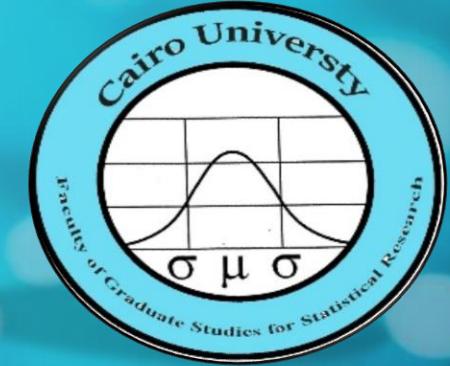




Cairo University



Information Security

(SE205)

Dr. Hany Mohamed

Course Objectives

- Explain the objectives of information security (Servers and Clients).
- Explain the importance of each of confidentiality, integrity, and availability.
- Understand the basic categories of threats to computers and networks.
- Understand various cryptographic algorithms.
- Describe public-key cryptosystem.
- Discuss the fundamental ideas of public-key cryptography.
- Describe the Secure Software design and programming techniques.
- Discuss Web security and Firewalls.
- Understand Intrusions and intrusion detection.
- Design Intrusion Detection System IDS (**python**).

Course Syllabus

- **Unit 1:** **attacks on computer and computer security:**
 - Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security.
- **Unit 2:** **Cryptography:** Concepts and Techniques: Introduction, **encryption** and **decryption**, plain text and cipher text, substitution techniques, transposition techniques.

Course Syllabus

Unit 3:

- Symmetric key Ciphers: Block Cipher principles & Algorithms(DES, AES, Blowfish), Differential and Linear Cryptanalysis, Block cipher modes of operation, Stream ciphers, RC4, Location and placement of encryption function, Key distribution.
- Asymmetric key Ciphers: Principles of public key cryptosystems, Algorithms(RSA, Diffie-Hellman, ECC), Key Distribution.

Course Syllabus

- **Unit 4:**

- **Message Authentication Algorithms and Hash Functions:** Authentication requirements, Functions, Message authentication codes, Hash Functions, Secure hash algorithm, Whirlpool, HMAC, CMAC, Digital signatures, knapsack algorithm
- **Authentication Applications:** Kerberos, X.509 Authentication Service, Public — Key Infrastructure, Biometric Authentication

Course Syllabus

Unit 5:

- **Secure Software design and programming techniques, Web security and Firewalls, Web security considerations, Secure Socket Layer and Transport Layer Security, Secure electronic transaction.**
- **Intruders, Virus and Firewalls: Intruders, Intrusion detection, password management, Virus and related threats, Countermeasures, Firewall design principles, Types of firewalls.**
- **Case Studies on Cryptography and security: Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability, Virtual Elections.**

Course References and Outcomes

TEXT BOOKS:

1. Cryptography and Network Security: William Stallings, Pearson Education.
2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill.

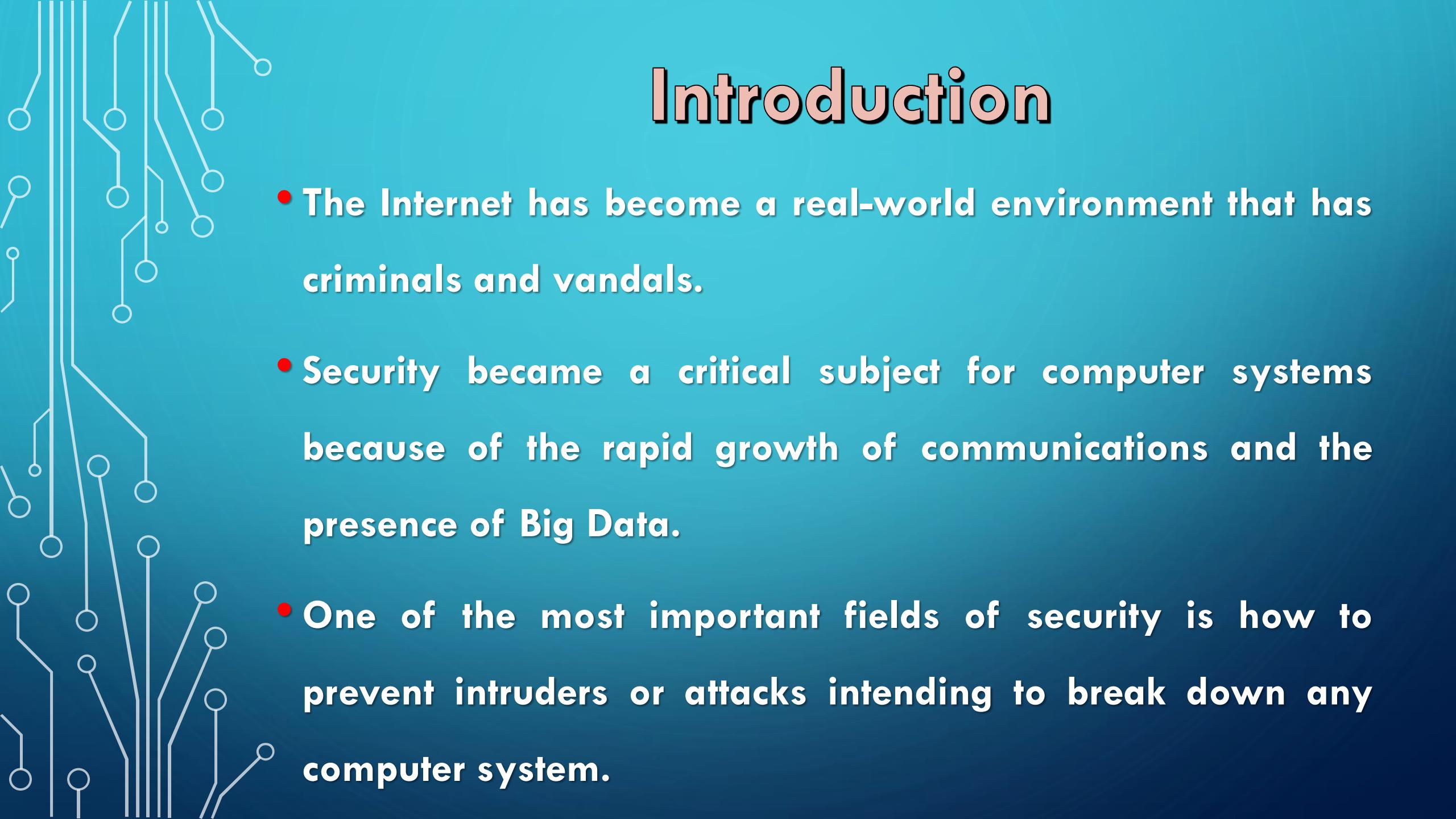
Outcomes:

- Student will be able to understand basic **cryptographic algorithms**, message and web authentication and security issues.
- Ability to identify information system requirements for both of them such as client and server.
- Ability to understand the current legal issues towards information security.
- Ability to understand the main principles during designing and development a secure system software.

Information Security

Unit 1: Attacks on Computers
and Computer Security



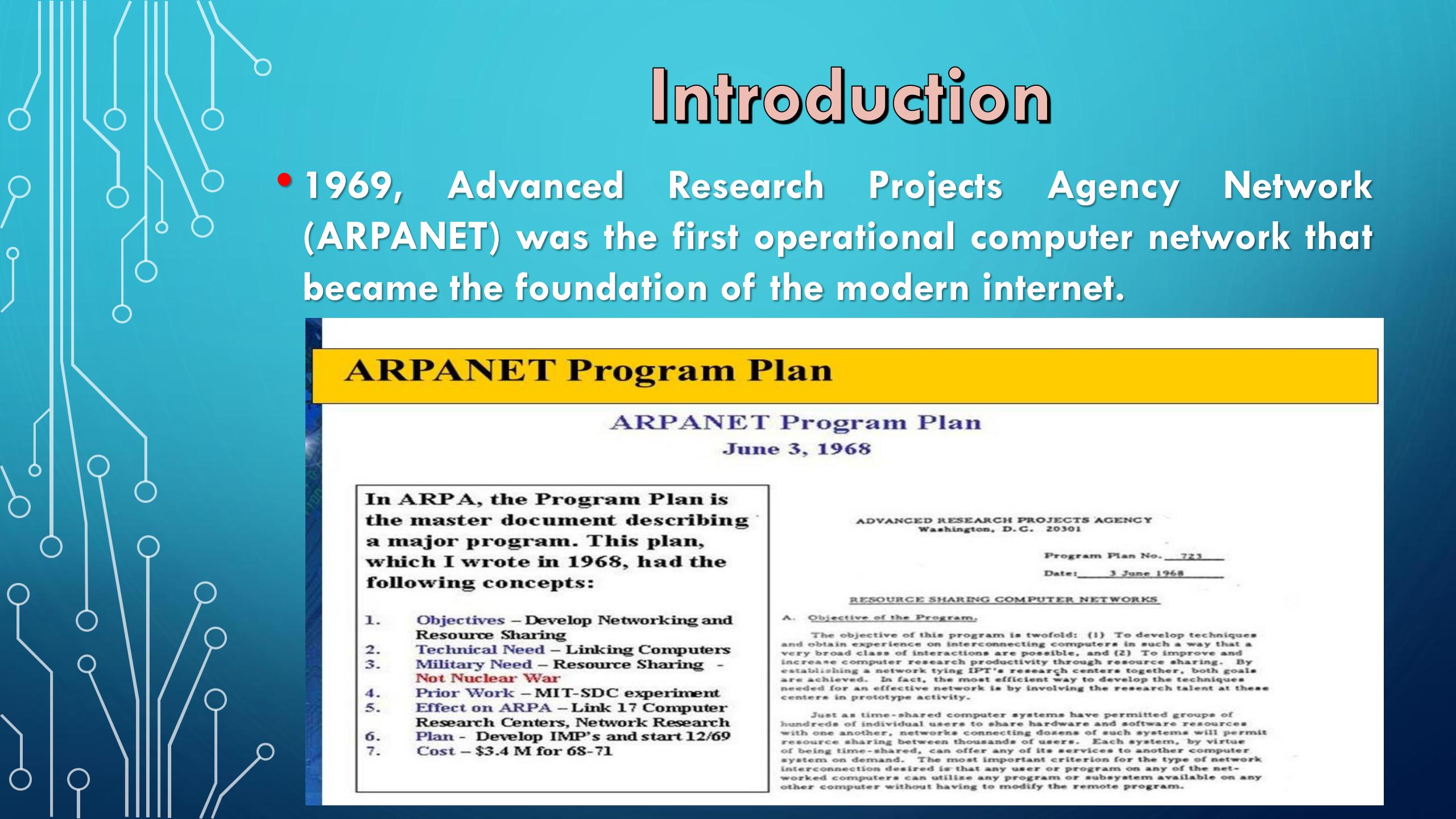


Introduction

- The Internet has become a real-world environment that has criminals and vandals.
- Security became a critical subject for computer systems because of the rapid growth of communications and the presence of Big Data.
