

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 2R211
- Email: N.Magaia@sussex.ac.uk
- Office Hours: Tuesdays 15:30 – 16:30 (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: Wednesday from 10:00 to 12:00. 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
 - Tuesday (Arts A A02) 13:00 - 14:00
 - Thursday (Arts A A02) 10:00 - 11:00
- Labs
 - Wednesday, CHI 015
 - 11:00 - 13:00
 - Thursday, CHI 017/018
 - 13:00 - 15:00
 - Friday, CHI 017/018
 - 13:00 - 15:00
 - 15:00 - 17:00

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



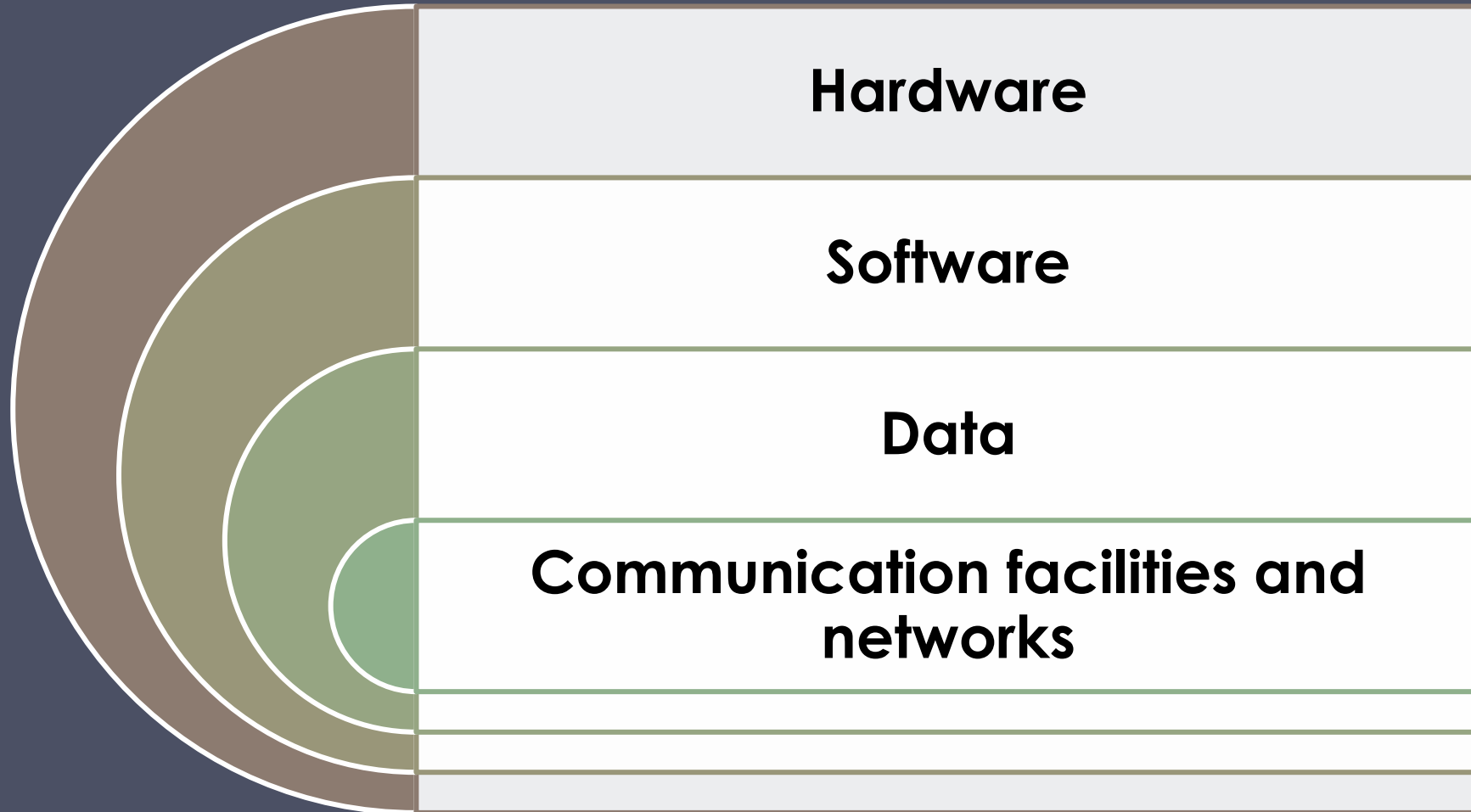
Module Overview: Lectures

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

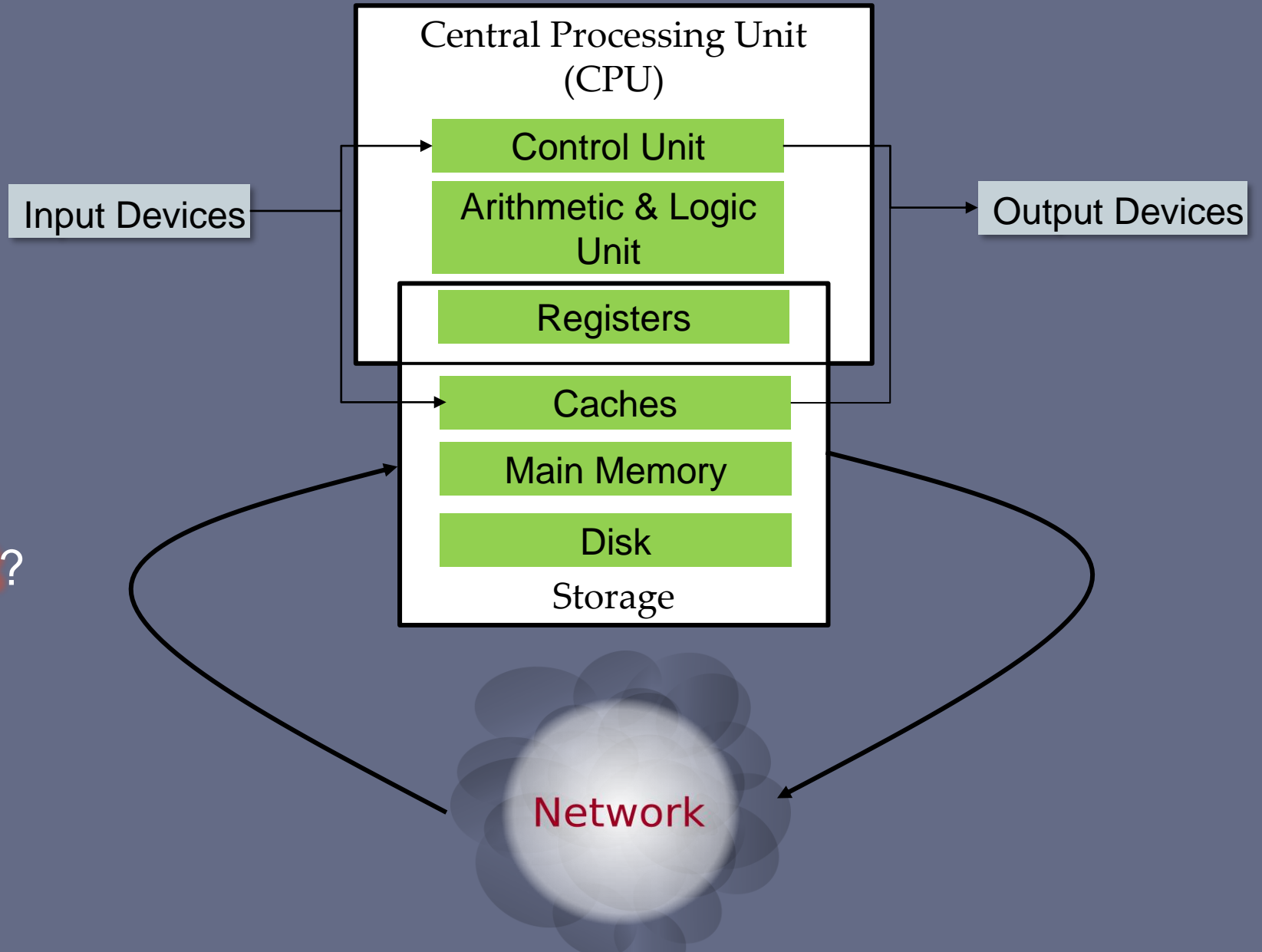
Module Overview: Labs

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

Assets of a Computer System



Computer Attack Possibilities



How can an attacker...

