EECE 412, Fall 2010

Quiz #1

Your Family name: _____

Your Given name: _____

Your student ID: _____

Questions:

1. (4 points) Based on the PC World article about Twitter Worm reproduced handout #1, analyze (1) the value of the assets at risk, (2) threats to these assets, and (3) threat agents, for the twitter users due to the described attack. If necessary, make reasonable assumptions and state them clearly. Classify which of the CIA properties of the valuable assets were reduced as a result of the incident.

Value of Assets	Threats	Threat Agents	CIA property
Information posted on user accounts	Sending gibberish to user's followers	hackers, malware maker	Integrity
Availability of Twitter page	Redirect visitors of the user's Twitter page to another website	Malware makers who wants to visit their website	Availability

(4)

2. (4 points) Consider the risks due to Twitter Worm explained for the previous problem. For each of the four ways of managing this risk, give one example of what Twitter users can do. Be specific.

1. Accept - user accepts the risk and do nothing about it. User will suffer from the Twitter Warm.

2. Avoid - Do not use Twitter at all. Existing user can close the account.

3. Transfer - Use a friend's user account.

4. Reduce - Use anti-virus or better computer security software.

9

10. Handout #2 contains a reproduction of Chrome OS security overview.

a. (7 points) For each principle for designing secure systems, **put a checkmark** in the following table for those aspects of Chrome OS that **enable** or **follow** this principle.

Attention: The total number of points for this question will be determine using the following formula: $R - W$, where R is the number of right checkmarks and W is the number of wrong checkmarks.

	OS hardening	Making the browser more modular	Web app security	Phishing, XSS, and other web vulnerabilities	Secure autoupdate	Verified boot	Rendering pwned devices useless	Mitigating device theft	Data protection	Account management	Biometrics, smart cards, and Bluetooth	Login	CAPTCHAs	Auto-login	Single signon
Least Privilege	√	√	√							√					
Fail-Safe Defaults							√								
Economy of Mechanism		√													
Complete Mediation						√									
Open Design			√	√	√				√						
Separation of Privilege															
Least Common Mechanism	√	√	√												
Psychological Acceptability					√	√		√		√			√	√	
Defense in depth	√		√		√	√	√		√			√			
Question assumptions					√								√		√

10

b. ~~(10~~ points) Write justification for the checkmarks in the above table.

OS hardening : - Least priviledge - reduce usefulness of successful user-level exploits

Least common mechanism - process sandboxing so processes won't be shared.

Defense in depth - layer of defense at OS-level

Making browser more modular : Least priviledge - White list unknown domains imply that by default, all ~~Least priviledge~~ - domains are blacklisted.

Economy of Mechanism - Modular = simpler

Least common mechanism - Sandboxing processes. Processes not shared.

Web app security : Least priviledge ✓ permission granted to different apps when necessary.

Open design - ✓security strategy should be open design and not on secrecy of implementation.

Least common mechanism - plugins - multi-tiered sandboxing strategy.

Defense in depth - layer defense on Web level.

Phishing, XSS, and other web : Open design ✓ HTML5 and Open Web Platform APIs deployed.

Secure auto-update : Open design - Auto-update should be open design & not on secrecy of implementation.

Psychological Acceptability - easy for user to use. Auto-update.

Defense in Depth ✓ - layer defense on update

Question/Assumption - Signed updates are downloaded over SSL.

↑ go back to consider signed updates.

What assumption being questioned?

Verified boot - Complete Mediation ✓ - Check for ~~ee~~ boot access.

Psychological Accept ✓ - More flexibility to users.

Defense Depth ✓ - Defense on boot level.

Rendering pwned devices useless - Depth Defense - defend layer in devices

FSD

Least Privilege :

Account Management - Whitelist users implies default blacklist users

✓

Psychological Accept - ✓ few clicks or keystrokes

Logic : Defense in Depth - layer def. for login.