



SRI AKILANDESWARI WOMEN'S COLLEGE, WANDIWASH

IOT SECURITY CHALLENGES

Class: PG COMPUTER SCIENCE

Mrs. D. MALATHI

Assistant Professor

Department of Computer Science

SWAMY ABEDHANADHA EDUCATIONAL TRUST-WANDIWASH

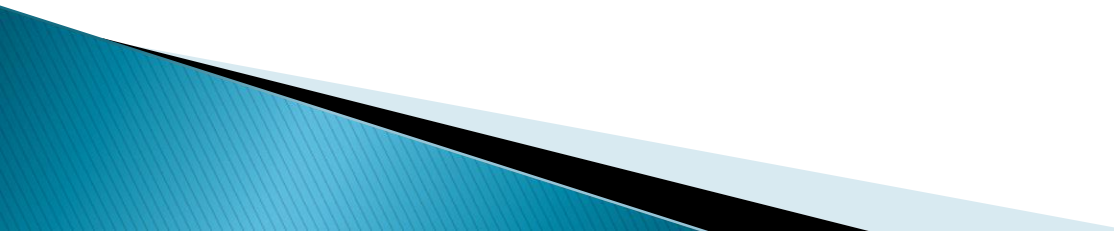
INTRODUCTION

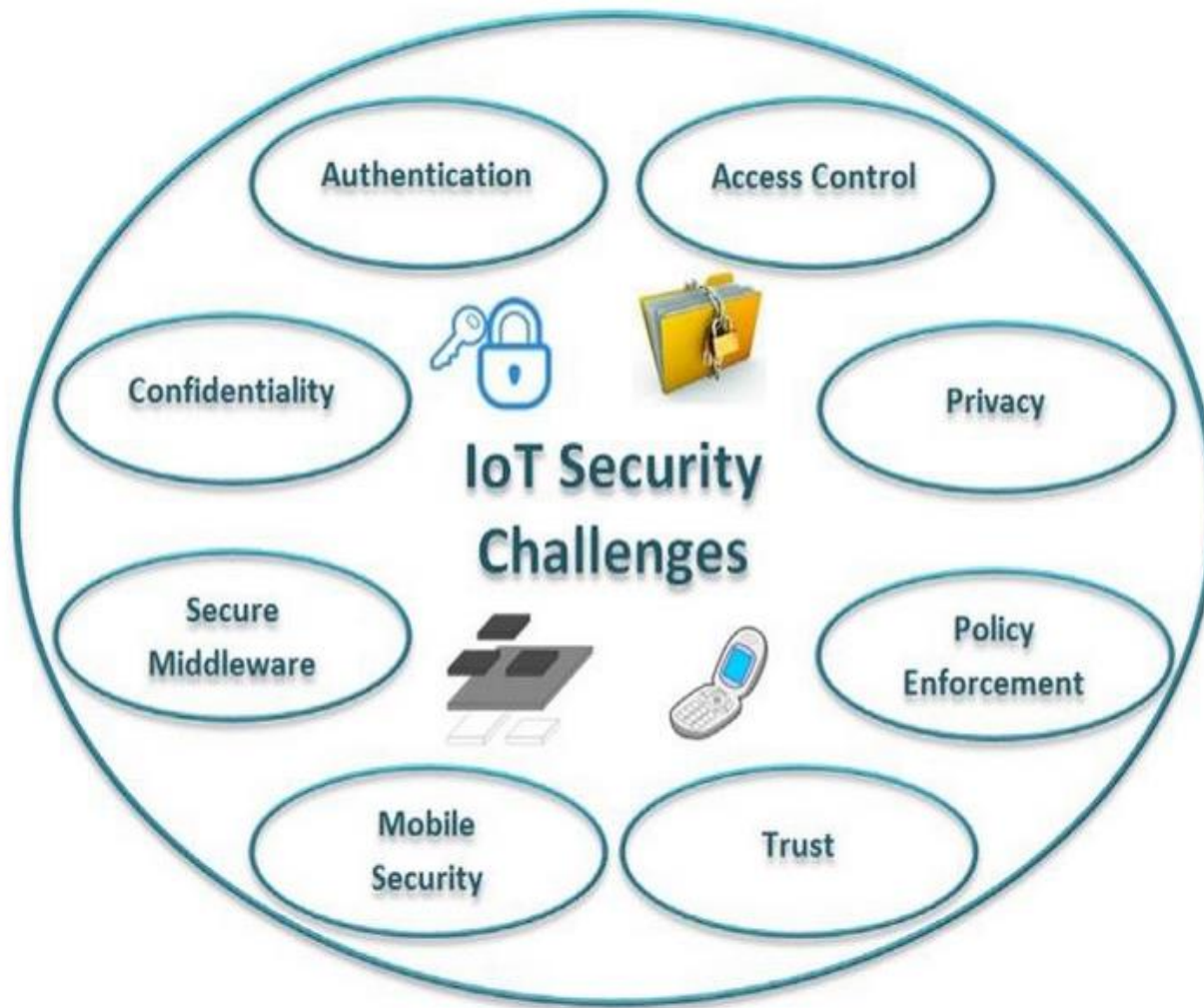
- ▶ Now, it is not only us with our computers, but there are also “things” that interact with the Internet without our intervention. These “things” are continually communicating with the Internet, a fridge sending an update of the food inside or our vehicle transmitting messages to the mechanic to inform its oil levels

