DI-FCT-UNL
Segurança de Redes e Sistemas de Computadores
Network and Computer Systems Security

Mestrado Integrado em Engenharia Informática
MSc Course: Informatics Engineering
2º Semestre, 2018/2019

User-Level Authentication

Multi-Level Authentication Examples

User Authentication	**User Authentication Factors and User Authentication Methods**
Application and Service Level Authentication	Kerberos, Email Authentication (ex., PGP, S/MIME), X509 Authentication, DKIM, Secure POP(3/4), Secure IMAP HTTPS Authentication, SSH-based Applications, RADIUS
Session-Layer Authentication	TLS, DTLS Authentication, SSH Authentication WTLS Authentication
Transport Layer Authentication	
Network LevelAuthentication (IPSec AH, ESP-AC)	IPSec Authenticated Protocols (IPSec AH, ESP-AC)
Data-Link, Network Access Authentication Control	802.11i (802.11i RSN – Robust Secure Network) Authentication, WEP, WPA, 802.1x,
HW or Device Level Authentication	

Outline

- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issued in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

Outline

- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issued in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

User Authentication Elements, Means or Factors

- **"Something we know" factors**
  - Shared Secrets, password, PINs, or answers to prearranged set of questions.
- **"Something we have" factors**
  - Possessed objects, matrix-codes' cards, one-time-pads, key-cards, smartcards, tokens, physical-keys, mobile-phones, …
- **"Something we are" factors**
  - Biometric factors
    - Physical static biometric factors: Examples include recognition by fingerprint, retina, and face.
    - Behavioural (or dynamic) biometric factors: voice pattern, handwriting characteristics, and typing rhythm.

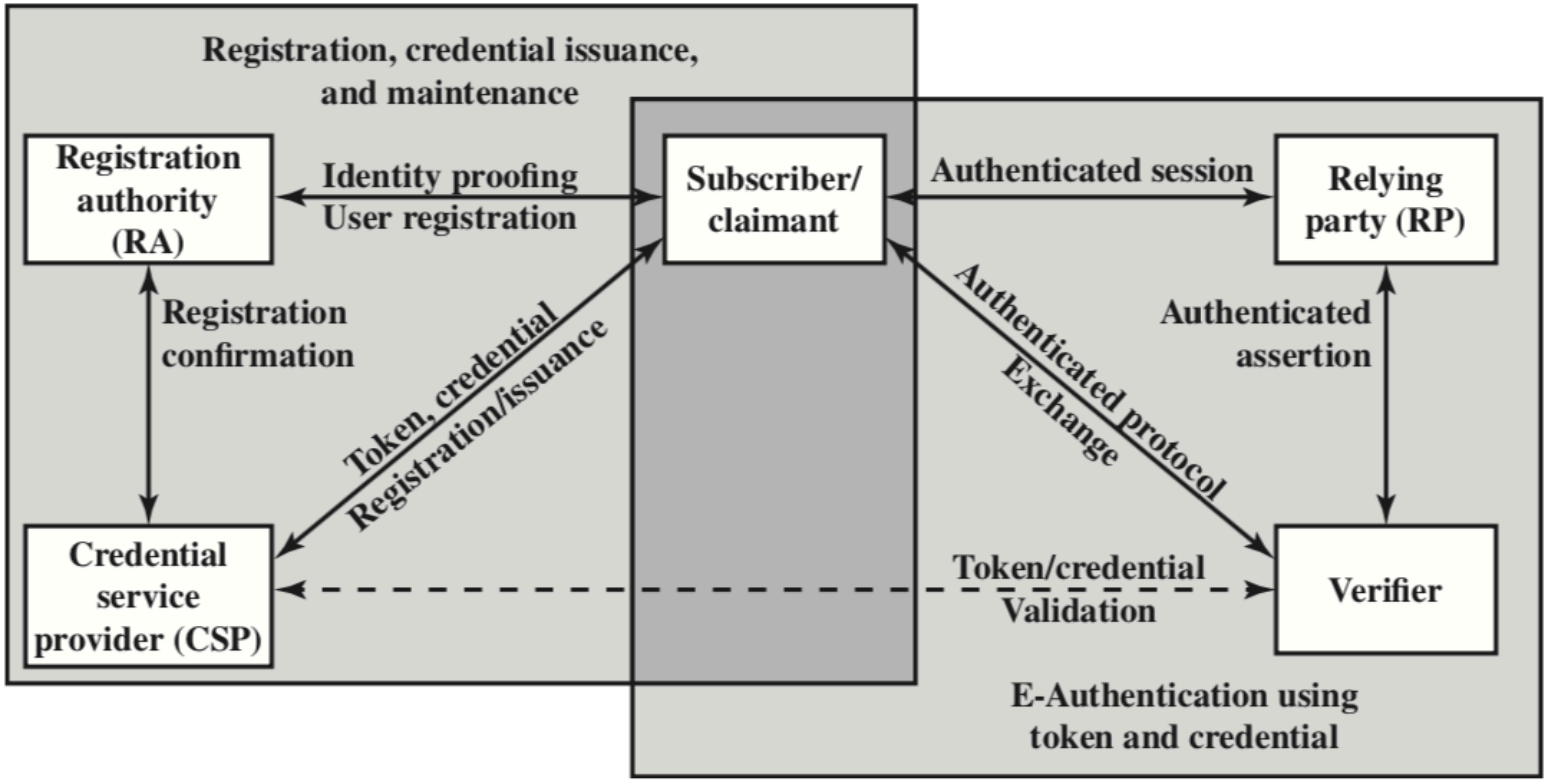
- Can combine different factors
  (same type or different types)
  - **Known as Multifactor Authentication (or MFA)**

Other possible factors

- **Something we recognize**
  - Cognitive factors
    - Implicit vs. Explicit factors
      - Media, Images, Sounds, …
- **Somewhere we are**
  - Location-based factors

NIST SP 800-63-2
E-Authentication Architectural Model

Authentication Framework Model
Initially defined in Aug/2013



Risk Assessment vs. User Authentication

- Closely-related categorizations:
  - **Establishment of Assurance Levels**
    - Ex., Four levels of Assurance defined in the NIST SP 800-63-2, Authentication Framework, Aug 2013
  - **Definition of Potential Impact**
    - Ex., FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*, 2004

Can map on regulatory issues:

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or organization liability	Low	Mod	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized release of sensitive information	None	Low	Mod	High
Personal safety	None	None	Low	Mod/ High
Civil or criminal violations	None	Low	Mod	High

Outline

- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issues in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

Password-Based Authentication

- Advantages: Simple, "Cheap"
- Drawbacks: vulnerabilities
  - Weak PWDs, Off-Line Dictionary Attacks
  - Cleartext transmission or weak-protection on transmission
    - Ex., HTTP Base Authentication, using RADIX / Base64 (or Armour) Transformations
  - Non-Immunity against Replaying Attacks

Top Ten 2014 de Splashdata

1. 123456
2. password
3. 12345
4. 12345678
5. Qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football

Password-Based Authentication

Drawbacks: vulnerabilities

- **Offline dictionary attacks**
  - Requires prevention against unauthorized access to password databases (or files), IDS on compromises and fast pwd reissuance
  - Protection of passwords in databases with strong cryptographic transformations
- **Specific account attacks by pwd guessing**
  - Requires account locking countermeasure mechanisms (after a certain number of attempts)
- **Popular passwords, guessing against user IDs**
  - Countermeasures include policies to inhibit the selection by users of common (weak) passwords + scanning the IP addresses of authentication requests + client cookies for submission patterns

Password-Based Authentication

Drawbacks: vulnerabilities

- **Password guessing against single user**
  - Exploit: Knowledge about the account holder and system password policies
  - Countermeasures include training in and enforcement of password policies that make passwords difficult to guess.

- **Workstation hijacking**
  - Exploit: wait until a logged-in workstation is unattended.
  - Countermeasure is automatically logging the workstation out after a period of inactivity. Intrusion detection schemes can be used to detect changes in user behavior.

- **Exploiting user mistakes:**
  - Includes all social-engineering exploits
  - Countermeasures: user training, intrusion detection, passwords combined with MFA mechanisms

Password-Based Authentication

Drawbacks: vulnerabilities

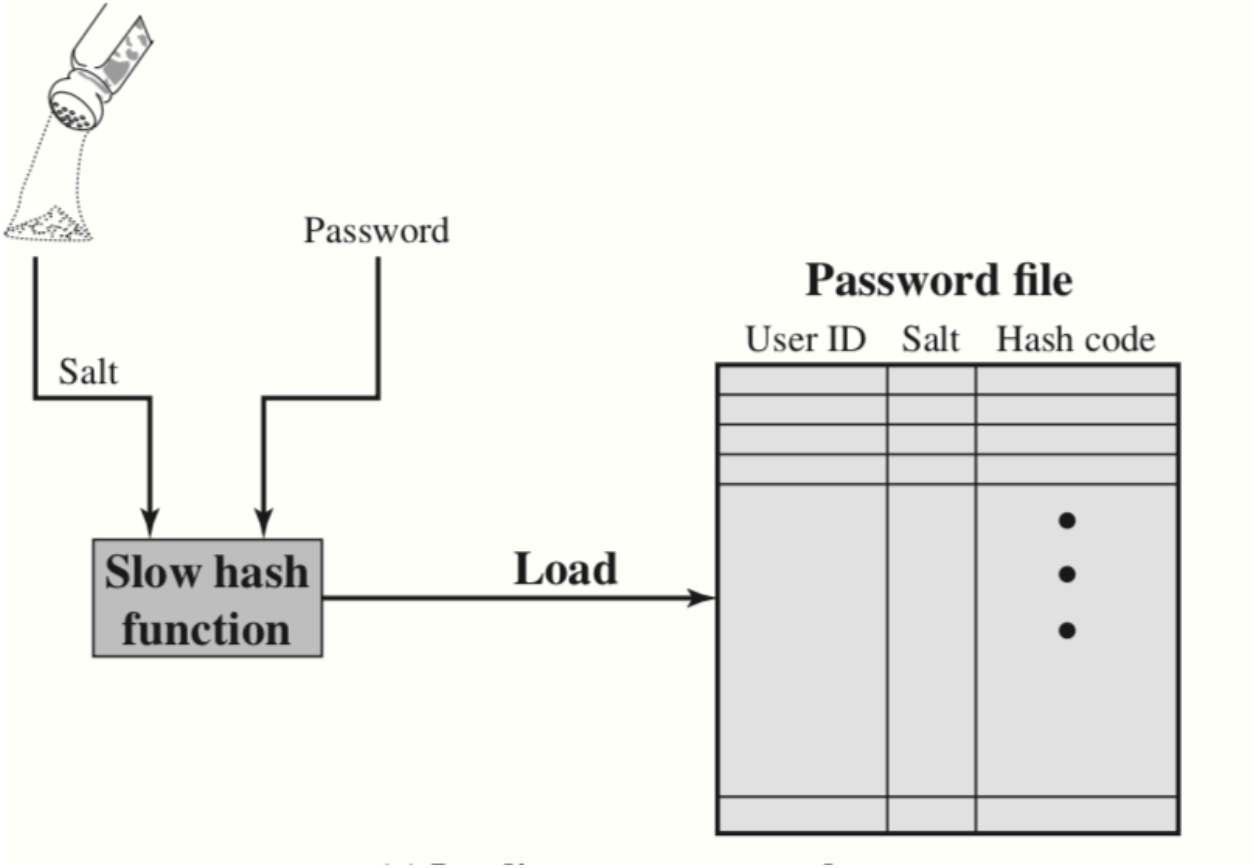
- **Exploits of multiple password use**
  - Exploit: Knowledge about the reuse of passwords in different systems, services, …(ex., big problem w/ social networks)
  - Countermeasures: a policy that forbids the same or similar password on particular network devices, services or systems out of control

- **E-Monitoring**
  - Exploit: passwords communicated across networks to log on to remote systems, vulnerable to eavesdropping
  - Countermeasure: use of secure channels with strong encryption arguments

- **Exploiting implementation/design mistakes or weaknesses:**
  - Hardwired / Not changeable / Not Patchable PWDs and verifications
  - Countermeasures: don't use such systems (big problem in current IoT devices)

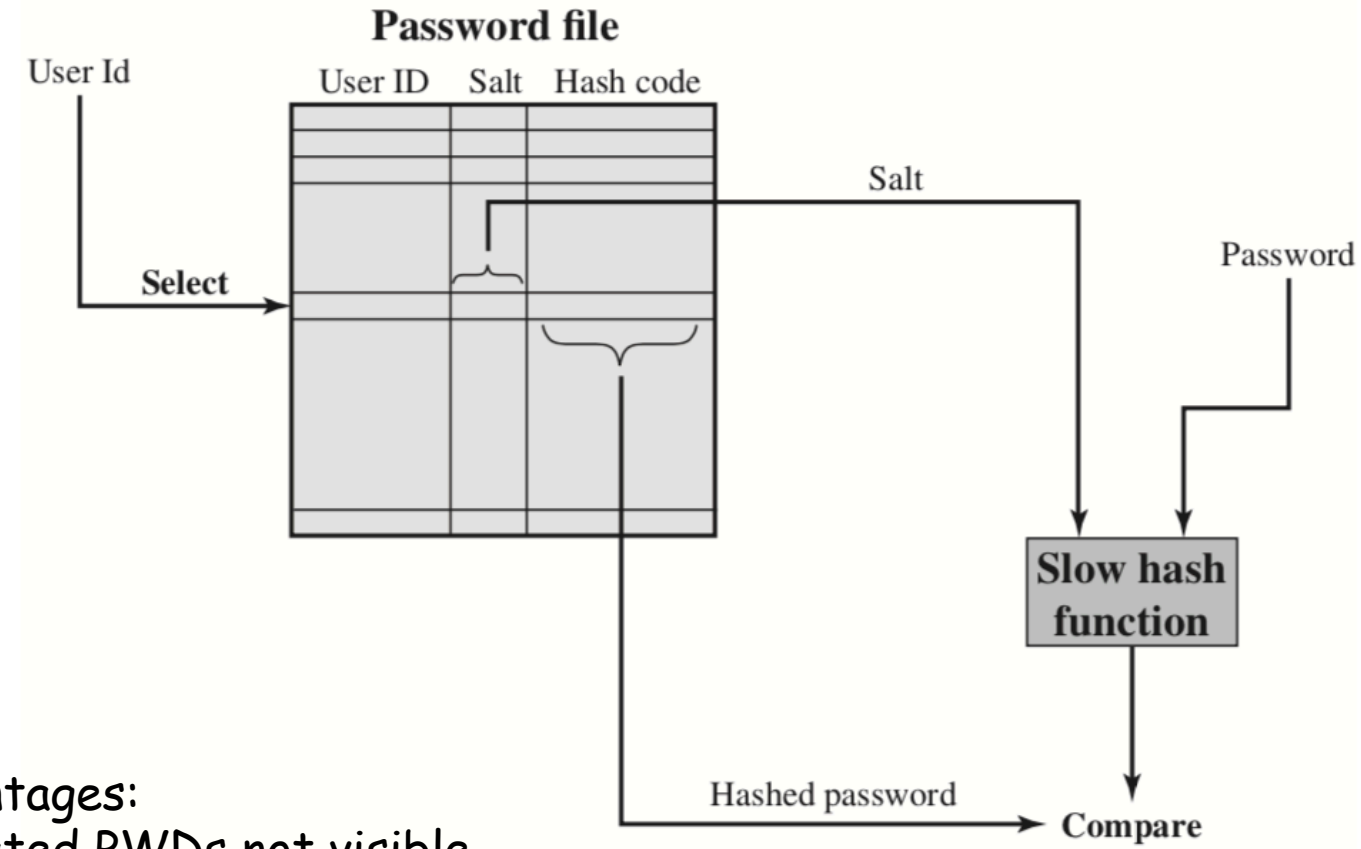
Use of hashed-passwords

Salt: Time-based information or currently a result of PRFs



Use of hashed-passwords

Salt: Time-based information or currently a result of PRFs



Salt advantages:

- Duplicated PWDs not visible
- Increases difficult for offline dictionary attacks
  - Salt with b bits => increase of 2^b the effort of guessing
- Minimizes exploits of multiple password use

Schemes for secure pwd storage

- **Crypt Scheme**: A PWD-based encryption scheme based in a a DES Variant used as an hash-based – not reversible computation (25 x modified DES loop)
  - Pwds w/ 8 characters + 12 bit salt
  - Today is not considered necessarily secure
- **MD5 pwd hashes** (in a 1000 x loop)
  - No limit for input PWDs, Salts 2/ 48 bits
- **Bcrypt**: use of a Blowfish based PBE method + salt of 128 bits
  - Can use longer PWDs – Different
    - Initially Bcrypt versions with different implementations ranging form using secure hash functions, as well as symmetric encryption methods
      - See: https://en.wikipedia.org/wiki/Bcrypt
  - Other schemes: **Argon2, scrypt, PBKDF2**
- See also more recent researched schemes in the TP2 FAQ
  - http://asc.di.fct.unl.pt/~hj/srsc1819/wa2/protected-password-storage.html

PWD Guessing Techniques

- **Large dictionary** of possible passwords and to try each of these against the password file.
  - Each password must be hashed using each available salt value and then compared with stored hash values.
  - If no match is found …
    - the cracking program tries variations on all the words in its dictionary of likely passwords.
    - Typical variations include backwards spelling of words, additional numbers or special characters, or sequence of characters.

PWD Guessing Techniques: Rainbow Tables

- Alternative to large dictionaries: trade-off space for time by pre-computing potential hash values.
- In this approach the attacker generates a large dictionary of possible passwords …
  - For each password, the attacker generates the hash values associated with each possible salt value.
  - The result is a mammoth table of hash values known as a **rainbow table**.
  - Study: 1.4 GB of data, could crack 99.9% of all alphanumeric Windows password hashes in 13.8 seconds. (see bibliography)
  - Conclusion: we need big salts !

PWD Guessing w/ Easily guessed PWDs (1)

- Circumvention against big salts
- PURDUE University study (see bibliography):
- 54 machines, representing approximately 7000 user accounts.
- Almost 3% of the passwords were three characters or fewer in length.
  - An attacker could begin the attack by exhaustively testing all possible passwords of length 3 or fewer.
  - Solution: Policy enforcement for generation of passwords with a minimum number of characters

PWD Guessing w/ Easily guessed PWDs (2)

- Circumvention against big salts + longer passwords
- Another study (see bibliography) on UNIX password files, containing nearly 14,000 encrypted passwords.
- Attack:
  - Try the user's name, initials, account name, and other relevant personal information. In all, 130 different permutations for each user were tried.
  - Try words from various dictionaries: 60,000 words, including the online dictionary on the system itself, and various other lists.
  - Try various permutations on the words from step 2. This included making the first letter uppercase or a control character, making the entire word uppercase, reversing the word, changing the letter "o" to the digit "zero," and so on. These permutations added another 1 million words to the list.
  - Try various capitalization permutations on the words from step2 that were not considered in step 3. This added almost 2 million additional words to the list

PWD Guessing w/ Easily guessed PWDs (2)

(CONT)

Results:

- The test involved nearly 3 million words
- Time to encrypt all these words for all possible salt values: ~1 hour
- Keep in mind that such a thorough search could produce a success rate of about 25%, whereas even a single hit may be enough to gain a wide range of privileges on a system.

PWD Guessing Tools

- Attacks that use a dual combination of brute-force and dictionary techniques have become common and integrated in many PWD cracking tools.
  - The "John the Ripper" Tool: an open-source password cracker first developed in 1996 and still in use until now, started by using such dual technique

- Other modern approaches and tools from more recent research
  - Use of "Fast HW", Parallelization with GPUs: today ~10^{10} PWD combination tests/s
  - More sophisticated alghoritms: probabilities of letters from natural language research, Markov modeling techniques, similarity analysis of very large PWD databases as training datasets
  - See Bibliography

Countermeasures

- Password File Access Control / use of Shadow PWD tables
- PWD Selection strategy
  - User education
  - Computer-generated passwords
  - Reactive password checking
  - Complex password policy
- Policies with Rule enforcements
- Passwords Checkers for Strong PWDs
  - Use of "Bad" PWD Dictionaries: problem is that we need very large dictionaries
  - Time constraints when using very large dictionaries
  - Solution: use of Bloom Filters

What is a Bloom Filter ?

- A Bloom filter of order k consists of a set of k independent hash functions
  - $H_1(x), H_2(x), \ldots, H_k(x)$

  - where each function maps a password into a hash value in the range 0 to $N - 1$.

That is, $H_i(X_j) = y$

$1 <= i <= k; \quad 1 <= j <= D; \quad 0 <= y <= N - 1$

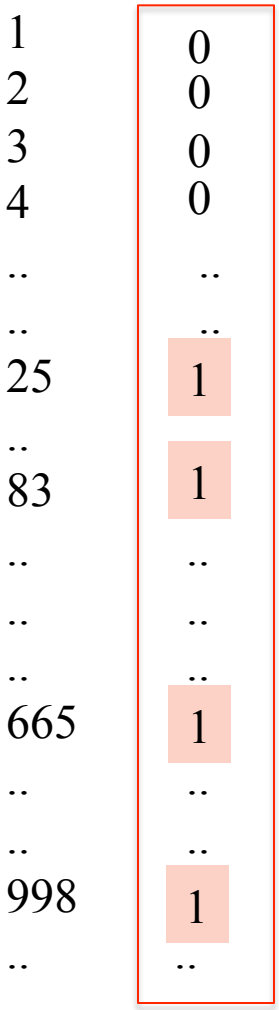
Xj : is the jth word in password dictionary
D = number of words in password dictionary

Checking w/ a Bloom Filter

- Example with two hash functions H_1, H_2 and two "bad" passwords in the dictionary: "undertaker", "hulkhogan"
- H_1(undertaker) = 25
- H_2(undertaker) = 998
- H_1 (hulkhogan) = 83
- H_2 (hulkhogan) = 665

For a given pwd "xG%#jj98":

- H_1 (xG%#jj98) = 665
- H_2 (xG%#jj98) = 998
- => THEN REJECT !



Checking w/ a Bloom Filter

- Problem: there is a probability of a password rejection with a false positive decision
  - Many false positives (acceptance rate) => a big number of PWD rejections (rejection rate) even for possible strong PWDs !
  - Difficult to select not rejected PWDs !

Expect number of bits in the hash-table = 0

$$\phi = \left(1 - \frac{k}{N}\right)^D$$

Probability P that an input word, not in the dictionary, will be falsely accepted as being in the dictionary:

$$P = (1 - \phi)^k$$

How to reduce false positives ?

How to reduce false positives ?

