COMP482
Cybersecurity
Week 4 - Wednesday

Dr. Nicholas Polanco
(he/him)

KALAMAZOO COLLEGE

Attendance

https://forms.office.com/r/eHWYpCSQN1

COMP482 - Week 4 Check-In

KALAMAZOO COLLEGE

Important Notes

- **We will not be having class on Friday**, the schedule is adjusted to reflect the changes in the coming weeks.
  - Also, a reminder if anyone hears any details about the day we will get off in the coming weeks please let me know :)
- Your presentations are due a **Week from today (Wednesday - Week 5)**
  - This is an academic presentation, you will need citations.
  - I'm not going to tell anyone to dress up, but be "presentable"
  - We will select the order on **Monday of Week 5**

Important Dates (Week 4)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
				Activity: Keylogger or Buffer Overflow Reflection Week 3		

Internet of Things Threats and Defenses

Outline

1. What is the Internet of Things?
2. IoT Architecture & Attack Surface
3. Threats in the IoT Ecosystem
4. IoT Defense Strategies
5. IoT Security Frameworks and Standards
6. TryHackMe: SQL Injection or Activity

What is the Internet of Things?

What is the Internet of Things?

The Internet of Things (IoT) refers to a network of physical objects—"things"—embedded with sensors, software, and other technologies that enable them to collect and exchange data over the internet.

What examples of IoT devices do we have *based on the above definition*?

Image Credit

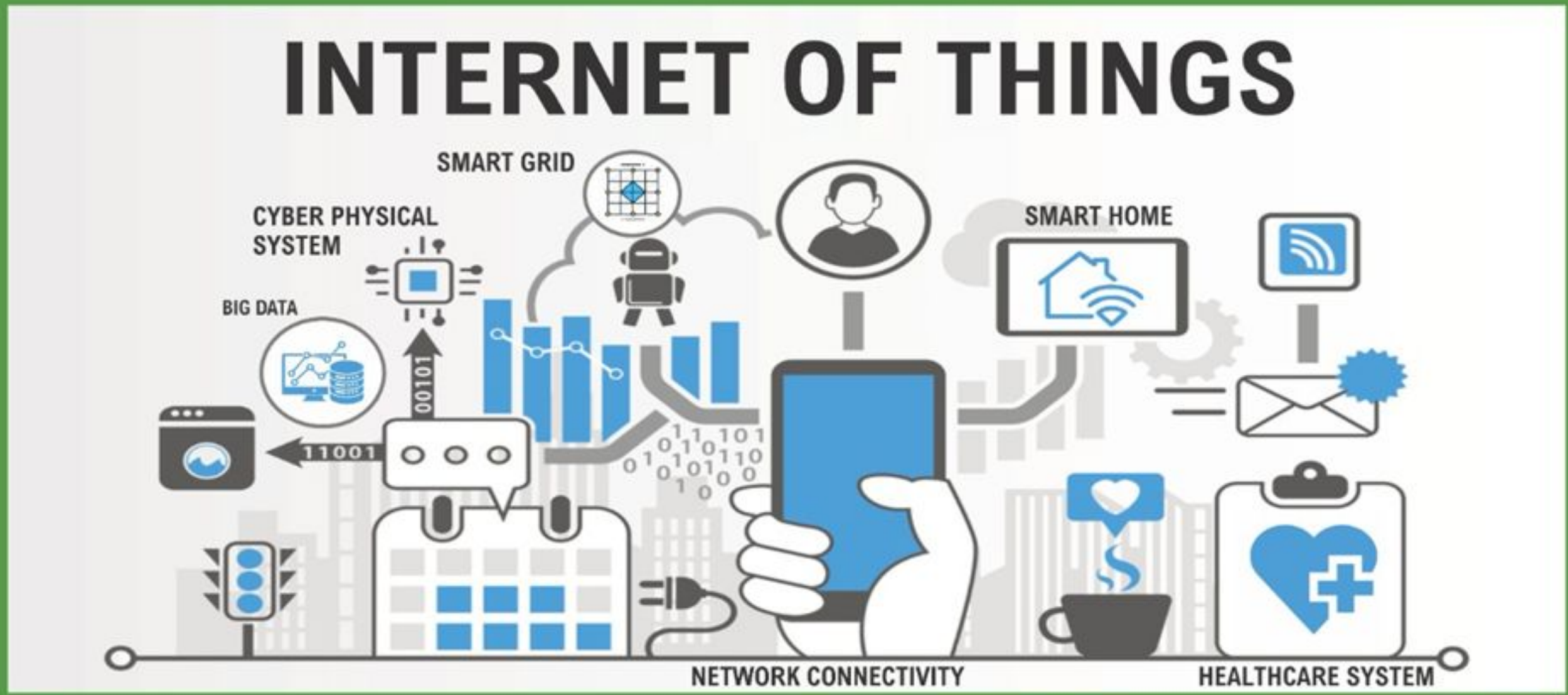

Image Credit
https://thehackersmeetup.medium.com/data-backup-recovery-in-iot-devices-818278615ec9

KALAMAZOO COLLEGE

What is the Internet of Things? (continued)

These IoT devices can include:

- Thermostats (e.g., Nest), lights, locks, security cameras.
- Wearables that track vitals, smart insulin pumps.
- Predictive maintenance for factory equipment.
- Traffic monitoring, waste management systems, environmental sensors.

