Basic Notions of Confidentiality Integrity Availability

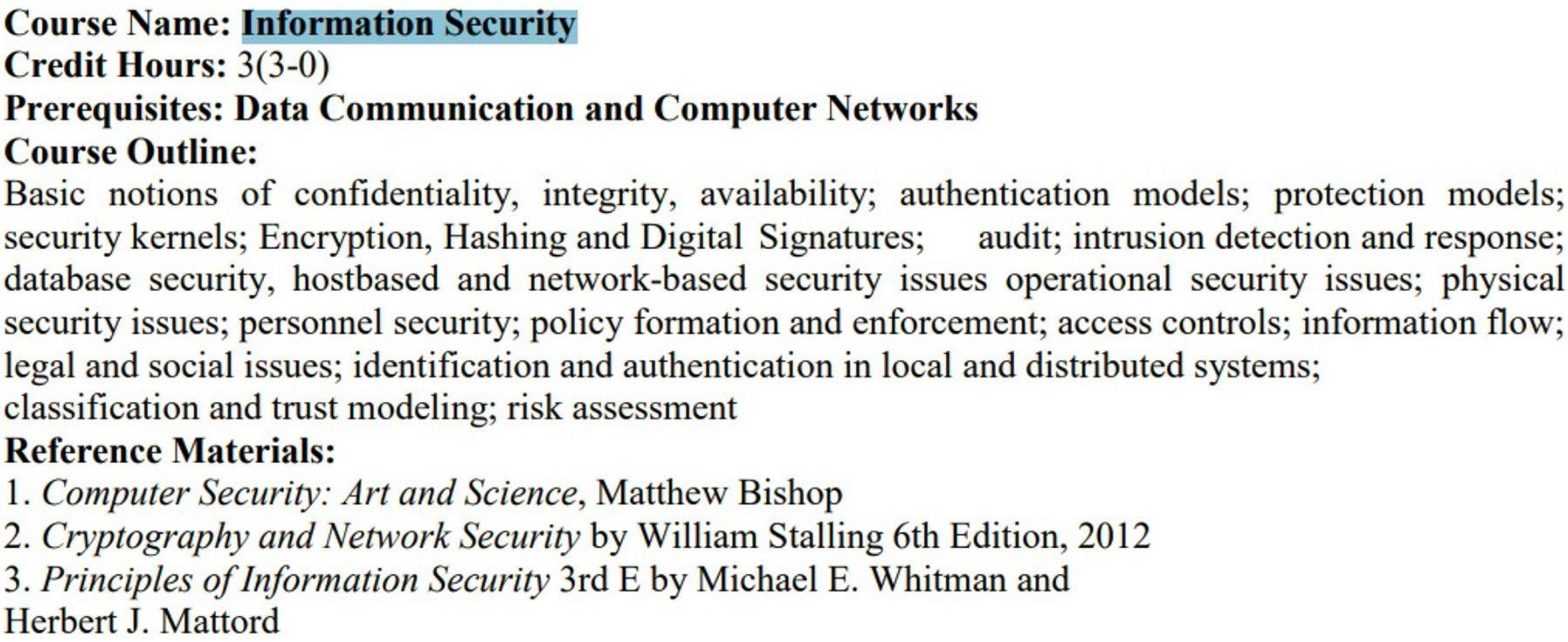
Information Security

ArfanShahzadTech

WhatsApp-Contact Us
0345-5922495

Arfan Shahzad
{ arfanskp@gmail.com }

Course Outline



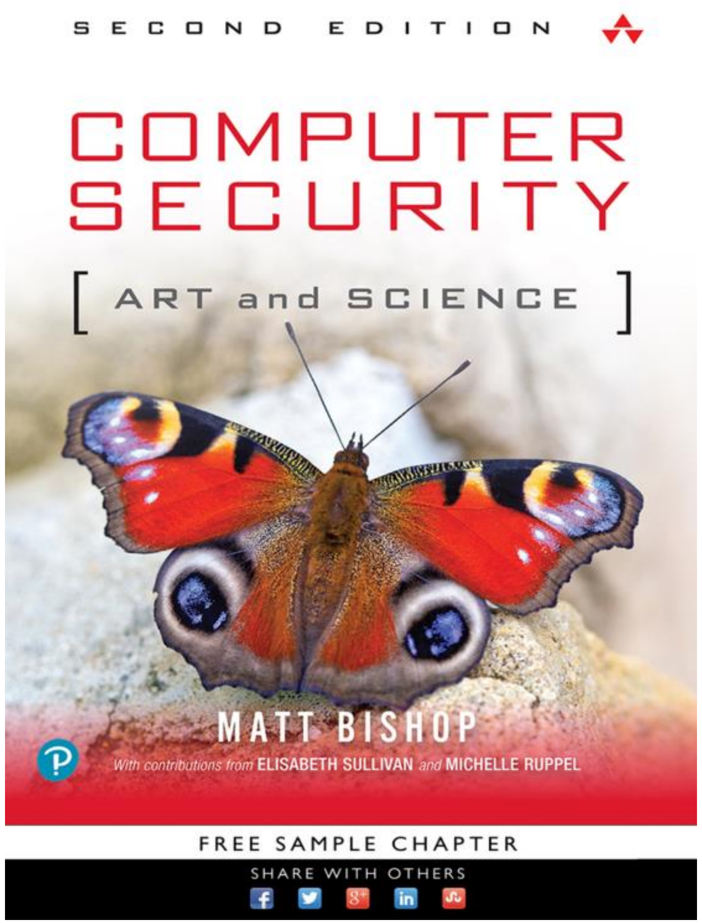
Course Name: Information Security
Credit Hours: 3(3-0)
Prerequisites: Data Communication and Computer Networks
Course Outline:

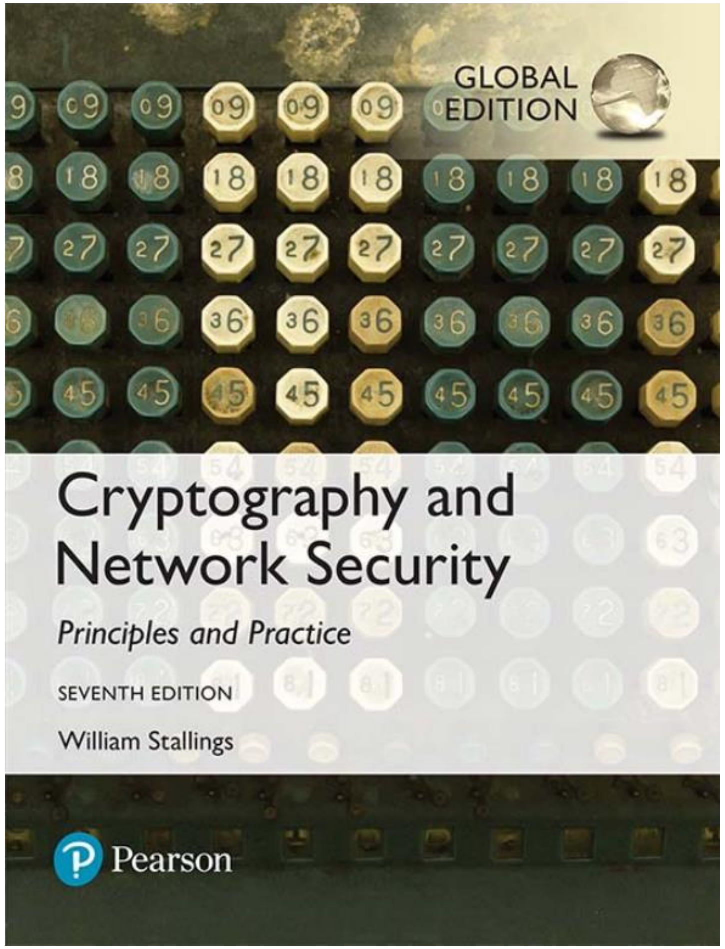
Basic notions of confidentiality, integrity, availability; authentication models; protection models; security kernels; Encryption, Hashing and Digital Signatures; audit; intrusion detection and response; database security, hostbased and network-based security issues operational security issues; physical security issues; personnel security; policy formation and enforcement; access controls; information flow; legal and social issues; identification and authentication in local and distributed systems;
classification and trust modeling; risk assessment

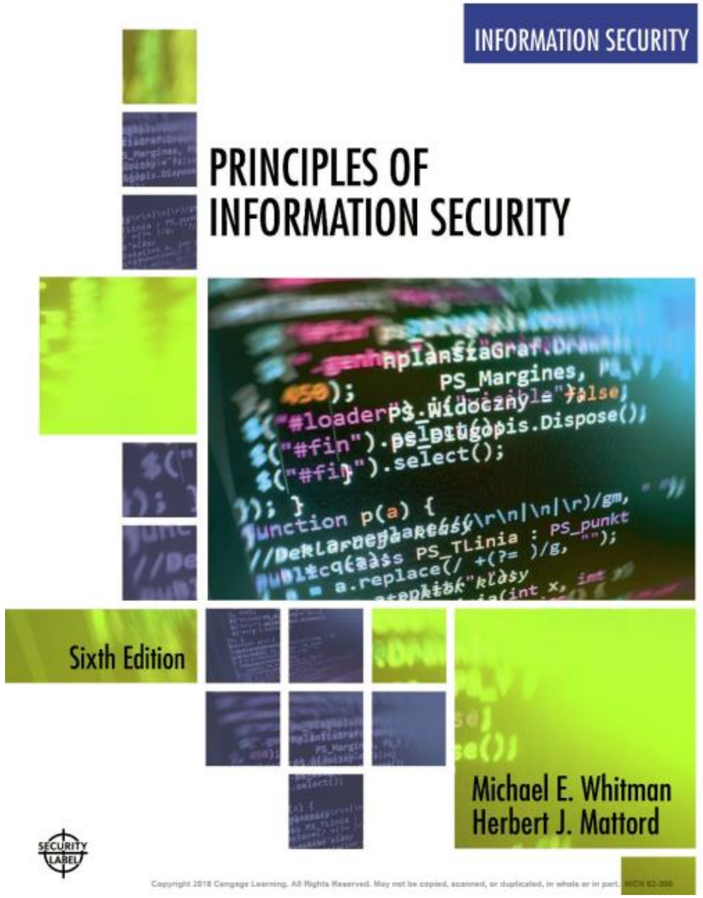
Reference Materials:

1. *Computer Security: Art and Science*, Matthew Bishop
2. *Cryptography and Network Security* by William Stalling 6th Edition, 2012
3. *Principles of Information Security* 3rd E by Michael E. Whitman and
Herbert J. Mattord

Text Books


SECOND EDITION
COMPUTER SECURITY
[ART and SCIENCE]
MATT BISHOP
With contributions from ELISABETH SULLIVAN and MICHELLE RUPPEL
FREE SAMPLE CHAPTER
SHARE WITH OTHERS


GLOBAL EDITION
Cryptography and Network Security
Principles and Practice
SEVENTH EDITION
William Stallings
Pearson

