Università degli Studi "Roma Tre"
Corso di "*Elementi di crittografia*" - A.A. 2004/2005

Crittografia e Sistemi Bancomat

A cura di:

Paolo Bernardi
Michele Bonaccorso
Roberto Zamponi

Sommario

- **Introduzione ai sistemi bancomat**
  - Funzionamento
  - Sicurezza del servizio bancomat
  - Sistemi più sicuri
- **Crittoanalisi del sistema bancomat**
  - Generazione codici PIN
  - Attacco alle Tavole di Decimalizzazione
  - Rimedi
- **Sviluppi futuri**
  - Smart card
  - Crittografia quantistica
  - Bancomat biometrico

Prima parte

I sistemi bancomat

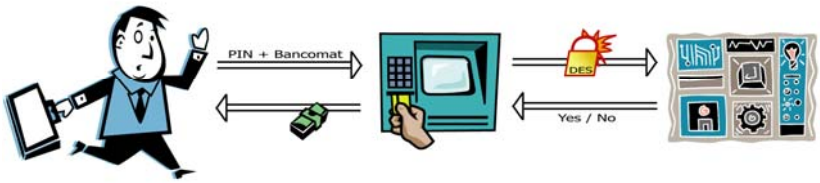
A cura di

Paolo Bernardi

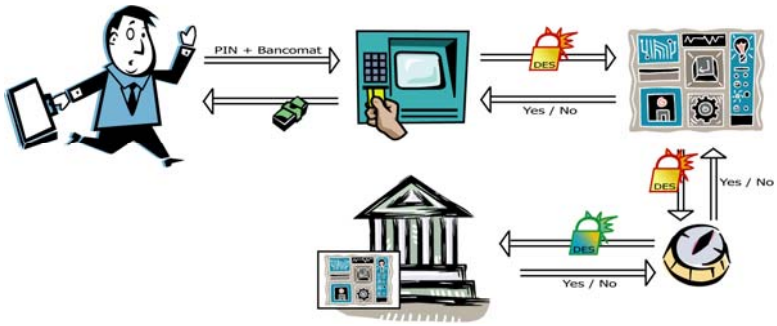
Introduzione

- Il servizio Bancomat locale è realizzato mediante l'integrazione di due apparati hardware:
  - ATM
  - HSM
- Il servizio Bancomat distribuito si appoggia alla rete ETFPOS (Electronic Funds Transfer at the Point of Sale).
  - La richiesta viene inoltrata alla banca di competenza e attraversa uno o più *switch*

Caso d'uso: Prelievo locale



Caso d'uso: Prelievo remoto



ATM

- Il compito degli Auto-Teller-Machines è quello di fornire un'interfaccia con l'utente, pertanto prevedono periferiche di I/O come monitor, tastiera, lettore di schede magnetiche e/o smartcard, un dispositivo per fornire il denaro richiesto e una telecamera.
- Gli ATM generalmente utilizzavano un sistema operativo della IBM e comunicavano con l'HSM mediante un protocollo di rete proprietario IBM chiamato SDLC.
- Ora gli ATM usano Windows Xp e TCP/IP.

HSM

- Gli HSM (Hardware Security Module) o MSS (Modular Security System) offrono un ristretto numero di API (Application Program Interface) per la generazione e validazione di codici PIN secondo gli standard utilizzati dalle diverse compagnie quali VISA, MasterCard, ecc.
- Sono dei critto-calcolatori dedicati
  - Possono utilizzare vari algoritmi crittografici quali il DES, 3DES, RSA e SHA1.
  - Hanno elevate prestazioni crittografiche e validano fino a 60 PIN / sec.

Switch

- La necessità di poter verificare un PIN di un'altra banca viene risolta introducendo le chiavi di zona, Zone Master Keys.
- Ogni banca conosce i propri PIN e possiede una chiave di zona per cifrarli / decifrarli.
- Il compito degli switch è quello di collegare le diverse banche nella rete ETFPOS e quello di tradurre PIN cifrati con chiavi differenti.

