IoT/Embedded Device Security: Small Devices with Big Threats.

POORNAMOL VETTIPARAMPIL DAMODARAN

About me

- **Name:** Poornamol Vettiparampil Damodaran (Poorna)
  Background:
- Master’s student in **Applied Cybersecurity**, TU Dublin
- **BTECH** in Information Technology
- Former **Security Analyst** at **Allianz Technology**
- **EJPT,ISO 27001 Lead Auditor** certified
- **Interests**: Pentesting /Network security

Key Discussion Points

- Introduction
- IoT Device Growth: 2015–2025
- Recent cyber attacks
- Common IoT Security Weaknesses
- Best Practices for Strengthening IoT Security
- Conclusion

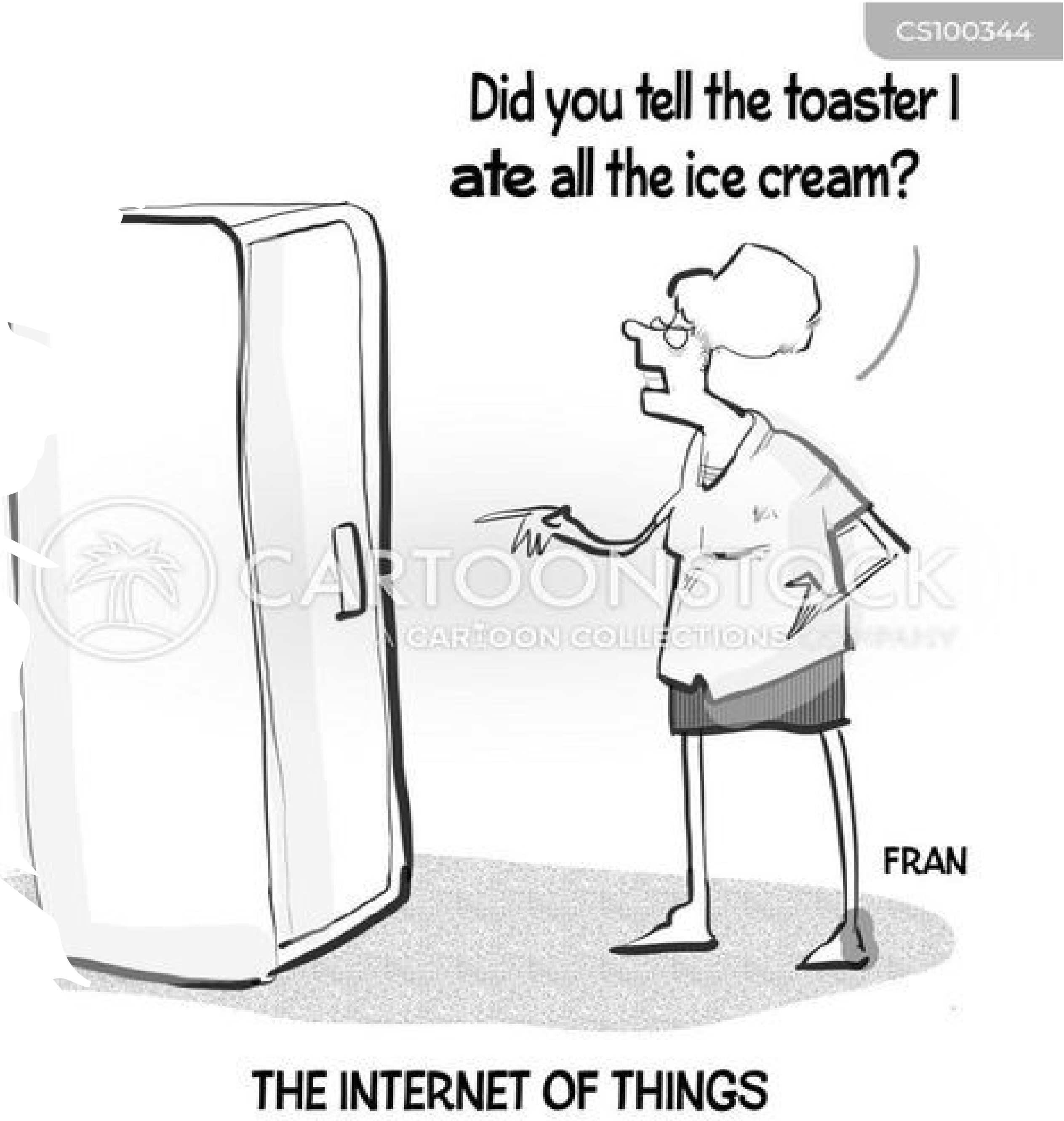
What is the Internet of Things?

