Unit-7

IoT Security

Introduction to IoT Security

Overview

- IoT is growing day by day, as we know it's about data and controlling of physical devices.
- Security and privacy are the two major concern in the field of IoT.
- Huge amount of sensed data contains private information so need to protect.
- All kind of securities of physical devices is considered in the IoT security.
- IoT is not possible without the Internet so Internet and network security issues also should be considered in it.

Introduction to IoT Security

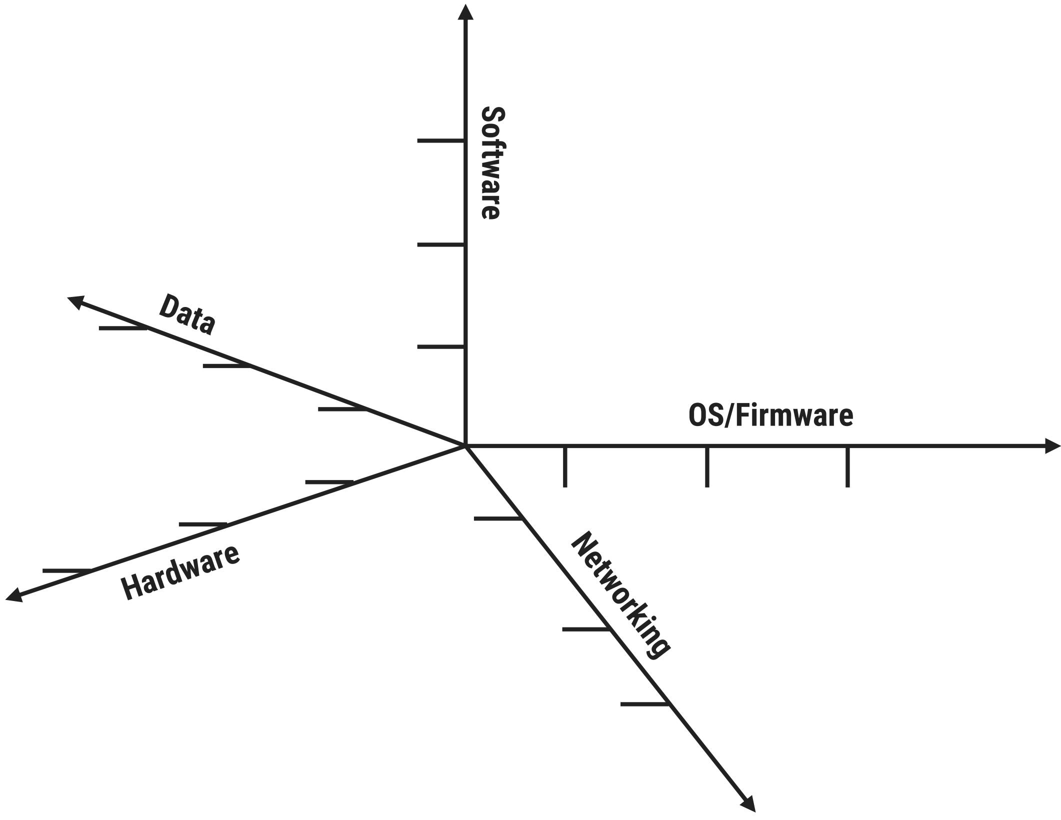
Overview

- IoT security is not traditional cybersecurity
- It's a fusion of cybersecurity with other engineering disciplines.
- It is much more than data, servers, network infrastructure, and information security.
- It includes the direct monitoring and control of the physical systems connected over the Internet.
- IoT devices are physical things, many of which are safety-related.
- The compromise of such devices may lead to physical harm of persons and property, or even death

