ISPAB Panel on Usable Security

Mary Frances Theofanos - NIST
Ellen Cram Kowalczyk - Microsoft
What is Usable Security?

• Usable Security is more than a well designed interface
• It is taking into account that the user is often the most important part of a security solution
  – Set a strong password and keep it secret
  – Keep smartcards in a secure place
  – Don’t download suspicious files
  – Update your system (or don’t turn off updating)
  – Don’t put unknown thumb drives, disks, etc. into your machine
Consequences of Security Solutions that are not usable include:

- People not working in the evening because smartcard/token left in car
- Passwords: different rules, expected to use unique passwords yet not able to write them down.
- BitLocker is more secure with PIN, but had to back down as to difficult for users. Some organizations backed out of BitLocker all together due to usability/support concerns.
- Didn’t consider issues with Virtual machines when requiring screensavers, and many users opted out.
- Policies around erasing mobile phones after a small number of access attempts lead to longer locking windows and easier passwords.
Usable Security Requires that we examine many human factors

• Cognitive and memory limitations
• Behavioral factors (not productive task)
• Incentives/Disincentives (think like an economist--externalities)
• Education versus Training
• A well designed user interface
  -- make it easy to do the right thing, hard to do the wrong thing and easy to recover when the wrong thing happens anyway
Current NIST Usable Security Work

• Policy makers often have very little usability data when they make security policy.
• NIST goal: Try to provide usability data in conjunction with the security data to policy makers so that they can make an informed policy decision.
  – Passwords: survey of federal employees on password usage
    • Average number of passwords
    • How they mange their passwords
    • What is the risk of password compromise
    • Do you know your password policy
  – Password policy research – developed a taxonomy of password policies
  – PIV card pilot
    • How do you transition from password to card and pin use,
    • What are the implications, what does this mean to user behavior, user acceptance, productivity,
Current NIST Usable Security Work

• Mental Models: survey of users perceptions of risk and awareness of cyber security – and threat models.
• Software Development Models that map user centered design process and security process models together.
Current MSFT Usable Security Work

• Usable Security in Products
  – Smart Screen in IE: Constantly tuning to keep users from hurting themselves
  – Office: intelligence around whether a user trusts a file
• Usable Security Research
  – Access control
  – Warnings
  – Secondary authentication
  – Identity Models
  – Quantified User Harm Metrics
• Usable Security Guidance
  – Guidance for warnings and prods focused on:
    • Architecting so you can avoid asking the user
    • Providing clear explanations and testing them
  – Starting work on UX Convention guidance
    • Icons, calling out verified vs. unverified data
Usable Security Challenges

• Beginning process of moving from assumptions and anecdotes on bad security usability to concrete data
  – Pockets of data on specific user bases, but significant variance and only partial coverage
• Easy to spot issues, often don’t have a good solution
  – Often what’s in place is the best known solution, but has major drawbacks
• Spoofing is very difficult to solve
  – Very little that a genuine product or solution can do that the attacker can’t
  – User’s aren’t focused on spotting the counterfeit, they want to get their job done
• Fundamentally, users will work around anything necessary to get their job done
  – Usable security has to get them to where they need to go, not just block unsafe actions.
Research Needs

• User’s Security Mental Model
  – Need a better understanding of how users perceive online security, and why they make the decisions they do.

• Quantified User Harm
  – Need quantifiable data about how users are actually getting malware, phished
  – This will provide prioritization of other research/solutions, allow measurement of success over time

• Usable Online Identity
  – Scalable (not 100 unique passwords)
  – Prevention of phishing/ID theft
  – Enablement of scenarios without encouraging over-collection of data

• Spoofing
  – Government and private companies need a way of communicating with people in a way that they can trust
  – Need a way to spot when user is being misdirected, help them find the site they want.

• Distributed Trust Model
  – Having users verify sites isn’t scalable
  – Current certificate model is too open – even malware is often signed, users don’t have relationship with signing companies
  – Need a model that enables users to establish trust with parties who can verify sites in a scalable way.
Security Solutions and Policies
Research

• Consider how a user will use a security solution or policy before putting it into place
  – What is their mental model of what’s going on?
  – What are the reasons the user might try to work around the solution or policy?
  – What can you do in the architecture to make the solution easier for the user?

• Determine ways your solution might be spoofed and address them

• Test security changes and policies on real people before deploying
  • this may require research into finding ways to quickly do research on new policies as they are being formed.

• Fundamentally: Make it easy to do the right thing, hard to the wrong thing and easy to recover when the wrong thing happens anyway.
Next Steps

• Encourage/fund research in usable security
• Ensure usability is considered in security solutions and security policies.

We have evolved from thinking
• “the user is the problem” to
• “technology is the solution” to
• “the user must be part of the solution”

*We can’t meet the cyber-security challenge without usable solutions*