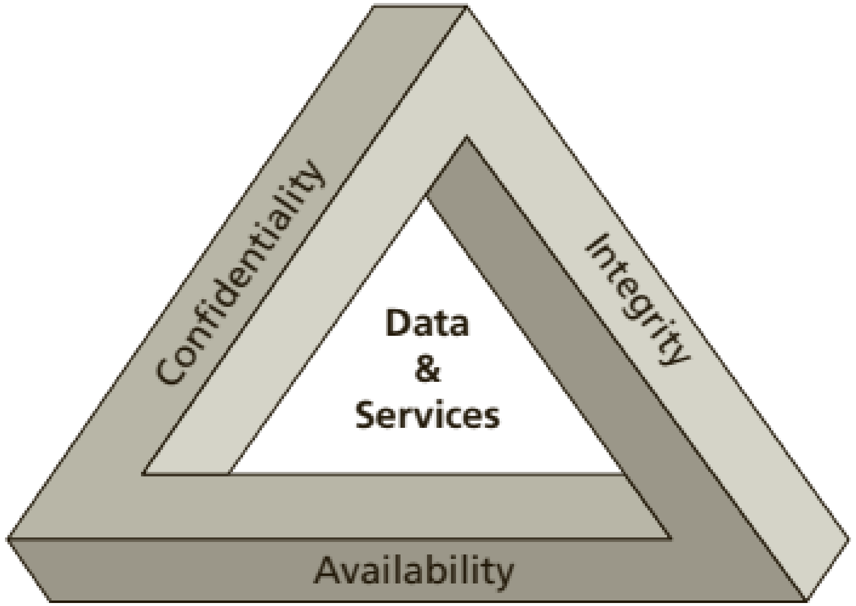

INFORMATION SECURITY
PRINCIPLES OF INFORMATION SECURITY
Sixth Edition
Michael E. Whitman
Herbert J. Mattord

Computer Security

- The NIST (**National Institute of Standards and Technology**) ***Computer Security Handbook*** [NIST95] defines the term *computer security* as follows:
- **Computer Security:** The protection afforded to an ***automated information system*** in order to attain the applicable objectives of preserving the ***integrity***, ***availability***, and ***confidentiality*** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Confidentiality, Integrity and Availability

- This definition introduces three key objectives that are at the heart of computer security:
- **Confidentiality**,
- **Integrity** and
- **Availability**

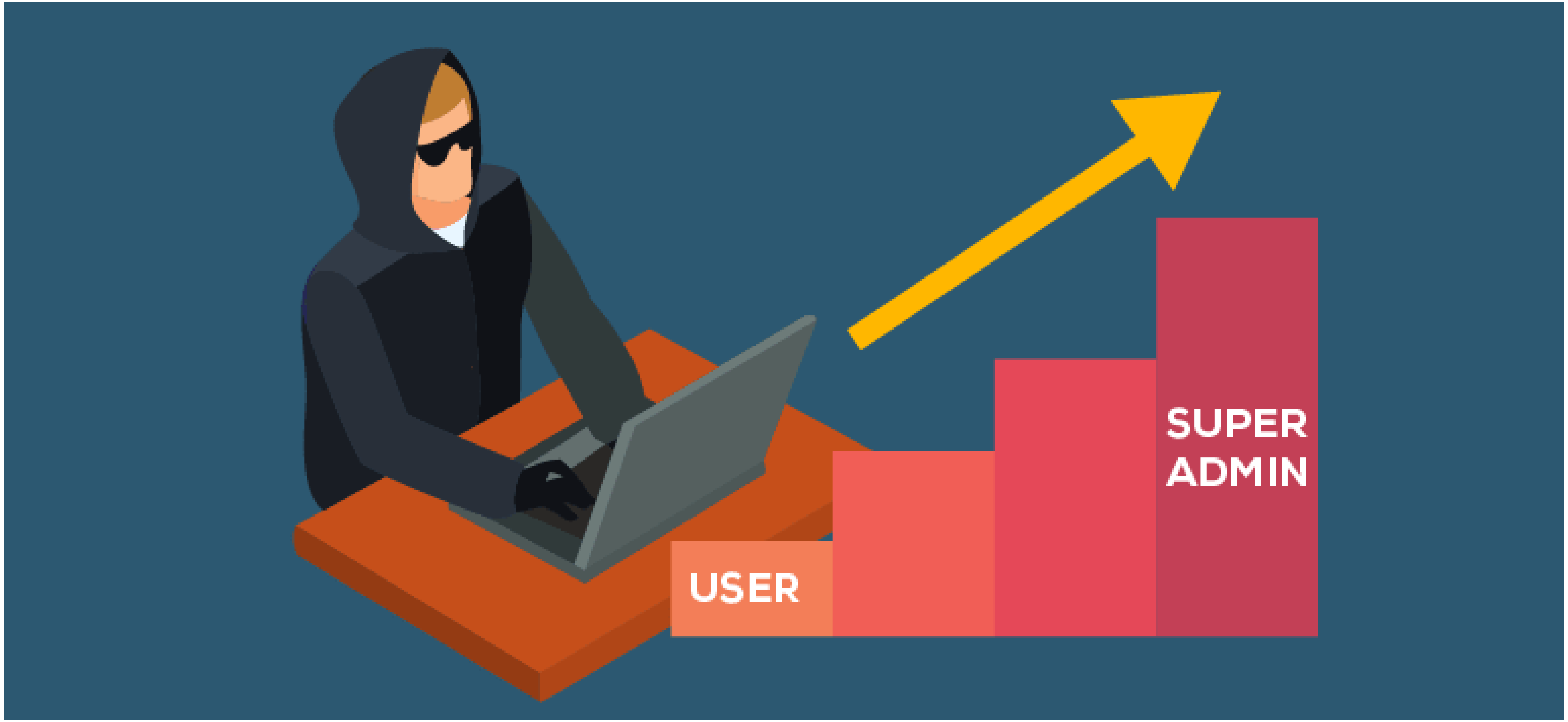


Confidentiality, Integrity and Availability cont…

- **Confidentiality:** This term covers two related concepts:

1. **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to ***unauthorized individuals***.
2. **Privacy:** Assures that ***individuals*** ***control*** or ***influence*** **what information related to them** may be **collected** and **stored** and by whom and to whom that ***information may be disclosed***.

