Exercises Lecture 5: Requirements and Assurance

September 28, 2020

1 Assurance - Practical

In assignment 3 problem 4 you will be implementing logging in an existing system as well as using a tool called spotbugs. In this portion of the exercise session, download spotbugs from here and install it. A handy guide can be found here for both how to install and run the software.

Select one of your own projects, or run it on the very well coded demo project that we have uploaded on learnit, just to familiarize yourself with the software. Can you correct any of the bugs?

2 Assurance - Theoretical

These are theoretical questions taken from the course last year. They might be relevant to think about for memorising theory, but you are not required to answer them unless you run out of things to do during this session. The last page contains definitions.

2.1 Assurance

Defining a trusted system:

- What are security requirements?
- What does it mean to do assurance on a system?
- What are security mechanisms?

2.2 Assurance

A vendor advertises that its system was connected to the Internet for three months, and no one was able to break into it. It claims that this means that the system cannot be broken into from any network.

Do you share the vendor's confidence? Why or why not?

If a commercial evaluation service had monitored the testing of this system and confirmed that, despite numerous attempts, no attacker had succeeded in breaking into it, would your confidence in the vendor's claim be increased, decreased, or left unchanged? Justify your answer.

2.3 Principles

Military intelligence services tend to keep highly classified information on machines with no physical connection to the internet.

This is an example of adherence to which security principle?

2.4 Principles

Back in the good old days, everybody had root-access to the development server because the IT-guy was tired of being asked to reset people's passwords.

This is an example of a violation of which security principle?

2.5 Principles

Edward Snowden and Bradley Manning both accessed enormous amounts of information classified by the US Government. Their accesses were apparently neither logged nor constrained in ways beyond having access to a particular network.

This is an example of violation of which security principle?

2.6 Principles

The computer games SimCity III and Diablo II both required an always-on internet connection to be playable, even in single-player mode, where the game otherwise did not need an internet connection. The connection was used to validate with the development companies that the game was a legitimate copy, as opposed to a pirated one. If the internet connection dropped for any reason, the game would be unplayable until it could re-connect to its home server and validate its legitimacy.

This is a (very customer unfriendly) example of adherence to which security principle?

2.7 Principles

A common technique for inhibiting password guessing is to disable an account after three consecutive failed login attempts.

Discuss how this technique might prevent legitimate users from accessing the system. Why is this action a violation of the principle of least common mechanism?

One can argue that this is an example of fail-safe defaults, because by blocking access to an account under attack, the system is defaulting to a known, safe state.

Do you agree or disagree with this argument? Justify your answer.

2.8 Mechanisms

Pop quiz!

- What is Authentication?
  - The process of verifying the identity of an entity
  - Mechanisms preventing unauthorized uses access to resources
  - A security principle
  - A mechanism for storing passwords
- What is access control?
  - Mechanisms preventing unauthorized uses access to resources
  - Policies describing which resources a user may access
  - A synonym for “authorization”
  - A synonym for “authentication”
- What is information flow control?
  - A way of distributing information among entities
  - A way of restricting information access for entities
  - A technique for drawing information flow diagrams in a controlled manner
  - A model displaying the structure of the system’s information flow
- What is auditing?
  - A way of halting the execution of malicious actions
  - A process for designing secure software by reviewing code
  - A mechanism for detecting anomalous behaviour in a system

2.9 Evaluation

What are the values of doing formal evaluation? What do you see as the drawbacks of evaluation?

3 Definitions (Assurance)

- "An entity is trustworthy if there is sufficient credible evidence leading one to believe that the system will meet a set of given requirements. Trust is a measure of trustworthiness, relying on the evidence provided."
- "Security assurance, or simply assurance, is confidence that an entity meets its security requirements, based on specific evidence provided by the application of assurance techniques."
- "A trusted system is a system that has been shown to meet well-defined requirements under an evaluation by a credible body of experts who are certified to assign trust ratings to evaluated products and systems."

4 Definitions (Design principles)

- "The principle of complete mediation requires that all accesses to objects be checked to ensure that they are allowed."
- "The principle of fail-safe defaults states that, unless a subject is given explicit access to an object, it should be denied access to that object."
- "The principle of least privilege states that a subject should be given only those privileges that it needs in order to complete its task."
- "The principle of separation of privilege states that a system should not grant permission based on a single condition."
- "The principle of economy of mechanism states that security mechanisms should be as simple as possible."
- "The principle of open design states that the security of a mechanism should not depend on the secrecy of its design or implementation"
- "The principle of defense in depth states that security should use independent and overlapping mechanisms to avoid a single point of failure."
- "The principle of psychological acceptability states that security mechanisms should not make the resource more difficult to access than if the security mechanisms were not present."
- "The principle of isolation states that security resources should be isolated into groups of similar needs."
- "The principle of minimum exposure states that the attack surface of a system should be as small as possible."
- "The principle of least common mechanism states that mechanisms used to access resources should not be shared."