- One of the most important fields of security is how to prevent intruders or attacks intending to break down any computer system.

Introduction

- 1969, Advanced Research Projects Agency Network (ARPANET) was the first operational computer network that became the foundation of the modern internet.



ARPANET Program Plan

ARPANET Program Plan
June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - **Not Nuclear War**
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research Plan - Develop IMP's and start 12/69
6. Cost – \$3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

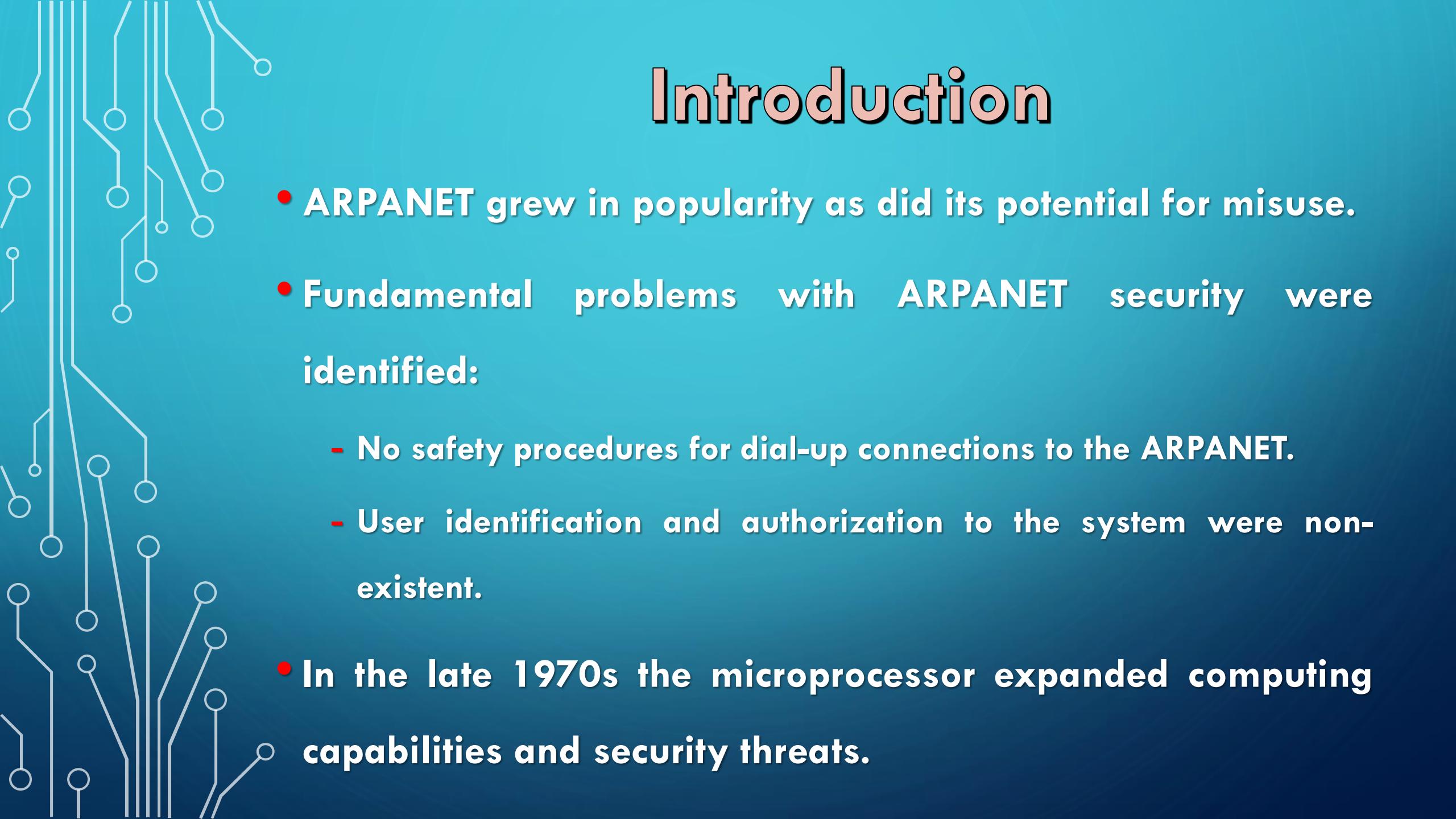
Program Plan No. 723
Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

