

# IoT Security

S. Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources. Thanks to all authors and sources made those contents public and usable for educational purpose

# Introduction

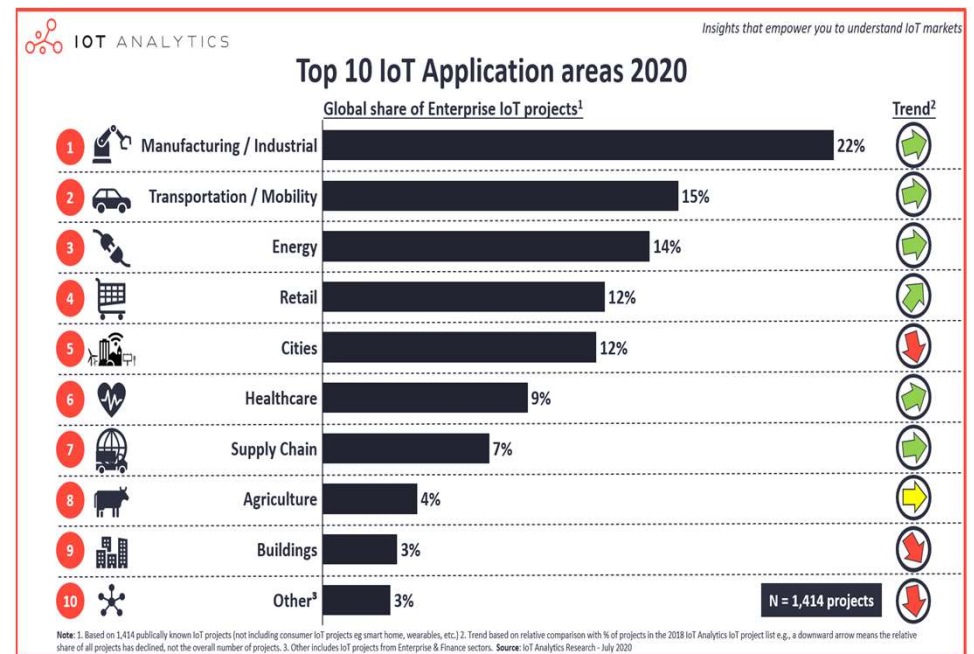
- It is the network of interconnected things/devices which are embedded with sensors, software, network connectivity and necessary electronics that enables them to collect and exchange data.
- The term "Internet of things" was coined by Kevin Ashton of Procter & Gamble, later MIT's Auto-ID Center, in 1999.
- What makes different
  - WWW and Ubiquitous Computing  
Ans: M2M, Both Push and Pull

# History

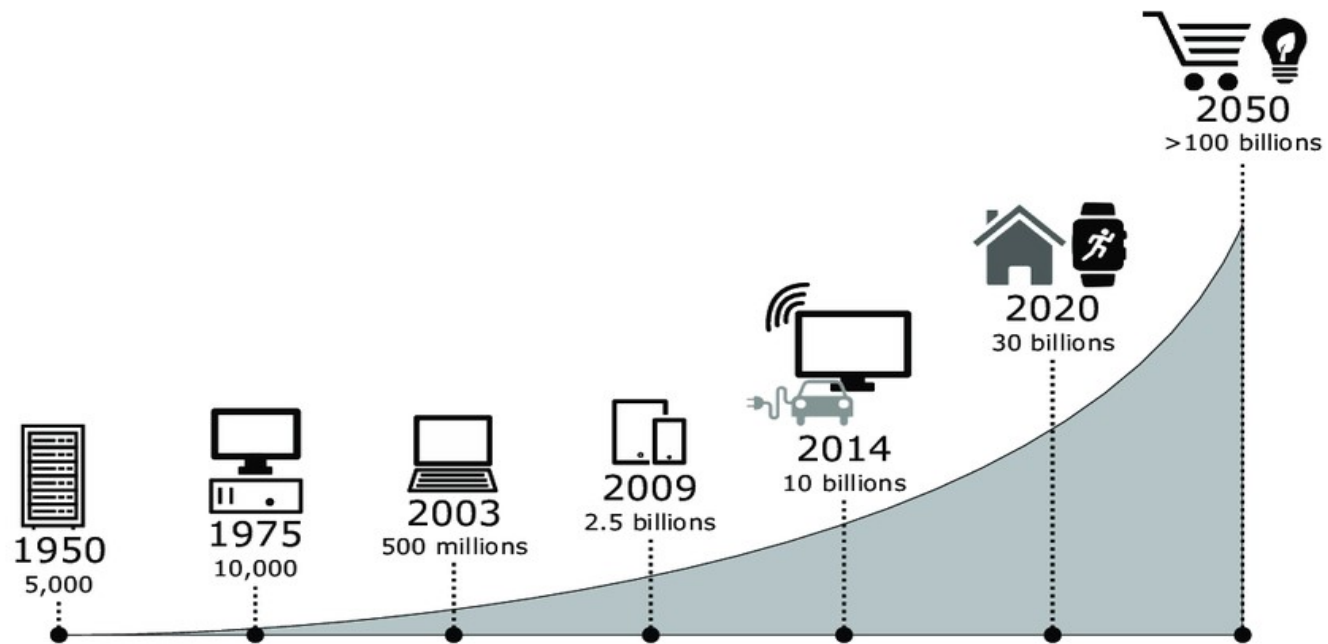
- According to IBM, the first IoT device was invented in 1982 when David Nichols, a Carnegie Mellon computer science grad student, was craving a Coke.
- Cold Coke - Nichols and his friends came up with the idea of installing micro-switches — connected to the department’s main computer via ARPANET — in the machine to notify them if any cold sodas were available.
- Although Nichols’s invention and John Romkey’s 1990 Internet-connected toaster were some of the first to be reported,
  - the term “Internet of Things” wasn’t coined until Kevin Ashton gave a presentation in 1999 where he referred to this technology as a connection of several devices via radio-frequency identification (RFID) tags.

