مركــز الخبيــر التربـوى
AL KHABEER

Cybersecurity

الأمن السيبرانى

By

Dr. Ezz Eldin Hemdan

Become a Cybersecurity Specialist

التأهيل لكى تصبح متخصص فى مجال الأمن السيبرانى

Course Overview

✓ As the course title states, the focus of this course is to explore the field of cybersecurity.

In this course, you will do the following:

- Understand the need for Cybersecurity.
- Learn basic knowledge of network infrastructure and topology.
- Learn about different classes of attacks and attackers.
- How organizations are protecting themselves against these attacks.
- Explore the career options in the arena of cybersecurity.
- Explore basic of ethical hacking process along with cybercrimes investigation.
- Understand the methods of cybercrime investigation.

Attention !

THE CONTENTS OF THIS PRESENTATION FOR EDUCATION PURPOSE ONLY

More Learn, More Power

The Real Experience = Hands On and Troubleshooting

No System is 100 % secure

What is Cybersecurity?

✓ Protection of networked system and data from unauthorized use or harm.

Levels of Cybersecurity

❑ **Personal level**

✓ You need to safeguard your identity, your data, and your computing devices.

❑ **Corporate level**

✓ It is everyone's responsibility to protect the organization's reputation, data, and customers.

❑ **State level**

✓ National security, and the safety and well-being of the citizens are at stake.

Online and Offline Identity

- ✓ **Offline Identity:** Your identity that interacts on a regular basis at home, school or work.
- ✓ **Online Identity:** Your identity while you are in cyberspace.

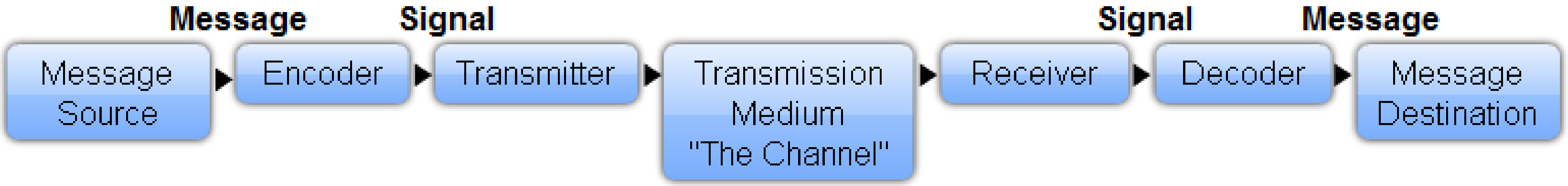
Why do they want your identity?

- Medical benefits, Open credit card accounts, and Obtain loans.

How do the criminals get your money?

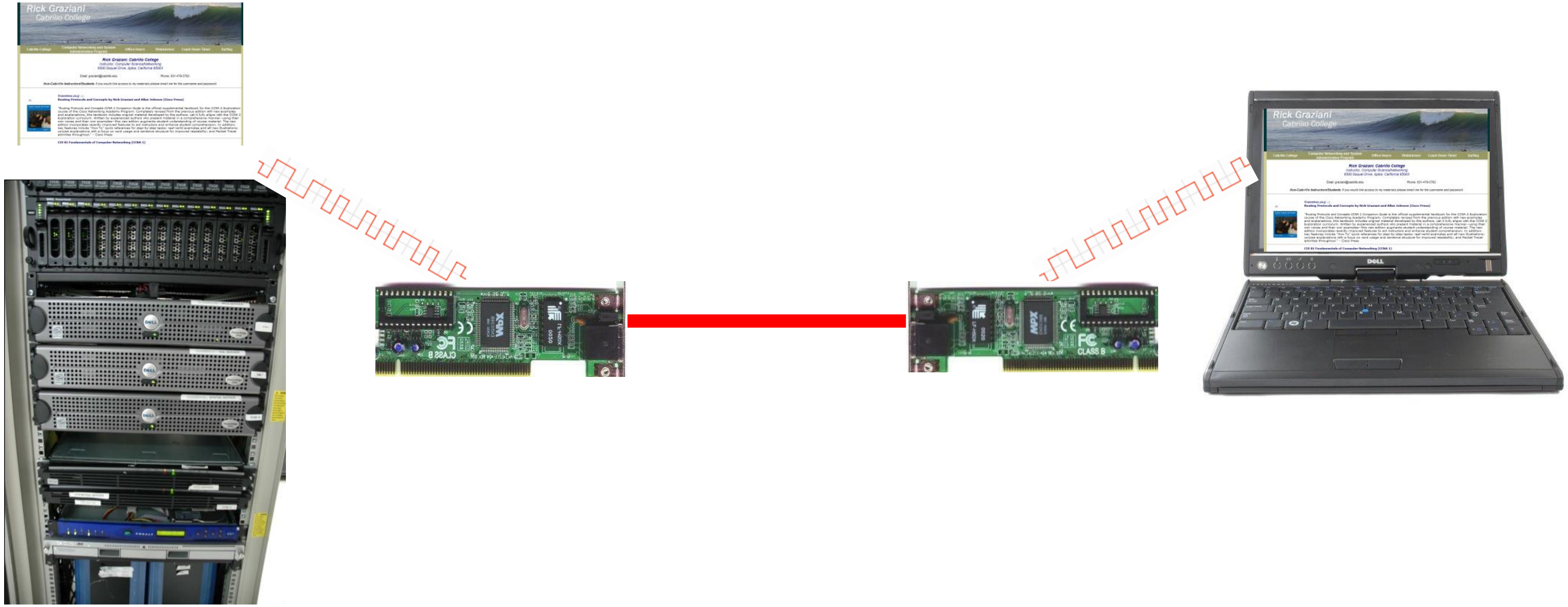
- **Online credentials**
  - ✓ Gives thieves access to your accounts
- **Creative methods**
  - ✓ Trick into wiring money to your friends or family