Eavesdrop?

Corrupt or disrupt?

Control?

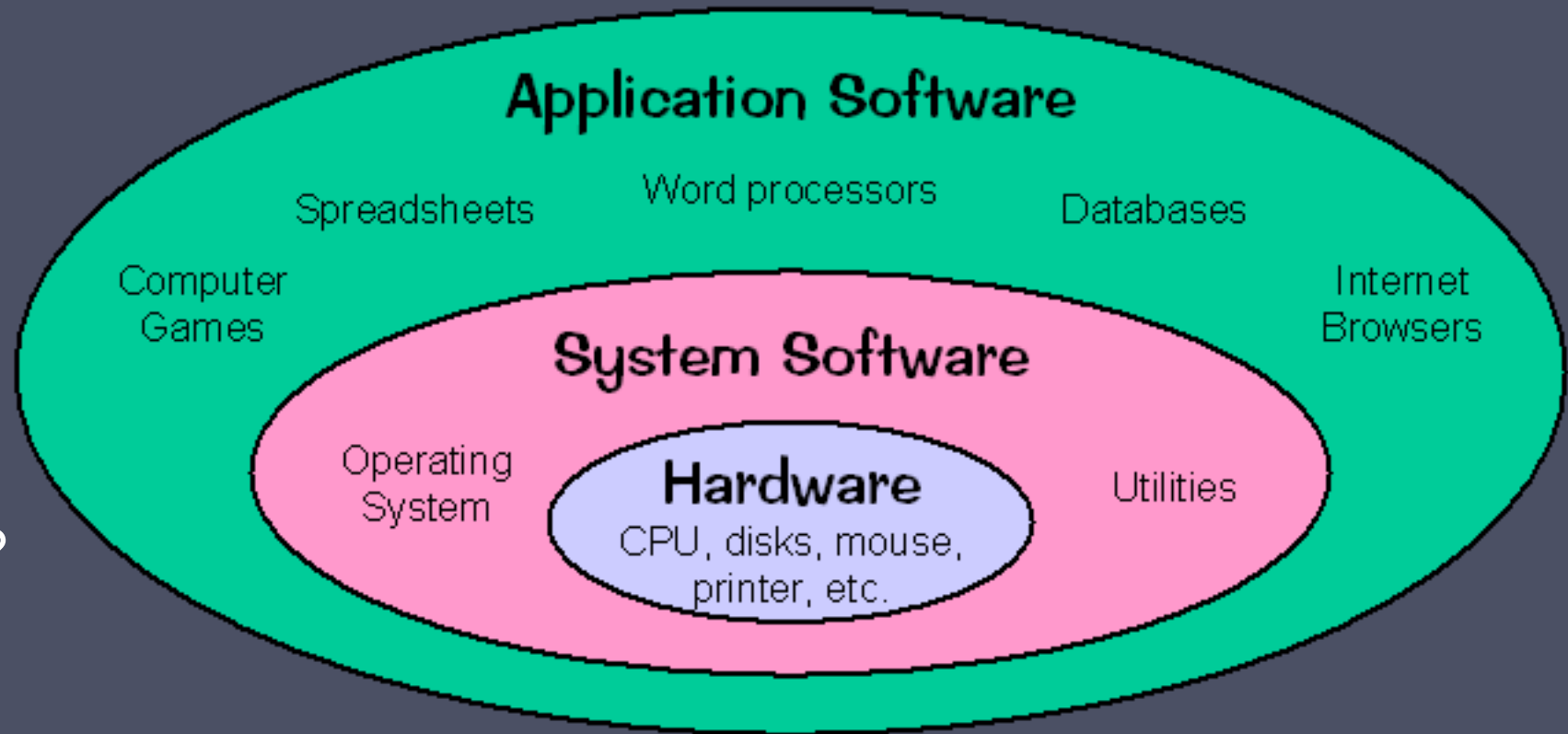
System Software Attack Possibilities

How can an attacker...

Eavesdrop?

Corrupt or disrupt?

Control?



