Feedback — week 4 quiz

Help

You submitted this quiz on **Sun 23 Nov 2014 9:12 AM PST**. You got a score of **33.00** out of **46.00**. You can attempt again, if you'd like.

Question 1

Why is waiting to think about security until after the software is built a bad idea?

Your Answer		Score	Explanation
○ You might miss important security requirements that necessitate a re-design			
○ You might make critical mistakes in the software's design			
○ Fixing problems once the software is built is more difficult and more expensive			
● All of the above	✔	2.00	
Total		2.00 / 2.00	

Question 2

What is an **abuse case**?

Your Answer		Score	Explanation
(•) A scenario that illustrates a potential failure in security under relevant circumstances	✔	2.00	
( ) A scenario that illustrates a system's functional requirements			
( ) An official report made by MITRE Corp that describes a discovered software vulnerability and possible abuse of it			
( ) An example of a heated disagreement between the security team and the development team			
Total		2.00 / 2.00	

Question 3

Which of the following is a reason to make an explicit threat model when designing a system?

Your Answer		Score	Explanation
So that you avoid an incoherent defense			
So you can defend against the most likely/costly/important attacks			
So you can explicitly list and challenge assumptions that underlie your design			
All of the above	✔	2.00	
Total		2.00 / 2.00	

Question 4

Suppose you design software for a bank and the bank's customers may remotely log into its site using commodity PCs. These PCs might have malware on them, which could log keystrokes or read files stored on the machine. Which threat model (using terms defined in the lectures) makes the most sense for you to consider, when designing the bank's site?

Your Answer		Score	Explanation
Co-located user			
Network	✖	0.00	Network users can only interact with a site via its normal network interface. As such, they

user		have no direct view of other users, but malware does have such a view.
Snooping user		
Malicious user		
Total	0.00 / 3.00	

Question 5

What is a good defense against powers that are particular to a *snooping user*?

Your Answer	Score	Explanation
Using passwords to authenticate users		
Using a firewall		
Using a type-safe language		

Using encryption	✔	3.00	Snooping users can view the network message traffic of others interacting with a site, so encrypting that traffic limits the negative effects of snooping
Total		3.00 / 3.00	

Question 6

A **denial of service attack** violates what security policy/goal?

Your Answer		Score	Explanation
Authentication			
Authorization			
Integrity			
Availability	✔	3.00	Denying service makes that service unavailable to users that depend on it
Total		3.00 / 3.00	

Question 7

When talking about computer security, what do we mean by the term, **principal**?

Your Answer		Score	Explanation
A rule of thumb for secure coding			
An actor, or role, that is the subject of a security policy	✔	2.00	Principals can be people, computer programs, or some other entity acting in a particular role, like *manager* or *client*
A method for delegation			
A foundational observation			
Total		2.00 / 2.00	

Question 8

Passwords, biometrics, and user-owned SMS-receiving mobile phones are useful for what security mechanism?

Your Answer		Score	Explanation
Audit			
Small trusted computing base (TCB)			
Authorization			
Authentication	✔	3.00	These are all methods by which a principal proves his identity to a system he is interacting with
Total		3.00 / 3.00	

Question 9

We identified three categories of secure design principles: *prevention*, *mitigation*, and *recovery*. Running each browser tab in a separate OS process (as done by the Chrome browser) is an example design illustrating which category?

Your Answer		Score	Explanation
Prevention	✖	0.00	Implementing a tab in a separate process does not prevent an exploit or breach of that tab (compared to a single process model) but does limit what such a breach can accomplish, because only that process's resources are accessible

Mitigation			
Recovery			
None of the above			
Total	0.00 / 3.00		

Question 10

Suppose you are implementing a graphical user interface for using a library implementing the RSA cryptosystem, and you want to give users a way to generate new keys. Which of the following designs most takes security into account?

Your Answer	Score	Explanation
Use a text box to ask the user to fill in how many bits they want their key to be		
Don't ask the user about key size at all -- always use 256 bits		
Allow the user to use a slider to choose the		

number of bits, setting slider initially to point at 2048 bits. As the user moves the slider to larger or smaller values, visualize the difference in relative protective power, e.g., using a meter.			
Ask the user, but set the default response to be 2048 bits, which is chosen based on the assumption of a strong adversary	✖	0.00	This is not a bad design, because it picks a safe default choice, but it could be better
Total		0.00 / 3.00	

Question 11

Suppose you are implementing an extensible data management system. You want to accommodate plug-ins that can implement storage rules and query processing functionality for different data formats (e.g., relational data, object data, XML data, etc.). Which of the following designs most takes security into account?