Problemi di sicurezza del servizio

- Per come è stato progettato, il servizio bancomat ha vari punti di debolezza:
  - L'ATM
  - La rete ETFPOS
  - L'HSM

ATM - problemi

- La migrazione del S.O. degli ATM da OS/2 a Windows Xp ha esposto gli ATM ai problemi di sicurezza tipici di un PC.
- Nei primi mesi del 2003 molti ATM della Diebold sono stati colpiti dal worm “Welchia” che sfruttava delle vulnerabilità nel servizio RPC (remote procedure call) di Windows Xp.
- Da allora anche negli ATM è stato installato un firewall per contrastare questo tipo di situazioni.
- Conviene utilizzare un S.O. generico come windows xp in ambienti dedicati quali gli ATM?

ETFPOS - problemi

- Vulnerabilità delle comunicazioni interbanca.
- Un utente collegato all’interno della rete potrebbe ricavare i PIN e i relativi numeri di conti correnti con uno sniffer.
- Utilizzo della crittografia:
  - I PIN attualmente vengono cifrati con il DES o il 3DES
- E’ sufficiente?
  - Brute force alla ZMK

HSM - problemi

- Brute force all'HSM
  - 5 cifre = 10^5 possibilità
  - 60 PIN/sec
  - 28 minuti nel caso peggiore
- Tecniche di critto-analisi
  - Attacco alla tabella di decimalizzazione

Evoluzione del sistema

- SmartCard
  - Possono memorizzare dati in modo sicuro
- Biometria
  - Può attestare la presenza fisica di una persona
- Crittografia quantistica
  - Approccio differente
    - Tolleranza (rivelazione) delle intercettazioni
    - Utile nello scambio delle chiavi

Seconda parte

Vulnerabilità
e
Tipi di Attacco

A cura di

Roberto Zamponi

Generazione PIN

- Il codice PIN viene generato cifrando il numero di conto stampato sulla carta bancomat con il DES mediante una chiave segreta chiamata **"PIN generation key".**
- Il ciphertext ottenuto è convertito in esadecimale.
- Si prendono le prime 4 cifre del ciphertext esadecimale
  - 4 caratteri che spaziano tra '0' e 'F'
- Vengono convertiti in decimale mediante una "**TABELLA DI DECIMALIZZAZIONE**" per poter essere digitati su una tastiera numerica.

Tabella di Decimalizzazione

- Usata per convertire il numero di carta cifrato con DES da esadecimale in decimale

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5

Generazione PIN - Esempio

- Numero Conto: **4556 2385 7753 2239**
- Num Conto DES: **3F7C 2201 00CA 8AB3**
- Prime quattro cifre: **3F7C**

Generazione PIN – Esempio(2)

- **Tabella di decimalizzazione:**

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5

- PIN in esadecimale: **3F7C**
- PIN naturale: **3572**
- Offset Pubblico: **4344**
- PIN Finale: **7816**

Perché?

- Possibilità per gli ATM offline di verificare il PIN di un cliente senza richiedere la memorizzazione di un DB di PIN di tutti i clienti.
- Il PIN di un cliente viene quindi calcolato a partire dal proprio numero di conto mediante cifratura con DES con una chiave segreta di cui solo la banca è a conoscenza.
- L'offset pubblico viene introdotto per permettere ai clienti di cambiare il loro PIN cambiando solo l'offset che verrà memorizzato nel DB del mainframe assieme al numero di conto

Hardware Security Module - HSM

- Modulo di Sicurezza Hardware
  - Modulo che si interpone tra gli ATM e il mainframe contenente i dati sensibili accessibili dall'esterno previa autenticazione
- Fornisce delle API che per motivi di sicurezza rispondono solo SI o NO alle interrogazioni ricevute.
- Nel caso della validazione di un PIN risponde:
  - SI se il PIN inserito è valido
  - NO se il PIN inserito non è valido

