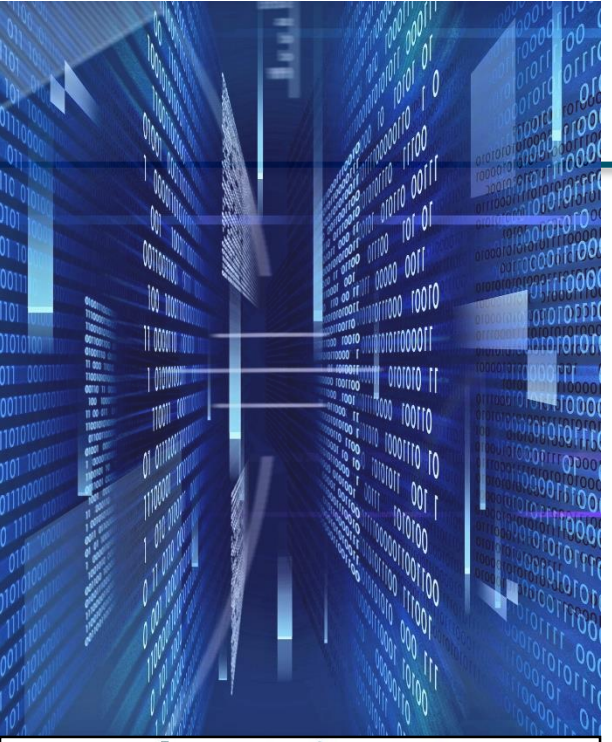


cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

Cyber Security Research Group

blog | twitter

UNIVERSITY OF Southampton

COMP6224 2019-20
Foundations of Cyber Security

Basic Security Concepts

Week 1 – Wednesday 2nd October 2019

Dr Leonardo Aniello

l.aniello@soton.ac.uk

Learning Outcomes

At the end of this lecture you should be able to

- LO1 Discuss the cyber security C.I.A. triad
- LO2 Explain the concepts of vulnerabilities, threats, attacks and assets

Outline

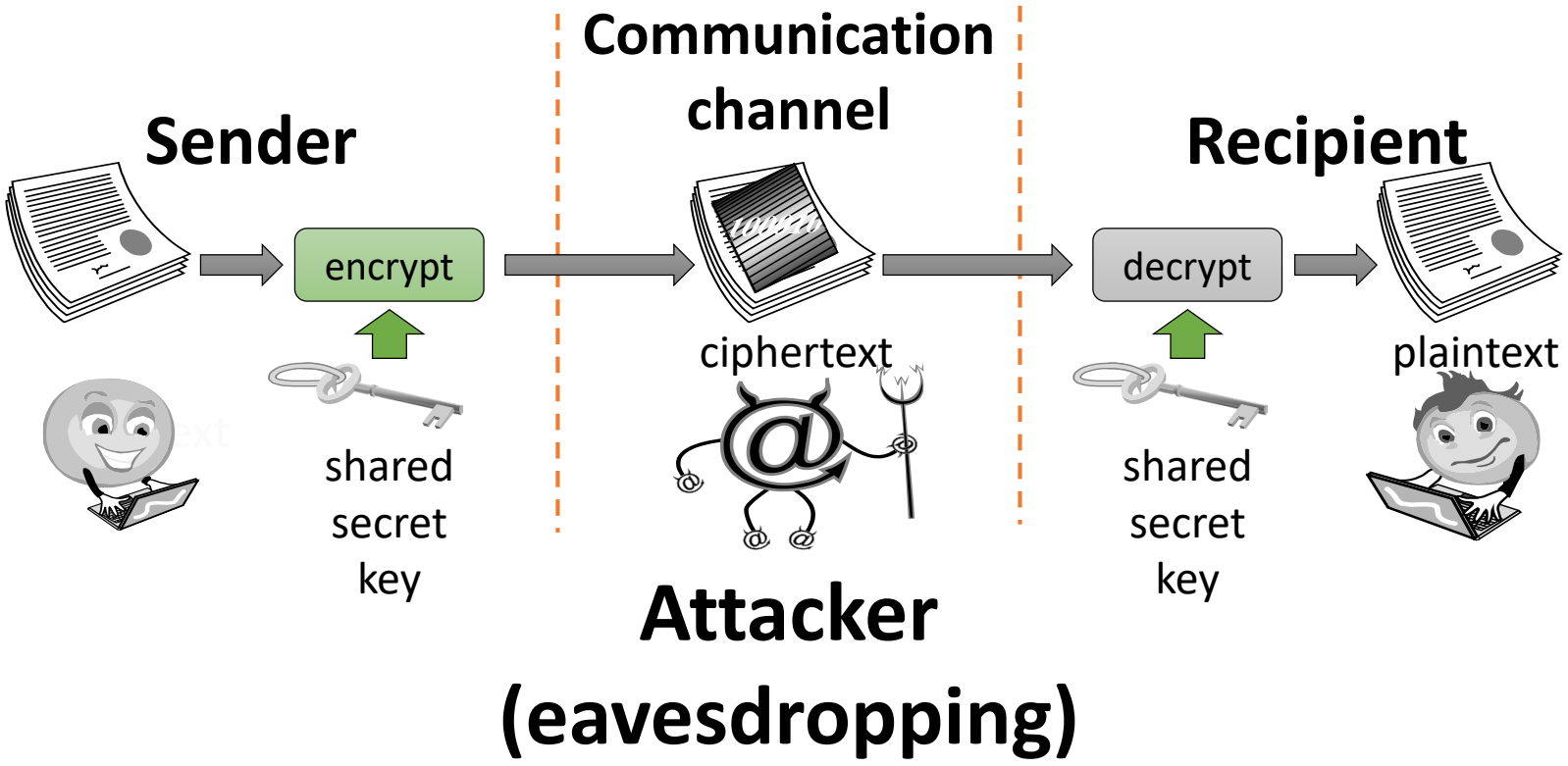
- **Cyber Security C.I.A. Triad**
  - Confidentiality Tools
  - Integrity Tools
  - Availability Tools
- A model of Computer Security
- Threat consequences

