

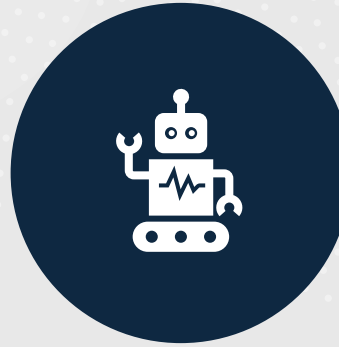


Introduction to IoT and Security Principles

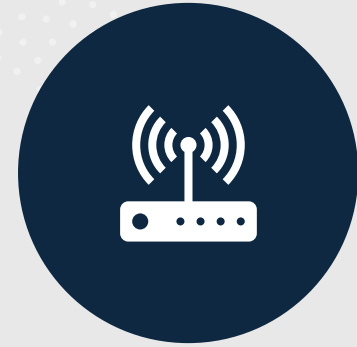
Marlon I. Tayag



Learning Objectives



UNDERSTAND THE
FUNDAMENTALS OF IOT.



RECOGNIZE KEY IOT
COMPONENTS AND THEIR
ROLES.



EXPLORE IOT-SPECIFIC
SECURITY RISKS AND
VULNERABILITIES.



CONDUCT A SIMPLE LAB
EXERCISE TO IDENTIFY
VULNERABILITIES.

What is IoT (Internet of Things)?

- The **Internet of Things (IoT)** refers to a network of interconnected devices and systems that communicate and exchange data with one another via the internet. These "things" can range from everyday objects, like home appliances, to sophisticated industrial equipment. The primary aim of IoT is to create a smart, interconnected world where devices work together seamlessly, making processes more efficient and lives more convenient.



Key Characteristics of IoT

1. Connectivity:

- Devices are connected to the internet or private networks to facilitate seamless data sharing and interaction.
- Connectivity standards include Wi-Fi, Bluetooth, Zigbee, and cellular networks (e.g., 4G, 5G).

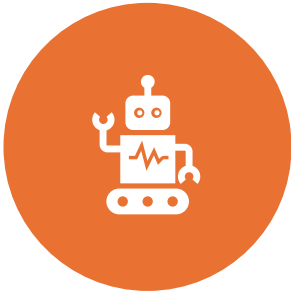
2. Embedded Systems:

- Devices are integrated with hardware (e.g., sensors, actuators) and software for specific functionalities.
- These systems are designed for low-power consumption and real-time data processing.

3. Real-Time Analytics:

- IoT devices collect and process data instantaneously, enabling real-time decision-making.
- For instance, smart cars use sensors and analytics to avoid collisions and optimize navigation.

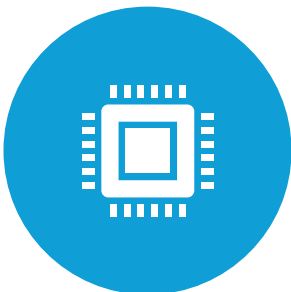
Advantages of IoT



Efficiency Improvement: Automation reduces human effort and increases operational efficiency.



Enhanced Decision-Making: Real-time data and analytics lead to informed decisions, especially in critical sectors like healthcare and industry.



Cost Reduction: Predictive maintenance and resource optimization save money in industrial and household settings.



Improved Quality of Life: IoT-enabled devices make everyday life more convenient and accessible.

Examples of IoT in Action

Smart Thermostats:

- Devices like Nest thermostats adjust the temperature in homes based on user preferences and real-time data, such as weather forecasts.
- They save energy by learning routines and operating efficiently.



Examples of IoT in Action

Wearable Devices:

- Fitness trackers (e.g., Fitbit, Apple Watch) monitor heart rate, sleep patterns, and physical activity.
- These devices connect to smartphones, offering users actionable health insights.



Examples of IoT in Action

- **Smart Home Appliances:**

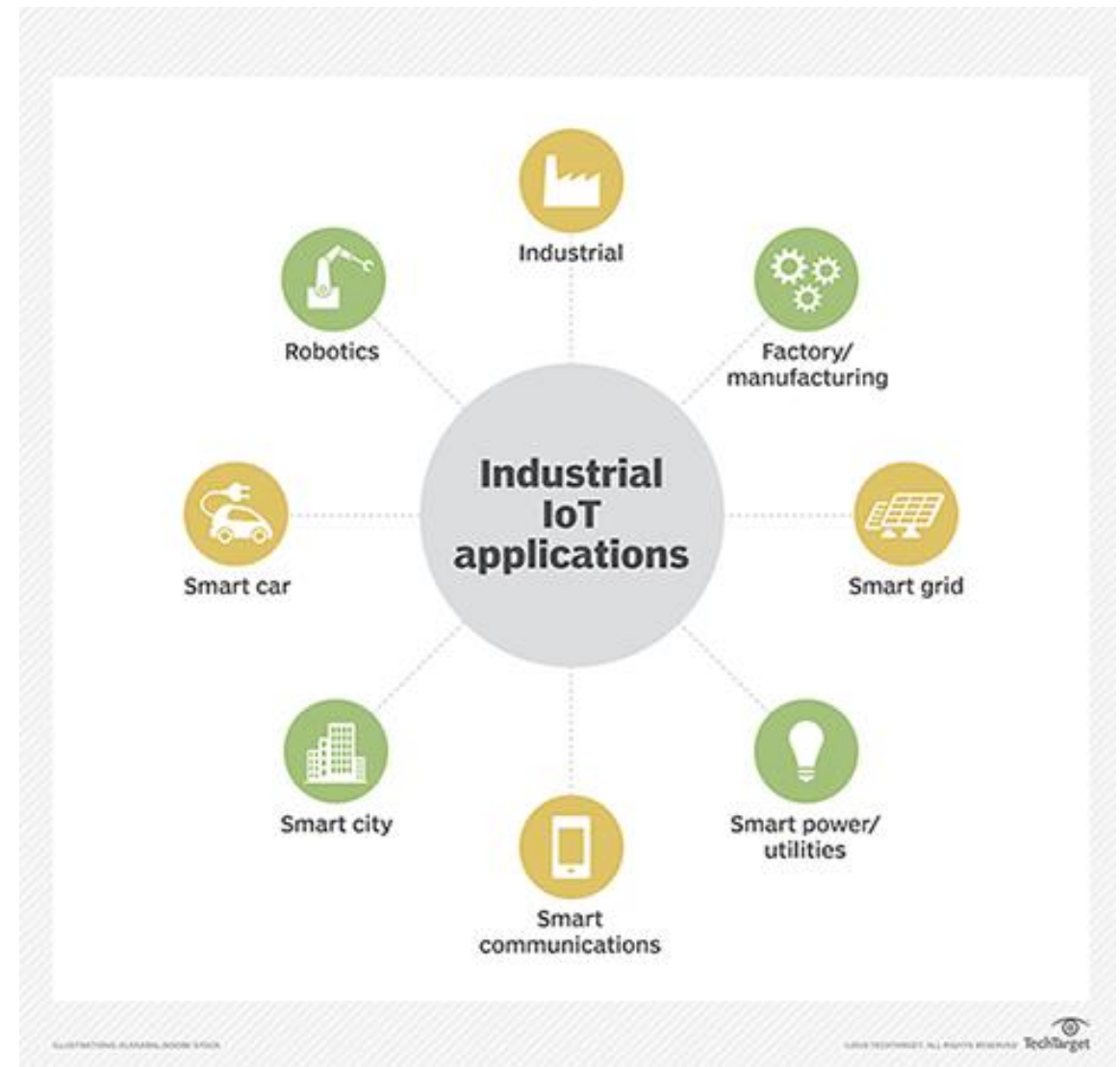
- Devices like Amazon Echo, Google Home, and smart refrigerators allow users to control lighting, order groceries, or play music using voice commands.
- Appliances can alert users when maintenance is needed or inventory is low.