Codice per Verifica PIN

```
Encrypted_PIN_Verify(
    A_RETRES , A_ED ,                          // return codes 0,0=yes 4,19=no
    trial_pin_kek_in , pinver_key ,            // encryption keys for enc inputs
    (UCHAR*)"3624 " "NONE “                    // PIN block format
    " F"                                       // PIN block pad digit
    (UCHAR*)" " ,
    trial_pin ,                                // encrypted_PIN_block
    I_LONG(2) ,
    (UCHAR*)"IBM-PINO" "PADDIGIT" ,            // PIN verification method
    I_LONG(4) ,                                // # of PIN digits = 4
    "0123456789012345"                         // decimalisation table
    “4556238577532239"                         // PAN_data (account number)
    "0000 “                                    // offset data
);
```


Input Sensibili

- **PAN_data**
  - Personal Account Number (il numero del conto del cliente)
- **Tabella di Decimalizzazione**
  - "0123456789012345"
- **Trial_pin**
  - Il PIN inserito che arriva all'HSM crittato con DES o 3DES.

Vulnerabilità

- **Nei Dati Sensibili:**
  - Trial_pin (PIN di prova)
  - PAN_data (Numero di C/C)
  - Tabella di Decimalizzazione
- **Nell'Architettura ETFPOS:**
  - Ethernet
  - Intrusione
  - Sniffer per intercettare dati

Attacco alle Tavole di Decimalizzazione

Il tipo di attacco più conosciuto individuato da Mike Bond e Piotr Zielinski ricercatori della University of Cambridge è chiamato :

Attacco alle Tavole di Decimalizzazione

Attacco alle Tavole di Decimalizzazione (2)

- **Fase 1:**
  - vengono determinate quali cifre sono presenti nel PIN da ricercare
- **Fase 2:**
  - sono testati tutti i PIN composti con le cifre identificate nella fase precedente.

Fase 1 (1)

- Sia D_{orig} la tavola di decimalizzazione iniziale:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5

- Sia $D_i[x]$ la tavola di decimalizzazione binaria in cui compare 1 se solo se D_{orig} ha *i* nella posizione x:

$$D_i[x] = \begin{cases} 1 & \texttt{se } D_{\text{orig}}[x] = i, \\ 0 & \texttt{altrimenti} \end{cases}$$

Fase 1 (2)

- Sia D_{orig} la tavola di decimalizzazione iniziale:

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5

- Ad esempio $D_3[x]$ è della forma: $D_i[x] = \begin{cases} 1 & \texttt{se } D_{\text{orig}}[x] = i, \\ 0 & \texttt{altrimenti} \end{cases}$

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0

Fase 1 (3)

- Per ogni possibile cifra i (da 0 a 9) viene inviata all'HSM
  - Numero di conto corrente (PAN_data) di cui si vuole trovare il PIN vero.
  - Tavola di Decimalizzazione D_i
  - PIN di prova (trial_pin) composto da soli numeri 0000
- Il test FALLISCE se e solo se il PIN vero contiene la cifra *i*.

Fase 1 - ESEMPIO (4)

- Il "nemico" è in possesso solo del Numero Conto:
  - **4556 2385 7753 2239**
- Cifrandolo con il DES tramite chiave segreta (non a conoscenza del "nemico"):
  - **3F7C 2201 00CA 8AB3**
- Prime quattro cifre che il "nemico" vuole trovare:
  - **3F7C**

Fase 1 - ESEMPIO (5)

- Illustriamo un passo della fase 1:
  Il nemico vuole sapere se il numero 2 è una cifra del PIN.
- Verranno passati come input all'HSM:
  - Il numero di conto corrente
  - Tavola di decimalizzazione binaria D_2
  - Pin di prova 0000

Fase 1 - ESEMPIO (6)

- Tabella di decimalizzazione D_2 :

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0

- L'ATM converte le cifre 3F7C con D_2 ottenendo il numero 0 0 0 1
- L'ATM confronta 0000 = 0001 ? NO
- Il Test fallisce → 2 è una cifra del PIN
- Con al massimo 10 tentativi verranno identificate le cifre contenute nel PIN.