IoT Security Prospective

IoT System Functionalities from Security Prospective

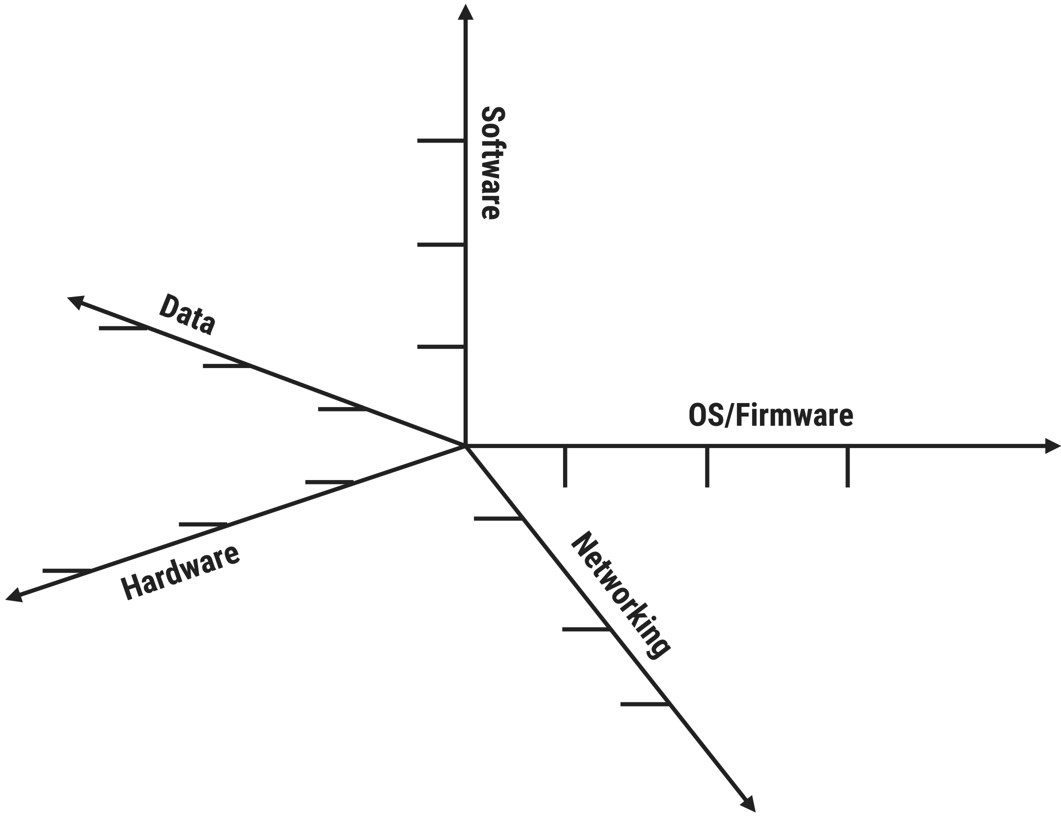
- Microcontroller unit carries firmware, need to protect it even while updating patch.
- Massage channels during the paring stage need to protect in the public networking, like
  - ⤷ Wi-Fi, Zigbee
  - ⤷ Bluetooth
  - ⤷ NFC
- An appropriate protocol should be followed while connecting the user and device.
- An authentication process is needed when the controller linking to a port in local network.



