جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

Resilient Computing and Cybersecurity Center

مركز أبحاث الأمن السيبراني والحوسبة الصامدة

Cybersecurity Week KAUST Academy

Day 1 – Morning Session (Theory)

Introduction to Cybersecurity

rc3.kaust.edu.sa

Presenter Name

City

February 2025

KAUST: Quick Facts

Graduate
merit-based university

Inter-disciplinary
education and research integration

Balanced
research and teaching

Global
robust international & Saudi community

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

Resilient Computing and Cybersecurity Center

Resilient Computing and Cybersecurity Center

PRINCIPAL INVESTIGATORS

Paulo Esteves-Veríssimo

Professor/Director

CYBERESIL

Architectures, middleware and algorithms for resilient modular and distributed computing. Security and dependability, autonomous vehicles from earth to space, digital health and genomics, SDN-based infrastructures, blockchain and cryptocurrencies.

Marc Dacier

Professor/Associate Director

SeRBER

Intrusion detection, intrusion tolerance, network security, cybersecurity, threat intelligence, fraud detection.

Marco Canini

Associate Professor

SANDS

Cloud computing, distributed systems and networking. Recent interest is in designing better systems support for AI/ML and providing practical Implementations deployable in the real-world.

Roberto Di Pietro

Professor

CRI-Lab

Cyber-physical Systems Security, IoT/PLC Security, Drones Security, Satellite/Maritime/Avionics Security, On-line Social Networks, FinTech, Blockchain, Cryptocurrencies.

Elmootazbellah (Mootaz) Elnozahy

Professor

IRS

Fault-tolerance, trusted environments, power management, distributed systems, operating systems, high-performance computing, computer architecture, simulation tools and recently, cryptography, recently, Cryptography and AI/ML implementations.

Shehab Ahmed Elsayed

Professor

MERGE

Power Conversion and Distribution, Subsurface Mechatronics, Renewable Energy Systems

Suhaib Fahmy

Associate Professor

ACCL

Hardware acceleration, hardware virtualisation, embedded systems and networks security, FPGA cloud computing.

Charalambos (Harrys) Konstantinou

Assistant Professor

SENTRY

Secure, trustworthy, and resilient cyber-physical and embedded IoT systems. Critical infrastructures security and resilience with focus on smart grid technologies, renewable energy integration, and real-time simulation.

Basem Shihada

Professor

NETLAB

Broadband wired and wireless comm's networks, incl. multi-hop, sensors, cognitive networks, fiber-wireless integration, optical networks, and green communication. Resilience of cyber-physical system infrastructures, internet and cloud resilience.

CRI-Lab - Cyber Security Research and Innovation Laboratory

PI: *Prof. Roberto Di Pietro, KAUST, CEMSE, RC3*

Vision: To achieve excellence in cybersecurity research addressing both fundamental and applied challenges in the field, as well as to have impact and to generate innovation.

- **Cyber-physical systems:**
  - Satellite/Avionics/Maritime Security
  - UAV Security
  - IoT/PLC Security
- **On-line Social Networks**
- **Fintech, Blockchain, Cryptocurrencies**

Outline

1. Course Introduction

- *Objectives*
- *Structure*
- *Final Exam*

2. Introduction to Cybersecurity

- *What is Cybersecurity?*
- *Security Goals*
- *Common Threats*

3. Famous Real-world Attacks

Course Introduction - Objectives

The objective of this course is to expose the students to **fundamentals, applications and technologies** related to **cybersecurity**, providing the methodological basis, **skills**, and **expertise** to further progress in the cybersecurity domain.

Course Introduction - Structure

- **16** modules (8 theory, 8 hands-on) over **6** days
- **Final exam** on the 7th day

Subjects:

- Introduction to Cybersecurity
- Digital Forensics
- Cryptography
- Authentication (Password Security)
- Network Security
- Web Security
- Social Engineering

Course Introduction - Final Exam

- A small assessment to check your final knowledge on the subjects we studied during the class
- 2 hours
- Multiple-choice questions + a few open questions

What is Security?

Security refers to **freedom** from, or **resilience** against, potential **harm** from external forces.

Beneficiaries of security may be persons and social groups, objects and institutions, ecosystems, and any other entity or phenomenon vulnerable to unwanted change by its environment.

