità all'indietro
2. Quando si installa Windows Server si deve disabilitare questo tipo di password
3. Non è del tutto sicuro ad attacchi ripetuti

## **8. *Shoulder (spalla) surfing***

1. L'attaccante osserva l'utente che batte la password
2. Anche pochi caratteri visti possono agevolare notevolmente l'attaccante nei tentativi

## 9. Keystroke Capture Software

1. La password può essere catturata
  1. Si può impiantare un programma per la cattura della battitura nel computer
2. Protected RAM password
  1. Quando viene battuta la password i caratteri vengono memorizzati in uno speciale buffer della RAM
  2. Per cattura la password basta leggere questo buffer
  3. Deve essere protetto: solo il Sistema Operativo può accedere a tale area
    1. Lo fanno: UNIX Window server, 2000 e XP professional
    2. Non lo fanno i sistemi operativi *consumer*: Windows 98, ME e XP home

### 3. Trojan Horse Password Capture Software

1. ***Un cavallo di Troia*** è un programma che sembra essere una cosa, ma in realtà è altro
1. L'attaccante impianta un cavallo di Troia
2. Per esempio
  1. Il programma presenta la solita faccia del programma di login
  2. Chiede all'utente di ribattere la password
  3. Cattura la password
  4. La trasmette all'attaccante

## **10. Windows 95 – 98 – ME**

1. Le versioni consumer non hanno una versione di login screen sicuro
  1. Può essere bypassato battendo escape
2. Le versioni professionali e server lo hanno sicuro

## **11. BIOS Password**

1. Permettono di mettere in sicurezza il boot
2. Ma attenzione: se l'attaccante ha il tempo e la tranquillità (non deve essere visto)
  1. Può rimuovere la batteria
    1. Vengono cancellati tutti i setup del BIOS
    2. Vengono ripristinati i setup precedenti, tranne la password
    3. la password è disabilitata

## **12. Screensaver con Password**

1. Lasciando il PC acceso dopo il login
2. La password viene bypassata
3. Usare screensaver con password (disponibile in Windows)
4. Non è un problema da sottovalutare

## **13. Windows NT / 2000 / XP**

1. Ha una gestione più robusta
2. Non si può bypassare il logon semplicemente con un escape

# Costruire la sicurezza

## 1. Mettere al sicuro l'edificio

1. Unico punto di ingresso
  1. Controllare l'accesso dall'esterno
  2. Un solo ingresso con i dovuti controlli di identità e di credenziali
2. Altri ingressi alternativi
  1. Porte antincendio
    1. Devono avere l'allarme
    2. Devono essere monitorate mediante telecamere a circuito chiuso (CCTV)

### **3. Security Centers**

1. Banca di monitor TV (CCTV) per visualizzare i corridoi e le porte critiche
2. Devono essere conservati i videotape
  1. Per evidenziare colpe
  2. Disciplinare i dipendenti
  3. Allarmi

### **4. Interior Doors**

1. È necessario che il centro si doti di porte interne
2. Riducono la mobilità in zone interne in cui il controllo è più difficile

## 5. Piggybacking

1. Tenere la porta aperta in modo che qualcuno possa entrare **senza identificazione**
2. È comune perché non ci si vuole comportare scorteseamente con chi viene dopo

## 6. Enforcing Policies

1. I tipi di errori di sicurezza precedenti mostrano la debolezza (non voluta, ma pur sempre debolezza)
2. Rinforzare le politiche di controllo

## 7. Training Security Personnel

1. Importanza dell'educazione e del training
2. Il personale di controllo deve imparare a controllare **con cura** l'identità e le credenziali