Multidimensional Prospective of IoT Security

IoT System Functionalities from Security Prospective

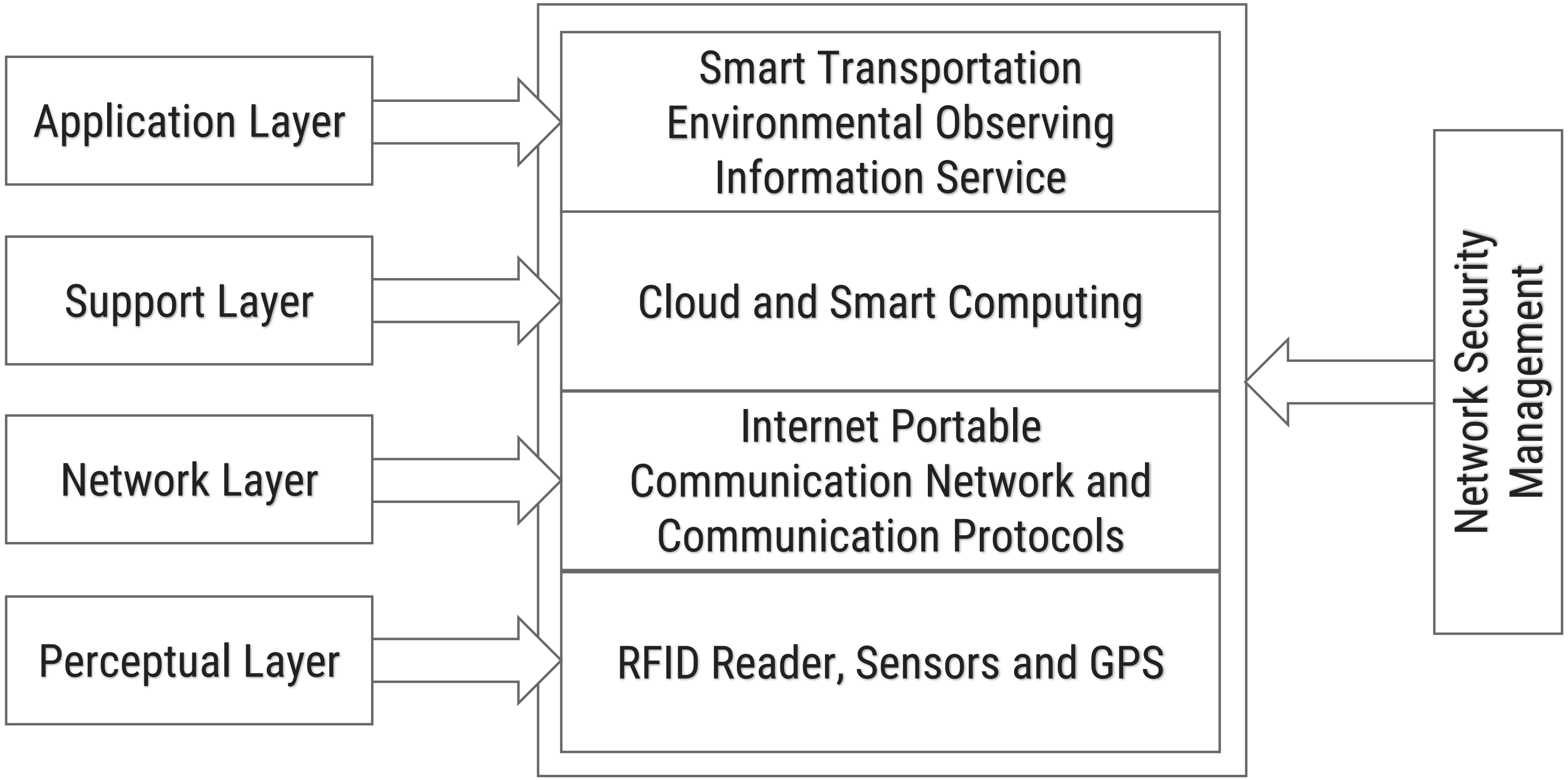
- If the controller is no internet then cloud services are used for authentication. multidimensional
- Big data analytics on the data collected are processed on cloud so cloud security is essential.
- Abnormal behavior should be monitored like too many login attempts



Multidimensional Prospective of IoT Security

IoT Security Architecture

- Information with network security should be prepared with the following properties.
  - Authentication
  - Privacy
  - Undeniability
- IoT will be needed extra care for advanced security and privacy across critical areas.

