Assignment - PSO 4

Purdue CS426 - Computer Security - Prof. Spafford

Harris Christiansen - March 6, 2018
christih@purdue.edu

Problem 1

List two methods to detect or prevent off by 1 errors. (10 pts.)

- Write tests which check various valid/invalid inputs (especially inputs at the low/high extremes), and make sure those tests always pass after any chance to the program. This will help detect off-by-1 errors early, and allow them to be fixed before release.
- To prevent off-by-1 errors, use enumerations instead of lists/arrays. You can then iterate through all the element of the enumeration without risk of stepping outside boundaries. Only the items in the enumeration will be iterated through.

Problem 2

What are the pros and cons between an access control list vs. access control matrix? (10 pts.)

- An access control list is a set of users and permissions that are attached directly to the file.
- An access control matrix is a single system wide file, containing a matrix where one dimension corresponds to an object or subject, and the other dimension corresponds to files or permission controlled objects.
- Access control lists are attached directly to the file, while a matrix is a single file containing all access control lists in a single place.
- A pro of access control lists is that they are attached directly to the file, and thus easier to require and verify for every file on the system.

Problem 3

What are the pros and cons between an access control lists vs. capabilities list? (10 pts.)

- An access control list specifies access permissions for all given actors/users.
- A capability list is a set of permissions that are passed with file pointers. They are set when the file is opened, and stay with that opened reference. Thus, if a file with a capability list is passed to another user/process, the correct permissions for who opened the file will be enforced.
- A capability list solves the important problem of the confused deputy. While an access control list will still allow a client to request a permitted server to open/access a restricted file, a server that receives a file with capability list will still be restricted from the file.

Problem 4

Describe what the confused deputy problem is and provide an example. (20 pts.)

- The confused deputy problem is a type of privilege escalation where a malicious actor successfully requests a server to perform an action that the malicious actor would otherwise not have permission to perform.
- The classic example is a client requesting a service to read/write to a file which the client does not and should not have access to itself.
- A modern example is cross-site request forgery (CSRF) attacks, where a malicious actor causes a device to make a web request from that device using that devices cookies/credentials, allowing the malicious actor access to something they are not authorized for.

Problem 5

Describe Role Based Access Control. What is an advantage it has over other Access Control? What is one disadvantage? (30 pts.)

- Role based access control is a method of access control where users are assigned roles, and roles have various privileges among systems and files.
- One advantage of role based access control is the ability to easily assign and verify permissions. Roles can be easily verified to ensure they only have permissions that they should, and thus users of that role also have appropriate permissions.

- Another advantage is that permissions for a role can be easily updated, and apply to all users. This makes it easier to maintain permissions as changes are necessary.
- One disadvantage of role based access control is that it is often necessary to give individual users varying access, which can lead to requiring a large number of roles. This goes against what role based access control tries to solve, and can even make the access control system more complicated.

Problem 6

What is the difference between Identification and Authentication? How do they work together in computing? (20 pts.)

- Authentication is the process of proving your identity to a system, often via username/password, or a key.
- In contrast, Identification is the process of simply identifying yourself to a system, without proving who you are. Identification should never be trusted without Authentication.
- Identification and Authentication can be used together to have a client identify itself to a system (Identification), and then prove they are they identity using a means of credentials (Authentication).

Problem 7

Why is it easier to use biometrics for authentication vs. identification? (20 pts.)

- When biometrics is used for identification, it must compare the biometric input data with all known candidates to attempt to determine the correct candidate.
- It is easier to use biometrics for authentication because the biometric input data must only be compared against the single candidate which is attempting to authenticate.

Problem 8

Why is it potentially more damaging when biometric data is compromised than something like a password? How can this risk be mitigated? (20 pts.)

- Unlike passwords, biometric data cannot be changed. Thus, if biometric data is compromised, that individual will forever have their biometric data leaked, and they will be unable to use biometric authentication safely.
- This risk can be mitigated by keeping biometric data secure on hardware implementations, and only storing a one-way hashed version of the biometric data. When a user attempts biometric authentication, their biometric data will be hashed and compared against the stored data on the secure hardware.

Problem 9

You are tasked with designing a server farm for a government agency. Describe how you would design the physical security for the facility. Identify at least 5 physical security measures/design practices you would use in designing the facility and how they would help in keeping the facility secure. (40 pts.)

- Setup a door lock security system with many rooms and like-purpose servers in the same room as each other. Door lock access for each room should only be given to individuals who should have access to those specific servers.
- Setup a surveillance system, including cameras and other sensors, which is monitored for both unauthorized activity on the premises, as well as tapping of the surveillance system.
- Build strong outer-walls for the building, and include gates and checkpoints, such that any physical attacks against the premises/building will be made more difficult.
- Make sure that all boxes, cargo, food, deliveries, shipments, and employees who enter/exit the facility do not have any computer devices or data on them which could be a threat or attempting to steal data.
- Use strong inventory controls for all data and equipment in the facility. This means tagging every piece of hardware, keeping track of where the hardware is assigned and located, and regularly verifying that the hardware is there.