Introduction and Basic Concepts

Introduction to Computer Security

Naercio Magaia and Imran Khan

Contents

- Module Introduction
- Module Overview
- Computer Systems
  - Hardware
  - Operating Systems and Applications
  - Networks and Enterprise computing
- Key Security Concepts
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability
- Vulnerabilities, Threats and Attacks
- Countermeasures

Teachers

- Tutors

  Naercio Magaia

  - Lectures convenor
  - Office: Chichester 2 building, Room 2R220
  - Email: N.Magaia@sussex.ac.uk
  - Office Hours: Tuesdays 10:00 – 11:00 (on Microsoft Teams and in-person). Please email me first.

  Imran Khan

  - Labs convenor
  - Office: Chichester 2 building, Room 2R302 (on top of the Chichester Road Bridge)
  - Email: imran.khan@sussex.ac.uk
  - Office Hours: Thursdays from 11:00 to 13:00. Please email me first.

- TAs

  Ziqi Yan

  - Email: zy203@sussex.ac.uk
  - Office Hours: by email only.

  Bo Wang

  - Email: bw268@sussex.ac.uk
  - Office Hours: by email only.

Teaching Sessions

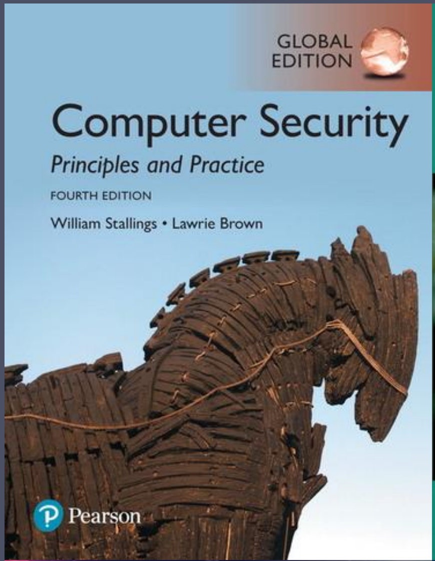
- Lectures
    - Monday (CHICH 1-LT) 10:00 - 11:00
    - Wednesday (CHICH 1-LT) 10:00 - 11:00
- Labs
    - Monday, CHI 014/015
        - 11:00 - 13:00
    - Thursday, CHI 014/015
        - 10:00 - 12:00
        - 15:00 – 17:00
    - Friday, CHI 014/015
        - 13:00 - 15:00

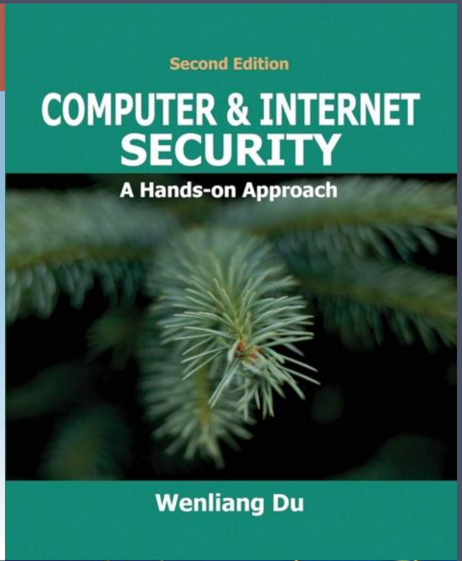
Module Assessment

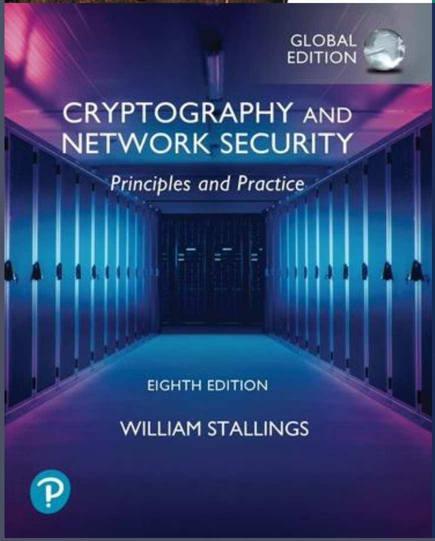
- Coursework (50% of total module marks)
  - Coursework will build on the labs, to be released later in the term
  - Due date: Week 11
- Exam (50% of total module marks)
  - Exam can draw from any of the material in the lectures or the labs
  - Due Date: TBA
- Ensure to always double-check assessment deadlines in Sussex Direct and Canvas.