Confidentiality, Integrity and Availability cont… Privilege Escalation



Confidentiality, Integrity and Availability cont…
Privilege Escalation

- Privilege escalation is the process by which **a user** or **program** ***gains more privileges than they are supposed to have***, allowing them to ***perform actions*** or ***access resources*** **that are usually restricted**.
- This can happen due to security vulnerabilities or misconfigurations in the system, allowing an attacker to take advantage of these weaknesses to escalate their privileges and gain more control over the system.

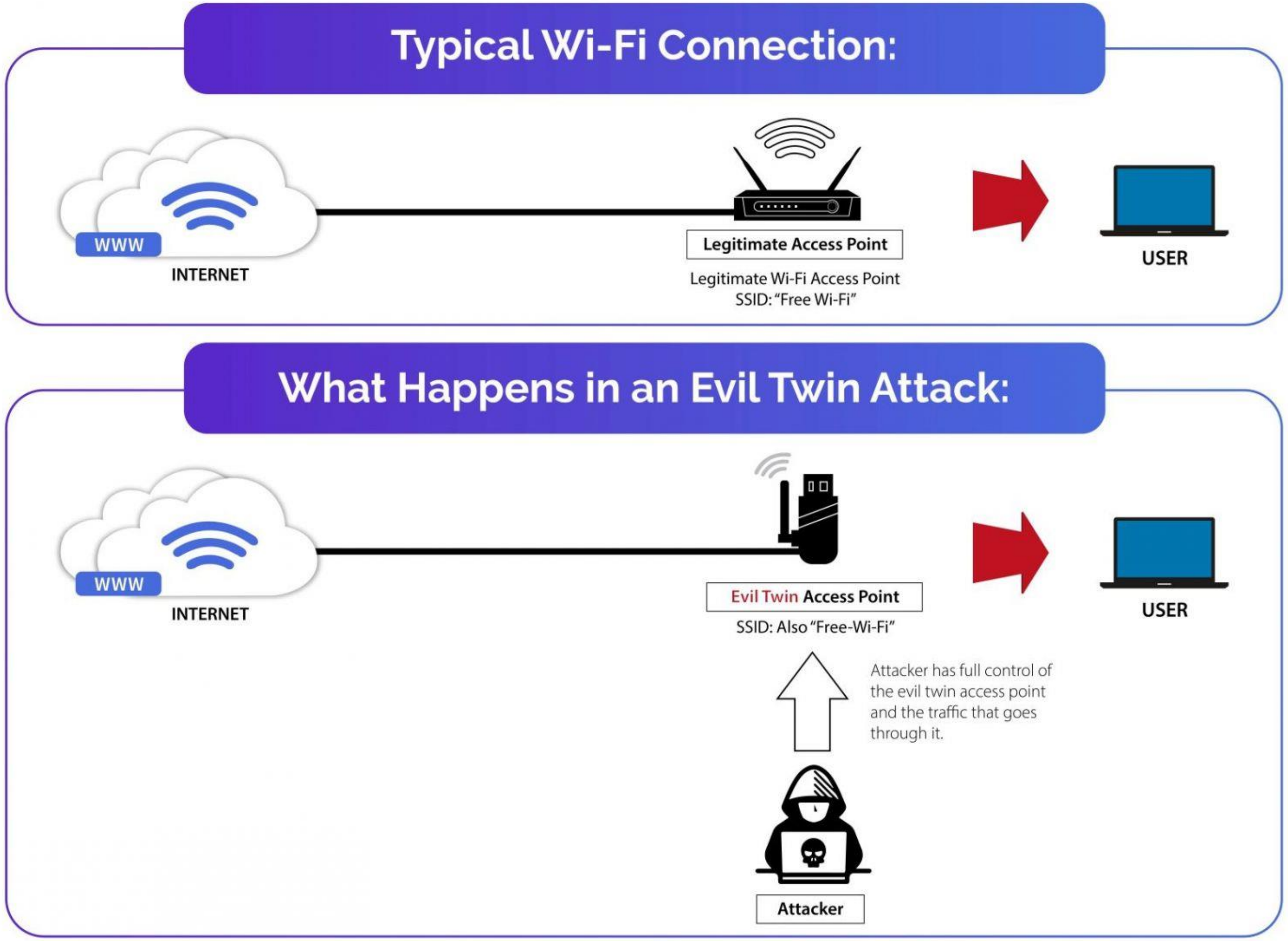
Confidentiality, Integrity and Availability cont…

Evil Twin

- The Evil Twin attack is a type of ***wireless network attack*** where an ***attacker sets up a rogue (rascal) access point*** that **mimics** ***a legitimate one (access point) in order to trick users into connecting to it***.
- Once the user connects, the **attacker can intercept** and **capture the user's network traffic**, potentially gaining access to sensitive information such as ***login credentials*** or ***personal data***.

Confidentiality, Integrity and Availability cont…

Evil Twin



Typical Wi-Fi Connection:

Legitimate Wi-Fi Access Point
SSID: "Free Wi-Fi"

What Happens in an Evil Twin Attack:

SSID: Also "Free-Wi-Fi"

Attacker has full control of the evil twin access point and the traffic that goes through it.