Examples of IoT in Action

Industrial IoT (IIoT):

- Factories use IoT-enabled sensors to monitor equipment performance, predict failures, and optimize workflows.
- Examples include predictive maintenance in manufacturing and real-time tracking in supply chain management.



Importance of IoT Security

- As the **Internet of Things (IoT)** continues to expand, the need for robust security measures becomes increasingly critical. IoT devices are often entry points for cyberattacks due to their interconnected nature, which makes securing them a top priority for businesses, governments, and individuals.

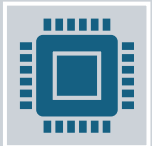
Growth of IoT Devices



The number of IoT devices globally is projected to reach 15 billion by 2023 and surpass 30 billion by 2030.



By 2024, IoT devices will generate over 79 zettabytes of data annually.



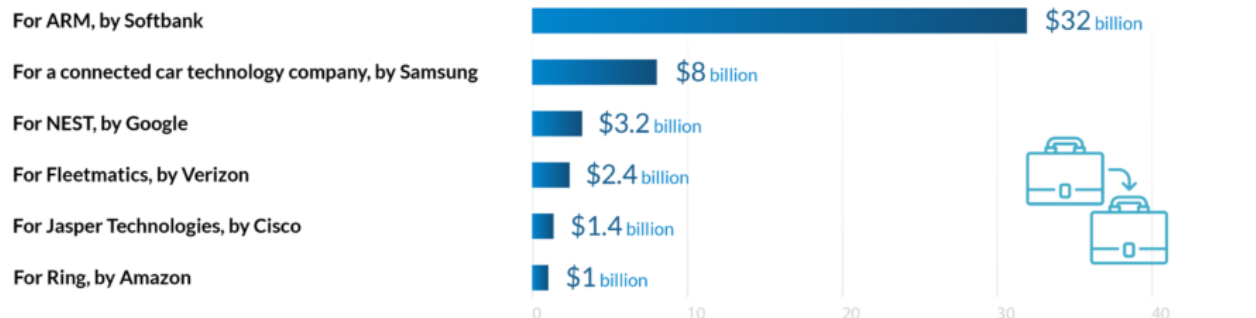
The surge in connected devices highlights the increasing attack surface for cybercriminals.

3 Key IoT Statistics You Should Know

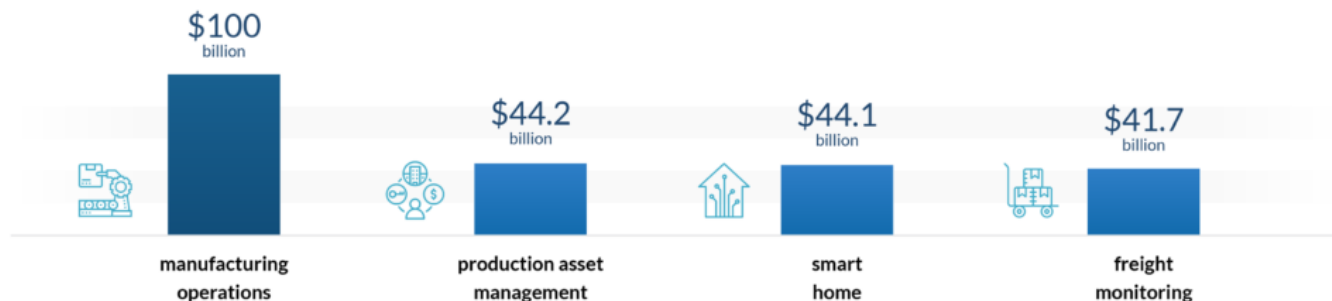
1 Number of installed IoT devices from 2015–2025



