5-899 / 17-500 Usable Privacy and Security
Trust and semantic attacks II

Lecture and notes written by *Ponnurangam K*

Lecture notes, Discussion and Activity

February 23, 2006

1 Topics covered

- Summary of Trust and semantic attacks I
- Semantic Attacks
- Phishing
- User studies
  - Why Phishing Works [2]
  - Do Security Toolbars Actually Prevent Phishing Attacks? [5]
- Summary
- Task

1.1 Summary of Trust and semantic attacks I

- Slides 3 - 4
  - What is trust?
  - Different positive and negative antecedents of trust
  - Discussion
    - Is there any comments, clarifications on the topic of trust modelling?

1.2 Semantic Attacks

- Slides 6 - 8
  - Security attack waves: physical, syntactic and semantic by *Bruce Schneier*[1]
  - Cyber attack sophistication continues to evolve [3, pp. 10]
  - Semantic attack: "... target the way we, as humans, assign meaning to content [1, Chapter 14]"
  - Differences between system model and mental model [4]
  - Discussion
    - What do you think about the classification of security attacks?
    - It would be interesting to have a third dimension with the number of successful attacks in the cyber attack sophistication graph in slide 7. What do you think?
    - What do you think about the difference between system model and mental model?

1.3 Phishing

- Slides 10 - 18
  - One type of semantic attack is phishing
  - An example of phish email from eBay
  - Phishing has many definitions; one of the definition is

    > ...the act of sending a forged e-mail (using a bulk mailer) to a recipient, falsely mimicking a legitimate establishment in an attempt to scam the recipient into divulging private information such as credit card numbers or bank account passwords [3].

  - Phishing is a growing problem
  - Some trends from APWG report[2]
  - One type of classification of phishing attacks [2]:

[1] http://www.schneier.com/essay-035.html
[2] http://apwg.org/reports/apwg_report_DEC2005_FINAL.pdf

    - Lack of knowledge
    - Visual deception
    - Bounded attention
  - Discussion
    - Is there anybody in the class who has not got a phish email?
    - What do you think about the different definitions of phishing?
    - What do you think about the additional losses due to consumer fears?
    - Why are the phishing sites lower for the month of October and November 05 (slide 16)?
    - Even though we think that there is lot of enforcement on removing the fake web sites, we see the average time online for site is 5.3 days and longest time online for site was 31 days. Can anybody think of any reasons?

1.4 User studies

- Why Phishing Works [2], slides 20 - 23
  - Goal: What makes a bogus web site credible?
  - Conclusions: existing browsing cues are ineffective, participants proves vulnerable to phishing attacks, lack of knowledge of web fraud and erroneous security knowledge
  - Suggestions: to understand what humans do well and what they do not do well and help user to distinguish legitimate and spoofed web site
  - Discussion
    - Studies show that people fall for phishing sites when they go to the web site; is it possible to train the users for not going to the web site from the email?
    - One of the suggestions given was ("to understand what humans do well and what they do not do well") was really broad, which is also difficult to achieve. What do you think about it?

- Do Security Toolbars Actually Prevent Phishing Attacks? [5], slides 24 - 32
  - Goal: To evaluate security toolbar approach to fight phishing?
  - Toolbars analyzed:
    * Spoofstick
    * Netcraft
    * Trustbar
    * eBay account guard
    * Spoofguard
  - Classified toolbars into the following:
    * Neutral-information
    * SSL verification
    * System decision
  - Conclusions: spoof scores of all the toolbars are greater than 0 and some toolbars would have better spoof rates than others
  - Suggestions: active interruptions are effective, tutorials are effective, knowing the user's intentions will be effective and user intentions should be respected
  - Discussion
    * What do you think about each tool bars?
    * One idea was to show the URL of the web site spaced out and in bigger fonts to avoid visual deception
    * A brief note on the preliminary study conducted by Lorrie on the different tool bars

1.5 Summary

- Slide 32
  - Phishing is effective
  - Need better user interfaces
  - Need more understanding of users' decision making process
  - Need education and expertise

- Discussion
  - Is there any questions?

1.6 Task

- Slides 34 - 35
  - As Bruce Schneier points out, education among the users about these internet attacks are essential. So the task for today in class is to come up with ideas to train four different groups of people. The groups are classified based on their vulnerability towards these attacks. The definition for vulnerability[3] is

    > susceptibility to injury or attack, for example clicking on the link in the email, giving username and password, etc.

  - The students were grouped into four teams; each team worked on a specific user type. The four user types are:
    1. Geek
    2. Expert
    3. Savvy
    4. Novice
  - Students came up with the following points for each group:
    1. Geek
       - Provision for showing google cached sites with respect to the phish web site
       - Provide a link or a button "to report to Slashdot"
       - Provision for launching application in a different environment
       - Mechanism for rating a web site
    2. Expert
       - Skeptical view toward the problem
       - To provide an easy way to retrieve the paths that the email had taken
       - To provide an useful spelling score for the email

[3] http://dictionary.reference.com/search?q=vulnerability

3. Savvy
    * Highlighting the cues
    * Tool bars to show the score / rating for the web site
4. Novice
    * Highlighting the cues by showing large popups
    * Showing the message "This is bad site! don't go"
    * Making a sound to show that the web site is bad
    * Shake the window or change the color of the window

References

[1] Cranor, L. F., and Garfinkel, S. *Security and Usability: Designing Secure Systems that People Can Use.* O'Reilly., Aug, 2005.

[2] Dhamija, R., Tygar, J. D., and Hearst, M. Why Phishing Works. *To appear in the Proceedings of the Conference on Human Factors in Computing Systems (CHI2006), 2006* (2006). Retrieved Feb 10, 2006, http://www.sims.berkeley.edu/ rachna/papers/why_phishing_works.pdf.

[3] James, L. *Phishing Exposed.* Syngress, November 10, 2005.

[4] Wu, M. *Fighting Phishing at the User Interface.* PhD thesis, MIT, 2004. Retrieved Feb 10, 2006, http://groups.csail.mit.edu/uid/projects/phishing/proposal.pdf.

[5] Wu, M., Miller, R. C., and Garfinkel, S. L. Do Security Toolbars Actually Prevent Phishing Attacks? *To appear in the Conference on Human Factors in Computing Systems (CHI 2006)* (2006). Retrieved Feb 10, 2006, http://www.simson.net/ref/2006/CHI-security-toolbar-final.pdf.