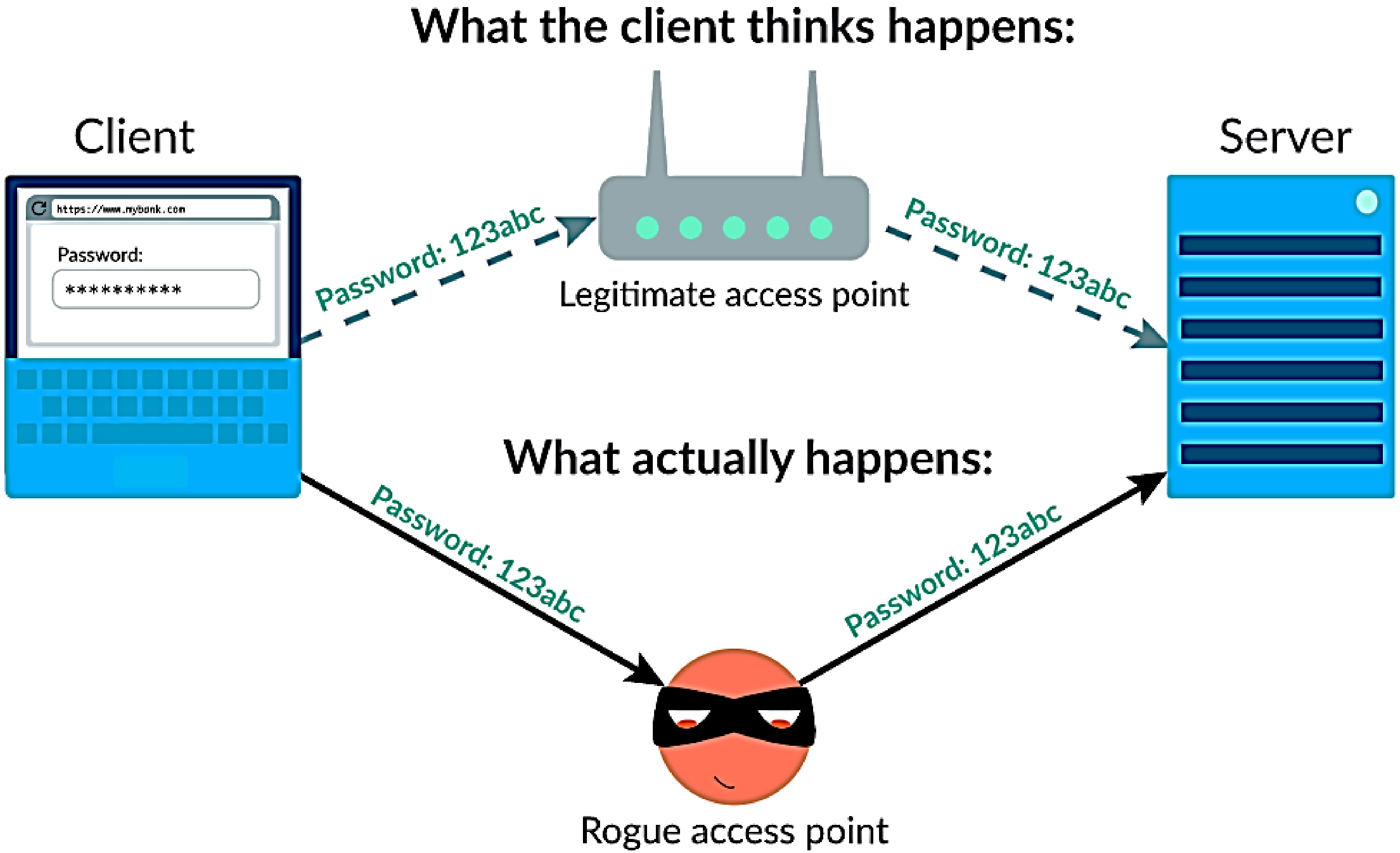
Confidentiality, Integrity and Availability cont…

Rogue Access Point

- A rogue access point is a ***wireless access point*** that ***has been installed on a network without authorization***, often by an attacker ***looking to gain unauthorized access*** to the network.
- A rogue access point may be set up in a **public location** or even in an **office** or other **private location**, and can be ***used to intercept*** and ***steal sensitive information*** or ***launch other attacks against devices connected to the network***.

Confidentiality, Integrity and Availability cont…

Rogue Access Point



Confidentiality, Integrity and Availability cont…

Rogue Access Point

- Organizations can protect against rogue access points by implementing ***wireless intrusion prevention systems*** (WIPS) and ***conducting regular network security audits*** to detect unauthorized devices.

Confidentiality, Integrity and Availability cont…
Rogue Access Point vs. Evil Twin

- A **rogue access point** is simply ***an unauthorized access point***, while an **evil twin** is a ***specific type of rogue access point*** that is ***set up to mimic a legitimate access point*** in order to ***deceive users into connecting to it***.

Confidentiality, Integrity and Availability cont…

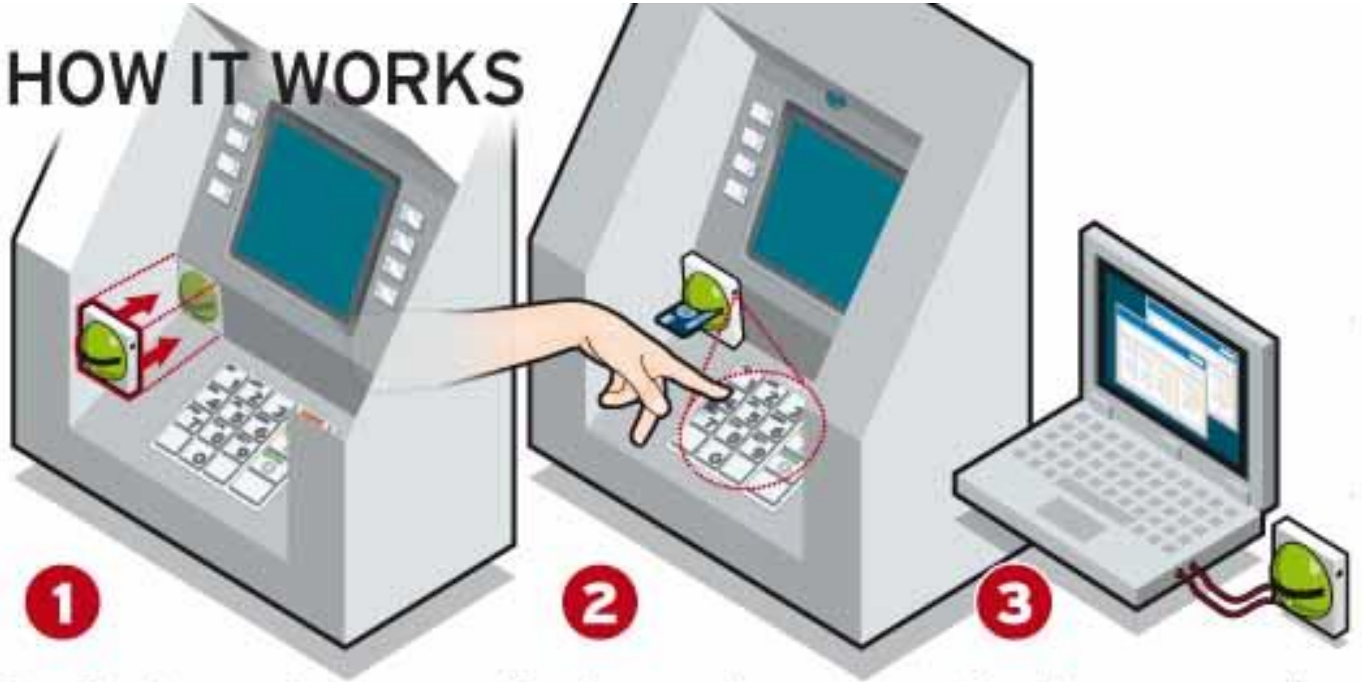
- **Integrity:** This term covers two related concepts:

1. **Data integrity:** Assures that **information** (both stored and in transmitted packets) and **programs** are changed only in a ***specified*** and ***authorized manner***.
2. **System integrity:** Assures that a **system performs** its ***intended function*** in an ***unimpaired manner***, free from ***deliberate*** or ***inadvertent unauthorized manipulation*** of the system.

Confidentiality, Integrity and Availability cont…

Skimming

HOW IT WORKS



1 Duplicate card reading device placed over existing one

2 Device reads your card while a pinhole camera records you entering PIN

3 Device removed and attached to a laptop to download card details

Confidentiality, Integrity and Availability cont…

Skimming

- Skimming is a type of fraud where ***criminals use a small device*** called a **skimmer** ***to steal credit or debit card information*** when the card is swiped at a point of sale terminal or an ATM.
- The skimmer is usually placed on the card reader, and it can be difficult to spot because it looks like a legitimate part of the machine.

Confidentiality, Integrity and Availability cont…

Skimming

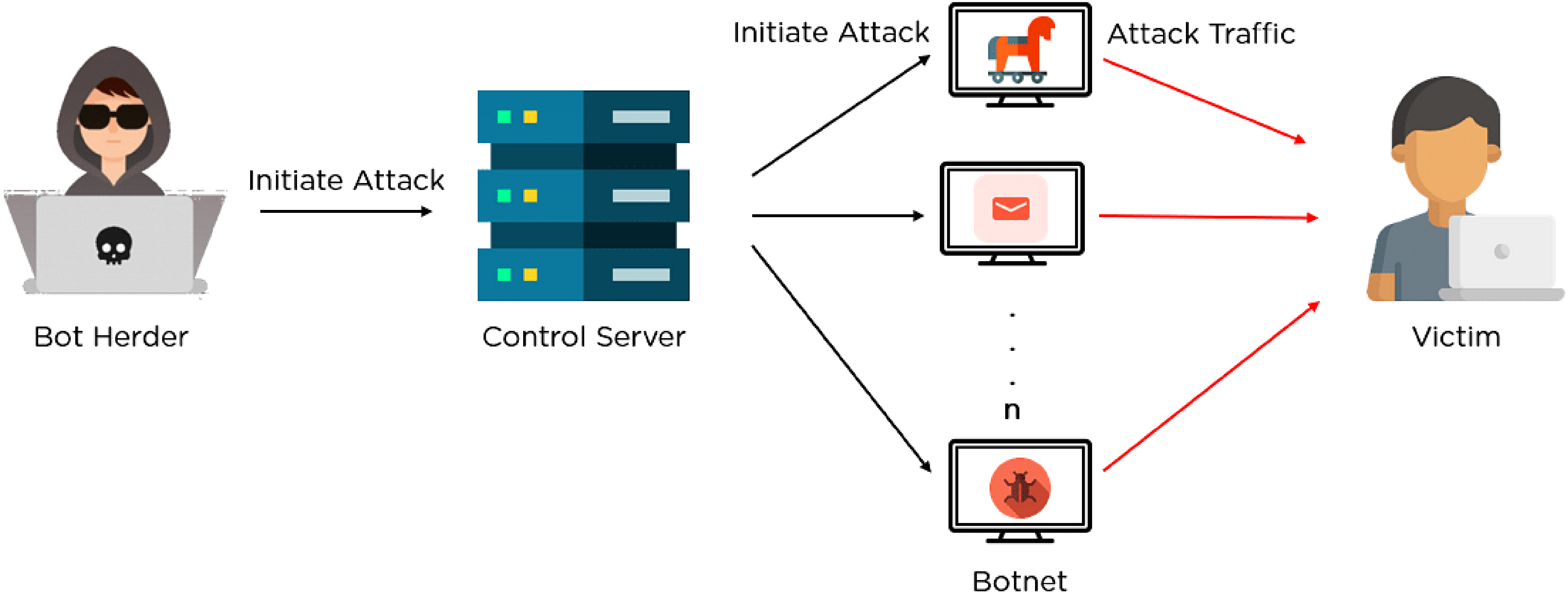
- Once the card information is captured, the criminals can use it to create a clone of the card or make fraudulent purchases.
- Skimming is a common tactic used by identity thieves and can result in significant financial losses for individuals and businesses.

Confidentiality, Integrity and Availability cont…

- **Availability:** Assures that systems work **promptly** and **service is not denied** to ***authorized users***.

