EECE 412, Fall 2012

Quiz #5

This quiz consists of 6 pages. Please check that you have a complete copy. You may use both sides of each sheet if needed.

Your Family name: ________________

Your Given name: ________________

Your student ID: ________________

Name of your left neighbor: ________________

Name of your right neighbor: ________________

#	Points	Out of
1		3
2		3
3		4
4		5
5		7
TOTAL		22

ATTENTION: When necessary, make reasonable assumptions and state them clearly in your solutions.

Notes:

1. Make sure your handwriting is legible. If the teaching staff does not understand what your wrote, they mark your answer as if the unreadable text is missing.

2. Aim to be precise and to the point. The experience of teaching this course since 2004 suggests that excessively long answers tend to correlate with lower marks.

3. As in real world, stated questions and/or accompanied descriptions in this quiz are often open-ended and one has to make assumptions in order to answer them. If you do make assumptions, state them clearly and explicitly.

4. The mark for this quiz will be pro-rated. That is, the best answer receiving 100% and the marks for all other answers being pro-rated accordingly. So, don’t panic if you feel like you are severely short on time. Everybody is. ☺

1. **(3 points) What are the top three types of bugs that are reported to Mozilla Corporation (1 point)? Briefly explain these vulnerabilities (2 points).** (presentation by Yvan Boily, Mozilla Corp.)

Bug #1: XSS – allows execution of a script supplied by an attacker on a targeted website

Bug #2:CSRF – allows to send a forged request from a website, controlled by an attacker, to any other website on behalf of a user.

Bug #3: SQLI – allows running an SQL script provided by an attacker on the website database. Often occurs due to bad sanitization of the user input.

2. **(3 points) What are the eight ways to exploit a "zombie" PC that make it valuable for criminals?** (presentation by Dmitriy Samosseiko, Sophos Labs)

Such PC can:

A) **Be used as a webserver to serve some pages**
B) **Participate in Bot activities (e.g., DDOS)**
C) **Send Spam**
D) **Steal account credentials**
E) **Steak financial credentials**
F) **Steal virtual goods, such as game characters, online game currency etc.**
G) **Hijacking of personal OSN accounts**
H) **Take PC as a hostage (as for ransom, fake AV)**

3. **(4 points) - What is phishing attack (2 points)? Why are users so vulnerable to such attack (2 points)?**

Phishing is an attack where attacker tries to get hold of users' private information (such as passwords, usernames, credit/debit card details etc.) by masquerading itself as a trustworthy entity in an electronic communication. This could be an email message or a fake website.

Users are vulnerable to such attacks because:

a) **User trust too readily phishing emails and websites.**
b) **It is very hard task for users to identify a phishing website by checking the URL, or examining PKI certificate.**
c) **Users are so overwhelmed by the number of warnings, requests, and other popups, that they do not pay attention to them.**

4. **(5 points) - Explain the following principles of secure systems (proposed by Lee, 2002).**

Path of least resistance

Align security with the most comfortable way to do tasks.

Active Authorization

Grant authority according with users actions indicating consent.

Revocability

Offer the user ways to reduce others' ability (authority) to access the user's resources.

Visibility

Maintain accurate awareness of others' authority as relevant to user decisions.

Self-awareness

Maintain accurate awareness of the user's own authority to access resources.

Trusted path

Protect the user's channels to agents that manipulate authority on the user's behalf.

Expressiveness

Enable the user to express safe security policies in terms that fit the user's task.

Relevant Boundaries

Draw distinctions among objects and actions along boundaries relevant to the task.

Identifiability

Present objects and actions using distinguishable, truthful appearances.

Foresight

Indicate clearly the consequences of decisions that the user is expected to make.

5. **(7 points) Assume you want to study the usability of three user interfaces for managing access to Facebook photo albums. The first interface shows the list of users who have access to the album on the sidebar when you enter the album. The second interface shows the list of users under the album name, and the third interface offers a control center with the list of all albums and users in a matrix.**
    a. **(4 points) If you want to compare the efficiency of setting access control policy using each interface, which of the following approaches would you use and why? (1) Field study (2) Lab study (3) Heuristic Evaluation (4) Survey. Justify your answer.**

Answers:

a)

The most optimal way is a lab study, since it gives you more precision and control over the experiment.

Field study is too long to run and might not give any benefits in comparison with the lab study.

Heuristic Evaluation might be a good option for preliminary evaluation, but it does not provide direct comparison between interfaces, since is done by HCI professionals, not representative users.

Survey is not applicable to such questions, since it does not really measure the efficiency in any way.

b. **(2 point) What will be your independent and dependent variables in the study?**

Independent variable: interface (1 Mark)

Dependent variable: time to completion (efficiency is fine as well) (1 Mark)

c. **(1 points) Should the study design use within-subjects or between-subjects approach? Justify in one or two sentences why.**

Both approaches are fine:

a) **Between subjects: because there is no carryover effect (learning, fatigue), shorter evaluation session,**
b) **Within subjects: because there is less variability, no assignment bias, less costly**