From the previous slide:

$$\phi = \left(1 - \frac{k}{N}\right)^D \qquad P = (1-\phi)^k$$

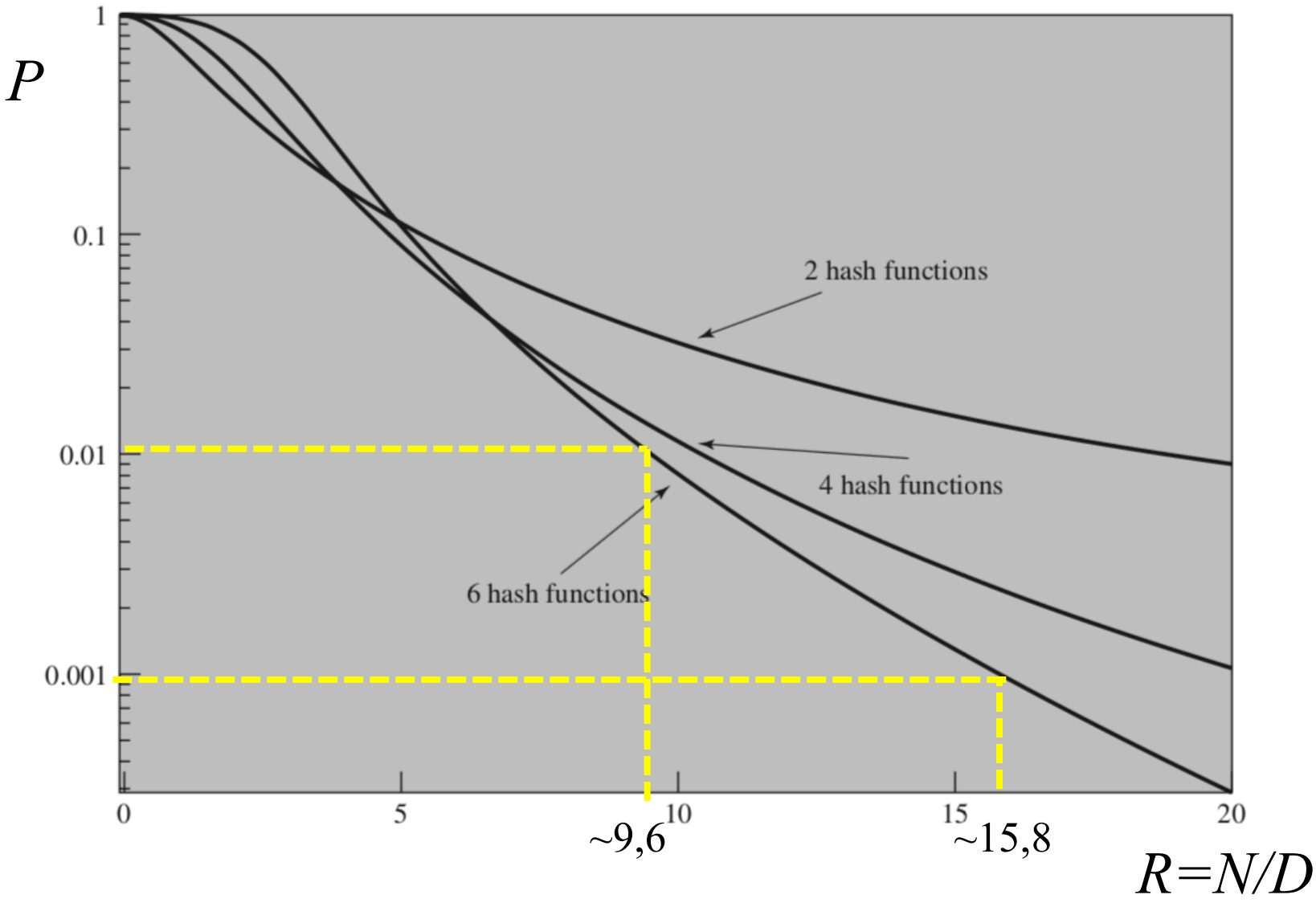
$$P \approx \left(1 - e^{-kD/N}\right)^k = \left(1 - e^{-k/R}\right)^k$$

$$R \approx \frac{-k}{\ln(1-p^{1/k})}$$

k = number of hash functions
N = number of bits in hash table
D = number of words in dictionary
R = N/D, ratio of hash table size (bits) to dictionary size (words)

Ex: P ~0,01, k=6 => R = (-6 / ln (1- (0,01)$^{1/6}$ ~ 9,6

Analysis: reduction of rejection rate

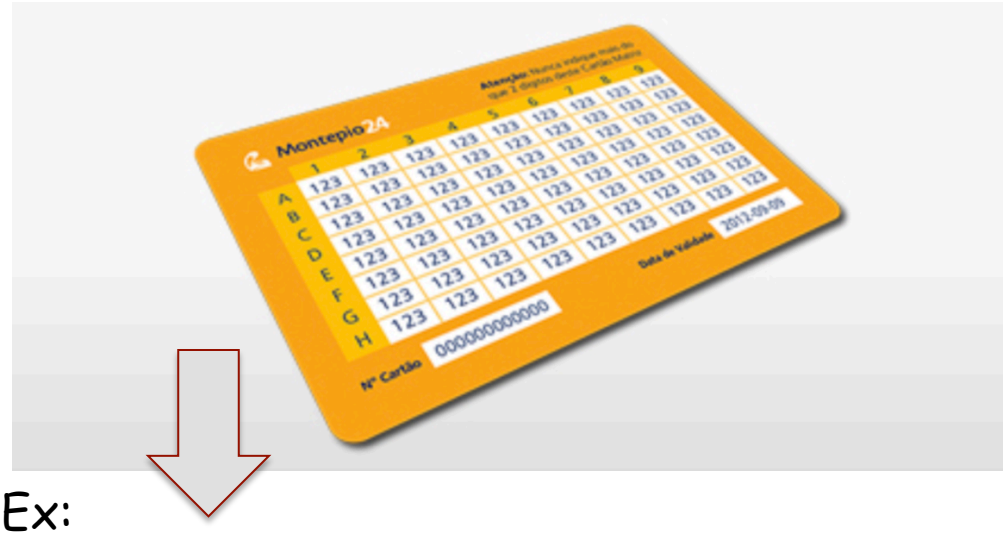


Outline

- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issues in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

One Time Passwords (w/ "cheap" physical tokens)

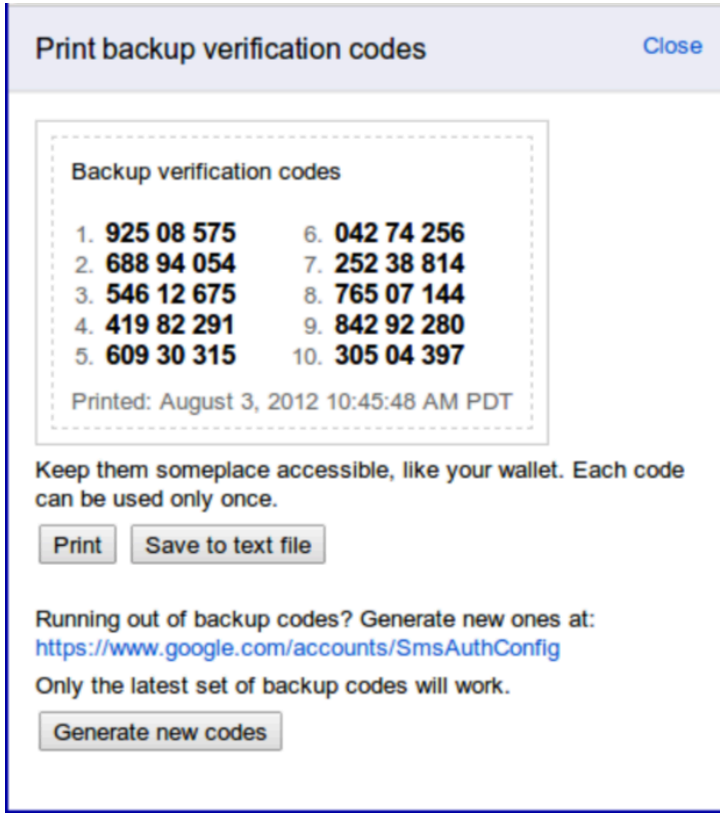
Another problem: how to distribute/obtain securely the these tokens for each correct user?



Ex:

3 coordinates + position: challenges
(Line vs. Column vs. Pos)

- Possible answer 000 to 999
- For random challenge: 1/1000
(1/500 for probability = 0,5)
- … But effectively only 8 x 9 x 3 x 3 = 648 different challenges



OTP Devices: Advantages vs. Drawbacks

Advantages

- Possible eavesdropping (MiM)
  - If no interception and illicit use before correct use !
- Possible additional PIN locking

Problems

- Management of credentials (for different situations)
- Require some sort of "synchronization"
  - Auth Claimant / Authenticator
- To be more effective, requires "special" devices

Example, RSA Secure IDs

- The user generates the OTP combined with the User ID using the number in the display
  - OTP = User ID, Token Number
    - Computed with TIME, using a Seed, one or more Keys and a possible combination of cryptographic operations (Secure Hash Functions and Symmetric Encryption Algorithms)
  - A server (RSA ACE Server) do exactly the same, verifying the equality

- Relaxed Clock-Synchronization with evolving Time-Correction (clock-deviations) in the authentication verification
  - Use of a "validation window" (possibly parameterization in the server side): tradeoff between security vs. usability
  - RSA Security Time Synchronization
- Robustness against weak PWDs, dictionary attacks and Phishing mitigation

RSA SecureIDs

RSA SecurID SID800

http://www.vasco.com/products/range.html

Product Range

Support & Downloads
Events / Training
Partners
Investors

Privacy Policy Email this Page

2005 FROST & SULLIVAN Vertical Market Penetration Award

Strong Authentication & e-Signature

Digipass Go 1 | Digipass Go 3 | Digipass Go 5
Digipass Go 6 | Digipass 250 | Digipass 260
Digipass 300 | Digipass 300 COMFORT | Digipass 300 Comfort Voice
Digipass 550 | Digipass 560 | Digipass 580
Digipass 585 | Digipass 700

RSA Secure ID

- UserID + Generated Token (computed by the device)

  OTP = User ID, Token Number

- RSA ACE Server do the same symmetric computation
  - Given User ID, can verify the token
- Requires a (Lazy) Clock synchronization
  - RSA Security Time Synchronization
    - Admited derivation DELTA as a parameter
    - Computation with different discrete DELTA generates accepted tokens in a valid interval
    - If token is in the interval, the time-deviation is synchronized for each user
- Once more: resistance against dictionary attacks and keys (token values) not chosen, anticipated or previously known by users

RSA SecurID SID800

Token-Devices for Challenge-Response

- Authenticator generates a challenge (randomly) to the claimer
- The challenge must be transformed by the claimant, using the authentication credentials
- Usually, with the Token, the challenge is introduced in the device (possibly with a previous local PIN to unblock the device)
  - Ex., Challenge Ra
  - R = $HMAC_K$ (Ra, Clock, R') or R = $HMAC_K$ (Ra, Seed, R')
    - With R' the previous R
    - K derived by Seed (Seed registered in the authenticator side)
- The result is computed by the internal algorithm running in the device, and shown in the digital display
- Symmetric computation in the server side for verification

Hybridization w/ multi-factor token devices

Universal reader + Smartcard
+ Biometric blocking

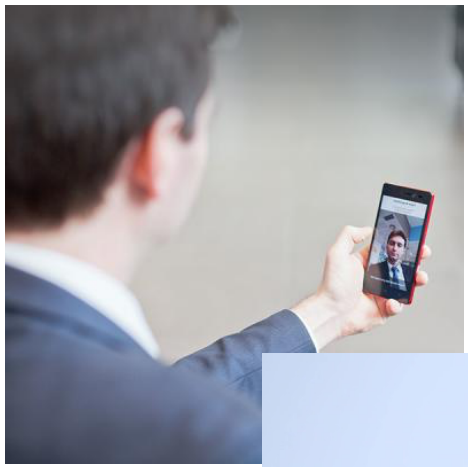
Universal reader + Smartcard
+ Keyboard locking
+ Keyboard Input for Multi-purpose Local Processing

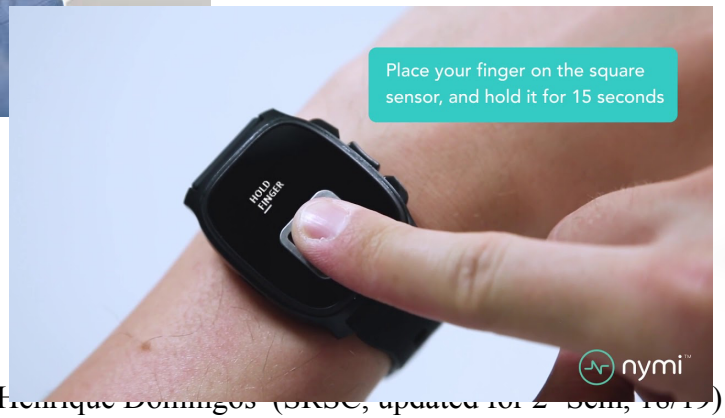
More Examples / Demos (Technology)

- http://www.vasco.com/products/applicationguide.html
- http://www.rsa.com/node.aspx?id=1159
- www.vasco.com
- https://www.rsa.com/en-us/resources?q=Authentication
- https://m.vip.symantec.com

MobilePhones and Wearables based tokens

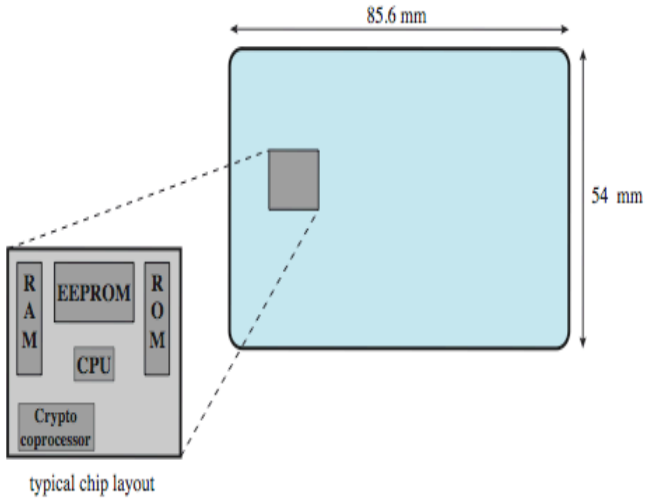
- Can use Mobile (Smart) Phones to implement a variety of tokens as Authentication Apps
- Emulation of previous physical devices ,,, or something more (using sensing data)
- An open possibility for behavioral biometry ?
  - Advantages, Drawbacks ? Discussion !