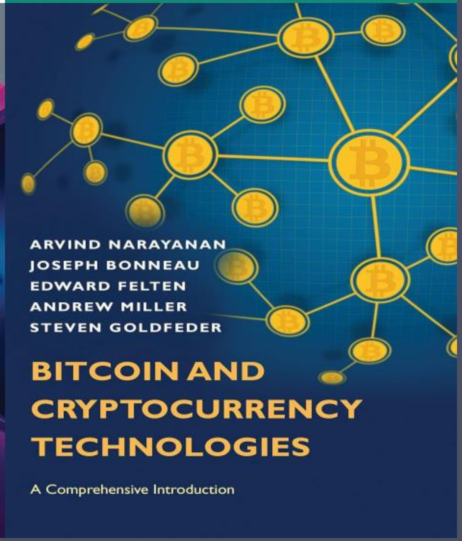
Readings

- Readings are on Canvas and the module reading list as eBooks and physical books:
  - **Computer security: principles and practice, Stallings and Brown, 2018**
  - **Computer & internet security: a hands-on approach, Wenliang Du, 2019**
  - **Cryptography and Network Security: Principles and Practice, William Stallings, 2022**
  - **Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Narayanan et al., 2016**
- The module draws upon much of the supplied material from these books









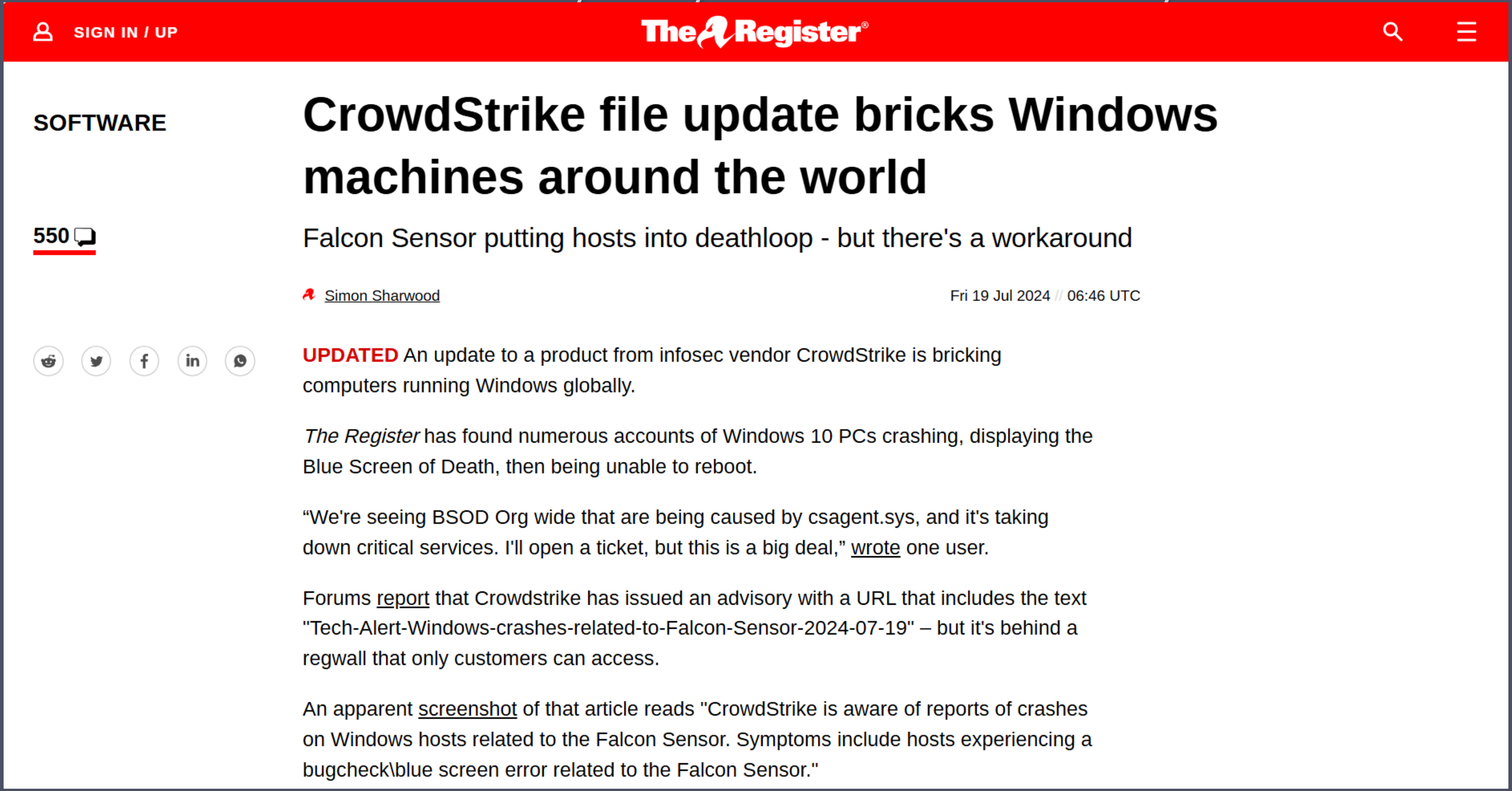
Module Overview: Lectures

1. Introduction
2. Technologies
3. Symmetric Cryptography – Hash Functions and AES
4. Public Key Cryptography
5. User Authentication
6. Access Control
7. Database Security
8. Malicious Software
9. Software Exploits
10. Secure Web
11. DoS Attacks
12. Firewalls
13. Intrusion Detection
14. Cloud and IoT Security
15. IT Security
16. Attack Analysis
17. Legal Framework
18. Cryptocurrency and Quantum Cryptography

Module Overview: Labs

1. Technologies lab: Linux and Amazon Web Services
2. Technologies lab and case study
3. Cryptography (Symmetric and Asymmetric)
4. Hashing
5. SQL Injection
6. Buffer overflow
7. Cross Site Scripting (XSS) attack
8. Cross-Site Request Forgery (CSRF) attack
9. Firewalls
10. Cloud security and fundamentals
11. Ethical Hacking

Your weekly cybersecurity hack



CrowdStrike file update bricks Windows machines around the world

Falcon Sensor putting hosts into deathloop - but there's a workaround

Simon Sharwood Fri 19 Jul 2024 // 06:46 UTC

UPDATED An update to a product from infosec vendor CrowdStrike is bricking computers running Windows globally.

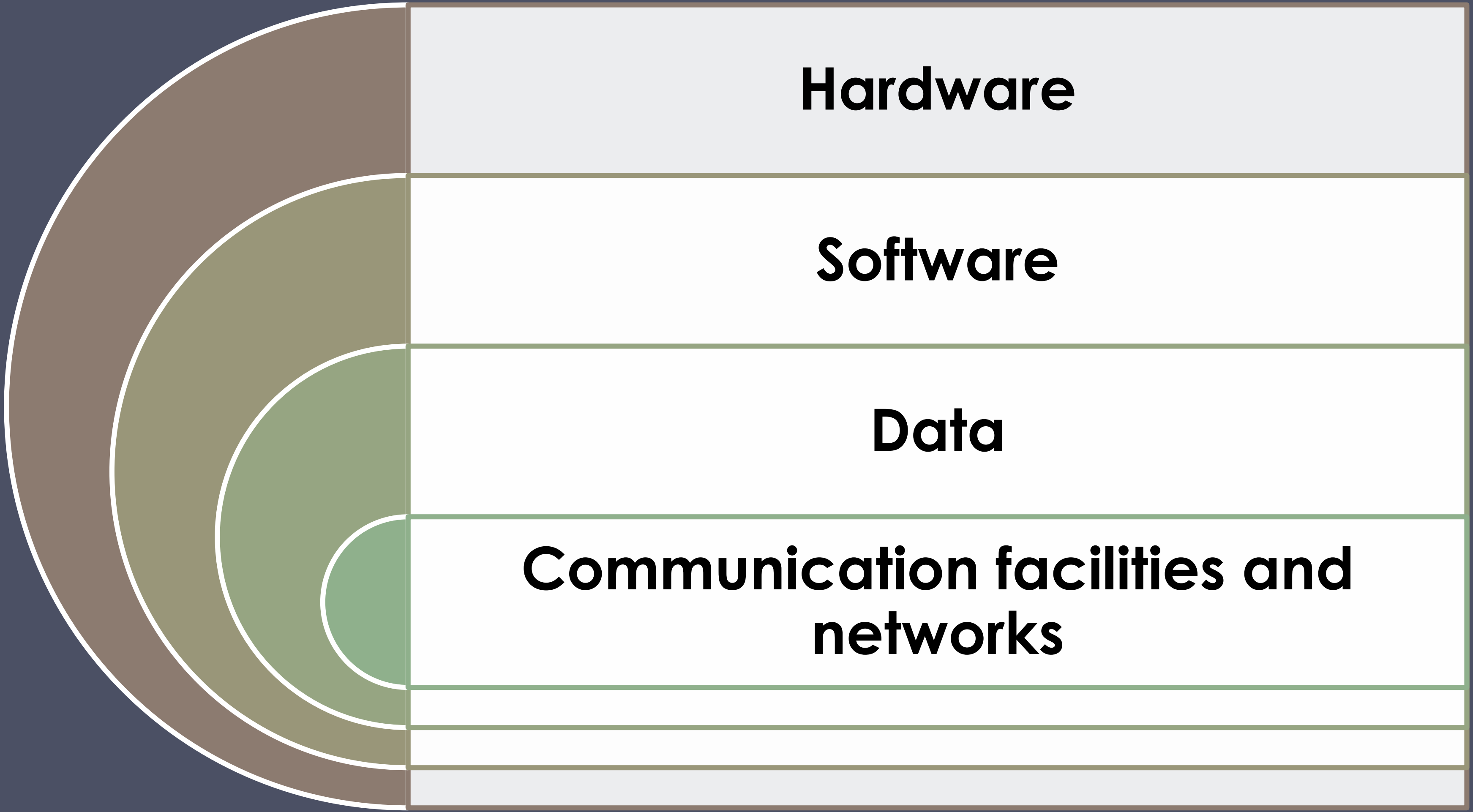
The Register has found numerous accounts of Windows 10 PCs crashing, displaying the Blue Screen of Death, then being unable to reboot.

“We're seeing BSOD Org wide that are being caused by csagent.sys, and it's taking down critical services. I'll open a ticket, but this is a big deal,” wrote one user.

Forums report that Crowdstrike has issued an advisory with a URL that includes the text "Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19" – but it's behind a regwall that only customers can access.

An apparent screenshot of that article reads "CrowdStrike is aware of reports of crashes on Windows hosts related to the Falcon Sensor. Symptoms include hosts experiencing a bugcheck\blue screen error related to the Falcon Sensor."

Assets of a Computer System



Hardware

Software

Data

Communication facilities and networks

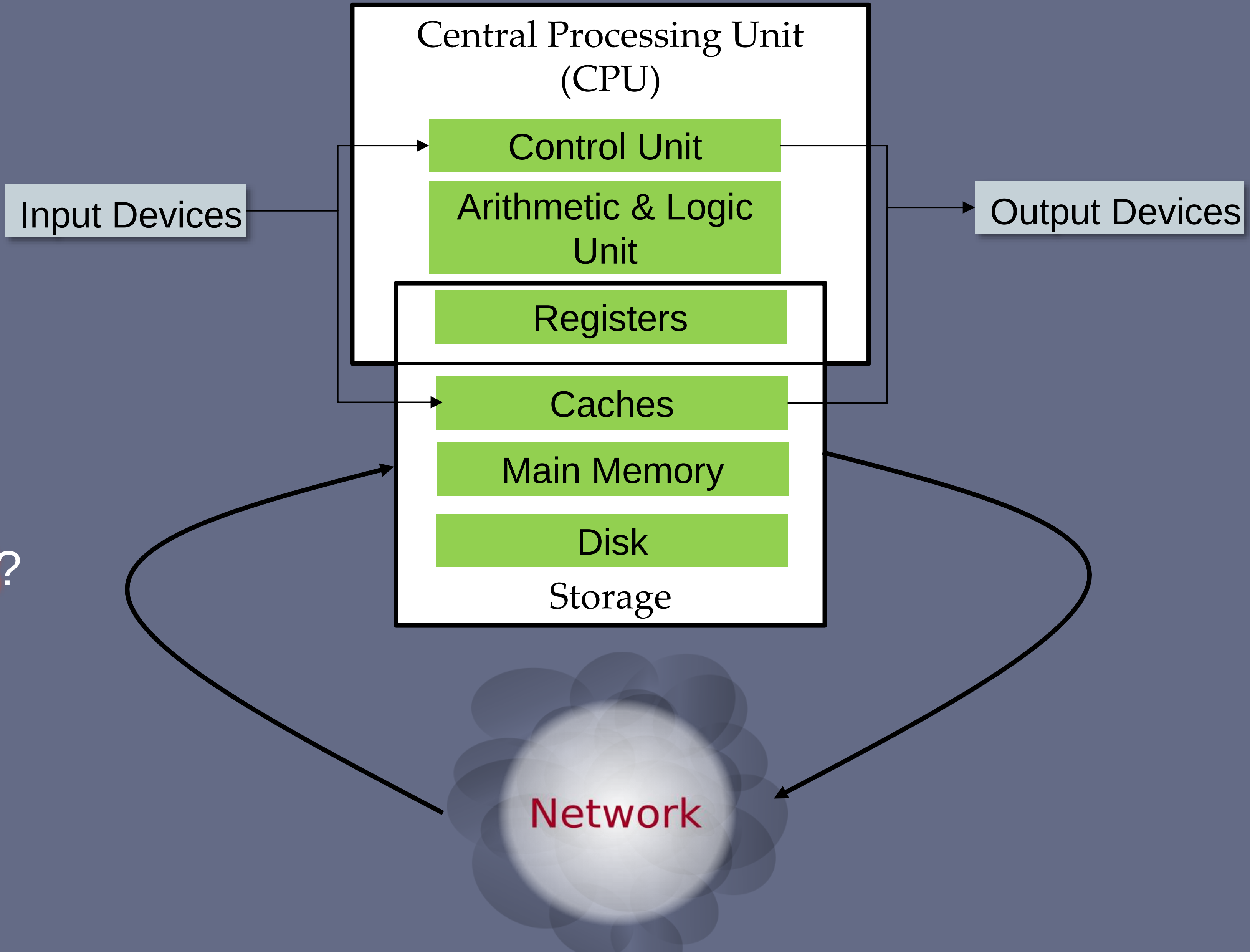
Computer Attack Possibilities

How can an attacker…

Eavesdrop?

Corrupt or disrupt?

Control?



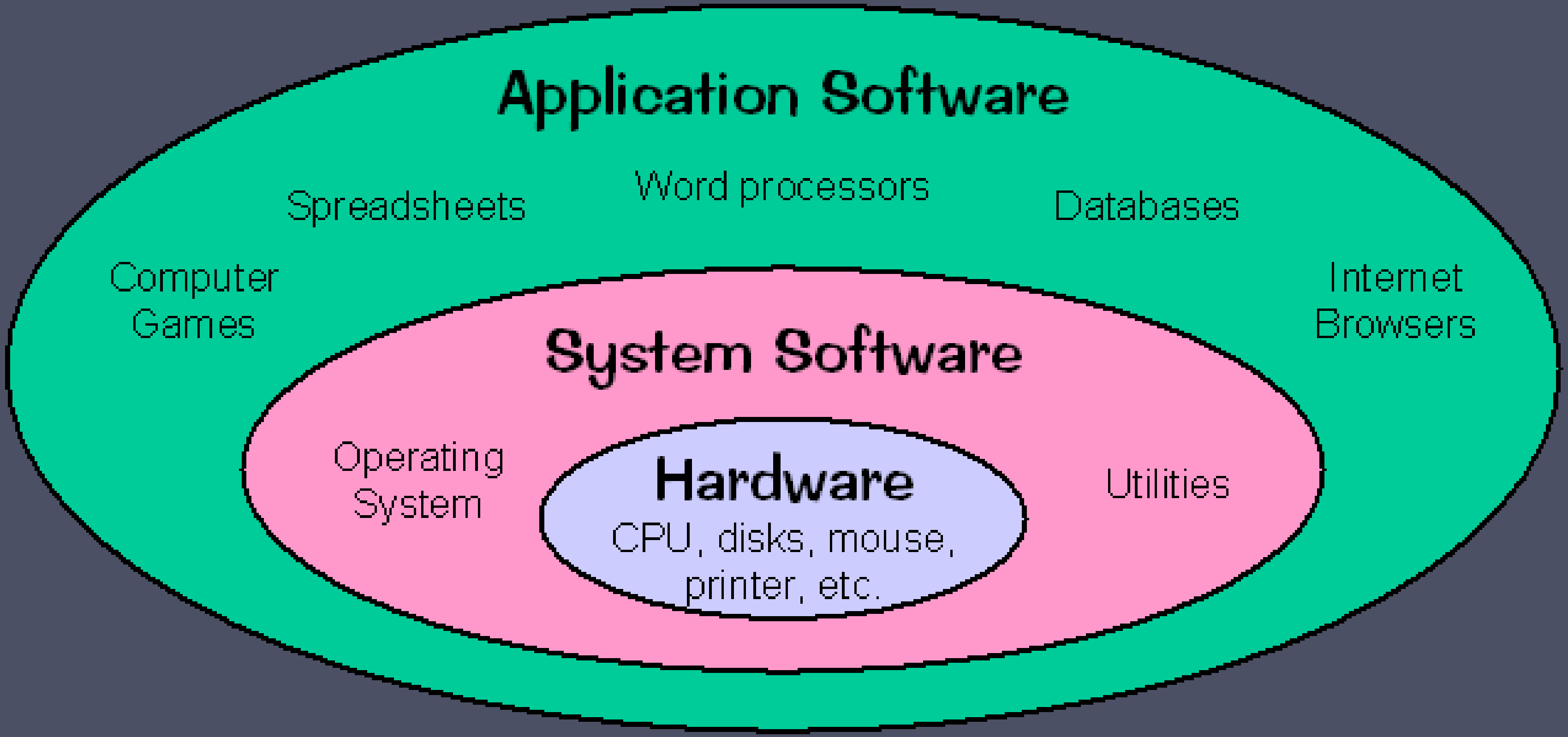
System Software Attack Possibilities

How can an attacker…

Eavesdrop?

Corrupt or disrupt?

Control?