Communication System



Message Signal Signal Message

Message Source → Encoder → Transmitter → Transmission Medium "The Channel" → Receiver → Decoder → Message Destination



Network Components

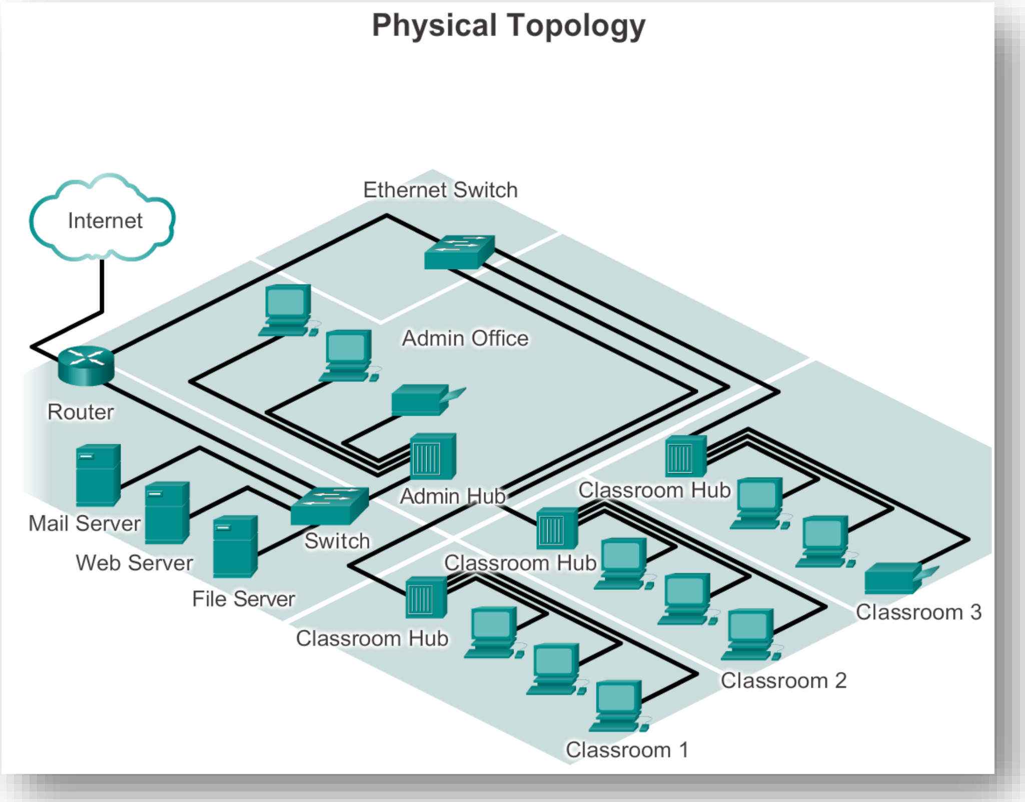
- ✓ **Network** is also defined as a group of two or more computer systems linked together and can communicate.