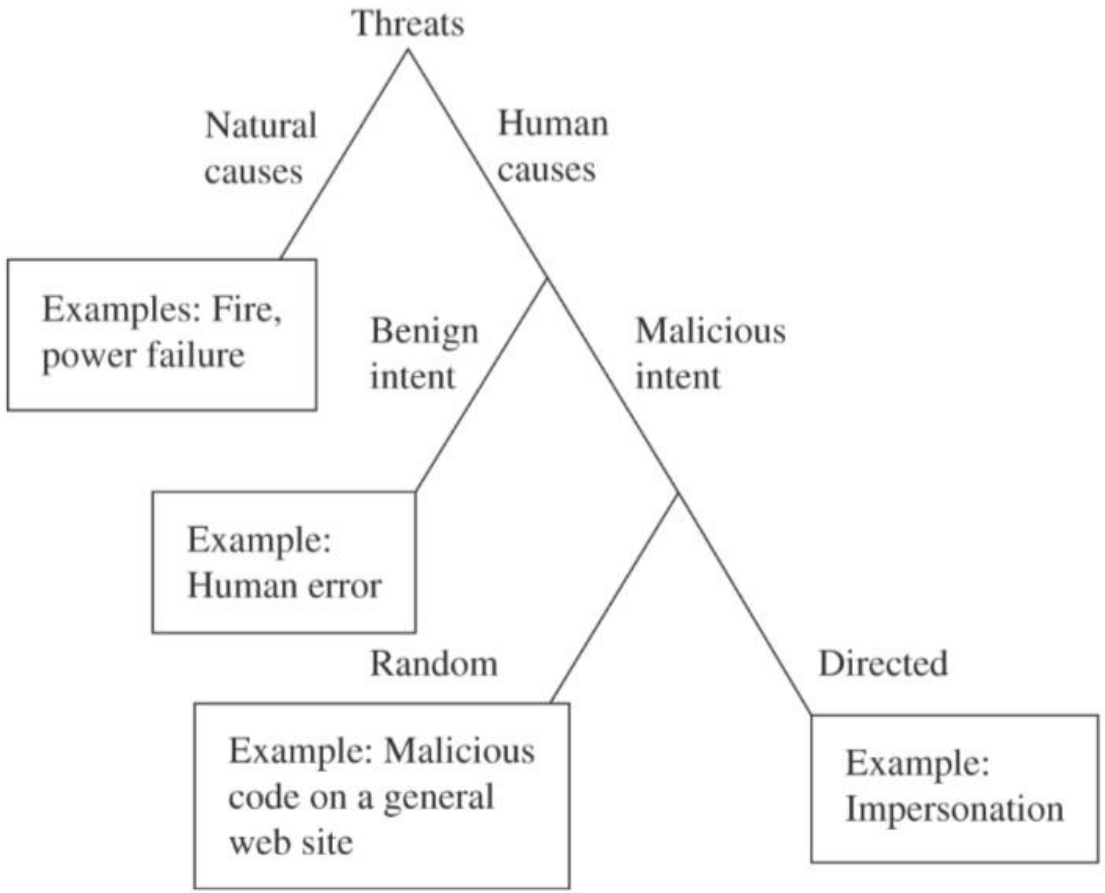
What is Cybersecurity?

Security, in Information Technology (IT), is the **defense** of digital **information** and IT **assets** against internal and external, malicious and accidental **threats**.

Important Terms

- ***Asset***: Stuff we care about, such as information, software, hardware, bandwidth, reputation, privacy, money, etc.
- ***Threat***: The potential for an occurrence that would cause an undesirable effect on an asset. Threats are often evaluated with respect to the CIA triad..
- ***Vulnerability***: A weakness in a system that allows a threat to affect an asset.
- ***Exploit***: A technique that takes advantage of a specific vulnerability to achieve some effect on an asset.
- ***Attack***: A human (so far) who exploits a vulnerability
- ***Controls or countermeasures***: action, device, procedure, or technique to remove or reduce a vulnerability

Kinds of Threats



Why Do Computer Attacks Occur?

- **Who are the attackers?**
  - *Criminals*
  - *Crime organizations*
  - *Rogue states*
  - *Industrial espionage*
  - *Angry employees*
  - *Bored teenagers*

- **Why they do it?**
  - *Profit*

  - *Fun*

  - *Fame*

Attacker Goals

Why are our systems and networks being attacked?

- Steal our information, gather information or money
- Use our hardware, software, or other assets
- Destroy or deny use of our assets (data, information systems, physical resources)
- Corrupt our information
- Harm reputations, make a statement
- Prepare for future action (e.g., botnets)
- Just to see if it can be done
- Penetration testing

Attack Phases

1. **Probe**: passive and active reconnaissance

2. **Penetrate**: gain initial access
   - *Software vulnerabilities*
   - *Weak passwords or configurations*
   - *Credential stealing, social engineering, insiders*

3. **Persist**: maintain access
   - *Compromised accounts, backdoors, rootkits, bots*
   - *Covering tracks*

4. **Propagate**: spread up and out
   - *Privilege escalation*
   - *Extend to other systems or networks*

5. **Profit**: achieve attack goals

Break Time…

Be back in 10 min

What is Digital Forensics?

Digital forensics is the process of **acquiring**, **preserving**, and **analyzing** digital information to be used as **evidence** in various cases.

Digital Evidence

Digital Evidence refers to data and information stored, transmitted, or received by an electronic device that can be used as evidence in an investigation.

Digital Evidence Types	
Volatile Evidence	• Memory • Network Connections • Running Process • Open Files
Non-volatile Evidence	• Hard Drives • USB Storages • CD/DVD

Digital Forensics Process

Identification	• Identify the purpose of the investigation. • Identify the required resources.
Preservation	• Secure, maintain, and ensure that the evidence is not tampered with or compromised.
Analysis	• Examine the evidence and recover relevant artifacts to draw clear conclusions.
Documentation	• Document the crime scene, including photographing, sketching, and crime-scene mapping.
Presentation	• Summarize and explain conclusions with the help of gathered facts.

Essential Tools in Computer Forensics

- **Autopsy**: Open-source tool for disk image analysis and file recovery.
- **Wireshark**: Analyzes network traffic to detect suspicious activities.
- **Volatility**: Memory forensics tool to identify malware and unauthorized access.
- **ExifTool**: Extracts metadata from files (e.g., images, documents).
- **Hex Editors**: Views and edits file content in hexadecimal format.

