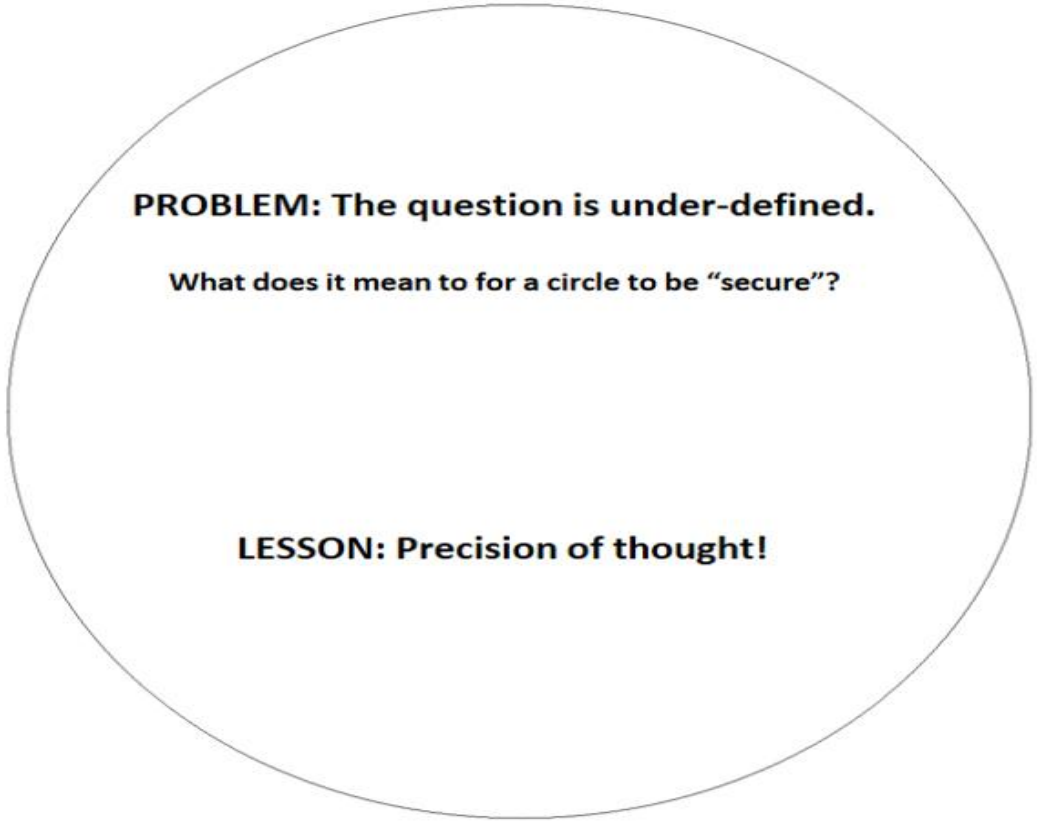
جَـامعة
المَـنارة
MANARA UNIVERSITY

Information Systems Security

Fall 2025

Information Systems Security
Overview

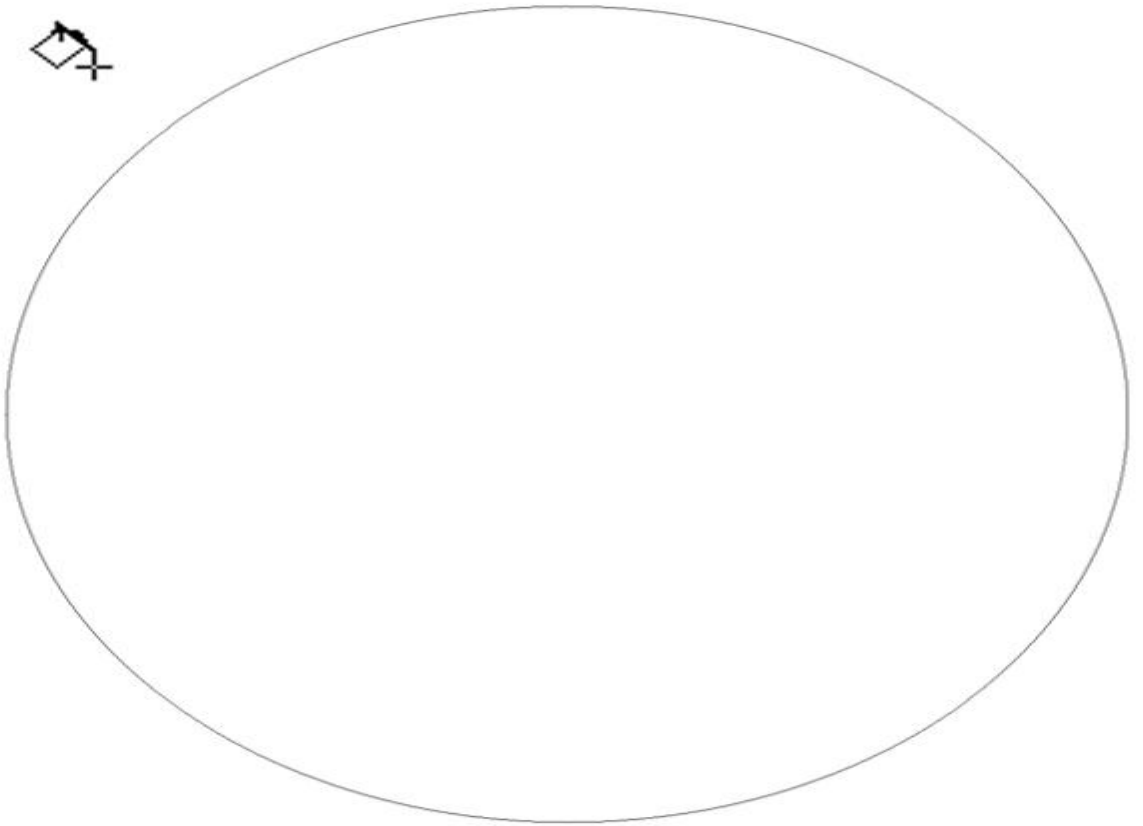
Is this circle secure?



2

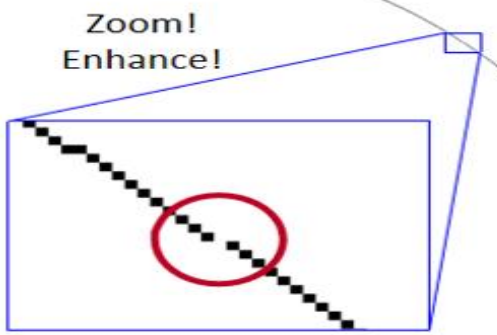
جَـامعة
المَـنارة
MANARA UNIVERSITY

If I flood-fill outside the circle, will the color penetrate it?



If I flood-fill outside the circle, will the color penetrate it?

Why?



PROBLEM: The defender needs 3000 perfect pixels, but the attacker just needs one flaw.

In computers, you need way more than just 3000 things to be right.

LESSON: Perfect security is usually impossible to prove.

Why that exercise?

- Why did we do this exercise? To put you in the right mindset.
  - We're about to define security and present the fundamental model for reasoning about it.
  - It will seem simple. You will be tempted to ignore it.
    - If you take that mental shortcut, you are inviting ruin.
  - If you want a perfect circle, you must make it **SYSTEMATICALLY AND PRECISELY**
  - ***Security models help us flawed humans avoid missing something!***

6

What is information security?

From "An Introduction to Information Security" (NIST Special Publication 800-12):

- Information Security:

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.

