

SECuR-IT Talk: Human-Centric Security

**Jennifer King, MIMS
Samuelson Law, Technology &
Public Policy Clinic
UC Berkeley**



Overview

- What is human-centric security?
- Why should you care?
- Three areas of concentration



My background

- Master's degree in information science, undergrad in sociology and political science
- Product Manager for 7 years, including at a Very Large Internet Company
- Developed expertise in online communities, deviant online behavior



Relevance

- Why care about the human side of security?
 - Your attackers are human (or at least they wrote the code), understanding their motivations, cultural orientation
 - If your work/product/etc. will be used by other humans, will they understand it? (mental models)
 - Understanding human weaknesses can inform your security models (and threat modeling)



Human Attackers

- Some points to consider:
 - Typically, there are only a few of you, and 100s/1000s/millions of them
 - Anything you release to the public will be scrutinized in far more detail than your QA team (if you even have one) ever will
 - Your users are often smarter than you
 - They will use your product in ways you will never imagine (often for illegal activities)



Human Attackers Cont'd

- There are people (young & old) around the world (sometimes paid by organized crime) to do nothing but look for security vulnerabilities in your code
- Organized crime may build a business on the back of whatever service you offer (botnets, p0rn)
- Difficulty: often these problems occur in private industry, and thus little public discussion
 - Click fraud, auction fraud



Usable Security

- Growing area of research
- Predicated on the assumption that if users can't understand the how and the why, it will be impossible to either get them to use something or to use it correctly
 - “Why Johnny Can’t Encrypt” - Whitten & Tygar
 - Usability evaluation of PGP 5.0
 - Task: have crypto novices encrypt an email message
 - Given 90 minutes, majority failed; interface design flaws primary issue



Definition:

- From Whitten & Tygar:
 - Security software is usable if the people who are expected to use it:
 - Are reliably made aware of the security tasks they need to perform
 - Are able to figure out how to successfully perform those tasks
 - Don't make dangerous errors
 - Are sufficiently comfortable with the interface to continue using it
 - Security is almost never a user's primary goal!



Usable Security: Phishing

- Phishing is becoming a classic example
 - Takes advantage of:
 - Lack of understanding/mental models of fundamentals of web technology
 - Issues with displaying secure connections in browser UI
 - Proclivity of users to click on links (foundation of the Web!)
 - Password management
 - Fear!
- Technological solutions exist - but can they ever “solve” the problem?



Human Weaknesses

- Humans are often the cause of security errors . . . and secure systems are only as strong as the weakest link!
- Social engineering
- Stolen laptops (usually w/unencrypted data!)
- Inability to manage multiple passwords
- Insider threats
- Lack of clear policies & procedures



Weaknesses cont'd

- Replacing human decision-making w/technology is not always a feasible or desirable decision
- Solutions need to be respectful, maintain dignity
 - Retail worker theft measures



Reading List

- *Security Engineering: A Guide to Building Dependable Distributed Systems*, Ross Anderson
- *Security & Usability: Designing Secure Systems That People Can Use*, Lorrie Cranor & Simson Garfinkel