Fase 2

- Vengono provate tutte le possibili combinazioni delle cifre individuate nella fase 1.
- Il loro numero dipende dal numero di cifre differenti nel PIN:

CIFRE	POSSIBILITA'
A	AAAA(1)
AB	ABBB(4), AABB(6), AAAB(4)
ABC	AABC(12), ABBC(12), ABCC(12)
ABDC	ABCD(24)

- Servono al più **46** tentativi: 36 nel caso di 3 cifre diverse + 10 per individuare le cifre.

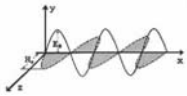
Possibili "Nemici"

- L'unico modo per sfruttare questa vulnerabilità è dall'interno del sistema informativo della banca:
  - Da un impiegato corrotto
  - Da un hacker esterno

Rimedi

- **Per rimediare a questa vulnerabilità si può:**
  - Porre controlli sulla tavola di decimalizzazione D_{orig}
  - Limitare il numero di verifiche su PIN di uno stesso conto corrente
  - Sicurezza sulla rete

...e nel futuro?



A cura di

Michele Bonaccorso

Terza parte: sommario

- Attualmente la ricerca, nonché il mercato, si stanno rivolgendo con sempre crescente interesse ad alcuni aspetti che si ritiene possano conferire solide garanzie agli utenti e ai gestori dei sistemi bancomat

1. Smart card
2. Crittografia quantistica
3. Biometria

Smart card

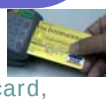
- Lo sviluppo delle carte a microprocessore (o smart card) può essere visto come uno dei fondamentali cambiamenti nell'industria dei pagamenti elettronici a livello mondiale
- **Banda magnetica**: introdotta circa 30 anni fa, non adeguata a far fronte ai bisogni crescenti di sicurezza e all'avanzare del fenomeno delle frodi
  - limite principale: non può conservare i dati relativi al proprietario della carta in modo sicuro

- Le smart card memorizzano le informazioni in modo **sicuro** per poi utilizzarle durante la transazione
  - possono essere utilizzate per accedere a più servizi: smart card "**multi-applicazione**"

Smart card

- EMV
  - standard nato dalla collaborazione dei principali circuiti di pagamento a livello mondiale (Europay, Mastercard, Visa)
  - nel 1993 hanno fondato una piattaforma di lavoro (EMVCo) per lo sviluppo delle specifiche che regolano le applicazioni di pagamento elettronico basate su smart card
- L' EMV stabilisce le regole che permettono alla smart card e al terminale di pagamento di interagire tra loro
  - basate sull' ISO 7816

Smart card



- EMV e sicurezza
  - EMV definisce requisiti minimi di sicurezza per le smart card, ma ogni circuito ha la facoltà di definire ulteriori parametri purché mantengano la compatibilità
  - quattro elementi principali per la sicurezza: autenticazione della carta offline, parametri di gestione del rischio, offline-pin, autenticazione della carta on-line
  - non vengono specificati gli algoritmi crittografici che devono essere usati nell'autenticazione, ma definisce un elemento di 8 bit chiamato **Application Cryptogram** che contiene in modo sicuro i dettagli di ogni transazione
  - autenticazione: CVV (banda magnetica); SDA, DDA, CDA

Crittografia quantistica

- Idea di "*Calcolatore Quantistico*": potenza di calcolo teoricamente infinita
  - cambiamento di strategia nella crittografia attuale
- Crittografia classica: si utilizzano tecniche matematiche per garantire la privacy delle comunicazioni
- Crittografia quantistica: sono le leggi della fisica a proteggere l'informazione
  - basata sulle leggi della meccanica quantistica: studio della fisica a livello microscopico delle particelle elementari della materia
- Principio di indeterminazione di Heisenberg:
  - "non è possibile conoscere simultaneamente la posizione e la velocità di una particella con precisione arbitraria "
    - ovvero: ogni misura effettuata su un sistema quantistico perturba il sistema stesso