Smartcards and Smart Dongles

- Credit Card Type
  - Processor, Memory and I/O ports
  - Wired (Contact) ou wireless (Contactless)
  - Can use a cryptographic Co-Processor
  - Memory: ROM, EEPROM, RAM
- Execution of authentication protocols protocols Computer-Reader
- Authentication protocols
  - Static
  - Dynamic password generator
  - Challenge-response:
- Other formats (ex.,"*USB dongles*")



typical chip layout

Types of Cards

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card

Requires special readers: increases the cost and creates the requirement to maintain the security of the reader's hardware and software.

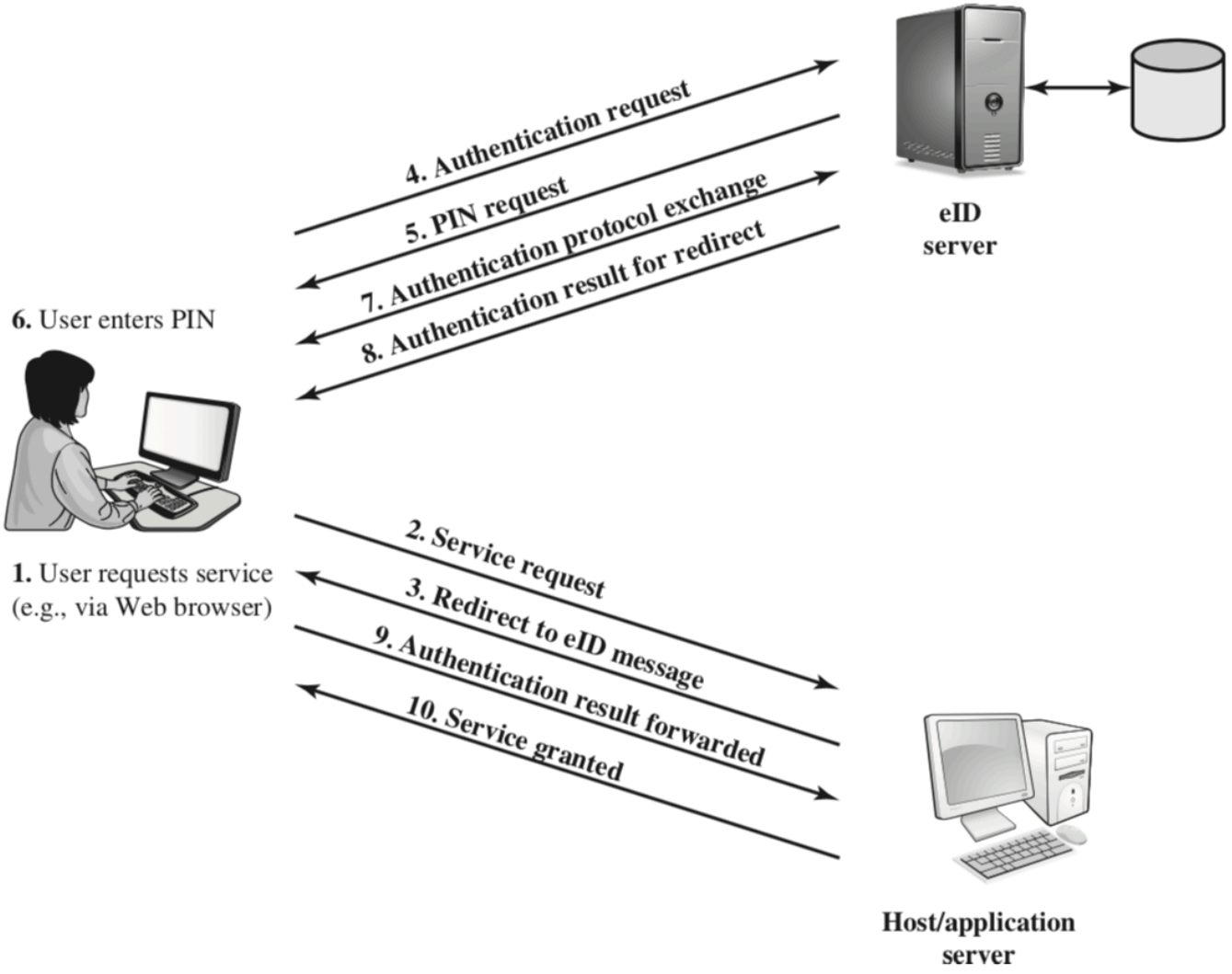
Token loss: A lost token prevents its owner from gaining system access. Administrative costs in replacing the lost token. In addition, if the token is found, stolen, or forged, then an adversary must determine the PIN to gain unauthorized access.

User dissatisfaction: memory card for ATM access, but use for computer access is many times nconvenient.

eID Cards

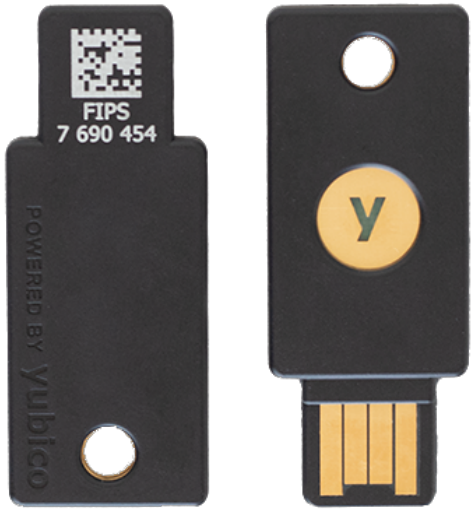
- Personal data or attributes:
- Document number:
- Card access number
- Machine readable zone (MRZ)
- eID Functions
  - ePass
  - eID

Authentication Services using eID Cards



Smart-Dongles: YubiKey example

- Personal Authentication, USB or NFC
- One-Time Key for each use, protection against dictionary-attacks (keys not chosen/not knoen previously by the users)
- USB Keyboard emulation
- Can be also used to store confidential data:
  - <Login, Pwd> Pairs for URLs
  - Blocked (vault-protection): unblocking requires user authentication
- Can also store a keypair (RSA, 2048 bits)
  - Implements the OpenPGP card protocol
  - Contactless access (via NFC)
  - Can be used for digital signatures (without exposing the private key)



YubyKey (Types)

See other types in:

https://www.yubico.com/products/yubikey-hardware-3/

Outline

- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issues in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

Biometric Authentication

- Authentication credential based on physical metrics (biometry) of body characteristic
  - Advantages of biometric credentials: no-memorization, no weaknesses due to bad user choices, not transferable (no delegation)

- Biometric credentials as individual authentication templates, to be compared against templates' references obtained and registered in a similar way, but in the context of an independent trustable enrolment process

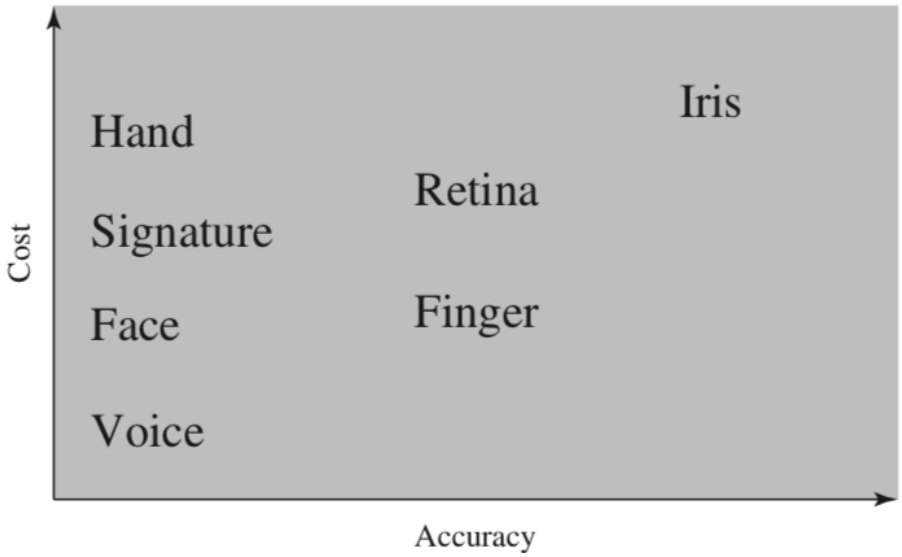
Biometric Drawbacks

- Can be expansive… More cheap => lower security
- Credentials cannot be changed (ex., if stolen)
- No delegation can imply on inflexibility for certain situations (or certain exceptional conditions)
- Involved risks for persons
  - Attacks against persons to remove parts of their bodies
- Not used for mutual remote authentication
  - Credentials obtained by local devices
  - Remote infrastructures (managing the biometric templates) are trusted
- Privacy issues
  - Ex., Biometry can reveal personal medical/health conditions

Biometric Authentication

Physical Characteristics

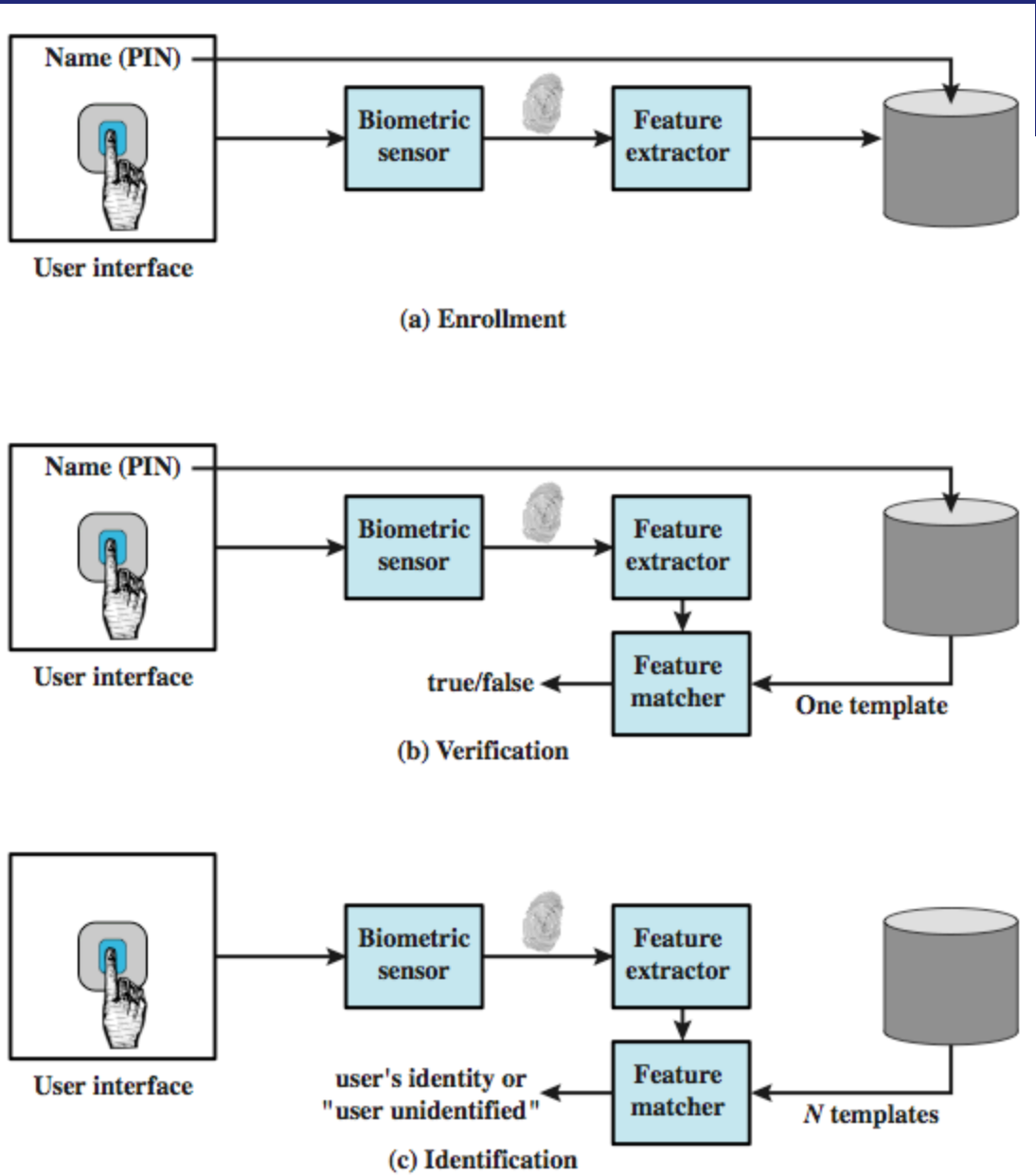
- Facial geometry characteristics
- Fingerprints
- Hand Geometry
- Retinal pattern (scan)
- Iris structure
- Handwriting Signatures
- Voice Patterns



