2019-02-11

IT Security #1

Basic security vocabulary – core concepts

Niels Christian Juul

Informatik
Datalogi
Roskilde Universitet

Roskilde Universitet
Niels Christian Juul
Hus 08.2-071
Universitetsvej 1
4000 Roskilde
ncjuul@ruc.dk

IT-security

Prerequisite for this course:

Basic security vocabulary

Based on Stallings & Brown, Chapter 1 (1.1-1.4 + 1.6-1.8)

1. Concepts
2. Threats, Attacks, and Assets
3. Functional Requirements
4. Design Principles
5. Management
6. Standards

Why IT-security?

What's the problem?

- Vulnerabilities
- Attacks

What's the solution?

- Defense
- Intelligence
- Recovery

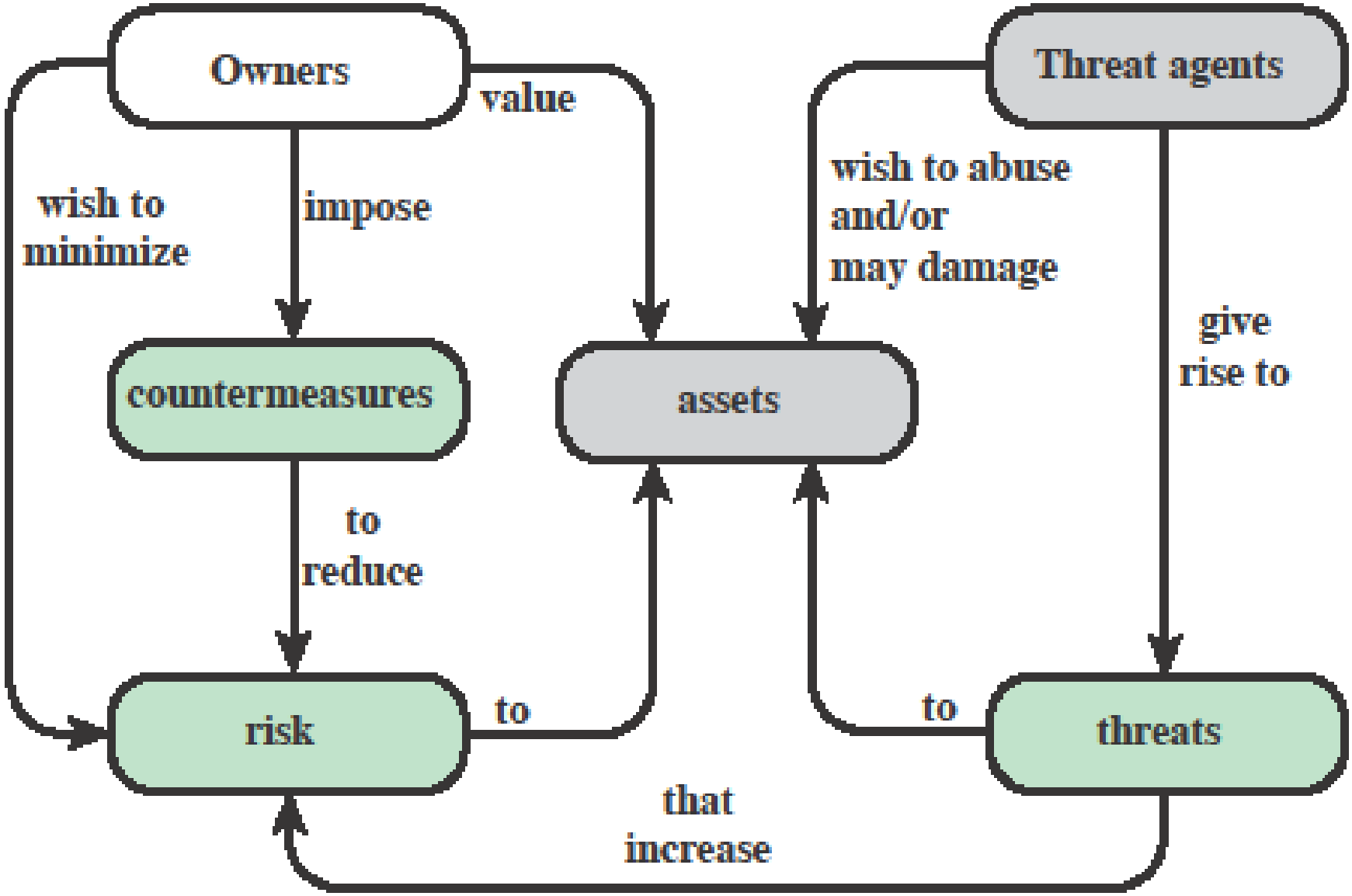
Computer Security Challenges

1. Computer security is not as simple as it might first appear to the novice
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features
3. Procedures used to provide particular services are often counterintuitive
4. Physical and logical placement needs to be determined
5. Security mechanisms typically involve more than a particular algorithm or protocol and also require that participants be in possession of some secret information which raises questions about the creation, distribution, and protection of that secret information
6. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security
7. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process
8. Security requires regular and constant monitoring
9. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs
10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

Vocabulary

- Adversary (threat agent)
- Attack
- Countermeasure
- Risk
- Security Policy
- System Resource (Asset)
- Threat
- Vulnerability

Source:
Computer Security Terminology, from RFC 2828, Internet Security Glossary, May 2000


Owners
value
Threat agents
wish to
minimize
impose
wish to abuse
and/or
may damage
give
rise to
countermeasures
assets
to
reduce
risk
to
to
threats
that
increase

Acronyms. What is the meaning of ?