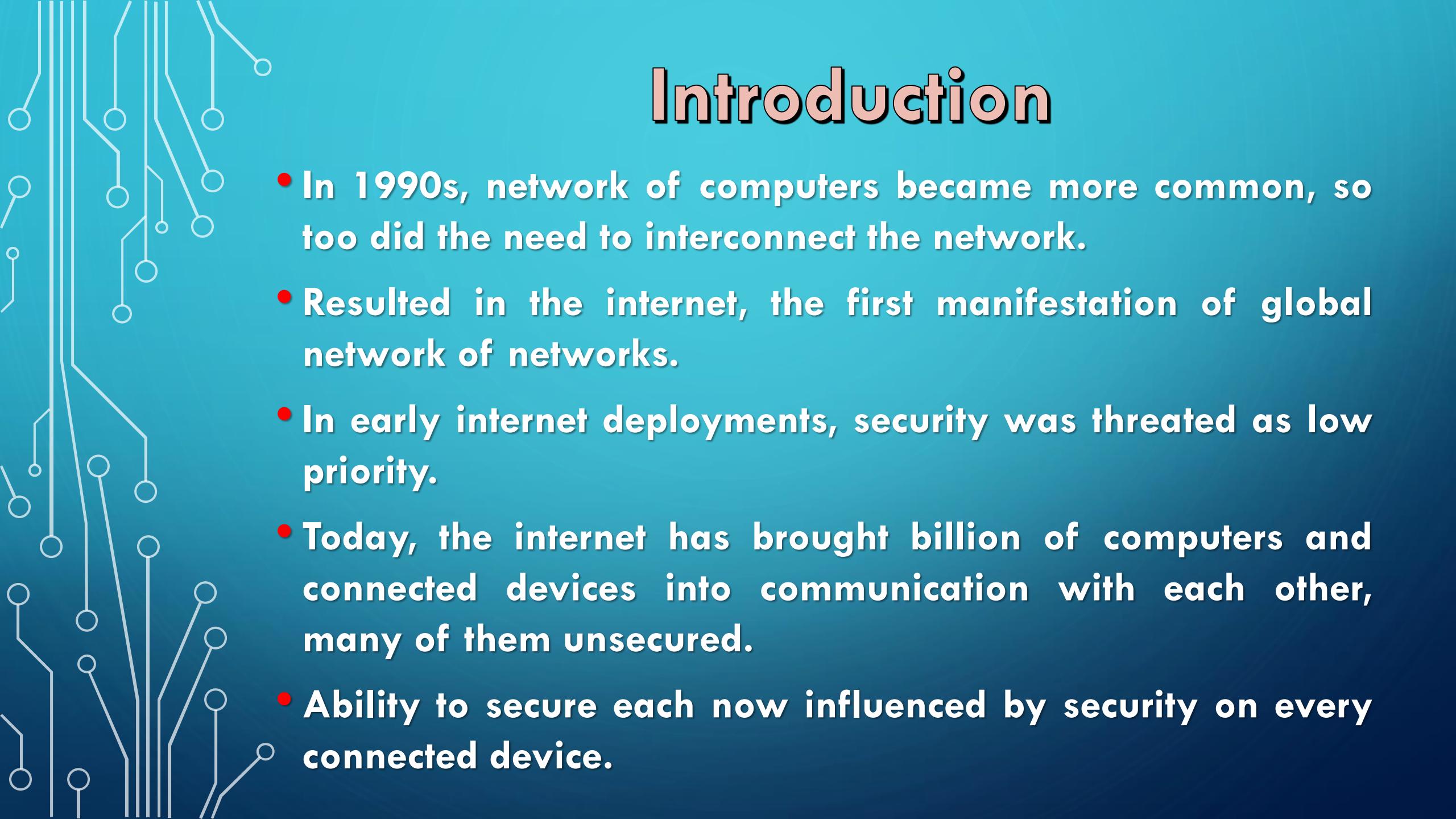
The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.



