October 31, 2011
Usable Security, Part1

Wontae Choi

November 15, 2011

1 Introduction

You may think that cryptographic protocols solve security problems, if it can be applied. It is not true. You might forget an important actor in security problems. Users. Users make seemingly horrible decisions. For example, they send both private and public key through email. Such user interactions nullify assumptions on which security protocols depend. Thus, to give users a guideline is as important as to investigate secure protocols in theory.

How to prevent user mistakes (Discussed)

1. Give them a simple one button solution. Never give them freedom to mischosse insecure options.
2. Show them how security experts do repeatedly. (kind of pair programming)
3. Use test cases resembling behavior of novice users.

How to prevent(Categorized) All approaches proposed above can be categorized into three item. (Small items are examples)

1. Pre-design Approaches
   (a) Psychological Analysis
   (b) Antrhopological Analysis
   (c) Talk to users
2. Design Approaches: Iterative redisgin by user
   (a) eXtream Programming
   (b) Paper Prototyping
3. Post-design Approaches
   (a) User Study

The Common Mistake Above all, developers are a bad user sample. To list few reasons, developers are highly educated and they tend to think analytically. These are not the case for majority or users. Developers are, indeed, extreme values in user distribution. [1]

2 Psychological Aspect of Security

2.1 Three modes of making decisions

Skill Sometimes, people acts without thinking, because the action is almost hard programmed in their nerves. This category includes walking and breathing.

Knowledge Based Reasoning On the contrary, some decisions require explicit deep reasoning using knowledge. Intellectual labors, for example, mathematical proving, are in this group.

Rule Based Reasoning Finally, there are reactions that are half automatic. According to psycholocial study, people maintain rules in brain, each are fetched at different contexts. A reaction is determiend by a fetched rule. So called habits can in this category.

This category is important for security's perspective, because many user behaviors, for example, how to react to an error message, are in this category.

According to psychological study, rules are evaluated based on frequency rather then adequacy. This gives two clues to understand user behavior.

1. Among entire web pages, malicious pages are just a tiny fraction. Thus, a rule to allow to click buttons on a webpage will be applied frequently, while a rule to suspect web pages will not.

2. If a browser generates too much false warnings, a rule to ignore warnings will be enforced. This phenomenon is called *habituation*. To fight against habituation, browsers should suppress false warnings. Also, browsers can refresh appearance of warnings periodically: a rule for ignoring warnings with an old appearance might not be triggered by warnings with a new appearance.

2.1.1 Decision Making Strategy

Satisficing Physiological study has also revealed that even knowledge based reasoning of human being is not reasonable enough. Our brain tries to find a good enough solution as fast as possible, instead of the optimal solution. This decision making strategy is called *Satisficing*. [2]

Implication on Security For users, security is not the primary concern. Their concern is to finish a main task effectively. They will consider both being insecure and timespending to be secure as an expense. Between perfectly secure system and easily usable and partial secure system, users might chose the second option, because it is easy and, at least, partially secure. From the security point of view, however partially secure system is, actually, insecure at all. Thus, a design of securiry products should aim simplicity and ease of use from the begining.

[1] According to the study conducted by Myers and Briggs, most programmers in Unitest States have INTJ personality, while only 2 percents of entire US population have that personality.

[2] The strategy aiming the optimal solution is called *Rational* decision making

2.2 Users have no domain specific knowledge

Users do understand something is wrong, when they face browser warnings. However, they don't understand what is wrong and how to react. In most cases, users might simply guess that internet connection is a problem.

User friendly design No one can be an expert of every subjects. We cannot teach users about security domain knowledge. In stead, we should design security related products considering that users have no domain knowledge from the very beginning.

3 Phishing

3.1 Black list vs white list

Current de-facto standard guard against phishing attacks is black list. White list approach is not suitable: At first, a user visit an enormous number of different web pages. Among those web pages, malicious web pages are only a tiny fraction. The second problem is that there must be unavoidable time gap between new safe web page creation and white list update. These implies, white list based phishing prevention techniques are doomed to generate tons of false warnings.

3.2 Security Indicators

Some web browsers use a special icon to show that a current web page is safe from phishing attacks. However, this approach is not effective. A malicious web page might render a fake browser with in a browser window and locate special security icon on the place. If a browser is in full screen mode, people may think that browser become window mode somehow and will keep browsing through a mallicious web page.

4 How to do good survey on Phishing

Representative sample Survey of "*Why Phishing Works*" paper has two problems. The first problem is that their sample group is too small. The second, more important, problem is that their sample group is from biased population: All samples are an university student. It is good to avoid biased population or sample, though additional statistical treatment might help this case.

Representative behavior Beware of observational effect. At first, inherently, people want to please each other: Attendances might lie to satisfy experimenters. The second, people are prone to be affected by authority of experimenters: Try hard to avoid to be authoritative. The third, people may believe that experimenters will not do any harm. This affect behavior of attendances significantly. Thus, experimenter have to fake attendance without causing any ethical problem.