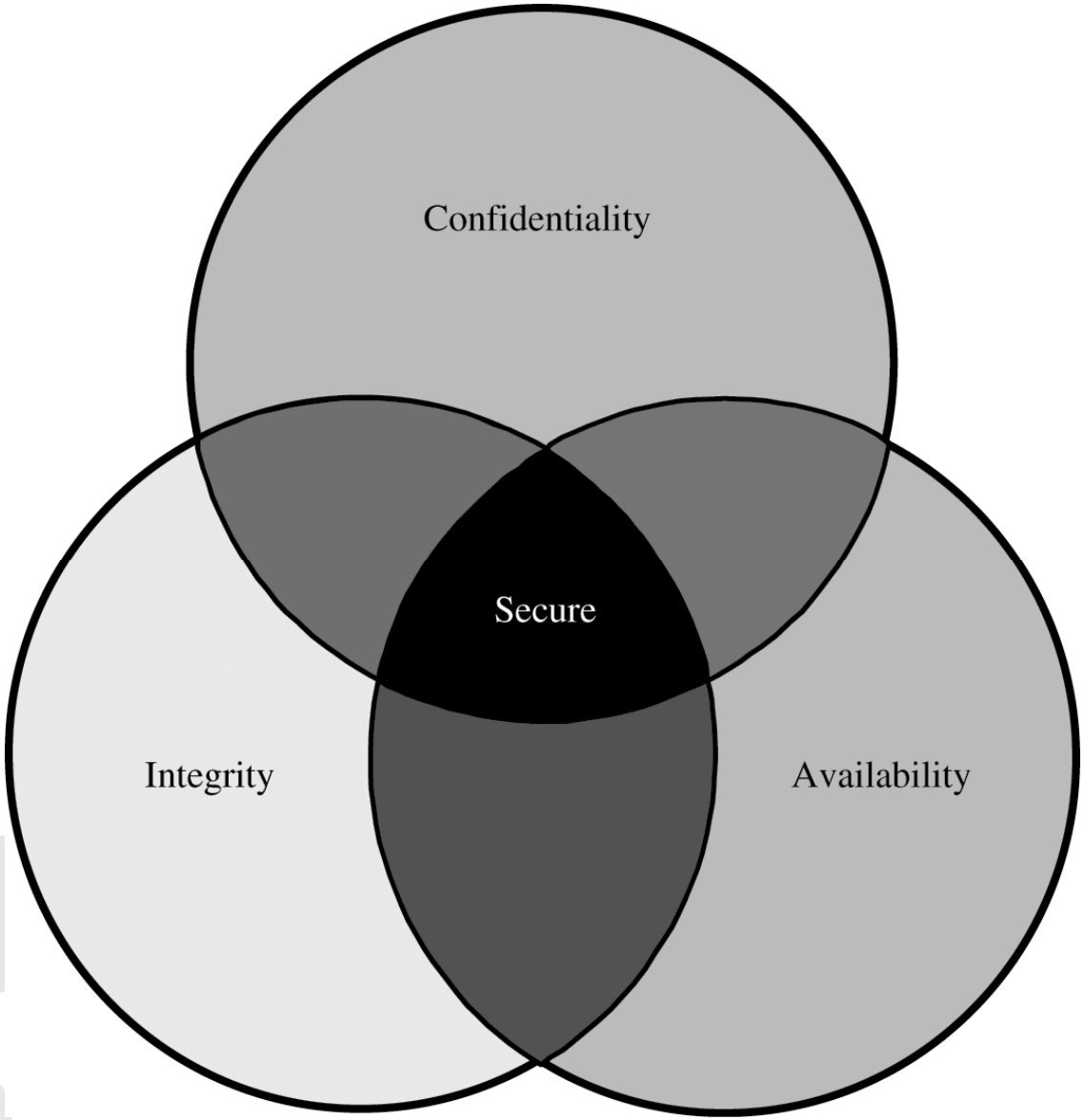
- RFC
- IETF
- NIST
- ISO
- FIPS
- DS
- TCP
- ISOC
- MD
- IEEE
- IP
- NSA
- ATM
- EFT
- POS
- PIN
- ITU
- PKI
- CIA
- DES
- SCADA
- AES
- KISS
- PGP
- ACM
- ECC
- RSA
- CA
- DDOS
- APT
- IAB
- ANSI

The NIST Internal/Interagency Report NISTIR 7298 (*Glossary of Key Information Security Terms* , May 2013) defines the term *computer security* as follows:

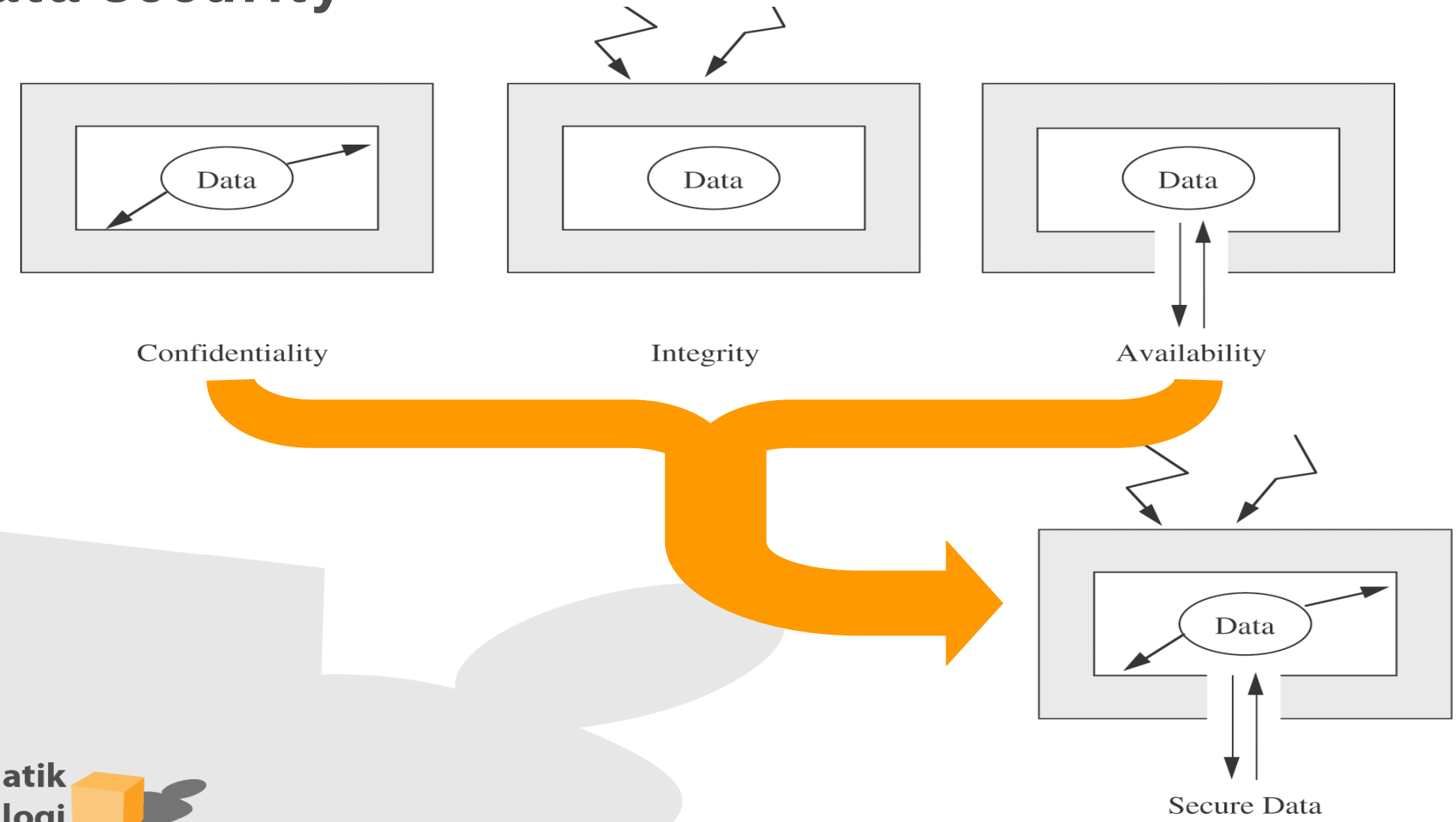
> " Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated."

