Biometric Security Threats and Remediation

Mark Crosbie
Senior Security Technologist

Office of Strategy and Technology
Hewlett-Packard Company

What are biometric security systems?

- Access control system where authentication of individuals is performed using biometrics
  - Fingerprint, iris, face, hand geometry
- Use biometrics for:
  - Convenience
  - Cost-effectiveness
  - Security
- Supporting infrastructure
  - Central storage of enrollments
  - Store biometric samples in document or centrally
  - Decentralised or centralised architectures

Common biometric types

- Fingerprint
  - Cheap sensors
  - Many algorithms
  - Accuracy issues
  - Physical contact
  - Speed of matching
- Face
  - Easy to acquire
  - Lower accuracy than finger/iris
  - Large sample sizes
- Iris scan
  - Very accurate
  - Fast to match
  - No physical contact
  - Some cultural issues with cameras
  - One vendor owns patents on matching algorithm!

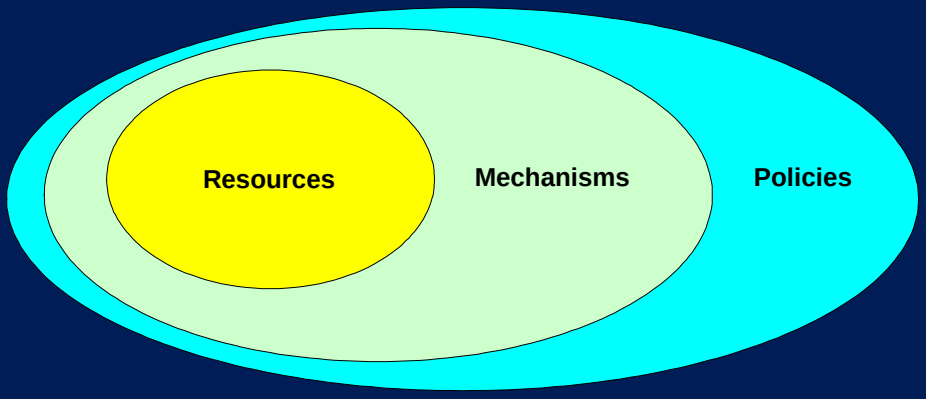
Two uses of biometrics

- **Verification**
- Prove someone is who they claim to be
- Claim of identity required
- Sample biometric
- Perform a 1-1 match
- Fast match
- Can perform offline/online

- **Identification**
- Verify someone is a member of a sub-group of population
- Probabilistic match
- Accuracy depends on population size
- Very fast algorithm required
- Must scan entire population
- Requires central online match

Security Threat Model

- What are you trying to protect (resources)
- What tools can you use? (mechansims)
- What rules do you put in place (policies)



- Architecture is driven by the threat model
- Protect what is most at risk first

Why are biometrics difficult to deploy?

- Biometrics require three things to work flawlessly:
  - 1. Hardware devices (readers, scanners)
  - 2. Software (capture, processing, storage and matching)
  - 3. Users (accept and know how to use system)
- Rarely do all three come together correctly
  - 1. Hardware: device failure, lack of accuracy
  - 2. Software: performance, accuracy, security, reliability
  - 3. Users: privacy concerns, human factors, no acceptance
- Operational issues are forgotten when deploying new technology

Biometrics = Probabilistic Authentication

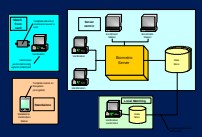
- A password either matches or it doesn't => boolean
- But biometrics are probabilistic matches
- Our model of authentication must change to reflect this

- On some days I may be "more authenticated" than on others!
  - Can I still perform every action on the system as before?

- System design can no longer assume definitive authentication.

Biometric Process flow

Physical Architecture



Measure, measure and measure again

- Biometric accuracy will vary in a real-world deployment
- Choice of sensor, algorithm and template format will impact the accuracy
- Construct a trial to simulate a real-world deployment
- Vary the trial protocol – how does the accuracy change?

Close the feedback loop

- Instrument the live systems once deployed
- Gather real-world accuracy and performance data
- Use this to “close the loop”
- Does your system perform as well as you require?
- On-line updates: push new accuracy settings out to devices as threats vary

Summary

Thank you!

Mark Crosbie
mark.crosbie@hp.com
http://www.hp.com/go/security

BACKUP SLIDES

Security Implications - Incorrect Sensor Choice

- Choose wrong sensor for environment
- Sensors fail, leads to user frustration
- Sensors may not capture clean images
- Security Implication
  - Overall system accuracy degrades
  - User frustration => they find a workaround
  - Need fall back mechanism if sensor fails

Server-centric Threat Model

- Database of biometrics is primary target
- Roles and privileges
- Audit for accountability
- Trusted path to/from server
- Secure recovery and replication

Local matching Threat Model

- Isolated from central server
  - Security of periodic synchronisation
  - How do enrolments get propagated?
- Typically a smaller PC in a kiosk
  - Not a hardened environment
  - No hardware crypto tokens
- No “global view” of activity at local level
  - Central aggregation of audits for post-event investigation
- Management plane for distributed kiosks
  - On-line tuning of accuracy and performance

An example of inappropriate use

- Payment for groceries at supermarket checkout
- Place finger on reader - you are identified.
- BUT – identification is probabilistic!
- What happens if multiple candidates are returned?
- Can I get you to pay for my groceries?
- Could I end up paying for someone else's groceries?

- Example of the incorrect use of identification
- Correct approach is authentication of individual using a claim of identity – e.g. a smartcard, swipe card.

Process flow security issues

- **Capture**
  - Is this a live sample? Is the reader intact?
  - Communications path from reader integrity
- **Quality Checks**
  - How strict to make checks?
  - Is there live feedback and adjustments?
- **Processing**
  - Template generation
- **Enrollment**
  - How did this person claim an initial identity?
  - Is this a duplicate of a prior enrollment under another name?
- **Matching** (Verification/Identification)
  - How strict a match to perform?