Defining a Usable Security Standard

Butler Lampson

Defining a Usable Security Standard

- How do we define trust? How does a user know they can trust what they see? Trust they are communicating with the person/group/organization they think they are talking to?
- How do people perceive risk? What does risk mean? Risk of exposure to private information, risk of failure?
- How do we elicit the mental models of computer security that users have now? How to determine and deploy better models? What abstractions are needed to improve usability?
- Assume worse case scenarios (users will make errors, systems be compromised); what kind of system should we build?
- Where is the money in usable security? How can the business model be adjusted to make usable security profitable?
- How to use machine learning from context to come up with security policy for a user without asking questions?

Defining a Usable Security Standard

- How to identify a good “green” machine or a bad “red” one?
- Epidemiological perspective –How many individual users with good security would it take to make a noticeable impact in improving security for the masses (by reducing botnets)?
- What are the “physics of security”? Is there a model with the concreteness and usefulness of the desktop / folder scheme?
- How can a user specify what is attributed to him and what should be anonymous?
- Is a system feasible where the user establishes policy by specifying desired outcomes and the system checks for consistency and completeness?
- What are the security, usability and usefulness of whitelisting vs. blacklisting approaches?