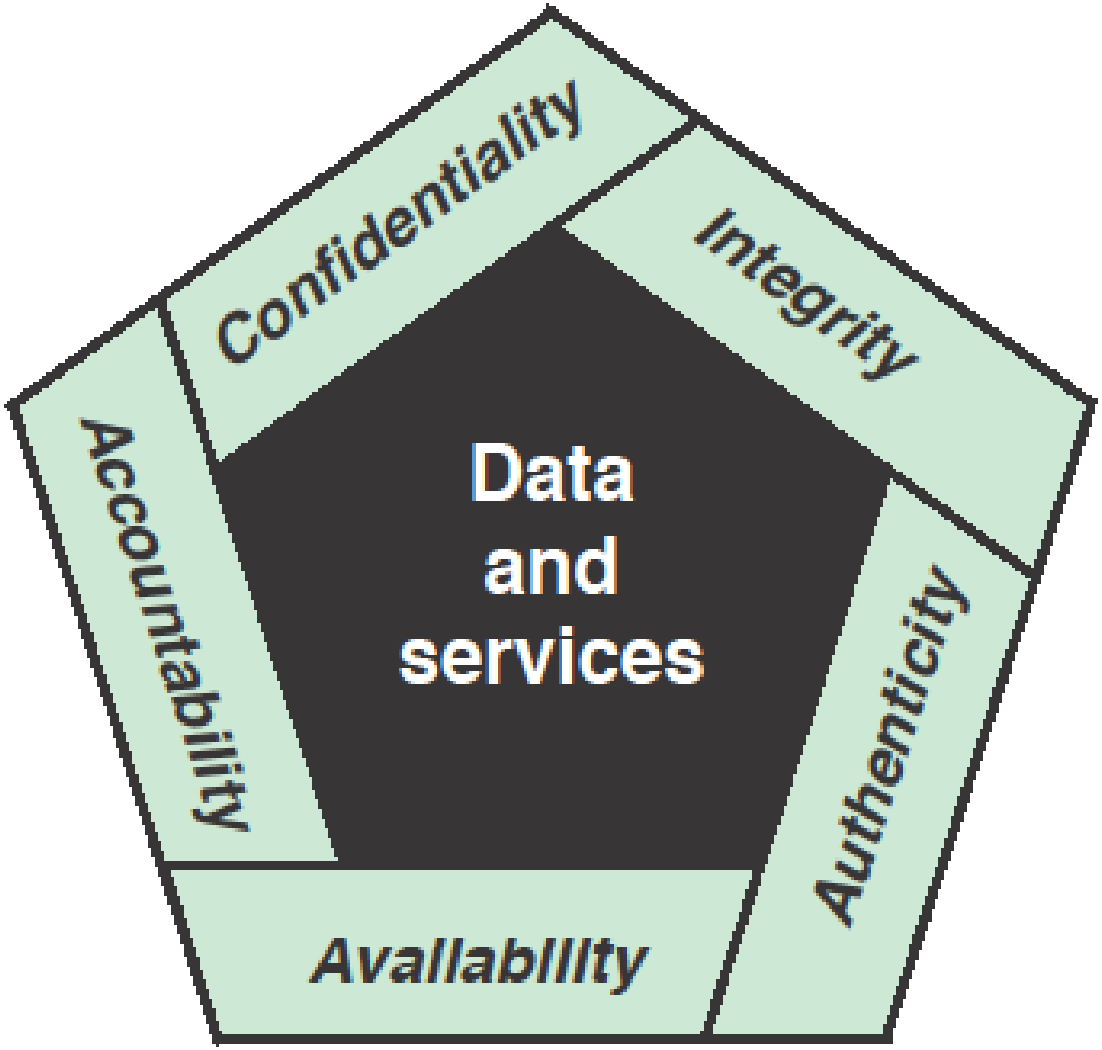
- **Confidentiality**
- **Integrity**
- **Availability**

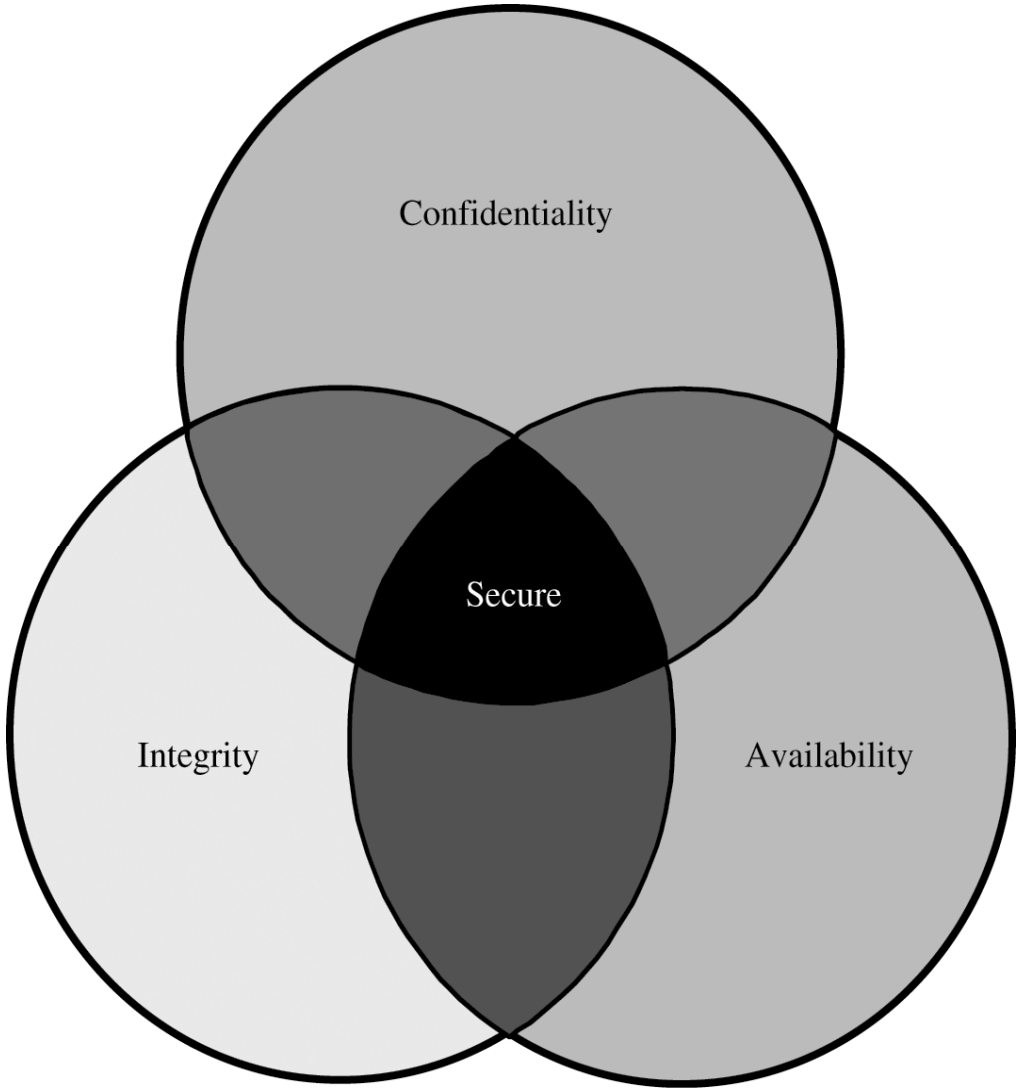
CIA



Data security




Confidentiality
Integrity
Accountability
Data and services
Authenticity
Availability