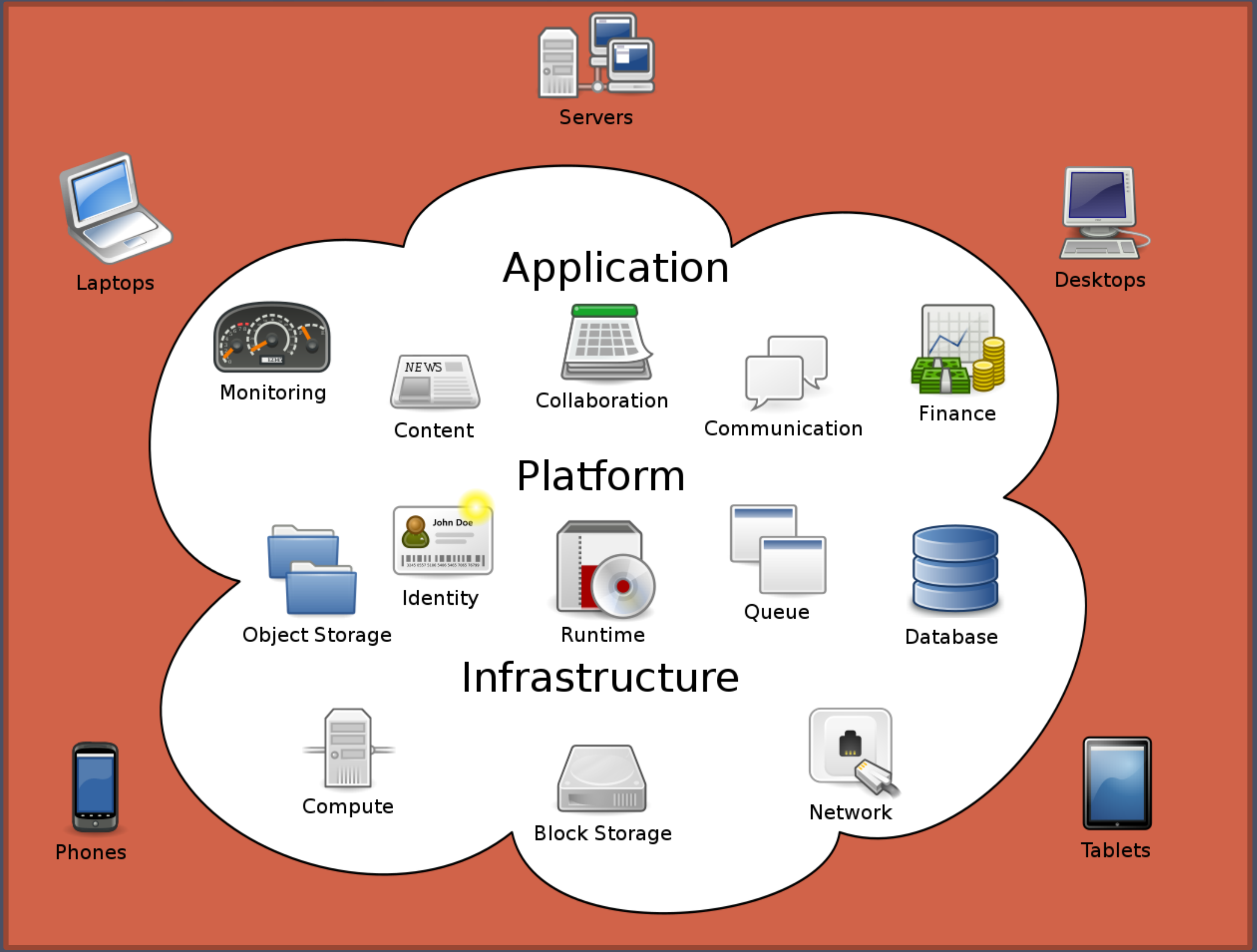
Enterprise System Attack Possibilities

How can an attacker…

Eavesdrop?

Corrupt or disrupt?

Control?



Key Security Concepts (1/2)

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Availability

- Ensuring timely and reliable access to and use of information

Key Security Concepts (2/2)

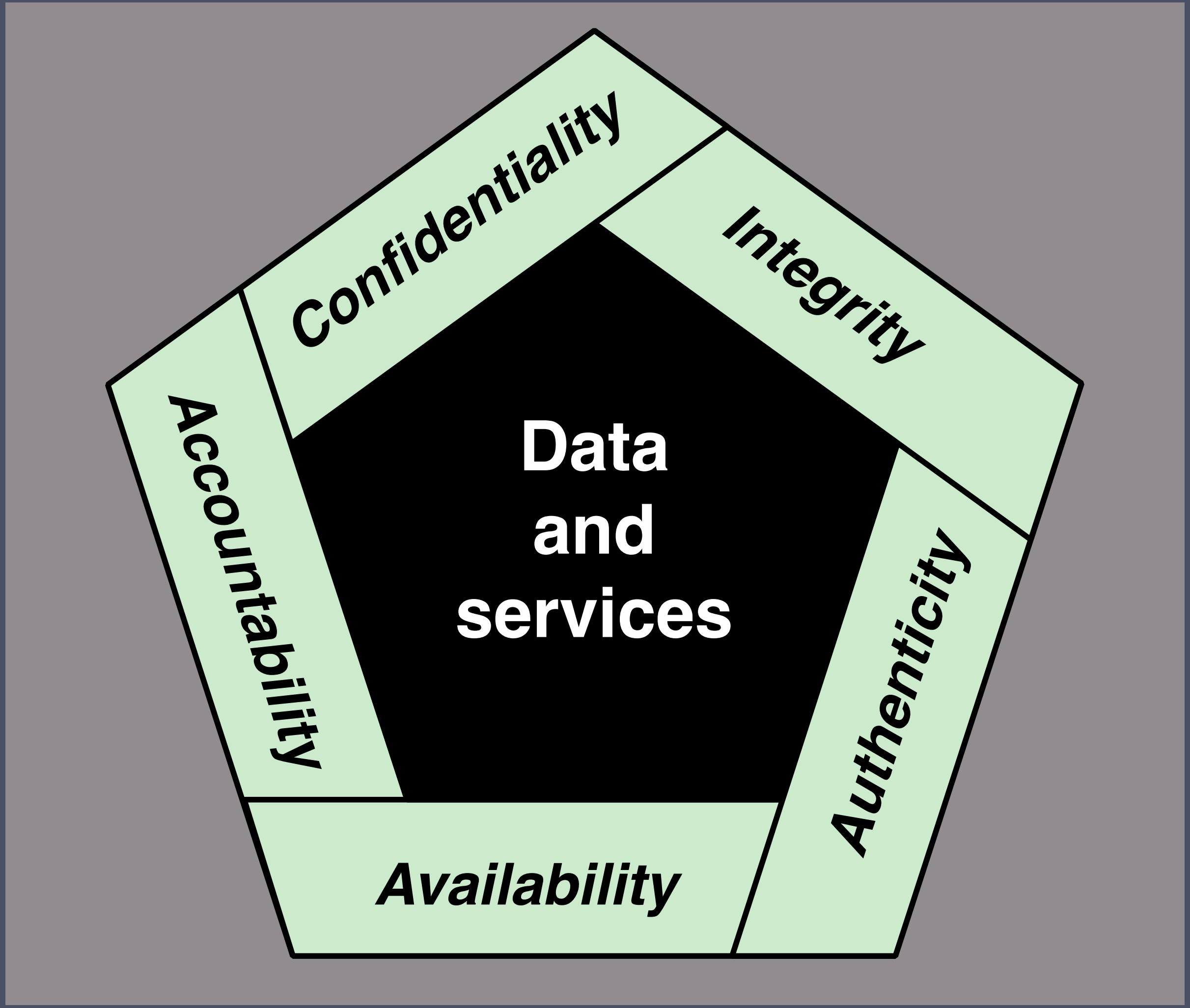
Authenticity

- The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, message or message originator. Requires verifying users checking the origin of each input

Accountability

- Providing the capability of actions being traced to their originator. Supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention. Records are kept to provide post-attack analysis and meet legal requirements

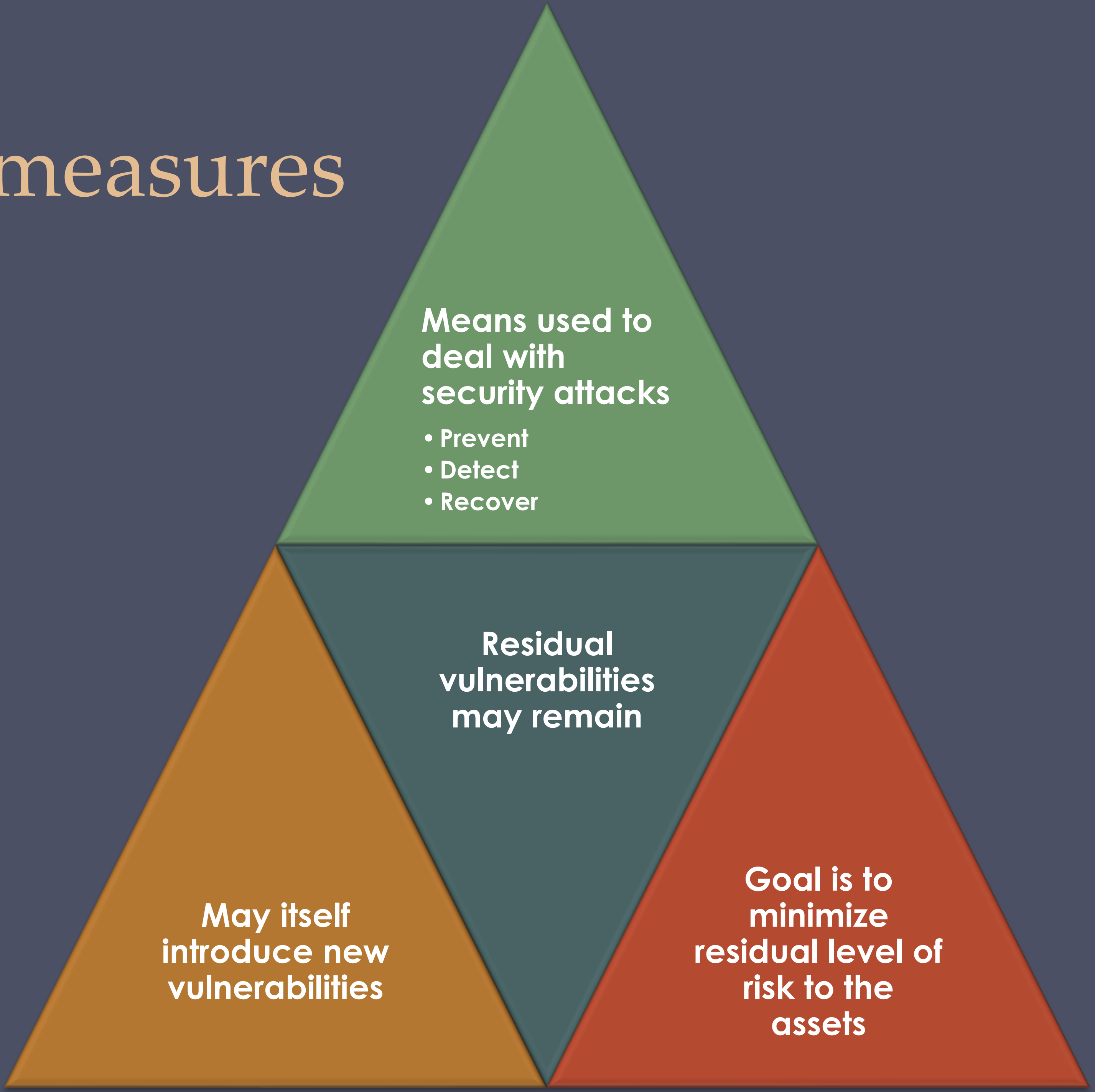
Essential Network and Computer Security Requirements