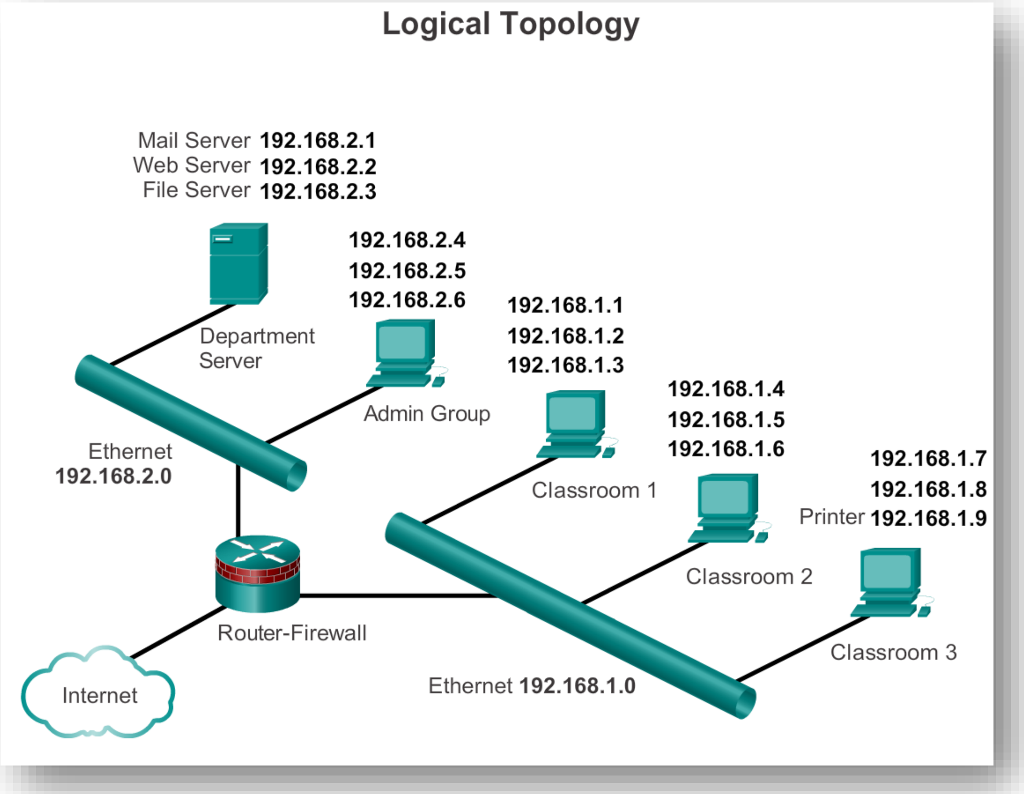
There are three categories of network components:

1. Devices
2. Media
3. Services

Network Topology

- **Topology:** How devices are connected together
  - ✓ **Physical Topology:** It describes how devices are physically cabled
  - ✓ **Logical Topology:** It describes **how devices communicate** across physical topology



