La firma elettronica

Codice dell'amministrazione digitale

D.Lgs. 7 marzo 2005, n. 82, aggiornato con D.Lgs. n. 159 del 4 aprile 2006

- Art. 1. Definizioni.

-q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;

Art. 21 Valore probatorio del documento informatico sottoscritto.

1)Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

La firma elettronica

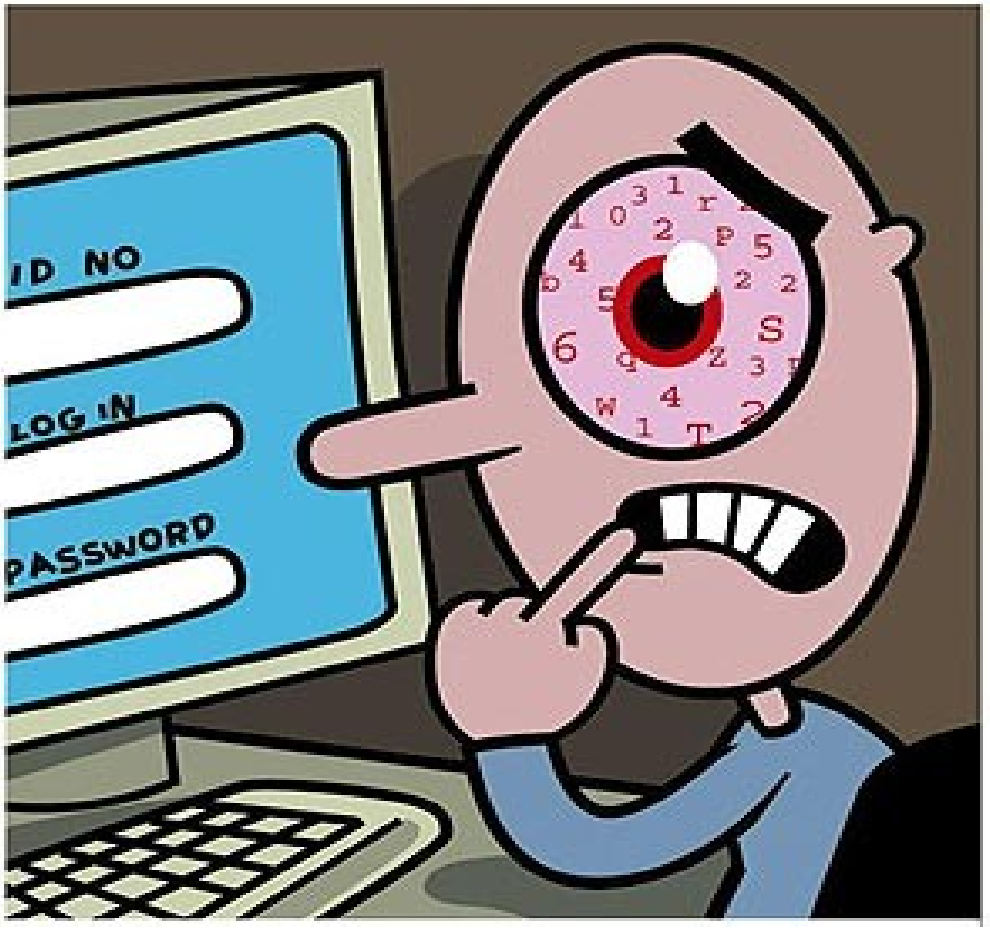
- La firma elettronica e' anche detta firma debole o leggera vs la firma digitale o forte o pesante
- La firma elettronica ha minori requisiti di sicurezza e quindi minore efficacia probatoria
- La firma elettronica puo' essere realizzata con qualsiasi strumento

  -password
  -PIN
  -digitalizzazione della firma autografa
  -tecniche biometriche...

  in grado di conferire un certo livello di autenticazione a dati elettronici

Le password

Le password



Autenticazione basata sulle password

- L'utente possiede una password segreta

  -tipicamente una stringa di 6-10 caratteri
- Il sistema la controlla per autenticare l'utente

  -e' una chiave segreta condivisa tra utente e sistema
- L'utente inserisce una coppia (userid,password)

  -userid e' la dichiarazione dell'identita'
  -password e' l'evidenza che supporta la dichiarazione sopra
- La dimostrazione della conoscenza della chiave e' accettata dal sistema come conferma dell'identita'

Autenticazione basata sulle password

- **Problemi**:

  -E' difficile mantenere segreto il file delle password (dove vengono memorizzate)

  -Quanto e' facile indovinare una password?

  -Come si controlla la password?

  -La password puo' essere vista mentre transita dall'utente al sistema

Autenticazione basata sulle password

- **Problemi**:

  -E' difficile mantenere segreto il file delle password (dove vengono memorizzate)

Autenticazione basata sulle password

- E' difficile mantenere segreto il file delle password (dove vengono memorizzate) (es. banca)

  -**File delle password in chiaro**

  -modo piu' ovvio

  -puo' essere protetto consentendo solo all'amministratore del sistema la lettura e scrittura

