EJ Cervantes

Gary

22FEB2019

CSCI240

1. What are the four key design properties of trusted systems?

* Functional Correctness
* Enforcement of Integrity
* Limited Privilege
* Appropriate confidence level

2. What is a kernel?

* Part of an operating system that performs the lowest-level functions such as synchronization, inter process communication, and message passing

3. What are the six reasons security functions should be isolated in a security kernel? Considering the [Top Ten Secure Coding Practices (CERT)](https://canvas.xavier.edu/courses/42475/pages/top-ten-secure-coding-practices-cert) which practices may be demonstrated in a security kernel?

* Coverage
* Separation
* Unity
* Modifiable
* Compactness
* Venerability

4. What does a reference monitor do? What are the three key characteristics? (Side note: the Dec VAX mentioned in the book was indeed one of the most secure machines designed, helping provide it a lifespan far longer than other limited aspects of its architecture and operating system would have made it deserve.)

* A reference monitor is the portion that controls accesses to objects.
* The three characteristics are tamper proof, unbypassable, analyzable

5. Which do you think is harder to design into an operating system, correctness or completeness? Why?

* Correctness implies that because an OS controls the interactions between subjects and objects, security must be considered in all portions.
* Completeness implies that security functionality be included in all places necessary.
* With this being said you cannot have completeness without correctness if you don't know where security must be considered making completeness more difficult to come by

6. Besides the four design properties of trusted systems, the book also describes eight design principles. Provide at least three ways the four design principles are demonstrations of a design principle for trusted systems.

* Simplicity of design is related to an open designed
* Layered design is related to least privilege
* Reference monitor is related to permission based

7. What are the three characteristics of a trusted system?

* A defined policy that details what security qualities come with it
* Appropriate measures and mechanisms by which it can enforce that security adequately
* Independent scrutiny or evaluation to ensure that the mechanisms have been selected and implemented properly so that the security policy is in fact enforced

8. What is the Orange Book? What has replaced it?

* The Orange Bookwas the first attempt to codify principles and requirements for secure computing systems and was later replaced by the CCITSE

9. Which of the four basic interactions of a Trusted Computing Base have we not discussed in this overview of operating systems?

* Process activation
* Execution domain switching
* Memory protection
* I/O operation

10. In what way is ctrl-alt-delete an example of a Trusted Path?

* The user is already logged in so they are allowed to delete/cancel third party applications

11. Consider two operating systems with the same feature. What is the difference the system with Common Criteria assurance level 1 for the feature versus the system with Common Criteria assurance level 5 for the feature?

* The lowest level of assurance is level 1. Meaning a lot less features would be implemented than in level 5