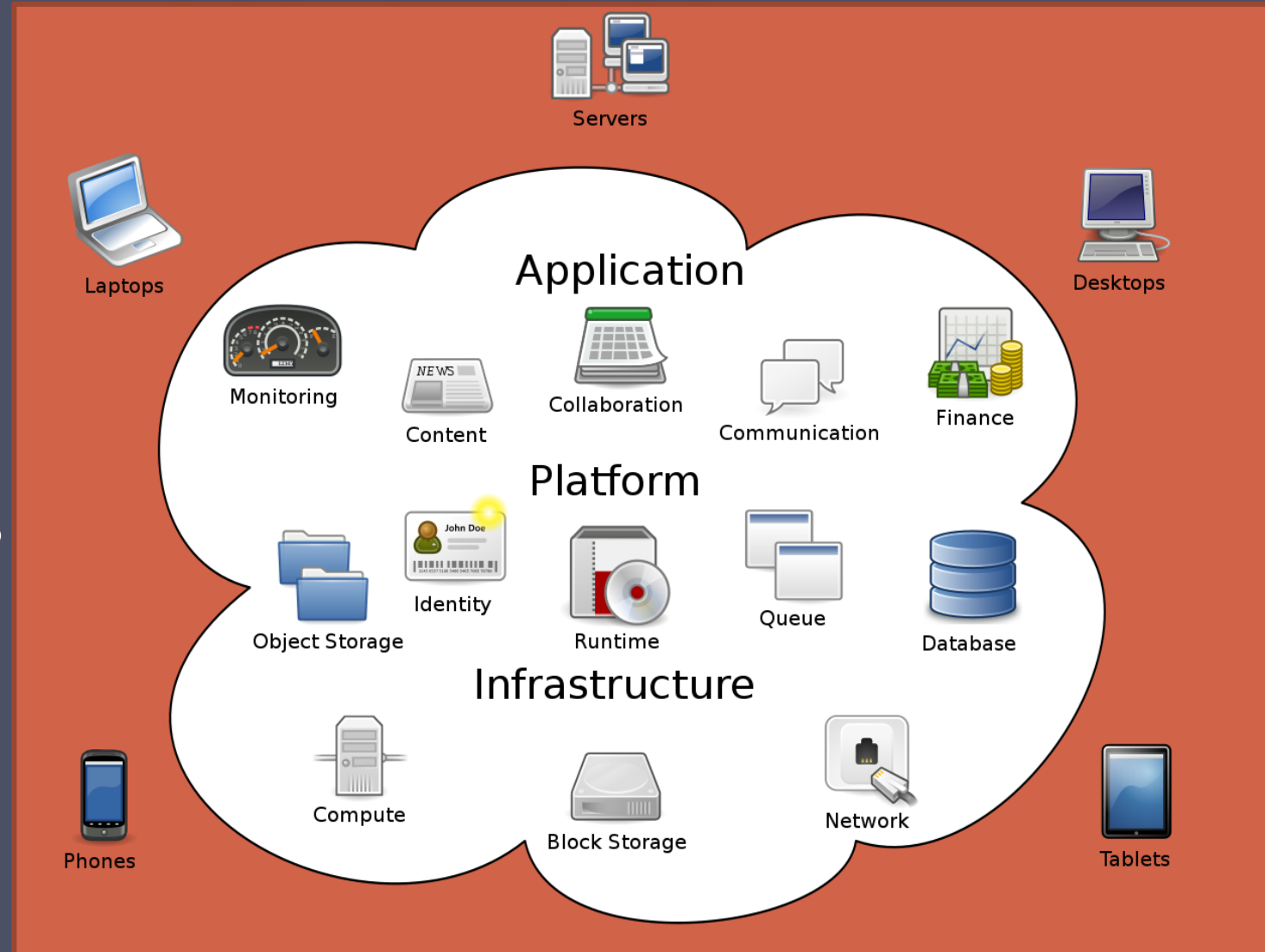
Enterprise System Attack Possibilities

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)