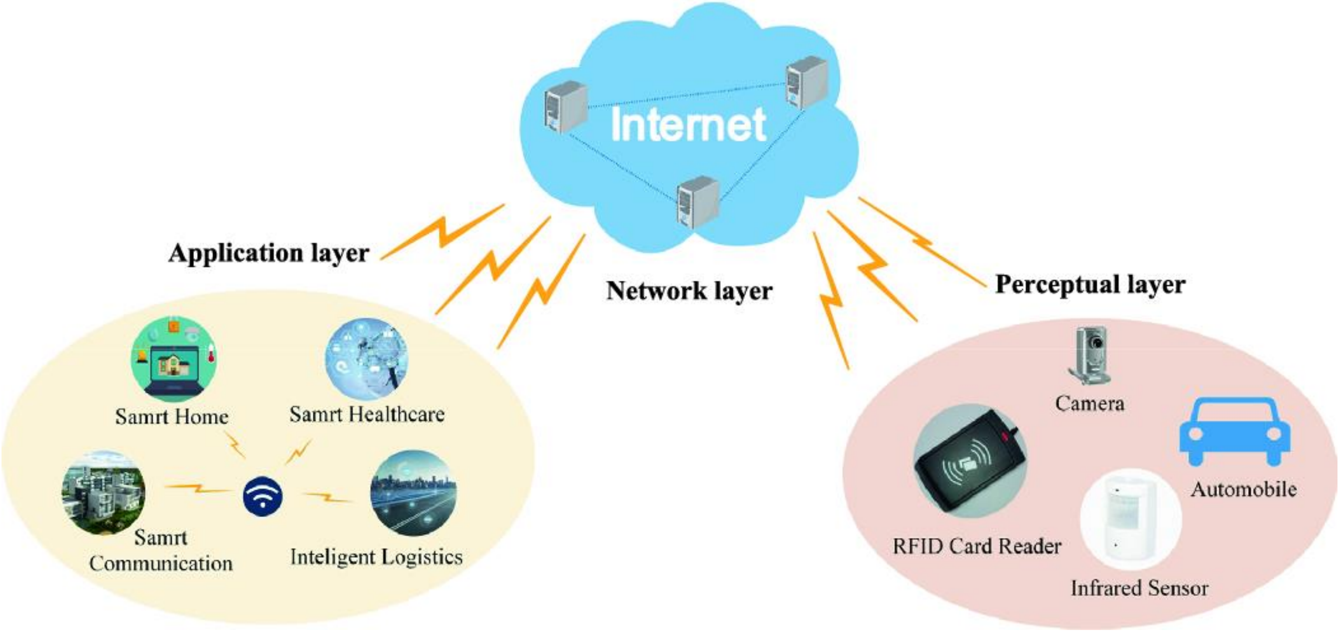


IoT Security Architecture

IoT Security Architecture

Perceptual Layer

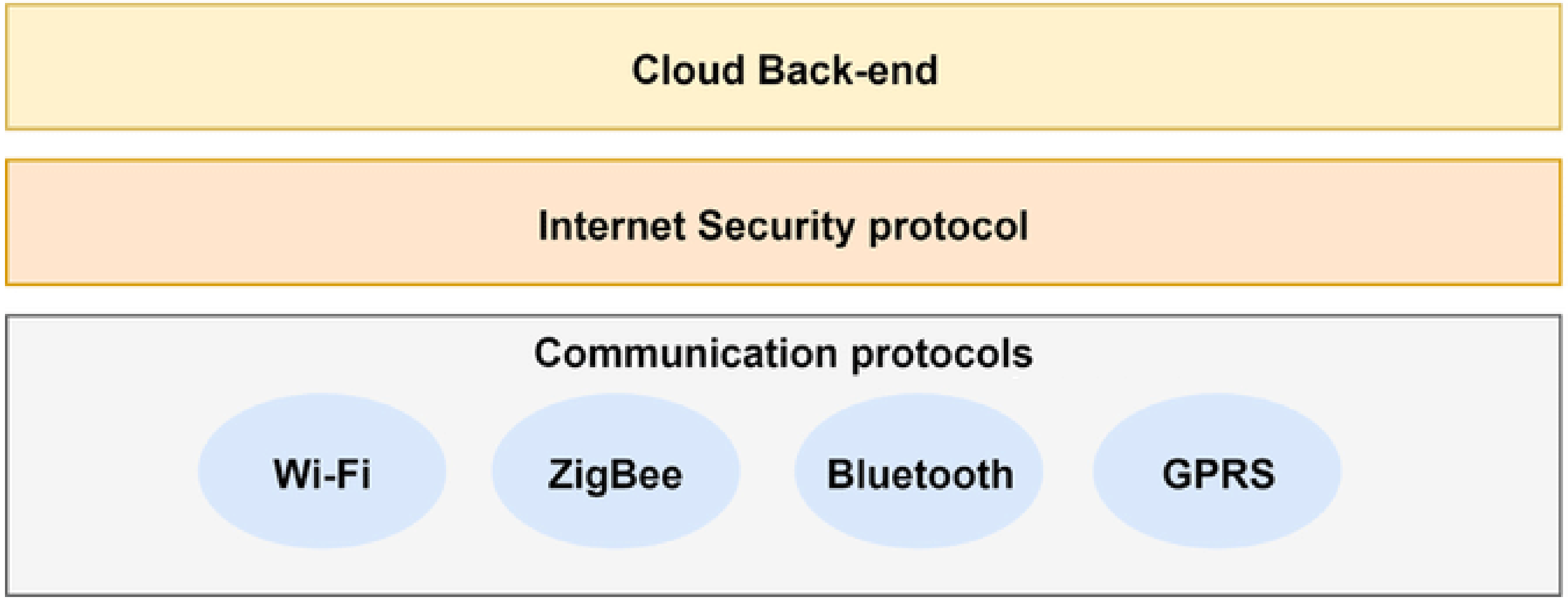
- Gathers all types of information with the help of physical equipment.
- Information of
  - Object properties,
  - Environmental condition and
  - The different physical equipment like
    - RFID reader,
    - GPS,
    - All kind of sensors, etc.
- It identifies the external world.
- The key component in this layer is the sensors.
- They are used for capturing and representing the physical world.



IoT Security Architecture

Network Layer

- Responsible for the dependable broadcast of data and information from the previous level
- Initially handling of the data collected from sensors, cataloging and polymerization.
- The data broadcast is trusted on many networks like
  - Mobile communication network
  - Wireless network
  - Satellite networks, etc.



