Distributed Systems

Smart Cards, Biometrics, & CAPTCHA

Paul Krzyzanowski
pxk@cs.rutgers.edu

Except as otherwise noted, the content of this presentation is licensed under the Creative Commons Attribution 2.5 License.

Carrying certificates around

How do you use your [digital] identity?

- Install your certificate in browser
- On-computer keychain file

Need there be more?

Smart cards

- Smart card
  - Portable device
    - credit card, , key fob, button with IC on it
- Communication
  - Contact-based
  - Contactless
    - Near Field Communication (NFC)
    - Communication within a few inches of reader
    - May draw power from reader's EMF signal
    - 106-424 kbps
  - Hybrid: contact and contactless

Smart cards

Capabilities

- Memory cards
  - Magnetic stripe: stores 125 bytes
  - Smart cards typically store 32-64 KB
  - Optional security for data access
- Microcontroller cards
  - OS + programs + cryptographic hardware + memory

Smart card advantages

- Security
  - on-board encryption, hashing, signing
  - data can be securely transferred
  - Store biometric data & verify against user
  - key store
    - store public keys (your certificates)
    - *do not* divulge private keys
    - perform digital signatures on card
- Convenience
  - more data can be carried on the card
- Personalization
  - e.g. GSM phone card

Smart card applications

- Stored-value cards (electronic purses)
  - Developed for small-value transactions
  - Mid 1990s in Europe and Asia
- GSM phone SIM card
- Credit/Debit
  - Stored account numbers, one-time numbers
  - EMV System (Europay, MasterCard, VISA)
- Passports
  - Encoded biometric information, account numbers
- Toll collection & telephone cards
  - Account number (EZ-Pass) or stored value (mass transit)
- Cryptographic smart cards
  - Authentication: pin-protected signing with private key

Example: Passport

- Contactless communication
- Stores:
  - Descriptive data
  - Digitized facial image
  - Fingerprints, iris scan, etc. optional
  - Certificate of document signer & personal public key
- Basic Access Control (BAC)
  - Negotiate session key using: passport #, date of birth, expiration date
  - This data is read optically – *so you need physical access*
  - Generates 3DESS "document basic access keys"
    - Fixed for life
  - German proposal to use Diffie-Hellman key negotiation

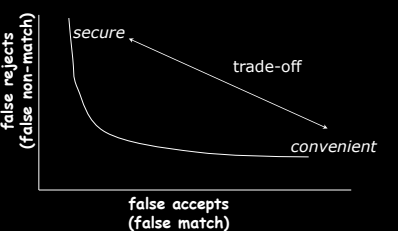
Example: Octopus

- Stored value card - contactless
  - Provision for automatic replenishment
  - Asynchronous transaction recording to banks
  - Two-way authentication based on public keys
    - All communications is encrypted
- Widely used in Hong Kong & Shenzen
  - Buses, stores, supermarkets, fast food, parking
  - Logs $10.8 million per day on more than 50,000 readers
- Available in:
  - Cards, fobs, watches, toys

Biometric authentication

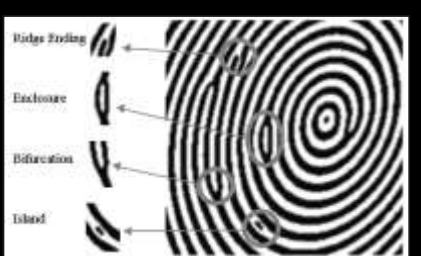
Biometrics

- Statistical pattern recognition
  - Thresholds
- Each biometric system has a characteristic ROC plot
  - (receiver operator curve, a legacy from radio electronics)



Biometrics: forms

Fingerprints
- identify minutia



source: http://anil299.tripod.com/vol_002_no_001/papers/paper005.html

Biometrics: forms

- Iris
  - Analyze pattern of spokes: excellent uniqueness, signal can be normalized for fast matching
- Retina scan
  - Excellent uniqueness but not popular for non-criminals
- Fingerprint
  - Reasonable uniqueness
- Hand geometry
  - Low guarantee of uniqueness: generally need 1:1 match
- Signature, Voice
  - Behavioral vs. physical system
  - Can change with demeanor, tend to have low recognition rates
- Facial geometry

Biometrics: desirable characteristics

- Robustness
  - Repeatable, not subject to large changes over time

  Fingerprints & iris patterns are more robust than voice
- Distinctiveness
  - Differences in the pattern among population

  Fingerprints: typically 40-60 distinct features

  Irises: typically >250 distinct features

  Hand geometry: ~1 in 100 people may have a hand with measurements close to yours.