Cyber Security C.I.A. Triad

- The three security objectives for information and information systems [NIST standard FIPS 199]
  - **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
    - A loss of confidentiality is the unauthorized disclosure of information
  - **Integrity**: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
    - A loss of integrity is the unauthorized modification or destruction of information
  - **Availability**: Ensuring timely and reliable access to and use of information
    - A loss of availability is the disruption of access to or use of information or an information system

Confidentiality Tools

- **Encryption**: the transformation of information using a secret (encryption key)
  - Transformed information can only be read using another secret (decryption key)



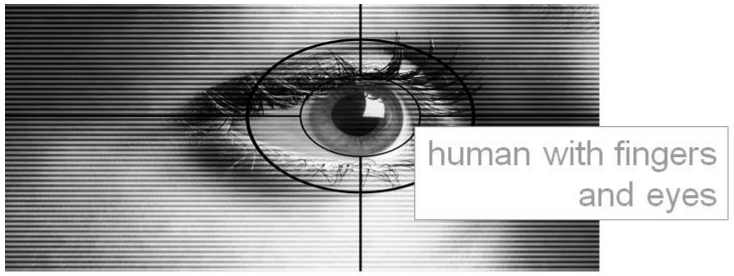
Confidentiality Tools

- **Access control**: rules, policies and mechanisms that limit access to confidential information to those people/systems with a “need to know.”
  - This “need to know” may be determined
    - by identity, such as a person’s name or a computer’s serial number
    - By the role(s) that a person has, such as being a manager or a computer security specialist.

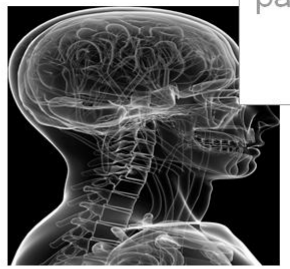
- **Authorization**: determining if a person or system is allowed access to resources, based on an access control policy.

Confidentiality Tools

- **Authentication**: the determination of the identity or role that someone has. This can be done in a number of different ways, usually based on (a combination of)
  - something the person has (like a smart card)
  - something the person knows (like a password)
  - something the person is (like a human with a fingerprint)



Something you are



Something you know

Something you have

Confidentiality Tools

- **Physical security**: the establishment of physical barriers to limit access to protected computational resources.
  - Such barriers include
    - locks on cabinets and doors
    - placement of computers in windowless rooms
    - use of sound dampening materials
    - construction of buildings or rooms with walls incorporating copper meshes (called Faraday cages) so that electromagnetic signals cannot enter or exit the enclosure

- Privacy is still an issue!

Integrity Tools

- **Backups**: periodic archiving of data, to enable to restore data

- **Checksums**: computation of a function that maps the contents of a file to a numerical value
  - A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value

- **Data correcting codes**: methods for storing data in such a way that small changes can be easily detected and automatically corrected

Integrity-related Concepts

- **Authenticity**: property of being genuine and being able to be verified and trusted
  - Confidence in the validity of a transmission, a message, or message originator
  - This means verifying that
    - users are who they say they are, and
    - each input arriving at the system comes from a trusted source

- **Accountability**: security goal that generates the requirement for actions of an entity to be traced uniquely to that entity
  - This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action
  - Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party
  - Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes

Availability Tools

- **Physical protections**: infrastructure meant to keep information available even in the event of physical challenges.