2 Biggest IoT acquisitions

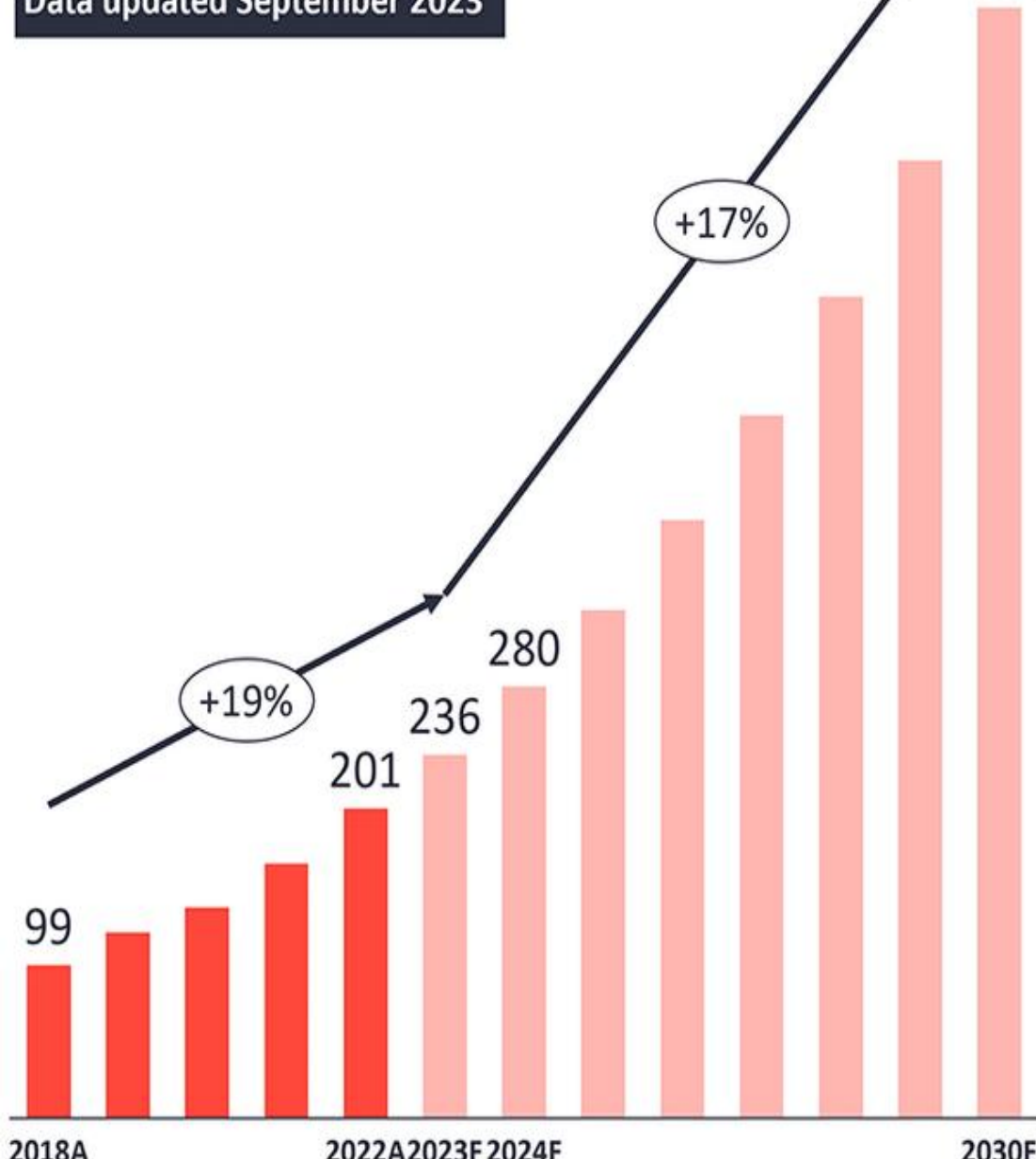


3 IoT use cases with the most investments



Global spending on enterprise IoT technologies in \$B

Data updated September 2023



Potential Risks in IoT Security

Data Breaches:

- IoT devices often collect sensitive personal or business data, making them prime targets for hackers.
- A compromised device can expose confidential information, leading to identity theft, corporate espionage, or financial losses.



Most Well-Known IoT Security Breaches



25 percent of the botnet consisted of non-computer gadgets, such as smart televisions, baby monitors, and domestic appliances.

2013 First Botnet

Mirai successfully attacked IoT devices such as routers, video cameras, and video recorders by trying to log in using a list of 61 commonly used hard-coded default usernames and passwords

2016 Mirai



Attacks mostly Linux-based devices. The botnet uses infected devices to scan and infect the network to other devices



2017 Reaper

Swiss hackers compromised 150,000 live camera feeds belonging to the security camera business Verkada



2021 Verkada

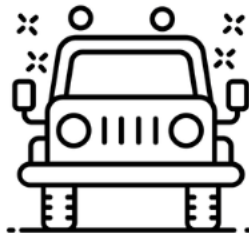
2010 Stuxnet

Stuxnet virus was used to physically harm Iranian centrifuges



2015 Jeep Grand Cherokee

Altering the radio station on the car's media center, activating the windshield wipers and air conditioner, and disabling the accelerator.



2017 St. Jude Medical

Embedded systems in radio frequency-enabled St. Jude Medical implanted cardiac devices, such as pacemakers, defibrillators, and resynchronization devices,



2020 Mirai

Transmit malicious payloads to unprotected Big-IP machines





Potential Risks in IoT Security

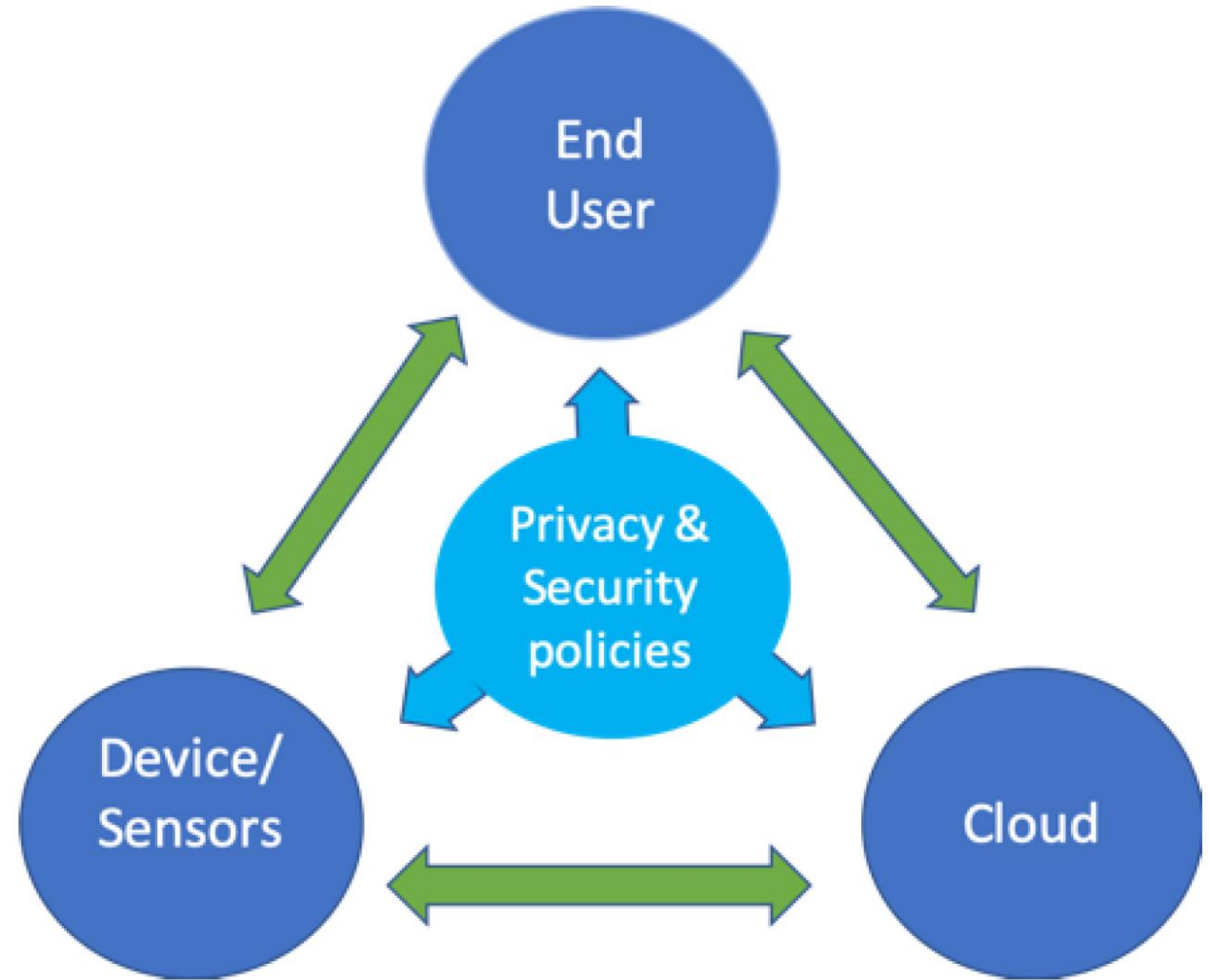
Device Manipulation:

- Cybercriminals can exploit vulnerabilities to take control of IoT devices.
- Examples include disabling smart security systems, hijacking connected vehicles, or tampering with medical devices like pacemakers.

Potential Risks in IoT Security

Privacy Violations:

- Many IoT devices collect user data (e.g., location, health metrics) without adequate encryption.
- This data can be intercepted or misused, violating user privacy and regulatory compliance (e.g., GDPR).



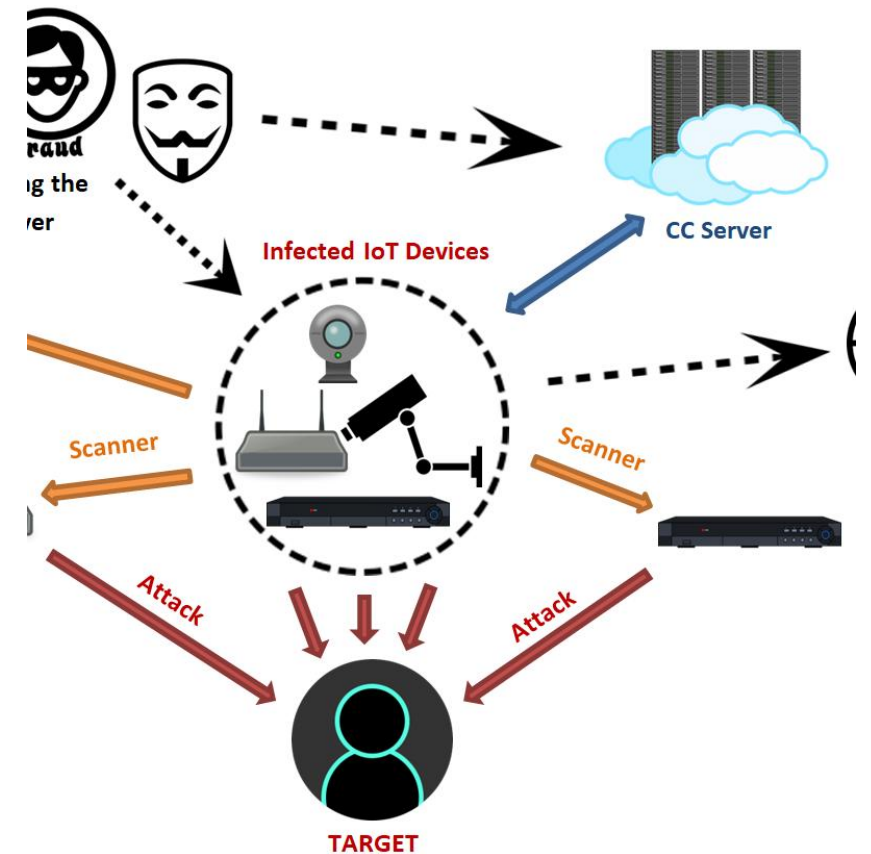
Case Study: Mirai Botnet Attack

Overview:

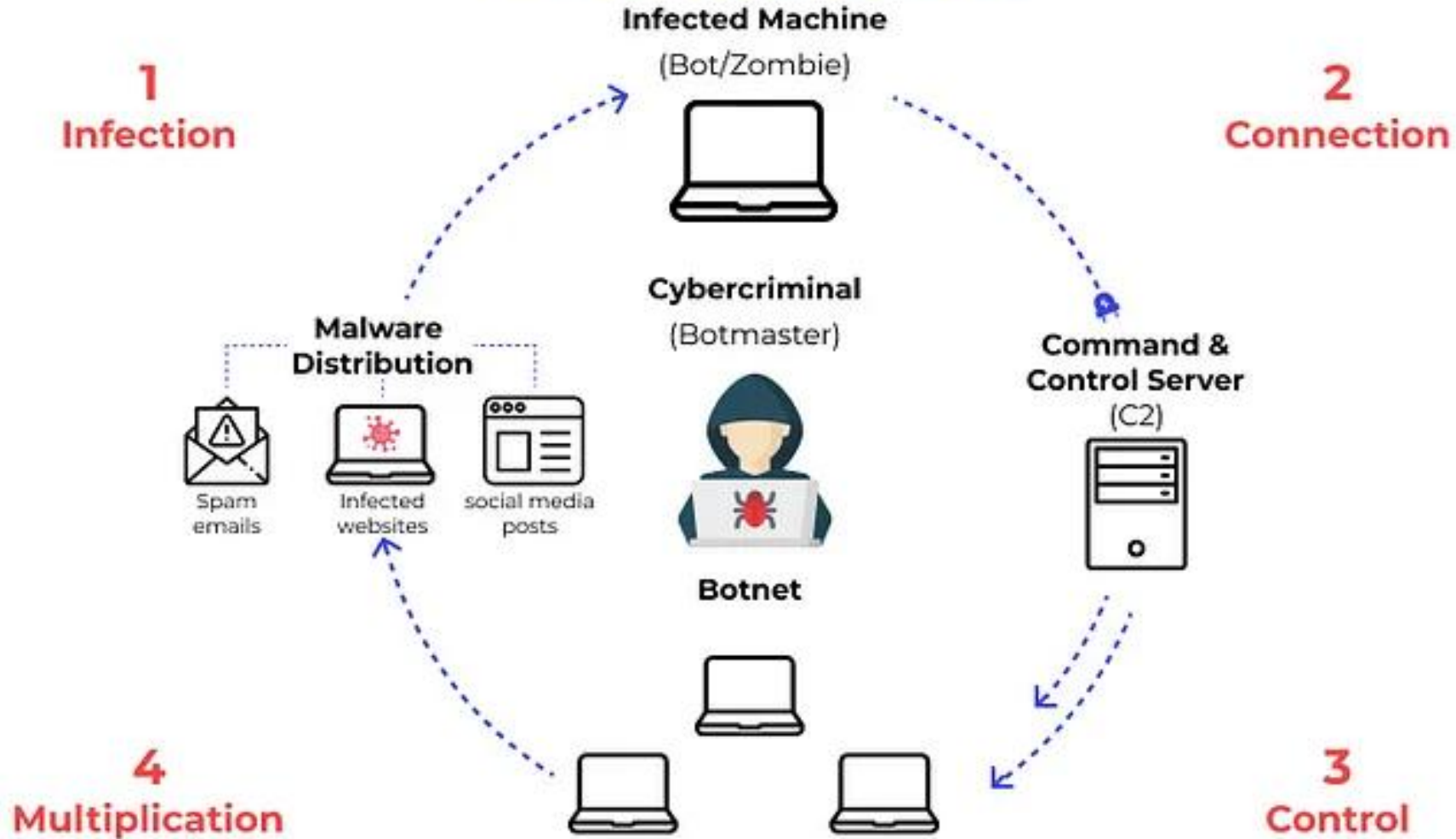
In 2016, the **Mirai Botnet** attack became one of the most significant IoT security breaches. The attack exploited IoT devices like DVRs, IP cameras, and routers, turning them into a network of bots to execute Distributed Denial of Service (DDoS) attacks.