  -un cattivo amministratore potrebbe mandare il file a qualcuno

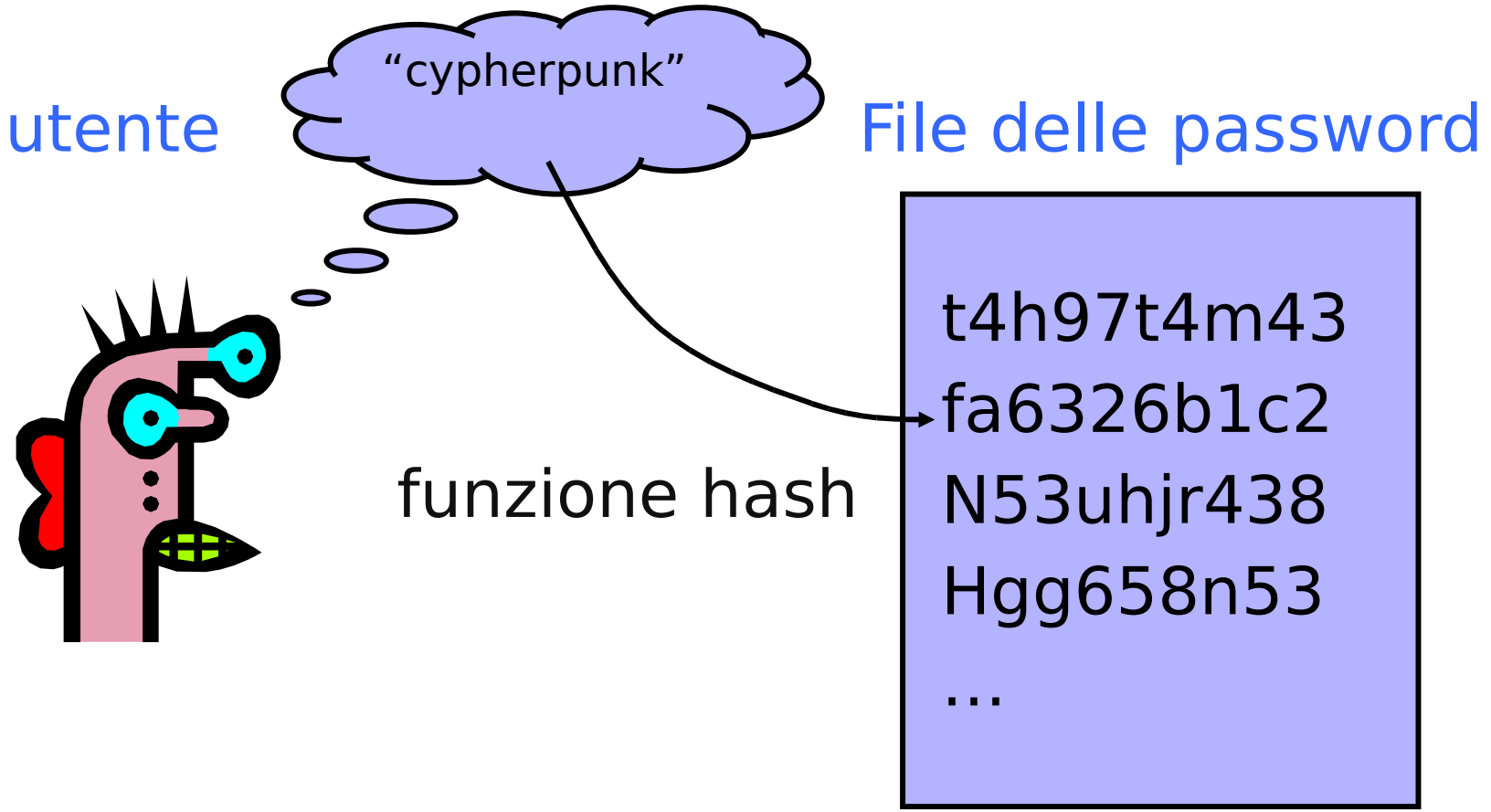
Autenticazione basata sulle password

- **File delle password crittato**

  -si memorizza l'hash one-way delle password, cioe' H(password) invece di password (quindi da H(password) e' difficilissimo ricostruire la password)

  -per verificare il sistema riceve una password, ne calcola l'hash e lo confronta con quello memorizzato

Esempio: file delle password in UNIX



Autenticazione basata sulle password

- **Problemi**:

-Quanto e' facile indovinare una password?

-Le password non sono veramente casuali: date 52 lettere (maiuscole e minuscole), 10 cifre, 32 simboli di punteggiatura, ci sono

$$(52+10+32)^8 = 94^8 \approx 6 \times 10^{16}$$

possibili password di 8 simboli

-Normalmente scegliamo parole che si trovano nel dizionario, nomi di persone o animali

$\approx$ 1 milione di password comuni

Attacchi con il dizionario

- Il file delle password che si trova in /etc/passwd e' accessibile da tutti

- L'attacco con il dizionario consiste nel calcolare l'hash di tutte le parole di un dizionario (lo si fa una volta per tutte) e controllare se il risultato si trova nel file delle password

  - un attacco di forza bruta (per tentativi) online si fa in media in 14 ore

Attacchi con il dizionario

- **Nuove regole:**

  -lunghezza minima della password

  -deve contenere almeno un carattere per ogni categoria (maiuscole, numeri,simboli)

  -verificare che la password non sia in qualche dizionario esistente

  -verificare che la password non contenga informazioni connesse all'account (login, ecc.)

- In generale si potrebbe usare un hash relativamente lento (per evitare attacchi per tentativi)
- Si potrebbe memorizzare una frase invece di una parola (passphrase)
- numero massimo di tentativi per rallentare