*At its core, IoT extends internet connectivity beyond standard devices like computers and smartphones to a wide range of devices and everyday objects. Once connected, these devices can communicate with each other and with centralized systems, often in real time.

Image Credit

Core Components of IoT Systems

Devices/Sensors - The "things" that collect data. These can measure temperature, motion, location, usage, etc.

Connectivity - The Wi-Fi, Bluetooth, 5G, Zigbee, LoRaWAN, or other protocols to transmit data.

Data Processing - The cloud or edge computing systems process and analyze the collected data.

User Interface - These are the dashboards, apps, or control systems where users interact with the devices.

Image Credit

Pause: Zigbee

ZigBee devices are based on a central ZigBee hub (gateway), which is connected to the Internet and controls all devices. The devices themselves communicate via a so-called mesh network.

- This means that each device not only receives signals, but also forwards them to other devices.

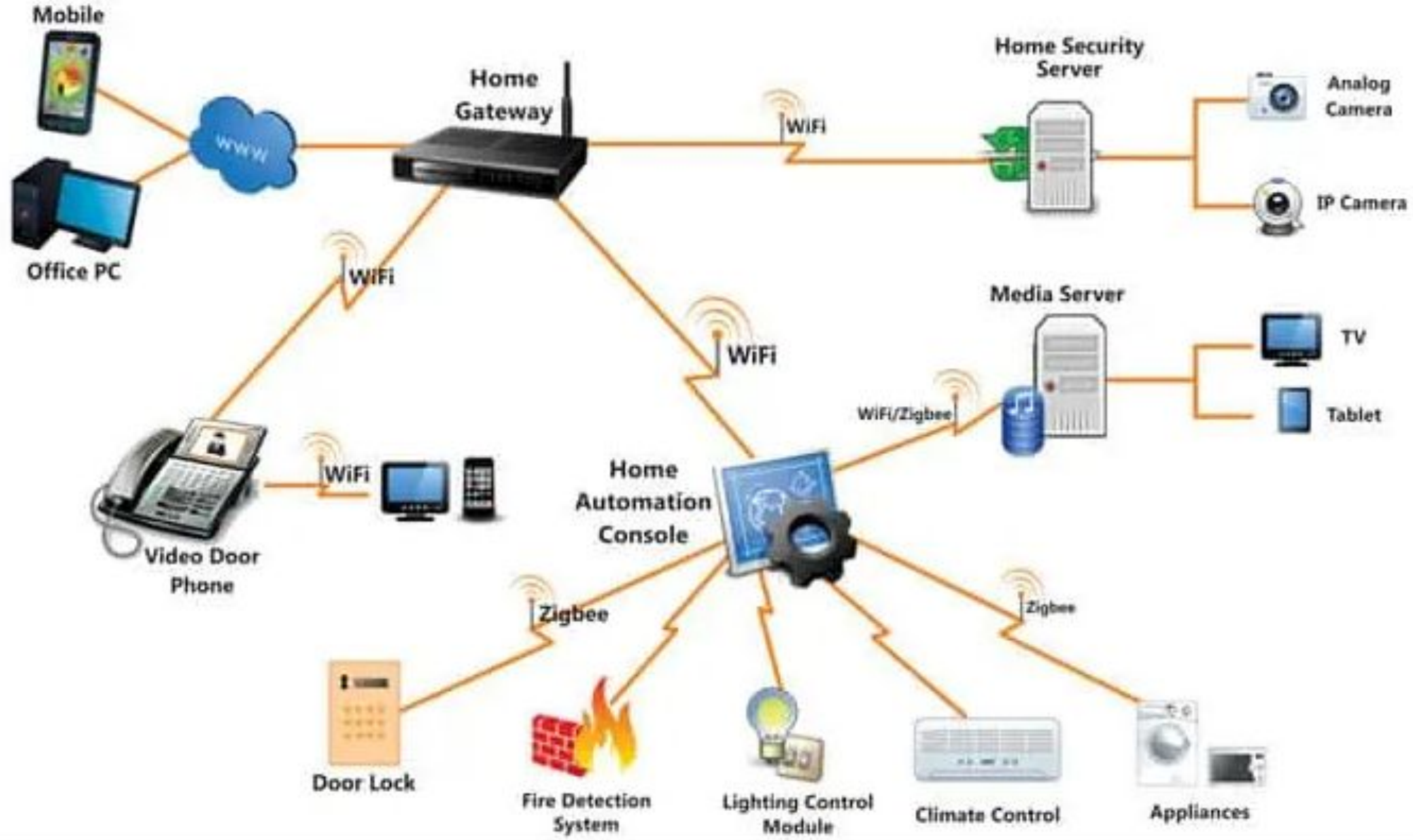

Image Credit
https://www.linkedin.com/pulse/what-zigbee-technology-how-works-nouman-arif

