Tutorial 1

Understanding the effect of cyberattacks Part 1

Basics

- Data VS Information (what is the difference between data and information?)
- Information means data that has some meaning (useful data). For example, 111989 is data. If we know that this data is the date of birth of a person, then it is information (1st of January 1989)
- Information security (what is information security?)
- Information security is all about protecting the information, which generally focus on the confidentiality, integrity, availability (CIA) of the information.

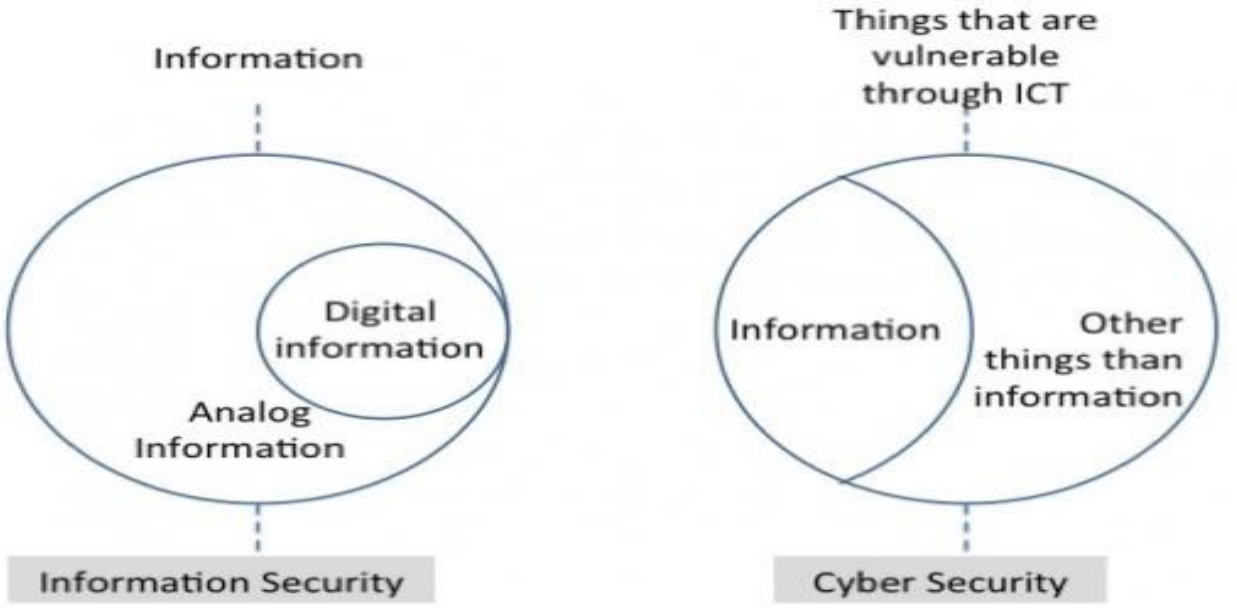
Basics

- Define confidentiality, integrity, and availability in your own words?

- Confidentiality: ensuring that no one can understand the message except the receiver/receivers.
- Integrity: ensuring that the receiver received the message without any unauthorized changes.
- Availability: ensuring that information is available when it is needed.

Basics

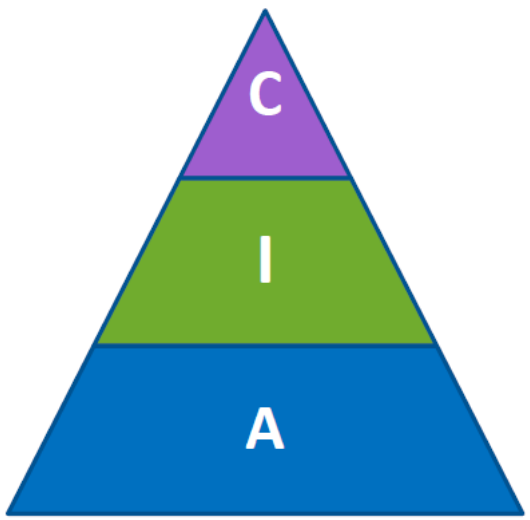
- Information security VS Cybersecurity
- Information security focuses on CIA
- Cybersecurity focuses on CIA Plus (CIA + Authenticity + Control + Utility)



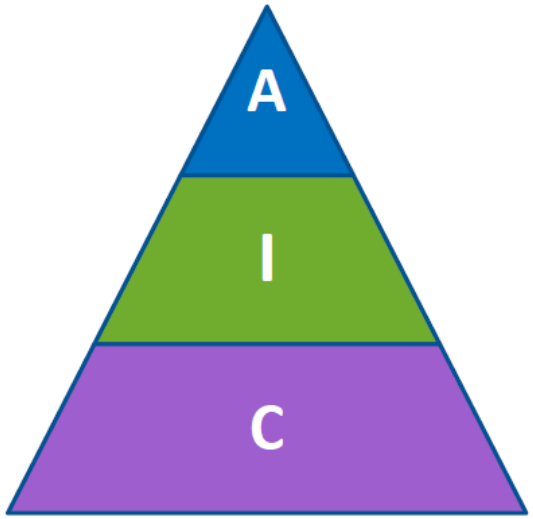
Basics

- **Cybersecurity:** The ability to protect or defend the use of cyberspace from cyberattacks.
- Targeted systems:

IT



ICS



Statistics of Cyberattacks

- Statistics of cyberattacks creates a complete picture of the motivations of attackers, attack techniques, and targeted systems.
- For example, http://www.hackmageddon.com

- This is a website that presents cyberattacks timelines.