## 8. Formazione degli impiegati

1. Tutti i dipendenti devono essere educati a segnalare ogni presenza di persona non abituale o sospetta
2. Generare un clima di attenzione a chi è presente
3. Tutti i dipendenti devono avere segnato in evidenza il numero di telefono del centro di sicurezza
4. Prestare attenzione al piggybacking
  1. deve essere assolutamente evitato
5. Attenzione al possibile ***dumpster diving*** (cercare negli scarti)
  1. Tenere gli scarti in un'area chiusa e visibile
  2. Spaccare, piuttosto che riformattare, i dischi e similari

# Access Cards

## **1. Identity badges o identity cards**

- Usate per l'accesso al centro e per le porte interne
- Usate per l'accesso all'account sul computer

## **1. Magnetic Strip Card**

1. Tipo il Bancomat
2. Possono contenere informazioni individuali

## **2. Smart Card**

1. Hanno un microprocessore e RAM
2. Permettono un processo di riconoscimento più sofisticato

### **3. Tokens**

3. Piccolo device con una password che cambia continuamente ed è visibile sullo schermo, che deve essere battuta
4. È una password one-time

### **4. Radio-Frequency ID (RFID)**

3. Può essere individuata e testata senza contatto fisico
4. Permette un facile controllo degli accessi

## **Card Cancellation**

Se la card o il token viene perso occorre provvedere subito a disabilitare l'accesso  
Necessità di un sistema centrale  
La perdita purtroppo è troppo frequente

## 2. Two-Factor Authentication

### 1. PIN

1. **Personal identification number** da battere quando si usano carte di accesso
2. Rappresentano una buona robustezza, soprattutto contro lo smarrimento di card

### 2. Short PIN

1. 4-5 cifre
2. Deve essere corto perché deve essere immesso manualmente
  1. Questa manualità consente ad un'eventuale attaccante di provare un PIN solo ogni 2 secondi
  2. Dovrebbe essere scelta una combinazione non ovvia (quale ad esempio 12345)
3. La combinazione card + PIN consente il **two-factor authentication**

# Autenticazione Biometrica

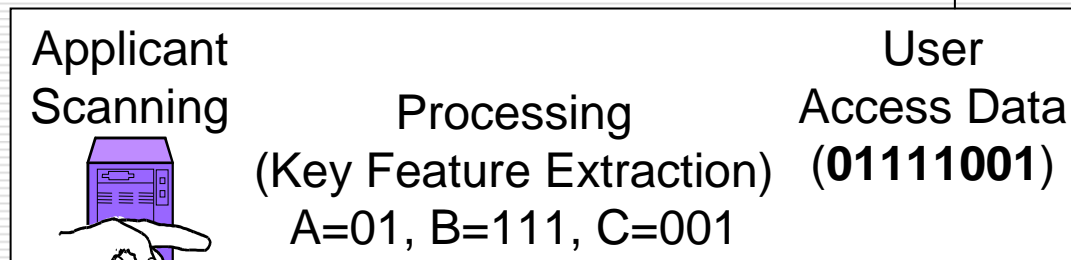
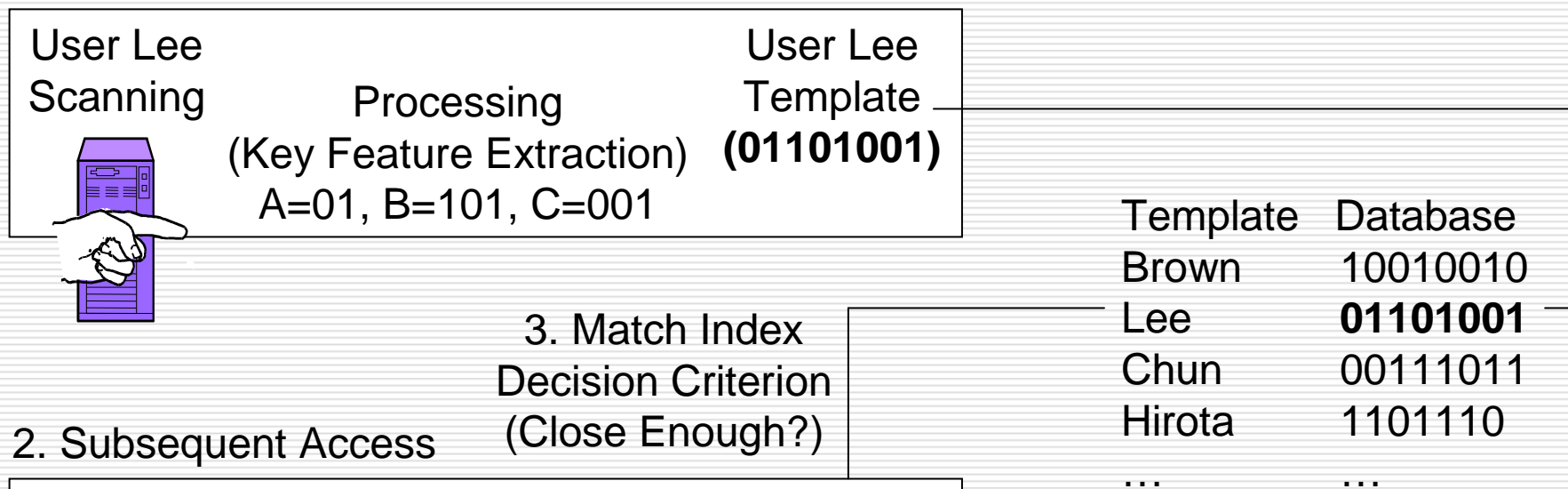
## 1. Biometric Identification