- light bulbs
- thermostats
- doorbells
- locks
- plugs/outlets
- speakers (e.g., Amazon Echo, Google Nest)
- Refrigerators
- GPS systems
- Fitness trackers

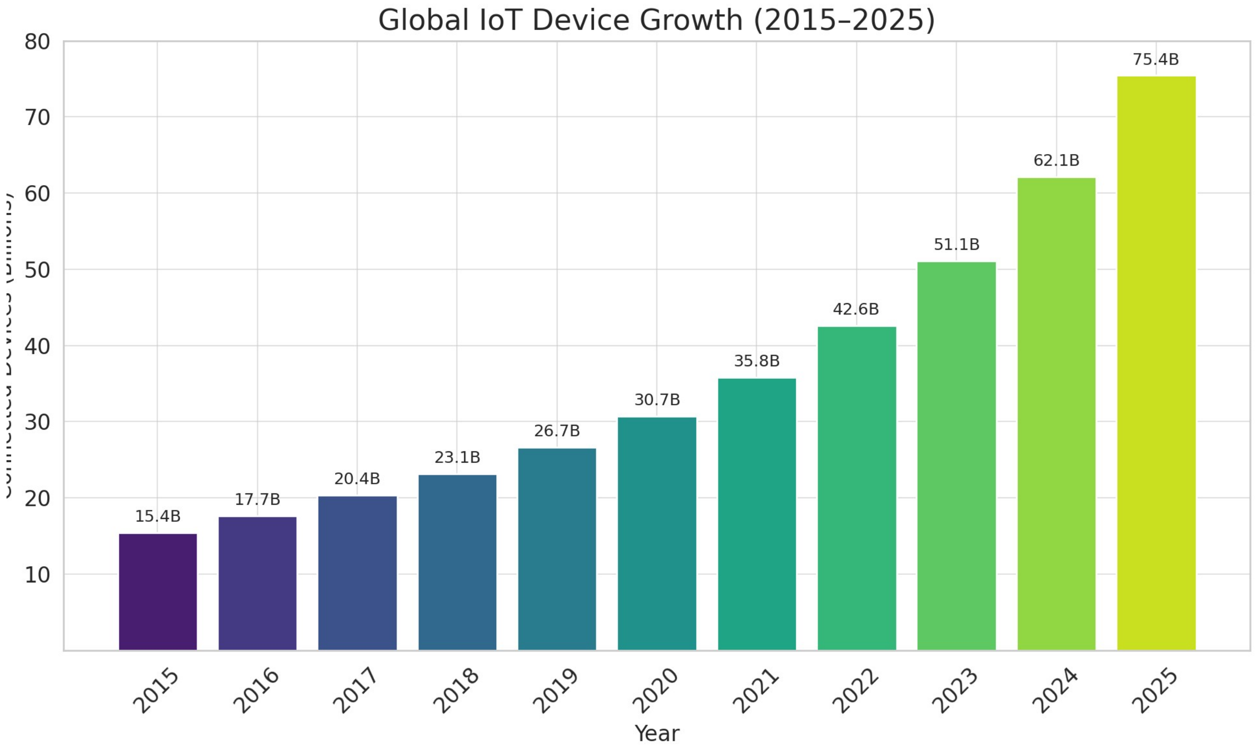
The Cool Stuff IoT Does

- Cost savings.
- Improved data collection.
- Increased automation.
- Efficiency.
- Safety.
- Convenient monitoring.
- Enhanced customer experiences.
- Accurate analysis.

But with great connectivity comes great vulnerability. Each device, no matter how small, can be a doorway for cyber threats!!!