User Authentication with Biometric Factors requires three main steps:

- Enrollment: provision and registration of biometric information (bio template) + identification
- Verification: verification of validity of the registered info
- Authentication of identification: unidirectional, possible false positives (FAR) and false negatives (FRR)

Operation Steps using a Biometric System



Biometry: Properties and Tradeoffs

- **Universality**
  - Applied to any individual person
- **Uniqueness**
  - Differentiation between any two individuals
- **Durability (or stability)**
  - Sustainability during all the individual life
- **Correction (or robustness) under FRA and FRR metrics**
  - Acquisition and distinction correctness (based on non-reproductible properties of subjects)
- **Commodity (or convenience)**
  - Minimal impact in the context of use
- **Acceptability**
  - Levek of rejection: fear of privacy-loss, ethics/social rejection, fear of health danger, …

Management of Biometric Tradeoffs

- Precision / Biometry Type and selection according to the usage scenarios (admissible FAR, FRR) according to "characteristic curves"
- The no reversibility problem (can not change the biomeric attributes)
- Possible regulatory and/or ethical limitations
- Environmental limitations in certain use contexts
- Requires physical presence (only for local/proximity authentication)
- Expensive, less commodity and less acceptability … particularly for the biometry with the high-precision rates
- …

- Use as a complementary factor in a multi-factor authentication strategy

Conventional and emergent biometric factors: some comparative issues

Veins recognition: reliability , fraud is difficult , high cost.

Fingerprints: fast, good reliability, low cost

Facial recognition: reliability, fast , low cost.

Iris scan: very reliable, immutability, high cost.

Retina recognition: reliable, immutability, difficult readings, no commodity, rejection, intrusive (requires to fix to a light point in veru stable conditions), high cost.

Voice recognition: reliability, environmental problems, mutability (stress, flu-status, hoarseness, delay/latency of recognition) low cost.

Hands geometry: reliability, physical-intrusions: rings, problems in use, medium cost.

More about biometric factors

Handwriting/Gestures: reliability, mutability, can be practical / gamification, agility, high acceptability – specific use contexts /, medium cost, environmental and mobility perturbations

Typing recognition: poor reliability, latency (enrollment and pattern-captures, low cost.

Emergent and Future Technologies (in on-going research):

- **Emergent/research factors**: Odor, salinity of human body, vein-patterns with thermal-images from the face, fist or hands, DNA-Analysis (very slow and very problematic)
- **Writing style, Cognitive factors / puzzle-games solution strategies**

Mobile behavioural biometry

- Laptops, mobile devices, IoT devices (new)
- Rressure, flight, movement/sequences …
- Research factors from smartphones or tablets:
  - Hit zone, pressure, orientation (how the user holds the phone), etc.
  - Future potential: multi-fator authentication w/ multi-device / multi-sensing data, indirect biometric information

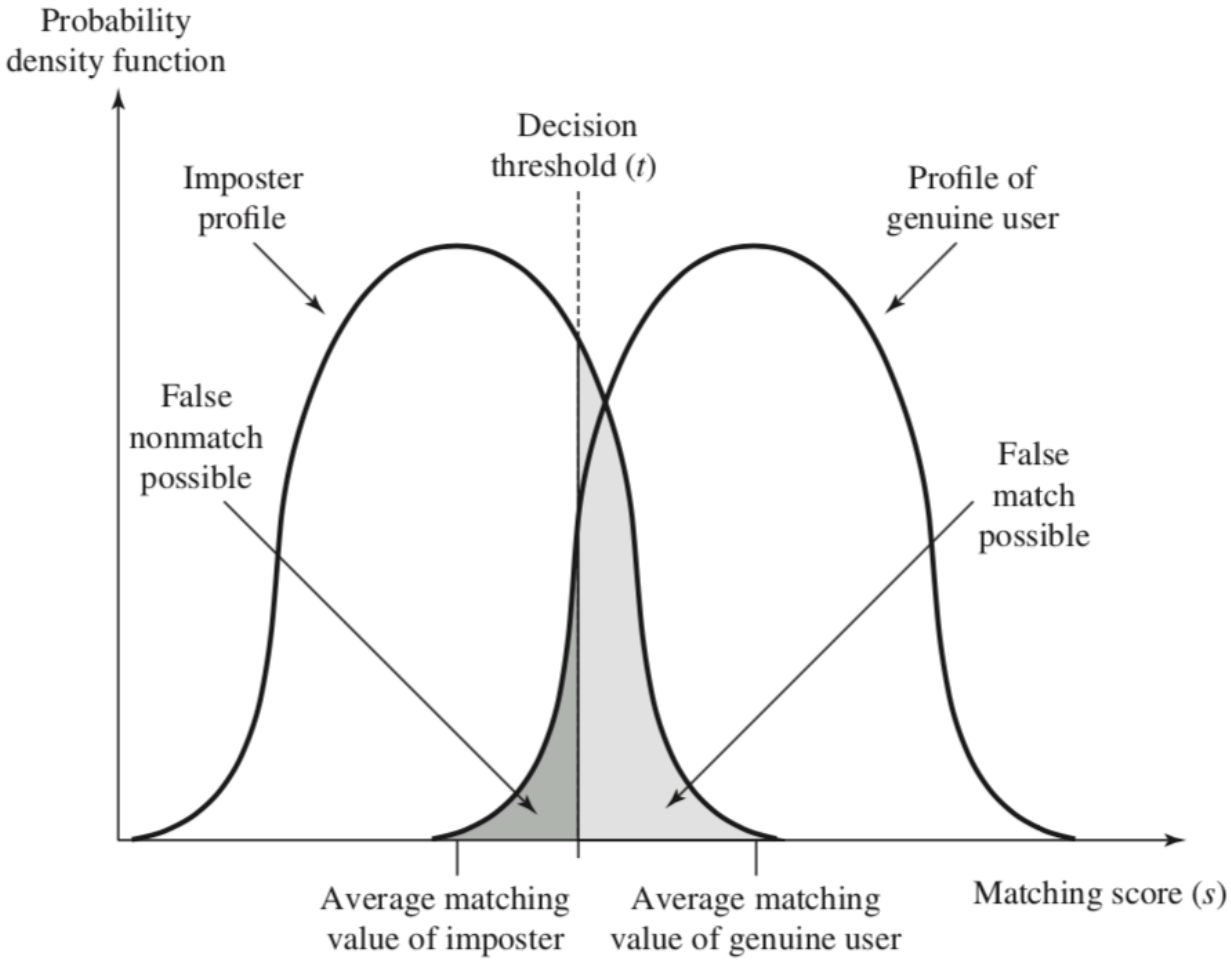
Technical Characteristics for Biometric Systems

- Technical correction characteristic of biometric factors:
  - False Positives Rate (FAR – False Acceptance Rate)
  - False Negative Rate (FRR – False Rejection Rate)

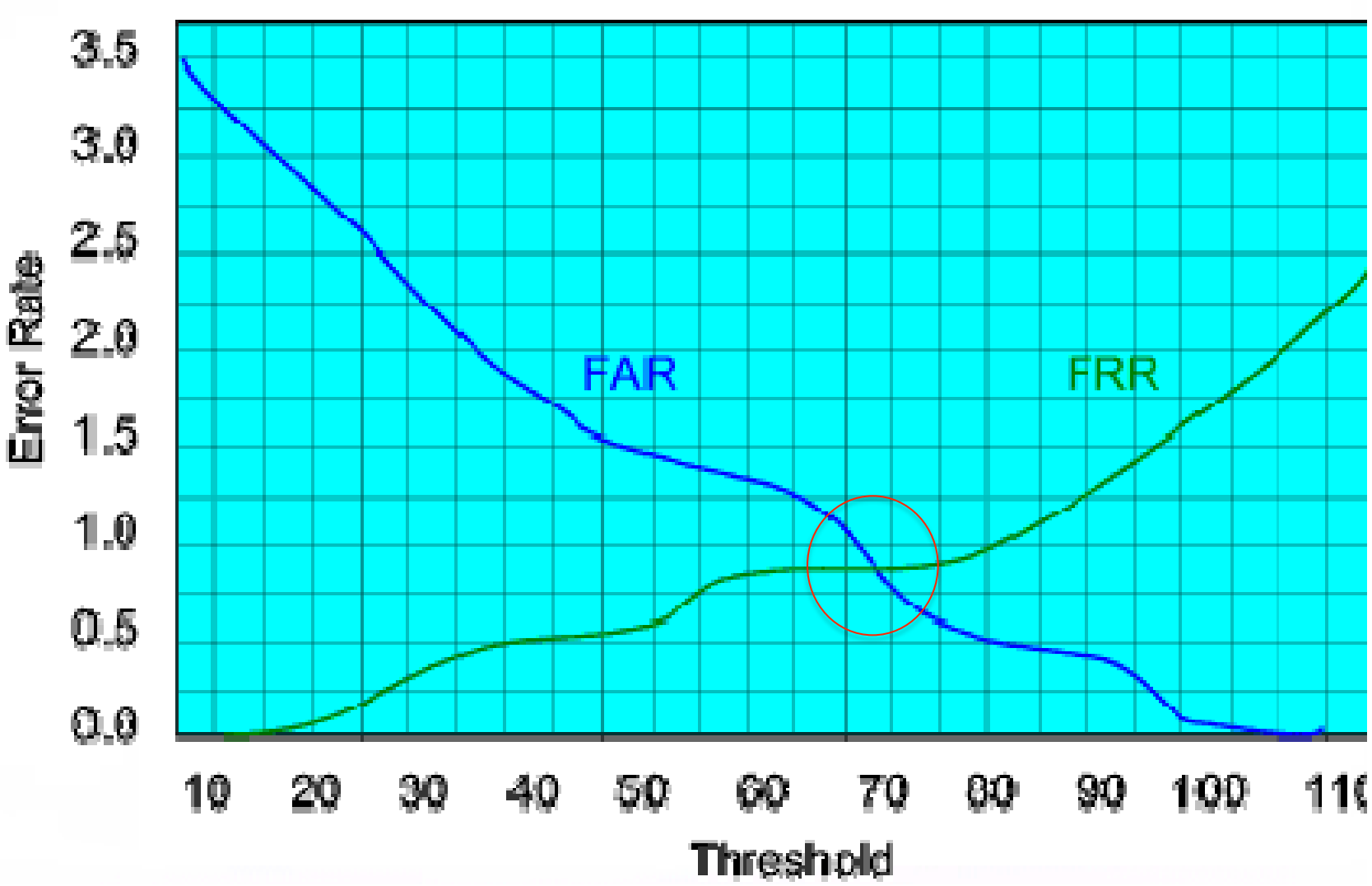
- The lower for FAR e FRR the better is the uniqueness property, for distinguishing any two subjects
  - Very sensitive for identification (open-space serach)
  - Not so sensitive for authentication (closed space search

- Calibration of biometric systems
  - How to choose the right parameters for FRR e FAR for the best connditions in a real application scenario ?