Passwords Are Like Underwear

Attacchi con il dizionario

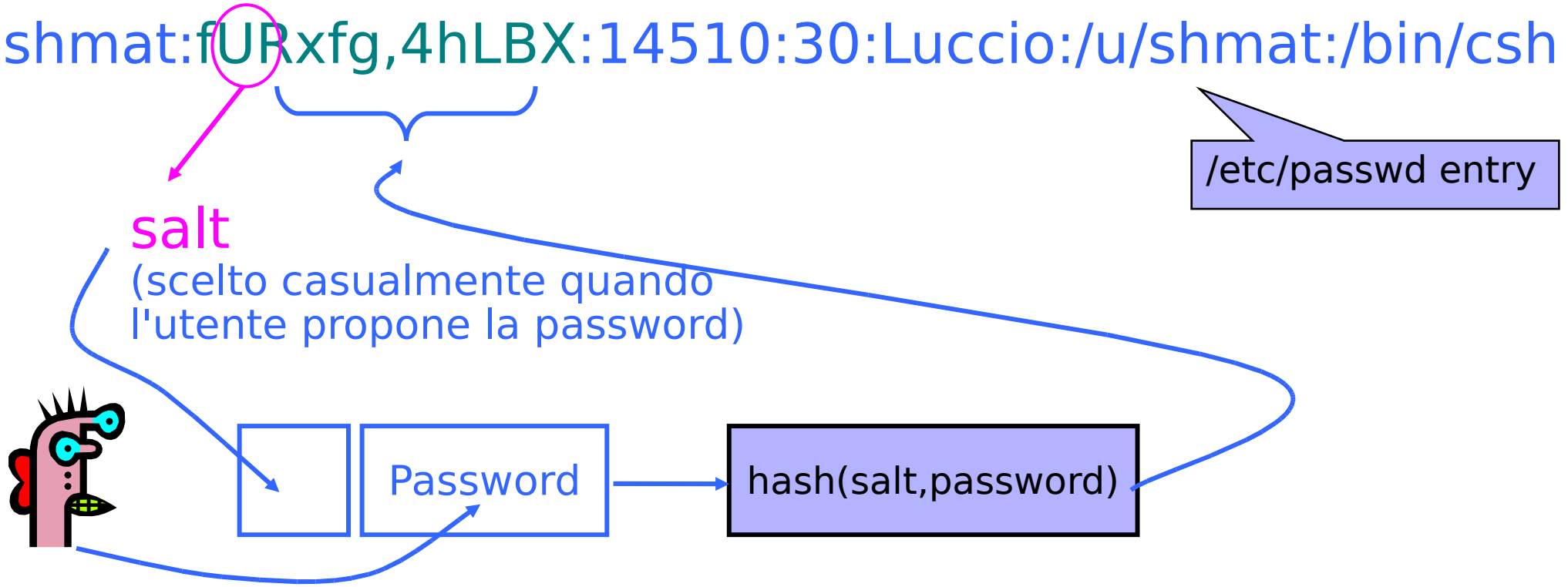
- **Il salt:**

  -Per diminuire la possibilita' di un attacco una password puo' essere aumentata con una stringa casuale di t-bit (salt o seme) prima di applicare la funzione hash one-way

  -La funzione hash della password e salt, unita al salt, vengono memorizzati nel file delle password

  -E' ancora possibile un attacco ma piu' difficile

Salt



- Utenti con la stessa password hanno entrate diverse nel file delle password

Shadow Passwords

shmat:x:14510:30:Luccio:/u/shmat:/bin/csh

in /etc/passwd

La password hashed non e' memorizzata in un file leggibile da tutti

- Le password hashed sono memorizzate nel file /etc/shadow leggibile solo dall'amministratore del sistema
- Si aggiungono anche date di scadenza delle password

I PIN

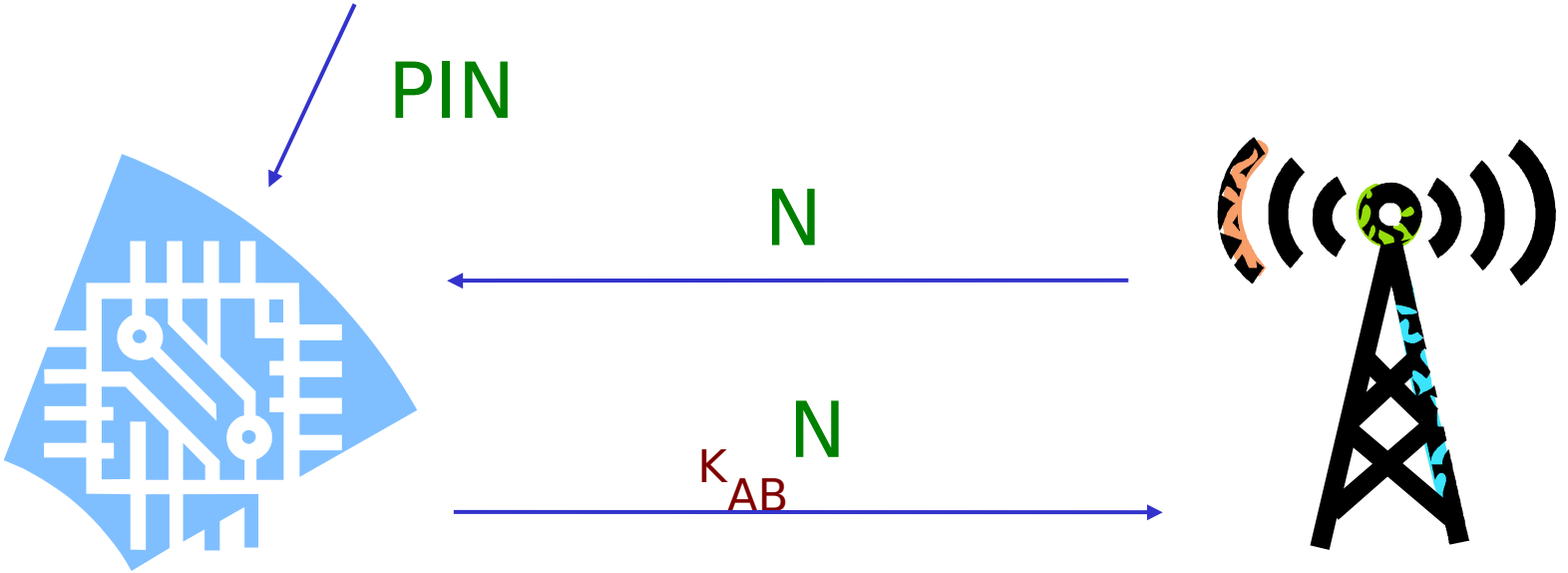
Smartcard: telefoni cellulari

- La smartcard e' una evoluzione della carta magnetica
- Simile a un piccolo computer: ha una memoria e un microprocessore
- Esegue algoritmi crittografici
- Memorizza informazione in modo sicuro
- Difficilmente clonabile