Your Answer		Score	Explanation
The plug-ins are implemented as separate OS processes; these processes communicate to/from the main process to handle queries/updates for the data formats	✔	3.00	This is the best choice: a vulnerability in a plug-in will affect that plug-in but will have limited impact (only what it can effect via the communication API) on the rest of the application

they support

The plug-ins and the main data management software are linked into the operating system kernel as a special kind of device driver, to give them direct access to stable storage and the network stack, while the OS can enforce their security	
The plug-ins are implemented as separate OS processes but which share memory with the main process, for better efficiency. Queries/updates occur via inter-process communication.	
The plug-ins are linked directly in the address space of the data management software, ensuring high performance	
Total	3.00 / 3.00

Question 12

Promoting privacy is a goal that follows from which category of secure design principle?

Your Answer		Score	Explanation
It is an example of *defense in depth* because privacy is a deep topic that is often debated.			
It is an example of *monitoring and recovery* because failure to promote privacy could be discovered by monitoring			
It is an example of *favoring simplicity* because privacy is quite simply the right thing to do			
It is an example of *trusting with reluctance* because promoting privacy means sharing private information with as few software components as possible, meaning that fewer need to be trusted to protect the information	✔	3.00	
Total		3.00 / 3.00	

Question 13

Encrypting a password database is an example of what category of design principle?

Your Answer	Score	Explanation

○ It is an example of *monitoring and recovery*			
◉ It is an example of *defense in depth*	✔	3.00	You could argue that it is defense in depth because while a system likely has defenses in place to prevent an adversary from directly accessing the database, encrypting the database protects that database even if these other defenses are breached
○ It is an example of *trusting with reluctance*			
○ It is an example of *favoring simplicity*			
Total		3.00 / 3.00	

Question 14

Which of the following vulnerabilities can VSFTPD's secure string library help protect against?

Your Answer	Score	Explanation

☑ Integer overflow	✔	1.00	Recall the code for copying a string checks to make sure that accounting for the null terminator will not overflow the integer containing the string's length
☑ Buffer overflow	✔	1.00	Strings are coupled with their allocated size and current length, so string operations -- like copying or concatenation -- can be checked to ensure they do not overflow a buffer
☐ Privilege escalation	✔	1.00	Privilege escalation is orthogonal to string construction
☐ SQL injection	✔	1.00	The secure string library pays no attention to the contents of strings, so it will happily construct SQL-injecting strings if instructed to do so
☑ Format string attack	✖	0.00	The secure string library deals with strings of type `struct mystr`, which are separate from the `char*` strings used for format strings
Total		4.00 / 5.00	

Question 15

VSFTPD forks a new process to handle each client connection. It could have, instead, spawned a thread within the main process to handle each connection, as is done in many servers. How would this alternative design compare to the original?

Your Answer	Score	Explanation

○ It would be more secure because we could apply the SecComp system call to these threads, but could not do so for processes			
○ It would be equally secure and would perform better because threads are cheaper to manage than processes			
○ It would be more secure because threads are not subject to denial of service attacks but processes are			
● It would be less secure because a compromise by a malicious client in one thread could (more easily) access data used by another client's thread, since they share the same address space	✔	3.00	This fact is due to threads sharing the same address space as their host process
Total		3.00 / 3.00	

Question 16

FTP servers can be asked to list a directory of files. VSFTPD could do this by calling the system's `ls` (or `dir`) command, displaying the result to a client. But VSFTPD does not do this, and implements directory listings using the relevant system calls

directly. Why might you argue that VSFTPD's design makes sense from a security perspective?

Your Answer		Score	Explanation
Using `ls` provides less control over the output, which leaves users open to XSS-style attacks			
Calling `ls` involves forking a new process, which is less secure than running within the same process			
Calling `ls` doesn't give us any way to employ fail-safe defaults	✖	0.00	This statement is not really true, as it's a question for the FTP server itself; by default it could call `ls` with few parameters unless directed by other measures to do otherwise.
`ls` does more than is needed, and thus unnecessarily expands the TCB			
Total		0.00 / 3.00	