Computer Security Issues

- **Malware**
  - *Ransomware*
  - *Spyware*
  - *Adware*
  - *Trojans*
  - *Worm*
  - *Rootkits*
  - *Keyloggers*
  - *Virus*
- **Distributed Denial of Service**

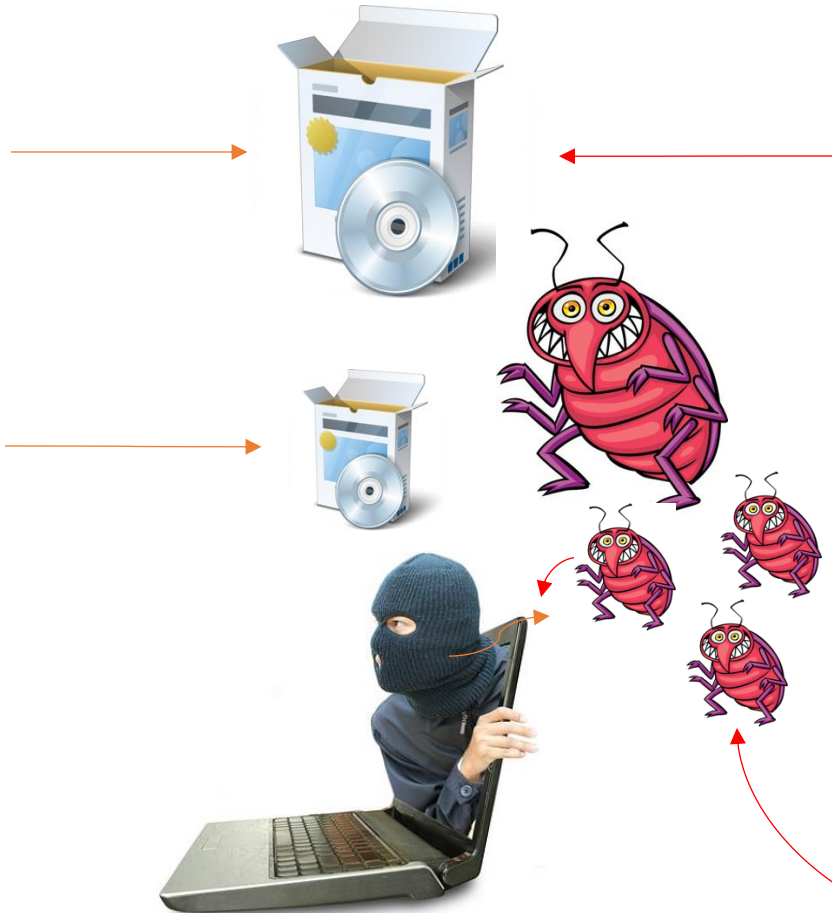
- **Social Engineering**
  - *Phishing*
  - *Baiting*
  - *Pretexting*
  - *Tailgating*
  - *Honeytrap*
  - *Smishing*
- **Zero-day**
- **Botnet**
- **Identity Theft**

Why do these attacks happen?

- **Economic factors**
  - *Lack of incentives for secure software*
  - *Security is difficult, expensive, and takes time*
- **Human factors**
  - *Lack of security training for software engineers*
  - *Largely uneducated population*
- **Technological factors**
  - *Unsafe program languages*
  - *Software are complex, dynamic, and increasingly so*
  - *Making things secure are hard*
  - *Security may make things harder to use*

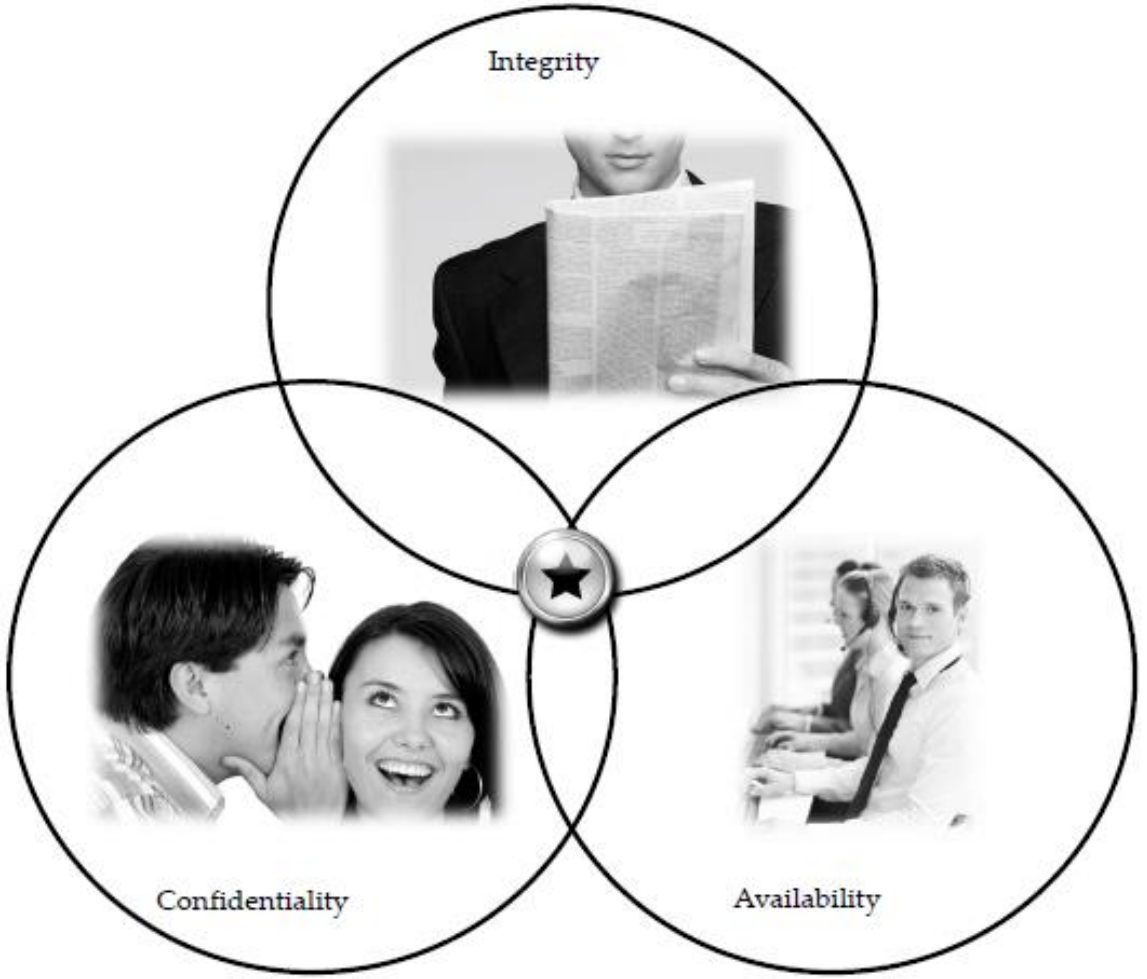
Software Threat Lifecycle

Software Developer



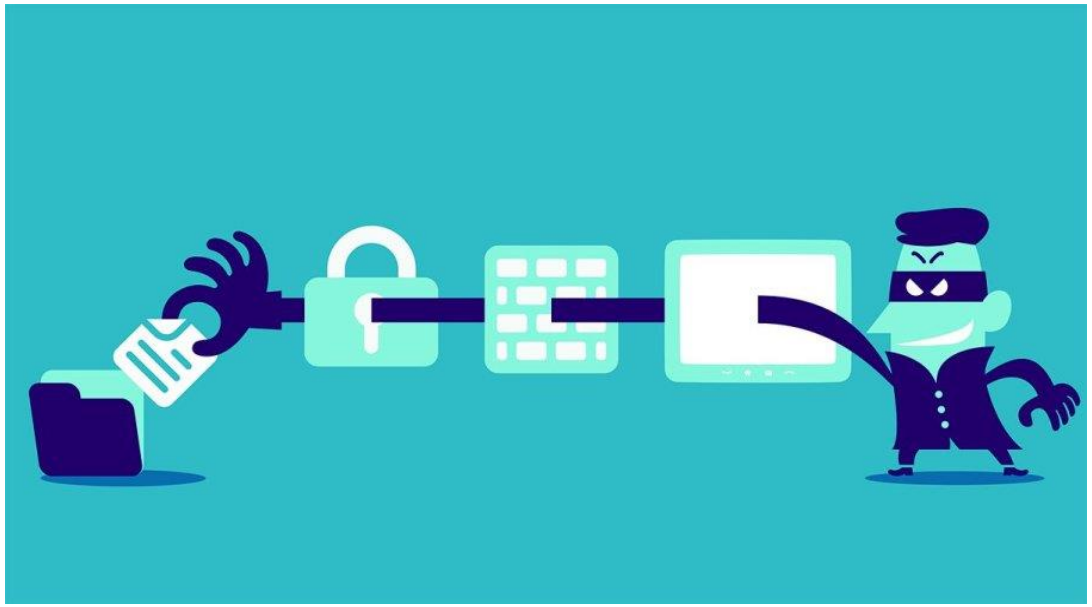
Cybersecurity Goals – The CIA Triad

- **Confidentiality**
  - Keeping data and resources hidden
- **Integrity**
  - Data integrity (integrity)
  - Origin integrity (authentication)
- **Availability**
  - Enabling access to data and resources