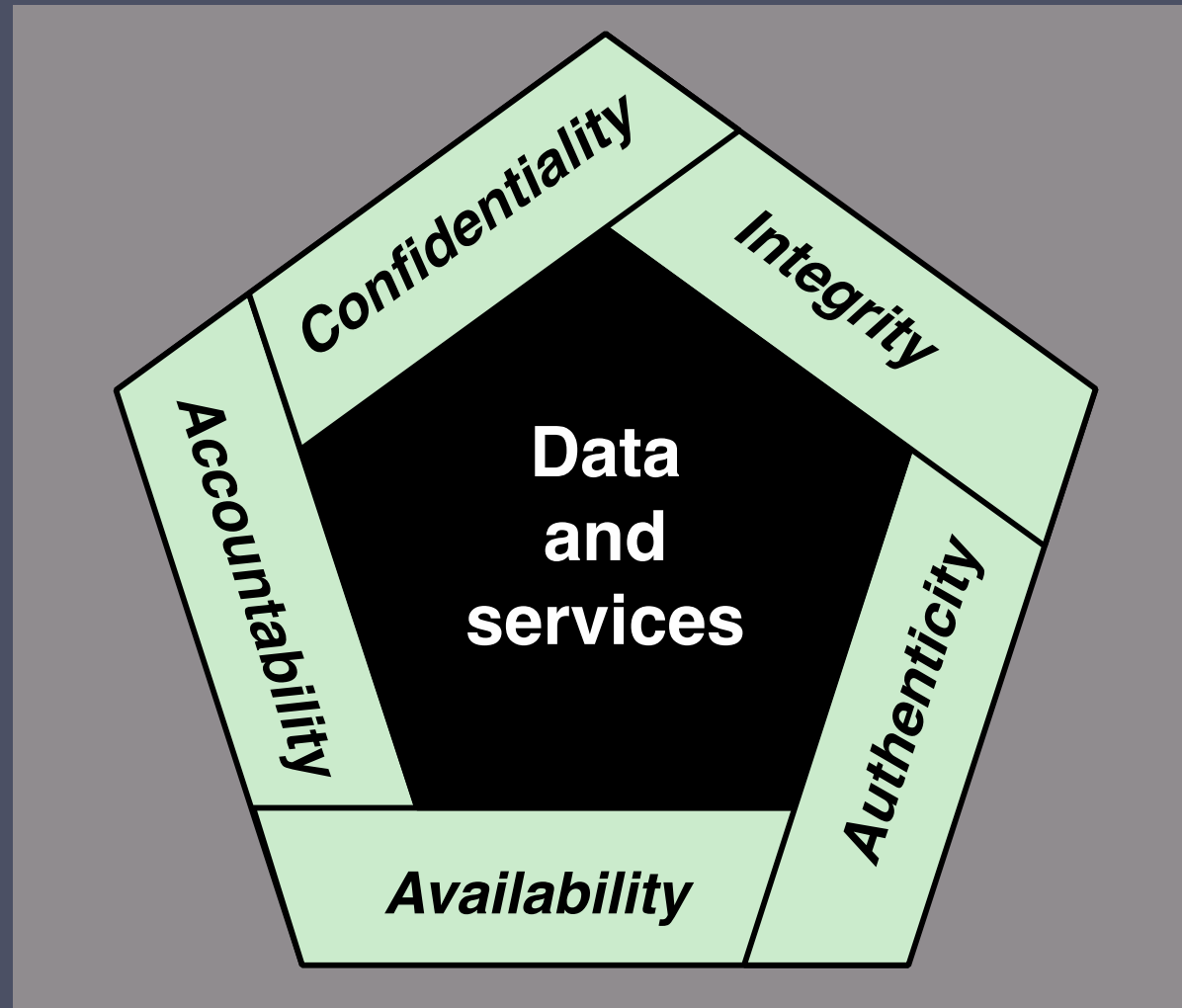
Authenticity

- 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