Cloud Back-end

Internet Security protocol

Communication protocols

Wi-Fi

ZigBee

Bluetooth

GPRS

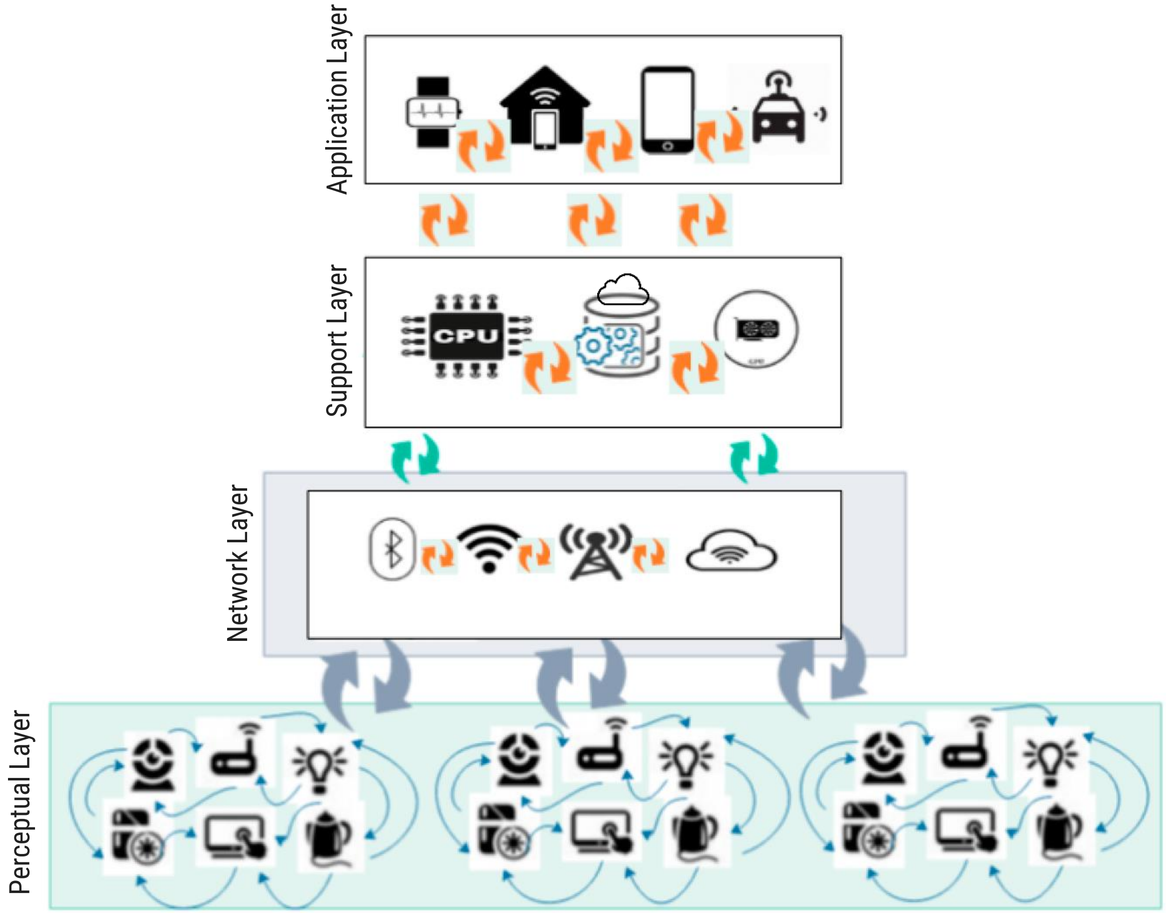
IoT Security Architecture

Support Layer

- A dependable platform for the application layer.
- Grid and cloud computing are mostly used for all kinds of intelligent computing powers.
- This layers helps merge the application layer upward and the network layer downward.