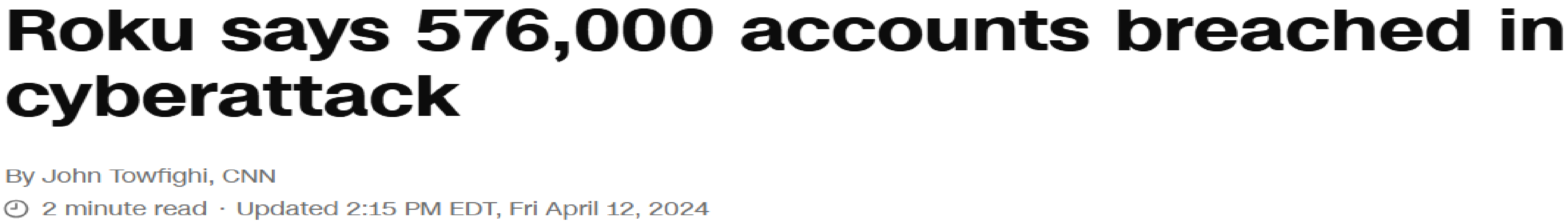
The Expanding Attack Surface



- The number of connected IoT devices has been growing exponentially over the past decade

- This rapid expansion underscores the increasing integration of IoT into various sectors, from consumer electronics to industrial applications.

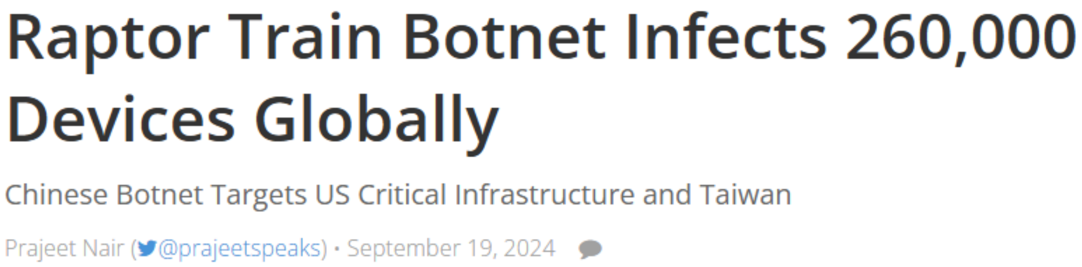
Recent cyber attacks



Roku says 576,000 accounts breached in cyberattack

By John Towfighi, CNN

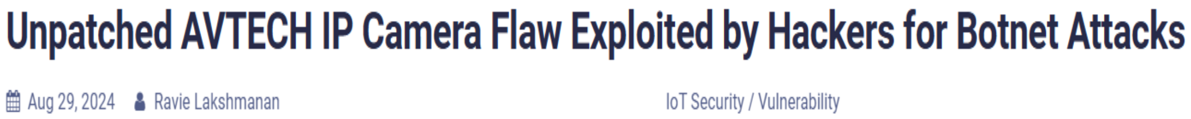
2 minute read · Updated 2:15 PM EDT, Fri April 12, 2024



Raptor Train Botnet Infects 260,000 Devices Globally

Chinese Botnet Targets US Critical Infrastructure and Taiwan

Prajeet Nair (@prajeetspeaks) • September 19, 2024



Unpatched AVTECH IP Camera Flaw Exploited by Hackers for Botnet Attacks

Aug 29, 2024 Ravie Lakshmanan IoT Security / Vulnerability

AVTECH IP Camera Exploitation

- **AVTECH IP Camera Exploitation**
- **Date**: August 2024
- **Scope**: Widespread across critical infrastructure sectors
- **Details**: An unpatched vulnerability in AVTECH IP cameras, known since 2019 but only assigned a CVE in 2024, was exploited to spread Mirai malware. These cameras are commonly used in sectors like finance, healthcare, and transportation, highlighting the risks of outdated security measures in critical infrastructure.

Raptor Train Botnet (Flax Typhoon)

- **Date**: September 2024
- **Scope**: Over 200,000 compromised IoT devices, including routers, IP cameras, and NAS systems
- **Details**: A Chinese nation-state group known as Flax Typhoon operated a botnet using a custom Mirai variant called "Nosedive." The malware exploited both known and zero-day vulnerabilities, primarily affecting small office/home office (SOHO) and IoT devices.