# Applications

- Home Automation
- Industrial Automation
- Smart Grid
- Medical
- So many

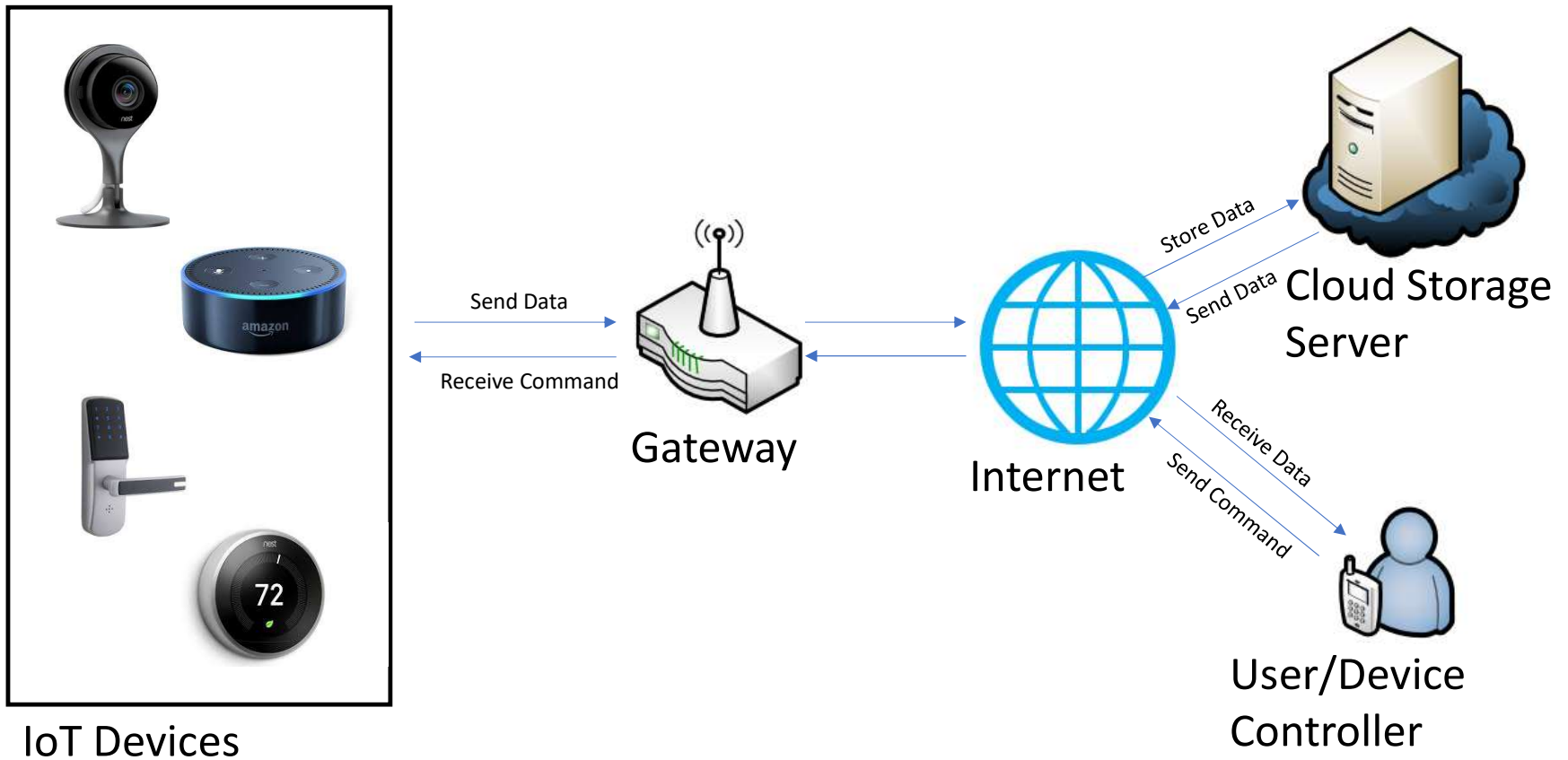


# Growth of IoT



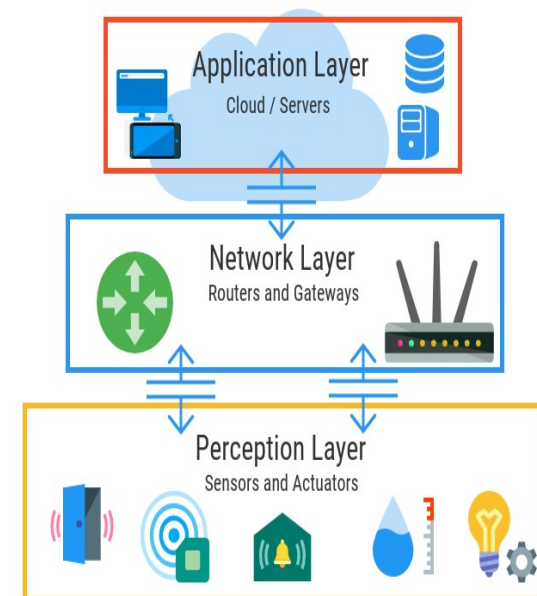
Maurizio Capra, Riccardo Peloso, Guido Masera, Massimo Ruo Roch and Maurizio Martina Edge Computing: A Survey On the Hardware Requirements in the Internet of Things World , Future Internet, MDPI

# IoT Communication



# Layers

- Perception:
  - This is where the sensors and connected devices come into play as they gather various amounts of data as per the need of the project.
  - These can be the edge devices, sensors, and actuators that interact with their environment.
- Network:
  - The data that's collected by all of these devices needs to be transmitted and processed.
  - It connects these devices to other smart objects, servers, and network devices. It also handles the transmission of all of the data.
- Application:
  - The application layer is what the user interacts with. Responsible for delivering application specific services to the user.
  - This can be a smart home implementation, for example, where users tap a button in the app to turn on a coffee maker.





# IoT Device

- NIST describes an IoT device as computing equipment with at least one transducer (i.e., sensor or actuator) and at least one network interface.
- All IoT products contain at least one IoT device and may contain only this product component.
- In many cases, the IoT product may be purchased as one piece of equipment (i.e., the IoT device) but still requires other components to operate, such as a backend (i.e., cloud server) or companion user application on a personal computer or smartphone.