Confidentiality

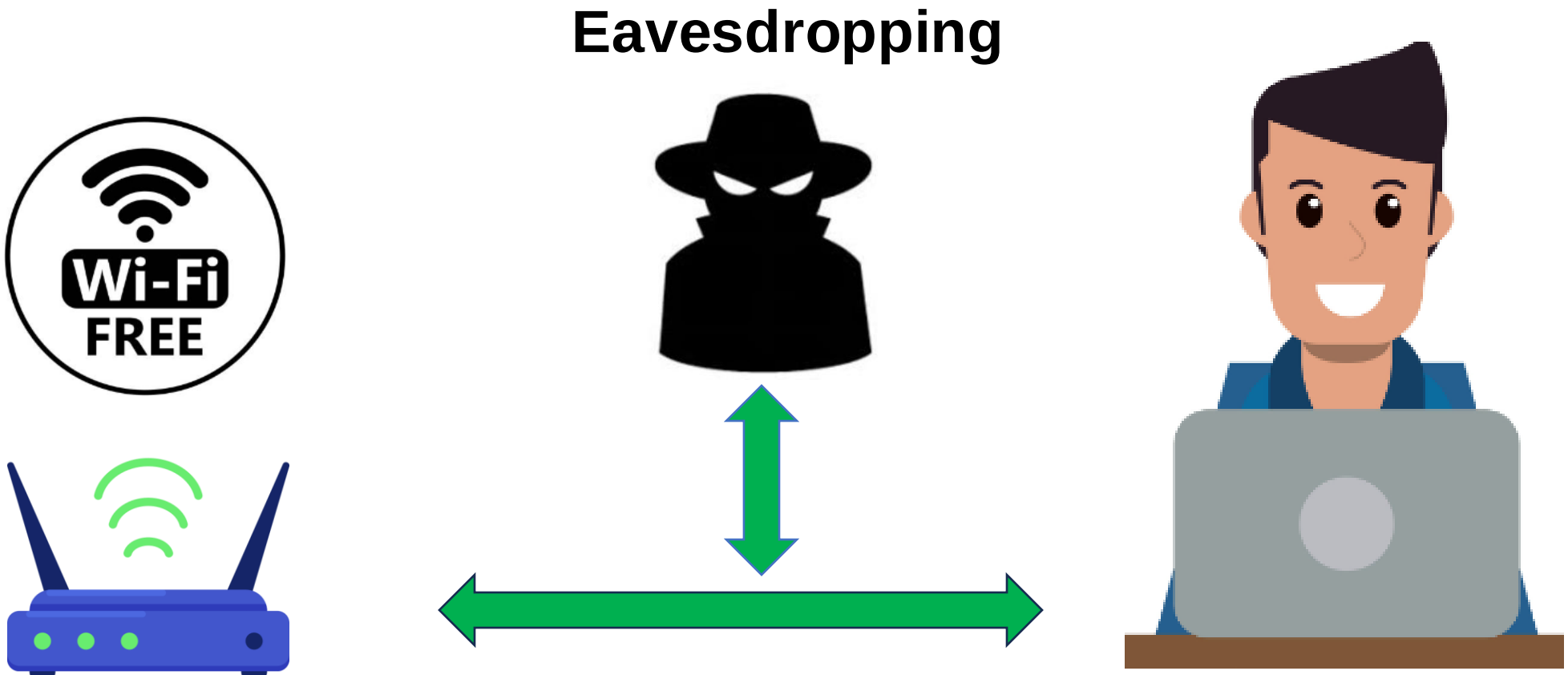
Protecting **information** from disclosure to **unauthorized** entities.



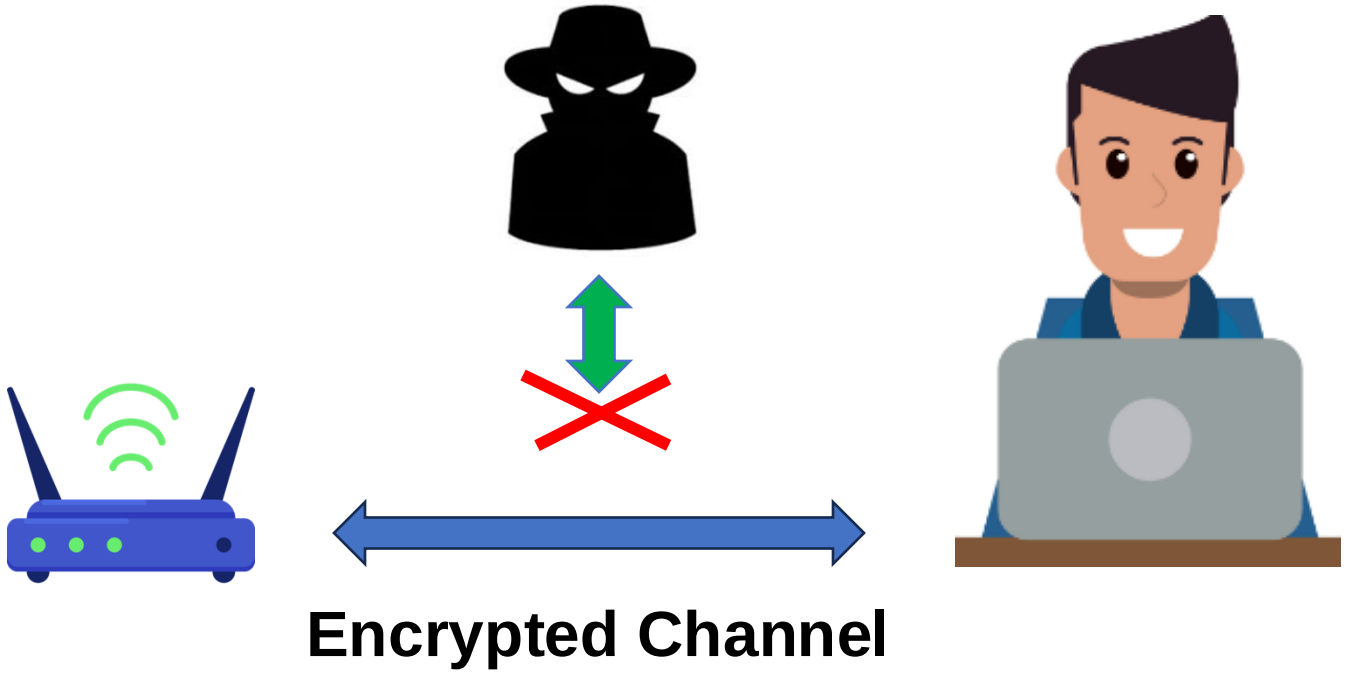
How:

- Encryption
- Access Control
- Authentication

Confidentiality - Example

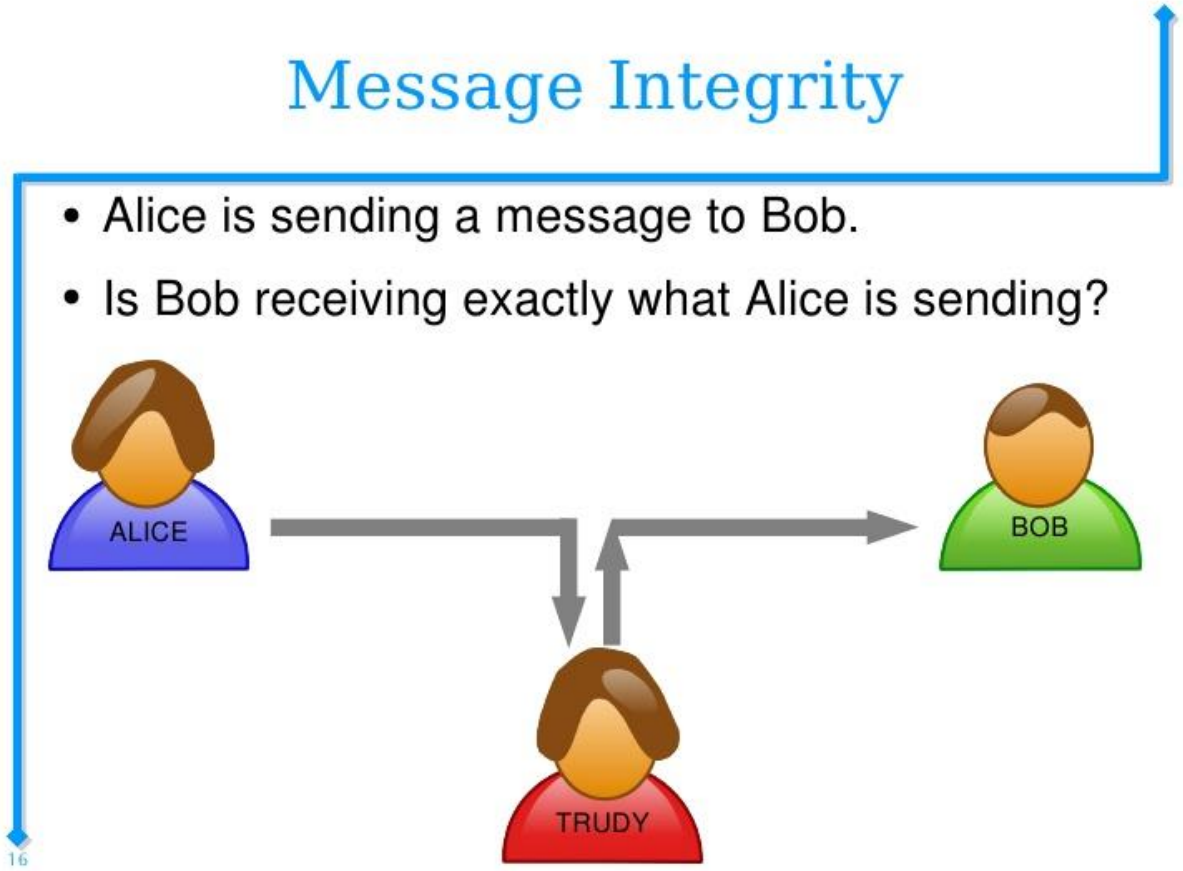


Confidentiality - Example



- Only use encrypted wireless channels
- WPA3 (January 2018) is the current WiFi standard
- Always use https:// (SSL/TLS) in your browser
- Use encrypted email if possible

