Principles of Computer Security

Alvin Lin

January 2018 - May 2018

Exam Key

1. (a) CI no-A: Each student can look up their own data and modify their registration for a semester (they can do both C and I), but SIS is down (no A) to the student.

   (b) IA no-C: Each student's data is public, but is only modifiable by an authorized faculty member.

2. The two steps of authentication are identification (where the subject presents an identifier) and verification (where the system corroborates the binding between the subject and presented identifier).

3. Capability lists are the rows of an access control matrix. Each row is for a subject (or role), which denotes the access privileges of that subject to different objects. For example, a subject Jo's capability list would show what Jo can do to each object.

4. (a) MAC Lattice

   (b) Clearance is a label associated with each subject while classification is a label associated with each object. Each label has two parts: a level of access and the applicable type of objects.

   (c) In Bell-LaPadula, a node x above another node y in the MAC lattice dominates y for **confidentiality (reading)**. When a subject Jo with clearance (Secret, Maps) wants to **read** RITCampusMaps with classification (Public, Maps), the BLP reference monitor checks the lattice, and grants access if Jo's label dominates the map's label. It rejects access otherwise to maintain confidentiality.

(d) In Biba, a node x above another node y in the MAC lattice dominates y for **integrity (writing)**. When a subject Jo with clearance (Secret, Maps) wants to **update** RITCampusMaps with classification (Public, Maps), the reference monitor checks the lattice and grants Jo permission to modify it if Jo's label dominates the map's label.

5. Because BLP restricts too much acces, it really needs the notion of a trusted subject for it to work correctly and efficiently. Having trusted subjects means that BLP is pushing a great deal of power to people who work outside the software system.

6. RBAC's drawbacks are that it is coarse-grained and requires a complex initial setup ahead of time.

7. ABAC's strengths are that it is flexible and fine-grained.

8. ABAC's drawbacks are that its run-time access decisions can't be analyzed ahead of time, policies are complex so making changes to permissions is hard, and it is difficult to review permissions.

9. "Encraption" does not meet the needs of a trusted cryptosystem as it may violate any or all of the following:

   (a) sound mathematics

   (b) anayzed by competent experts and found to be sound

   (c) stood the test of time

10. Homomorphic encryption permits operations on ciphertext, reducing opportunities for information leakage.

11. ElGamal supports homomorphic addition between two ciphertexts, and thus scalar multiplication. Therefore, the scalar has to be in plaintext and so the threshold value used in the secure comparision protocol is also in the clear. This limits existing solutions to be in two-party settings only.

12. (a) Economy of mechanism: security mechanisms should be as simple as possible.

    (b) Open design: security of a mechanism should not depend on the secrecy its design or implementation.

(c) Separation of privilege: must not grant permission only on a single condition.

(d) Complete mediation: check each object access to ensure they are allowed.

13. (a) Physical access to a computer renderse all software security meaningless. Servers and protected data should also be physically isolated, locked, and protected.

(b) Human error and bad practice renders security systems meaningless. A human writing passcodes on paper negates the purpose of a password authentication system.

(c) Attacks should not be able to compromise all systems irreversibly. Sensitive data should be encrypted and backed up.

14. (a) Active risks should be monitored constantly, with prevention systems ready to address and mitigate the disaster. Prevention systems should be prioritized by the threat level.

(b) Prevention systems should be used to address and mitigate disaster. The scope and effect should be minimized as much as possible.

(c) If the prevention systems were not effective, they should be modified and adjusted according to the threat. Damage assessment and correct should also occur after the disaster.

You can find all my notes at `http://omgimanerd.tech/notes`. If you have any questions, comments, or concerns, please contact me at alvin@omgimanerd.tech