

Usability, Security and Privacy of Computer Systems: Workshop

Breakout Session:

How do we measure Usable
Security?

Session Leads:

Frank L. Greitzer

Charles P. Pfleeger

How to Measure Usable Security?

- How do we define security?
- How do we define usability?
- Can we separately study security and usability? *[Session leads think this is NOT advisable]*
- How “perfect” does the security have to be, before considering usability?
- Are usability and security always opposing forces?
- How does privacy interact with usability and security? *[can envision a set of experiments that could be done...]*
- What are usability criteria? [System/User Tasks/Goals inform SYSTEM REQUIREMENTS – what are the most critical requirements?] (criteria for accepting a usable/security system)
- What process should be used to narrow the criteria?

How to Measure Usable Security?

- How do we define context for a security/usability decision?
- What research gets us a checklist? [are we suggesting development of guidelines/standards?]
- How can we design systems such that the most secure method of use is also the easiest to use?
- Cost benefit analysis needs more research to be easy to use!
- Can we define a set of metrics for applications that will yield an 80% solution? (80/20 rule)
- What example applications do we pick as benchmarks for security and usability?
- How do we break apart categories of common interest / security domains within which we can use the same weighting approach such that you can get to an easy checklist for risk-based, cost-based decisions?

How to Measure Usable Security?

- Which requirements/metrics are most relevant to the federal government?
- Which specific metrics do we want to pose first?
- What are the most common domains for perspective that we should examine: i.e., sysadmin, security professional, system owners, end users, security designers, programmers, etc.?

Variables to Study (preliminary ideas)...

Usability Measures

- User errors
- Time to set up/modify
- Time to learn/proficiency
- Satisfaction/ratings/preferences
- etc...

Effectiveness (Utility)

Measures

- Actual level of protection
- Performance of system in simulated scenario?

Independent Variables: Security Method/Scheme etc.

Privacy Level

Dependent Variables: Usability, Utility

Security Variables to Study

- Method (a, b, c, ...)
- Context (authentication, ...)
- Degree of user control
- ???

