N Stage Authentication with Biometric Devices

Presented by:
Nate Rotschafer
Sophomore
Peter Kiewit Institute

Revised: July 8, 2002

N Stage Authentication

- Outline
  - Background on Authentication
  - General Network Security
  - Need for High Grade Authentication
  - Need for Multiple Factor Authentication
  - Background on Error Types
  - Forms of Biometric Authentication
  - Pros and Cons of Each Biometric Technology
  - What's Hot? What's Not?
  - Major Players
  - Network Management with Biometric Devices
  - Problems
  - Proper Network Security with Biometric Devices
  - Demos and Discussion
  - Prognosis

Background on Authentication

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 against a database of known information.

Examples: Passwords,
Fingerprints, Iris Prints,
Negotiation

Development of Authentication

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

General Network Security

Security is NOT

- Installing a firewall
- A product or Service
- Running an audit and shutting things off

Security IS

- Working productively and without interruptions
- Only as good as the weakest link
- Risk management of resources (equipment, people)
- Physical security
- A process, methodology, policies and people
- Is 24x7x365

General Network Security

- No silver bullet to network security
- Replay attacks
- Denial of Service ((D)DoS)
- Spoofing
- Users
- Dictionary Attacks

Security Thoughts

- 80-90% are internal issues
- Hard drive crash (what did you loose, and how long to get back up?)
- Firewall penetration (what can they do, what do they see?)
- Internet failed (how much lost productivity/revenue, backup net connection?)
- Some can always get in

General Network Security Conclusion

- Biometrics will help but will not solve all problems
- Users are the “weakest link”
- Proactive security plan

Need for High Grade Authentication

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

Background on Error Types

Type I Error --- Accept in Error

- Balance Between Type I and Type II Error
- Most Dangerous
- High Exposure
- Preventable
- Need for Additional Security Measures

Type II --- Deny in Error

- Balance Between Type I and Type II Error
- Only an Inconvenience
- Prventable
- Established by a High Security Policy

Forms of Biometric Authentication

Forms of Biometric Devices

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

Pros and Cons of Each Biometric Technology

Fingerprint Scanners

- Pros
- Cons

Retina Scanners

- Pros
- Cons

Iris Scanners

- Pros
- Cons

Voice Print Scanners

- Pros
- Cons

Handwriting Recognition

- Pros
- Cons

Personal Geometry

- Pros
- Cons

Face Recognition

- Pros
- Cons

DNA

- Pros
- Cons

What's Hot? What's Not?

What's Hot?

- Fingerprint Scanners
- Iris Scanners
- N Stage Authentication
- Interoperability
- Interchangeability
- Standards
- Server Signature Storage

What's Not?

- Retina Scanners
- DNA
- 1 or 2 Stage Authentication

Major Players

Major Players

- Most ISP NOCs
- Healthcare Organizations
- Banking Industry
- Military/Government Agencies
- Department of Defense
- Schools?

Network Management with Biometric Devices

Cost

- Fingerprint Scanner --- $100-150
- Retina Scanner --- $400-500
- Iris Scanner --- $200-300
- Voice Print Scanner --- $150-200
- Face Recognition --- $150-250

Ease of Deployment

- Fingerprint Scanner --- Easy
- Retina Scanner --- Hard
- Iris Scanner --- Hard
- Voice Print Scanner --- Medium
- Face Recognition --- Easy

