IOT SECURITY 101

WHO AM I?

- **LinkedIn** – @iamrakeshnaik
- **Career** – Senior Security Analyst at Alliant Cybersecurity
- Interested in Defensive side of security such as Cloud Security, Incident Response, Security Network Security.

TOPICS

- Introduction to IoT Security
- Common IoT Security Challenges
- Types of IoT Security Threats
- Mitigations/Best Practices for IoT Security
- Future of IoT Security
- Conclusion

INTRODUCTION TO IOT SECURITY

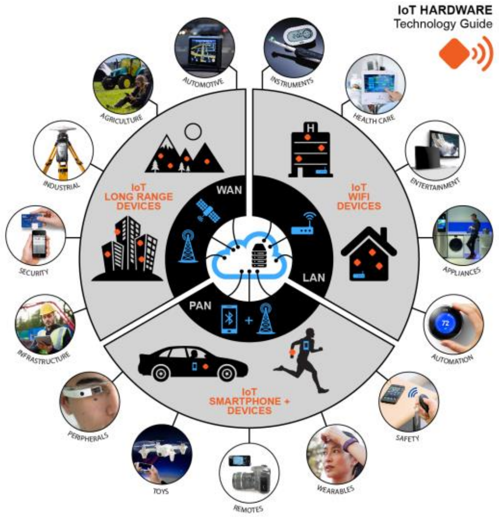
What is IoT

The Internet of Things (IoT) refers to the interconnected network devices that collect and exchange data.

Importance of IoT Security

- ❖ With the increasing number of connected devices, securing these devices is crucial to prevent unauthorized access and data breaches.

- ❖ Implementing robust IoT security measures is crucial to prevent data breaches, protect privacy, and ensure the safe operation of connected devices



COMMON IOT SECURITY CHALLENGES

- ❖ Weak authentication and authorization
- ❖ Lack of encryption
- ❖ Vulnerabilities in firmware and software
- ❖ Insecure communications
- ❖ Difficulty in patching and updating devices

TYPES OF IOT SECURITY THREATS

- **Denial of Service (DoS)**

  Overwhelming the IoT Devices with huge traffic than it can handle.

- **Botnet Attacks**

  Using the Compromised IoT Devices to join a Botnet and Launch DDos Attacks.

- **Supply Chain Attacks**

  This involves compromising the integrity of IoT devices through vulnerabilities in the supply chain, potentially embedding malware before the devices reach end-users

- **Firmware Hijacking**

  Attackers may exploit outdated firmware by injecting malicious code during updates, allowing them control over the device

- **Malware and ransomware attacks**

  IoT devices can be infected with malware, leading to data theft or device malfunction.

MITIGATIONS/BEST PRACTICES FOR IOT SECURITY

- **Implement Strong Authentication Mechanisms:**
  Use strong, unique passwords and multi-factor authentication
- **Use Encryption for Data Transmission:**
  Encrypt data both in transit and at rest
- **Regularly Update and Patch Devices:**
  Ensure devices are regularly updated with the latest security patches
- **Monitor Network Traffic for Unusual Activity:**
  Use network monitoring tools to detect and respond to suspicious activity
- **Segment IoT Devices on Separate Networks:**
  Isolate IoT devices from critical networks to limit the impact of a breach

FUTURE OF IOT SECURITY

❖ **Advanced Data Encryption:**

Data encryption will be critical in safeguarding sensitive information transmitted between IoT devices and backend systems. Protocols like TLS/SSL will be widely adopted to prevent eavesdropping and tampering, making it significantly harder for attackers to access data.

❖ **AI-Driven Security Solutions:**

Artificial Intelligence (AI) will play a pivotal role in enhancing IoT security. AI algorithms can analyze vast amounts of data generated by IoT devices, enabling automated threat detection and response, predictive maintenance, and real-time anomaly identification. This proactive approach will help organizations stay ahead of potential threats.

❖ **Enhanced Device Authentication:**

As IoT devices proliferate, robust authentication methods will become essential. Techniques such as cryptographic keys, biometric authentication, and secure digital certificates will ensure that only authorized devices can connect to networks, reducing the risk of unauthorized access

CONCLUSION

- Check for default/ weak credentials.
- Patch regularly.
- Enable encryption.
- Isolate the IoT devices in the Network.
- Monitor the traffic inbound and outbound from IoT devices.

RECENT EXAMPLE

- Hackers take control of robot vacuums in multiple cities, yell racial slurs

Presentation: Sucking dust and cutting grass: reversing robots and bypassing security - media.ccc.de

THANK YOU