Confidentiality
Secure
Integrity
Availability

IT-security

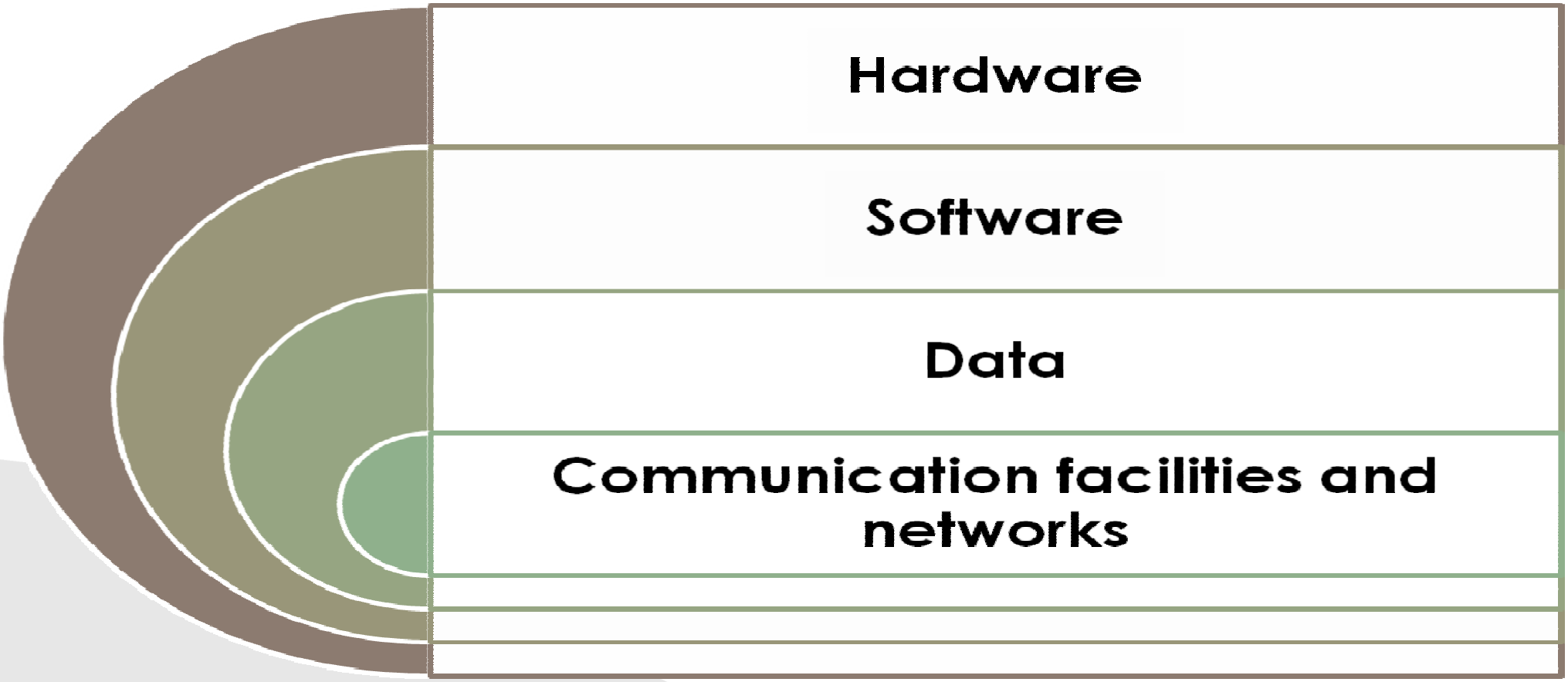
Prerequisite for this course:

Basic security vocabulary

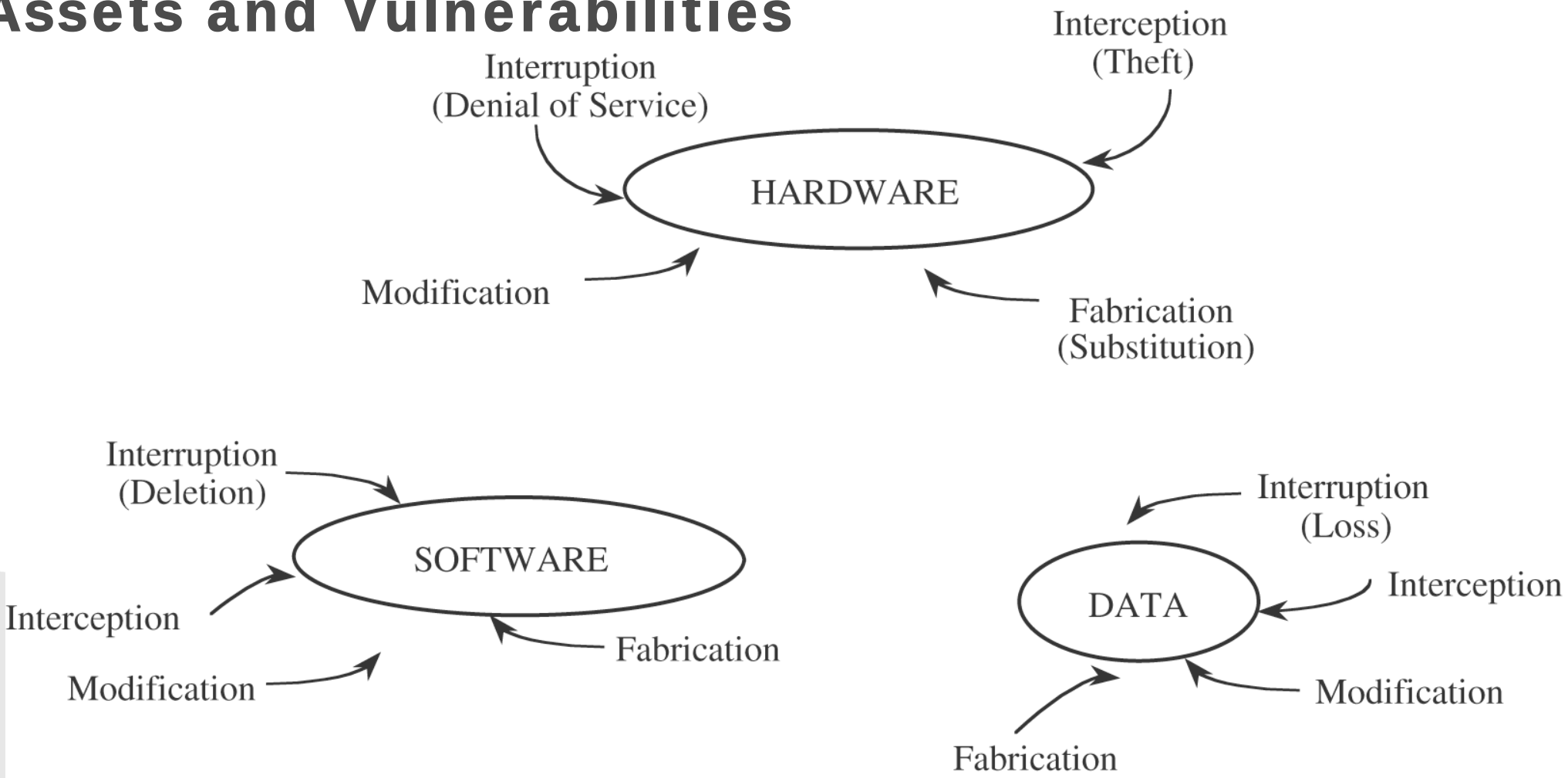
Based on Stallings & Brown, Chapter 1 (1.1-1.4 + 1.6-1.8)