KALAMAZOO COLLEGE

Pause: LoRaWAN

LoRaWAN is a low-power, wide-area network protocol that uses the LoRa radio modulation technique to wirelessly connect devices to the internet. It's designed for long-range, bi-directional communication and is popular for IoT applications requiring low power consumption and long-distance connectivity

Image Credit

LoRaWAN® Architecture

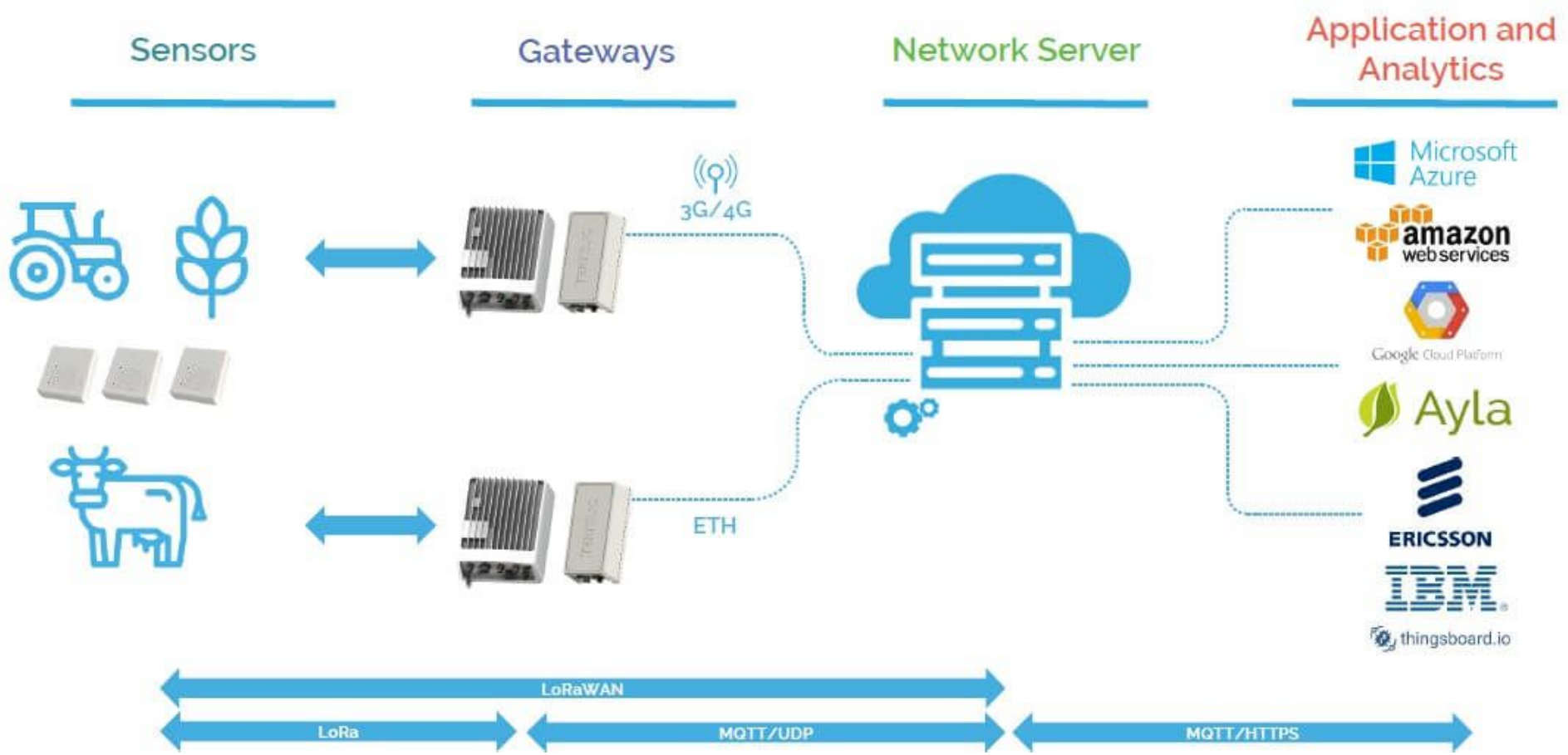

Image Credit
https://tektelic.com/expertise/what-is-lorawan/

KALAMAZOO COLLEGE

Pause: Edge Computing

Edge computing allows devices in remote locations to process data at the "edge" of the network, either by the device or a local server. Then, when data needs to be processed in the central datacenter, only the most important data is transmitted, thereby minimizing latency.

