6.857 Rivest
L23.1 5/4/09

Admin: Guest lecturer on Wed
Paul Ducklin from Sophos
"live malware" demo
in Kiva / Patil - 32G-449 (11-12:30)
(check your email for possible changes)
Then projects

Outline: User identification & authentication

- ☐ Problem defns
- ☐ Approaches & examples
- ☐ Desirable properties
- ☐ Biometrics
- ☐ Using biometrics remotely (secure sketches & fuzzy extractors)

☐ What's next

User identification & authentication

- **Identification:** "Who are you?"
  result = name or unique id
  one-of-many discrimination
  ✓cooperative, vs uncooperative/absent/remote

- **Authentication:** "Is it really you?"
  result = accept/reject
  based on previously establish template of authentication parameters
  so: two parts
  ① enrollment/registration: obtain authentication info
  (save in DB keyed by name)
  ② test/recognition/authentication:
  test if user authenticates w.r.t. stored template

Authentication methods may be based on:

① Something you know (password) (SSN) (mother's maiden name)

② Something you own (token, CC, key)

③ Something you are (biometrics; fingerprints, etc.) (photo)

④ Where you are

- Can have two-factor authentication (e.g. password + biometric)
- May be static or dynamic (e.g. voice analysis)

M y ngs the

the

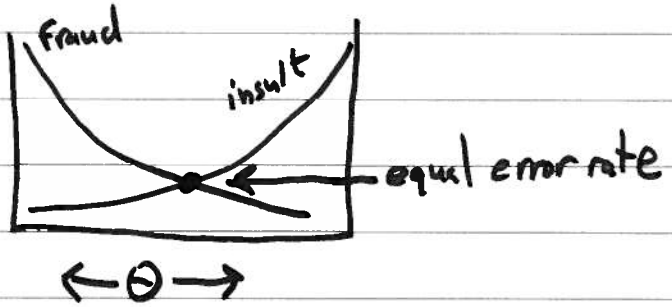
y

g pn

p p l

Considerations:

- **Universality** : works for everyone (missing finger?)
- **Ease of use** : long passwords — time taken
  retinal scan
- **Psychological acceptability**: (e.g. putting eye near machine)
- **Cost**: equipment, CPU time
- **Ease of changing/updating authentication parameters**
  - password easy to change; retinal scan not
- **Reliability / maintainability**: dirt on sensors, etc.
- **Effectiveness**: Low "fraud rate"
  Prob (accept incorrectly)
  Low "insult rate"
  Prob (reject incorrectly)
- **Adjustable threshold**:



- **Resistance to deceit / counterfeiting / circumvention**:
  (not same as fraud rate)

Considerations (cont):

- **Cooperation required?**
- **Tranferability:** (e.g. delegation/theft)
- **Local vs Remote:** (both for enrollment & testing)
  (note possibility of attacking channel or remote reader)
  (where is template stored? ~~turned out to "scenes sketches"~~)

Note progression: user ⟷ remote computer

better ↓
1. merely identify yourself
2. identify yourself & authenticate (e.g. with password)
3. identify yourself & use authentication to establish shared secret key (for enc. & MAC's)

(2 risks hijacking of session)

methods
- 3 ⇒ PAKE = password-authenticated key exchange (elaboration of DH)
- 2 ⇒ hash(key) & look up

So: natural question is: does method support authenticated key exchange, authenticated key establishment?

Schneier: "Biometrics are powerful & useful, but they are not keys. They are useful in situations where there is a trusted path from reader to verifier; in these cases all you need is a unique ID. They are *not* useful when you need characteristics of a key: secrecy, randomness, the ability to update or destroy. Biometrics are unique identifiers, but they are not secrets."

Relevant to difference between fraud rate & resistance to malicious attack.

6.857 Rivest
L23.6 5/4/09

Biometric methods:

- Fingerprints
- Iris scan
- Hand geometry
- retinal scan
- facial recognition
- typing characteristics
- speaker recognition (voice)
- signature dynamics
- ... EEG? (future?)
- ... DNA? (more for ident than auth)

Equal error rates vary (hard to get good #'s for this)
but here are some I've seen claimed:

- fingerprint 1/20 (my laptop is much worse, high insult rate!)
- voice 1/50
- signature 1/50
- hand geometry 1/1000
- iris scan $1/10^5$

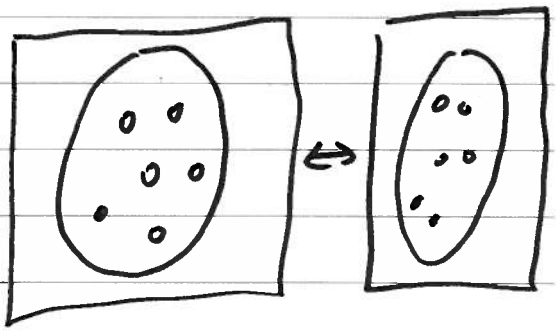
Matching fingerprints:

- Basic type: whorl, arch, loop
- identify minutia type & location

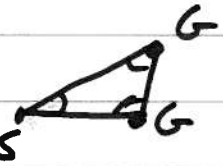
G gap

S split

E end



- match against template, measure quality of correspondence ("distance") scale-free & rotation-free manner
- e.g. triangulate ⇒ graph, feature = triangle, types of vertices & angles



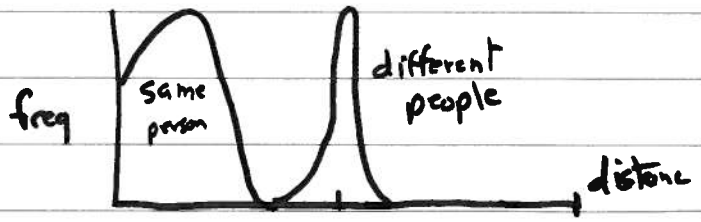
(G, G, S, 45°, 100°, 35°)

accept ± 10° on angles...
match ≥ fraction Θ of features in template...

Matching iris: [show slide]

need to consider pupil size
wavelet transform used
⇒ 2048-bit iris code
compare # matching bits

side note:
reflections in eye form covert channel
e.g. for screen.



6.857 Rivest
L23.8 5/4/09

[Gummy fingers slides] - re resistance to malicious attack

Secure Sketches & Fuzzy Extractors

sketch (bad name): x = fingerprint template
x' = measured fingerprint; "close" to x
x' + sketch ⇒ x
(maybe call it "corrector"?)
but sketch doesn't reveal info about x !

fuzzy extractor:

- how to use fingerprint as crypto key (e.g. key establishment?)

- can be built from secure sketch & standard "extractor" (hash fn)
  key = "hash" of corrected fingerprint & random value that is shared (i.e. share both sketch & random value)
  (≈ PAKE?)

[Dodis/Reyzin/Smith slides: "Generating Strong Keys from Noisy Data"]

6.857 Rivest
L23.9 5/4/09

What's next?

- New course in fall, taught by Nickolai Zeldovich on systems security.
- 6.875, 6.876 – graduate crypto classes