- **Computational redundancies**: computers and storage devices that serve as fallbacks in the case of failures.

Outline

- Cyber Security C.I.A. Triad
  - Confidentiality Tools
  - Integrity Tools
  - Availability Tools
- **A model of Computer Security**
- Threat consequences

A model of Computer Security

- **Asset**, or system resource
  - **Hardware**: Including computer systems and other data processing, data storage, and data communications devices
  - **Software**: Including the operating system, system utilities, and applications
  - **Data**: Including files and databases, as well as security-related data (e.g. passwords)
  - **Communication facilities and networks**: Local and wide area network communication links, bridges, routers, and so on

A model of Computer Security

- Types of asset **vulnerabilities**
  - The system can be **corrupted**, so it does the wrong thing or gives wrong answers.
    - For example, stored data values may differ from what they should be because they have been improperly modified.
  - The system can become **leaky**.
    - For example, someone who should not have access to some or all of the information available through the network obtains such access
  - The system can become **unavailable** or very slow.
    - For example, using the system or network becomes impossible or impractical.

- Each vulnerability corresponds to a **threat** capable of exploiting it
  - A threat represents a potential security harm to an asset

A model of Computer Security

- An **attack** is a threat that is carried out
  - If successful, leads to an undesirable violation of security
  - The agent carrying out the attack is referred to as an **attacker**, **threat agent** or **adversary**
- Attack classification based on impact to assets
  - **Active attack**: An attempt to alter assets or affect their operation.
  - **Passive attack**: An attempt to learn or make use of information from the system that does not affect assets.
- Attack classification based on attack origin
  - **Inside attack**: Initiated by an entity inside the security perimeter (an “insider”). The insider is authorized to access system resources but uses them in a malicious way
  - **Outside attack**: Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an “outsider”)

Threats and Assets

Find examples of cyber/physical threats that break C.I.A properties of assets in the cyber space by operating at different levels: HW, SW, data, communication infrastructure

	Confidentiality	Integrity	Availability
Hardware			
Software			
Data			
Communication Lines and Networks			

Threats and Assets

UNIVERSITY OF Southampton

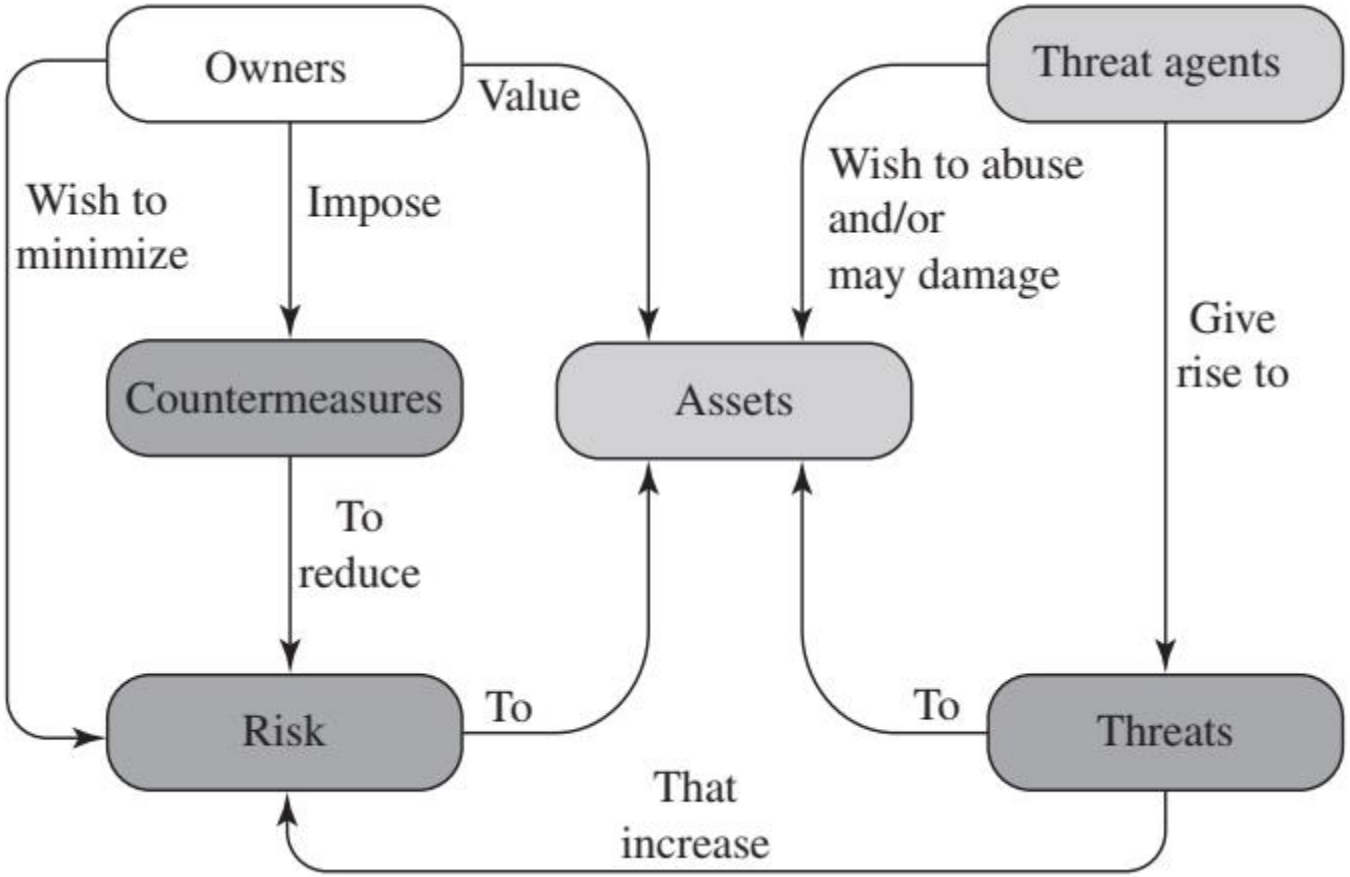
Possible examples	Confidentiality	Integrity	Availability
Hardware	An unencrypted USB drive is stolen	Some HW component is replaced with a malicious part	Equipment is stolen or disabled, thus denying service
Software	An unauthorized copy of software is made	A working program is modified, to cause it to fail during execution or do some unintended task	Programs are deleted, denying access to users
Data	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data	Existing files are modified or new files are fabricated, without authorisation	Files are deleted without authorisation, denying access to users
Communication Lines and Networks	Messages are read. The traffic pattern of messages is observed	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable

A model of Computer Security

- **Risk** is a measure of the extent to which an asset is threatened by a potential circumstance or event, and typically a function of
  - the adverse impacts that would arise if the circumstance or event occurs; and
  - the likelihood of occurrence

- A **countermeasure** is any means taken to deal with a security threat/attack
  - Detection
  - Prevention
  - Mitigation
  - Recovery

A model of Computer Security



Outline

- Cyber Security C.I.A. Triad
  - Confidentiality Tools
  - Integrity Tools
  - Availability Tools
- A model of Computer Security
- **Threat consequences**

Threat Consequences

1. **Unauthorized Disclosure**. An entity gains access to data for which the entity is not authorized

2. **Deception**. May result in an authorized entity receiving false data and believing it to be true

3. **Disruption**. Interruption or prevention of the correct operation of system services and functions

4. **Usurpation**. Control of system services or functions by an unauthorized entity

Threat Consequences

- (1) Unauthorized Disclosure
  - **Exposure**: Sensitive data are directly released to an unauthorized entity
  - **Interception**: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations
  - **Inference**: An unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications
  - **Intrusion**: An unauthorized entity gains access to sensitive data by circumventing a system's security protections

Threat Consequences

- (2) Deception
  - **Masquerade**: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity
  - **Falsification**: False data deceive an authorized entity
  - **Repudiation**: An entity deceives another by falsely denying responsibility for an act

Threat Consequences

- (3) Disruption
  - **Incapacitation**: Prevents or interrupts system operation by disabling a system component
  - **Corruption**: Undesirably alters system operation by adversely modifying system functions or data
  - **Obstruction**: A threat action that interrupts delivery of system services by hindering system operation

Threat Consequences

- (4) Usurpation
  - **Misappropriation**: An entity assumes unauthorized logical or physical control of a system resource
  - **Misuse**: Causes a system component to perform a function or service that is detrimental to system security

Recap

- Cyber Security C.I.A. Triad
  - **Confidentiality**: private/confidential information is not made disclosed to unauthorized individuals, individuals control how information related to them can be managed
  - **Integrity**: information and programs are changed only in a specified and authorized manner, a system performs its intended function in an unimpaired manner
  - **Availability**: systems work promptly and service is not denied to authorized users
- A model of Computer Security
  - Assets, vulnerabilities, threats, attacks, attackers, countermeasures, risk
  - Threats against assets: CIA against HW, SW, data, communication infrastructure
  - Threat consequences: unauthorized disclosure, deception, disruption, usurpation

References

- Stallings, W. and Brown, L., 2018. Computer Security, Principles and Practice, 4: th ed.
  - Sections 1.1, 1.2