Image Credit

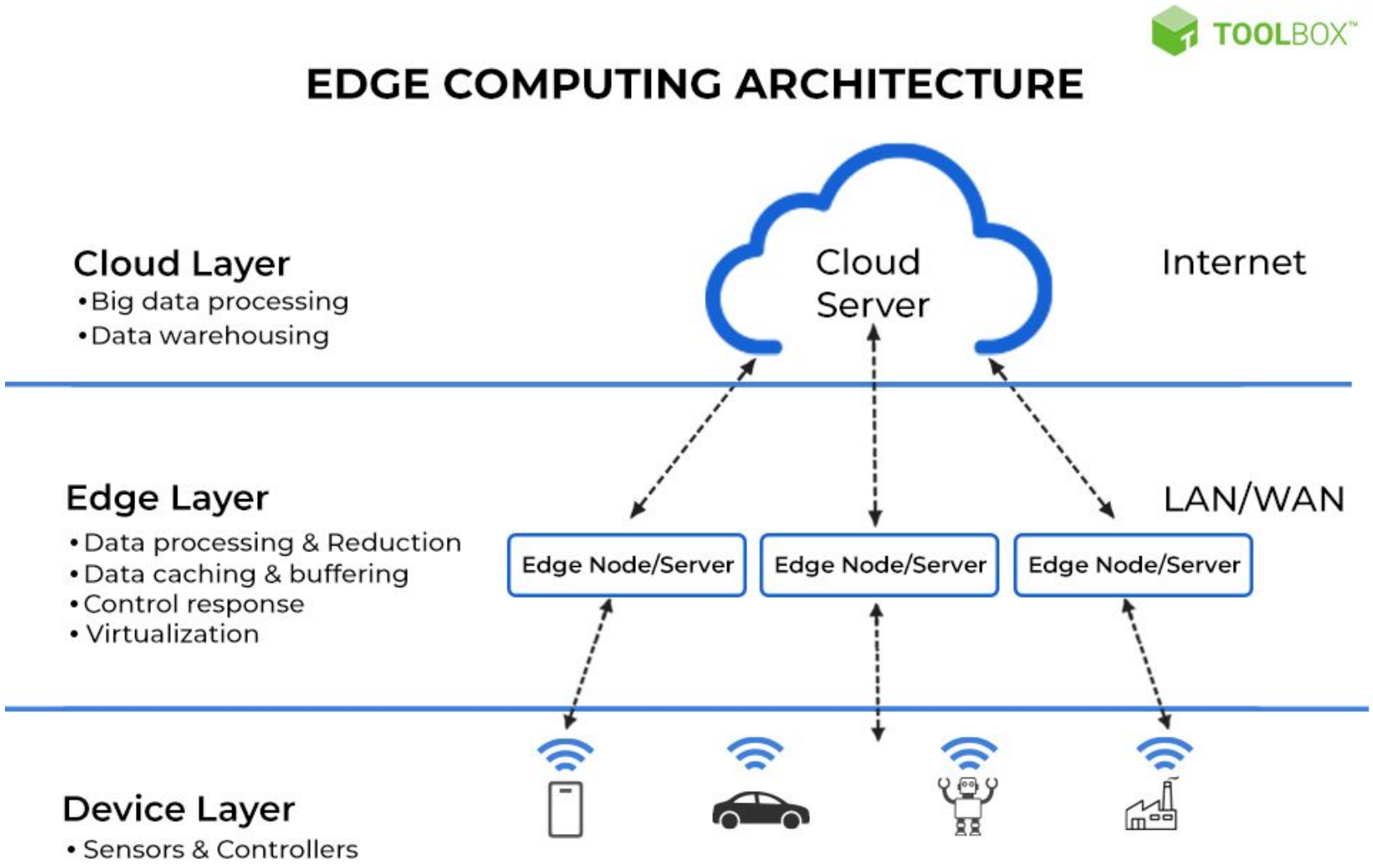

Image Credit
https://www.spiceworks.com/tech/edge-computing/articles/what-is-edge-computing/

KALAMAZOO COLLEGE

Discussion Questions

Why do we think we have seen a large growth of IoT devices?

Should IoT security be prioritized differently across industries? Why or why not?

How can future IoT development be guided to avoid today's cybersecurity pitfalls?

Image Credit

IoT Growth

Convenience & Automation - We have devices like smart thermostats, lights, cameras, and doorbells make life easier by automating everyday tasks and allowing remote control from smartphones.

- How many of you would still use these for convenience despite possible cybersecurity risks? Why or why not?

Falling Costs - As the tech becomes cheaper and more accessible, it's easy for consumers and businesses to adopt IoT devices in bulk.

- Does anyone remember Nintendo Wii remotes?