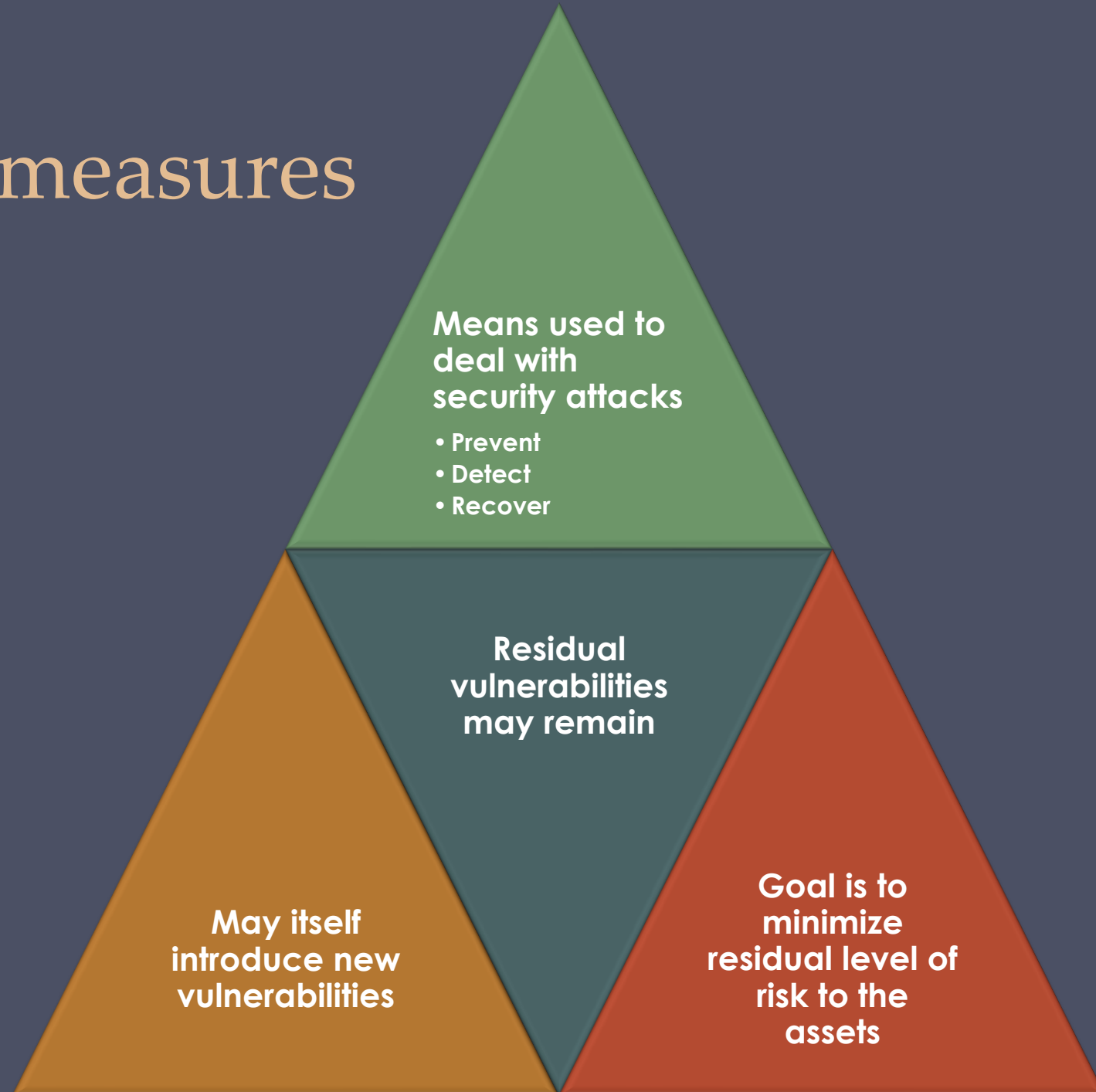
Essential Network and Computer Security Requirements