1. Concepts
2. **Threats, Attacks, and Assets**
3. Functional Requirements
4. Design Principles
5. Management
6. Standards

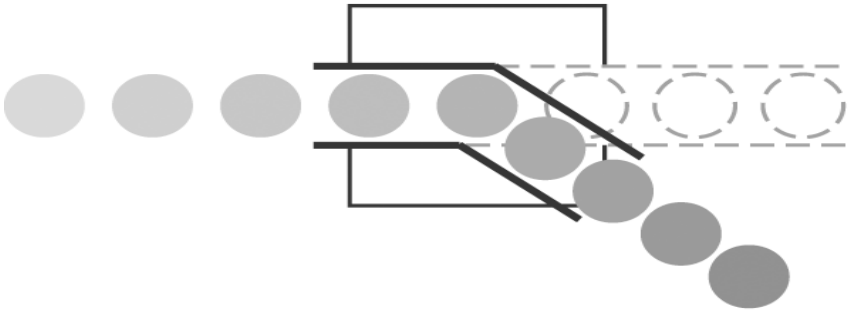
Assets of a Computer System



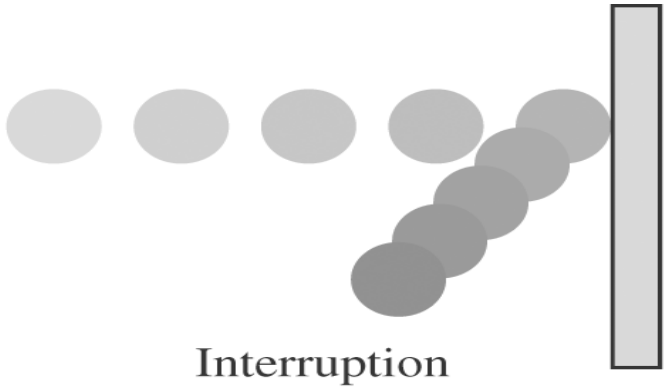
Assets and Vulnerabilities



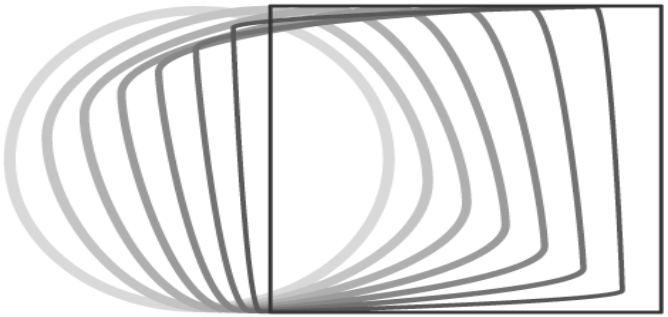
Attack types



Interception



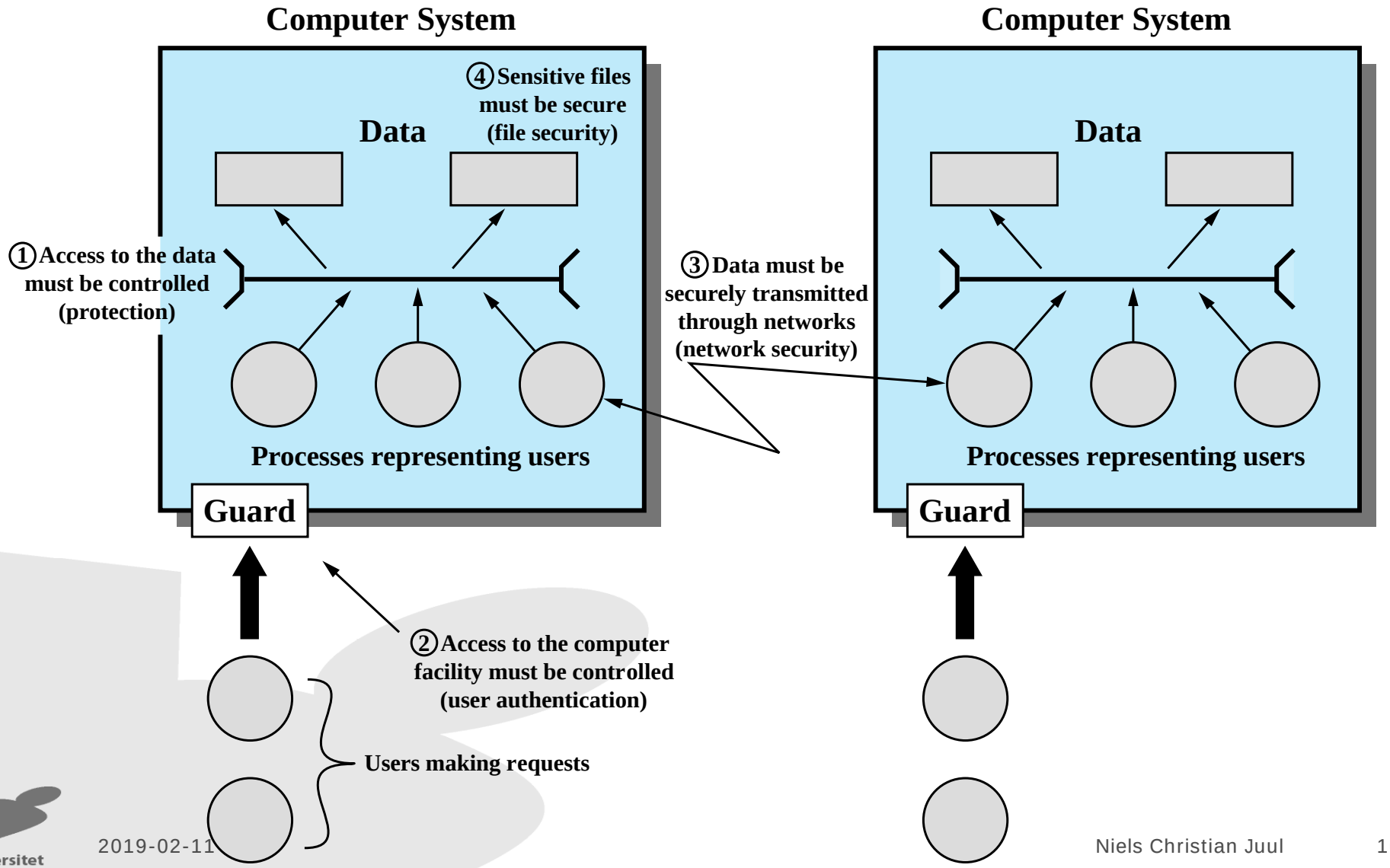
Interruption



Modification

Fabrication

Threats and computer assets



Choose your tools depending on the challenges

Different types of challenges:

- Organizational challenges
- Human challenges
- Technical challenges
- Physical challenges

Remember: The evil attacker

Essential ingredients:

- An attack **method**, including
  - Knowledge, tools, education,...
- An **opportunity**, including
  - Time and access
- A **motive**,
  - A reason to attach this system

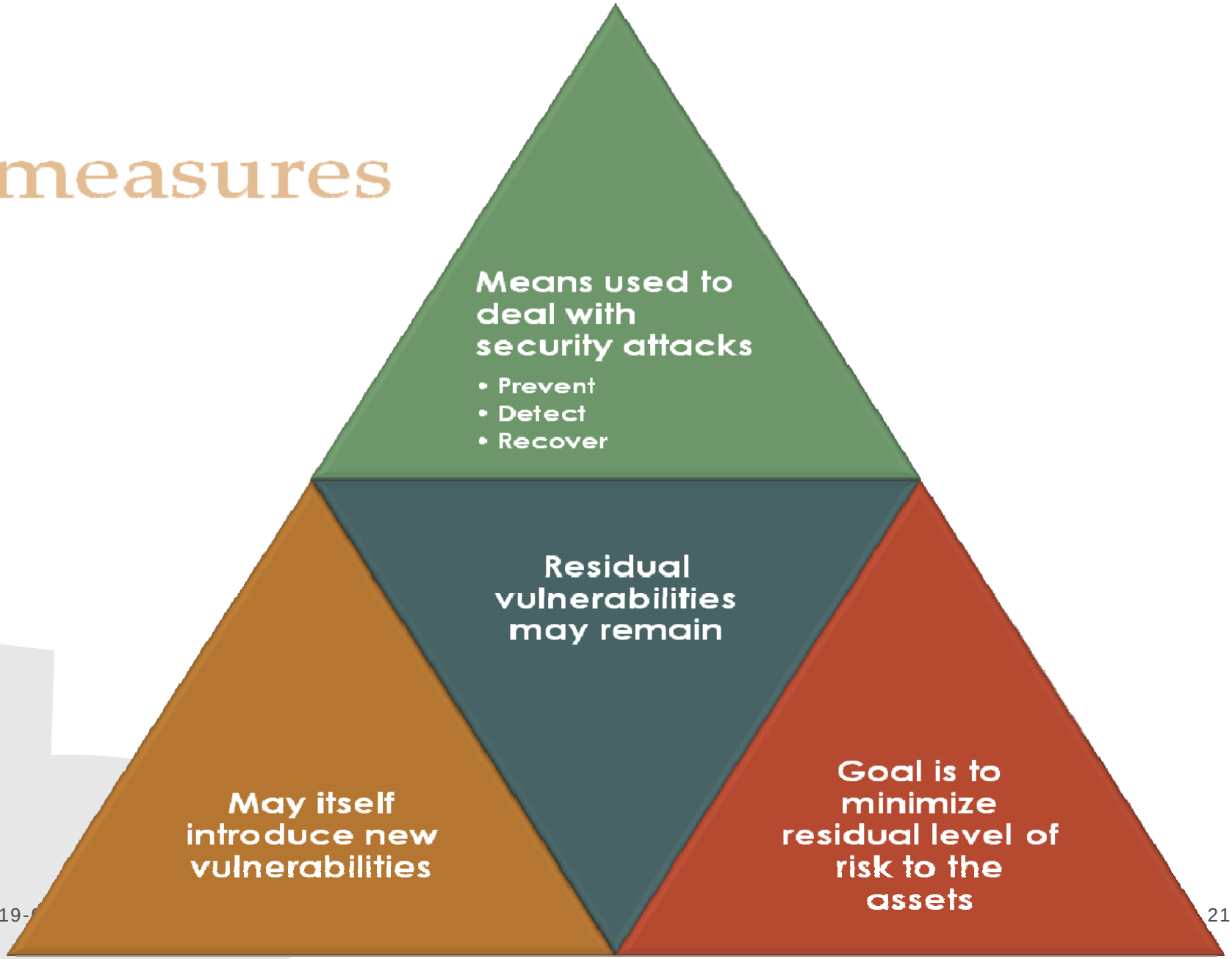
Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)
- Threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Attacks (threats carried out)
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security parameter
  - Outsider – initiated from outside the perimeter

Threat Consequences and Threat Actions

- Unauthorized disclosure
  - Exposure
  - Interception
  - Inference
  - Intrusion
- Deception
  - Masquerade
  - Falsification
  - Repudiation
- Disruption
  - Incapacitation
  - Corruption
  - Obstruction
- Usurpation