Confidentiality, Integrity and Availability cont…

Bots



Confidentiality, Integrity and Availability cont…

Bots

- Bots, short for "**robots**", are ***automated software programs*** that perform repetitive tasks on the internet.
- These bots can be ***beneficial*** or ***malicious***, depending on their **intended purpose**.
- Good bots are designed to ***crawl web pages*** and ***index them for search engines***, ***provide customer service***, ***automate social media postings***, etc.

Confidentiality, Integrity and Availability cont…

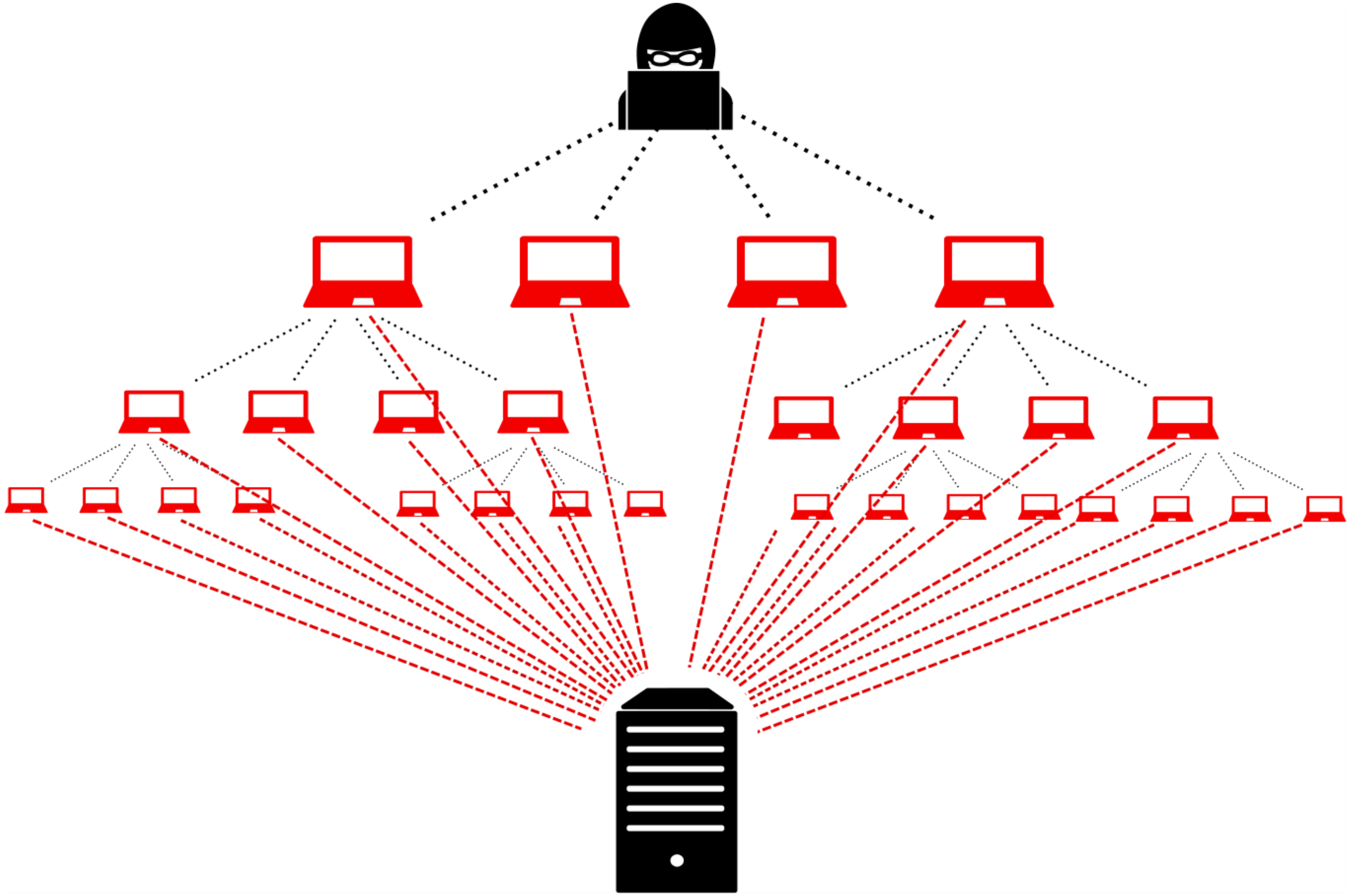
Bots

- On the other hand, **bad bots** can perform various **malicious activities**, such as ***web scraping***, ***distributed denial-of-service attacks***, ***account takeover***, and ***spreading malware***.
- Botnets are networks of infected devices that can be controlled by a single **command and control** server, making them a powerful tool for cybercriminals.