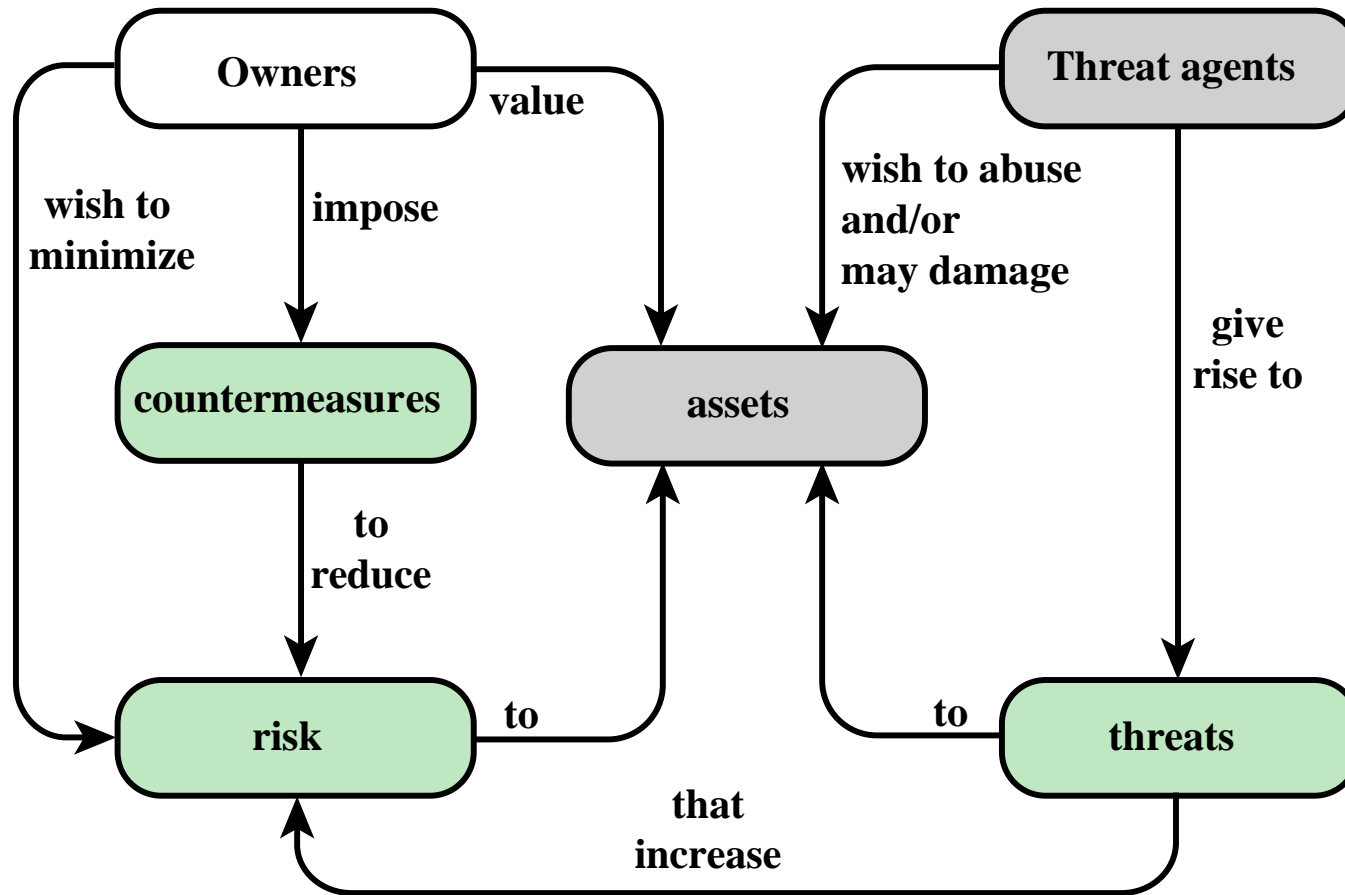
Vulnerabilities, Threats and Attacks

- 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



Security Concepts and Relationships



Conclusion

- Do read and ensure you understand the definitions above



Your weekly cybersecurity hack

 SIGN IN / UP


The  Register®



SECURITY

Thousands of Juniper Junos firewalls still open to hijacks, exploit code available to all

Unauthenticated and remote code execution possible without dropping a file on disk

 [Jessica Lyons Hardcastle](#)

Mon 18 Sep 2023 // 22:30 UTC

6 



About 79 percent of public-facing Juniper SRX firewalls remain vulnerable to a single security flaw can allow an unauthenticated attacker to remotely execute code on the devices, according to threat intelligence platform provider VulnCheck.

Juniper revealed and addressed five flaws, which affect all versions of Junos OS on SRX firewalls and EX Series switches, in an out-of-cycle security bulletin on August 17. The networking and security company updated the advisory on September 7, after security researchers published a proof-of-concept (PoC) exploit, and Juniper detected exploit attempts.

Two of the flaws are PHP external variable modification vulnerabilities (CVE-2023-36844 and CVE-2023-36845). The other three are described as "Missing Authentication for Critical Function vulnerability" (CVE-2023-36846, CVE-2023-36847, and CVE-2023-36851).