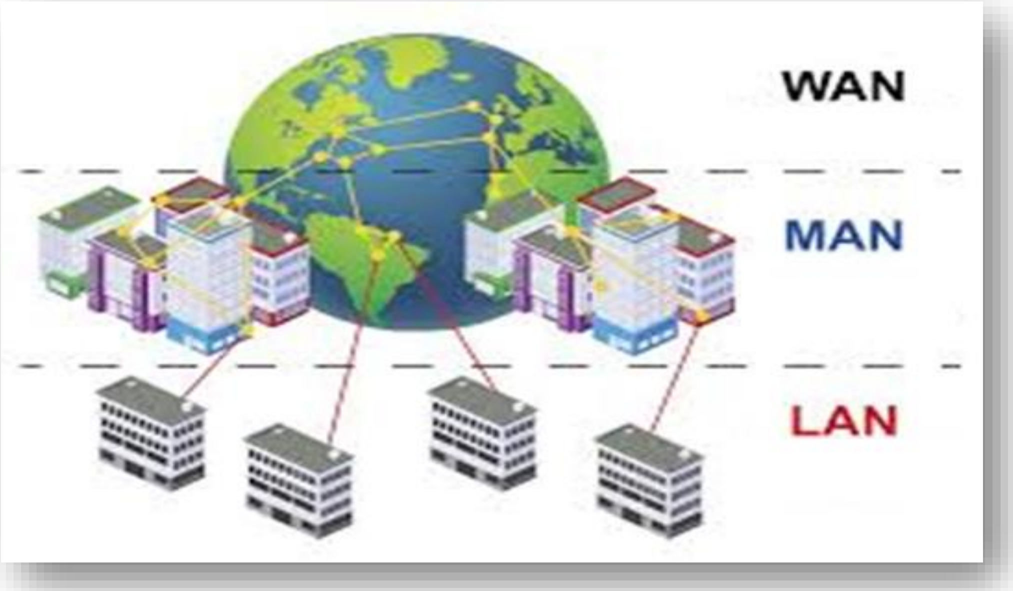


Types of Networks

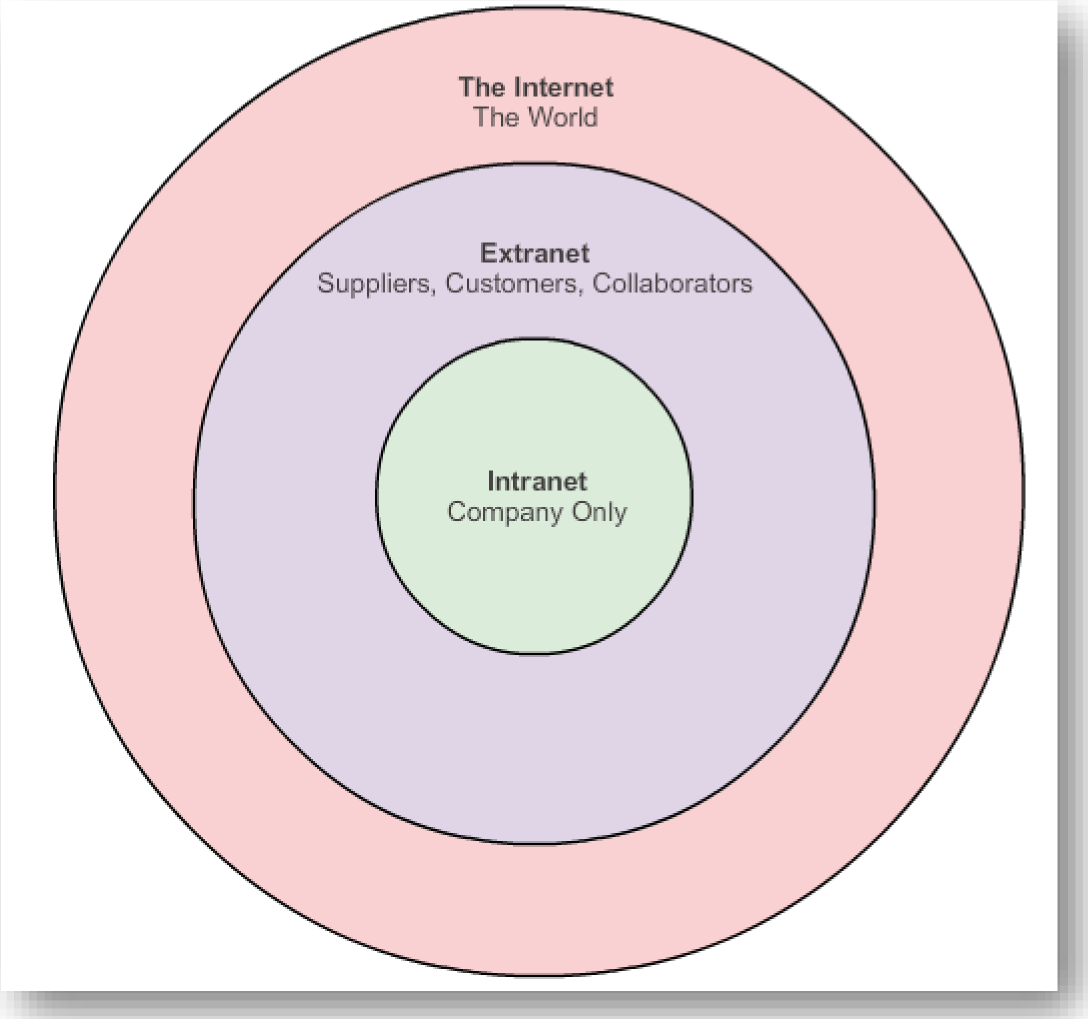
- ✓ **Local Area Network (LAN):** An individual network usually spans a single geographical area, providing services and applications to people within a common organizational structure, such as a single business, campus or region.

- ✓ **Metropolitan Area Network (MAN):** is a group of LANs that are interconnected within small area.

- ✓ **Wide Area Networks (WANs):** are LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