Smartcard: telefoni cellulari

La chiave K_{AB} è memorizzata sulla smartcard
-e' condivisa fra utente e provider

Tecniche combinate: Alice deve ricordare solo un PIN
(Personal Identification Number)



Alice: il dichiarante

Provider: il verificatore

Smartcard: telefoni cellulari

-Un meccanismo di protezione del PIN si basa sul limitare il numero di tentativi possibili

-Per iniziare una nuova comunicazione l'utente e il provider si accordano su una chiave di sessione (utilizzando la chiave condivisa)

-la comunicazione GSM e' crittata

Rafforzare il sistema di password

-Basarsi sulla difficolta' del computer di
  -riconoscere visi diversi, per le persone e' piu' semplice (es. per entrare in un sistema l'utente deve scegliere lo stesso viso in una sequenza di tanti visi diversi)
  -riconoscere immagini diverse gli attacchi col dizionario alle immagini sono difficili: le immagini sono considerate oggetti molto casuali
  -soluzione difficoltosa perche' bisogna memorizzare le immagini

-Aggiungere meccanismi biometrici (es. timbro vocale, ecc.), la revoca pero' diventa piu' difficoltosa

Ricordarsi vs. riconoscere, un approccio diverso!

Bisogna RICORDARSI una password

Basta RICONOSCERE una faccia

Simile al test sotto dove bisogna “completare”

Completare la sequenza

1 2 3 g f w y

_____

Scelta multipla

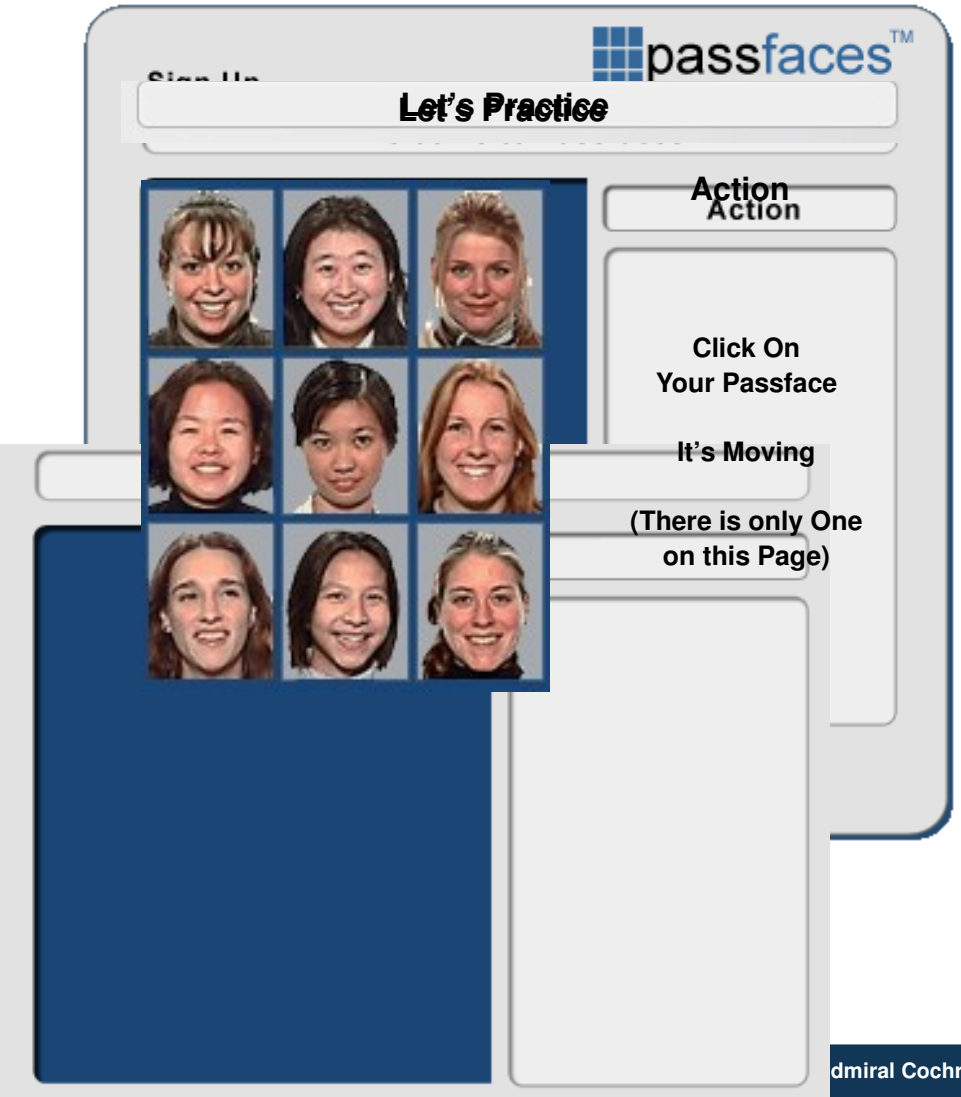
Come funziona Passfaces?