Healthcare IoT Ransomware Attack

- **Date**: February 2024
- **Scope**: Multiple U.S. hospitals
- **Details**: Hackers targeted IoT-connected medical devices, including patient monitors and infusion pumps, with ransomware. The attack forced hospitals to revert to manual procedures, exposing vulnerabilities due to outdated security patches and insufficient network segmentation

- **The truth is, the attacks are many more and never-ending!!!!**

How Hackers Hack Smart Devices

- ✓Default passwords like “admin/admin”
- ✓Unsecured ports
- ✓Outdated software with known vulnerabilities

Common IoT Security Weaknesses

Unencrypted Data in Storage & Transit
Sensitive information (e.g., PII, video/audio feeds) is sometimes stored or transmitted without encryption, exposing it to interception.

Lack of Centralized Management
Many IoT ecosystems lack tools for inventory, monitoring, and updates—resulting in poor visibility and high operational overhead.

Exposure to Lateral Network Attacks
IoT devices connected directly to the internet can serve as gateways for attackers to infiltrate internal systems.

Insecure Remote Access for Vendors
Third-party maintenance team

Common IoT Security Weaknesses

- **Default Passwords Left Unchanged**
  Many IoT devices come with factory-set credentials that are rarely updated, making them easy targets for attackers.
- **Unpatched Firmware Vulnerabilities**
  IoT firmware often contains zero-day flaws. Yet, organizations tend to prioritize CVEs for servers and PCs over those affecting IoT devices.
- **Easy Physical Reset Access**
  Devices can often be reset to factory defaults using a simple button press, allowing malicious insiders to bypass security settings.

How Do We Fix This?

The good news?