Introduction

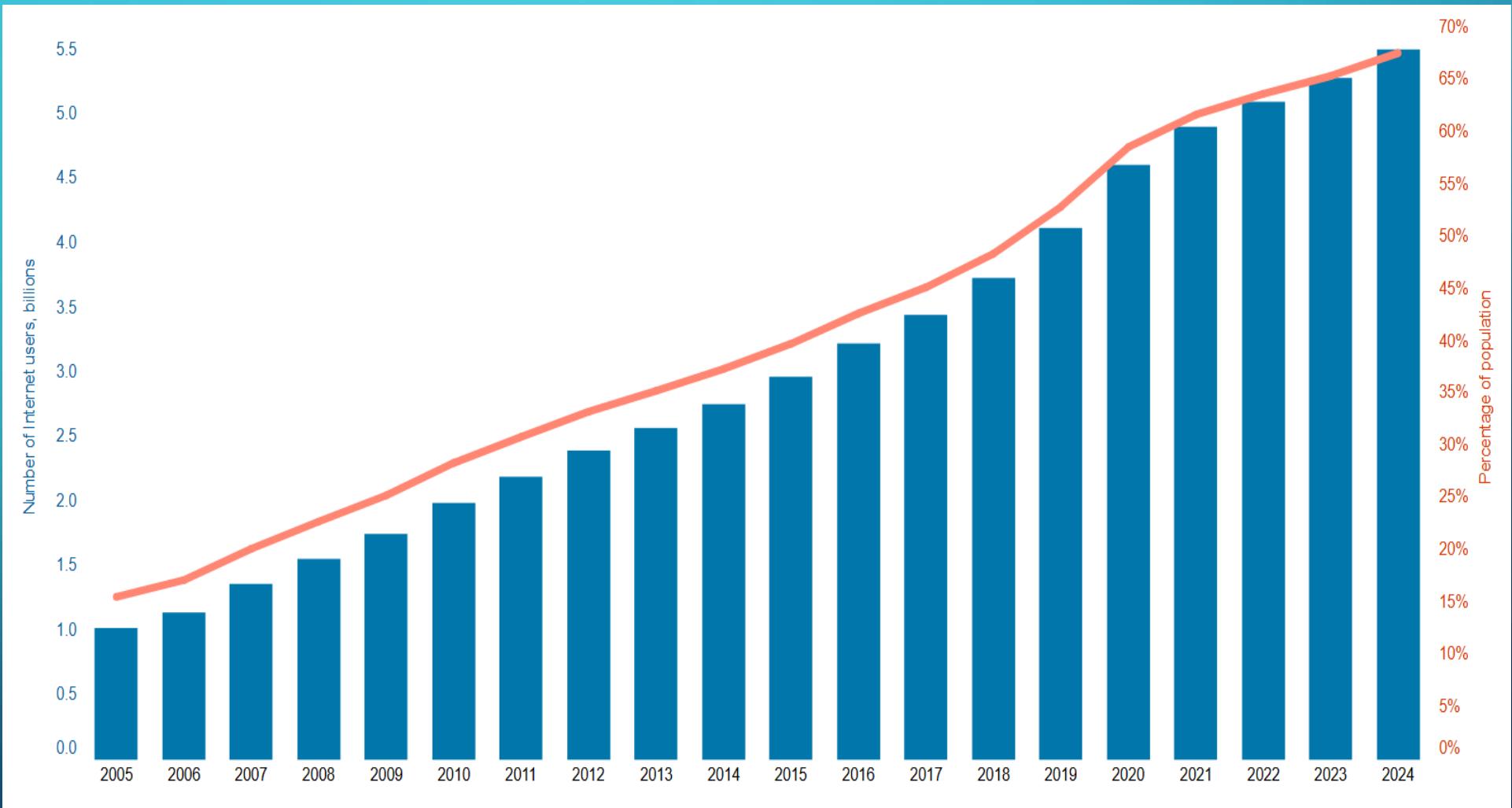
- ARPANET grew in popularity as did its potential for misuse.
- Fundamental problems with ARPANET security were identified:
 - No safety procedures for dial-up connections to the ARPANET.
 - User identification and authorization to the system were non-existent.
- In the late 1970s the microprocessor expanded computing capabilities and security threats.



Introduction

- In 1990s, network of computers became more common, so too did the need to interconnect the network.
- Resulted in the internet, the first manifestation of global network of networks.
- In early internet deployments, security was treated as low priority.
- Today, the internet has brought billion of computers and connected devices into communication with each other, many of them unsecured.
- Ability to secure each now influenced by security on every connected device.

Introduction



ITU estimates that approximately 5.5 billion people are using the Internet in 2024