Libreria di facce

Interfaccia utente

A ogni utente e' associato un insieme di 5* Passfaces

I nuovi utenti seguono una procedura per imparare a usare il sistema



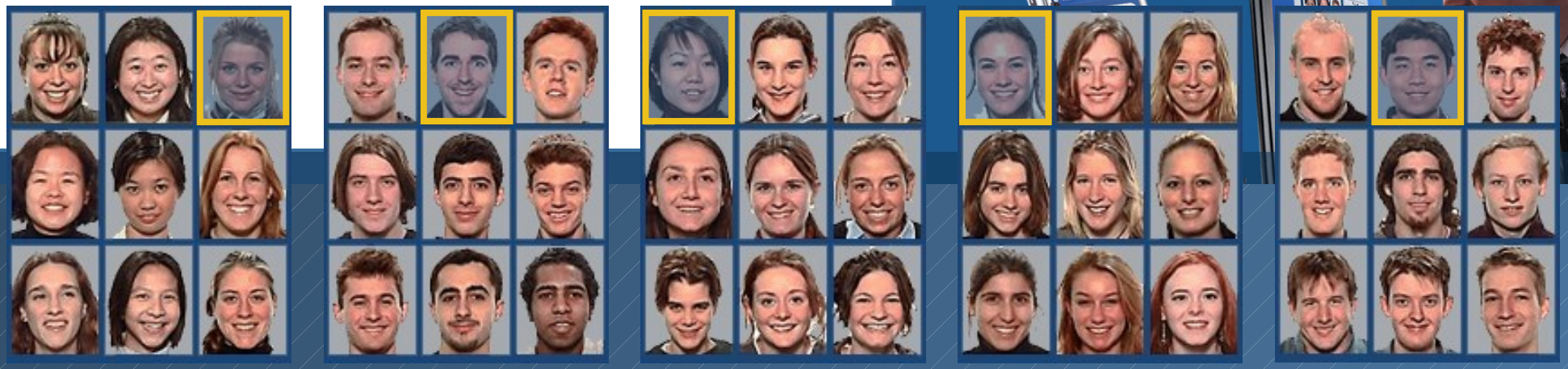
- La procedura dura 2-4 minuti e l'utente impara a usarla

Come funziona Passfaces

- vengono scelte 5 Passfaces e 40 visi diversi
- Le Passfaces vengono presentate in 5 matrici 3x3 contenenti 1 Passface e 8 visi diversi

passfaces™
STRONG AUTHENTICATION

The Only Fully Scalable Means to Replace or Reinforce Passwords



Un nuovo meccanismo di autenticazione

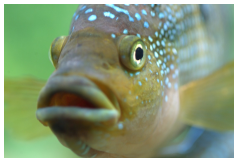
- **Passfaces rappresenta un nuovo meccanismo di autenticazione basato sul riconoscimento:**

  la "*Cognometrics*"

Scegliere immagini diverse

Bisogna inventarsi una
storia per una immagine
o una sequenza di immagini
(bisogna ricordarsi l'ordine)

pesce-donna-ragazza-mais




Sistemi biometrici

Sistemi biometrici

- Biometrica, dal greco bìos (= vita) e metros (= misura)
- La biometria è la scienza che ha come oggetto di studio la misurazione delle variabili fisiologiche o comportamentali tipiche degli organismi, attraverso metodologie matematiche e statistiche.

Sistemi biometrici

- In informatica, i sistemi biometrici misurano e analizzano le caratteristiche del corpo umano allo scopo di identificare una persona
  - Impronte digitali
  - Pattern dell'iride e della retina
  - Riconoscimento del viso
  - Geometria delle mani e delle dita
  - Riconoscimento firma
  - Riconoscimento voce
  - DNA
  - Riconoscimento scrittura alla tas
  - .....

Sistemi biometrici statici e dinamici

- Statici (fisici) : sfruttano una caratteristica sempre presente
  - Impronte digitali, iride o retina, ...
- Dinamici (comportamentali): sfruttano una caratteristica comportamentale
  - Modo in cui si firma, modo in cui si digita sulla tastiera, modo in cui si parla, ...

Esempio

- sistema di riconoscimento dell'iride all'aeroporto di Heathrow

Esempi di sensori

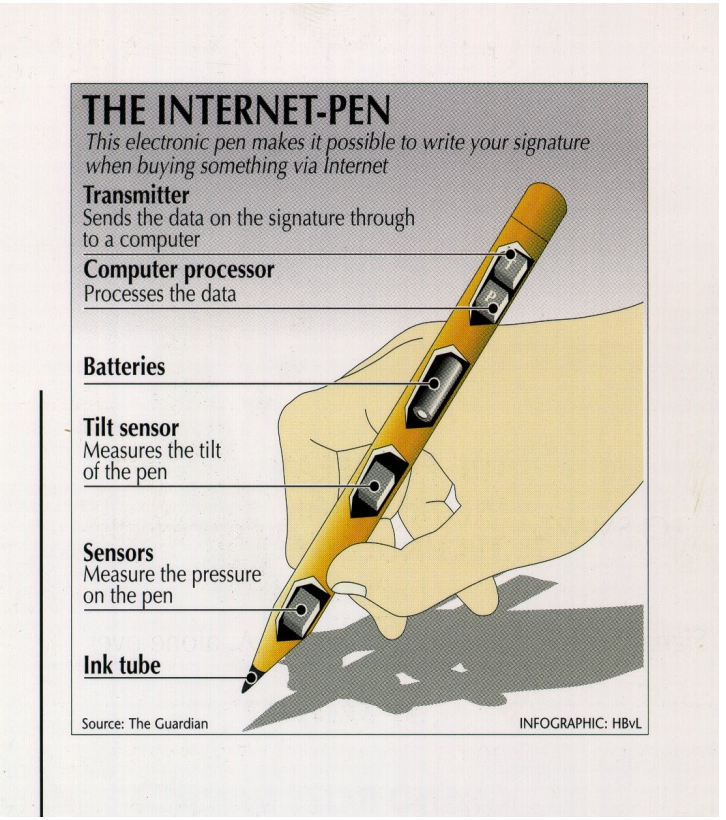
Optical fingerprint sensor
[Fingerprint Identification Unit FIU-001/500 by Sony]