- Complex IoT products may contain multiple physical IoT devices, contain other kinds of equipment, or connect to multiple backends or companion applications as components

# IoT Product Components

- Networking/gateway hardware (e.g., a hub within the system where the IoT device is used).
- Companion application software (e.g., a mobile app for communicating with the IoT device).
- Backends (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device).

# Eco-system

- IoT Device
- Communication Device
- Cloud
- Mobile Application

# IoT vs IIoT

- The Industrial Internet of Things (IIoT) focuses on the industrial sector.
- It involves the application of IoT technologies to industrial applications and processes, such as manufacturing, logistics, and energy management.
- IIoT leverages technologies such as machine learning, big data, smart sensors, and machine-to-machine (M2M) communication to enhance industrial processes.
- The most notable difference is that while IoT primarily,

IoT	IIoT
Focuses on consumer usage and improving life quality	Focuses industrial applications, aiming to improve efficiency and productivity in industrial settings.

# Internet of Everything (IoE)

- CISCO coined the term IoE.
- It is a networked connection of people, process, data, and things.
- By comparison, the “Internet of Things” (IoT) refers simply to the networked connection of physical objects (doesn’t include the “people” and “process” components of IoE).
- IoT is a single technology transition, while IoE comprises many technology transitions (including IoT).

# Protocols

- Application Protocol - Constraint Application Protocol (CoAP), MQTT, others
- Network/ Link Layer Protocol – WiFi, Bluetooth, Zigbee, LoWPAN, others