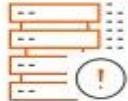
Introduction

2021 SONICWALL CYBERATTACK TRENDS

January 2021 - September 2021



3.9 Billion
MALWARE ATTACKS



3.9 Trillion
INTRUSION ATTEMPTS



70 Million
CRYPTOJACKING ATTACKS



42.9 Million
IoT MALWARE



6 Million
ENCRYPTED THREATS



495.1 Million
RANSOMWARE ATTACKS

-9%

+11%

+21%

+33%

+87%

+148%

sonicwall.com

SONICWALL*

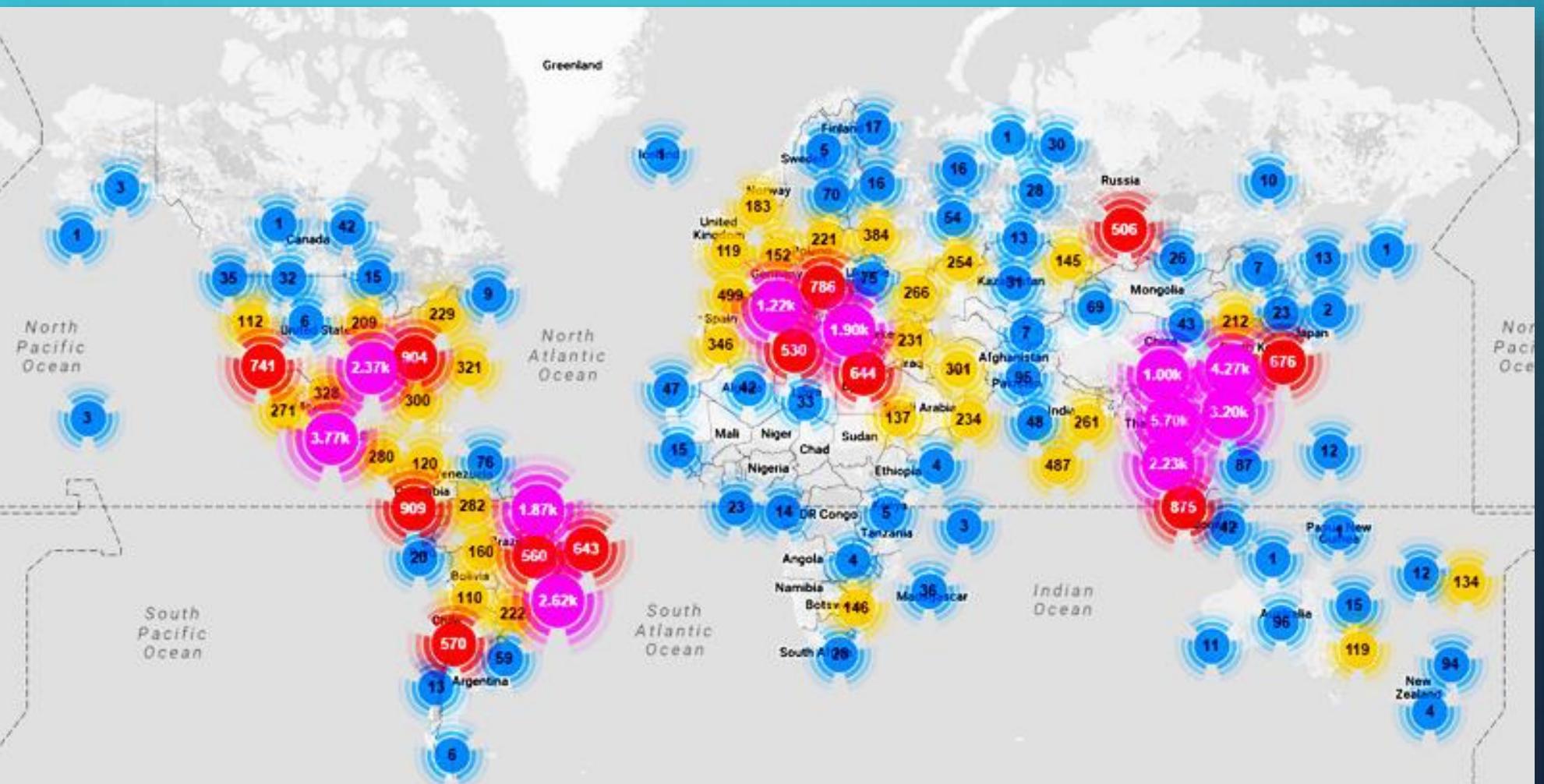
SONICWALL cyberattack trends and types in 2021

Computer security threats

- In 2016, the largest **DDoS attack** ever was launched on service provider **Dyn** using an **IoT botnet “Mirai”** led to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN.
- Once infected with **Mirai**, computers continually search the internet for vulnerable IoT devices and then use known default **usernames** and **passwords** to log in, **infecting them with malware**.



Computer security threats



Spread of the “Mirai” Botnet attack around the world

Computer security threats

- In 2017, An **electrical power station** in **Ukraine's** Ivano-Frankivsk city was targeted for a cyberattack which affected a colossal impact on **1.4 million people** putting them in the dark.
- The attack was done using the **spear-phishing email** and "**Black Energy**" malware based on "**Mirai**" causing **deleting the data, destroying hard drives**, and taking **control of infected computers**.



Computer security threats

- Another incident was the **Amazon Ring camera breach**. In 2019, multiple families' security systems were compromised.
- Hackers used the hacked **cameras** to **invade** people's **privacy** and even **demand ransoms**.

abcNEWS VIDEO LIVE SHOWS CORONAVIRUS ☰ ⌂

Amazon, Ring face \$5 million proposed class action lawsuit that alleges camera 'vulnerable' to cyber-attacks

Several Ring customers have reported their camera systems were hacked.

By Christina Carrega
28 December 2019, 05:06 • 5 min read



Computer security threats

- In **2020**, researchers **discovered** a new **IoT virus**, named "**Katana**," that has been infecting **thousands** of **IoT devices daily**.
- According to **Avira Protection Lab**, this advanced virus, containing still **unknown "malware binaries"** has the **ability** to make your **device** inoperable or **deny** you **access** to your **own data** by **encrypting** it.

The screenshot shows a blog post from Avira's website. The header features the Avira logo and navigation links for 'For Home', 'For Business', and 'Support'. Below the header, a breadcrumb trail indicates the post is under 'Technology Insights' with the specific title 'Katana: a new variant of the Mirai botnet'. The main content area contains a large image of a computer circuit board with green glowing lines, overlaid with a semi-transparent hexagonal box containing the text 'Katana, a new Mirai variant under development'. At the bottom of the image is the Avira OEM logo. To the right of the image, there is a sidebar with a button labeled 'ALL ARTICLES' and the title 'Katana: a new variant of the Mirai botnet' followed by the date '20 October 2020 by Avira Protection Labs'. At the very bottom right, there is a timestamp '7 months ago' and a duration indicator '4 minutes'.

Computer security threats

- In 2021, A **cyberattack** attempted to **poison** the **water supply** in **Florida** and managed by increasing the amount of **sodium hydroxide** to a potentially dangerous level.
- The cyber criminal was able to **breach** **Oldsmar's computer system** and briefly **increased** the amount of sodium hydroxide from 100 parts per million to 11,100 parts per million.

 Marco Rubio  @marcorubio · 8h
I will be asking the @FBI to provide all assistance necessary in investigating an attempt to poison the water supply of a #Florida city.
This should be treated as a matter of national security.
vice.com/en/article/88a... via @vice



Hacker Tried to Poison Florida City's Water Supply, Police Say
The hacker tried to drastically increase sodium hydroxide levels in the water, Pinellas County, Florida, officials said on Monday.
vice.com

255 245 630

Computer security threats

- In 2023, The U.S. Cybersecurity and Infrastructure Security Agency (**CISA**) added a recently patched critical security flaw in **Zyxel gear** to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.
- The Shadow Server Foundation said the flaw is "being actively exploited to build a **Mirai-like botnet**" since May 26, 2023.
- Cybersecurity firm Rapid7 has also warned of "**widespread**" in-the-wild abuse of CVE-2023-28771.

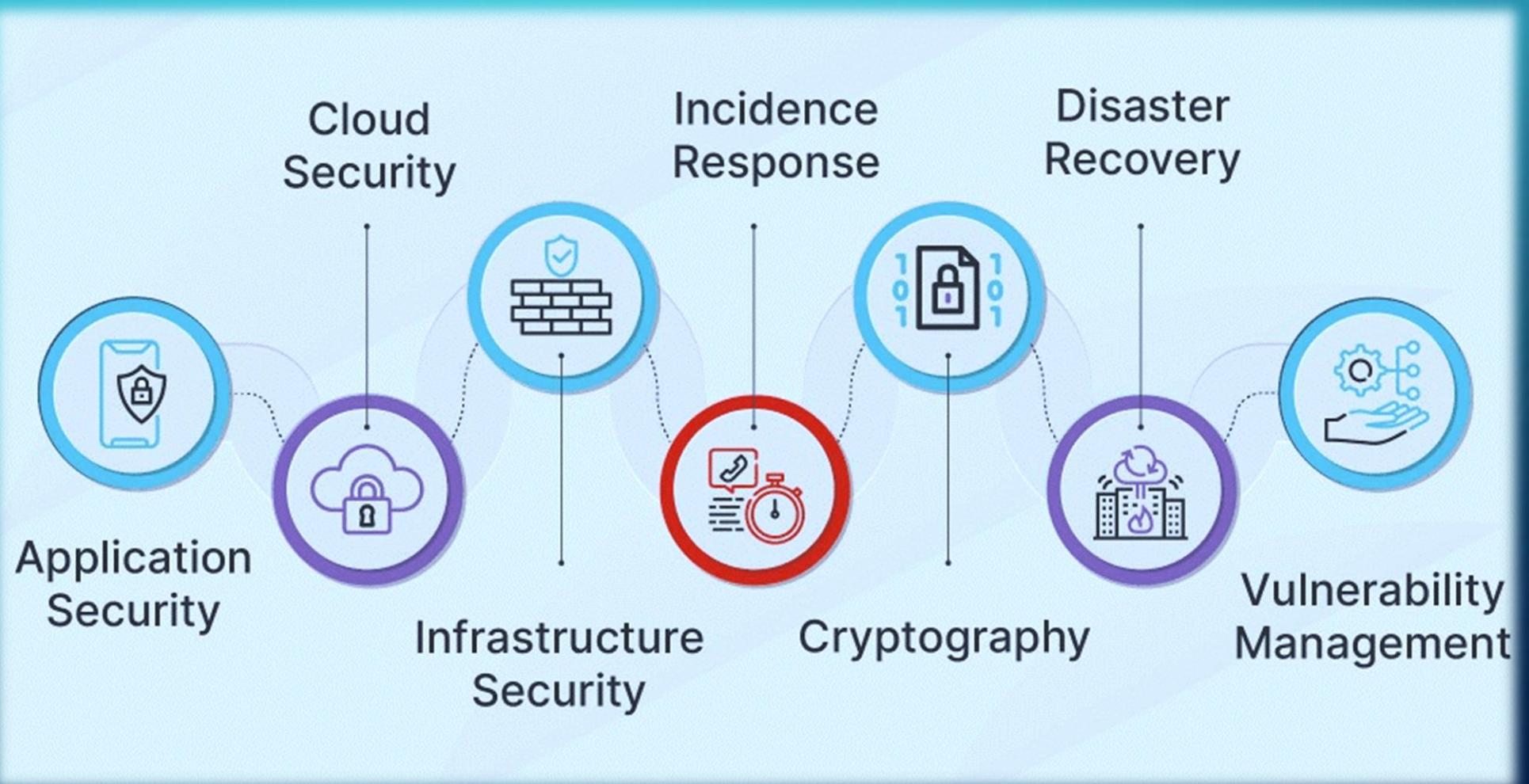




Information Security

- 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**).