- The main fields of reports on this website are as follows: ID, Date, Author, Target, Description, Attack, Target Class, Attack Class, Country, Link, Tags.

HACKMAGEDDON

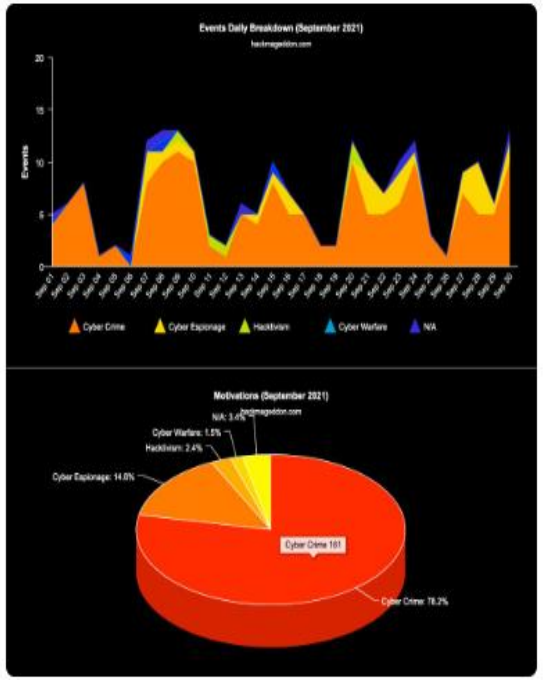
- 1. ID: An integer unique to that half-month le
- 2. Date: The date the attack was reported
- 3. Attack: The type of attack (e.g. DDoS)
- 4. Target Class: The targeted sector.
- 5. Attack Class: Cyber War, Cyber Crime, Cyber Espionage, or Hacktivism
- 6. Country: ISO alpha-2 country code (e.g. US)
- 7. Link: A URL for a new article describing the attack
- 8. Tags: Important keywords

HACKMAGEDDON

DONATE ABOUT TIMELINES STATISTICS CLOUD-NATIVE THREATS DATA BREACHES LEAKY BUCKETS INFOGRAPHICS SUBMIT

ID	DATE REPORTED	DATE OCCURRED	DATE DISCOVERED	AUTHOR	TARGET	DESCRIPTION	ATTACK	TARGET CLASS	ATTACK CLASS	COUNTRY	LINK
1	16/09/2021	16/9/2021	16/9/2021	?	VoIP.ms	Threat actors target voice-over-Internet provider VoIP.ms with a DDoS attack and extorting the company to stop the assault that's severely disrupting the company's operation.	DDoS	J Information and communication	CC	CA	Link
2	16/09/2021	During 2020	During September 2021	?	Multiple U.S. government sites	Multiple U.S. government sites using .gov and .mil domains have been seen hosting porn and spam content, such as Viagra ads, in the last year, due to a vulnerability in a common software product provided by Laserfiche, a government contractor.	Vulnerability	O Public administration and defence, compulsory social security	CC	US	Link
3	16/09/2021	-	"Recently"	?	Multiple	Security researchers from	Malware	Y Multiple	CC	>1	Link

campaigns fuelled by the massive exploitation of #vulnerabilities... hackmageddon.com/2021/10/28/sep…



7h

Real-life example: Solarwinds cybersecurity event (2020-2021)

1- Targeted system: Solarwinds is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure.

2- Summary of cybersecurity event:

A- In early 2020, hackers secretly broke into Texas-based SolarWind's systems and added malicious code into the company's software system.

B- In March of 2020, SolarWinds sent out software updates to its customers that included the hacked code.

C- The code created a backdoor to customers' information technology systems, which hackers then used to install even more malware that helped them spy on companies and organizations (up to 18,000 customers)

Solarwinds cybersecurity event (2020-2021)

3- Cyber mitigation:

A- "Only install signed versions" doesn't help because this software was signed.

B- "Update your software to the latest version" doesn't help because the updated software was the infected one.

C- "Monitor software behavior" detect anomaly behaviour

D- "Data backup" use data backup when original data is lost.

C- "Monitoring network traffic by using IDS and IPS" detect anomaly behaviour and prevent attacks.

Exercise:

- Let's divide the students into 4 groups such that each group has 2 students.

1- Select one cybersecurity event from the website.

2- In 20 min, define the targeted system, summary of the event, and mitigation of the cyberattack that related to the selected cybersecurity event.

3- Then, each group should discuss this event in 10 min.