The Need for Biometric Authentication

- Presented previously at:
  InfoTec 2002
  DefCon 10 in Las Vegas
  NebraskaCERT 2002
  Mutual of Omaha
  ConAgra Foods

Presented by:
Nate Rotschafer
Peter Kiewit Institute

Revised: August 8, 2005

Multi-Stage Authentication

- Outline
  - Background on Authentication
  - General Network Security
  - Need for High Grade Authentication
  - Error Types
  - Forms of Biometric Authentication
  - Issues Surrounding Biometric Technology
  - What’s Hot? What’s Not?
  - Planning Points
  - Discussion

Identification

- The method used by a system (not necessarily a computer) to uniquely identify an individual or group.

Examples: User names, Driver’s
License, School ID,
Security Badge,
Passport

Authentication

- The method(s) used to verify the given identification.

  Examples: Passwords, Fingerprints, Iris Prints, Negotiation

Authorization

- Used by a system to determine if an authenticated user can have access to an object.

  Example: User belongs to a specific group, user has specific security clearance, etc.

Access

- A user is allowed access once they have authenticated and it is determined that the user is authorized to have access to an object.

Development of Authentication

- What you know…
- What you have…
- What you are…
- Future Development: How you are…

Security

- **IS NOT JUST:**
  - Installing a firewall
  - A product or service
  - Running an audit and shutting things off
  - A one time thing
- **IS:**
  - Working productively and without interruptions
  - Only as good as the weakest link
  - Risk management
  - Physical security
  - A process, methodology, policies and people
  - Operational not just procedural
  - 24x7x365
  - Access to only the information required to do your job

General Network Security

- No silver bullet to network security
- Threats:
  - Replay attacks
  - Denial of Service ([D]DoS)
  - Spoofing
  - Users
  - Dictionary Attacks
- Biometrics will help but will not solve all problems
- Users are the "weakest link"
- Proactive security plan

Need for High Grade Authentication

- High Security Areas
- Multiple Factor Authentication
- Challenge and Response Authentication
- High Assurance of Proper Identification
- Data Retrieval Based on the Person

Why would you be rolling them out?

Error Types

(Common to all biometrics)

- Type I Error - Accept in Error (False Positive)
  - Balance Between Type I and Type II Error
  - Most Dangerous
  - High Exposure
  - Preventable
  - Need for Additional Security Measures
- Type II Error - Deny in Error (False Negative)
  - Balance Between Type I and Type II Error
  - Only an Inconvenience
  - Preventable
  - Established by a High Security Policy

- What is the balance for you organization?

Forms of Biometric Authentication

- Fingerprint Scanners
- Iris Scanners
- Voice Print Scanners
- Retina Scanners
- Handwriting Recognition
- Face Recognition
- Personal Geometry
- DNA

Simply a collection of data points.

Securing Biometric Signatures

- Tamper resistant storage
- Protection from corruption
- Secure signature changes
- Secure backups
- Stop signature interception
- Protect latent signatures
- Legal implications if not protected

- You organization needs an action plan for each bullet point.

Logon Security

- Trusted path to authentication device
- Tamper resistance
- Clear or encrypted transmission?
- Continuous monitoring
- What "goes down the wire"?
- Real biometric?

Your organization needs an action plan for each bullet.

Both biometrics and passwords needed

- Driving force behind biometrics is multiple factor authentication
- If you replace passwords with biometrics you do not increase the factors, but you do inherit all the risk
- With both biometrics and passwords you are required to know 2 things (user id and password) and have one thing (your biometric)

Consistency

- Environmental effects
  - Backup plan
- All network users adhere to the same policy
  - Define policy
- All network machines configured identically
  - Define configuration specification
  - Breadth of implementation
- Trade-offs
  - Support model (help desk, desktop support, etc)
  - User portability

What’s Hot?/What’s Not?

- Hot:
  - Technology
    - Fingerprint Scanners
    - Iris Scanners
  - Issues
    - Multi-Stage Authentication
    - Interoperability
    - Interchangeability
    - Standards
    - Server Signature Storage?
- Not:
  - Technology
    - Retina Scanners
    - DNA
  - Issues
    - 1 or 2 Stage Authentication

Planning Points

- What are we fixing?
- What objectives are we trying to meet?
- What will be fixed or advanced?
- Have we mitigated as much of the risk as possible?
- Have we contingency planned?

Thanks To:

- Dr. Blaine Burnham, Director of NUCIA
- Defcon 10
- Peter Kiewit Institute
- InfoTec 2002
- NebraskaCERT 2002
- Mutual of Omaha Companies
- ConAgra Foods --- Info. Safety and Security

Discussion/Q&A

- Contact Info:
  - E-Mail: nrotschafer@gmail.com
  - Website: www.geniussystems.net
- Slides available on my website