You don’t need a PhD in cybersecurity to protect your smart fridge

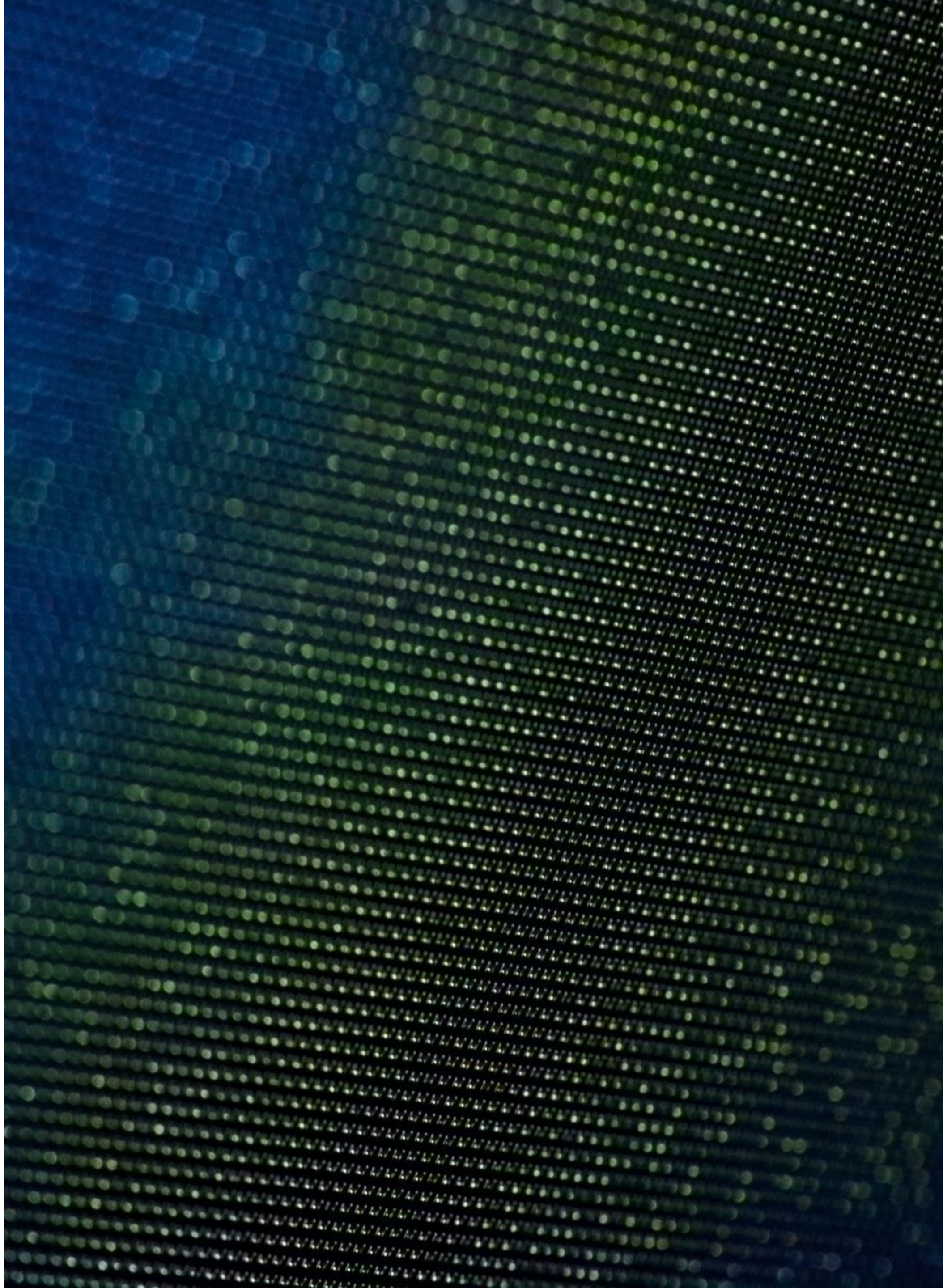
Change default passwords

Regularly update firmware

Use a guest network

Enable firewalls

Buy from reputable manufacturers

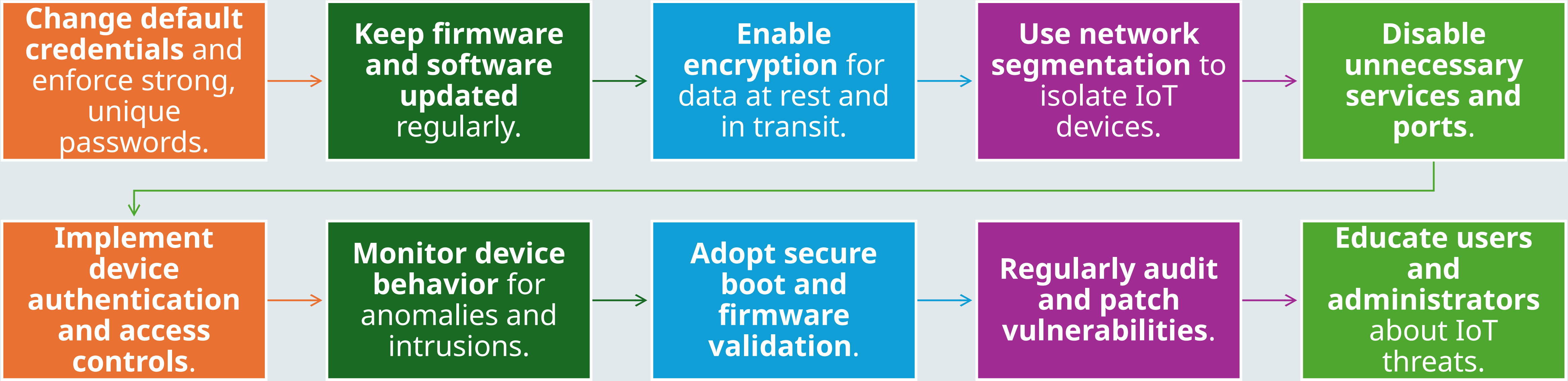


What Can Companies Do?

For developers/manufacturers:

- Build security into the design
- Ship with strong default settings
- Offer timely updates And don’t hardcode “123456” into the firmware

Best Practices for Strengthening IoT Security



Change default credentials and enforce strong, unique passwords.

Keep firmware and software updated regularly.

Enable encryption for data at rest and in transit.

Use network segmentation to isolate IoT devices.

Disable unnecessary services and ports.

Implement device authentication and access controls.

Monitor device behavior for anomalies and intrusions.

Adopt secure boot and firmware validation.

Regularly audit and patch vulnerabilities.

Educate users and administrators about IoT threats.

Conclusion

- IoT is transforming our world—but also expanding the attack surface.
- Many devices lack basic security features.
- Recent attacks show how vulnerable connected systems can be.
- “Security by design” is essential for future-proofing.
- Cybersecurity professionals must drive secure IoT adoption.

The more connected we become, the more protected we must be.

Thank you!!!

- *Email: poornamol@gmail.com*
- *Linkedin: https://www.linkedin.com/in/poornamol/*