1. Autenticazione basata su misure del corpo o dei suoi movimenti
2. Non si ha il problema di perdita o dimenticanza
3. Ognuno porta con sé il proprio corpo
4. Le misure possono essere basate su
  1. Impronta digitale
  2. Configurazione dell'iride
  3. Volto
  4. Geometria della mano

## 2. Biometric Systems

### 1. Registrazione, successivi tentativi di accesso, accettazione o rifiuto

#### 1. Initial Enrollment



### 3. Verifica ed autenticazione

#### 1. Verifica

1. Il candidato è chi dice di essere?
2. Viene fatto il confronto con **un solo** template
  1. **One-to-one compararison** tra il candidato e un singolo profilo
  2. Il sistema prende la decisione di accesso sulla base della probabilità che il candidato sia effettivamente chi dice di essere

#### 2. Identificazione

1. Chi è il candidato
2. È compito del sistema identificare il candidato
3. Viene confrontato con tutti i template
4. Più difficile della verifica: decisione effettuata sulla base del match più probabile

### **3. Confronto tra i due metodi**

1. La verifica è ovviamente più facile dell'identificazione
2. La verifica va bene per rimpiazzare le password
3. L'identificazione va bene per l'accesso a porte e altre situazioni in cui introdurre il nome risulta difficoltoso

## 4. Precisione

1. Alcuni metodi fanno meno errori di altri
2. Può dipendere dalle condizioni ambientali

### 1. False Acceptance Rate (FAR)

1. Percentuale di persone non autorizzate accettate
  1. Persona accettata erroneamente come membro di un gruppo
  2. Persona che può passare attraverso una porta (e quindi entrare in un particolare ambiente) senza permesso
  3. Le accettazioni errate sono molto pericolose per la sicurezza

## 2. False Rejection Rate (FRR)

1. Percentuale di persone autorizzate che vengono rifiutate
  1. Ad esempio ad una persona valida viene negato l'accesso ad una porta o ad un server

## 3. Può essere ridotta permettendo più tentativi

1. Alte FRR possono infastidire gli utenti e causare il rigetto di tale tecnica di riconoscimento

## 4. Vendor Claims

1. Le dichiarazioni dei venditori sia per i FAR sia per i FRR tendono ad essere esagerati perché spesso i test vengono eseguiti in ambienti ideali
  1. Pochi soggetti presenti nel database
  2. Illuminazione perfetta e lettori perfettamente puliti

