Moving User-Centered Security from Grand Challenge to Standards Work

http://www.w3.org/2006/WSC/

Lotus software

Mary Ellen Zurko
IBM Software Group
W3C WSC WG Chair
mzurko@us.ibm.com

User-Centered Security is a Grand Challenge

- Psychological Acceptability - Saltzer and Schroeder, “The Protection of Information in Computer Systems”, **1975**
  - “It is essential that the human interface be designed for ease of use, so that users **routinely** and **automatically apply** the protection mechanisms **correctly**. Also, to the extent that the user’s **mental image** of his **protection goals** matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors.”
- **User-Centered Security** - Zurko and Simon, “User-Centered Security”, **1992**
  - “**security** models, mechanisms, systems, and software that have **usability** as a primary motivation or **goal**”
- **Grand Challenges** in Information Security & Assurance - Computing Research Association, **2003**
  - “Give end-users **security** controls they can **understand** and **privacy** they can **control** for the dynamic, pervasive computing environments of the future.”

User-Centered Security Opportunities

I. Human and Social Relationship to Security
   I. **What is the best we can hope for when we ask humans to understand a quality of the system so complex that it cannot be understood by any single architect, developer, or administrator?**
   II. Since humans are part of the system and the system's security, how much responsibility should be assigned to them?
   III. Since usable security is so obviously a universally desirable attribute, why aren't we applying resources to it commensurate with its desirability?

II. Technical Challenges Best Attacked With Research
   I. How can we incorporate models of user behavior into models of security, so that real user behavior is taken into account?
   II. How do we design systems so that security related decisions and actions are minimized, and always made by the person who has the ability to make them?
   III. **How do we design systems so that all the parts that determine the user's ability to interact with them securely are actually secured?**

III. Further difficulties with implementation and deployment
   I. How can we integrate the lessons from practice into our research thinking so that we achieve usable security in practice?
   II. **How can we specify and implement reusable security components that support a user-centered security model in the system they're integrated into?**

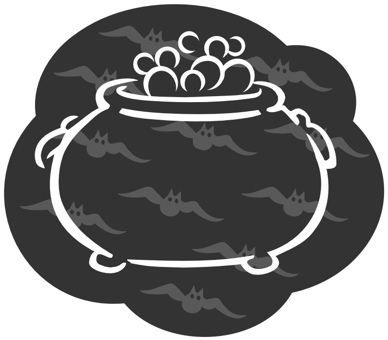
Understanding vs. Effectively Using Security Controls

- If we go on explaining, we shall cease to understand one another.
  - Talleyrand

- User Risk Management
  1. What could go wrong?
  2. How likely is it, and what damage would it cause to me or to others if it did?
  3. How would I know if something went wrong?
  4. What reason do I have to believe that it won't?
  5. Who is responsible to ensure that it doesn't, and what recourse do I have if it does?

- Give all users (including developers, administrators, and end-users) **security** controls that **protect** them, their systems, and their privacy, that they can **use** appropriately in the dynamic, pervasive computing environments of the present and the future.
  - Users must understand the risks, not the security controls
  - Users must be able to use the security controls to manage the risks

Assurance For the User



- But yet I'll make assurance double sure
  - Macbeth, Act IV, scene i
- Users make trust and security decisions based on all the information available to them
  - Including how professional the UI design is
- Traditional security assurance is pared down to the smallest possible code scope
  - Reference Monitor - compact
  - Security policy – formal and provable
- Encryption alone will not make a system secure
- If we're asking the user to make security decisions, the whole UI is part of the computing base that needs to be robust against attack and understandable

Components Contributing to Usable Security

- With these kinds of proposals, the devil is in the details
  - John B. Larson
- Reuse is good for security and it's good for usability
  - Concentrates security knowledge and functionality
  - Makes security more homogeneous and predictable
- Reuse is bad for usable security
  - Error cases are stripped of their context and relationship to users
- SSL/JSSE in a rich client example
  - User action no longer transparently tied to SSL operation
  - Should I care that the server certificate's validity time period has not begun?
- User or system actions to avoid or recover from security related errors need to be part of reuse contract or interface of the component

Current State of User-Centered Security

- Advice on process and application of process or principles
- Applying Human Computer Interaction techniques to security functionality
  - HCI expert evaluations of security functions
  - Usability testing in the lab and in context
- Principles of Usably Secure Systems
  - Safe staging
  - Evaluate risks of usability failures
  - Integrate security into user tasks
  - Security transparency within the task
  - Reliance on trustworthy authority
- Authentication and passwords much studied
- Phishing drawing a lot of attention
  - W3C Web Security Context Working Group

W3C Web Security Context Working Group
http://www.w3.org/2006/WSC/

- First known standards effort in usable security
- Secure and usable presentation of security context information to enable users to make better trust decisions on the web
  - Using the existing web infrastructure
- Aimed at attacks that involve impersonation of web site/server/service and some user action (e.g. phishing)
- Areas under discussion for recommendations include:
  - Banishing useless and confusing errors
  - Presenting security context information robustly (so it cannot be changed or emulated by web content)
  - Useful and usable identification of web sites
    - Particularly of web sites you've visited before
    - And sent information to before
  - Guidance to web application developers and deployers
  - Tighter security constraints during high risk browsing behavior

Thank You

mzurko@us.ibm.com
http://www.w3.org/2006/WSC/

Lotus software