[TravelMate 740 by Compaq und Acer]

Esempi di sensori

- la penna elettronica

Electronic pen [LCI-SmartPen]



Problematiche

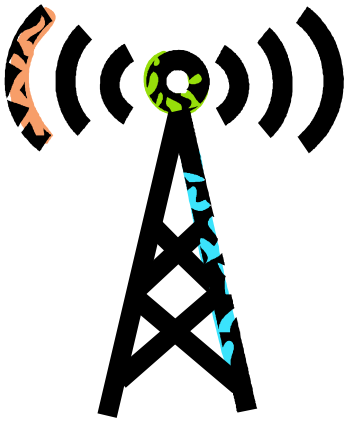
- Il confronto è l'elemento chiave:
  - Un utente onesto potrebbe non essere riconosciuto
  - Un impostore potrebbe essere autenticato
  - Si devono ridurre e "bilanciare" questi due errori
- I sensori e la caratteristica biometrica devono essere sufficientemente stabili
- I dati biometrici devono essere protetti!
  - Sono adatti per identificazione locale
  - Stesse problematiche di password ma
    - Non li possiamo cambiare se vengono rubati
    - Non sono segreti

Protezione dei dati biometrici

Japanese handset
[F505i by NTT DoCoMo]

Impronta digitale di Alice

Dati biometrici



Provider: il verificatore

Protezione dei dati biometrici

Japanese handset
[F505i by NTT DoCoMo]