Biometry Accuracy

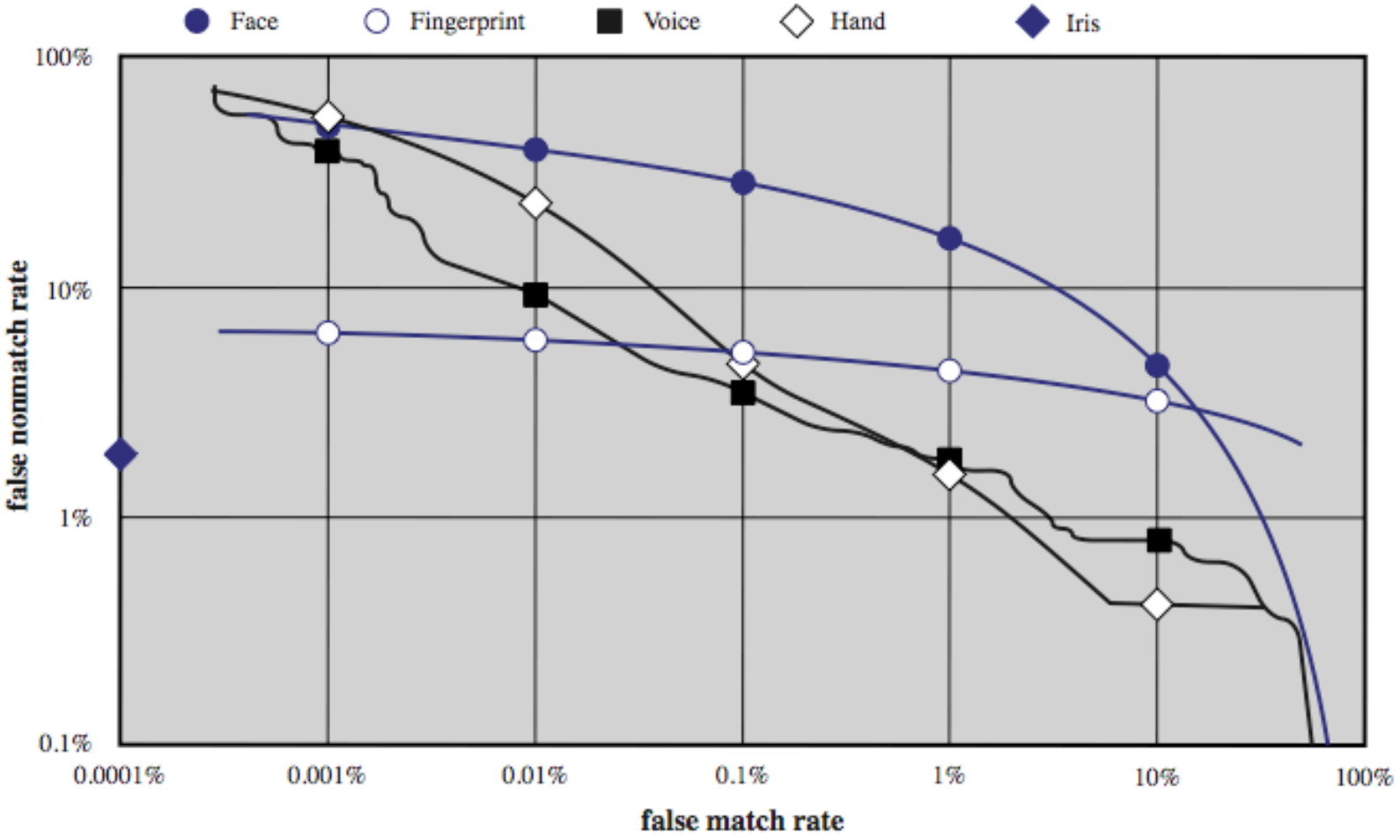


Approach for FAR vs. FRR Tradeoff

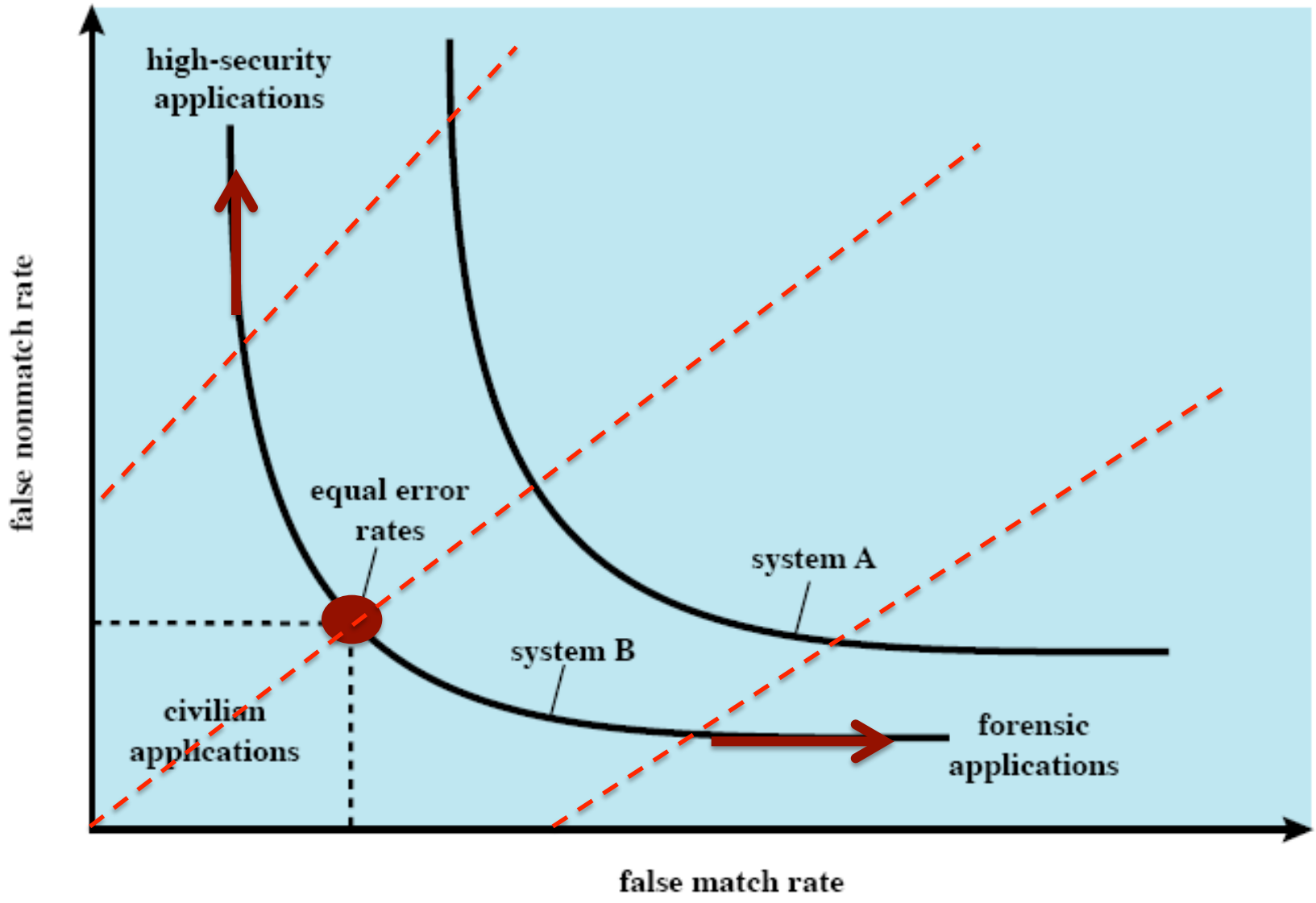


Reliability of Biometric Systems

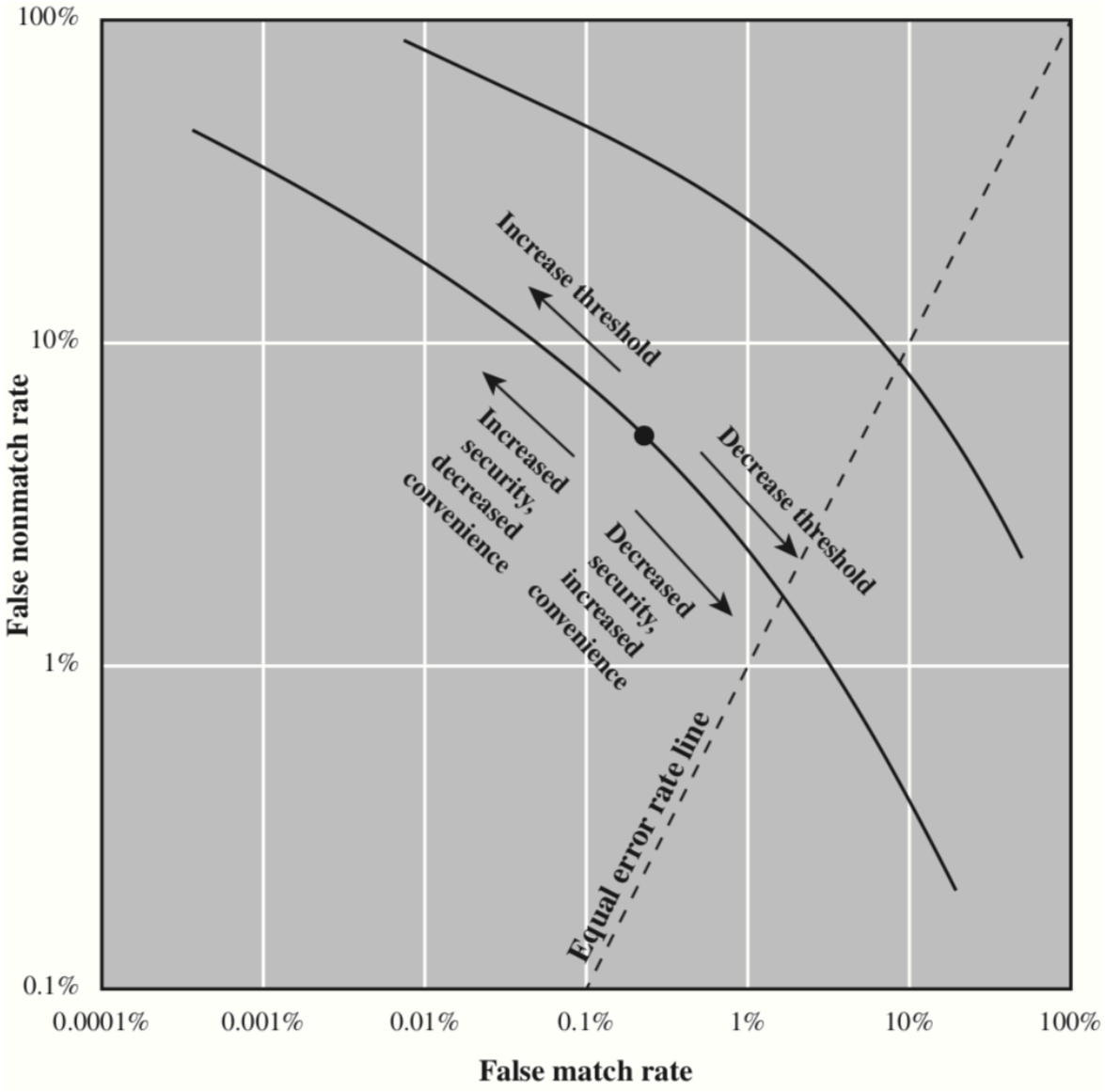
- Based on Correction Curves for Biometric Devices: "Threshold balancing error rates" help for the decision of FRR and FAR tradeoff



