Designing Security Prompts

Slides, courtesy of Rob Reeder, Microsoft Usable Security Team
Users are faced with a lot of challenging trust-related decisions.
An example problem: IE6 mixed context

Vague threat. What’s the risk? What could happen?

“Yes”, the possibly less safe option, is the default

How should the user make this decision? No clear steps for user to follow.
Even better: load the safe content, and use the gold bar to enable the rest
Guidelines

• Philosophy:
  – Does the user have unique knowledge the system doesn’t?
  – Don’t involve user if you don’t have to
  – If you involve the user, enable them to make the right decision

• Make sure your security dialogs are NEAT:
  – **Necessary:** Can the system take action without the user?
    If the user has no unique knowledge, redesign system.
  – **Explained:** see next slides
  – **Actionable:** Can users make good decisions with your UI in both malicious and benign situations?
  – **Tested:** Test your dialog on a few people who haven’t used the system before -- both malicious and benign situations.
Example 1: bad explanation

Most users will not understand “revocation information”. Choices are unclear, consequence is unclear.
Better explanation

Source
- There is a problem with this website's security certificate.
- The security certificate presented by this website was not issued by a trusted certificate authority.
- Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

Risk
- We recommend that you close this webpage and do not continue to this website.

Choices
- Click here to close this webpage.
- Continue to this website (not recommended).

Process
- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.
- If you choose to ignore this error and continue, do not enter private information into the website.

For more information, see "Certificate Errors" in Internet Explorer Help.
Example 2: bad explanation

AutoPlay dialog in Vista

Attacker can abuse explanation causing bad user decisions.

Used by Conficker spread through USB drives.
A better design

Windows 7 AutoPlay removed the auto-run option
THE END