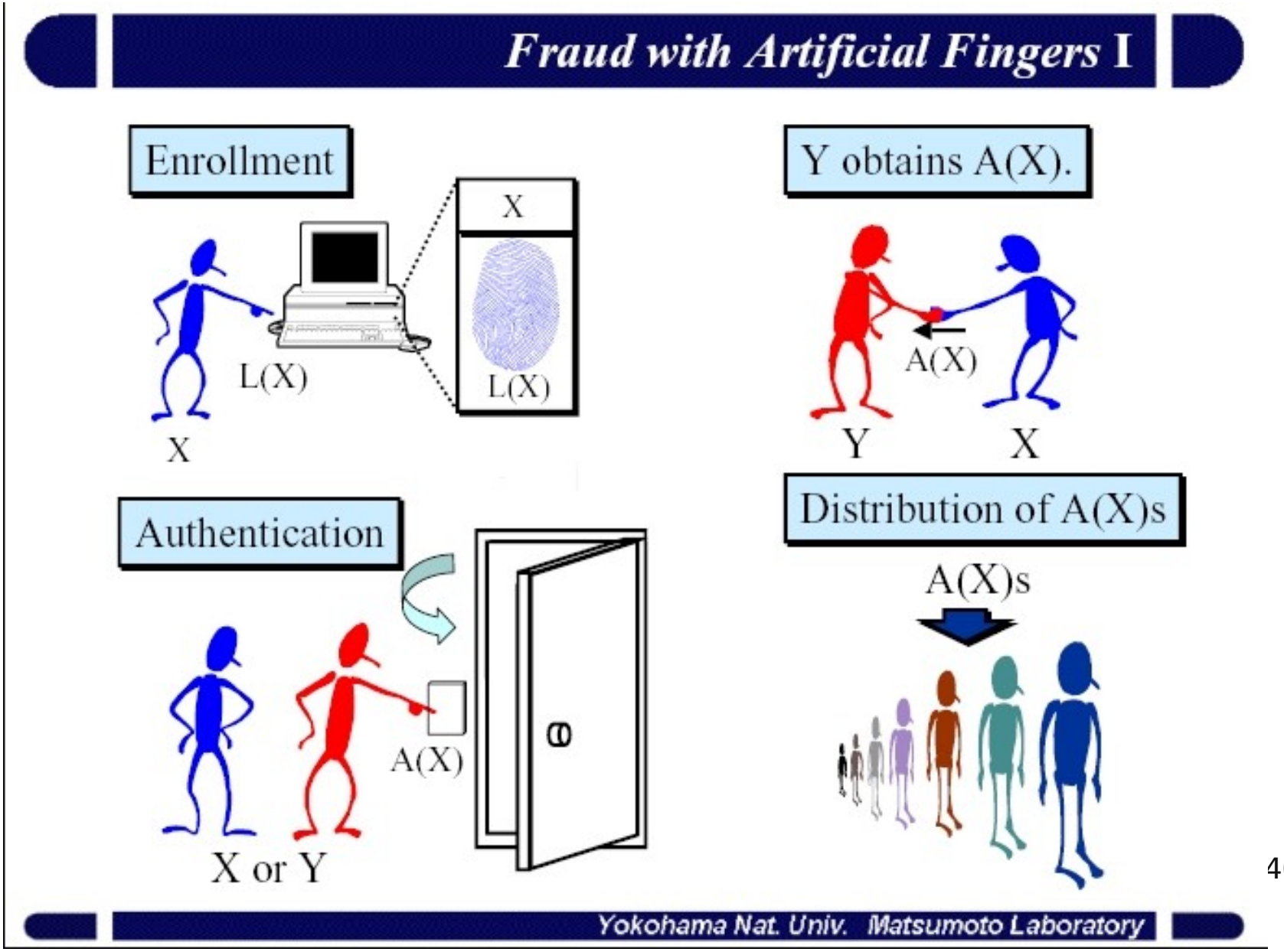
Impronta digitale di Alice

N

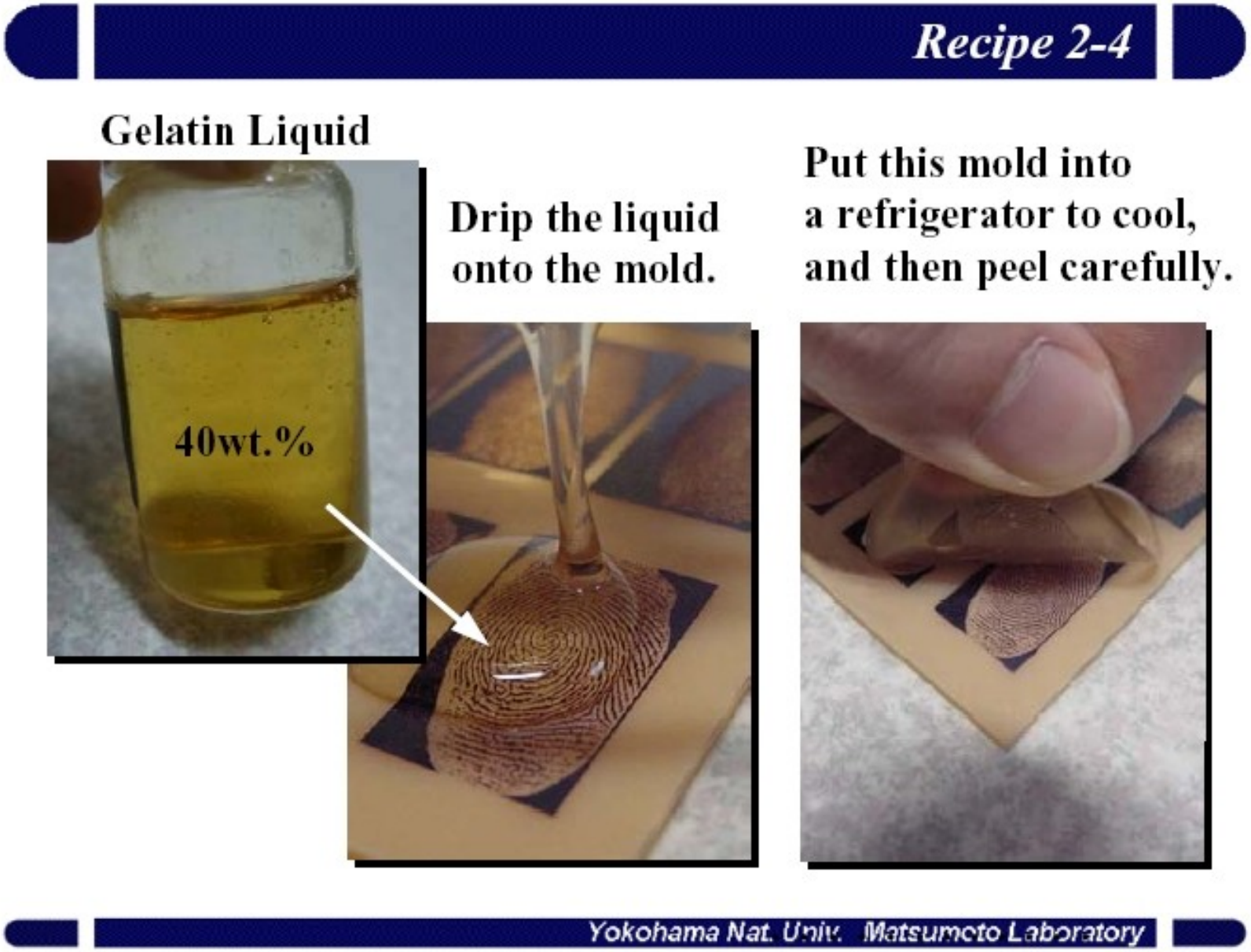
K_{AB} N

Provider: il verificatore

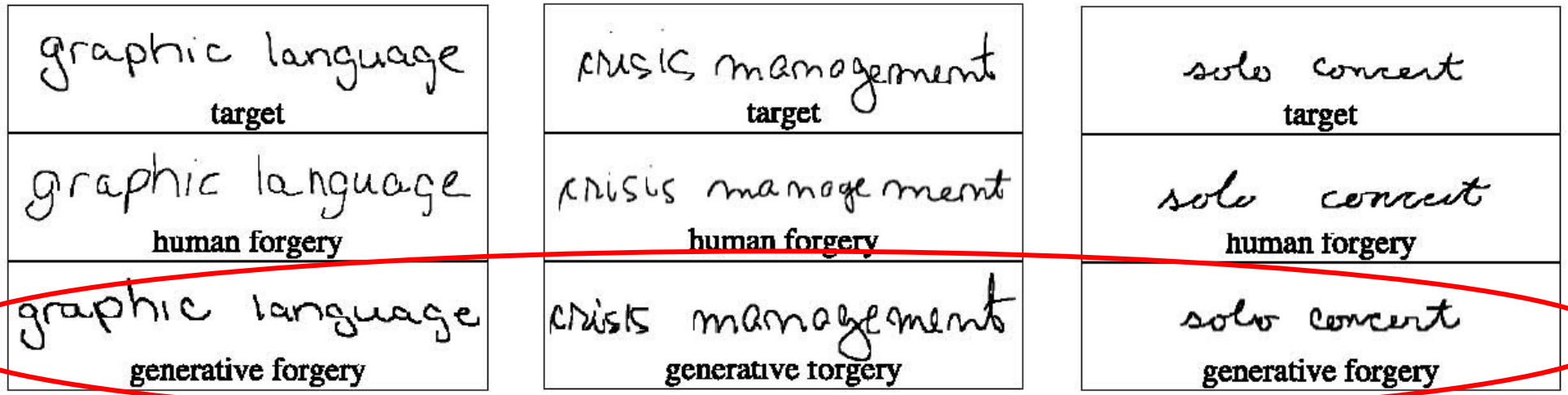
Esperimento alla Yokohama Univ.