Application Layer

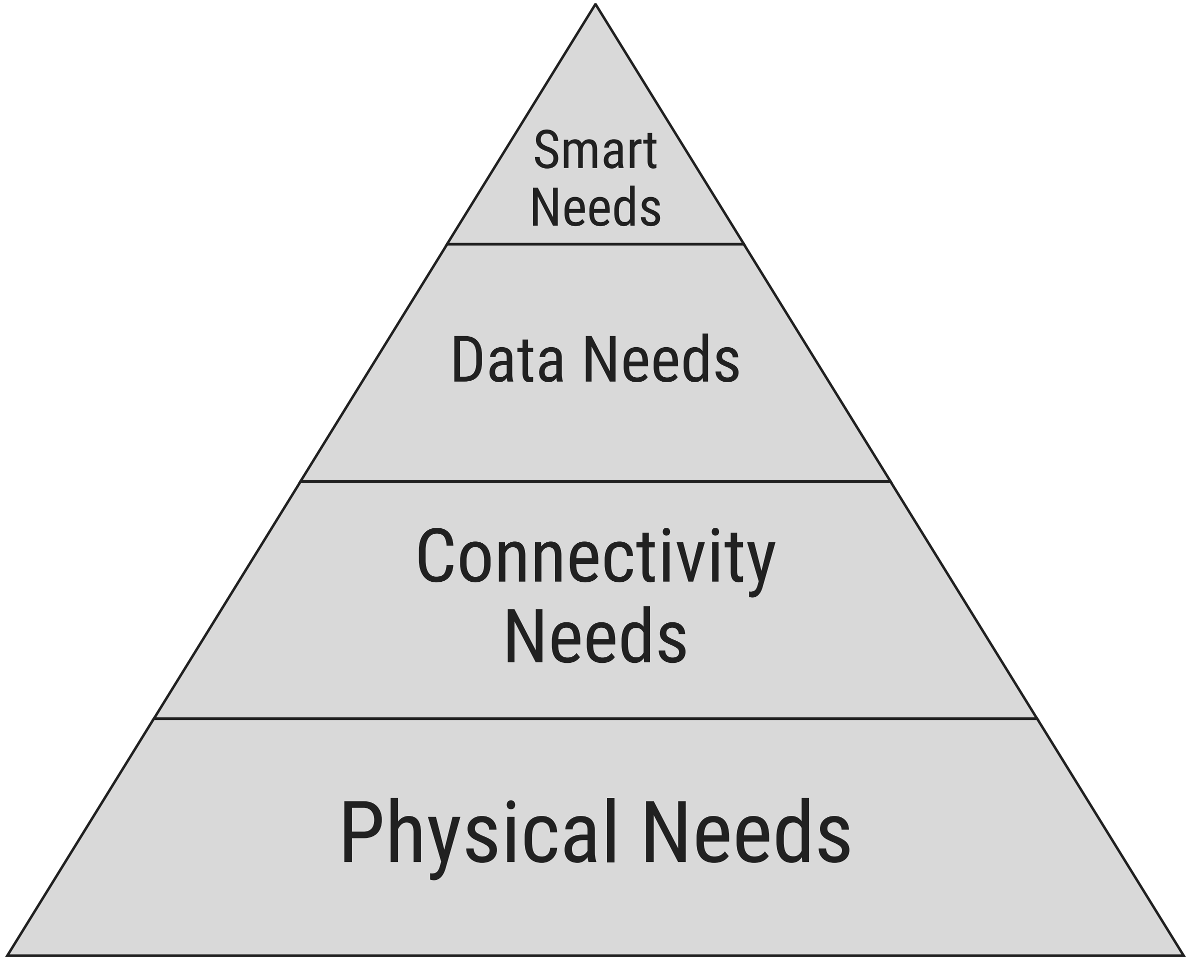
- This layer delivers the personalized services based on the users’ need.
- It helps users access IoT through the interface using personal computer, mobile equipment, etc.



Security Features Need Across Four Layers

Perceptual Layer

- With a simple architecture and less power, this layers dose not have storage and computation power.
- Appling public key encryption algorithm and frequency hoping communication is not possible here.
- So security is necessary and needed for some threats from external network like DoS attacks.
- Due to all the reason the sensor data to be protected for authenticity, integrity, and confidentiality.



Security Needs

Security Features Need Across Four Layers

Network Layer

- Security vulnerabilities are like man-in-the-middle attack, still exists even the main network has enough safety feature.
- Malwares and junk mails cannot be ignored.
- Data blocking may occurs because of huge amount of data transmission.
- Because of all the above reason security methods are needed.

Support Layer

- It is a challenge to increase the ability to identify malicious data in this layer due to the huge amount of data processing and mining.

Application Layer

- In this layer, security needs may differ from application to application
- Data sharing property of the layer does lead to privacy problem, access control issues, and information revelation to unintended persons.

Security Requirements

- A dynamic IoT technology has lots of security challenges.
- The laws and regulations surrounding the challenges also play a significant role.