Intranet and Extranet



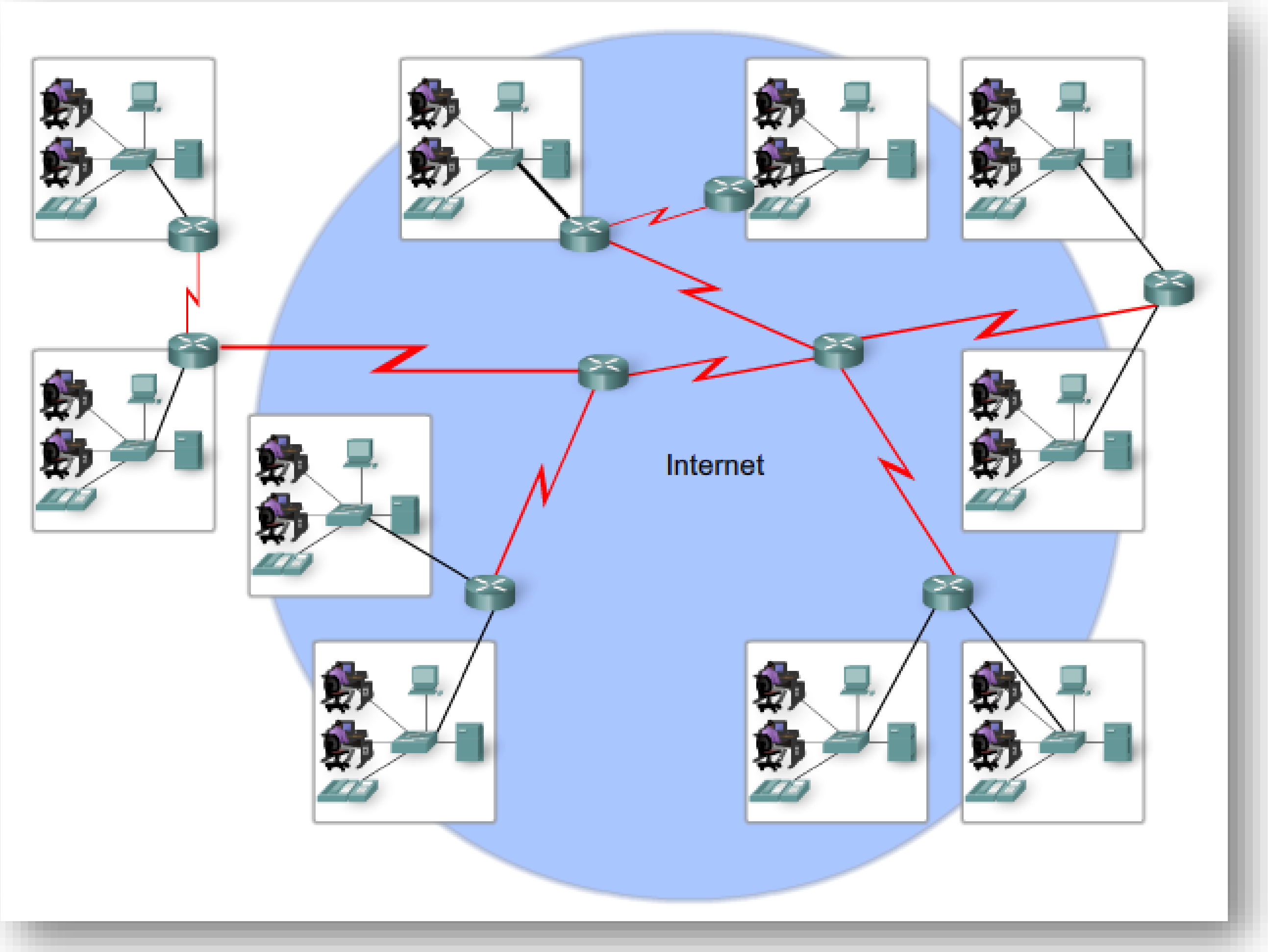
The Internet
The World

Extranet
Suppliers, Customers, Collaborators

Intranet
Company Only

The Internet

- ✓ The **Internet** is defined as a **global mesh of interconnected networks**.



Securing Devices in Network

- ✓ Part of network security is **securing devices**, including **end devices** and **intermediate devices.**
- ✓ Default **usernames and passwords** should be changed immediately.
- ✓ Access to system resources should be restricted to only the individuals that are **authorized** to use those resources.
- ✓ Any unnecessary services and applications should be turned off and **uninstalled**, when possible.
- ✓ **Update** with security patches as they become available.

Basics of Information Security

Proactive and Reactive Security

There are two basic methods of dealing with security breaches:

- ❑ **Reactive Method** is **passive**; when a breach occurs, you respond to it, doing damage control at the same time **you track down how the intruder or attacker got in and cut off** that means of access so **it will not happen again**.

- ❑ **Proactive Method** is **active**; instead of waiting for the hackers to show you where you are vulnerable, **you put on your own hacker hat in relation to your own network** and **set out to find the vulnerabilities yourself**, before **anyone else discovers and exploits them**.

- ✓ **The best security strategy** employs both **reactive** and **proactive** mechanisms. **IDS**, for example, are **reactive in that they detect suspicious network activity so that you can respond to it appropriately.**

Security Concepts

- **Attack**
  - It is any action that br**eaching/violating** security.
- **Hack Value**
  - It is the notion among hackers that something is **worth** doing or interesting.
- **Threat**
  - An action or event that may **compromise security**. A threat is a potential violation of security.
- **Malware**
  - **Malware** is an acorn of **Ma**licious Soft**ware** that describes any malicious software like program or code that harms systems.

Security Concept (cont.)