# Challenges with IoT Devices

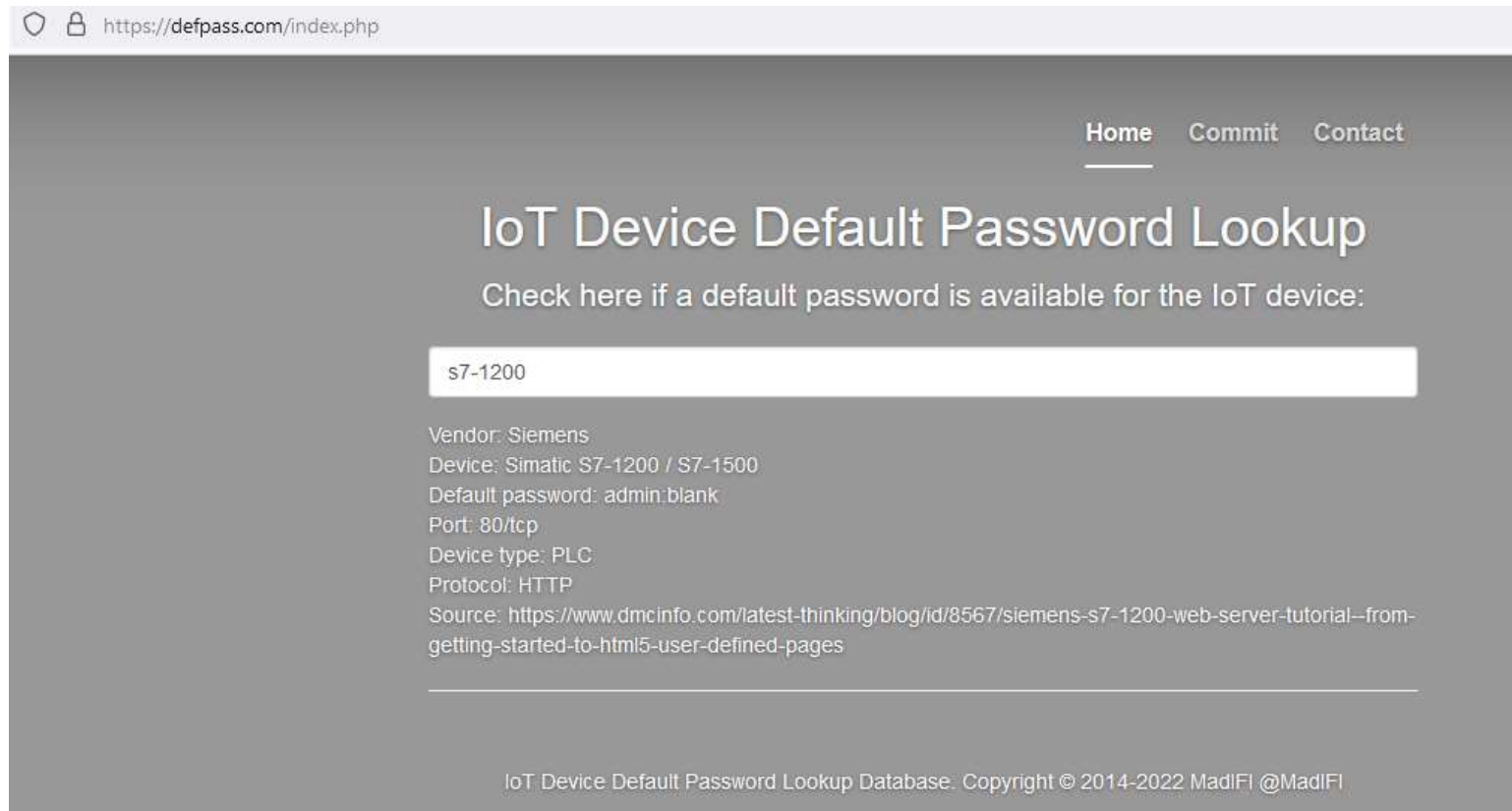
- No mandatory guidelines for Hardware and Software
- Manufacturers stop providing security updates
- Small and inexpensive

# Risk

- Exposed to Natural Elements.
- Public Access
- Variety
- Volume
- Consequence
- Constraints



# Check the devices default password



The screenshot shows a web browser window with the URL <https://defpass.com/index.php>. The page has a dark grey background and a white navigation bar with links for [Home](#), [Commit](#), and [Contact](#). The main heading is "IoT Device Default Password Lookup" in a large, white, sans-serif font. Below the heading is a sub-heading: "Check here if a default password is available for the IoT device:". A white search input field contains the text "s7-1200". Below the search field, the following information is displayed in a smaller white font: Vendor: Siemens, Device: Simatic S7-1200 / S7-1500, Default password: admin:blank, Port: 80/tcp, Device type: PLC, Protocol: HTTP, and Source: <https://www.dmcinfo.com/latest-thinking/blog/id/8567/siemens-s7-1200-web-server-tutorial--from-getting-started-to-html5-user-defined-pages>. At the bottom of the page, there is a footer: "IoT Device Default Password Lookup Database. Copyright © 2014-2022 MadIFI @MadIFI".