Image Credit

IoT Growth (continued)

Cloud Connectivity & Big Data - IoT devices feed data to cloud systems, enabling smarter analytics, personalized services, and automation at scale.

- How many of you have looked up at Meijer in the self-checkout?

Industry Demand (Industrial IoT) - In manufacturing, healthcare, and logistics, IoT helps monitor machinery, track shipments, and improve efficiency—fueling adoption in enterprise environments.

Smart Home & Lifestyle Appeal - The idea of a "smart home" has gone mainstream, and people love the tech-forward, integrated lifestyle it offers.

IoT Architecture & Attack Surface

IoT Architecture

IoT systems are typically built on a layered architecture. A commonly used model includes the following four layers:

1. Perception Layer (Sensing Layer)
2. Transport/Network Layer
3. Processing Layer (Middleware Layer)
4. Application Layer

Image Credit

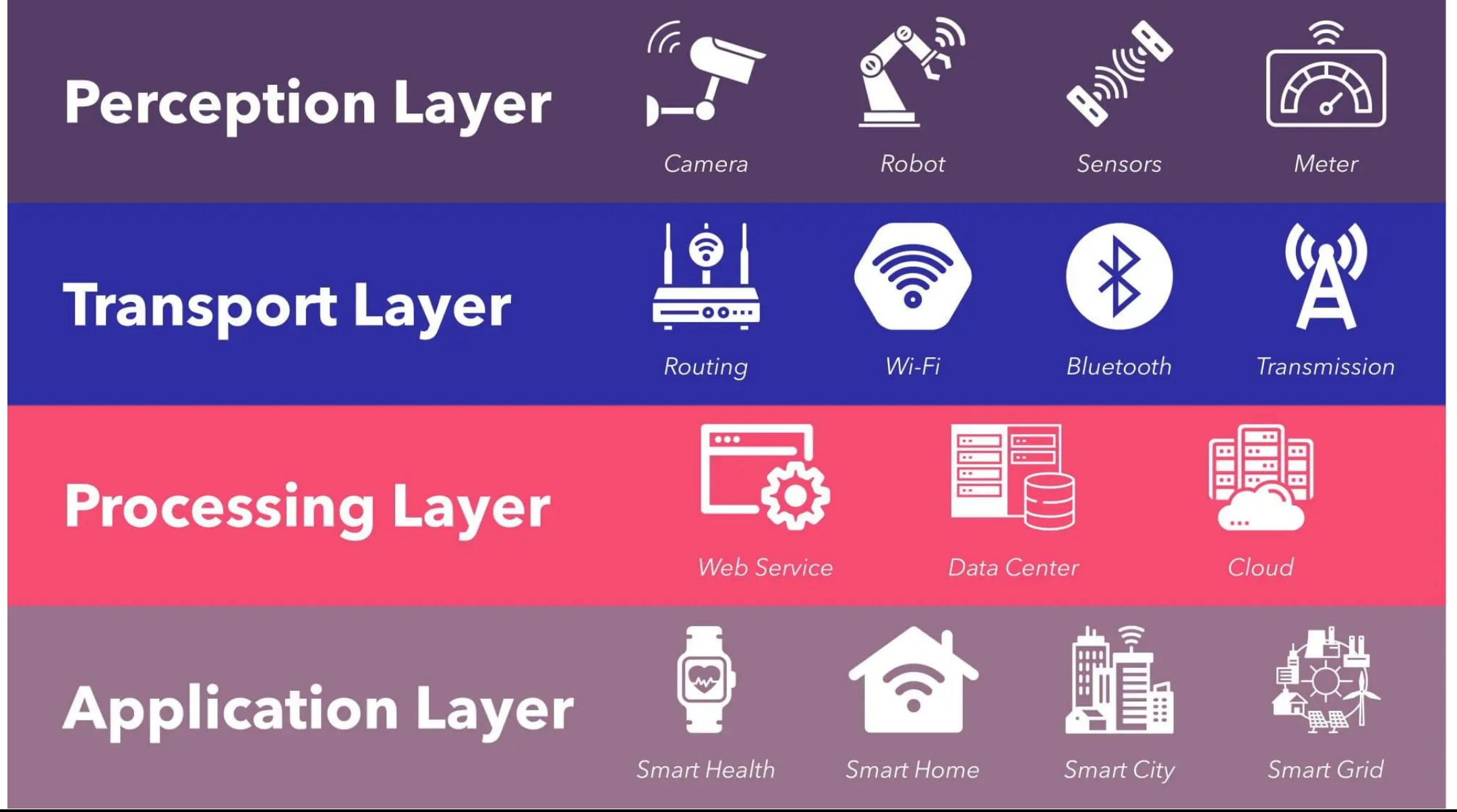

Image Credit
https://dgtlinfra.com/internet-of-things-iot-architecture/

KALAMAZOO COLLEGE

IoT Architecture (continued)

1. Perception Layer (Sensing Layer)

- Purpose - This is responsible for collecting data from the physical environment.
- Components - It can include sensors, actuators, RFID tags, cameras, GPS, etc.
- Function - This detects physical changes and sends raw data to the network layer.