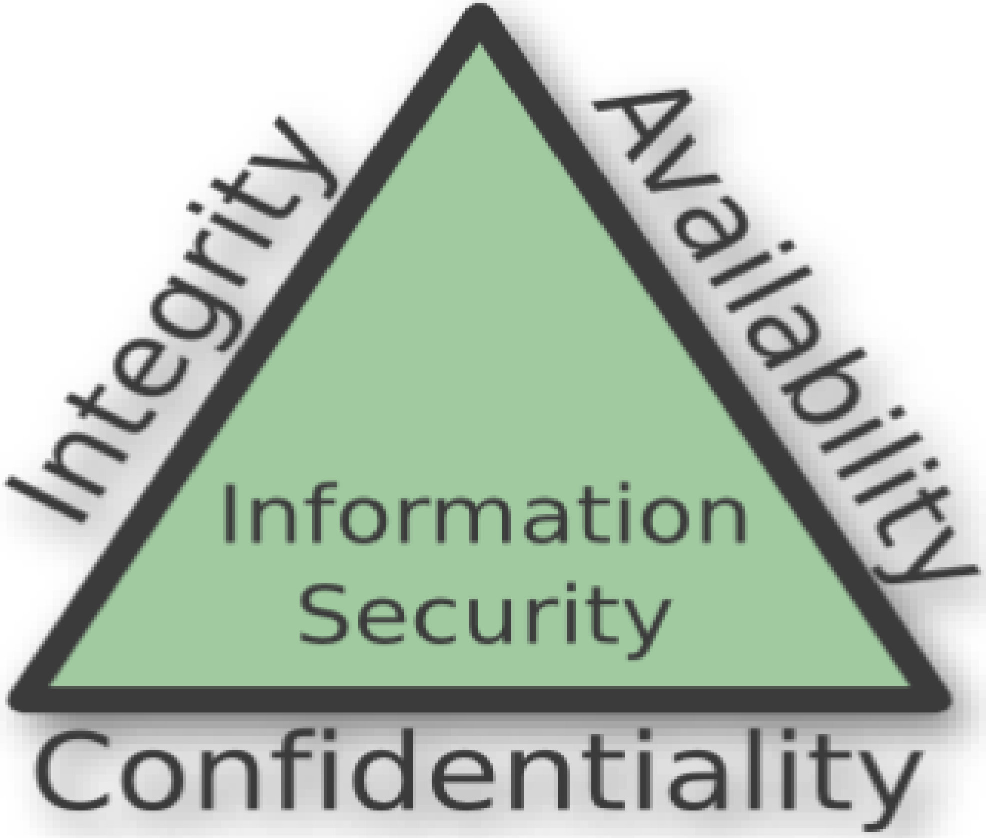
- **Vulnerability**
  - Existence of a weakness design, implementation error that can lead to unexpected breaching of system security.
- **Exploit**
  - A defined way to breach the security of IT system through a **vulnerability**.
- **A Zero-Day**
  - A computer that tries to exploit computer application vulnerabilities that are **unknown** to others or undisclosed to the software developer.
- **Target of Evaluation**
  - It is the **IT system** or **product** that is identified to a **required security evaluation**.

Security Evaluation Plan

Security professionals use their skills to perform **security evaluations**. These tests and evaluations have **three phases**, generally ordered as follows:

1. **Preparation:** The Preparation phase involves a **formal agreement between the security professionals** **or** **security tester** **and** **the organization**. This **agreement** should include the full scope of the test, the types of attacks (**inside** or **outside**) to be used, and the testing types: **white**, **black**, or **grey** box.
2. **Security Evaluation:** During Security Evaluation phase, the tests are conducted, after which the tester prepares a **formal report of vulnerabilities and other findings**.
3. **Conclusion:** The findings are presented to the organization in the **conclusion phase along with any recommendations to improve security.**

Elements of Information Security



These three elements known as CIA or Security Triangle.

Elements of Information Security (cont.)

- **Confidentiality**
  - Assurance that the information is accessible only to authorized users.
- **Integrity**
  - Assurance that not changing or tampering in the information by unauthorized users.
- **Availability**
  - Assurance that the systems that responsible of delivering, processing and accessing information are available when are required by authorized users.