# IoT Vs IT Security

- IoT security is more challenging than IT security because of two key factors:
  - Enormous attack surface presented by the anticipated billions of IoT devices,
  - Increased vulnerability of many of those devices.
- Many devices will be low-cost end nodes, with low (or no) budget for security measures such as physical tamper-proofing .
- Many devices will have resource constraints that lead to vulnerabilities (e .g ., insufficient compute power for encryption capability) .
- Many IoT devices will be more readily physically accessible (e .g ., smart light bulbs, smart thermostats, smart power meters, smart roadside sensors) than traditional IT equipment .
- The great diversity in IoT devices—from tiny microcontroller based sensors to powerful server-class computers—will make it difficult for device manufacturers to incorporate a single standard of security .
- IoT devices will be created by a much larger pool of developers

# Security Requirements

- Physical Security: IoT devices placed in public places may be physically accessed by attackers, which should not be allowed.
- Data Security: The sensitive data stored in the devices should not be accessible by the attacker if the system is compromised.
- Communication Security: The network traffic should be confidential, either using a secure or non-secured protocol with encryption.
- Hardware Security: The devices can have the TPM to prevent the boot virus, etc. Also, it should have the sensing to control data leakage for external access.
- Software Security: The updated and secure software has to be used on IoT devices. No vulnerable Operating Systems or firmware's, drivers and interfaces
- Management Security: Hardening of security by having only needed software's on the device.

# Layers of Devices – As per our Guidelines

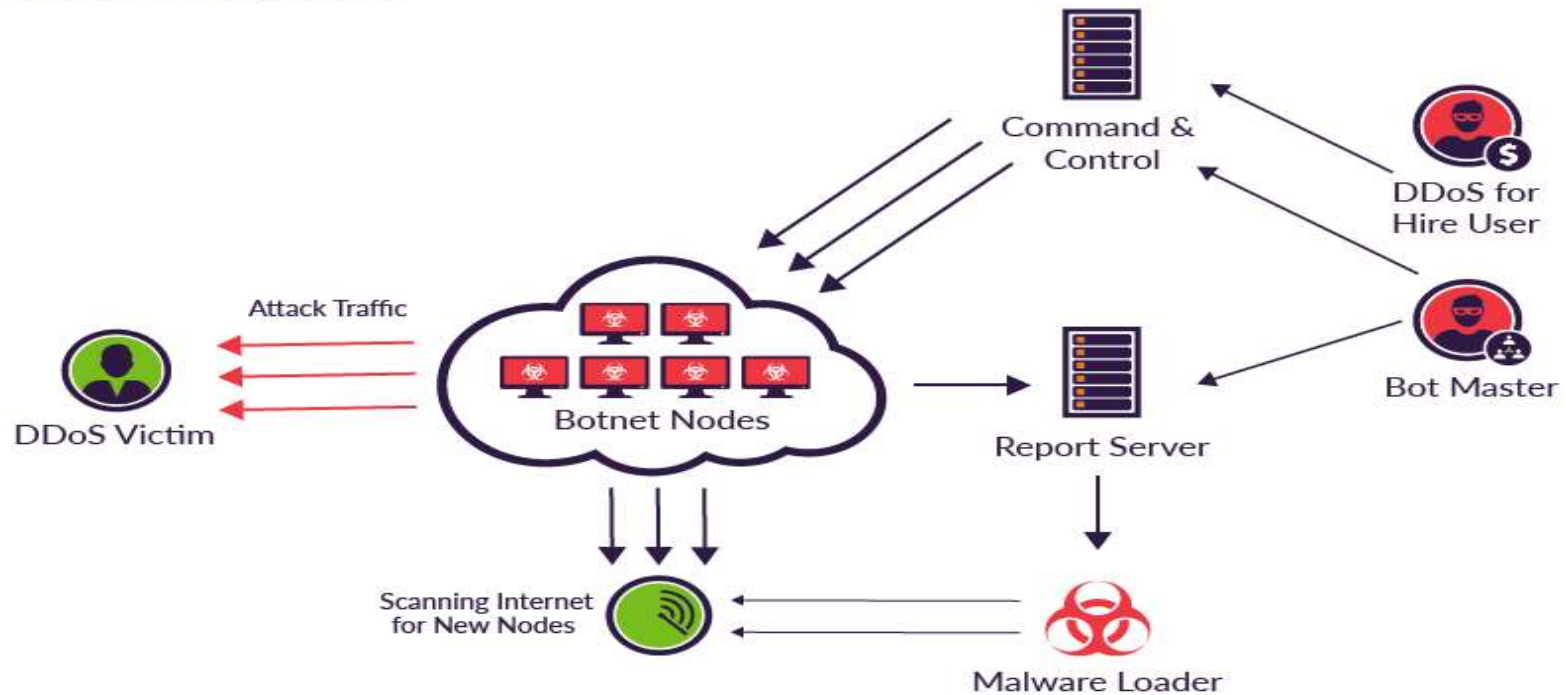
1. Application
2. Session
3. Network
4. Operating System
5. Memory
6. Firmware
7. Hardware