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

Countermeasures



Means used to deal with security attacks

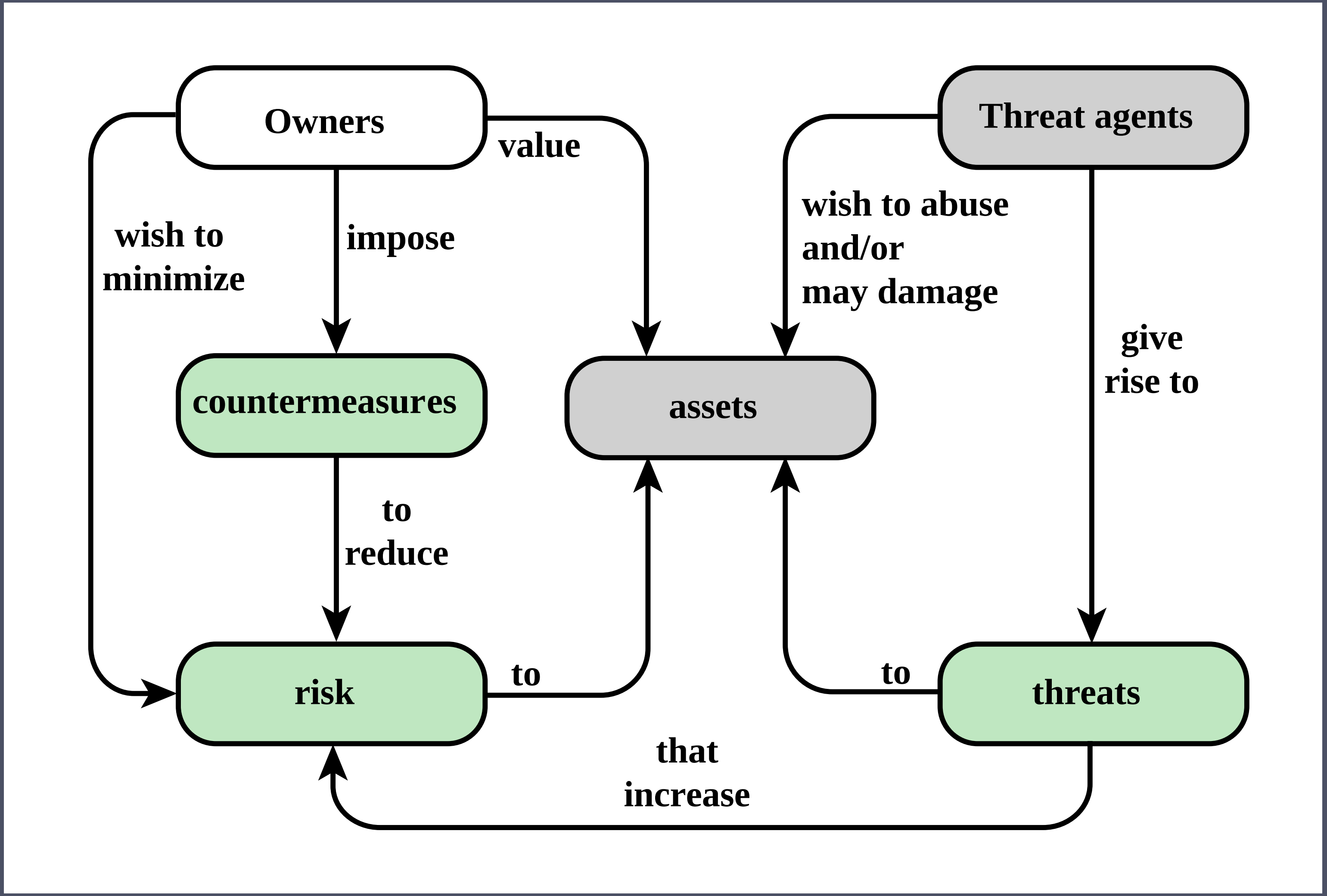
- Prevent
- Detect
- Recover

Residual vulnerabilities may remain

May itself introduce new vulnerabilities

Goal is to minimize residual level of risk to the assets

Security Concepts and Relationships



Conclusion

- Do read and ensure you understand the definitions above