Impronta di gomma, da impronta vera



Autenticazione dalla firma



Generato da un algoritmo al calcolatore
addestrato a riprodurre esempi di parole scritte a mano

Autenticazione dalla firma

- "Fraud rate" vs. "insult rate"
  - Fraud = il sistema accetta una falsificazione (falsa accettazione)
  - Insult = il sistema rifiuta un utente valido (falso rifiuto)
- Aumentando la soglia di accettazione si aumenta la fraud rate, e si diminuisce la insult rate
  - si sceglie il valore che pone fraud rate = insult rate
- Per i parametri biometrici le banche in U.K. mettono un fraud rate dell'1%, e un insult rate del 0.01%

Autenticazione basata sulle password

- **Problemi**:

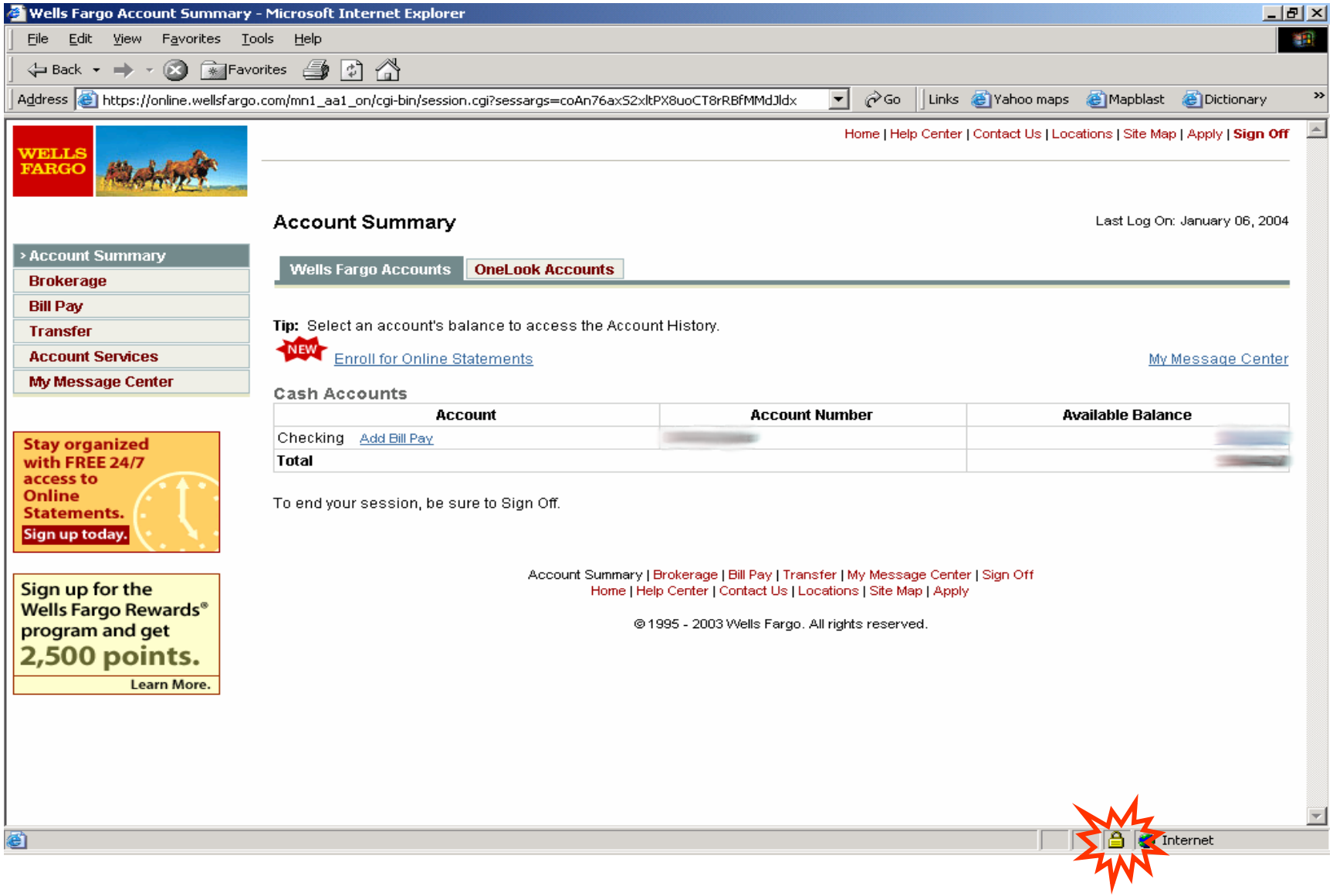
  -La password puo' essere vista mentre transita in chiaro dall'utente al sistema
- L'hash della chiave non risolve il problema
- Al posto della password ci potrebbe essere un numero di carta di credito
- Un nemico potrebbe far finta di impersonare il sito su cui mandare la password o il numero della carta di credito

Soluzione: SSL e TLS

- Il protocollo Transport Layer Security (TLS), versione 1.0
  - E' lo standard per la sicurezza in Internet
  - E' usato per proteggere la comunicazione tra un browser e un Web server. Fornisce autenticazione e segretezza (tramite la cifratura)
- E' basato sul protocollo Secure Sockets Layers (SSL), versione 3.0
  - E' lo stesso protocol design, differisce negli algoritmi
- Utilizzato in quasi tutti i Web browser
- Bisogna controllare che il link abbia https e non http

SSL e TLS

Protegge solo da attacchi a livello di applicazione



Limiti

- Dal certificato l'utente non ha informazioni riguardo l'affidabilita' del server (venditore) e l'autorizzazione a ricevere pagamenti con carta di credito
- Il server (venditore) non sa se l'utente e' affidabile ed e' ad esempio autorizzato a fare pagamenti con le carte di credito (la carta potrebbe essere rubata...)