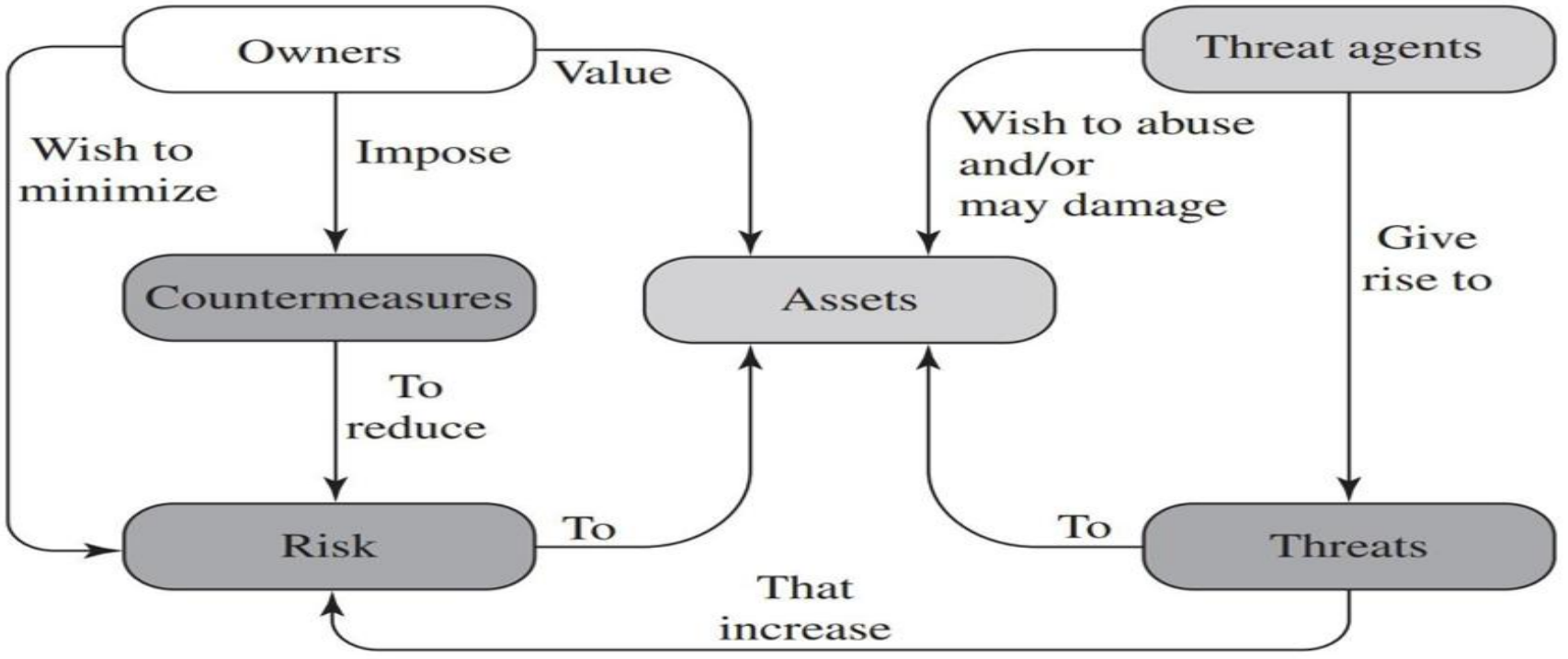
The CIA Triad

There are like 900 pictures of the CIA triad on google, but this was the ugliest one.

The CIA triad

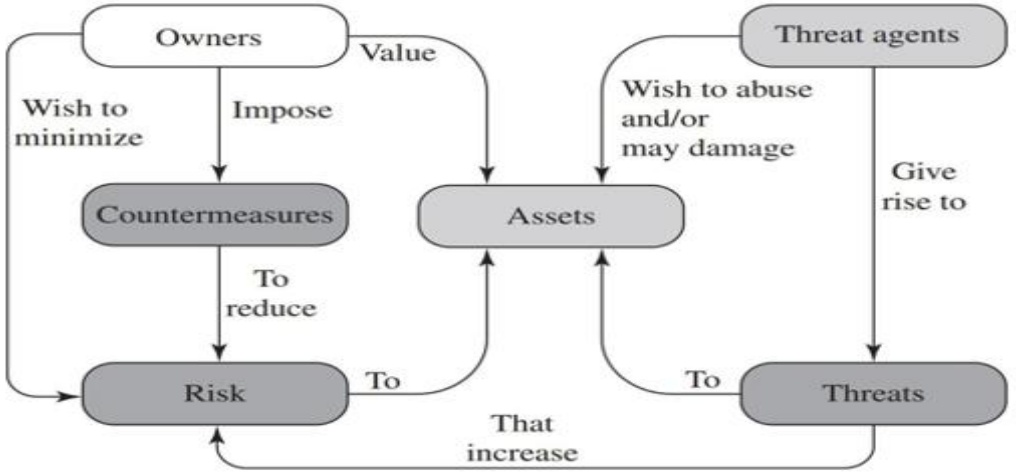
- **Confidentiality**: Preserving authorized access controls and disclosure restrictions to protect personal privacy and proprietary information
- **Integrity**: Guarding against improper information modification or destruction and ensuring information non-repudiation[1] and authenticity.
  - Data Integrity – The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
  - System Integrity – Ability of a system to perform its intended function without impairment or unauthorized manipulation.
  - **Availability**: Ensuring timely and reliable access to and use of information.

Computer Security Model



Components of the Computer Security Model

- **Assets**: The valued hardware, software, data, and communications.
- **Threats**: *Specific* attacks against an asset.
- **Countermeasures**: *General* defenses for an asset.
- **Risk**: We don't know the threats, so we summarize our perception of exposure to threats as *risk*.



