Presentation Florian Müller

Keyword Based Security Awareness Warnings for Websites

LFE Media Informatics – Project Thesis
Tutor: Dipl.-Medieninf. Max-Emanuel Maurer
06.07.2010
1. Description of the topic

2. Related Work

3. Implementation of the Browser Plugin

4. Study – Design and Preparation

5. Results of the Study
Description of the Topic
General:

- Today's Browser often try to protect their uses with static indicators
- This technique causes a large number of false alarms
  - so the Users attention get lost

Task:

- Users should be warned in case they enter critical Data
- Browser should make this input more prominent
- Browser should provide additional help trusting a Website
Related Work
Keyword Based Security Awareness

- Basic URL Obfuscation (Use of JPEG Images, HTML Redirection)
- Use of alternate encoding schemes
  » J. Milletary et al. [1]
- A good Phishing Website can fool more than 90% of the Participants
  » R. Dhamija et al. [2]
- Lock icon is often looked, but there is only few interaction with it
- Even experienced web users do not take any notice of the cues
- People tend to stop looking for security information after signing into a site
  » T. Whalen et al. [3]
Keyword Based Security Awareness

- failed to prevent users from being spoofed by fraudulent websites
  - M. Wu et al. [4]
Implementation of the Browser Plugin
Plugin was developed for Mozilla Firefox

Used programming languages:

- XUL: XML User Interface Language
- Javascript (adjusted for XUL)

Used programming environment:

- Normal text editor
- Netbeans IDE 6.5.1
Functionality:

- The plugin searches for inputs within the website and save them in an array.
- If a Key is pressed the Plugin look for the inputfield in which is currently written.
- If it detects one of the following critical Inputs, it generates the Warning:
  - Entry of a Password
  - Entry of Transaction Numbers
  - Entry of Creditcardnumbers
Online-Banking: Anmelden

VORSICHT!
Diese Eingabe könnte gestohlen werden:

TAN
Domainname: www.bankingportal.sparkasse.de
Die Daten werden bei der Übertragung NICHT verschlüsselt!
Keyword Based Security Awareness

VORSICHT!
Diese Eingabe könnte gestohlen werden:

Kreditkartennummer

Domainname: webmail.ifi.lmu.de
Die Daten werden bei der Übertragung verschlüsselt.

Vertrauen

VORSICHT!
Diese Eingabe könnte gestohlen werden:

Passwort

Domainname: webmail.ifi.lmu.de
Die Daten werden bei der Übertragung verschlüsselt.

Vertrauen
Study – Design and Preparation
Design:

- Two Groups having each 12 participants
- Independent Variable: with Plugin/without Plugin
- Using a 6x6 Latin Square to shuffle the experiment's order
- All Participants should be computer/internet affine
- The participants should not know the real goals of the Study
- Real Goal: Can the Plugin support the Participants to recognize fraudulent Websites
- Qualitative questionnaire at the End of the Study

Hypothesis:

- The group with the Plugin is able to recognize more fraudulent Websites than the group without the Plugin.
Keyword Based Security Awareness

Verhalten im Internet

Presentation Florian Müller

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
Keyword Based Security Awareness
Results of the Study
Main Findings:

- With Plugin: 20 of 36 fraudulent Websites were found -> 55.55%
- Without Plugin: 5 of 36 fraudulent Websites were found -> 13.89%
- The statistical Significance was considered by an independent T-Test
- The Effect Size amounts $r = .62$ which implies a large effect

Proved Hypothesis:

- On average, the group with the Plugin is able to recognize (very) significantly more fraudulent Websites than the group without the Plugin.
  $$T(18) = 3.425, p = .003, r = .62$$
Important qualitative findings:

- Possible advantages of the Plugin

- Possible disadvantages of the Plugin

- Additional Informations for the Plugin and the generated Warning
Thank you for your Attention!
Sources: