User authentication and identification

PV018

Identification vs. Authentication

Determination of a person's identity. (1:N)

"Positive authentication"

Hard to achieve

- Small user groups.
- Low accuracy.
- Exception: iris scan.

Verification of a person's identity claim. (1:1)

Easier than identification.

User group size – accuracy!

Means of authentication

- something you know (password, PIN)
- something you have (key, smartcard)
- something you are - biometrics
- or combination of the above

Access to a service

- Access by a person (process) that knows a secret.
- Access by a person possessing a “key”.
- Access by a person with this characteristic.

Something you know

+ Easy transport
+ Not a physical object
+ Easy & Fast control
+ Easy maintenance
+ (Low cost)

– Easy to copy after discovery
– Can be discovered without user's knowledge
– Limited by human memory
– Can be forgotten

Something you have

+ Hard to copy
+ Loss easy to discover
+ The object itself can process information

– Need of reader
– User is not recognized without the object
– The object must be complicated so that it is hard to copy
– Can break down, this often not detected easily

Something you are

+ Is part of a person
+ Cannot be lost

– Accuracy
– Protests/resistance of users
– Hard to measure
– Limited number of object to use ☺

Combine!

- Multifactor authentication
  - Something you know
  - Something you have
  - Something you are
- ATM/Banking card – card + PIN
- Spoken passphrase – passprase + speaker recogn.
- Really smart smartcard – card + PIN + fingerprint

Passwords

- Group passwords common to all users (in a group) of a system
- Passwords unique to individual users
- Non-unique passwords confirming identity
- One-time passwords

Don’t store passwords in clear text!

- Salting technique
  - userID, salt, hash(password, salt)
  - Effective password
    - Longer
    - Not a common word/combination
  - Two users with the same password have different entries in the password database.

Passwords

Human memory vs. security

(short easy-to-guess string vs. long complicated string)

- Dictionary attack
  - All combinations of up to 5-8 characters.
  - Common words and user-related values.
  - Usual success rate 20-40%

Choice of passwords – problems

- Easy to remember for the user and hard to guess for anyone else

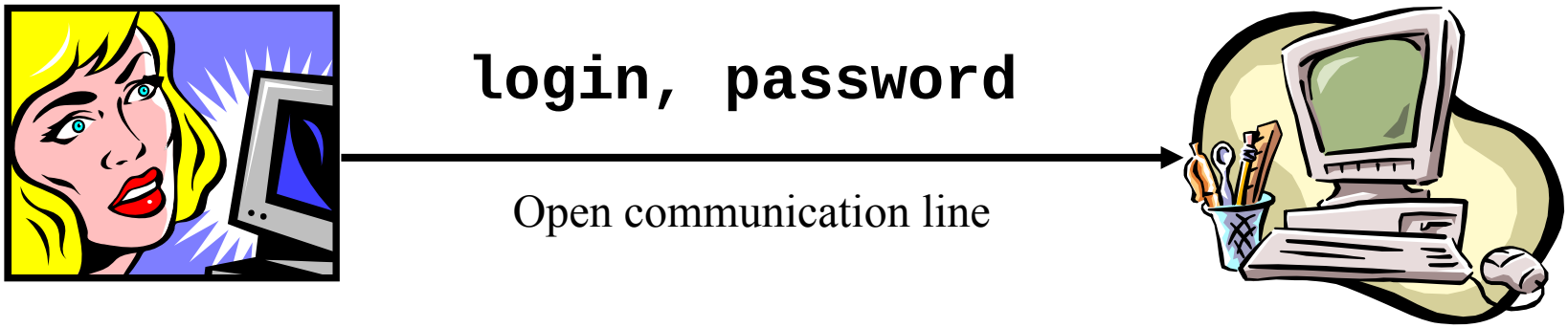
- Requested change (password “circulation”)
- Password selection without user input ☹
- Same password over more systems

Choice of passwords – suggestions

- Password (choice) quality control!!!
- Special characters, Shift, substitutions (phonetic, mnemonic)
- Use phrases: *Early One Morning With Time To Kill* (☺ Sting) – EY1ghe2KL

- Enforce your password security policy through some mechanism!!!