Key Details:

- **Method of Attack:** The Mirai Botnet scanned the internet for IoT devices with default usernames and passwords, exploiting weak or nonexistent security protocols.
- **Impact:** It brought down major websites, including Twitter, Netflix, and Reddit, by targeting Dyn, a DNS service provider, with massive DDoS traffic.
- **Scale:** The attack generated traffic exceeding **1 Tbps**, making it one of the largest DDoS attacks in history.



How a Botnet works



Why IoT Security is Crucial

Protecting Critical Infrastructure:

- IoT is integral to smart cities, healthcare, and industrial operations. A security lapse can disrupt essential services.

Preserving Consumer Trust:

- Data breaches and device manipulation erode user confidence in IoT technologies.

Compliance and Legal Implications:

- Regulatory frameworks (e.g., GDPR, HIPAA) mandate stringent data protection standards for IoT devices.

Mitigating Financial Losses:

- Cyberattacks on IoT systems can lead to significant monetary damages due to downtime, lawsuits, and reputational harm.



How Is IoT Security Different than Traditional IT Security?

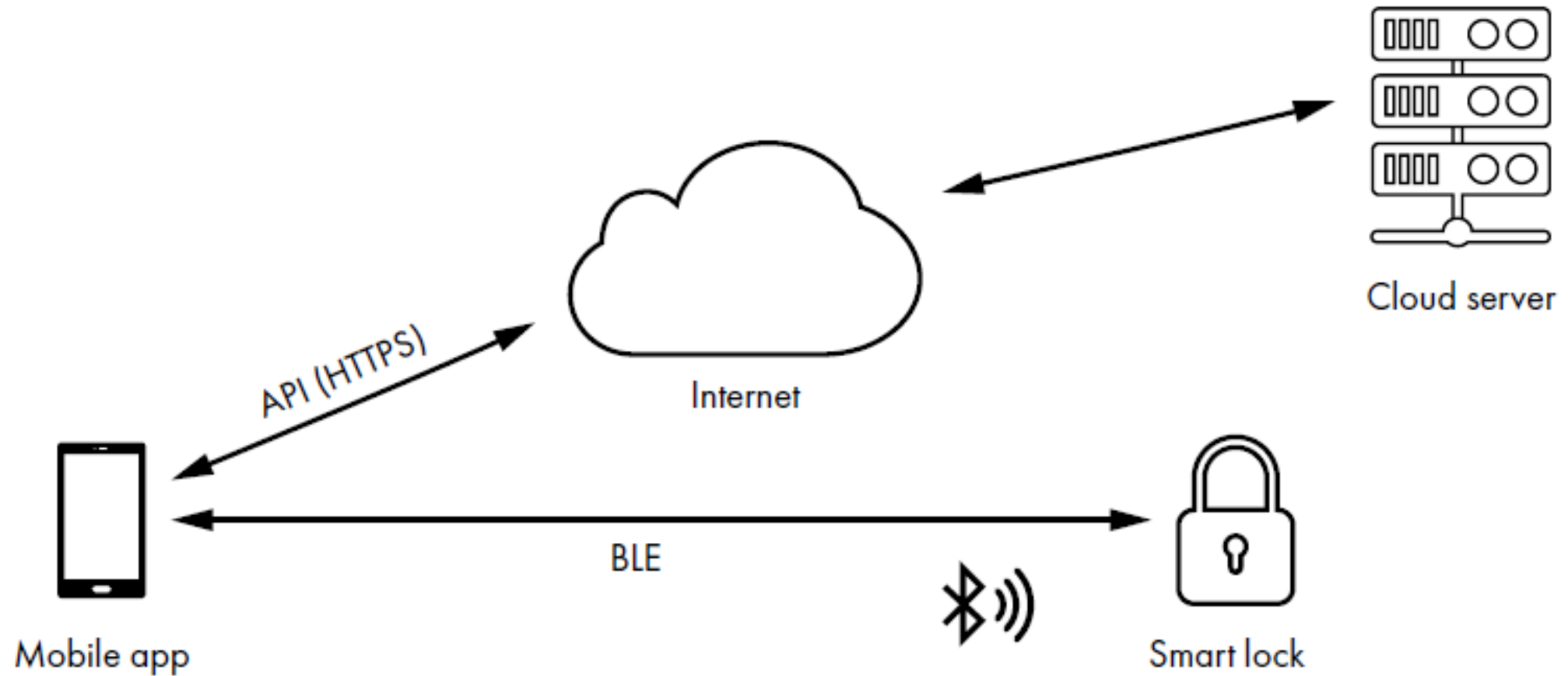


Aspect	IoT Security	Traditional IT Security
Consequences	<ul style="list-style-type: none">- Immediate impact on physical systems (e.g., critical healthcare devices, industrial control systems).- Potential for life-threatening scenarios (e.g., failure in medical devices or autonomous vehicles).- Data breaches leading to privacy violations (e.g., personal health data, smart home data).	<ul style="list-style-type: none">- Business and financial loss (e.g., data breaches, intellectual property theft).- Reputational damage to organizations.- Legal and compliance risks due to breaches of regulations (e.g., GDPR).
Adversaries	<ul style="list-style-type: none">- Hacktivists targeting smart cities or infrastructure.- Cybercriminals aiming to exploit device vulnerabilities for financial gain.- State-sponsored attackers targeting critical IoT infrastructure (e.g., healthcare, utilities).- Insiders with access to IoT devices and systems.	<ul style="list-style-type: none">- Cybercriminals seeking financial gain (e.g., ransomware, theft of data).- Hacktivists targeting organizations based on political, social, or ideological motivations.- Nation-state actors focusing on corporate espionage or infrastructure disruption.- Insiders with access to sensitive data or systems.

