

Review Aid for Final Exam

CS 5323 Principles of Information Security

December 2007

Gollman Chapter 8

- When a security model is given as a state machine, how can security properties be modeled? What does it mean that a transition function preserves the security property? Why is this important?
- What security policy does the Bell-LaPadula (BLP) model enforce? The BLP model is given by a state machine. What are the components of the state? Explain the structure and purpose of each component¹. What are the simple security property and the star property? What does it mean for a state to be secure in this context? What does it mean for a transition to be secure in this context?
- Why did McLean argue that BLP's notion of security property was unsatisfactory?
- What security objective does the BLP model focus on?
- What security objective does the Biba model focus on? In what sense is the Biba model dual to the BLP model?
- What are some strengths and weaknesses of security models based on Dynamic Integrity Levels?
- Explain the Chinese Wall Model. What security objectives does it focus on?

Badger et al.

- Is DTE a MAC or a DAC (discretionary) system? DTE enhances simple type enforcement. What are those enhancements designed to achieve and to overcome?
- Recall that DTE associates a domain with each subject and a type with each object. How does DTE define the association of types with objects?
- In the DTE Language (DTEL), domain statements define entry points, access rights on objects and access rights on subjects. What are entry points and what do they accomplish. What Unix structure do they resemble? What is the difference between exec and auto access modes? How are they used?
- Explain each of the statements in example 3. Do programs that are run as system.d subjects have to be DTE-aware?

Flask Paper

- One of the primary goals of the Flask architecture is to ensure that subsystems have a consistent view of policy decisions as these decisions change. What does it mean to have a consistent view in this context?
- What is the purpose of the Access Vector Cache (AVC)?
- What is a callback and how does registering callbacks enable the object manager to receive notifications of policy changes?
- The object manager and the security server collaborate in associating security attributes with objects. Outline how this is accomplished.

¹Notice that while b defines the accesses that are actually authorized by the system, M expresses discretionary permissions.

- Outline how the AVC module coordinates between the object manager and security server, caching access decisions for subsequent use, but ensuring that cached decisions are removed when the relevant policy changes.
- Explain what it means for revocation to take place atomically. Why might this be important in effective policy enforcement?