Biometric Credentialing for Biometrically Challenged Users

Ron Sutton

BearingPoint, LLC

November 7, 2007

Why use biometric credentials?

- Provides mechanism for limiting credential holders to a single identity within a credentialing system
  - 1:N search ties applicant's biometric(s) to an identity
  - Cannot verify the identity against any objective reality

- Increase certainty that the credential can be used only by the person to whom it is issued
  - Biometrics are only useful if the credential's biometric features are used
    - No increased security in flash-pass systems
    - No increased security in card + PIN systems

- Applicable to Physical & Logical Access Control Systems

Who can take full advantage of biometric credentials?

- Various estimates exist
  - Industry conventional wisdom says that biometric products have a 1% to 5% Failure To Enroll rate; this rate varies by product and by biometric type
  - NISTIR 7271, "The Myth of Goats:How many people have fingerprints that are hard to match?", reports on a population in which less than 0.05% had fingers that were usually hard to match

- Everyone appears to agree that there is some group of people that cannot be served by any given biometric technology

Why don't biometrics work for some?

- There are a variety of reasons a given biometric technology will not provide satisfactory results for a given individual.
  - Lack of the physical feature from which biometric samples are derived
  - Injuries to the physical feature from which biometric samples are derived
  - Physical characteristics that make biometric samples from the individual unusable
  - Physical handicaps that make the usual biometric sample devices difficult or impossible for the individual to use
  - Use of cosmetic devices that interfere with sample capture
- Some issues can be mitigated to provide for successful use
  - Dry fingers can often be overcome with oil
  - Patterned contact lens wearers can forego their use

How many are affected?

- HSPD-12 requires that all executive branch employees and contractors be issued PIV II credentials that contain fingerprint and facial biometric templates
  - If only 1% are unable to use biometrics, this translates to 10,000 of every 1,000,000 credential holders

- TSA intends, by some estimates, to issue TWICs to over 6,000,000 transportation workers
  - If 2% are unable to use biometrics then 120,000 workers would be affected

If we don't plan to serve this population, implementation of large-scale biometric access control systems will founder due to legal and social sensibility considerations

Impact to system security

- Increased security is primary motivation for use of biometrics
  - Credential-only systems allow access to anyone possessing a genuine credential, even if they're not the owner
  - PIN-based systems are only slightly better since PINs can easily be compromised
  - Biometric credential can, in theory, only be used by its owner

But… the overall security of a biometric system is compromised if some credential holders don't use biometrics

Operational options for biometric access control systems

- Alternate provisions must be made for those who cannot use the primary biometric (fingerprints)
  - Alternative biometric access (face, iris, etc)
    - Facial biometric devices could operate on PIV II facial templates
    - Other biometrics will require use of a server-based matching subsystem
  - Non-biometric access
    - Credential + PIN
    - Opens the door to misuse of credentials by unauthorized persons
  - Pseudo-biometric access
    - Credential contains identifier in biometric template indicating cardholder status
    - No more secure than non-biometric access, but helps to conceal the identity of those holding non-biometric cards
    - Only useful for persons possessing the biometric feature

Summary

- Biometric credentials enable implementation of more secure access control systems
- Such systems are only as secure as their weakest link
- There is no generally accepted approach for serving people with no or unusable biometric features
- Systems implemented without considering this population will encounter resistance and possibly prevent implementation of biometric access controls
- System operators *will* adopt a solution; if no guidance is provided these solutions may weaken security
- Without consistent, cost-effective solutions we may be issuing the world's most expensive flash passes and proximity cards

Contact Information

Ron Sutton

BearingPoint, LLC

ron.sutton@bearingpoint.com