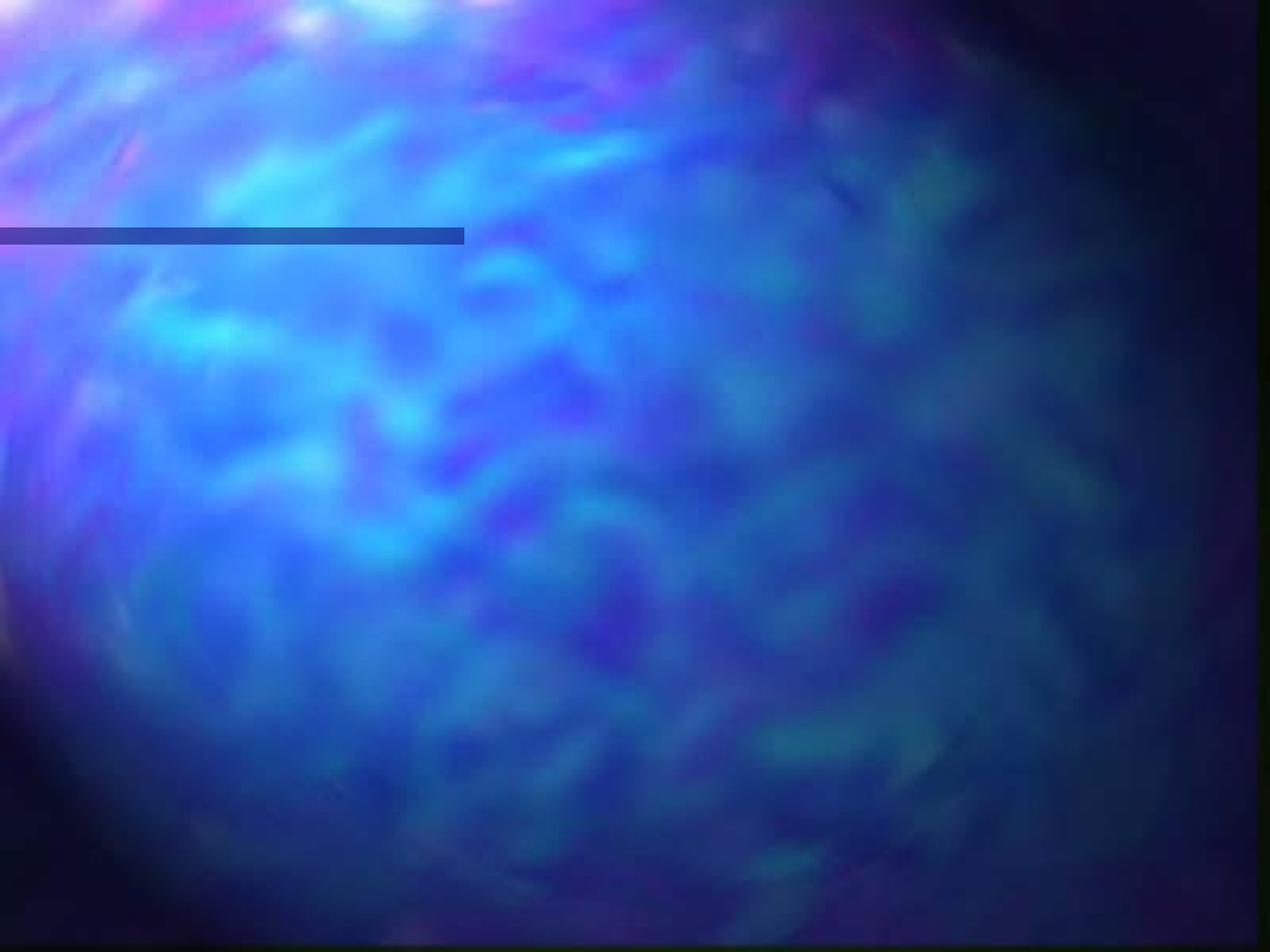
Ease of Management

- Fingerprint Scanner --- Easy
- Retina Scanner --- Medium
- Iris Scanner --- Medium
- Voice Print Scanner --- Easy
- Face Recognition --- Medium

User Effects

- Fingerprint Scanner --- Medium
- Retina Scanner --- Medium
- Iris Scanner --- Medium
- Voice Print Scanner --- High
- Face Recognition --- Medium

Problems



Proper Network Security With Biometric Devices

Securing Biometric Signatures

- Tamper resistant storage
- Protection from corruption
- Secure signature changes
- Secure backups
- Stop signature interception
- Protect latent signatures

Logon Security

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

Bypass Prevention

- Tamper resistance at the local machine
- Enhanced biometrics to tell a real biometric from a fake biometric
- Both biometrics and passwords needed

Consistency

- Environmental effects
- All network users adhere to the same policy
- All network machines configured identically

Can Biometrics be Bypassed?

- How they are connected
- The device can be fooled
- Consistency

Demos and Discussion

Demo of Fingerprint Scanner Authentication

Demo of Iris Scanner Authentication

Wire Capture Analysis

Recent Bypassing Methods

How to Bypass

Question and Answer

Thanks To:

- Dr. Blaine Burnham, Director of NUCIA
- Defcon 10
- Peter Kiewit Institute
- Dan Devries

Contact Info

- E-Mail: nrotschafer@geniussystems.net
- Slides: http://www.geniussystems.net
  - Goto the :. Talks .: section and then to the “Biometrics” folder then to the “Defcon” folder and download the .ppt slides of the presentation.

Links

- http://www.theregus.com/content/55/24956.html
- http://www.heise.de/ct/english/02/11/114/
- http://www.precisebiometrics.com/
- http://www.saflink.com/
- http://stat.tamu.edu/Biometrics/
- http://www.biometrics.org/
- http://biometrics.cse.msu.edu/