# Breaches

- SolarWinds Orion 2020 supply chain attack
- IoT malware and Ryuk ransomware attacks during COVID-19
- Mirai botnet attacks - hundreds of thousands of IoT devices accessed
- Stuxnet attack: IoT devices used to damage Iran's nuclear program

# Machine to Device – Mirai Bot

## Mirai at a Glance

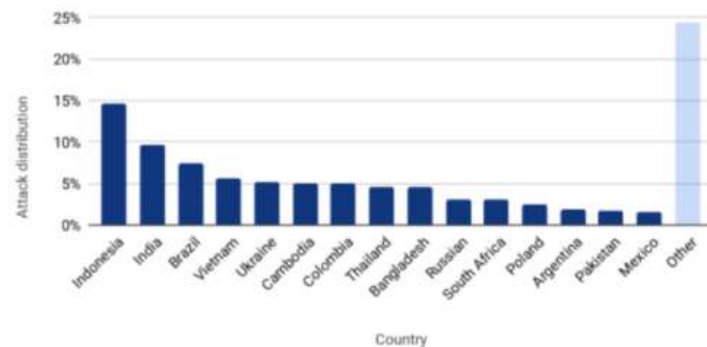


October of 2016 – Massive DDoS on Dyn DNS server

# Cloudflare: Mirai Botnet Launched Record-Breaking DDoS Attack' July 21

Attack Source by Country

Top countries



Distribution of the attack sources by top countries

Mirai botnet variant tracked as 'V3G4' targets 13 vulnerabilities in Linux-based servers and IoT devices to use in DDoS (distributed denial of service) attacks

<https://www.esecurityplanet.com/threats/cloudflare-mirai-botnet-ddos-attack/>  
<https://www.bleepingcomputer.com/news/security/new-mirai-malware-variant-infects-linux-devices-to-build-ddos-botnet/>

## The TRENDnet Webcam Hack (2012)

- TRENDnet marketed its SecurView cameras for various uses ranging from home security to baby monitoring and claimed they were secure, the FTC said.
- However, they had faulty software that let anyone who obtained a camera's IP address look through it — and sometimes listen as well.
- Although users can set up the cameras with a password, the videostream from even a password-protected camera is available to anyone who knows the camera's net address, which consists of an IP address, and a sequence of 15 digits that are the same for every computer.



# IoT Attack Surfaces

Attack Surface	Vulnerability
Ecosystem Access Control	<ul style="list-style-type: none"><li>• Implicit trust between components</li><li>• Enrollment security</li><li>• Lost access procedures</li></ul>
Device Memory	<ul style="list-style-type: none"><li>• Cleartext usernames</li><li>• Cleartext passwords</li><li>• Third-party credentials</li><li>• Unencrypted data</li></ul>
Device Physical Interfaces	<ul style="list-style-type: none"><li>• User CLI</li><li>• Admin CLI</li><li>• Privilege escalation</li></ul>
Device Web Interface	<ul style="list-style-type: none"><li>• SQL Injection</li><li>• XSS</li><li>• Weak Passwords</li></ul>
Device Firmware	<ul style="list-style-type: none"><li>• Hardcoded credentials</li><li>• Sensitive information (URL) disclosure</li><li>• Encryption keys</li></ul>
Device Network Services	<ul style="list-style-type: none"><li>• Denial of Service</li><li>• Buffer Overflow</li><li>• Poorly implemented encryption</li></ul>

# Matter Protocol

- It is for the interoperability
- Matter uses the Thread networking protocol, which is an IPv6-based wireless networking protocol designed for low-power devices.
- When a new device is added to a Matter network, it goes through a simple setup process, allowing it to connect to the network and begin communicating with other devices.
- The setup process includes authenticated device pairing, which ensures that only authorized devices can join the network.
- *End-to-end Encryption*
- Uses a *public key infrastructure* (PKI). Certificates play a critical role in the Matter PKI, as they are used to authenticate devices and encrypt data transmissions.