Perceptual Layer

- Authentication is the first level of security measure and is always essential to prevent any illegal access to the node.
- Information confidentiality is taken care during transmission between nodes
- Because of limited resource, lightweight encryption technology may help in stronger data safety measures. It including cryptographic protocol and algorithms.
- Similarly need care for the authenticity and integrity of the data in this layer

Network Layer

- Establishing data confidentiality and integrity mechanism is the priority in these days.
- Identity verification is one of the methods to avoid illegal nodes.
- DDoS attack in the network is a serious issue in the IoT domain.

Security Requirements

Support Layer

- Cloud computing along with secure multi-party computation falls under this layer of security needs.
- Different encryption algorithms along with the encryption protocol and tougher system security technology are hence essential in this layer.

Application Layer

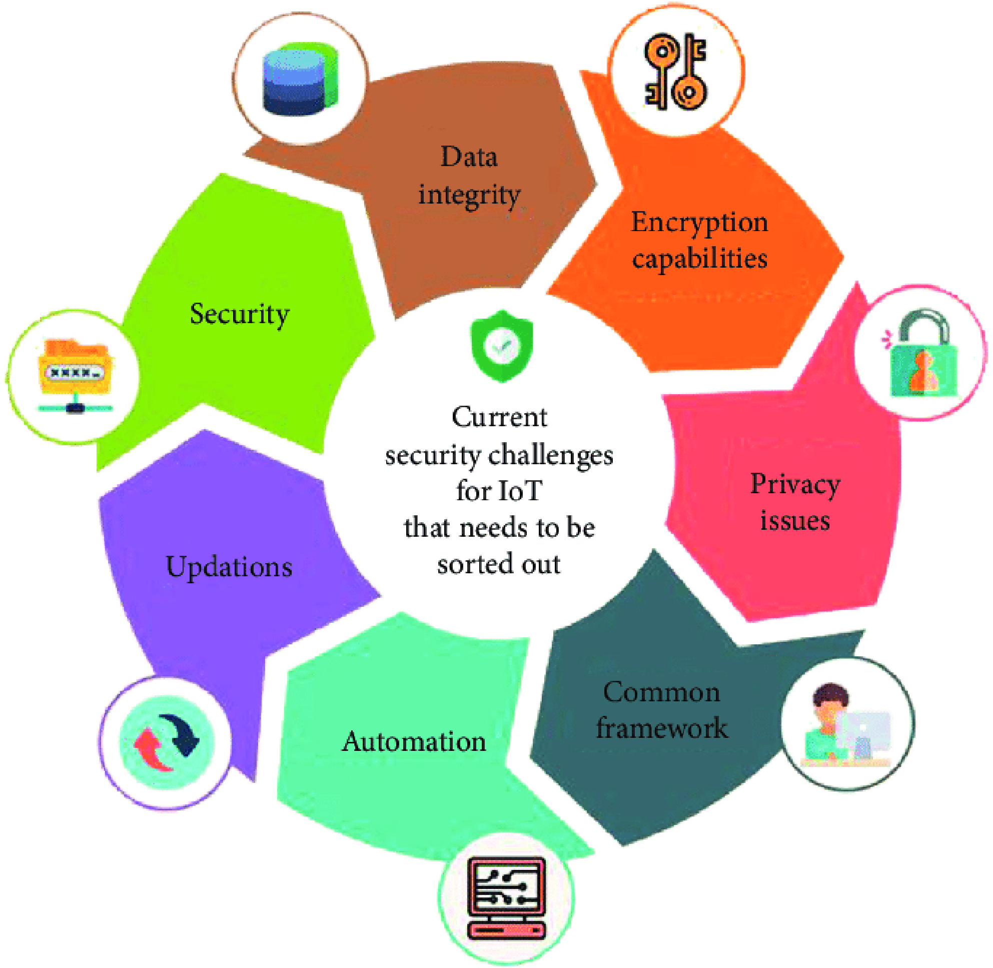
- In the topmost layer, verification and key contract across the varied network needed as security features.
- Also consider the user’s confidentiality protection in the layer.
- Along with these two aspects education and management are also very imperative for data security.
- This helps IoT security consulting and certification services.

Challenges in IoT Securities

- In the raising IoT field many problems to be solved to build an efficient and effective product.
- Securities challenges are one of them.

Encryption

- Encryption play key role in the security, but many devices cannot perform the complex encryption and decryption quickly because of limited resource.
- Products with constrained resources are most likely to attacks.
- Reverse engineering of algorithm is possible on it.