Top IoT Security Risks

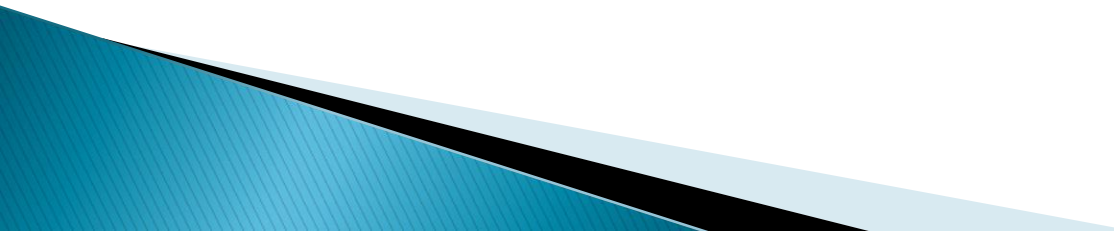
Returning to what happened in 2016, the lack of compliance on the part of IoT manufacturers led to weak and unprotected passwords in some IoT video cameras, which, in turn, led to one of the most damaging botnet attacks, the Mirai malware. There are many IoT security threats, but we will be highlighting the most important.

Top IoT Security Risks

- ▶ Returning to what happened in 2016, the lack of compliance on the part of IoT manufacturers led to weak and unprotected passwords in some IoT video cameras, which, in turn, led to one of the most damaging botnet attacks, the Mirai malware. There are many IoT security threats, but we will be highlighting the most important.
- 



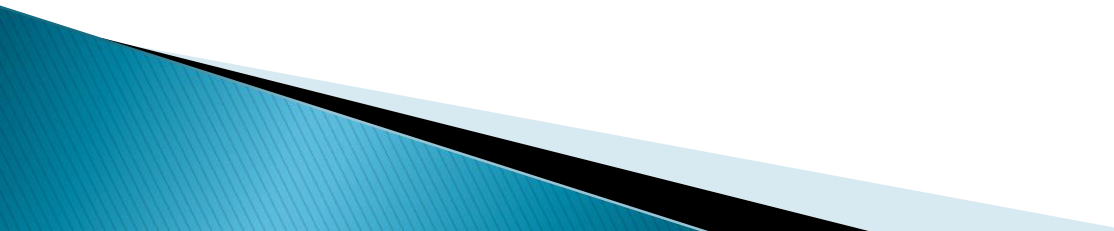
1) Lack of Compliance on the Part of IoT Manufacturers

- ▶ Hardware issues
 - ▶ Lack of a secure update mechanism
 - ▶ Old and unpatched embedded operating systems and software
 - ▶ Insecure data transfer and storage
 - ▶ Weak, guessable, or hard-coded passwords
- 

2) Lack of User Knowledge & Awareness

- ▶ Tricking a human is, most of the time, the easiest way to gain access to a network. A type of IoT security risk that is often overlooked is **social engineering attacks**. Instead of targeting devices, a hacker targets a human, using the IoT.

3) IoT Security Problems in Device Update Management

- ▶ Another risk is that during an update, a device will send its backup out to the cloud and will suffer a short downtime. If the connection is unencrypted and the update files are unprotected, a hacker could steal sensitive information.
- 

4) Lack of Physical Hardening

- ▶ Users are also responsible for keeping IoT devices physically secured. A smart motion sensor or a video camera that sits outside a house could be tampered with if not adequately protected.

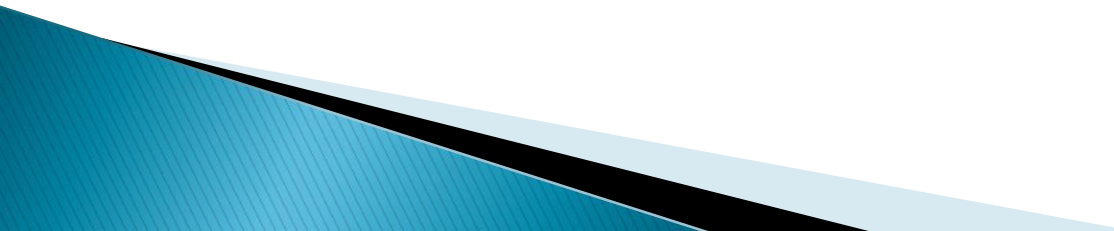
5) Botnet Attacks

- ▶ A single IoT device infected with malware does not pose any real threat; it is a collection of them that can bring down anything. To perform a botnet attack, a hacker creates an army of bots by infecting them with malware and directs them to send thousands of requests per second to bring down the target.

