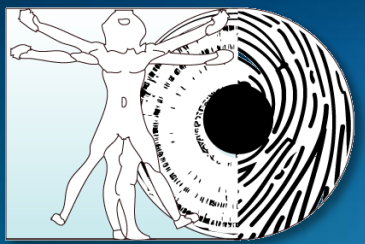
National Institute of Standards and Technology
U.S. Department of Commerce

Information Access Division
Visualization and Usability Group

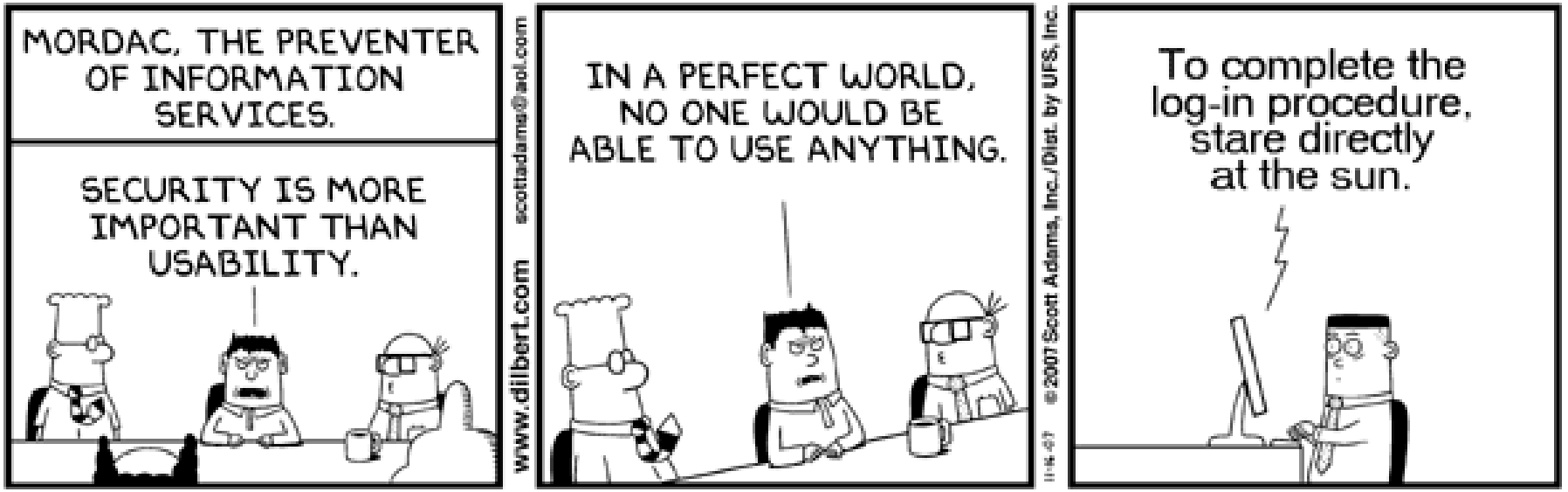
Poor Usability: The Inherent Insider Threat

Mary Theofanos

March 21, 2008



Biometrics and Usability



"Sorry about the odor. I have all my passwords tattooed between my toes."

The weakest link in the chain?

Is it because the User is:

- Careless and Ignorant

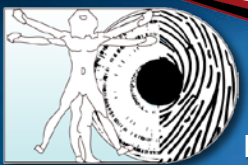
OR

- Frustrated and Overwhelmed

What is usability?

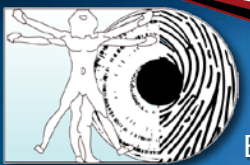
ISO 9241-11 defines usability as:

"the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"



First Tenet: Know thy User

- Policy Makers
- Security Organization
- End-Users



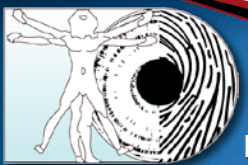
User goals and mission are not similar

End-User

- Task oriented – production tasks vs supporting tasks
- Performance metric: efficiency, effectiveness of production tasks
- The organization's mission relies on the production tasks

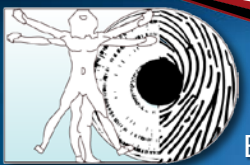
Security Organization

- Security is the production task
- Performance metric: how secure
- Mission is Security but how does it relate to overall mission of the larger organization



User Perception Influences Behavior

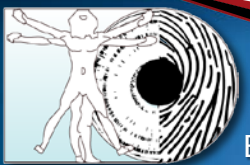
- Impossible demands
- Need --Value
- Complexity
- Awkward Behavior



Context of Use

Differences in physical location and devices influence usage

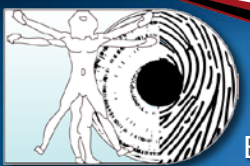
- Laptop
- Desktop
- Office, Home, Airport, Battlefield



Today's usability is one-sided

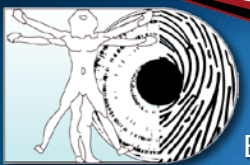
In favor of the Security Organization

- "Command and Control" approach
- Policies constructed top-down, enforced through sanctions
- Compliance monitored by checklists
- One size fits all



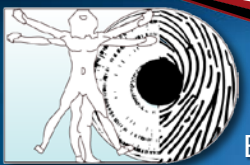
What can we do?

- Integrate Security and Usability
- Include usability in software development cycle
- Apply user-centered design to security design
- Establish a partnership with users



Good Usability Strengthens Security

- Easier to implement security policies, processes and procedures
- Encourages users to follow good security practices
- Reduces users inadvertently undermining security



- The goal is to build systems that are actually secure not theoretically secure:

- Security Mechanisms have to be usable in order to be effective