Passwords – replay attack



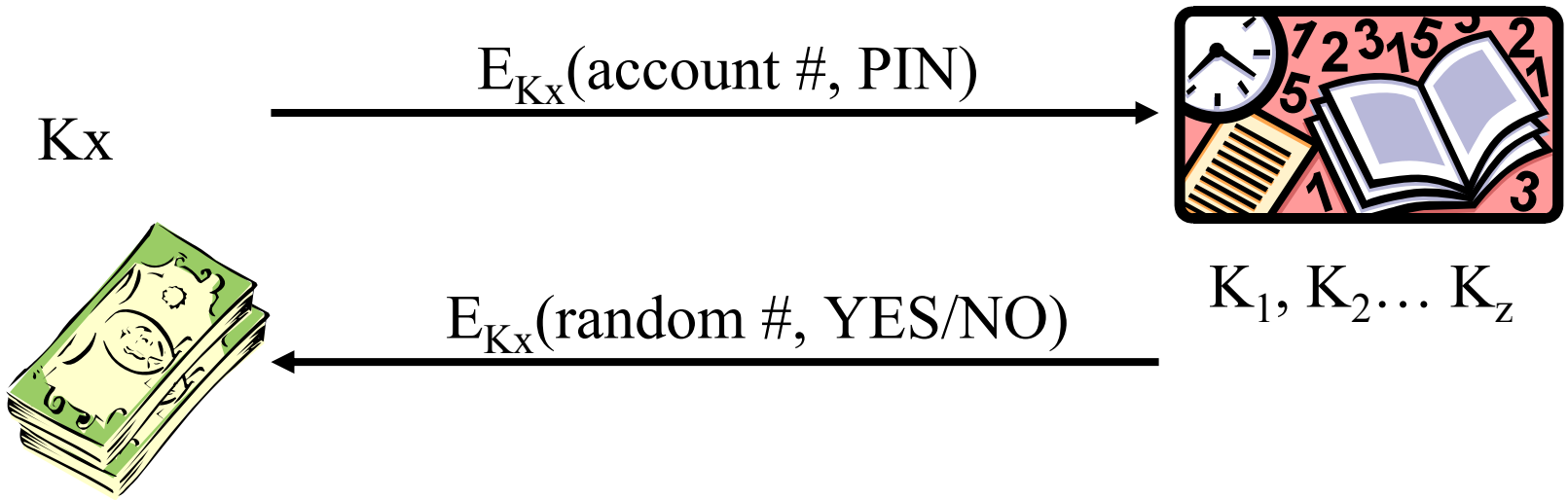
- One-time password
  - Pre-generated (password list).
  - Time/challenge based (usually with a token).
- Hash function to mask the password
  - Possibly also with a random value

Banks – card & PIN

- Personal Identification Number
  - Every combination with same probability
  - Not discarding “easy” combinations
  - Not only 4, but up to 8 (6) digits
  - Markus Kuhn – Cambridge (UK) – ref. later
- Distribution of card, PIN
  - Both via different routes (or instances)
  - Personal retrieval (of at least one)
  - PIN of own choice

PIN verification

- Offline – usually ATMs have the same key K, the card carries *x=f(K,PIN)*
- Online:



Suggested (not required) readings

- M. Kuhn: *Probability Theory for Pickpockets – ec-PIN Guessing*
  http://www.cl.cam.ac.uk/~mgk25/ec-pin-prob.pdf
- J. Yan et al.: *The memorability and security of passwords – some empirical results*, University of Cambridge Computer Laboratory Technical Report No. 500
  http://www.cl.cam.ac.uk/TechReports/

Token

- The dictionary says…
  - Projev, znamení, upomínka, památka
  - Známka pravosti
  - *By the token...* Na důkaz toho
  - *Token money...* Mince kryté zlatem