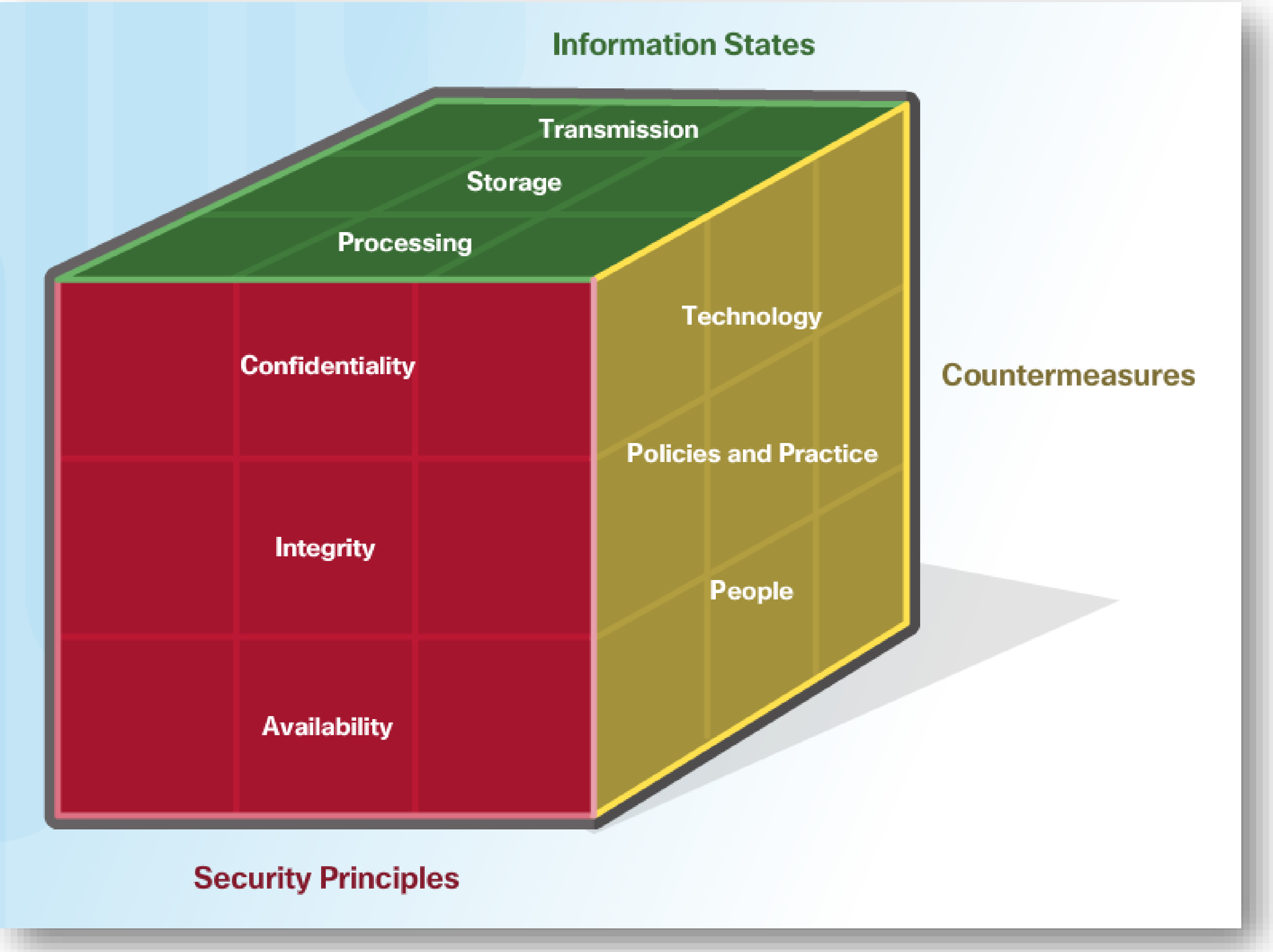
C-I-A-S for Indusial Control System

✓ One of the fundamental tenets of industrial security is to reverse the "**C-I-A**" priority of **Confidentiality**, **Integrity**, and **Availability** because in industrial systems availability is always the **top priority**. However, there is a new letter is "**S**" for **Safety**.

✓ **Cyber attacks** crossing into the physical world of industrial systems means that not only may physical systems go down, but **a sophisticated attack** could further cross the line into **actually taking human life.**

✓ **Thankfully**, that is a line we haven't seen crossed yet, but the evidence and research is mounting that **the risk here is real**.

Cybersecurity Cube



Dimension One: Cybersecurity Principles CIA

- **Confidentiality:** assurance that sensitive information is not intentionally or accidentally disclosed to unauthorized individuals.
- **Integrity:** assurance that information is not intentionally or accidentally modified in such a way as to call into question its trustworthiness or reliability.
- **Availability:** ensuring that authorized individuals have both timely and reliable access to information and information systems.

Dimension Two: Information (data) States

- **Storage:** data at rest (stored in memory, on a drive, or USB flash drive).

- **Transmission:** transferring data between systems.

- **Processing:** performing operations on data like modification, backup, correction

Dimension Three: Security Countermeasures or Safeguards

- **Policy and practices:** administrative controls, such as information security policies, procedures, guidelines, and management directives.

- **Human factors:** ensuring that the users of information systems are aware of their roles and responsibilities. Requires awareness and education programs.

- **Technology:** software- and hardware-based solutions designed to protect information systems, like anti-virus, firewalls, and IDS/IPS systems.

Authentication, Authorization, and Accounting (AAA)

- ❑ **Authentication**: Users and administrators must prove their **identity**. Authentication can be established using **username and password** combinations, challenge and response questions, token cards, and other methods.

- ❑ **Authorization:** Determines **which resources the user can access** and **the operations that the user is allowed to perform**.

- ❑ **Accounting:** Accounting is also known as **auditing**. It means recording what the user accessed, the amount of time the resource is accessed, and any changes made.