Correction Curves vs. Application Types



Biometry Operating Characteristic Curve



Outline

- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issues in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

Remote Authentication

- Problems:
  - Client Attacks
  - Server Attacks
  - Channel Attacks: *eavesdropping*, *replay*, *DoS*, etc …
- Generically
  - User sends the identifier
  - Server sends a challenge (r) as a nonce
  - Client computes f(r,h(PWD)) sending the result
  - Server validates
- Entropy + Complexity of f() and h() van prevent different types of attacks

With *passwords*

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{r, h(), f()\}$	random number h(), f(), functions
P' password r', return of r	$f(r', h(P')) \rightarrow$	
	$\leftarrow$ yes/no	if $f(r', h(P')) =$ $f(r, h(P(U)))$ then yes else no

(a) Protocol for a password

With *tokens*

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, \text{h}(), \text{f}() \}$	r, random number h(), f(), functions
$P' \rightarrow W'$ password to passcode via token r', return of r	$\text{f}(r', \text{h}(W')) \rightarrow$	
	$\leftarrow$ yes/no	if $\text{f}(r', \text{h}(W')) =$ $\text{f}(r, \text{h}(W(U)))$ then yes else no

(b) Protocol for a token

With Static Biometry

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, \mathrm{E}() \}$	r, random number E(), function
$B' \rightarrow BT'$ biometric D' biometric device r', return of r	$\mathrm{E}(r', D', BT') \rightarrow$	$\mathrm{E}^{-1}\mathrm{E}(r', P', BT') =$ (r', P', BT')
	$\leftarrow$ yes/no	if $r' = r$ and $D' = D$ and $BT' = BT(U)$ then yes else no

(c) Protocol for static biometric

With Dynamic Biometry

Client	Transmission	Host
U, user	$U \rightarrow$	
	$\leftarrow \{ r, x, \mathrm{E}() \}$	r, random number x, random sequence challenge E(), function
$B', x' \rightarrow BS'(x')$ r', return of r	$\mathrm{E}(r', BS'(x')) \rightarrow$	$\mathrm{E}^{-1}\mathrm{E}(r', BS'(x')) = (r', BS'(x'))$ extract B' from $BS'(x')$
	$\leftarrow$ yes/no	if $r' = r$ and $x' = x$ and $B' = B(U)$ then yes else no

(d) Protocol for dynamic biometric

Outline

- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issues in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

Security Tradeoff:

Attacks against different authentication factors

Attacks	Authenticators	Examples	Typical Defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts; theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of service	Password, token, biometric	Lockout by multiple failed authentications	Multifactor with token

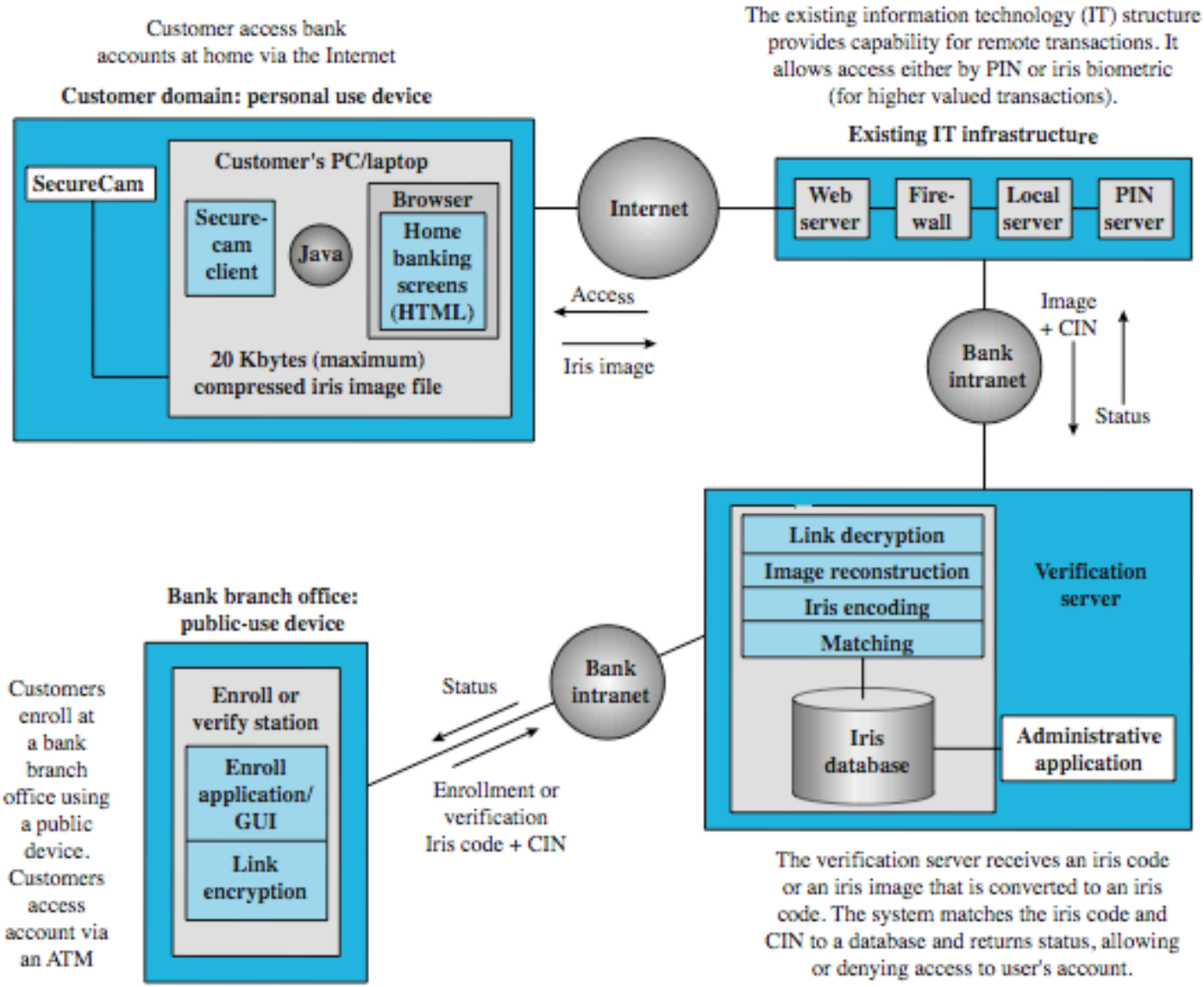
Outline

- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issues in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

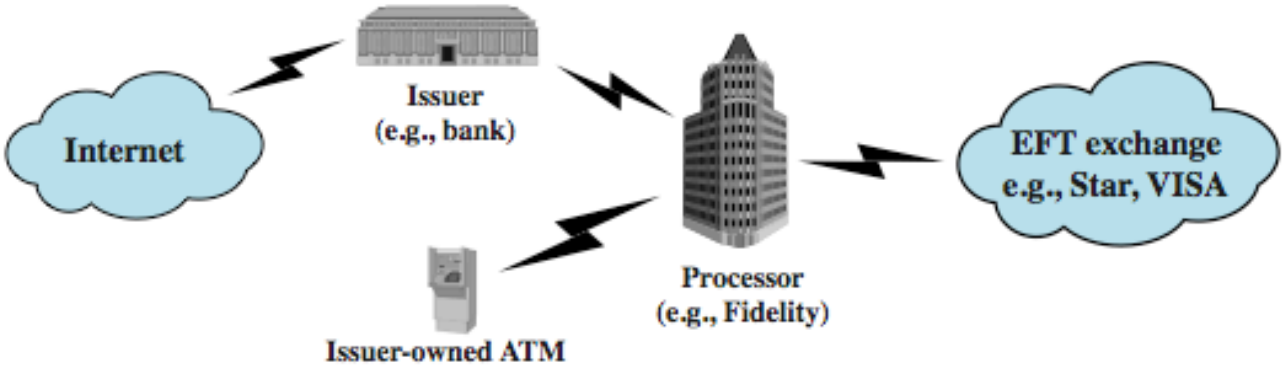
Application Scenarios

- See available bibliography:
  - Use of IRIS Biometric System
  - Case Study (Summary) for ATM Authentication

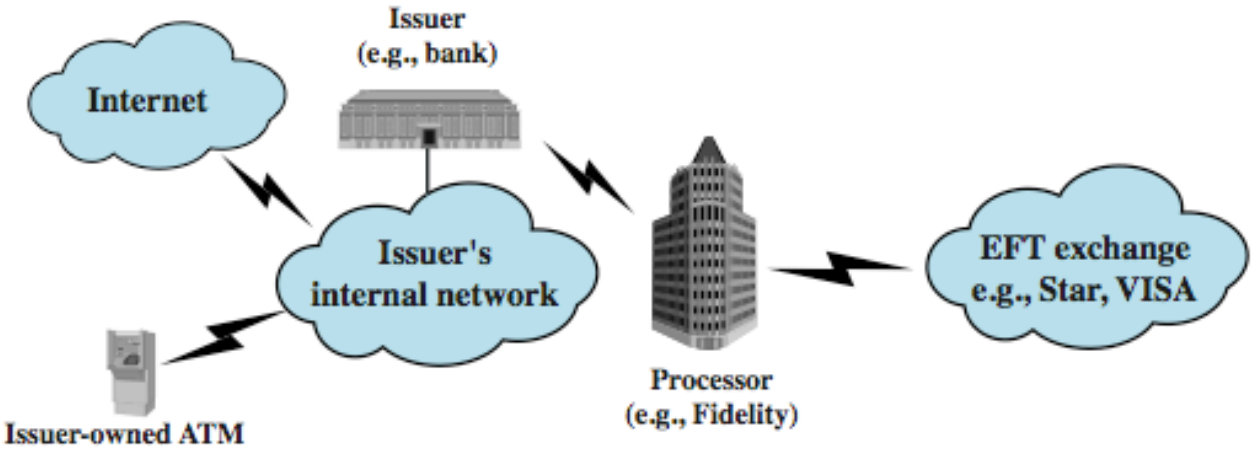
Aplicações práticas



ATMs



(a) Point-to-point connection to processor



eBanking Platforms: Multifactor Authentication

- Case Study: Caixa Direta OnLine
  - Platform Architecture and Authentication System
  - Presentation and discussion in class

MFA Example

Caixadirecta

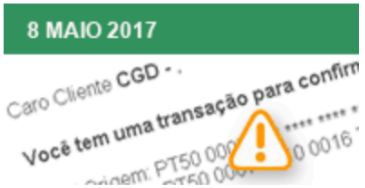
Voltar ao CGD.pt

Bem-vindo(a) ao
Caixadirecta

Contrati (Id) _____

Pwd (static) _____

Esqueceu o código de acesso?

O QUE HÁ DE NOVO	EM DESTAQUE	SABIA QUE...	A PENSAR EM SI	TENTATIVAS DE FRAUDE
				
Depósito 18 Meses - 3ª Série Certo, certo, é RECEBER JUROS de 6 em 6 meses. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Crédito Habitação** Primavera ou Verão, ESCOLHA CASA para qualquer estação. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Cartão Caixa Break** Mais acessos na consulta de movimentos. No Portal Pré-Pagos e no Caixadirecta A Caixa. Portuguesa. Com certeza. **saiba mais >>**	**Serviço 3D Secure** Seguro, simples e de adesão e utilização gratuita. **saiba mais >>**	**Esteja atento e defenda-se...** Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos. **saiba mais >>**

MFA Example

Caixadirecta

Voltar ao CGD.pt

Bem-vindo(a) ao
Caixadirecta

Contrati (Id)

Password

Esqueceu o código de acesso?

9	6	8	0	3	APAGAR
7	4	1	2	5	ENTRAR

Contraste do teclado

O QUE HÁ DE NOVO

Depósito 18 Meses - 3ª Série

Certo, certo, é RECEBER JUROS de 6 em 6 meses.
Na Caixa. Portuguesa, com certeza.
saiba mais >>

EM DESTAQUE

Crédito Habitação

Primavera ou Verão, ESCOLHA CASA para qualquer estação.
Na Caixa. Portuguesa, com certeza.
saiba mais >>

SABIA QUE...