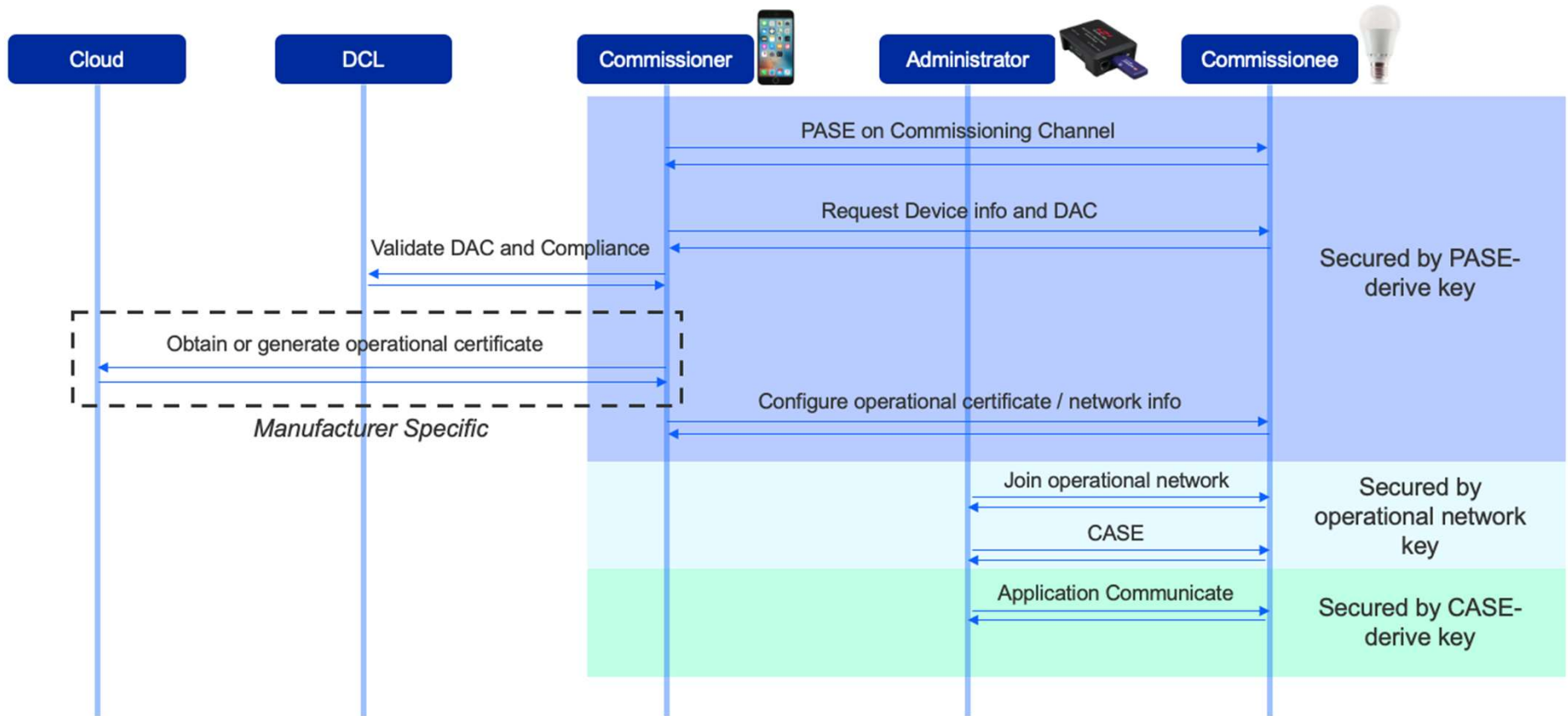
# Matter Network Commissioning

- Device discovery: New devices advertise their presence to the controller through the following methods:
  - Bluetooth LE, DNS-SD, or Wi-Fi Access Point (planned for future releases).
  - The advertisement priority is provided in the device's onboarding data.
- Security setup: The first session between devices is established using the Passcode-Authenticated Session Establishment (PASE) protocol, which is exclusive to the commissioning process.
- Establish fail-safe: The new device backs up its original configuration. This is also used as a timer that sets a limit for the entire commissioning process.
- Preliminary node configuration: The controller reads the Basic Information Cluster of the new device, and configures the device with regulatory information, including location and current UTC time.

# Matter Network Commissioning

- Certificate verification: The controller checks whether the new device is Matter-certified. If the validity and ownership of the Matter Device Attestation elements cannot be proven, the verification fails.
- Install operational credentials: The controller installs the Node Operation Certificate (NOC) and Operation ID on the new device, making it the new node on the Matter fabric.
- Network commissioning: The controller provisions the new node with operational network credentials, either Wi-Fi or Thread, and requests that it connect to the network.
- Operational discovery: The controller discovers that new node on the operational network using DNS-SD.
- Security setup with CASE: Secure communication is established using the Certificate-Authenticated Session Establishment (CASE) protocol, which handles the exchange of NOCs to set up a session that is secured with a new pair of keys.
- Disarm fail-safe: The new device removes the configuration backup, which also stops the fail-safe timer.

# Matter Client Connection Process



# Application



Alexa Open the Door

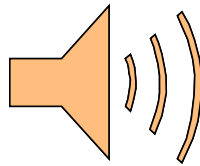


## Attack Vectors

- Voice Recognition
- Speaker Recognition [Noise or changed voice]
- Command Execution

# Adversarial Attacks: Speech Recognition

Hello Darkness  
My Old Friend



Deactivate Security Camera  
And Unlock Front Door

(Schoenherr et al, NDSS 2019)