How do threats work?

- **Threats** try to exploit one or more **vulnerabilities** of the asset.
  - Vulnerability may be a design flaw (e.g. a bug or misconfiguration) or a resource constraint (e.g. amount of server resources).
- An **attack** is a threat that is carried out leading to a violation of CIA triad:
  - Information leakage (failure of confidentiality)
  - Doing the wrong thing or giving wrong answer (failure of integrity)
  - Becoming unusable or inaccessible (failure of availability)
- **Countermeasure** deals with a particular class of attack
  - **Ideally prevent attack; failing that, at least detect attack and recover.**

11

How do threats work?

- **Threats** try to exploit one or more **vulnerabilities** of the asset.
  - Vulnerability may be a design flaw (e.g. a bug or misconfiguration) or a resource constraint (e.g. amount of server resources).
- An **attack** is a threat that is carried out leading to a violation of CIA triad:
  - Information leakage (failure of confidentiality)
  - Doing the wrong thing or giving wrong answer (failure of integrity)
  - Becoming unusable or inaccessible (failure of availability)
- **Countermeasure** deals with a particular class of attack
  - **Ideally prevent attack; failing that, at least detect attack and recover.**

Thinking about reducing risk

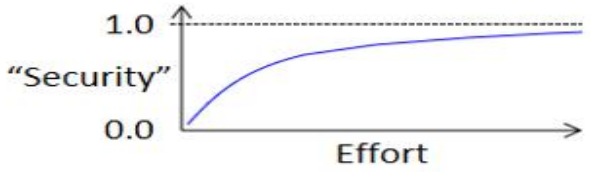
- **Security of a system is boolean**: vulnerable or not vulnerable
- As it is not possible to *prove* the security of a system,

we do not know this boolean's value

- As such, we apply *countermeasures* to **reduce the probability of attacks succeeding**, given our incomplete knowledge
- This is what we mean by "**reducing risk**"

- This thought process is so common, security professionals may use the verbal shorthand "**this makes the system *more secure***".

- Danger of this shorthand: implies that if you do it enough, you reach "secure". You don't.



12

"More secure" vs "secure"

"More secure"
(a real concept)

=

"Has countermeasures which, all things being equal, reduce the probability of an exploitable vulnerability being available to attackers, but this probability never reaches zero."

"Fully secure"
(a fool's delusion)

- I'm racking up Security Points and if I get enough I win security!
- If I deploy this one thing, I am entirely secure.
- It's so *simple* we don't have to think about it!

13

Classes of threats (1)

RFC4949 defines four broad classes of attack (with sub-types):

1.Unauthorized disclosure

- **Exposure** of sensitive information intentionally (e.g. from insider)
- **Interception** of info in transit (e.g. network sniffing)
- **Inference** of info given public data (e.g. an exercise app shows popular exercise locations; this reveals base locations in warzones)
- **Intrusion** into the system (traditional "hacking" into a server)

2.Deception

- **Masquerade** as someone else (e.g. forging the sender on an email asking for something)
- **Falsification** of data (e.g. changing your homework grade in Canvas)
- **Repudiation**: denying you send/received particular data (e.g. "I didn't tweet that, I was ~*hacked*~!")

Classes of threats (2)

RFC4949 defines four broad classes of attack (with sub-types):

3.Disruption

- **Incapacitation** of a system (e.g. denial-of-service attack)
- **Corruption** of data (e.g. “my username is `";DROP ALL TABLES;--`”)
- **Obstructing** communications (e.g. wifi jamming)

4.Usurpation

- **Misappropriation** of service (e.g. Captain Crunch’s use of telephone services)
- **Misuse** of service (e.g. misconfiguring a mail system so it floods someone with email)

Matching assets against the CIA triad

	Availability	Confidentiality	Integrity
Hardware	Equipment stolen/disabled	Physical media stolen	Hardware modified to include tracking or control (e.g. keylogger or keyboard emulator)
Software	OS or program files corrupted, causing loss of service	Proprietary software is stolen	Software is modified to include tracking or malicious control (e.g. malware)
Data	Database or files deleted or corrupted, causing loss of service	Unauthorized reading of user data	Files are modified by malicious actor
Communications	Messages blocked or communication line damaged or shut down	Messages intercepted and read or traffic pattern is analyzed	Messages are modified, duplicated, fabricated, or otherwise molested in transit.