  - Misappropriation
  - Misuse

Countermeasures



Passive and Active Attacks

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

IT-security

Prerequisite for this course:

Basic security vocabulary

Based on Stallings & Brown, Chapter 1 (1.1-1.4 + 1.6-1.8)

1. Concepts
2. Threats, Attacks, and Assets
3. **Functional Requirements**
4. Design Principles
5. Management
6. Standards

Security Requirements (1)

- Access control
- Awareness and training
- Audit and accountability
- Certification, accreditation, and security assessments
- Configuration management
- Contingency planning
- Identification and authentication
- Incident response
- Maintenance

Security Requirements (2)

- Media protection
- Physical and environmental protection
- Planning
- Personnel security
- Risk assessment
- Systems and services acquisition
- System and communications protection
- System and information integrity

IT-security

Prerequisite for this course:

Basic security vocabulary

Based on Stallings & Brown, Chapter 1 (1.1-1.4 + 1.6-1.8)

1. Concepts
2. Threats, Attacks, and Assets
3. Functional Requirements
4. **Design Principles**
5. Management
6. Standards

Fundamental Security Design Principles

Economy of mechanism	Fail-safe defaults	Complete mediation	Open design
Separation of privilege	Least privilege	Least common mechanism	Psychological acceptability
Isolation	Encapsulation	Modularity	Layering
	Least astonishment		

is this new?