## 5. User acceptance

1. È cruciale
2. Una forte resistenza da parte degli utenti può rendere inservibile il sistema
  1. L'impronta digitale può avere una connotazione criminale
3. Alcuni metodi sono complicati da usare
  1. Ad esempio il riconoscimento dell'iride richiede che l'occhio sia in una particolare posizione per avere un buon riconoscimento

## **6. Metodi di riconoscimento biometrico**

### **1. Fingerprint recognition**

1. Riconoscimento delle impronte digitali
2. Semplice, poco cara, ben provata
3. Sicurezza debole
  1. Può essere ingannata facilmente con copie nei casi in cui non ci sia il controllo 3D
  2. Possono essere ingannati da impronte prelevate da quelle lasciate su oggetti
  3. Utile nelle area con una modesta richiesta di sicurezza

## 2. Iris recognition

1. Determinazione di configurazione nella parte colorata dell'occhio
2. È probabilmente la più sicura
  1. FAR veramente bassa
3. È piuttosto cara e difficoltosa, per cui se ne fa un uso limitato
  1. L'occhio deve essere ben posizionato altrimenti viene rigettato
  2. L'utente deve essere abituato
  3. Alta FRR

### **3. Face recognition**

1. Le caratteristiche del volto possono essere rilevate da alcuni metri di distanza
2. Utile per il controllo degli accessi alle porte
3. Facile identificazione di persone non autorizzate
4. Sensibile alla differenza di illuminazione

### **4. Hand geometry**

1. Basati sulla forma della mano
2. Abbastanza facile misurare le caratteristiche di una mano
  1. Lunghezza delle dita
  2. Larghezza delle dita
  3. Larghezza del palmo
3. Usato per l'accesso alle porte

## **5. Voice Recognition**

1. Facile da usare
2. Alta FRR (frustra gli utenti)
3. Debole: facile da ingannare mediante registrazioni

## **6. Keystroke Recognition**

1. Ritmo di battitura
2. Normalmente usato per le password
3. Utilizzato durante una sessione potrebbe permettere una continua autenticazione

## **7. Signature Recognition**

1. Basato sul riconoscimento della configurazione e della dinamica della firma

## **8. Si può ingannare la biometria?**

### **1. Applicazioni di face recognition per aeroporti generano troppi errori**

1. Prova di 4 settimane di face recognition a Palm Beach International Airport
  1. Usati solo 250 volontari in database degli utenti (non realistico – troppo piccolo)
  2. I volontari sono passati e ripresi 958 volte
  3. Sono stati riconosciuti 455 volte (50 % !!)
2. La percentuale di riconoscimento diminuisce ancora di più se le persone portano occhiali (in particolare lenti colorate)
3. C'è da aspettarsi un peggioramento
  1. Con database più larghi
  2. Con foto più scadenti

## 9. U.S. Department of Defence

1. Test indica un basso livello di accettazione
  1. 270 persone
  2. Face recognition ha riconosciuto solo il 51 % di volte
  3. Iris recognition il 94 % di volte (errore del 6% non è accettabile)
2. C'è da aspettarsi un ulteriore peggioramento con database di grandezza reale

## **10. Tecniche di imbroglio 😊**

### **1. Un magazzino tedesco ha notato un inganno con la maggior parte dei sistemi face e fingerprint recognition**

#### 1. Per i fingerprint

1. Bastava soffiare sui sensori per ingannare il sistema
2. Mettendo un sacchetto con acqua sui sensori il sistema lo riconosceva come il precedente utente

### **2. Il prof. Matsumoto**

#### 1. Ha creato un calco in gelatina di impronte

1. È riuscito ad ingannare per l'80 % di volte 11 scanner commerciali

#### 2. Ha creato dei calchi di impronte dall'impronta latente sul vetro (invisibile a occhio nudo)

1. Anche in questo caso ha avuto un 80 % di inganni-successo