Types of Information Security





Security Threats

- Security Threats, are any type of **malicious** activity or **attack** that could potentially cause **harm** or **damage** to an organization, its **data** or its **personnel**.
- Security threats may refer to **physical threats**, such as **theft** or **vandalism**, as well as **digital threats**, such as **malware** or **ransomware**.

Security Services

- The fundamental principles (**services**) of information security are **Confidentiality**, **Integrity**, and **Availability**.
- Every element of an information security program (and all three types of security controls put in place by an entity) should be designed to achieve one or more of these principles. Together, they are called the **CIA Triad**.



CIA Triad

Security Services

- **Confidentiality** measures are an essential component of data security, as they aim to safeguard sensitive information against any unauthorized access or disclosure.
- The primary goal of implementing confidentiality principles is to maintain the privacy and confidentiality of confidential information, ensuring that it remains accessible only to authorized individuals who require such information to carry out their job responsibilities.



CIA Triad

Security Services

- **Integrity** focuses on preventing any unauthorized modifications, deletions, or additions to the data.
- It is designed to ensure that data is accurate and trustworthy, and that it has not been tampered with or altered in any way without proper authorization.
- By upholding integrity principles, organizations can maintain the quality and reliability of their data, thereby enhancing their decision-making capabilities.



CIA Triad

Security Services

- **Availability** involves ensuring that data is accessible to its users at all times, whenever they require it.
- This principle is concerned with the functionality of support systems, including hardware, software, and network infrastructure, and ensuring that they remain operational and responsive to user needs.
- By maintaining availability principles, organizations can ensure that their users can access the data they need to make informed decisions, thereby enhancing their productivity and efficiency.



CIA Triad



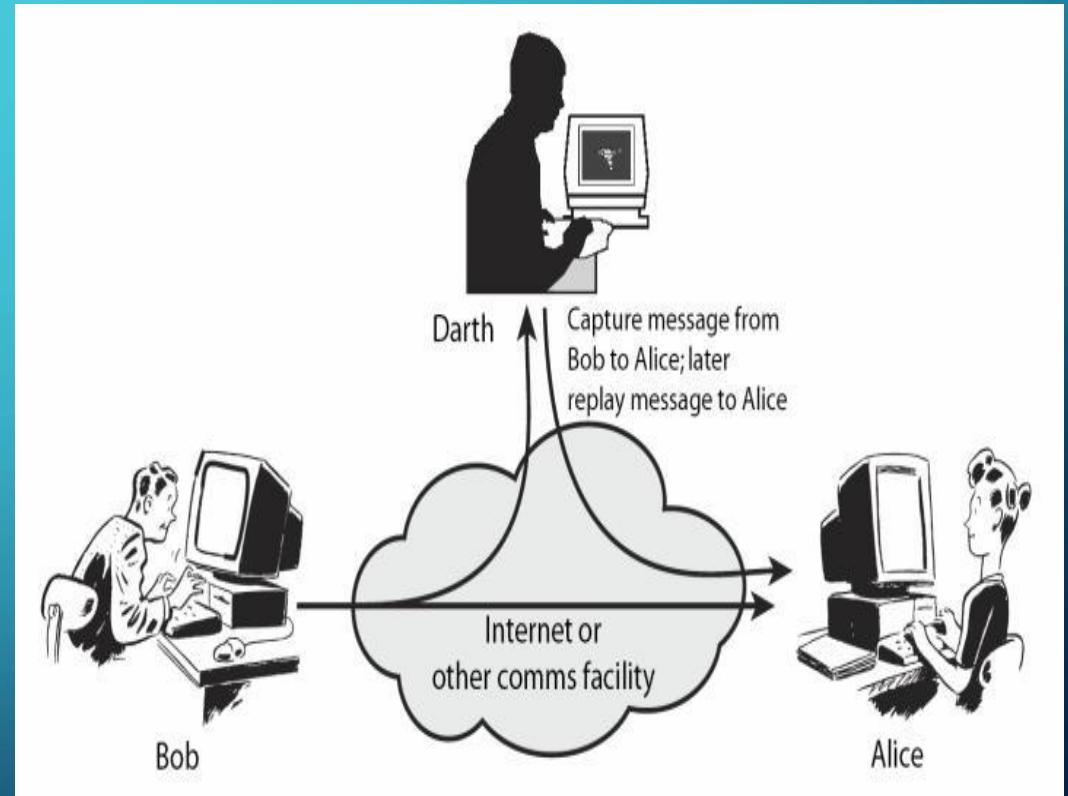
Security Attacks

- here are basically two forms of threats:
- active attacks.
- passive attacks.



Security Attacks

- An active attack is an attack in which attackers directly harm your computer systems.
- They can create several problems, such as:
 - Crashing files.
 - Encrypting data for ransom.
 - Stealing data, etc.



Security Attacks

- A **passive attack** refers to an attack in which the attackers quietly watch and collect the information without your knowledge.
- Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted.