# Authentication

- Voice Biometrics are easy to spoof
- Fingerprint/passwords will be annoying



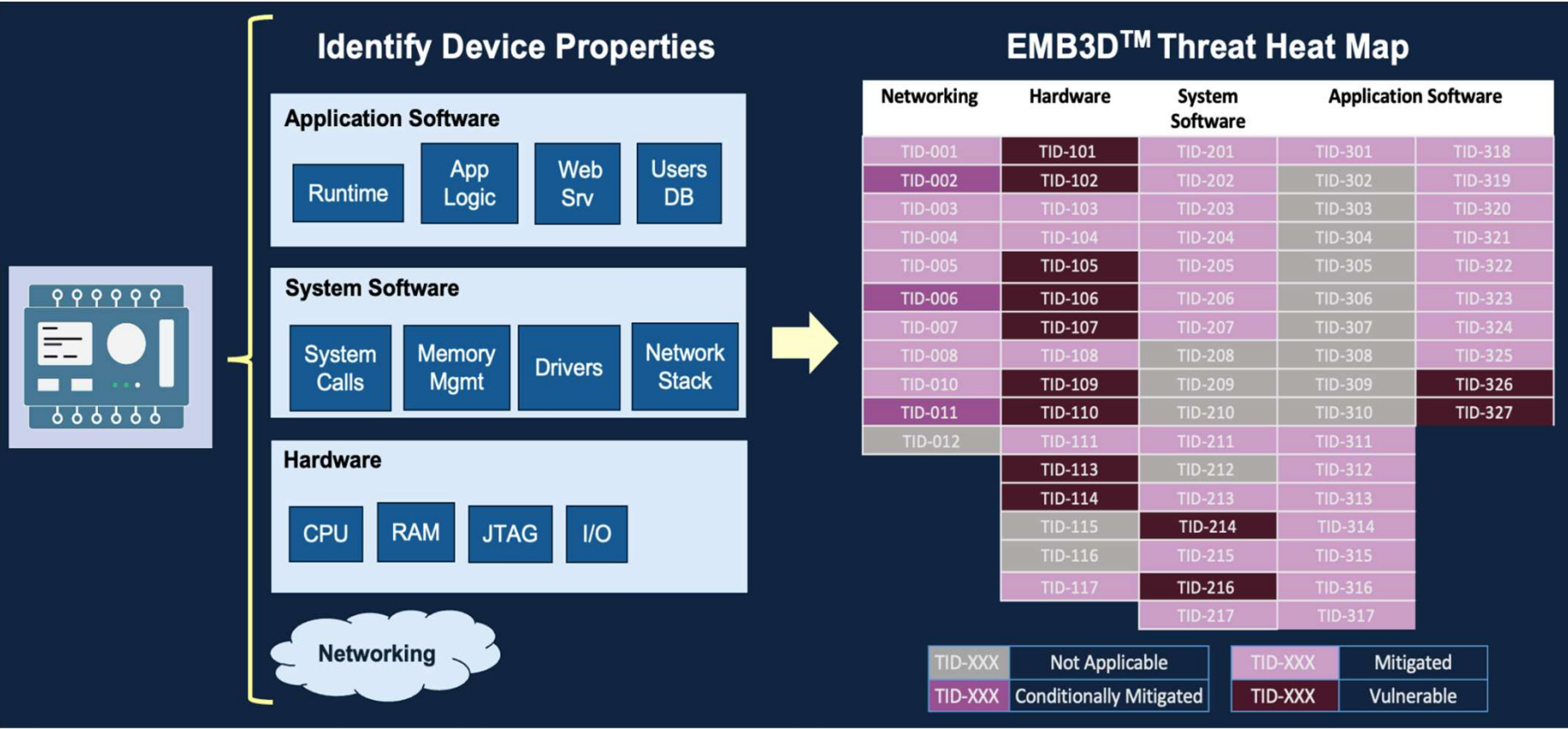
# Privacy

- Voice Enabled Devices listen everything

# Device Auditing

- **AWS** - A set of predefined checks for common IoT security best practices and device vulnerabilities.
  - Example – Hardcoded Password
- **Risk Classification**
  - **Critical:** Require urgent attention.
    - Critical issues often allow bad actors with little sophistication and no insider knowledge or special credentials to easily gain access to or control of your assets.
  - **High:** Require urgent investigation and remediation planning.
    - Like critical issues, high severity issues often provide bad actors with access to or control of your assets.
    - However, high severity issues are often more difficult to exploit.
    - They might require special tools, insider knowledge, or specific setups.
  - **Medium:** Require attention as part of your continuous security posture maintenance.
    - Might cause negative operational impact, such as unplanned outages due to malfunction of security controls.
    - These issues might also provide bad actors with limited access to or control of your assets, or might facilitate parts of their malicious actions.
  - **Low:** Require attention as part of your continuous security posture maintenance.
    - Although they might not cause an immediate security impact on their own, these lapses can be exploited by bad actors.

# MITRE EMB3D Threat Model



# TPM role

- To avoid spoofing
- Unique identification
- Use Physically Unclonable Function (PUF)