Really old stuff – but still valid

- Saltzer, Jerome H. & Schroeder, Michael D. "The Protection of Information in Computer Systems," 1278-1308. *Proceedings of the IEEE 63,* 9 (September 1975).
- The paper is available on the web here http://www.cs.virginia.edu/~evans/cs551/saltzer/

- Old examples based on old technology (>40Y) but amazing how the principles last

Two times Thirteen security design principles

1. Economize mechanism
2. Fail safe defaults
3. Complete mediation
4. Open design
5. Separation of privileges
6. Least privilege
7. Least common mechanisms
8. Psychological acceptability
9. Isolation
10. Encapsulation
11. Modularity
12. Layering
13. Least astonishment

Stallings & Brown, 2018

1. Secure the weakest link
2. Defend in depth
3. Fail securely
4. Grant least privilege
5. Separate privileges
6. Economize mechanism
7. Do not share mechanisms
8. Be reluctant to trust
9. Assume your secrets are not safe
10. Mediate completely
11. Make security usable
12. Promote privacy
13. Use your resources

Saltzer & Schroeder, 1975

Another set of Recognized Security Principles

1. Grant least privilege
2. Secure the weakest link
3. Defend in depth
4. Separate privileges
5. KISS
6. Don't rely on obscurity
7. Use secure defaults
8. Fail securely
9. Assume externals are untrusted
10. Audit sensitive events

BUITA:
Rozanski&Woods, Ch. 25

IT-security

Prerequisite for this course:

Basic security vocabulary

Based on Stallings & Brown, Chapter 1 (1.1-1.4 + 1.6-1.8)

1. Concepts
2. Threats, Attacks, and Assets
3. Functional Requirements
4. Design Principles
5. **Management**
6. Standards

Security differs

- Case by case

- No such thing as ***absolute secure or not***

rather:

- Security is ***risk management***
  i.e. balancing security risks against cost of guarding against them or coping with the incident afterwards

