Lecture 6: Security Design Principles*

CS 392/6813: Computer Security

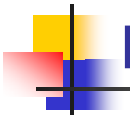
Fall 2010

Nitesh Saxena

*Adopted from a previous lecture by Nasir Memon

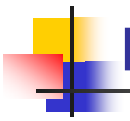
Design Principles for Secure Systems

- Two basic themes:
  - Simplicity – KISS
    - Makes design and interactions easy
    - Easy to prove its safety
  - Restriction
    - Minimize the power of entities



Principles of design

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability



Principle of least privilege

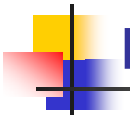
- Entity should be given only those privilege needed to finish a task
  - Temporary elevation of privilege should be relinquished immediately
  - Granularity of privileges
  - Append permission only for logging process.

Principle of fail-safe defaults

- Unless a subject is given explicit access to an object, it should be denied access to the object.
  - Default access to an object is *none*
  - Access Control Lists (ACLs), firewall examples.
  - Restricting privileges at the time of creation

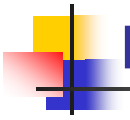
Principle of economy of mechanism

- Security mechanism should be as simple as possible.
  - Fewer errors
  - Testing and verification is easy
  - Assumptions are less
- Interface to other modules
  - Implicit assumptions of modules
  - Finger example



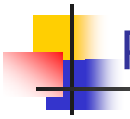
Principle of complete mediation

- All accesses to objects should be checked to ensure they are allowed.
  - UNIX file descriptor
  - DNS cache poisoning.
  - Restrict caching policies
  - Security vs. performance issues



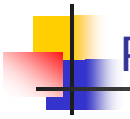
Principle of open design

- Security of a mechanism should not depend upon secrecy of its design or implementation (why not?)
  - Secrecy != security
  - Complexity != security
  - "Security through obscurity"
  - Cryptography and openness



Principle of separation of privilege

- System should not grant permission based on single condition
  - Company checks over $75,000 to be signed by two officers.
  - Example: "su" on BSD requires
    1. User be in group "wheel"
    2. User knows root password
  - Restrictive because it limits access



Principle of least common mechanism

- Mechanisms used to access resources should not be shared
  - Restrictive because it limits sharing
  - Amazon website – Denial of service attacks!!

Principle of psychological acceptability

- Security mechanism should not make the resource difficult to access
- Recognizes the most important element in computer security? **Human**

Example 1

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

- Viruses cause havoc because, any program or script that is downloaded or received as email attachment, runs with the privileges of the user that runs them. Or worse the privileges of the application.
- What is the problem?
- What design principles are being exploited?

Example 2

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

- Unix password authentication
- Which design principle is being adhered to mainly?

Example 3

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

- "poly11" is the wireless LAN to be used by Poly faculty, students and staff. Earlier, even a guy from Au Bon Pain could use it!!!!!!
- What design principles are being violated?

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

Example 4

- A bluetooth Device A wants to establish a key with another bluetooth device B

Mechanism 1: they agree upon a common trusted CA, get certificates from this CA and for example, use STS protocol to establish a key

Mechanism 2: they use a physical channel (e.g., an audio channel) to establish a key

- Which mechanism adheres better to the principle of economy of mechanism?

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

Example 5

- TLS defines a mandatory server side certificate and an optional client side certificate. Though highest level of security is achieved using client and server side certificates, client side keys did not become very popular because of administrative overhead (Installation, expiration of client side certificates).
- What design principle is being violated?

Example 6

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

- COCA (Cornell Online Certification Authority) distributes the operation of issuing certificates among multiple servers
- What is the main principle COCA is trying to adhere to?

Example 7

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

- Polynomial secret sharing
- What principle is being adhered to?

Example 8

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

- Various cipher machines were developed and used during the two World Wars. For example, Enigma, Schlusselzusatz, Purple, etc. It was believed that keeping secret the design of the machines will help boost the security.
- Which principle is being violated?

Example 9

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

- Everytime A receives a certificate from B, she should verify if B's certificate is not revoked. We studied the mechanism of CRLs to achieve this.
- Which principle is being violated by CRLs?
- What would be a better solution?
  - Online Certificate Status Protocol (OCSP)

Example 10

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability

- Policy on password selection to access machines at Poly:
  - Use both uppercase and lowercase letters if the computer system considers an uppercase letter to be different from a lowercase letter when the password is entered.
  - Include digits and punctuation characters as well as letters.
  - Choose something easily remembered so it doesn't have to be written down.
  - Use at least 8 characters. Password security is improved slightly by having long passwords.
  - A password should be easy to type quickly so someone cannot follow what was typed by watching the keyboard.
  - Use two or more short words and combine them with a special character or a number, like ROBOT4ME or EYE-CON.
  - Put together an acronym that has special meaning to you, like NOTFSW (None Of This Fancy Stuff Works) or AVPEGCAN (All VAX Programmers Eat Green Cheese At Night).
- Which principle is being violated?