Aspect	IoT Security	Traditional IT Security
Economics	<ul style="list-style-type: none">- Cost constraints on many IoT devices prevent robust security features.- High volume of devices, leading to scalability issues in patch management and security updates.- Low-cost nature of many devices encourages the use of insecure or outdated hardware and software.	<ul style="list-style-type: none">- Higher budget allocations for security in traditional IT systems due to standardized, higher-cost hardware.- Investment in security infrastructure like firewalls, intrusion detection systems, and security operations centers.- More focus on proactive defense and security testing, with larger financial resources for cybersecurity.

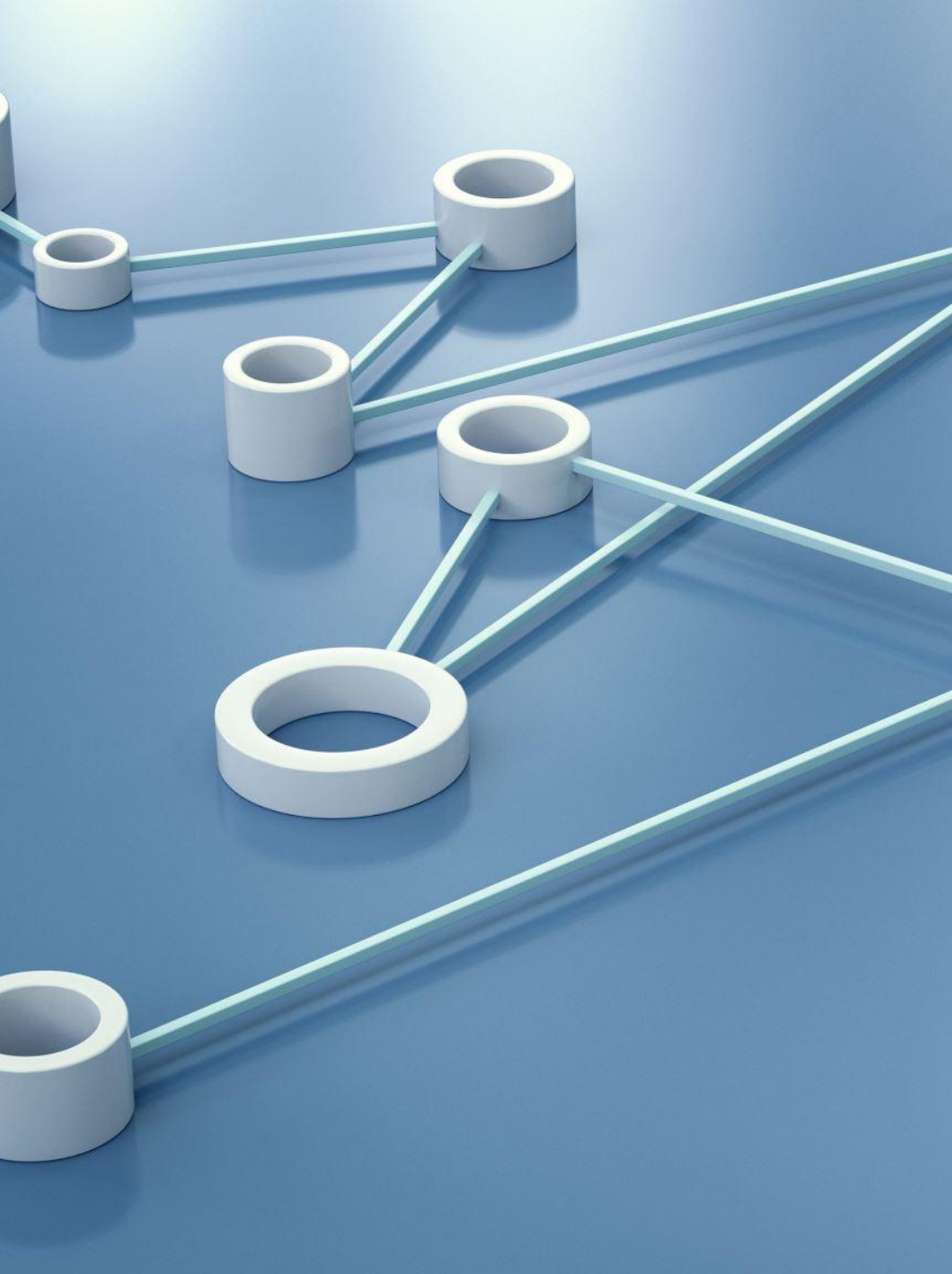
Aspect	IoT Security	Traditional IT Security
Timescales	<ul style="list-style-type: none"> - Shorter product lifecycle: IoT devices are often produced quickly, leading to inadequate security testing and patching. - Faster deployment of IoT devices, which can result in the integration of devices without adequate security measures. - Long-term exposure: Devices, once deployed, may stay in the field for years without updates, creating vulnerabilities. 	<ul style="list-style-type: none"> - Longer product lifecycle: IT systems are usually more stable, with longer periods between updates or replacements. - Ongoing security updates: Traditional IT systems often have regular security patching schedules, although challenges may arise in keeping systems up-to-date. - Continuous monitoring and response to new security threats, with proactive approaches to mitigate risks over time.

What's Special About IoT Hacking?





Frameworks, Standards, and Guides



Challenges in IoT Security Standardization

- **Fractured Landscape:** The plethora of standards and frameworks shows a lack of consensus on universally accepted practices. This fragmentation can create barriers to implementation and interoperability.
- **Rapid Evolution:** Standards often struggle to keep pace with emerging technologies, leaving gaps in security for new IoT applications.
- **Interoperability Issues:** While standards like IPv4 and Wi-Fi address interoperability effectively, security-specific standards often lack uniform adoption across industries.

Interrelation Between Design and Operation

The design phase dictates what security measures can be implemented during operation. This relationship underscores the importance of security by design, where:

Capabilities Introduced in Design: Secure updates, forensic evidence capture, and device segmentation are examples of design features that enhance operational security.

Operational Constraints: Without appropriate design considerations, operators face limitations in securing devices, which can lead to vulnerabilities.

A large orange circle is positioned on the left side of the slide, partially cut off by the edge.