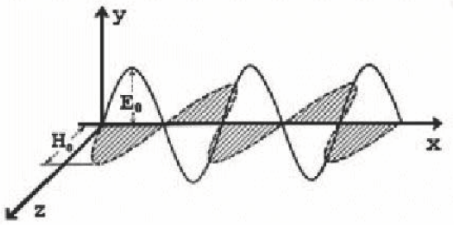
Crittografia quantistica

- Si sfrutta questa proprietà per garantire una comunicazione sicura
  - nessuno è in grado di intercettare un messaggio senza modificarne il contenuto
- Crittografia quantistica: utilizzata convenzionalmente per scambiare la chiave di cifratura di due interlocutori e non il messaggio vero e proprio
  - successivamente con la chiave di cifratura ed un algoritmo di tipo simmetrico è possibile cifrare le comunicazioni

Crittografia quantistica

- Lo scambio dell'intero messaggio su un canale quantistico non protegge in sé l'informazione
  - consente solo di stabilire se non ci sono intrusi in ascolto
  - è conveniente generare a caso una chiave di cifratura, inviarla su di un canale di comunicazione quantistico e determinare se è stata o meno intercettata
- Polarizzazione dei fotoni: si utilizza come canale quantistico un cavo in fibra ottica per il passaggio dei fotoni (elementi costitutivi della luce)

Crittografia quantistica

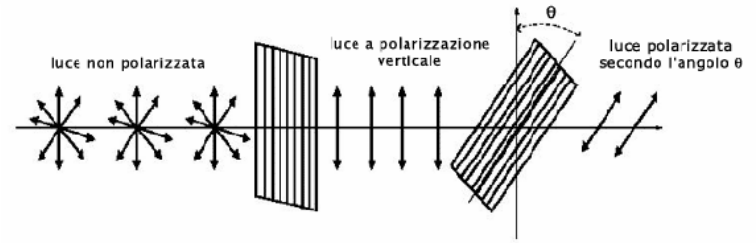


- un fotone a monte del filtro polarizzato con un angolo ϕ oltrepassa un θ-filter con probabilità:

$$p_\theta(\phi) = \cos^2(\phi - \theta)$$

- la probabilità che lo stesso fotone sia invece "respinto" dal filtro è naturalmente:

$$1 - p_\theta(\phi) = \sin^2(\phi - \theta)$$



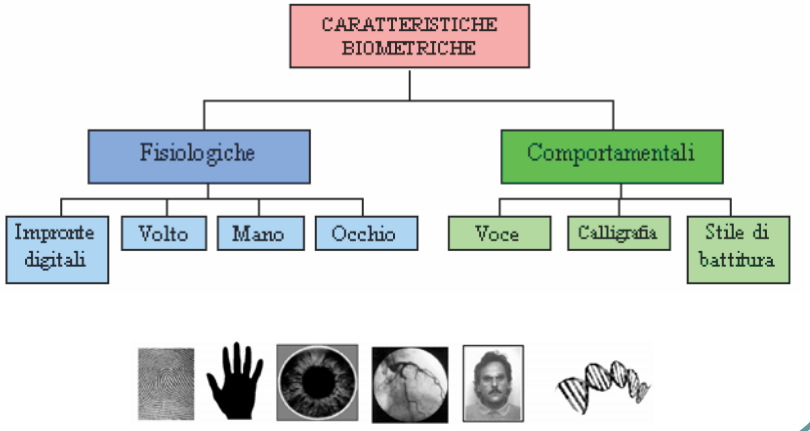
Crittografia quantistica

- Crittografia quantistica: utilizzata per effettuare una transazione elettronica di denaro (tra il municipio di Vienna ed una banca austriaca) utilizzando fotoni “entangled”
  - un fotone di ogni coppia correlata è stato poi inviato dalla banca al municipio attraverso una fibra ottica
  - giunti a destinazione è stato osservato il loro stato di polarizzazione: in questo modo entrambe le estremità del collegamento avevano a disposizione lo stesso dato
- I fotoni "entangled" (correlati quantisticamente) obbediscono agli strani principi della meccanica quantistica
  - disturbando lo stato di uno, si disturba automaticamente anche l'altro, non importa a che distanza si trovino
- Settembre 2004: finanziato dal “*Ministero dell'Università e della Ricerca Scientifica*” un progetto del dipartimento di Fisica dell‘Ateneo di Camerino teso a realizzare un **Bancomat supersicuro** con la crittografia quantistica

Biometria

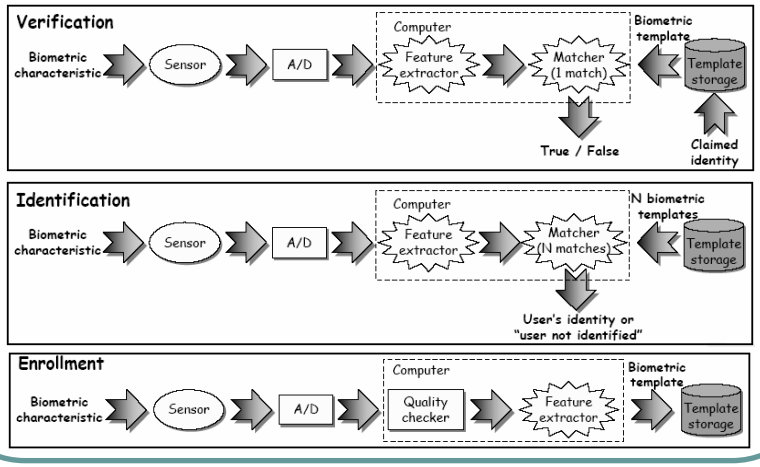
- **Sistemi biometrici**: dispositivi automatici per la verifica di identità o identificazione di una persona sulla base di caratteristiche biologiche (di varia natura)
  - fisiologiche
  - comportamentali
- Texas, 1999: primo esperimento biometrico in ambito bancario
  - una banca ha utilizzato come tecnologia di riconoscimento la **scansione dell'iride**
- Tokyo, autunno 2004: introdotto da Bank of Tokyo-Mitsubishi
  - sportelli ATM polifunzionali dotati di tecnologie di identificazione e autenticazione biometriche
  - la piattaforma utilizzata consente di riconoscere i clienti dal **percorso del sistema venoso** delle loro mani
  - il percorso delle vene di ogni individuo è unico e praticamente impossibile da duplicare o clonare