Image Credit

IoT Architecture (continued)

2. Network Layer
- Purpose - This transmits data from the perception layer to processing centers (like cloud servers or local gateways).
- Components - This can include Wi-Fi, 4G/5G, Bluetooth, ZigBee, LoRaWAN, etc.
- Function - This ensures data routing, transmission, and sometimes initial processing.

IoT Architecture (continued)

3. Processing Layer (Middleware Layer)
   - Purpose - This is data aggregation, filtering, and decision-making.
   - Components - These are cloud platforms, edge/fog computing, databases, AI/ML systems.
   - Function - Analyzes data to generate actionable insights or trigger responses.

Image Credit

IoT Architecture (continued)

4. Application Layer

- Purpose - This interfaces with end-users and business logic execution.
- Components - The mobile apps, web dashboards, control systems, industry apps.
- Function - This delivers services like home automation, smart healthcare, industrial monitoring, etc.

Image Credit

Attack Surface

Lack of Built-in Security - We have many IoT devices that are designed with minimal security—weak passwords, no encryption, outdated firmware—making them easy targets for hackers.

Sheer Volume & Scale - The massive number of devices increases the "attack surface" dramatically.

- Why?

Default Credentials & Poor User Practices - The users often don’t change default passwords or update firmware, leaving devices wide open to exploitation.

Image Credit

Attack Surface (Continued)

Botnet Threats - These infected IoT devices can be harnessed into large botnets to carry out massive DDoS attacks.

Data Privacy Risks - IoT devices collect tons of personal data—location, voice, video, habits—which can be intercepted or leaked if not properly secured.

Hard to Patch or Update - The devices are hardwired with firmware that’s not easily updatable, or manufacturers don’t bother pushing out updates.

Image Credit

Threats in the IoT Ecosystem

Threats in the IoT Ecosystem

1. Perception Layer (Sensing Layer)

Security Concerns

- Physical tampering (e.g., replacing sensors).
- Side-channel attacks.
  - An exploit that targets a system by gathering information or influencing its execution through *indirect effects* of the system's hardware or implementation, rather than by directly attacking the code or algorithm.
- Lack of data encryption in transmission.
- Fake data injection (spoofed sensor readings).

Image Credit

Image Credit

KALAMAZOO COLLEGE

Threats in the IoT Ecosystem (continued)

2. Network Layer

Security Concerns

- Man-in-the-middle (MitM) attacks.
  - Wi-Fi Eavesdropping (fake router), Packet Sniffing, Session Hijacking (steal valid session tokens), TLS Intercept (connections are either decrypted or just inspected), ARP Cache Poisoning (impersonate a PC and steal traffic), DNS Spoofing (send a modified or malicious DNS record)
- Denial of Service (DoS) and Distributed DoS (DDoS).
  - Botnets, Scalability (a single botnet can have many IoT devices), Geographic Distribution (IoT botnets can come from various locations, making it difficult to trace their origin)

Image Credit

Threats in the IoT Ecosystem (continued)

3. Processing Layer (Middleware Layer)

Security Concerns

- Data integrity and confidentiality issues.
- Malicious data manipulation.
- Unauthorized access to processing logic or storage.
- Poor API security (vulnerabilities in platform interfaces).

Threats in the IoT Ecosystem (continued)

4. Application Layer

Security Concerns

- Weak authentication and authorization
- Over-permissioned apps
  - Those granted access to more resources or functionalities than they actually need to operate.
- Social engineering attacks
- Exposure of sensitive user data

Pause: Mirai Botnet Attack

The Mirai Botnet was a network of compromised IoT devices that were hijacked and turned into bots that could be remotely controlled by the attackers.

The botnet itself was formed by thousands of these IoT devices, many of which were poorly secured, and could be easily exploited to launch large-scale attacks.

Image Credit

Pause: Mirai Botnet Attack (continued)

What Happened

The Mirai botnet sent huge amounts of traffic to Dyn's infrastructure, causing widespread outages for popular websites and online services that relied on Dyn for DNS services, including Twitter, Reddit, Netflix, and Spotify.

- The attack on Dyn lasted for several hours, causing widespread disruptions across the East Coast of the United States and affecting millions of users globally.

Pause: Mirai Botnet Attack (continued)

How it Worked

1. The Mirai malware would scan the internet for IoT devices that used default usernames and passwords (such as "admin" or "12345").
2. Once it found these vulnerable devices, it would infect them by exploiting weak security and use them to join the botnet.
3. The infected devices would then receive commands from the attackers to send massive amounts of traffic to target IP addresses.