Cartão Caixa Break

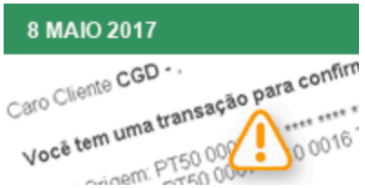
Mais acessos na consulta de movimentos. No Portal Pré-Pagos e no Caixadirecta
A Caixa. Portuguesa. Com certeza.
saiba mais >>

A PENSAR EM SI

Serviço 3D Secure

Seguro, simples e de adesão e utilização gratuita.
saiba mais >>

TENTATIVAS DE FRAUDE



Esteja atento e defenda-se...

Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos.
saiba mais >>

MFA Example (with a dynamic OTP Token)

MFA Example (with a SW-Token)

MFA and types of Tokens

Exemplos de autenticação multifator

Caixadirecta

Voltar ao CGD.pt

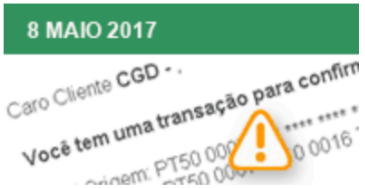
Bem-vindo(a) ao
Caixadirecta

Contrati (Id)

Password

9 6 8 0 3 APAGAR
7 4 1 2 5 ENTRAR
Contraste do teclado

Sign in

O QUE HÁ DE NOVO	EM DESTAQUE	SABIA QUE...	A PENSAR EM SI	TENTATIVAS DE FRAUDE
				 8 MAIO 2017 Caro Cliente CGD - Você tem uma transação para confirm
Depósito 18 Meses - 3ª Série	**Crédito Habitação**	**Cartão Caixa Break**	**Serviço 3D Secure**	**Esteja atento e defenda-se...**
Certo, certo, é RECEBER JUROS de 6 em 6 meses. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	Primavera ou Verão, ESCOLHA CASA para qualquer estação. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	Mais acessos na consulta de movimentos. No Portal Pré-Pagos e no Caixadirecta A Caixa. Portuguesa. Com certeza. **saiba mais >>**	Seguro, simples e de adesão e utilização gratuita. **saiba mais >>**	Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos. **saiba mais >>**

Exemplos de autenticação multifator

Caixadirecta

Voltar ao CGD.pt

Bem-vindo(a) ao
Caixadirecta

Challenge

O QUE HÁ DE NOVO	EM DESTAQUE	SABIA QUE...	A PENSAR EM SI	TENTATIVAS DE FRAUDE
				8 MAIO 2017 Caro Cliente CGD - . Você tem uma transação para confirm origem: PT50 000 **** **** * 0016
Depósito 18 Meses - 3ª Série Certo, certo, é RECEBER JUROS de 6 em 6 meses. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Crédito Habitação** Primavera ou Verão, ESCOLHA CASA para qualquer estação. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Cartão Caixa Break** Mais acessos na consulta de movimentos. No Portal Pré-Pagos e no Caixadirecta A Caixa. Portuguesa. Com certeza. **saiba mais >>**	**Serviço 3D Secure** Seguro, simples e de adesão e utilização gratuita. **saiba mais >>**	**Esteja atento e defenda-se...** Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos. **saiba mais >>**

Example with MFA using Tokens from Smartcards

Other Examples

Other Examples

Other Examples

Other Examples

Caixadirecta

Voltar ao CGD.pt

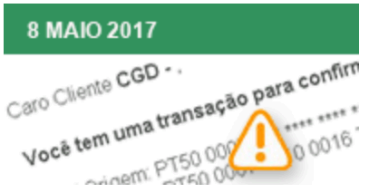
Bem-vindo(a) ao
Caixadirecta

Contrati (Id)

Password

9 6 8 0 3 APAGAR
7 4 1 2 5 ENTRAR
Contraste do teclado

Sign in

O QUE HÁ DE NOVO	EM DESTAQUE	SABIA QUE...	A PENSAR EM SI	TENTATIVAS DE FRAUDE
				
Depósito 18 Meses - 3ª Série Certo, certo, é RECEBER JUROS de 6 em 6 meses. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Crédito Habitação** Primavera ou Verão, ESCOLHA CASA para qualquer estação. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Cartão Caixa Break** Mais acessos na consulta de movimentos. No Portal Pré-Pagos e no Caixadirecta A Caixa. Portuguesa. Com certeza. **saiba mais >>**	**Serviço 3D Secure** Seguro, simples e de adesão e utilização gratuita. **saiba mais >>**	8 MAIO 2017 Caro Cliente CGD Você tem uma transação para confirm **Esteja atento e defenda-se...** Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos. **saiba mais >>**

Other Examples

Caixadirecta

Voltar ao CGD.pt

Bem-vindo(a) ao
Caixadirecta

Challenge

O QUE HÁ DE NOVO	EM DESTAQUE	SABIA QUE...	A PENSAR EM SI	TENTATIVAS DE FRAUDE
				8 MAIO 2017 Caro Cliente CGD - . Você tem uma transação para confirm origem: PT50 000 **** **** * 0016
Depósito 18 Meses - 3ª Série Certo, certo, é RECEBER JUROS de 6 em 6 meses. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Crédito Habitação** Primavera ou Verão, ESCOLHA CASA para qualquer estação. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Cartão Caixa Break** Mais acessos na consulta de movimentos. No Portal Pré-Pagos e no Caixadirecta A Caixa. Portuguesa. Com certeza. **saiba mais >>**	**Serviço 3D Secure** Seguro, simples e de adesão e utilização gratuita. **saiba mais >>**	**Esteja atento e defenda-se...** Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos. **saiba mais >>**

Other Examples

Caixadirecta

Voltar ao CGD.pt

Bem-vindo(a) ao
Caixadirecta

Challenge

O QUE HÁ DE NOVO

Depósito 18 Meses - 3ª Série

Certo, certo, é RECEBER JUROS de 6 em 6 meses.
Na Caixa. Portuguesa, com certeza.
saiba mais >>

EM DESTAQUE

Crédito Habitação

Primavera ou Verão, ESCOLHA CASA para qualquer estação.
Na Caixa. Portuguesa, com
saiba mais >>

TENTATIVAS DE FRAUDE

8 MAIO 2017

Caro Cliente CGD -
Você tem uma transação para confirm

Esteja atento e defenda-se...

Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos.
saiba mais >>

Other Examples

Caixadirecta

Voltar ao CGD.pt

Bem-vindo(a) ao
Caixadirecta

Challenge

O QUE HÁ DE NOVO

Depósito 18 Meses - 3ª Série

Certo, certo, é RECEBER JUROS de 6 em 6 meses.
Na Caixa. Portuguesa, com certeza.
saiba mais >>

EM DESTAQUE

Crédito Habitação

Primavera ou Verão, ESCOLHA CASA para qualquer estação.
Na Caixa. Portuguesa, com
saiba mais >>

TENTATIVAS DE FRAUDE

8 MAIO 2017

Caro Cliente CGD

Você tem uma transação para confirm

Esteja atento e defenda-se...

Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos.
saiba mais >>

Other Examples

Caixadirecta

Voltar ao CGD.pt

Bem-vindo(a) ao
Caixadirecta

Challenge

O QUE HÁ DE NOVO	EM DESTAQUE	SABIA QUE...	A PENSAR EM SI	TENTATIVAS DE FRAUDE
				8 MAIO 2017 Caro Cliente CGD - . Você tem uma transação para confirm origem: PT50 000 **** **** * 0 0016
Depósito 18 Meses - 3ª Série Certo, certo, é RECEBER JUROS de 6 em 6 meses. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Crédito Habitação** Primavera ou Verão, ESCOLHA CASA para qualquer estação. Na Caixa. Portuguesa, com certeza. **saiba mais >>**	**Cartão Caixa Break** Mais acessos na consulta de movimentos. No Portal Pré-Pagos e no Caixadirecta A Caixa. Portuguesa. Com certeza. **saiba mais >>**	**Serviço 3D Secure** Seguro, simples e de adesão e utilização gratuita. **saiba mais >>**	**Esteja atento e defenda-se...** Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos. **saiba mais >>**

Other Examples

Caixadirecta

Voltar ao CGD.pt

Bem-vindo(a) ao Caixadirecta

Challenge))))))

O QUE HÁ DE NOVO

Depósito 18 Meses - 3ª Série

Certo, certo, é RECEBER JUROS de 6 em 6 meses.
Na Caixa. Portuguesa, com certeza.
saiba mais >>

EM DESTAQU

Crédito Habita

Primavera ou Ve… ESCOLHA CASA… para qualquer es…
Na Caixa. Portug…
saiba mais >>

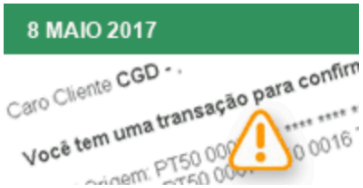
…de …é-Pagos e …n certeza.

A PENSAR EM SI

Serviço 3D Secure

Seguro, simples e de adesão e utilização gratuita.
saiba mais >>

TENTATIVAS DE FRAUDE



Esteja atento e defenda-se...

Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos.
saiba mais >>

Other Examples

Caixadirecta

Voltar ao CGD.pt

Bem-vindo(a) ao
Caixadirecta

O QUE HÁ DE NOVO

Depósito 18 Meses - 3ª Série

Certo, certo, é RECEBER JURO
de 6 em 6 meses.
Na Caixa. Portuguesa, com
saiba mais >>

EM DESTAQUE

ão Caixa Break

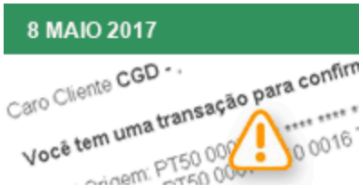
s acessos na consulta de
ovimentos. No Portal Pré-Pagos e
no Caixadirecta
A Caixa. Portuguesa. Com certeza.
saiba mais >>

A PENSAR EM SI

Serviço 3D Secure

Seguro, simples e de adesão e
utilização gratuita.
saiba mais >>

TENTATIVAS DE FRAUDE



Esteja atento e defenda-se...

Conheça as **últimas tentativas de fraude** e saiba como evitar situações que podem comprometer a privacidade e a segurança de clientes de Internet Banking da CGD e de outros bancos.
saiba mais >>

Outline

- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issues in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

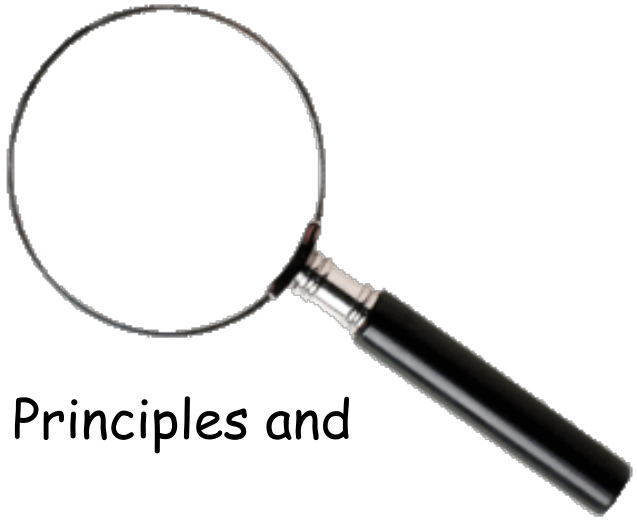
Outline

- Authentication
- Authentication approach levels
- User Authentication, Authentication Factors and MFA
- Authentication with Passwords
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Security Issued in User Authentication
- Practical Applications
- User Authentication Protocol for WA #2

WA #2 – Authentication Service

- Discussion

Revision: Suggested Readings and Study



Readings:

W. Stallings, L. Brown, Computer Security – Principles and Practice, 3rd Edition, Ed. 2015,

- Chap 3 - User Authentication

See CLIP

Revision: Complementary Readings

See the other references on the slides
and also other bibliog. references in the textbook