Usable Privacy and Security Breakout Session Notes

- Relatively new area of research
  - SOUPS conference now in its 4th year
  - Increasing number of usable privacy and security papers at CHI and
    security conferences

- Evaluation is difficult
  - How do you "prove" something is usable?
  - It is hard to convince security reviewers without a proof
  - Usability studies are time consuming and expensive (especially if
    you study people other than CS students
  - Security researchers don't know how to do them
  - Difficult to study security and usability without the experiment
    itself impacting results - you can't tell subjects you are
    studying security
  - We need metrics for security and usability

- We need standards for getting credit for this work

- Need to understand what people think
  - Not just what they do, but also their cognitive models
  - Learn from other fields: warnings science, safety systems,
    aeronautics
  - But, usable security is different because usable security has to
    account for attackers
  - Usable security often involves trade offs between security or
    privacy and usability/utility

- Need to build usability in from the beginning, don't retrofit later
  - Security/crypto people are not usability experts -- need
    partnerships and collaboration

- Are there market incentives for companies to make security more
  usable?

- Many interesting and difficult research problems in this area
  - Making privacy implications visible to users and communicating
    about privacy in a way that is not annoying
  - Usable configuration for end users and system administrators
  - And many more....

Lorrie Faith Cranor • lorrie@cmu.edu • http://lorrie.cranor.org/ Associate Professor,
Computer Science and Engineering & Public Policy CMU Usable Privacy and Security
Laboratory • http://cups.cs.cmu.edu/ Carnegie Mellon University, 5000 Forbes Ave.,
Pittsburgh, PA 15213