Integrity

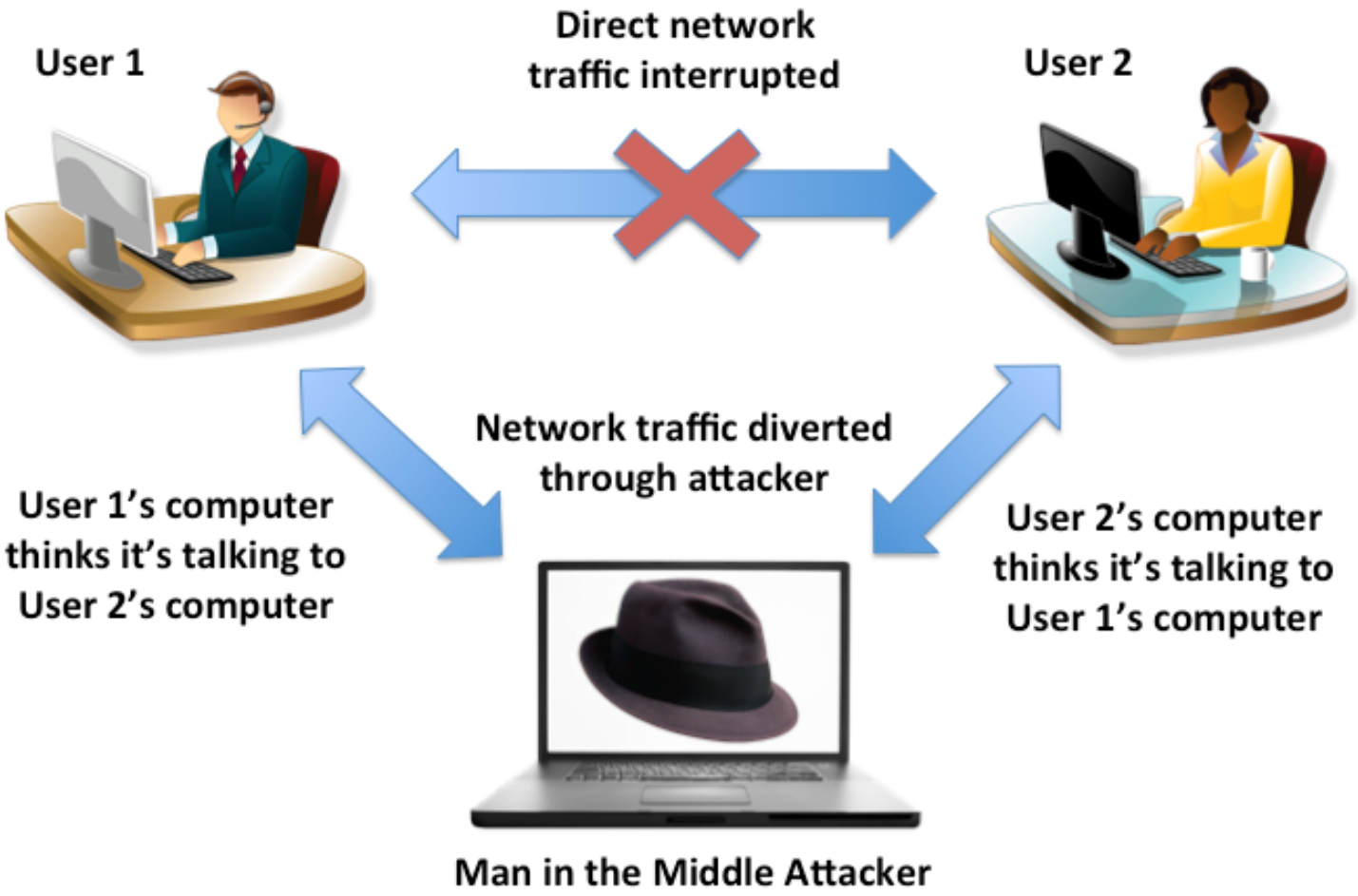


The property that **information** has not be **altered** in an unauthorized way.

How:

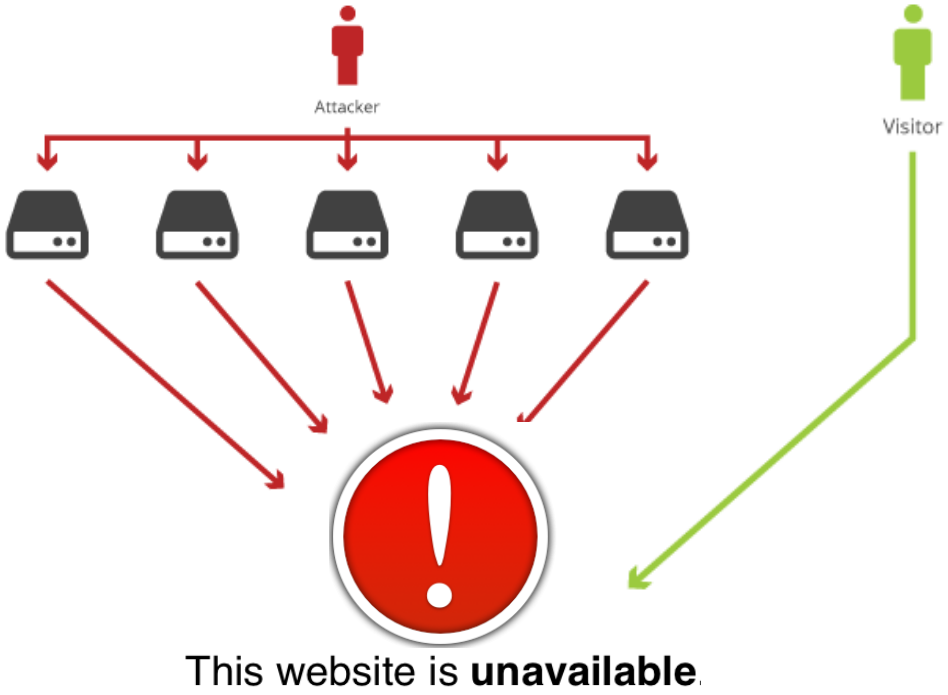
- Checksums
- Error Correcting Codes
- Hashing

Integrity - Example



Availability

For any information system to serve its purpose, the information must be available when it is needed.