Biometrics: desirable characteristics

Biometric	Robustness	Distinctiveness
Fingerprint	Moderate	High
Hand Geometry	Moderate	Low
Voice	Moderate	Low
Iris	High	High
Signature	Low	Moderate

Irises vs. Fingerprints

- Number of features measured:
  - High-end fingerprint systems: ~40-60 features
  - Iris systems: ~240 features
- Ease of data capture
  - More difficult to damage an iris
  - Feature capture more difficult for fingerprints:
    - Smudges, gloves, dryness, …

Irises vs. Fingerprints

- False accept rates
  - Fingerprints: ~ 1:100,000 (varies by vendor)
  - Irises: ~ 1:1.2 million
- Ease of searching
  - Fingerprints cannot be normalized
    1:many searches are difficult
  - Irises can be normalized to generate a unique IrisCode
    1:many searches much faster

Biometrics: desirable characteristics

- Cooperative systems (multi-factor)
  - User provides identity, such as name and/or PIN
- Non-cooperative
  - Users cannot be relied on to identify themselves
  - Need to search large portion of database
- Overt vs. covert identification
- Habituated vs. non-habituated
  - Do users regularly use (train) the system

Identification vs. Verification

- Identification: *Who is this?*
  - 1:many search
- Verification: *Is this X?*
  - Present a name, PIN, token
  - 1:1 (or 1:small #) search

Biometric: authentication process

1. Sensing
   - User's characteristic must be presented to a sensor
   - Output is a function of:
     - Biometric measure
     - The way it is presented
     - Technical characteristics of sensor

2. Signal Processing
   - Feature extraction
   - Extract the desired biometric pattern
     - remove noise and signal losses
     - discard qualities that are not distinctive/repeatable
     - Determine if feature is of "good quality"

Biometric: authentication process

3. Pattern matching
   - Sample compared to original signal in database
   - Closely matched patterns have "small distances" between them
   - Distances will hardly ever be 0 (perfect match)

4. Decisions
   - Decide if the match is close enough
   - Trade-off:
     ↓ false non-matches leads to ↑false matches

Biometric: authentication process

0. Enrollment
   - The user's entry in a database of biometric signals must be populated.
   - Initial sensing + feature extraction.
   - May be repeated to ensure good feature extraction

Detecting Humanness

Gestalt Psychology (1922-1923)

- Max Wertheimer, Kurt Koffka
- Laws of organization
  - Proximity
    - We tend to group things together that are close together in space
  - Similarity
    - We tend to group things together that are similar
  - Good Continuation
    - We tend to perceive things in good form
  - Closure
    - We tend to make our experience as complete as possible
  - Figure and Ground
    - We tend to organize our perceptions by distinguishing between a figure and a background

Source: http://www.webrenovators.com/psych/GestaltPsychology.htm

Gestalt Psychology

18 x 22 pixels

Gestalt Psychology

HELLO

Gestalt Psychology

HELLO

Authenticating humanness

- Battle the Bots
  - Create a test that is easy for humans but extremely difficult for computers
- CAPTCHA
  - **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part
  - Image Degradation
    - Exploit our limits in OCR technology
    - Leverages human Gestalt psychology: reconstruction
  - 2000: Yahoo! and Manuel Blum & team at CMU
    - **EZ-Gimpy**: one of 850 words
  - Henry Baird @ CMU & Monica Chew at UCB
    - **BaffleText**: generates a few words + random non-English words

Source: http://www.sciam.com/print_version.cfm?articleID=00053EA7-B6E8-1F80-B57583414B7F0103
http://tinyurl.com/dg2zf

CAPTCHA

Hotmail

Yahoo

See captchas.net

The end.