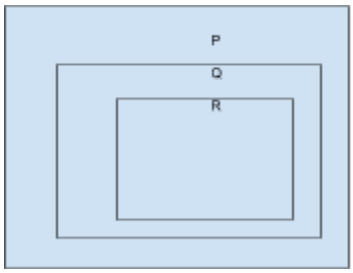
Lecture 2 - 09/09/2019

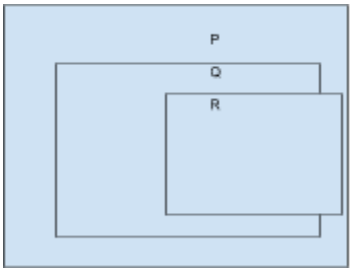
Secure States

Let P be the set of all possible states of a system

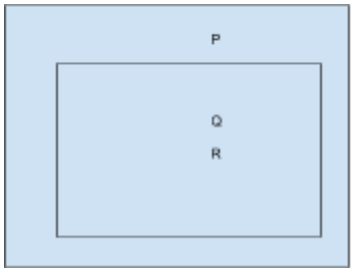
Q = set of secure states (Defined by sec policy)
R = set of states allowed be secure mechanical systems



Secure and inprecuse



Too broad



Secure and precise

Course Overview

“Security engineering is about building systems to remain dependable in the face of malice, error, or mixchance”

If policy, mechanisms, and specification are done properly, suste is dependable.

Goals of security:

- Prevention: Attackers are out there are we want to prevent those attackers from being able to cause their attacks
- Detection: We want to be able to detect these attacks before too much damage is done
- Recovery: Be able to recover data and the system state - Restore confidence

Building systems

Everything starts with your

Threat model:
- Who are my attackers
- What are they going for
- Why are they doing it

Security Policy:
- Given this attacker, I am going to define what is allowed and not allowed in my system.

Security Mechanisms:
- Crypto
- Access control
- E.t.c.

Security policy + mechanisms; This combination is a security specification. Design comes from the security specification. Then we implement our system. Finally we operate and maintain it.

Operational and human issue:
- Cost/benefit analysis - is the cost of the implementation worth the benefit
- Risk analysis - How likely are the potential threats.
- Laws/customs - What is and isn't legal in the area you're operating in
- Organizational problems - When people start asking questions about who is responsible and whose job it is to put security in place. Who can I blame.
- People problems - people are bypassing controls, or might to subvert security mechanisms

Basic components of computer security:

Confidentaitlty: concealment of information or resources.
- Encryption: Data is in the open but is not in plain text
- Access control: Data is in plain text but is not out in the open

Integrity: trustworthiness of data or resources
- Is the data true and is the origin of the data true
- Blocking unauthorized attempts to change data

Availability: the ability to use information or resources
- Denial of service

Design Principles - Principles for the design and implementation of security mechanisms

Lease Privilege - a subject should only be given the privilege they need
- Privilege is not assigned by identity, but by their job function

Fail-safe defaults - Your system needs to fail in a safe way.
- Rollbacks must be able to occur

Economy of mechanism - You want to use security mechanisms that are as simple as possible.
- Complexity is the enemy of security

Complete mediation - Going to sit in the middle of all access requests

Open Design - The security of a mechanism should not rely n the secrecy of its design

Separation of Privilege - A system should not grant access to critical resources on a single policy
- If you want to perform an action, you must go through multiple checks

Least common mechanism - Mechanisms used should not use shared resources, i.e.memory.

Psychological acceptability - the mechanisms you put in place must be usable by real people

Passwords

- Any form of known text that you use to verify that you are a legitimate user
- By definition, must be memorable and therefore should be memorable by others

Common problems with passwords:

- Naive users
    - Easy passwords
    - Telling friends
    - Default passwords
- Too many passwords
    - Cope by using the same password
    - When required to change, they make trivial changes
- Design or operational errors
    - Systems use passwords that are easy to find out
    - Users not allowed to change passwords
    - Plaintext passwords

Threats:

- Targeted attack at a specific users account
- Penetrating any account, naive attack
- Penetrating any account on any system on a domain
- Denial of Service

Measures to protect passwords:

- User training
- Interface design
    - Make sure your physical or front end design is conducive to the security of the system
- Protect pwd in transit
    - Secure tunnel / SSL
- Trusted path
    - Make sure you are entering your password where you should be
- All-or-nothing error messages
    - Make sure your error message does not disclose issues with an incorrect password
- Protect log file
- One-way function of passwords in pwd file
- Hide pwd file
- Exponential backoff or disconnection
- Password aging
- Using graphical passwords

- Use salting