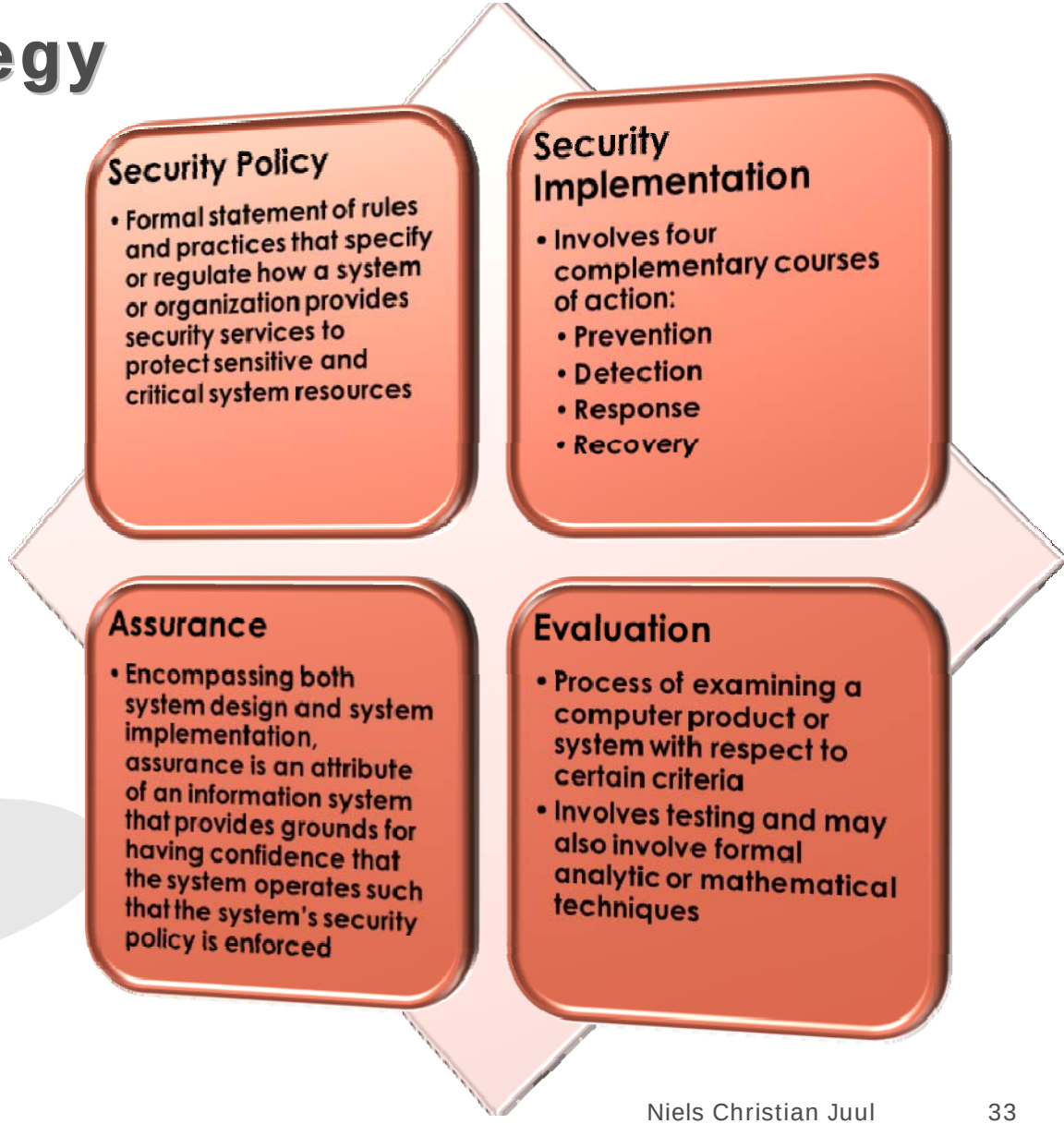
  Tradeoffs

Computer Security Strategy

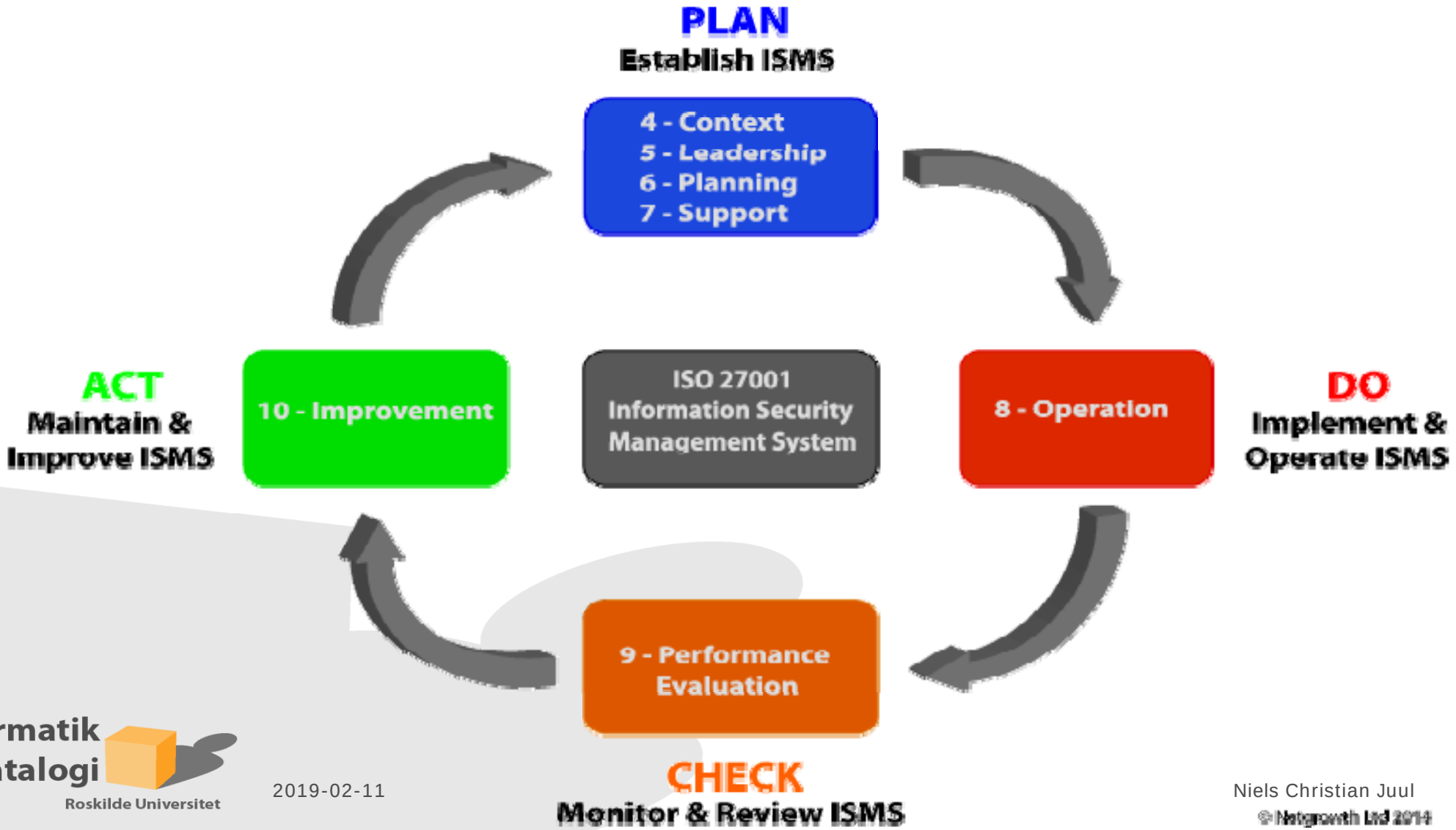
Please consider for each:

- Who is responsible?
- Who does the work?

and prepare your arguments!



Information Security Management System



Working with Information Security

- Security Policy,
- Threats (consequences and likelihood),
- Risk analysis,
- Prevention
- Security planning (BCP, DRP,...)
- Security organization.

- In Denmark, based on standards like the ISO 27000 series (formerly DS-484).

IT-security

Prerequisite for this course:

Basic security vocabulary

Based on Stallings & Brown, Chapter 1 (1.1-1.4 + 1.6-1.8)

1. Concepts
2. Threats, Attacks, and Assets
3. Functional Requirements
4. Design Principles
5. Management
6. **Standards**

Information security

- DS 484 - ISO 17799 - or the British BS xxx
- Sarbanne-Oxley Act
- EuroSOX
- COBIT,...

- Now ISO 27000 series
  - 27001

https://en.digst.dk/policy-and-strategy/information-security/standard-for-information-security/

Policy and strategy

Digital Strategy

Cutting red tape in Denmark

Mandatory digitisation

Digital welfare

Open government

Information security

Privacy

Standard for information security

Strategy for ICT management

Danish Cyber and Information Security Strategy

Standard for information security

Since January 2014 all government institutions in Denmark must follow the international standard for Information Security ISO/IEC 27001.

In 2010, the Danish government decided that government institutions must follow the international standard, ISO/IEC 27001, when an update and a translation into danish of the standard had been completed. The update was published in January 2014 therefore ISO/IEC 27001 now has replaced DS 484 as the national standard for information security management.

DS 484 was previously the security standard in government institutions and was based on the international standard ISO/IEC 27002 "Code of practice for information security management", modified to suit Danish conditions. With the introduction of this standard, IT security management in all ministerial areas was structured according to a common concept.

Activities to develop, maintain and inform users about the requirements of the standard are handled by the Ministry of Finance, represented by the Agency for Digitisation, in collaboration with other authorities in the public sector.

Contact

Eskil Sørensen

ess@digst.dk
+45 3392 8749

Standards

- Standards have been developed to cover management practices and the overall architecture of security mechanisms and services
- The most important of these organizations are:
  - **National Institute of Standards and Technology (NIST)**
    - **NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation**
  - **Internet Society (ISOC)**
    - **ISOC is a professional membership society that provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards**
  - **International Telecommunication Union (ITU-T)**
    - **ITU is a United Nations agency in which governments and the private sector coordinate global telecom networks and services**
  - **International Organization for Standardization (ISO)**
    - **ISO is a nongovernmental organization whose work results in international agreements that are published as International Standards**

IT-security

Prerequisite for this course:

Basic security vocabulary

Based on Stallings & Brown, Chapter 1 (1.1-1.4 + 1.6-1.8)

1. Concepts
2. Threats, Attacks, and Assets
3. Functional Requirements
4. Design Principles
5. Management
6. Standards

Summary

- Computer security concepts
  - Definition
  - Challenges
  - Model
- Threats, attacks, and assets
  - Threats and attacks
  - Threats and assets
- Security functional requirements
- Fundamental security design principles
- Computer security strategy
  - Security policy
  - Security implementation
  - Assurance and evaluation
- Standards