Frameworks vs. Standards

Frameworks:

1. Provide high-level goals and are often "evergreen," meaning they remain relevant despite technological changes.

2. Encourage adaptability and application across diverse use cases, making them particularly valuable for long-term security strategies.

Examples: NIST Cybersecurity Framework, Cloud Security Alliance IoT Security Controls Framework.

Comparison with Standards

While frameworks provide the "what," standards define the "how." Standards are more detailed, use-case-specific, and often become outdated as technologies change. For example:

A **framework** might recommend "ensuring secure communications."

A **standard** would specify "using TLS 1.3 for encryption."



Examples of Frameworks

NIST Cybersecurity Framework (CSF):

- Developed by the National Institute of Standards and Technology (NIST), the CSF provides a comprehensive, flexible approach to cybersecurity.
- It is organized into five core functions: Identify, Protect, Detect, Respond, and Recover.
- While it does not mandate specific technologies, it helps organizations create a robust cybersecurity posture.

Why Frameworks Are Valuable?

Frameworks vs. Standards

Standards:

1. Offer detailed processes and technical specifications for achieving security goals.

2. Are more rigid and tailored to specific contexts, which can lead to rapid obsolescence as technologies evolve.


Examples: ETSI's Technical Specification for Cyber Security, NIST IoT Core Baseline.



Examples of Standards

ETSI's Technical Specification for Cyber Security for Consumer IoT:

- Created by the European Telecommunications Standards Institute (ETSI), this standard outlines specific provisions for building IoT devices securely.
- It includes requirements for encryption, secure software updates, and other security features tailored for consumer IoT.

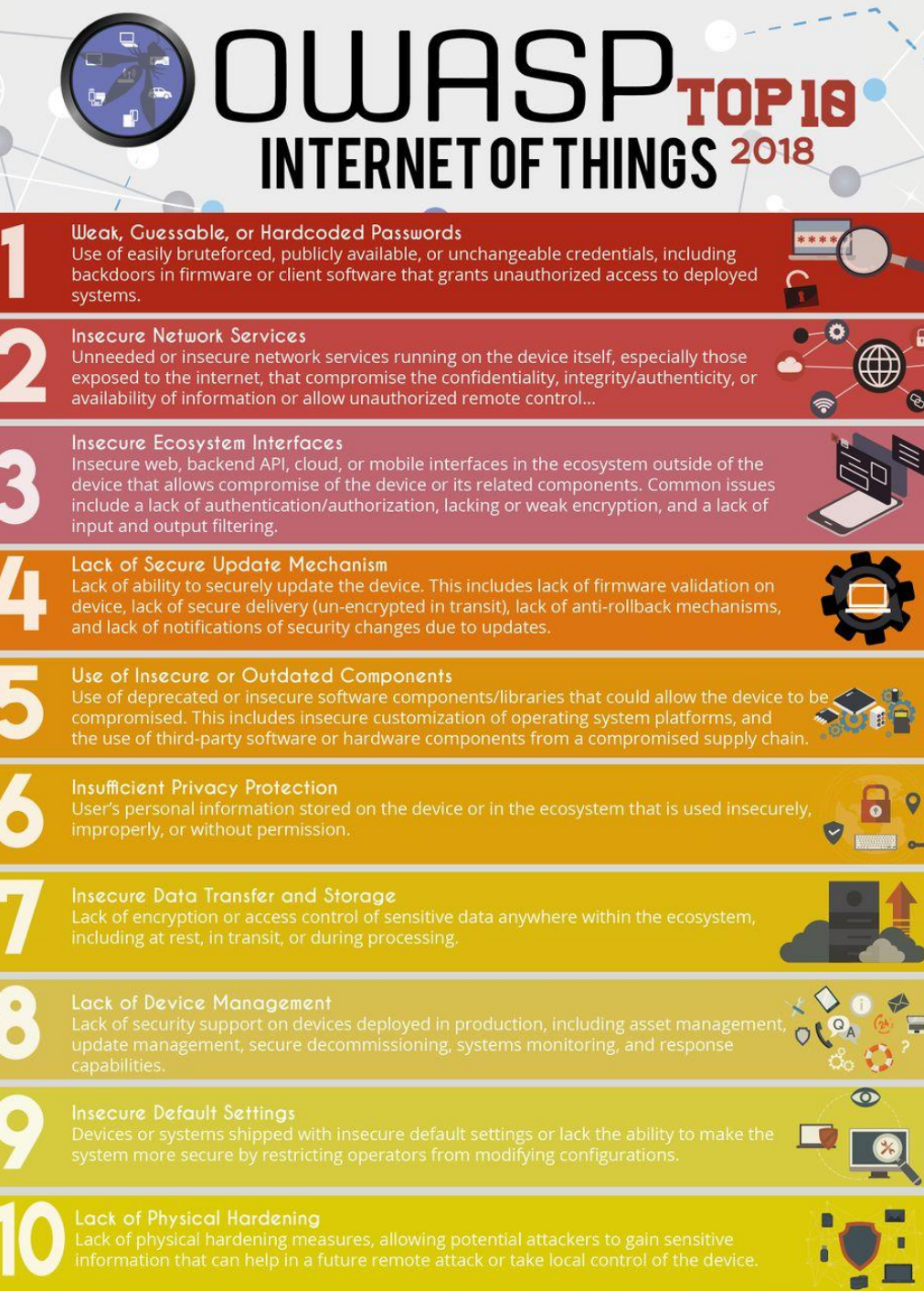


Why Standards Are Valuable?

Guidance Documents

- Guidance Documents for Internet of Things (IoT) security focus on providing frameworks and best practices to address the unique cybersecurity challenges posed by connected devices. These documents help manufacturers, developers, and organizations implement security measures throughout the IoT device lifecycle, from design to deployment and maintenance.





OWASP Top 10 IoT

- The OWASP (Open Web Application Security Project) Top 10 IoT represents the most critical security concerns for Internet of Things devices. This list, maintained by cybersecurity experts, helps developers, manufacturers, and organizations understand and address key vulnerabilities in IoT systems.

Case Study Analysis: Finding, Reporting, and Disclosing an IoT Security Issue

- This case study outlines the process and ethical considerations of discovering, reporting, and disclosing a vulnerability in the **Animas OneTouch Ping insulin pump** by Jay Radcliffe, a security researcher and type I diabetic. It emphasizes the balance between protecting affected individuals, working within legal frameworks, and maintaining trust between researchers and manufacturers.



