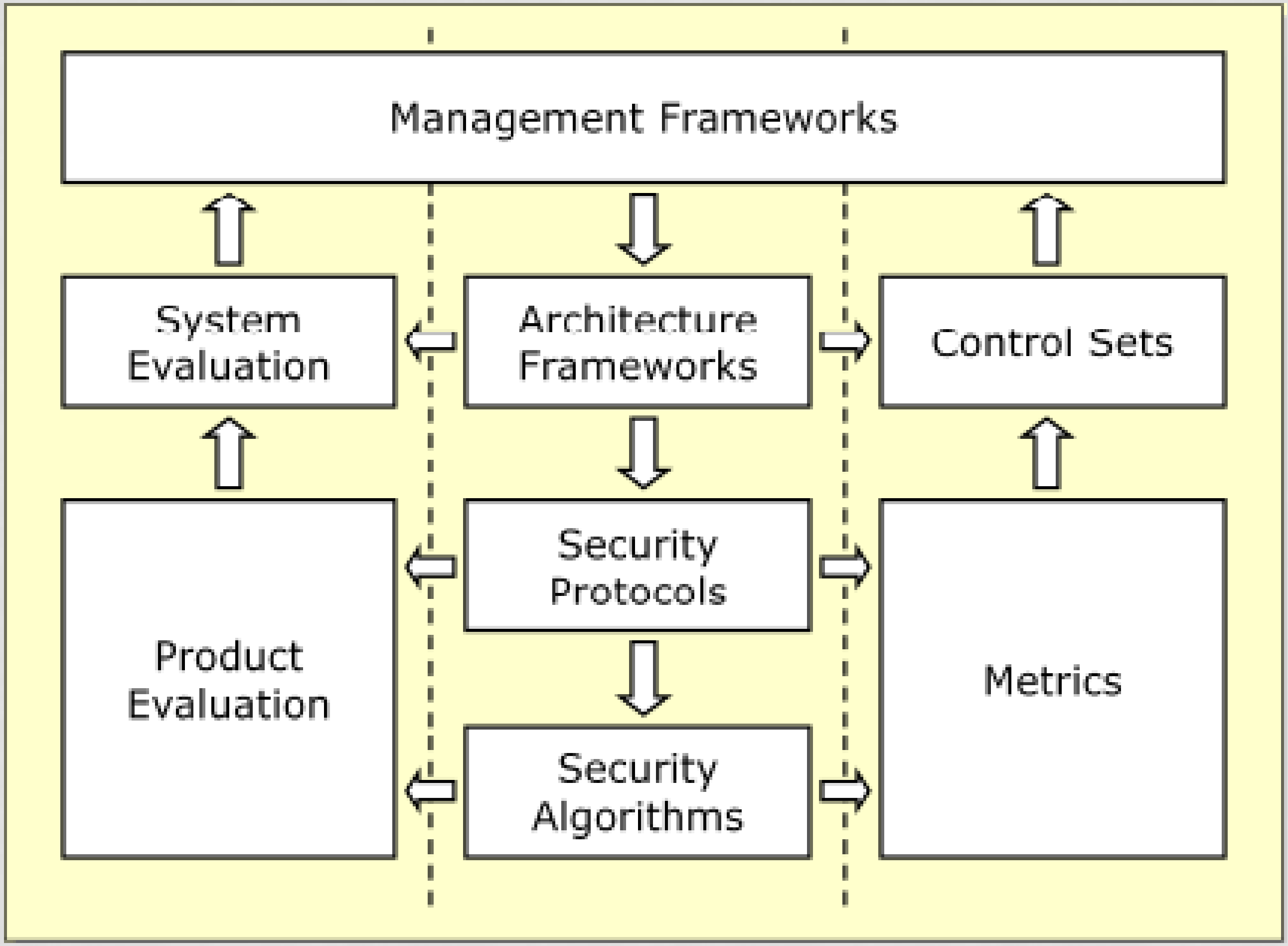
CSC429 – Computer Security

LECTURE 10
SECURITY STANDARDS AND PRINCIPLES

Mohammed H. Almeshekah, PhD
meshekah@ksu.edu.sa

Computer Security Standards

Computer Security Standards



How to Use a Standard

- How to use a standard:
  - Certification, e.g. ISO 27001.
  - Compliance
  - Guidance.

- Where are the standards:
  - International; ISO, IEC, ITU.
  - Regional; European (CEN, etc).
  - National; ANSI (US), BSI (UK), JISC (Japan), etc.
  - Professional; IEEE, NIST.
  - Company Standards; PKCS (RSA), etc.

Security Design Principles

Saltzer and Schroeder

- “The Protection of Information in Computer Systems” in 1975:
  - Many of the ideas they discuss are as relevant today as they were then.
  - They describe eight design principles that are of particular relevance when designing security mechanisms.
- Other Models exist:
  - E.g. Gollmann’s Design Decisions.

The Principles

1. Economy of mechanism
2. Fail-safe defaults
3. Complete mediation
4. Open design
5. Least privilege
6. Least common mechanism
7. Separation of privilege
8. Ease of use

Economy of Mechanism

- The design of a protection mechanism should be as simple as possible.
  - Errors in design or implementation may lead to false grants and will cause vulnerabilities.
  - The simpler the mechanism the more likely errors will be detected during development and testing.

Fail-Safe Defaults

- Access should be denied unless it is explicitly authorized.
  - If no protection is specified access will be denied
  - If the mechanism has implementation errors it is more likely to be noticed
    - Fail-safe defaults will lead to false denies
    - If authorized users have requests denied they are likely to bring it to the attention of the systems administrator.

Complete Mediation

- Every attempt to access resources must be intercepted and evaluated by the protection mechanism.
  - The reference monitor in access control

Open Design

- Do not make the security rely on “security by obscurity”.
    - The strength of a protection mechanism should be independent of knowledge of the working of the mechanism.
    - The strength should depend on the secrecy and strength of the secret values used as input to the protection mechanism such as cryptographic keys or passwords.
    - Users should feel more confident in the quality of a protection mechanism if it has been subject to independent scrutiny and been found to be secure.

Least Privilege

- Only give a program access to resources if it requires access.
  - This is a variant of the military “need-to-know” principle
  - If an incorrect program malfunctions or a malicious program exploits a vulnerability the fewer privileges it has the less damage it can do
  - This lesson is frequently forgotten by system administrators
    - Unnecessary access rights are assigned to users
    - Unnecessary programs and utilities are installed (as part of a generic build) on machines (or not “uninstalled” from “out-of-the-box” configurations).

Least Common Mechanism

- The use of shared resources should be minimized.
  - Taken to its extreme this principle requires that each program should run on its own dedicated machine.
    - Physically distinct machines
    - Logically distinct machines
  - Clearly this is likely to conflict with functional requirements and lead to poor resource utilization.
  - Right balance must be made.

Separation of Privilege

- Wherever possible two or more independent checks should be used to confirm that a request is authorized.
  - E.g. Two-factor authentication
  - It should be impossible for a single user to perform a sequence of mission- or business-critical actions
    - Two different generals must separately arm and launch a nuclear missile
    - Two different individuals must separately authorize checks over $5000.

Ease of Use

- Never underestimate the unwillingness of users to interact with security mechanisms!

  - The human element of computer systems is probably the most significant vulnerability
    - Choice of passwords
    - Security of passwords
    - Configuration errors

  - If a security mechanism is invisible, or easy to use when visible, users are more likely to use it rather than circumvent it.

Next Lecture

- Market Failure of Secure Software
- Readings for next lecture:
  - Anderson’s Book – Sections 7.3.3, 7.5.2 and 7.5.3