Usability aspect of security

October 30, 2008. (Thursday)

Scriber: Yamini Kannan

This lecture is about a different side of security – the usability side of security – how do you ascertain that the technology being developed to increase web security reaches the people.

One important caveat to keep in mind, while designing security measures, is to remember that "you" are not the typical user. Specifically, the population of computer geeks is very different from the general population. For example, there is a higher proportion of male, the average financial standing is higher etc. This is corroborated by an interesting statistic from the results of Myers-Briggs type indicator. An overwhelming majority of the computer scientists have a score of __TJ, while only 8% of all population falls in this category.

Psychologist's perception:

It is important to understand the decision making process of the human mind in order to design good strategy for security. Typically, a good enough decision made within a short time is better than an optimal one that takes much more time.

Types of decision making process:

1) Knowledge-based reasoning – conscious deliberate thought is involved in making the decision. One weighs the different alternatives before taking the decision.
2) Rule based reasoning – the mind develops a series of patterns based on past situations and maintains the actions that were successful in those situations.

   It then uses "pattern matching" to identify situations from the past that are similar to the current one, and takes the decision to perform the action that was taken in those situations.

   ```
   If (rule_1) then action_1
   If (rule_2) then action_2
   ...
   ```

   This kind of reasoning is exploited by attacks such as clickware, where the site exploits the fact that the user is conditioned to click 'ok' when a message box is presented, without really thinking about what the click leads to.

   Such rule-based thinking process is also susceptible to phishing attacks. For example, users are conditioned to enter information such as login and password, if text boxes for the same are provided.
3) Satisficing attitude – sometimes the decision is made by trying a few things till one stumbles onto something that seems to work reasonably well. This is also susceptible to phishing attacks – user might end up at a fake site, while trying a number of avenues to reach the intended site.

Strategies:

- "Don't shop when you are hungry". Security strategies should not interfere with the user's main task. For example, a security message box displayed in the middle of a task is not very effective, since users have the tendency to dismiss it as a distraction.
- One should remember that users are not good at identifying attacks.

Possible Solutions:

- Better web authentication. Use browser mechanisms to enforce better authentication.
- Keep the user ignorant of the secret authentication key. The user is a weak link since he / she can be deceived. Hence, instead of asking the user to enter the secret information for authentication, the site can use a cookie to store the information. Some banking sites use persistent cookies that are stored on the machine after the first access.
    - The problem with this approach is that there is a need for bootstrapping. The initial step of setting up this persistent cookie becomes the weak link. How to protect the user when he/she is accessing the site for the first time?
    - Solution 1 – Most banks use a challenge-response model to bootstrap.
        - However, this is susceptible to man-in-the-middle attack. An attacker can take the password from the user, send it to the bank, and redirect the challenge question from the bank back to the user.
        - Or a phishing site can present the user with a drop box with all possible questions, telling the user to choose the right question and enter the corresponding response.
    - Solution 2 – Use email as a secure channel.
        - Problem: the e-mail account can be phished or the email can be intercepted in some way. Hence, the protected site is only as secure as the email site.
        - Or one can think of phishing sites which now proceed to fool the user into forwarding the mail sent by the bank to the attacker, under pretext of asking for information for debugging purposes.
    - Solution 3 – Use 2-factor authentication – have a separate secure channel like phone / snail mail to exchange initial secret key
- One common strategy used by banks is to use some kind of transaction code and ask for confirmation for important user transactions
    - Problem: Susceptible to man-in-the-middle attack. Attacker can intercept the user's request and change information before sending to bank. Here since the user is expecting a confirmation request from the bank, he / she doesn't notice anything suspicious
    - Fix: Include more information in the confirmation message – give full details about the transaction. And use a secure channel for sending the confirmation message

Another aspect that is important in developing security strategies is conducting usability studies and deciding what experimental methodologies should be employed to evaluate the effectiveness of your

security strategy. There were a number of issues with the experimental section for the paper (Why Phishing Works). The following section discusses the shortcomings of this section in the paper and the issues in conducting usability studies in general:

- Small sample size: this is a tough problem to tackle since user studies is very time intensive process.
- The paper does not perform any statistical analysis of their findings
- User studies are usually not conducted in their natural environment. So the tests are not really a reflection of the real-world user behavior.
    - In the paper, the users knew that they were looking for attacks. This is not their normal browsing attitude. Even though this results in an artificial situation, it was not an issue in this paper, since the result obtained was negative. That is, in spite of the users being extra vigilant, it was still difficult to distinguish the fake sites from the real ones.
    - In the usability study in the paper, the users were not at any real risk. So they might not have been very serious in identifying the attack. They knew their money and identity was not at stake.
- Presence of authoritative figure: experiments were conducted in the presence of the developers. The user looks up to the developer in this case and tends to give very high weight to what they say. This creates some bias and adds to the lack of normalcy to the situation.
- Demand effects: the user tries to guess what the experimenter is looking for, and tries to provide that result to please the experimenter
    - Fix: use placebo to negate this effect. Might be difficult to design placebo for phishing attack studies
- The paper only talks about half of the phishing problem. It does not talk about how to get the user to go the fake site. It lacks a good simulation of the attack – it takes the user directly to the fake site.

One solution adopted to deal with the artificial effects of the test environment is to employ deception. For example, the user is given a false idea about the goal of the study and the amount / type of information collected. In this case, the user has to be informed of the real goal once the test is concluded. In case the user is no longer willing to be part of the study, the data that was collected from that user should be discarded. However, there are ethical issues in doing this and one has to be really careful to not get into trouble.