10/12/12 - Usable Security and Phishing

Edward K. Lu

October 14, 2012

1 Usable Security

- In Professor Wagner's opinion, the security field needs to hear the gospel of usable security.
- Useful in many different fields. For example, aeronautics.
  - Aeronautic engineers made planes extremely safe, but crashes still happen due to pilot error.
  - The interface was too difficult. Engineers share the blame for this.
  - How do you build simplier interfaces?
- One of compsci's problems is that we fix our own mistakes and think users are just like us. But we differ from them in many ways:
  - More technical experience
  - Predominately male, privileged, etc.
  - Think differently (logically and analytically, like engineers).
  - To show this, we did a survey on the class's Myers-Brigg personality test results.
    - Extrovert: 2 Introvert: 15
    - Sensing: 0 iNtuition: 6
    - Thinking: 14 Feeling: 1
    - Judging: 2 Perceiving: 1
    - Most compsci people are Thinking and Judging (over 50
  - In sum, we have a large cognitive bias.
- Usuable security started with a crypto paper, "Why Johnny Can't Encrypt"
  - Cryptographers were puzzled about encrypted email's lack of adoption. They thought it was very straightforward to use.
  - The paper described a user study that asked users to send sensitive email using encryption with PGP. Results were that the majority couldn't use PGP securely:
    - They didn't know what the difference was between public and private keys. Some sent the private key with the email.
    - Some couldn't use the tool.
    - Some sent the email in the clear.

        * They thought it was too hard and there was too much jargon in the explanations.
    - The paper was an eye opener, showed how different the general public was from cs engineers.

- How can we overcome this cognitive bias?
    - User studies
    - Surveys, feedback, focus groups
    - Work in diverse teams
    - Model/measure complexity
    - Anthropology - adapt program to what users are currently using
    - Make security invisible, automatic, and always on. This is like Skype, who always encrypts calls.
    - Psychology.

2 Phishing

- We have three kinds of behaviors. Knowledge-based, rule-based, and skills.
    - Knowledge-based involves self aware thinking, rational thought, and a long decision process.
    - Rule-based involves reacting according to patterns learned in past experiences.
    - Skills are automatic/subconscious responses, such as riding a bike.
    - Rule-based behaviors are learned. Responses are ranked according to number of successes. This supports habituation. For example, if you keep logging in and get rewarded with access and no bad events, you will be inclined to keep doing so even if its a phishing website.
- One reason why phishing is so effective is that users don't have any idea that they're under attack. When faced with a strange situation that they can't understand, they make up stories to explain it.
- Another reason is that people are optimistic when they compare their own chances with others.
    - A survey asking respondents how good they are at driving showed that 60
    - This is a form of risk acceptance. For example, the Challenger explosion:
        * Engineers thought the risk of explosion was 1 in 50 to 1 in 100.
        * Management thought it was more like 1 in 10^4 to 1 in 10^5.
        * Management was trained in the past to accept the risks that the engineers had told them. "If it worked before under those risks, it'll work again!"
    - You see this in people dismissing browser warnings and Vista UAC prompts.
- It is probably better to have infrequent warnings with high
- Limitations of "Why Phishing Works"'s experimental design and how "You've Been Warned" addresses this:

- Small sample size. Though, this may be okay for exploratory purposes. YBW solves this by recruiting more people.
- Demand effects. This is when subjects know what the purpose of the test is and subconsciously tries to please the researcher. YBW solves this through deception.
- Bias through the environment. The test only used a mac, with firefox, and was done in a lab.
- There may have been an authority figure effect, where subjects would act more obediently in the face of an authoritative figure (in this case, the researcher).
- Sense of risk. Subjects did not feel at risk. There was no money on the line and they were in a "safe" environment. YBW solves this by attacking them through emails and making them spend their own money with their own credit cards.
- Non-representative sample. The test consisted only of students and faculty. YBW solves this by recruiting from the streets, craigslist, etc.

- Today's phishing exploits:
  - Spear phishing:
    - This is a custom phishing attack that is customized to each recipient using information from social networks and other places.
    - U of Indiana tried to do this by sending an email to each student, spoofed to look like it was from a friend. 16
  - Mobile phishing:
    - On mobile devices, a web page can go full screen, without any visible address bar or anything else from the browser. This removes cues from the browser about phishing.
    - A study done in UC Davis tried this attack on experienced cs people. 96