Usability Issues in Security-Related Tasks

- **Robert W. Proctor [1]**
- **Mei-Ching Lien [1]**
- **E. Eugene Schultz [1&2]**
- **Gavriel Salvendy [1]**

[1]Purdue University; [2] Global Integrity Corporation

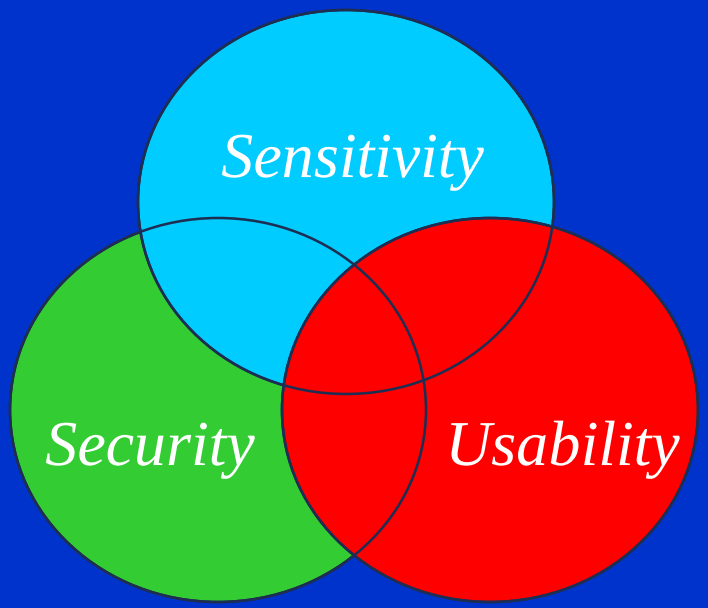
Email: proctor@psych.purdue.edu

Usability Problems in Security-Related Tasks

- **Numerous security mechanisms have been developed, many of which rely on individuals to implement and use them properly.**

- **Acceptance of security measures by users and their willingness and ability to follow the required procedures are necessary if the systems are to be effective.**

Research Direction and Goal



- *To consider the overall performance goal of the system in terms of device sensitivity, security, and usability.*
- *To create a taxonomy that outlines the nature of the security tasks and apply systematic human factors analyses to it.*

Major Types of Security-Related Controls and the Threats they Counter

CONTROL TYPE	THREAT TYPE
• Identification / Authentication	Masquerading as another user Repudiation
• Data Integrity	Unauthorized deletion or changes
• Data Confidentiality	Unauthorized disclosure or possession
• Data Availability	Unauthorized deletion of data or the databases/programs used to store and retrieve them; denial of service attacks
• System Integrity	Unauthorized deletion or changes to system data/configuration files; theft; denial of service attacks
• Intrusion Detection	Unauthorized access to systems; denial of service attacks

Identification / Authentication

- **Identify the User**

  Methods: Password

  Global Position System (GPS)