Biometria



Biometria

Architettura di un sistema biometrico

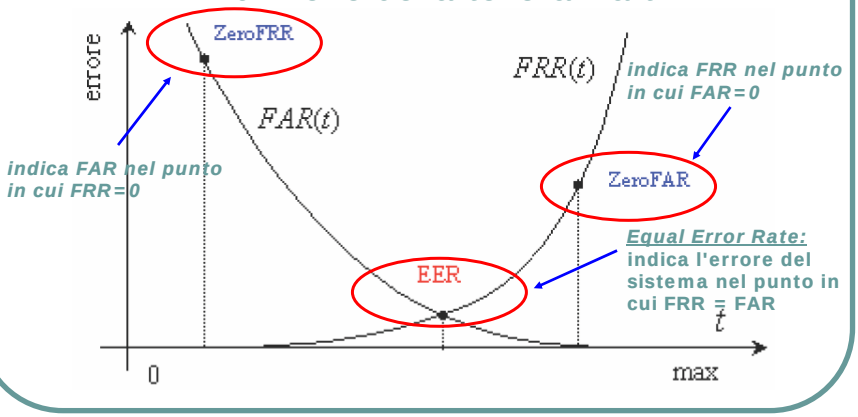


Biometria

- L'affidabilità del risultato di un confronto di istanze diverse delle stessa caratteristica biometrica non è del 100%
- Vari aspetti causano differenze tra acquisizioni successive della stessa caratteristica:
  - variazioni sopravvenute nella caratteristica biometrica
  - errato posizionamento rispetto al sensore
  - salienti modificazioni dell'ambiente di acquisizione
- Due istanze di una caratteristica biometrica non è detto che coincidano: al più si può affermare che due istanze sono sufficientemente simili
- Due tipi di errore che un sistema biometrico può commettere; la probabilità di tali errori è espressa da due parametri:
  - *FRR:* False Rejection Rate (frequenza di falsi rifiuti)
  - *FAR:* False Acceptance Rate (frequenza di false accettazioni)
- *Soglia di sicurezza t*: parametro che stabilisce quanto stringenti debbano essere i requisiti di somiglianza delle caratteristiche biometriche

Biometria

Errori nei sistemi biometrici: FAR e FFR in funzione della tolleranza t



Biometria

- Classificazione dei sistemi biometrici: cooperativo/non cooperativo, evidente/velato, frequentato/non frequentato,...
- Parametri comuni di confronto:
  - *unicità*: il grado con cui si può trovare la stessa caratteristica tra due soggetti diversi
  - *permanenza*: se la caratteristica varia o meno nel tempo
  - *esecuzione*: il raggiungimento preciso dell'identificazione

	universalità	*unicità*	*permanenza*	*misurabilità*	*esecuzione*	*accettabilità*	*insidia*
Impronta	Medio	Alto	Alto	Medio	Alto	Medio	Alto
Retina	Alto	Alto	Medio	Basso	Alto	Basso	Alto
Volto	Alto	Basso	Medio	Alto	Basso	Alto	Basso
Mano	Basso	Basso	Basso	Alto	Basso	Alto	Basso
Firma	Basso	Basso	Basso	Alto	Basso	Alto	Basso
Voce	Medio	Basso	Basso	Medio	Basso	Alto	Basso

Biometria

- Un sensore, capace di leggere e identificare i dati biometrici, è uno dei modi migliori per aumentare la sicurezza
  - nei nuovi ATM è incorporato un lettore (uno scanner ad infrarossi) che "legge la mano" del cliente senza che questi sia costretto a toccare alcunché
- Ma il sistema biometrico è realmente inattaccabile?
- Molti di questi sistemi sono vulnerabili a diversi tipi di attacchi

Biometria: conclusioni

- Attacchi
  - *replay attack*: l'hacker ruba una copia dell'immagine digitalizzata della caratteristica biometrica e se ne serve per "proiettarla" in un'altra occasione
  - uso di un "trojan"
  - attacchi consistenti nella manipolazione del valore di soglia di ciascun sistema, aumentando il valore del FAR e rendendo più facili gli accessi da parte di intrusi
  - ai dispositivi: smontando o sostituendo alcuni componenti del sistema per catturare informazioni
  - ai collegamenti tra dispositivi
- Risposta agli attacchi:
  - crittografia
  - client/server: (attacchi ai collegamenti in rete) protocolli per transazioni sicure (SSL, TSL)

Bibliografia

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

HEOS.it

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

BIOMETRIA.INFO

- *Mike Bond, Piotr Zielinski* - Decimalisation table attacks for PIN cracking
- *Giovanni Manca* - L'uso della biometria per l'accesso alle smart card
- *Paolo de Andreis* - La Biometria è inevitabile
- *Leopoldo Fabiani* - Bancomat, basta un'occhiata
- *Heos.it* - Bancomat supersicuro con la crittografia quantistica
- *Biometria.Info* - ATM biometrici
- *Paolo Canali* - Le tecnologie biometriche
- *Enrico Zimuel* - Uno sguardo alla crittografia moderna
- *Dario Maio* – Introduzione ai sistemi biometrici