Tokens

- Keys
- Magnetic cards (3-track strip ~ 250 B)
  - Easy to copy
    - Shifting tracks of limited use
    - Individual characteristics of tracks can be of some use
  - PIN manipulation also easy
- Bank cards – with signature, possibly PIN
  - *Customer Not Present* transactions problematic

Smartcards

- Smartcard vs. Chipcard
- Can store (some even work with) a crypto key
- Cash-loading (anonymous vs. loss-recoverable)
- GSM – authentication key; PIN-PUK
- Implementation in bank cards
  - Compatibility – users, retailers(!) (VISA – 2007)
  - Potentially can be used with biometrics

Authentication calculators

- Challenge-response based
  - Response = *f(secret key, challenge)*
- Time-based (SecurID)
  - Server takes care of time-frame shifts

- Transfer – manual vs. automatic
- PIN – standard and emergency

Biometrics

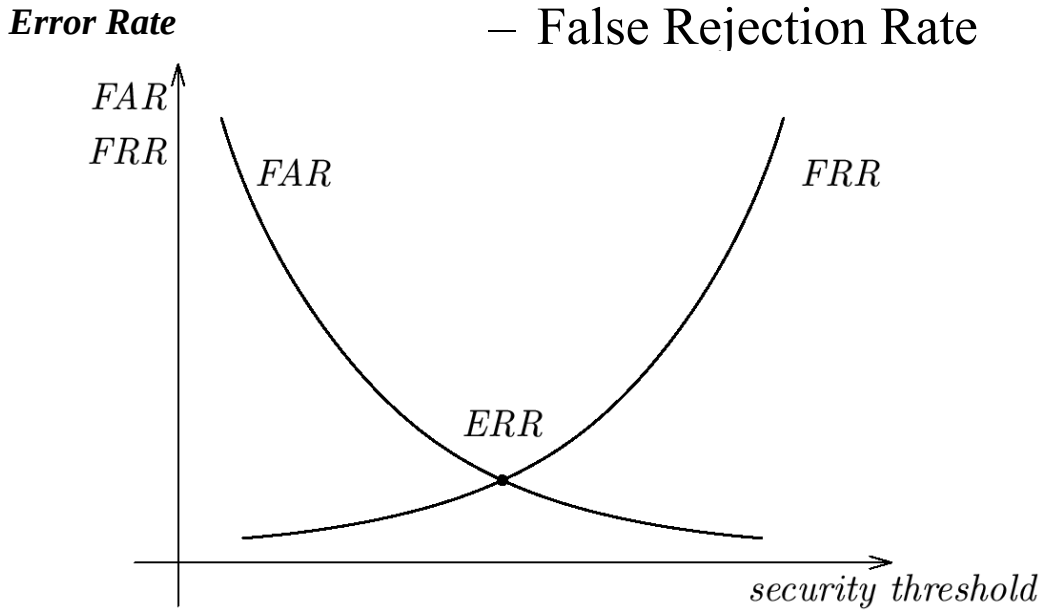
- PIN/password either matches (at 100%) or not
- Biometrics rarely match at 100% (often taken as a fake/attack).
- Threshold-based decision introduces the rates of false acceptance and rejection
- **Verification** (of identity) - 1:1 match)
- **Identification** - 1:N search for the best match

Biometrics - how to evaluate

- Do you have it?
  - Finger, iris, palm, face...
- Can you do it?
  - Sign
  - Read a sentence
  - Type on keyboard
  - Move your face

Devices:

- readers/verifiers
- acceptance threshold:
  - False Acceptance Rate
  - False Rejection Rate



Biometrics – major issues

- Biometrics are very sensitive
- Biometrics are not secrets
- Copying: neither trivial nor hard
- New attack countermeasures are followed by newer attacks

Related topics – to be discussed later

- Biometrics – to be continued…
- Authentication of data/messages – protocols

- Course PV157 “Authentication and Access Control”

Questions?

Reminder:

Term project topic agreed by March 9!