  Smart Cards

  Digital signatures

  Biometrics Approach

  Physiological based: Fingerprints

  Retinal/Iris scanning

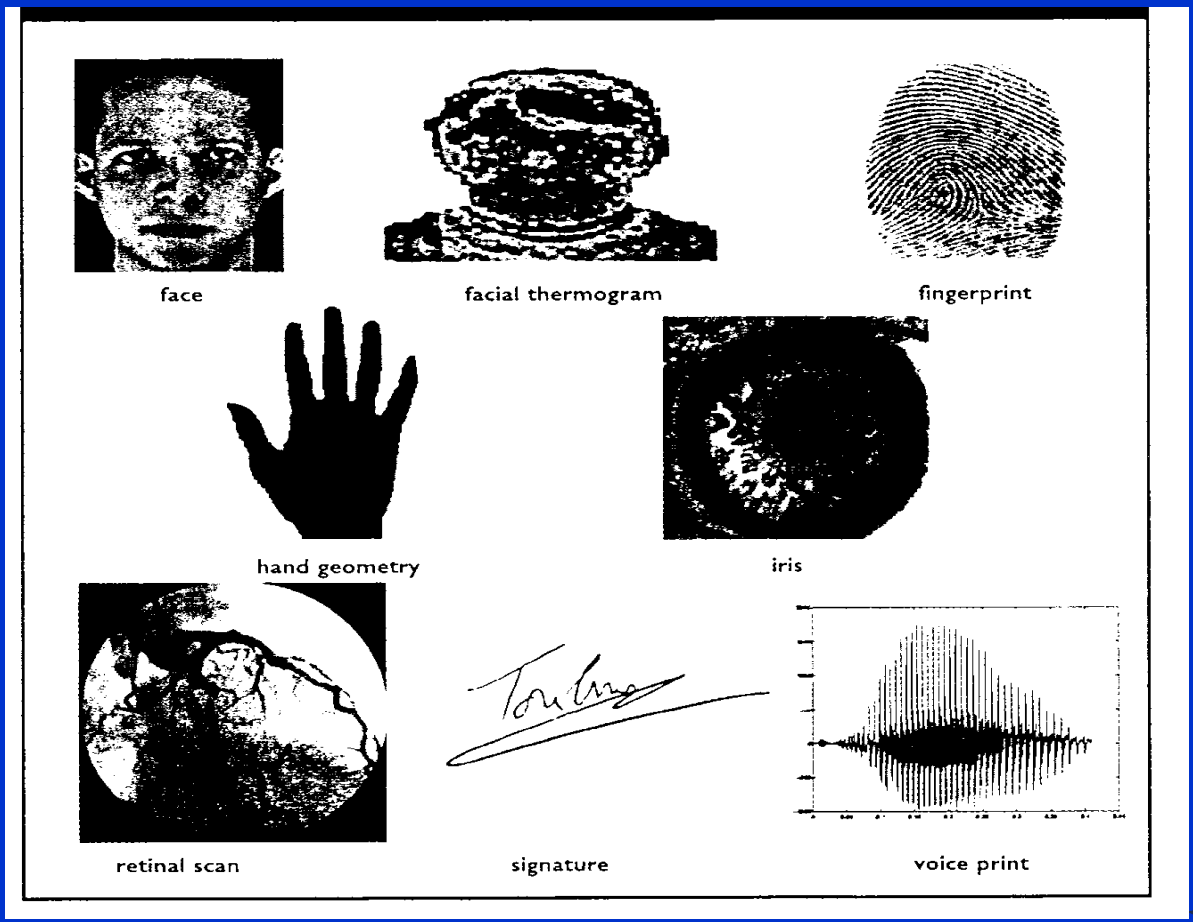
  Facial recognition

  Behavioral based: Keystroke patterns

  Signature

  Voice recognition

Examples of Different Biometric Methods



Usability Factors in Identification /Authentication

- ***High memory demand*; Require user to maintain and act on knowledge that is sometimes detailed.**
- **Install and maintain the necessary software and hardware components. For example, a fingerprint scanner has to capture good quality images of users' fingers to ensure accurate authentication and enrollments.**
- **The authentication systems have to consider the anthropometric constraints, such as the design of retinal readers must accommodate the needs of the handicapped and of short and tall persons.**

Integrity, Confidentiality, and Availability of Data

- **Ensuring that data have not been modified or deleted**

  Methods: Backups

  Integrity verification

  Encryption

  Cyclic Redundancy Checks (CRCs)

  Setting files and directories

  Time Stamping

  Event Logging

  Anti-viral Software

Usability Factors in Confidentiality, Integrity, and Availability of Data

- ***Attention resource demand*; Require monitoring and continuous verification.**
- **Require user to understand and recognize the commands and options.**
- **Manage backup media and store backups properly.**
- **Maintaining privilege control.**
- **Inspect files to ensure they have not been changed.**

Intrusion Detection

- **Detect the unauthorized user**

  Methods: System audit logging

  Intrusion detection systems

  Tripwire

  Monitoring

Usability Factors in Intrusion Detection

- User's privacy can be compromised.
- Report disruption of service.
- Responding to intrusions in an appropriate way.
- Execution of incident response procedures.
- Use of automated response software.
- Correlated multiple sources of data.
- Implement additional defensive measures.

An Example of Information Display in Intrusion Detection

12/03/97	02:19:48	0	206.256.199.8	19 -> 192.168.102.3	666
12/03/97	02:21:53	0			
12/03/97	02:28:20	0			
12/03/97	02:30:29	0			
12/03/97	02:30:44	0			
12/03/97	02:34:47	0			
12/03/97	02:35:28	0			
12/03/97	02:36:56	0			
12/03/97	02:39:23	0			
12/03/97	02:41:55	0			

12/03/97	02:19:48	0	206.256.199.8	19 -> 192.168.102.3	666
12/03/97	02:21:53	0	206.256.199.8	19 -> 164.256.23.100	666
12/03/97	02:28:20	0	206.256.199.8	19 -> 164.256.140.32	666
12/03/97	02:30:29	0	206.256.199.8	19 -> 192.168.18.28	666
12/03/97	02:30:44	0	206.256.199.8	19 -> 164.256.67.121	666
12/03/97	02:34:47	0	206.256.199.8	19 -> 164.256.140.32	666
12/03/97	02:35:28	0	206.256.199.8	19 -> 147.168.130.93	666
12/03/97	02:36:56	0	206.256.199.8	19 -> 192.168.18.28	666
12/03/97	02:39:23	0	206.256.199.8	19 -> 147.168.153.78	666
12/03/97	02:41:55	0	206.256.199.8	19 -> 147.168.130.93	666

- **Most intrusion detection systems scan over five events per second and have more than one detect window.**
- **Administrators have to detect the intrusions or to recognize the patterns in a short period of time.**

An Example of Task Analysis: The Use of Fingerprint Recognition

1. Visually sighting a prompt on the display terminal
2. Visually sighting the fingerprint reader
3. Moving a hand towards the fingerprint reader until it is in close proximity
4. Rotating the hand until the palm side is down
5. Extending a finger until it fits over the reader
6. Visually sighting the display terminal (or listening for auditory feedback) for confirming that the fingerprint was read successfully

7. Moving the hand and finger away from the fingerprint reader
8. Confirming that fingerprint has been processed properly and is valid (actual method will vary)
9. Reading a prompt that begins the “normal” username-password entry sequence
10. Homing the hand on the keyboard
11. Repeating the steps involved in a normal username-password-based logon

Possible Errors Involved in the Use of Fingerprint Recognition

1. Performance of certain critical steps in the wrong order
2. Failure to place a finger in the proper position in the fingerprint reader
3. Placement of the “wrong” finger (i.e., a finger with a cut, which is likely to render the fingerprint read invalid) in the fingerprint reader
4. Failure to keep the finger sufficiently still to enable the fingerprint to be read

Issues of Concern

- **What is the trade-off among information security control, usability, and device sensitivity?**
- **Can analyses of human performance be incorporated into analyses of system performance to predict the overall performance of the security control?**
- **What training and instructions are necessary to allow system administrators to implement effective security measures?**

Conclusions

- **Usability, sensitivity, and security are significant components of information security methods.**
- **Developing metrics for human usability based on task analysis and performance modeling will allow specification of the usability costs and benefits associated with alternative security methods and designs.**