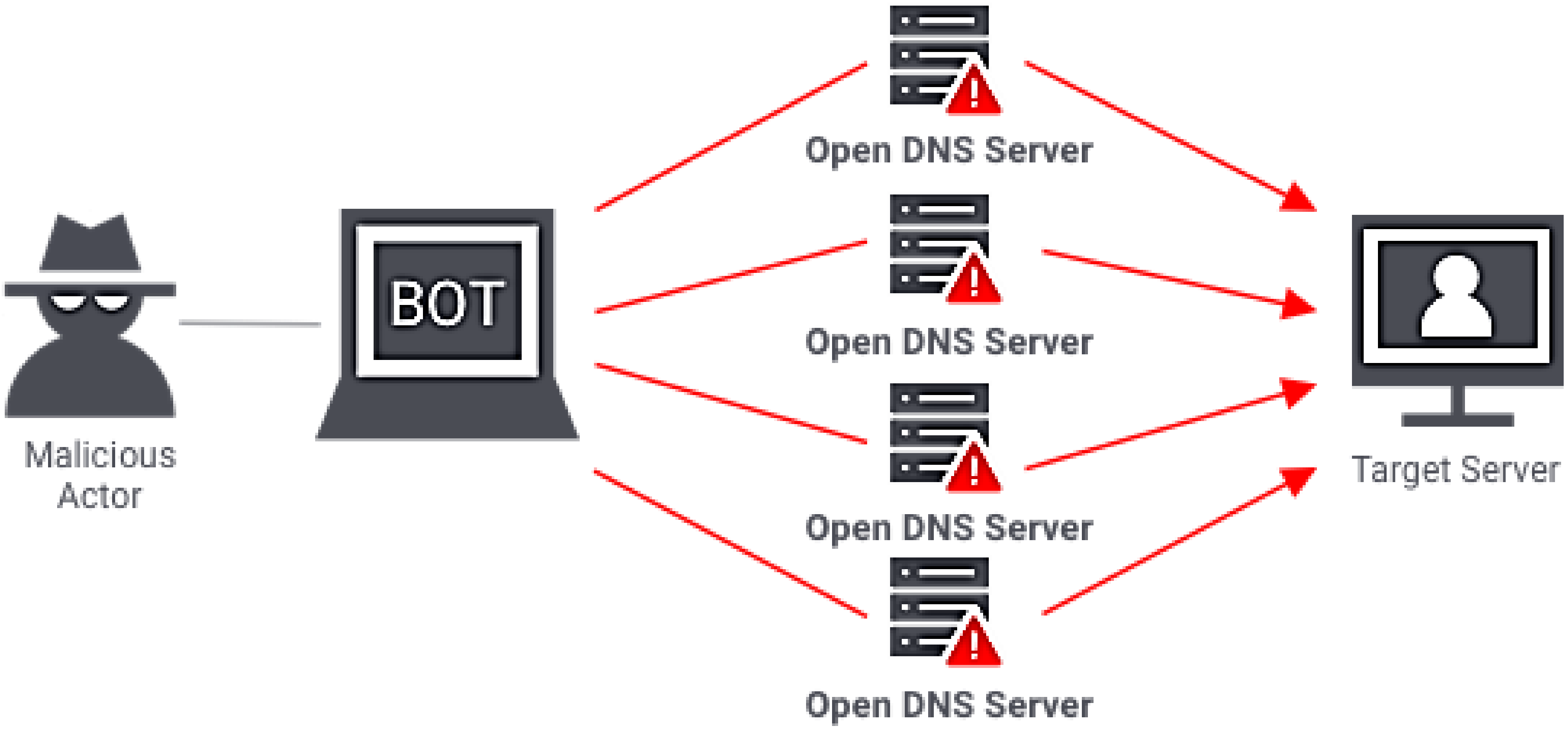
Confidentiality, Integrity and Availability cont… Distribute Denial of Services (DDoS)

- Distributed Denial of Service is a type of cyber attack that aims to **make a website or online service** **unavailable** ***to its intended users***.
- In a DDoS attack, the ***attacker uses*** a ***network of compromised computers*** (**called a botnet**) ***to flood the target website*** or ***service*** **with a huge amount of traffic**, overwhelming its servers and ***causing it to crash*** or ***become extremely slow***, making it **difficult** or **impossible** for ***legitimate users to access it***.

Confidentiality, Integrity and Availability cont…
Distribute Denial of Services (DDoS)



Confidentiality, Integrity and Availability cont… Distribute Denial of Services (DDoS)



Confidentiality, Integrity and Availability cont…

- These three concepts form what is often referred to as the **CIA triad**.
- The three concepts embody the fundamental security objectives for both data and for information and computing services.
- For example, the NIST standard **FIPS 199** (***Standards for Security Categorization of Federal Information and Information Systems***) lists confidentiality, integrity, and availability as the ***three security objectives*** for **information** and for **information systems**.

FIPS (Federal Information Processing Standards)

Confidentiality, Integrity and Availability cont…

- FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:
- **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.

Confidentiality, Integrity and Availability cont…

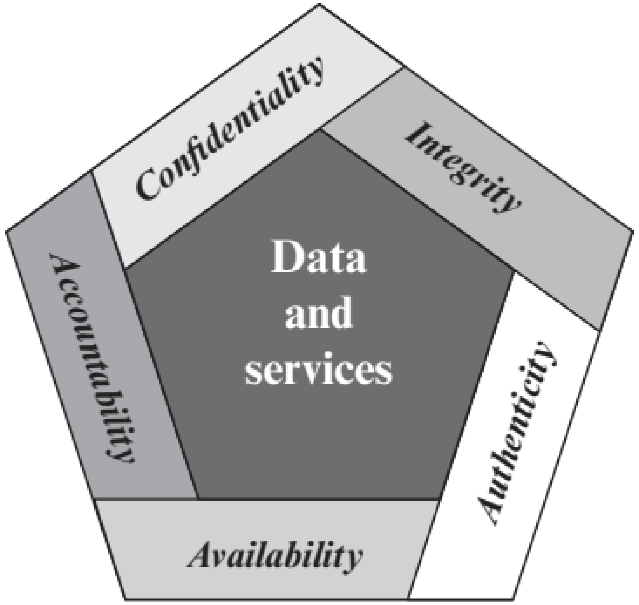
- **Integrity:** Guarding against ***improper information modification*** or ***destruction***, including ***ensuring information nonrepudiation*** and ***authenticity***.
- A loss of integrity is the **unauthorized modification** or **destruction of information**.

Confidentiality, Integrity and Availability cont…

- **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, Integrity and Availability cont…

- Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture.
- Two of the most commonly mentioned are as follows:



Confidentiality, Integrity and Availability cont…

- **Authenticity:** The 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 that each input arriving at the system ***came from a trusted source***.

Confidentiality, Integrity and Availability cont…

- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
- Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.
- Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party.