*The attack was particularly effective because of the scale and diversity of the devices involved, making it difficult to defend against.

Image Credit

root:xc3511	root:root
root:vizxv	root:12345
root:admin	user:user
admin:admin	root:pass
root:888888	admin:admin1234
root:xmhdipc	root:1111
root:default	admin:smcadmin
root:juantech	admin:1111
root:123456	root:666666
root:54321	root:password
support:support	root:1234
admin:password	root:klv123

Table 2. A snippet of the hardcoded credentials list in the Mirai sample

Image Credit
https://www.cyfirma.com/blogs/mirai-the-botnet-that-made-iot-dangerous/

KALAMAZOO COLLEGE

Discussion Questions

Can we learn any lessons from Mirai that we don't already know? What are they?

Who is at fault, the user or the company for the default credentials? Why?

Do any of you have IoT devices, and have you updated the login credentials?

Image Credit

IoT Defense Strategies

IoT Defense Strategies

Device-Level Defenses
- Secure boot
- Hardware-based security modules (TPMs)
- Tamper detection

Network & Communication Defenses
- Network segmentation
- Encrypted communication (TLS, DTLS)
- Firewalls and IDS tailored for IoT

IoT Defense Strategies (continued)

Software and Update Management

- OTA (Over-the-Air) updates
- Secure firmware design
  - We want to be incorporating security features during **the firmware development process**
- Vulnerability disclosure programs
  - A structured framework or process that organizations use to receive reports of security vulnerabilities from external sources, like security researchers and ethical hackers.

Image Credit

Pause: Over-the-Air (OTA) Updates

Over-the-Air (OTA) updates are a method of delivering new software or firmware to a device wirelessly, often over the internet or a cellular network. This allows devices to receive updates and enhancements without requiring physical access or a trip to a service center.

What types of systems could really benefit from these? Do we see risks with a system like this?