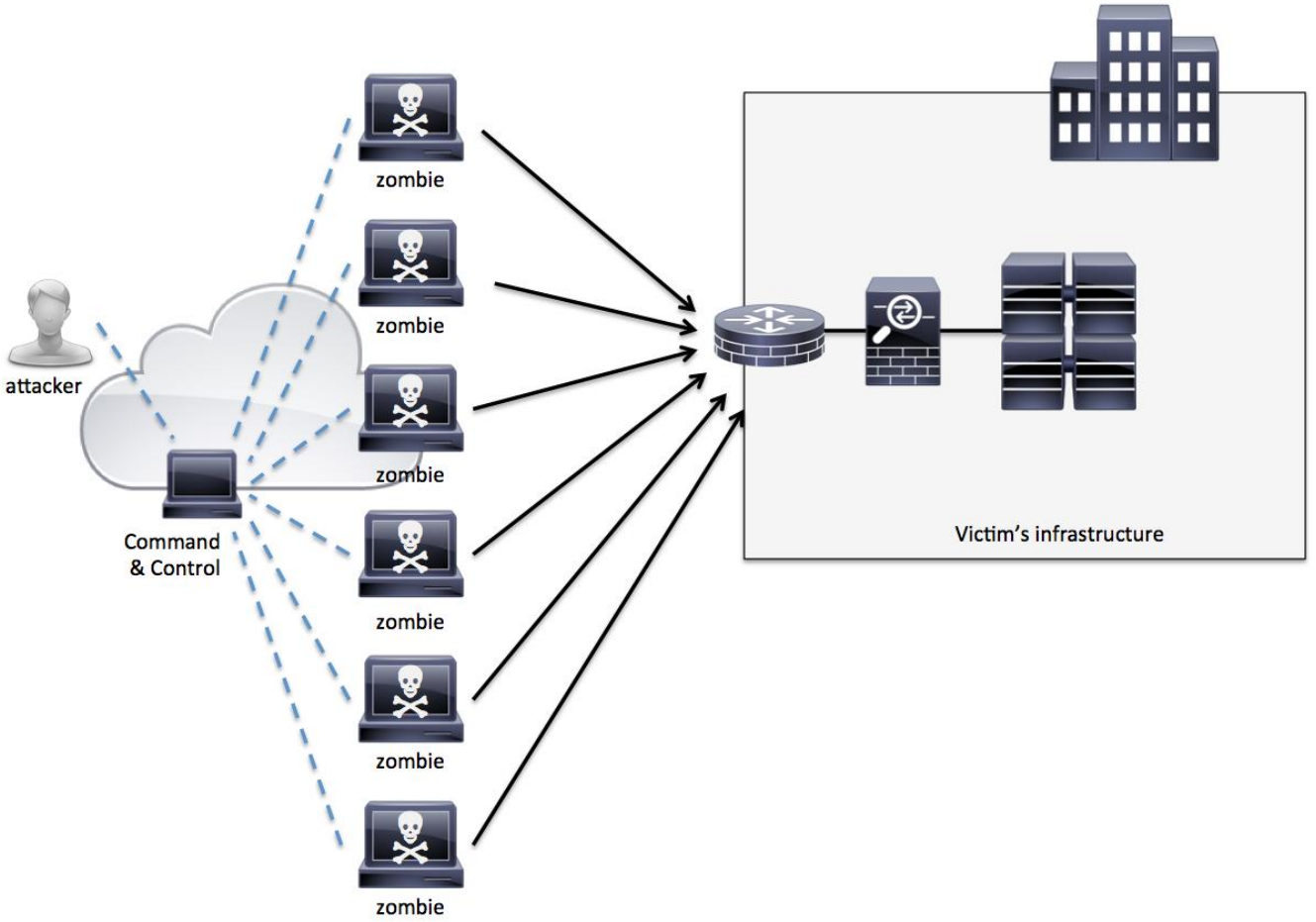


How:

- Physical Protections
- Computational Redundancies

Availability - Example

- A cyberattack in which the perpetrator aims to make a machine or a network resource **unavailable** to its intended users.
- Leverages a network of compromised computers (BotNets, Zombie Computers) to send huge amounts of data (random data or legitimate requests) to overwhelm the target.



More definitions

Policy

- A statement of what is and what is not allowed
- Divides the world into secure and non-secure states
- A secure system starts in a secure state. All transitions keep it in a secure state.

Mechanism

- A method, tool, or procedure for enforcing a security policy

More Definitions

Assurance

- Evidence of how much to trust a system
- Evidence can include
  - *System specifications*
  - *Design*
  - *Implementation*
- Mappings between the levels

Example:

- Why do you trust Aspirin from a major manufacturer?
  - *FDA certifies the aspirin recipe*
  - *Factory follows manufacturing standards*
  - *Safety seals on bottles*
- Analogy to software assurance

Biggest Data Breaches

1) Yahoo August 2013

- 3 Billion Accounts

2) Alibaba November 2019

- 1.1 Billion pieces of user data, including usernames and mobile numbers

3) LinkedIn June 2021

- Data associated with 700 Million users

4) Weibo March 2020

- 538 Million User Accounts

5) Facebook April 2019

- Information related to more than 530 million Facebook users and included phone numbers, account names, and Facebook IDs

6) Marriot September 2018

- Data associated with 500 Million users

Biggest Ransomware Attacks

1) NotPetya 2017

- Physhing
- Estimated Monetary Impact $10 billion

2) Wannacry 2017

- vulnerability in SMB protocol
- Estimated Monetary Impact $4 billion

3) GrandCrab 2018/2019

- Phishing
- Estimated Monetary Impact $2 billion

4) Locky March 2020

- phishing emails distributing a macro in a Word document
- Estimated Monetary Impact $1 billion

5) Ryuk 2018-present

- initial compromise, usually TrickBot infection
- Estimated Monetary Impact $150 million

6) REvil 2019/2021

- zero-day vulnerability
- Estimated Monetary Impact $70 million

Worst Phishing Attacks in History

1) Facebook/Google Scam

- carefully crafted phishing emails with fake invoices, contracts and letters to employees at both these tech giants, falsely billing them for millions of dollars over a period of two years between 2013 to 2015.

2) NotPetya

- In June 2017, the world woke up to the most devastating cyberattack in history that spread across the planet like wildfire, ushering in a new era of cyber warfare.

3) Ukrainian Powe Grid

- In December 2015, a Ukrainian electricity distribution company, became the world's first power grid provider to be taken down in a cyberattack. The threat actors were able to attack the target and force a blackout through a phishing email.

جامعة الملك عبدالله للعلوم والتقنية
King Abdullah University of Science and Technology

Resilient Computing and Cybersecurity Center

Do you have any questions?

rc3.kaust.edu.sa

Follow us @rc3kaust