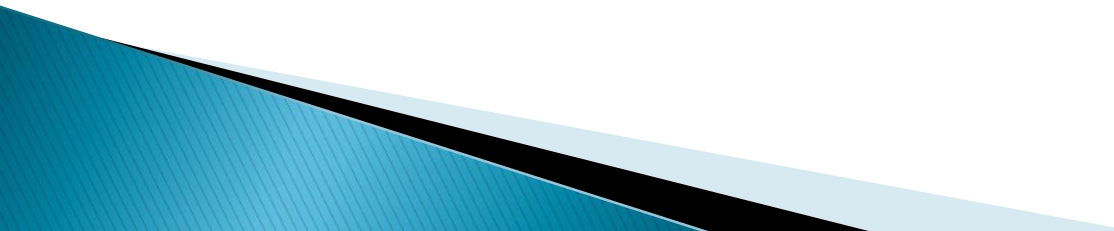
6) Industrial Espionage & Eavesdropping

- ▶ If hackers take over surveillance at a location by infecting IoT devices, spying might not be the only option. They can also perform such attacks to demand ransom money.

7) Hijacking Your IoT Devices

- ▶ Ransomware has been named as one of the nastiest malware types ever existed. Ransomware does not destroy your sensitive files — it blocks access to them by way of encryption. Then, the hacker who infected the device will demand a ransom fee for the decryption key unlocking the files.
- 

8) Data Integrity Risks of IoT Security in Healthcare

- ▶ As a result, a hacker can **gain access to a medical IoT device, gaining control over it and being able to alter the data it collects.** A controlled medical IoT device can be used to send false signals, which in turn can make health practitioners take actions that may damage the health of their patients
- 

9) Rogue IoT Devices

- ▶ **But rogue devices or counterfeit malicious IoT devices are beginning to be installed in secured networks without authorization.** A rogue device replaces an original one or integrates as a member of a group to collect or alter sensitive information. These devices break the network perimeter.

10) Cryptomining with IoT Bots

- ▶ Mining cryptocurrency demands colossal CPU and GPU resources, and another IoT security issue has emerged due to this precondition — crypto mining with IoT bots. This type of attack involves infected botnets aimed at IoT devices, with the **goal not to create damage, but mine cryptocurrency.**

Advantages of IoT

▶ **1. Enhanced Efficiency:**

- ✓ The integration of IoT enables automation and real-time monitoring, enhancing overall operational efficiency. IoT streamlines tasks from smart homes to industrial processes, reduces manual intervention, and optimizes resource utilization.

▶ **2. Data Collection and Analysis:**

- ✓ IoT devices generate large amounts of data, offering valuable insights into user behavior, preferences, and system performance. This data-driven approach facilitates informed decision-making, helping businesses and individuals adapt to changing conditions.

▶ .

Advantages of IoT

▶ **3. Improved Productivity:**

- ✓ In an industrial setting, IoT enhances productivity by providing real-time visibility into equipment status and production processes. This proactive monitoring minimizes downtime, streamlines workflows, and ensures optimal utilization of resources.

▶ **4. Cost Savings:**

- ✓ IoT applications contribute to cost savings through efficient resource management, predictive maintenance, and energy optimization. Smart energy grids, for instance, can automatically adjust power consumption based on demand, leading to reduced operational costs.

Advantages of IoT


▶ **5. Enhanced Connectivity:**

- ✓ IoT fosters seamless connectivity, allowing devices to communicate and collaborate.

▶ **6. Innovative Services:**

- ✓ IoT opens the door to innovative services and business models.

▶ **7. Environmental Impact:**

- ✓ IoT technologies contribute to environmental sustainability by enabling smart solutions for waste management, energy conservation, and pollution control.
- 

Disadvantages of IoT

- ▶ **1. Security Concerns:**
- ▶ The interconnected nature of IoT devices raises significant security challenges. Vulnerabilities in one device can compromise the entire network, leading to data breaches, privacy issues, and unauthorized access.
- ▶ **2. Privacy Issues:**
- ▶ The extensive data collection by IoT devices raises concerns about user privacy. Personal information, habits, and preferences are often transmitted and stored, raising ethical questions about how this data is used and protected.
- ▶ *Learn more with our latest blog on "[How to Control IoT Devices](#)"*

Disadvantages of IoT

- ▶ **3. Complexity in Implementation:**
- ▶ Implementing IoT solutions can be complex, requiring integration across diverse devices, platforms, and protocols. This complexity can lead to interoperability challenges, making it difficult for devices from different manufacturers to work seamlessly together.
- ▶ **4. High Initial Costs:**
- ▶ The deployment of IoT infrastructure often involves significant upfront costs. Businesses and individuals may face expenses related to device acquisition, installation, and system integration, which can be a challenge for widespread adoption, especially for smaller entities.

Thank you