Image Credit

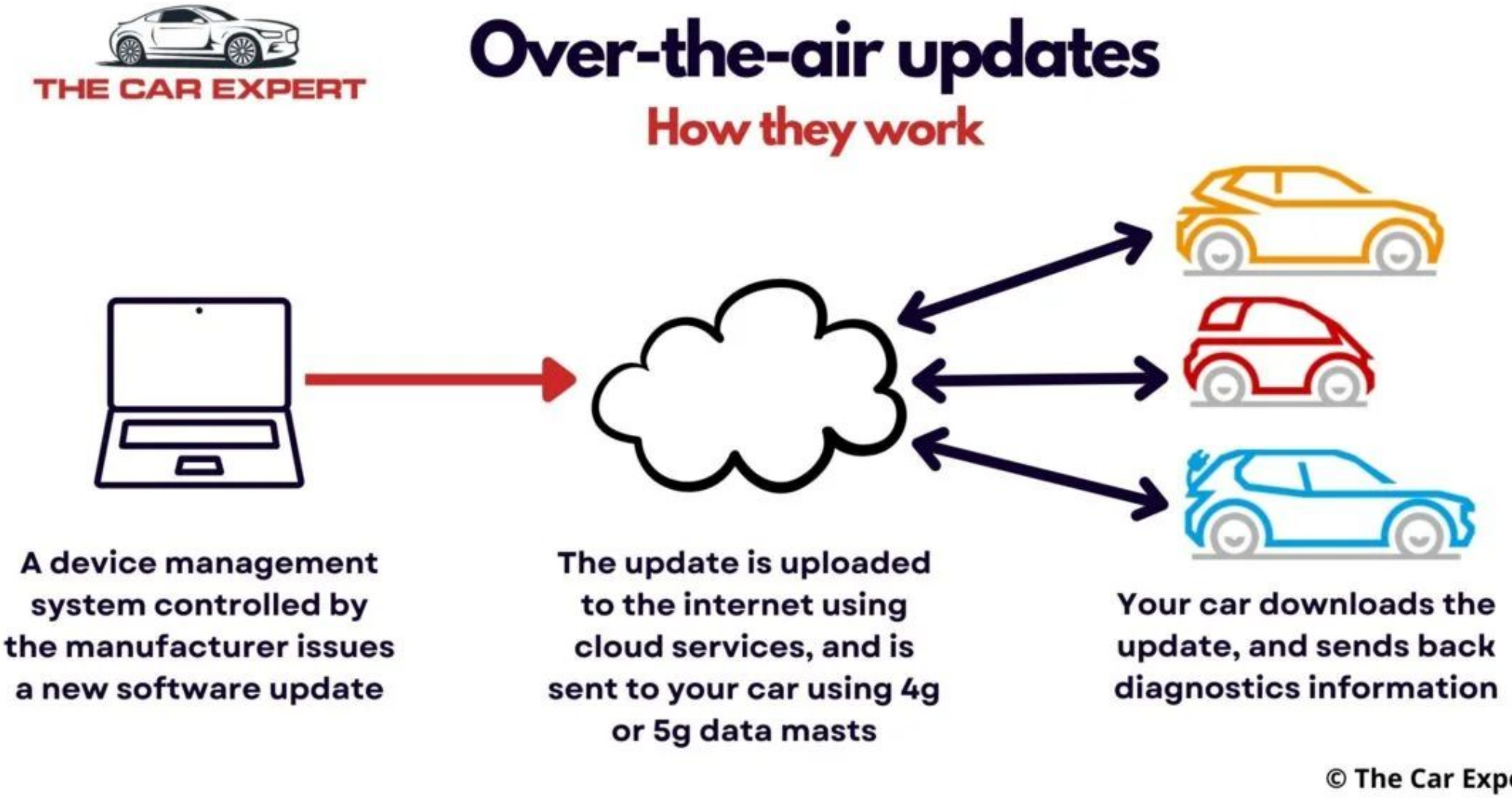

Image Credit
https://www.thecarexpert.co.uk/over-the-air-software-updates/

KALAMAZOO COLLEGE

IoT Security Frameworks and Standards

IoT Security Frameworks and Standards

NIST IoT Cybersecurity Framework

A set of guidelines developed by the National Institute of Standards and Technology (NIST) to help organizations manage cybersecurity risks associated with IoT devices. This is a structured approach to:

- Identifying risks introduced by IoT devices
- Implementing security measures to mitigate those risks
- Ensuring that IoT devices are integrated securely into larger IT systems

Image Credit

IoT Security Frameworks and Standards (continued)

NIST IoT Cybersecurity Framework (continued)

IoT Device Cybersecurity Capability Core Baseline (IR 8259A) - This outlines what security capabilities IoT devices should have:

- Device Identification
- Device Configuration
- Data Protection
- Logical Access to Interfaces
- Software Update Mechanisms
- Cybersecurity Event Logging

These are the minimum capabilities expected from IoT device manufacturers.

IoT Security Frameworks and Standards (continued)

NIST IoT Cybersecurity Framework (continued)

Non-Technical Supporting Capabilities (IR 8259B) - These are organizational practices (not device features) that support device cybersecurity:

- Documentation
- Information sharing
- Education/training
- Vulnerability management

<u>Do we think information sharing is good or bad for cybersecurity? Why?</u>

Image Credit

IoT Security Frameworks and Standards (continued)

NIST IoT Cybersecurity Framework (continued)

Function	IoT Example
Identify	Understand what IoT devices are in use and what risks they introduce
Protect	Implement access controls, encrypt data, secure firmware updates
Detect	Monitor for unusual device behavior or unauthorized access
Respond	Take action on discovered threats or incidents involving IoT devices
Recover	Restore device functionality and improve processes post-incident

Image Credit

IoT Security Frameworks and Standards (continued)

OWASP IoT Top 10 (2024)

A project by the Open Worldwide Application Security Project (OWASP) that identifies the top security vulnerabilities commonly found in Internet of Things (IoT) devices and ecosystems.

<u>Do we want to try to guess some?</u>

IoT Security Frameworks and Standards (continued)

OWASP IoT Top 10 (2024) (continued)

1. Weak, Guessable, or Hardcoded Passwords - Use of default, easy-to-guess credentials or hardcoded passwords that cannot be changed.
2. Insecure Network Services - Services running on the device that are unnecessary, insecure, or improperly configured.
3. Insecure Ecosystem Interfaces- Weaknesses in APIs, web interfaces, or mobile apps interacting with the IoT device.
4. Lack of Secure Update Mechanism - No way to securely update firmware or software, or updates that can be tampered with.
5. Use of Insecure or Outdated Components - Reliance on outdated software libraries or OSes with known vulnerabilities.

Image Credit

IoT Security Frameworks and Standards (continued)

OWASP IoT Top 10 (2024) (continued)

6. Insufficient Privacy Protection - Poor handling of personal or sensitive data collected by IoT devices.
7. Insecure Data Transfer and Storage - Data is not properly encrypted in transit or at rest.
8. Lack of Device Management - No way to manage devices securely over their lifecycle (e.g., onboarding, monitoring, decommissioning).
9. Insecure Default Settings - Devices ship with settings that are not secure out of the box
10. Lack of Physical Hardening - Devices are physically accessible and lack protection from tampering.

Discussion Questions

Why do you think IoT security should be discussed at all?

Do you think things like OWASP IoT Top 10 or NIST IoT Cybersecurity are actually useful? Why or why not?

Image Credit

Activity: IoT Activity

Activity: IoT Activity

OR

Activity: Keylogger and Buffer Overflow

OR

Topic Presentation

OR

Course Project

*For those of you interested in doing **lots** of hands-on hacking and activities, check out the Dam Vulnerable Web Application (DVWA)

- https://github.com/digininja/DVWA

Image Credit

Questions?