APPLICATION FOR APPROVAL TO USE HUMANS AS EXPERIMENTAL SUBJECTS

1. Title of Study:

Anti-PhAshing

2. Purpose of Study:

PhAshing [fæʃing] refers to the attack of faked application through web browsers. The approach of counter measures against PhAshing is Anti-PhAshing.

Phishers are always trying their best to make the faked web pages look and behave as similar as possible to the real web pages. As the web browsers are adding more and more features (Java Script, ActiveX, Java Applet, Macromedia Flash, etc.), plug-ins (Adobe Acrobat, Google Toolbar, MSN Toolbar, OICQ, etc.), these features and applications are making web browsers "too" powerful that their UI is no just limited to the client windows in web browsers any more. Hence local applications, including the anti-phishing applications can be faked. A video at http://www.mit.edu/~ayf/my_free_sw/activeXAttack.zip demonstrates how ActiveX can take control the entire computer screen.

In this investigation, we use Web Wallet (an anti-phishing sidebar, www.mit.edu/~minwu) as an example to propose improved UI designs. We plan to use the following counter measures in the user study.

Control Study:
We provide control study UI, as shown in Figure 1, to make the other UI *anti-phAshing* improvements comparable. The difference from original *Web Wallet* design is that we use isolated window rather than embedding it into IE.

Application Trace:
We want to redesign a visual indicator, *Application Trace*. To testify one visual area is real, we have to set somewhere in the screen that cannot be faked. We tried to put the indicator as an icon in taskbar. However we found it is not secure, because the taskbar can be faked. Hence, we propose to put the visual indicator at a fixed physical area on the computer screen, e.g., at one of the four corners/sides of the screen, as shown in Figure 2.

Genuine Skin:
Genuine Skin is a method that can mitigate the difficulty of automatic *PhAshing* detection. There are several guidelines to design *Genuine Skin*, (a) *Genuine Skin Patter* is like trade mark, it is identical for a certain company, and a series of products of this company can use the same *Genuine Skin*. We consider it as illegal to use the images identical or similar to the *Genuine Skin* belongs to one company without authentication. (b) There's one *Anti- PhAshing* engine running in the client side to detect similar patterns to the *Genuine Skin Pattern* which are not in the known positions. (c) The design of *Genuine Skin Patterns* should be both easily recognizable by both human eyes and computers. We need to train the *Anti-PhAshing* engine to simulate the average human classification curve, such that we can reduce the numbers of both false positive and false negative. Good design of *Genuine Skin* can help reduce the false cases. Figure 3 shows two examples of *Genuine Skin* pattern designs for *Web Wallet*. (d) The suspected area will be circled and alert will given out if found, as shown in Figure 4. If the faked *Web Wallet* doesn't have *Genuine Skin*, then users will not tend to believe it is real, as shown in Figure 5.

Merged Approach:
The Anti-PhAshing task is difficult and there's no single tool can prevent users from PhAshing attacks at 100%. We have a hypothesis that if we use more anti-phishing techniques, we can gain more security. Hence, we would like to integrate Application Trace and Genuine Skin to carry out one user study to learn the effectiveness, as shown in Figure 6.

Figure 1 The Control Study UI

Figure 2 Application Trace Prototype

(a) Example 1

(b) Example 2

Figure 3 Genuine Skin Patter Examples

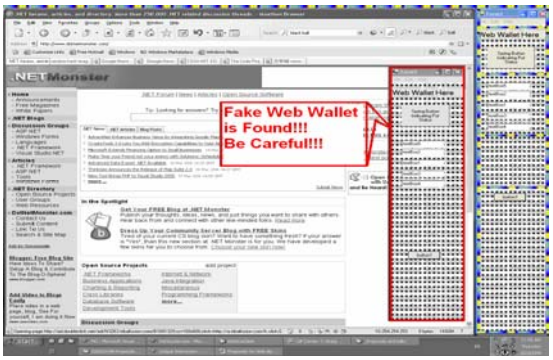

Figure 4 Anti-PhAshing engine found suspected pattern and gives out alert.

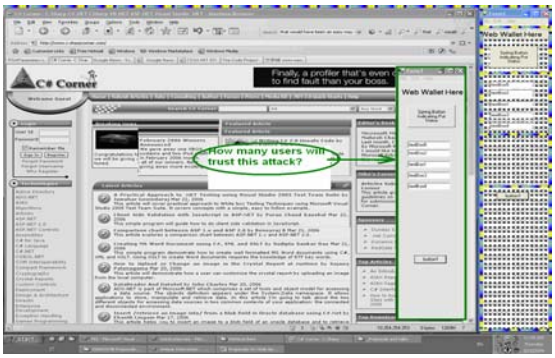

Figure 5 Users can easily recognize the faked Web Wallet

Figure 6 Prototype for merged anti-phAshing approach

3. Study Protocol:

We will recruit 4 groups of users. Each group contains 10 users to test one of the four types of methods (Control Study, Application Trace, Genuine Skin, and Merged Approach). We will design 10 "yes/no" questions for each user to answer whether the currently given Web Wallet is trustable. For each group, we will design 3 or 4 phishing attacks.

Subjects

4. Estimated Number of Subjects:

40 (10 for each method)

5. Estimated Age of Subjects:

6-80

6. Criteria for inclusion/exclusion of subjects:

7. Recruitment: *Identification and recruitment of subjects must be ethically and legally acceptable and free of coercion. Describe below what methods will be used to identify and recruit subjects:*

8. Compensation:

9. Potential Risks: *A risk is a potential harm that a reasonable person would consider important in deciding whether to participate in research. Risks can be categorized as physical, psychological, sociological, economic and legal, and include pain, stress, invasion of privacy, embarrassment or exposure to sensitive or confidential data. All potential risks and discomforts must be minimized to the greatest extent possible by using e.g. appropriate monitoring, safety devices and withdrawal of a subject if there is evidence of a specific adverse event:*

What are the potential risks/discomforts associated with each intervention or procedure in the study:

What procedures will be in place to prevent/minimize potential risks or discomfort:

10. Potential Benefits.

What potential benefits may subjects receive from participating in the study?

What potential benefits can society expect from the study?

*Complete version of the proposal is available at
www.mit.edu/~ayf/publication/US%20Proposal%20double%20columns.pdf