Practical Sessions

Introduction to Cybersecurity Labs

By

Dr. Ezz Eldin Hemdan

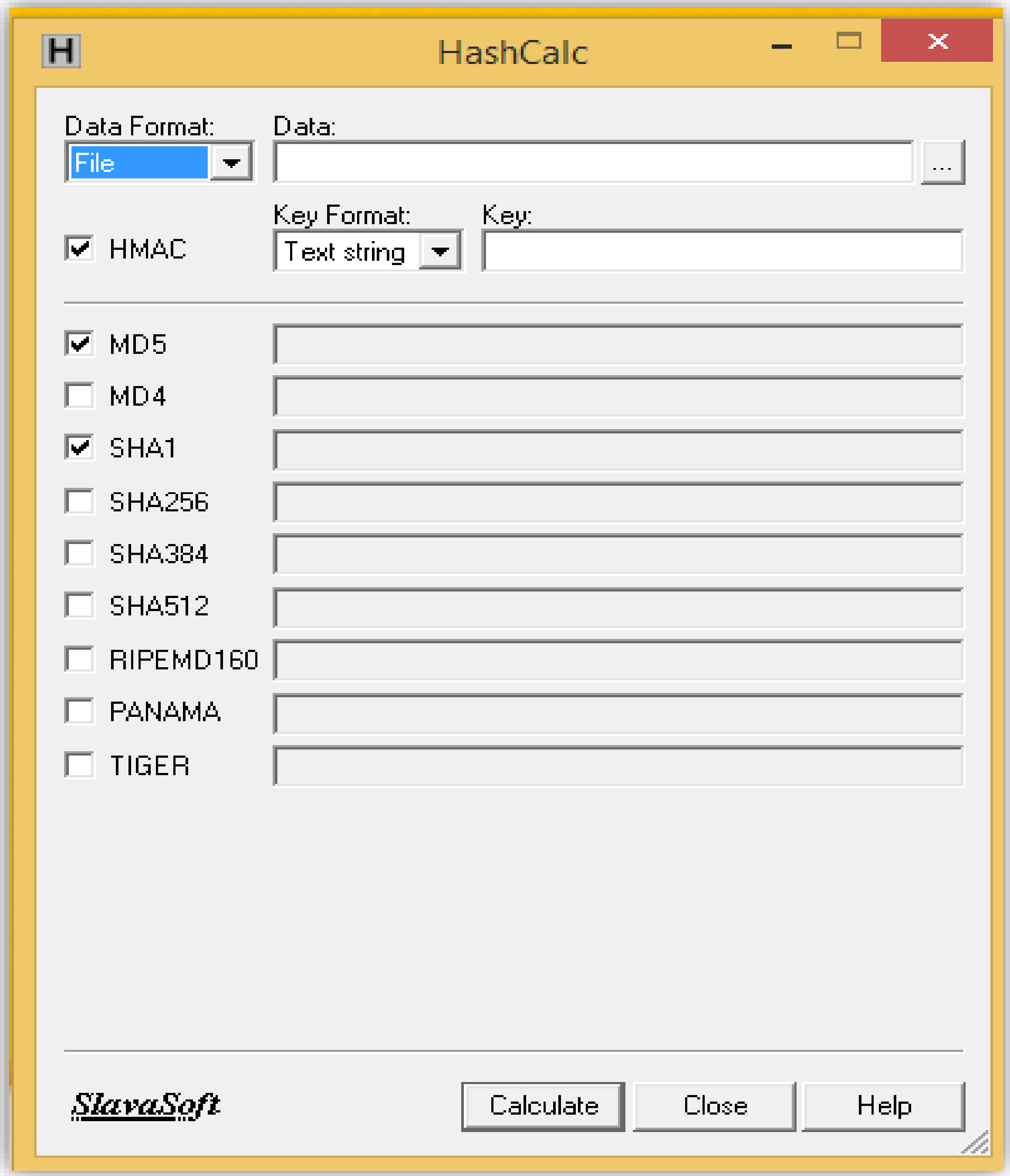
Lab 1: Compare Data with a Hash using HashCalc

✓ Use a hashing program to verify the integrity of data.

Step 1: Create a Text file

- Search your computer for the Notepad program and open it.
- Type some text in the program
- Choose File > Save.
- Navigate to Desktop.
- Type Hash in the File name: field, and click Save.

HashCalc



Data Format: File

Data:

☑ HMAC

Key Format: Text string

Key:

☑ MD5

□ MD4

☑ SHA1

□ SHA256

□ SHA384

□ SHA512

□ RIPEMD160

□ PANAMA

□ TIGER

Step 2: Install HashCalc

- Open a web browser and navigate to http://www.slavasoft.com/download.htm/
- Click Download in the HashCalc 2.02 row.
- Open the hashcalc.zip file and run the setup.exe file inside.
- Follow the installation wizard to install HashCalc.
- Click Finish on the last screen, and close the README file if it opened. You may read the file if you wish.
- HashCalc is now installed and running.

Step 3: Calculate a hash of the File.txt file

Set the following items in HashCalc:

- Data Format: File.
- Data: Click the … button next to the Data field, navigate to the Desktop and choose the File.txt file.
- Uncheck HMAC.
- Uncheck all hash types except MD5.
- Click the Calculate button.

Step 4: Make a change to the File.txt file

- Navigate to the Desktop and open the Hash.txt file.
- Make a minor change to the text, such as deleting a letter, or adding a space or period.
- Click File > Save, and close Notepad.

Step 5: Calculate a new hash of the File.txt file

- Click the Calculate button in HashCalc again.

What is the value next to MD5?

Is the value different from the value recorded in Step 3?

- Place a check mark next to all of the hash types.
- Click Calculate.
- Notice that many of the hash types create a hash of a different length. Why?

Thank you