Vulnerabilities of Biometric Technologies

20 September 2006
Biometric Consortium 2006, Baltimore
Victor Minchih Lee, Senior Consultant
vlee@biometricgroup.com
www.biometricgroup.com

About International Biometric Group

- Leading biometric consulting, integration and research firm since 1996
  - Main Office: New York City
  - Also: Washington, D.C., London
- Unique: vendor-independent, technology-neutral experts
- Technical and business expertise
  - Highest-quality, proven biometric management systems
  - Benchmark market and technology reports
  - Strategy consulting, program management, risk assessment, vulnerability and penetration testing
  - Independent Technology Validation and Verification
- Extensive relationships: 14,000+ contacts
Addressing Biometric Vulnerabilities

- Attacks
- Countermeasures
- Mitigation

Attacks
- Input-Level Attacks
  - Spoofing
  - Bypassing/Overloading
- Backend- and Storage-Level Attacks
  - Implantation
  - Infiltration
  - Hacking
- Processing and Transmission-Level Attacks
  - Hacking
  - Skimming/Sniffing - Hill-climbing

- Backend- and Storage-Level Attacks
  - Implantation
  - Infiltration
  - Hacking
**Input-Level: Spoofing**

- **SPOOFING** = presenting *artifacts* to sensors for enrollment or recognition, or to *circumvent* enrollment and recognition processes
  - Or dead body parts.

**Examples:**

- **Fingerprint Recognition**
  - Prostheses
  - Props / Gag Items
  - Photographs
  - Residual Prints
  - Latent Prints
- **Iris Recognition**
  - Prostheses
  - Playback
  - Photographs
  - Imprinted Contact Lenses
- **Face Recognition**
  - Photographs
  - Disguises / Masks
- **Hand Geometry**
  - Prostheses
  - Props / Gag Items
- **Voice Recognition**
  - Playback Recordings
  - Composite Recordings

**Spoofing Countermeasures**

- **LIVENESS DETECTION**
  - *Examples:*
    - **Fingerprint Recognition**
      - Spectroscopy
      - Temporal Variation in Perspiration
    - **Iris Recognition**
      - Photonic and spectrographic countermeasures (e.g. – red eye)
      - Behavioral countermeasures (e.g. – blinking)
      - Analog physical attack countermeasures (e.g. – dye detection)
      - Digital replay attack countermeasures (e.g. – byte scrambling)
    - **Facial Recognition**
      - Reactivity to Cues
    - **Voice Recognition**
      - Recitation of Randomly Generated Passphrases
**Input-Level: Bypassing/Overloading**

- Bypassing via “overloading”
- “Overloading” = attempting to defeat or circumvent a system through damaging or overwhelming input sensors or devices

- Attacks
  - Bright Flashes / Strobes
  - Water → Short circuiting
  - Smoke
  - Heat sources

- Countermeasures:
  - Supervision
  - “Ruggedization”
  - Conscientious form factor design
  - Strong fallback procedures and processes

**Processing- and Transmission-Level**

- Attacks
  - Hacking
  - Skimming/Sniffing
  - Hill-climbing

- Countermeasures
  - Firewalls
  - Encryption
  - Limited Range of (Transmission), Protection of Score Data
Backend- and Storage-Level

- Attacks
  - Implantation
  - Infiltration
  - Hacking
- Countermeasures
  - (Change) logs
  - Auditing
  - Firewalls
  - Random template review

Further Countermeasures/Mitigation

- Countermeasures
  - Multi-factor/multimodal authentication
    - Multiple biometrics
    - Biometrics + Related Technologies (e.g. smart cards / PINs)
  - Randomization
    - Variable Modality
    - Target of Interest
  - Challenges
    - Random
    - Cued
  - Internal / Subcutaneous (Supplementary) Focus
- Mitigation
  - Cancelable Biometrics
    - IBM
    - Biometrics Engineering Research Center (Korea)
  - Strong Backup Processes and Procedures
  - Central Databases vs. Local Databases vs. On-Card Storage
Contact Information

vlee@biometricgroup.com

212.809.9491