<https://share.vidyard.com/watch/VR9Gwizko9jwJAAtMDCKvSK?>

Key Phases of the Project

1. Preparation and Testing

- **Device Acquisition:** Jay purchased the insulin pump and built a dedicated test lab to simulate real-world scenarios without impacting actual users.
- **Legal Consultation:** He sought legal advice to ensure compliance with local and national laws, which was critical in avoiding potential legal consequences.
- **Threat Identification:** Identified specific threats and created proof-of-concept demonstrations to understand and exploit vulnerabilities.

Key Phases of the Project

- **2. Coordinated Vulnerability Disclosure**
- **Manufacturer Coordination:** Jay followed the manufacturer's disclosure policy and communicated vulnerabilities via email, phone, and in-person meetings. His communication included:
 - **Technical Details:** How the vulnerabilities functioned.
 - **Impact Assessment:** Implications for patient safety.
 - **Mitigation Recommendations:** Steps the manufacturer could take to resolve the issues.
- **Proof-of-Concept:** Demonstrated the vulnerabilities to validate his findings and provided a code to highlight the exploit.

Key Phases of the Project

- **3. Decision-Making and Public Disclosure**
- **Manufacturer's Response:** The manufacturer decided not to fix the vulnerabilities in the current hardware and instead focused on developing a new version.
- **Public Statement:** Jay disclosed his findings publicly but reassured patients about the relative safety of the device despite its imperfections.
- **Conference Cancellation:** Prioritized patient communication by canceling his scheduled conference talk to ensure that affected individuals were informed through trusted channels (doctors and the manufacturer).

Lessons Learned

1. Ethical Responsibility

- Jay prioritized patient safety by ensuring that no harm came to users during the testing phase.
- He avoided creating panic by carefully timing his public disclosures and allowing patients to receive news from trusted sources rather than through media reports.



Lessons Learned

2. Balancing Technical and Practical Realities

- Acknowledged the manufacturer's focus on future devices instead of older ones and refrained from demanding immediate fixes.
- Supported long-term improvements by maintaining a constructive relationship with the manufacturer.



Lessons Learned

3. Leadership and Collaboration

- Established trust with stakeholders, including patients, regulators, and manufacturers.
- Engaged with the security community to promote better practices for securing medical devices.



Lessons Learned

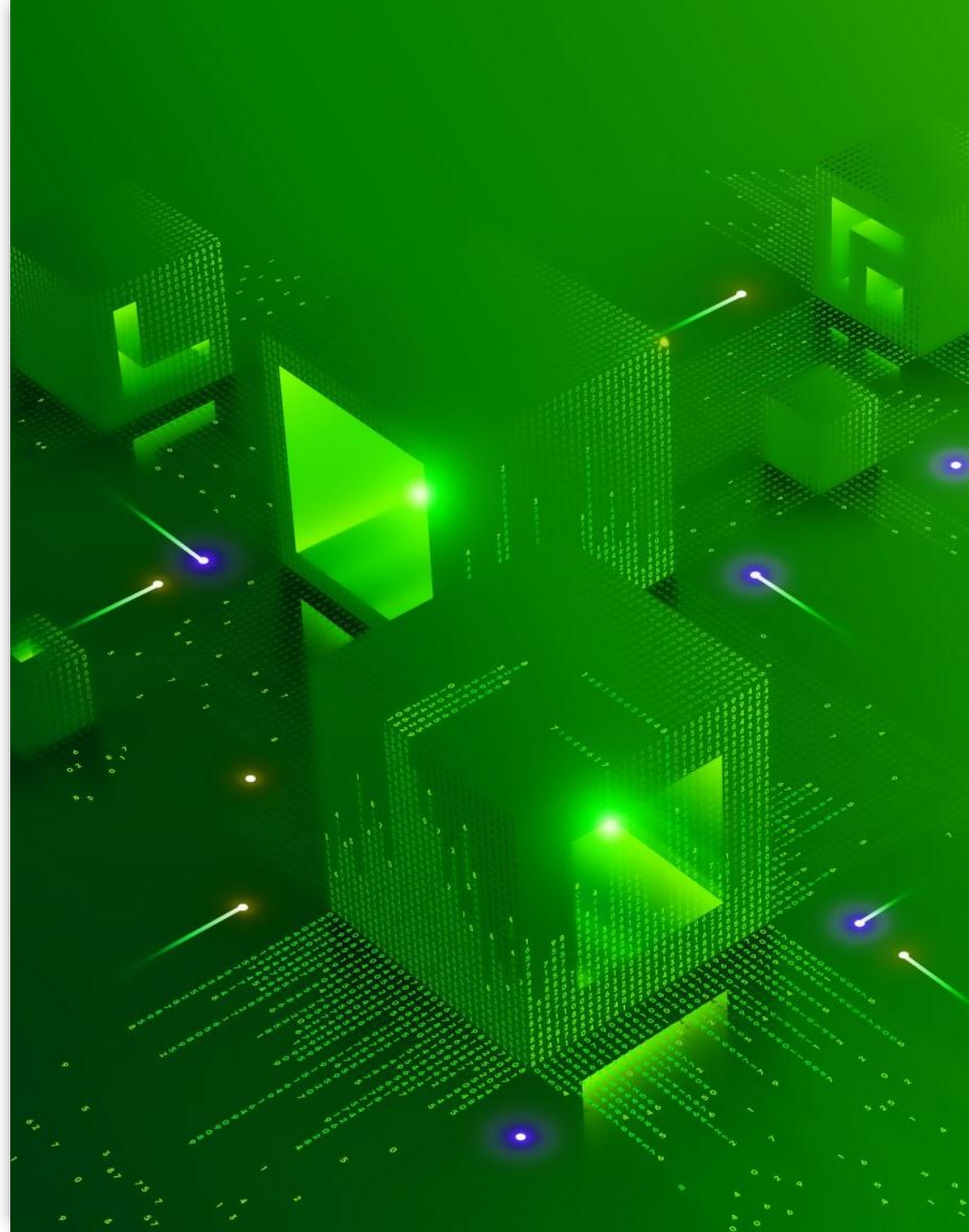
4. Legal Awareness

- By adhering to coordinated vulnerability disclosure protocols, Jay avoided legal repercussions and maintained a professional approach.
- Highlighted the importance of legal consultation and compliance with relevant laws and policies.



Conclusion

- The rapid expansion of the Internet of Things (IoT) has revolutionized the way devices and systems interact, offering significant advantages in efficiency, decision-making, and convenience. However, this growth also brings unique security challenges, including data breaches, device manipulation, and privacy violations, underscoring the critical importance of robust security measures.
- Through this lesson, you have gained a comprehensive understanding of IoT fundamentals, key characteristics, and security risks. The exploration of frameworks and standards, along with the case study on ethical vulnerability disclosure, highlights the need for proactive and collaborative approaches to safeguarding IoT ecosystems.



Questions



End-of-Presentation