Challenges in IoT Securities

Authorization and Authentication

- Device authorization and authentication is critical to securing IoT products
- The things establish their identity before accessing gateway and other cloud related activities.
- IoT platform with two factor authentication and usage of strong passwords or certificates can help to solve this issue.
- They can also help to know which services or apps each device has access to throughout the system.

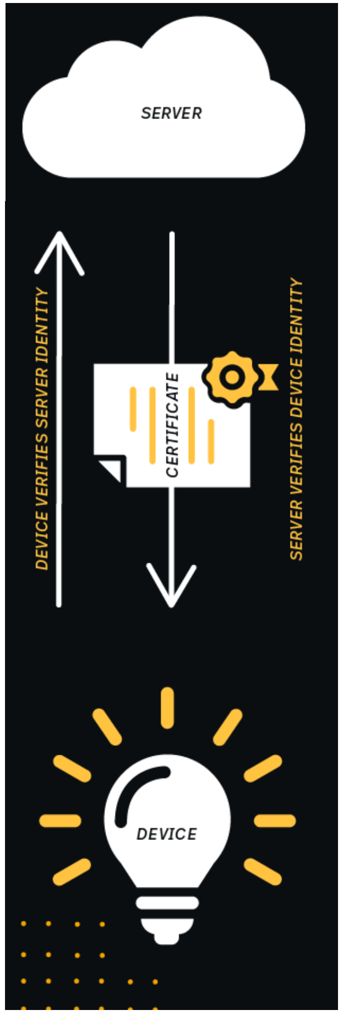
Challenges in IoT Securities

Firmware Updates

- Device updates needs to be managed effectively.
- Security patches to firmware or software will have a number of challenges.
- Over-the-air updates may not be possible with all types of IoT devices.
- The device owners may also not show much interest in applying an update to the system.

Communication Channel

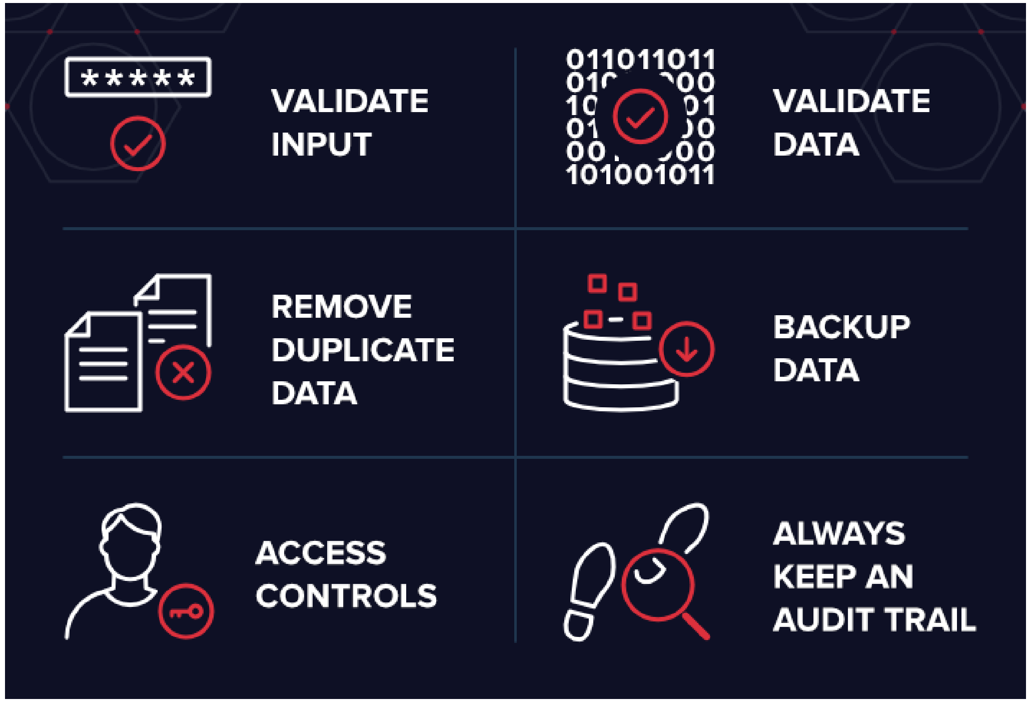
- The communication channel needs to be secure as well
- Encrypting messages before transfer is good but it is better to use transport encryption and to adopt standards like TLS.


SERVER
DEVICE VERIFIES SERVER IDENTITY
CERTIFICATE
SERVER VERIFIES DEVICE IDENTITY
DEVICE

Challenges in IoT Securities

Data Storage and Integrity

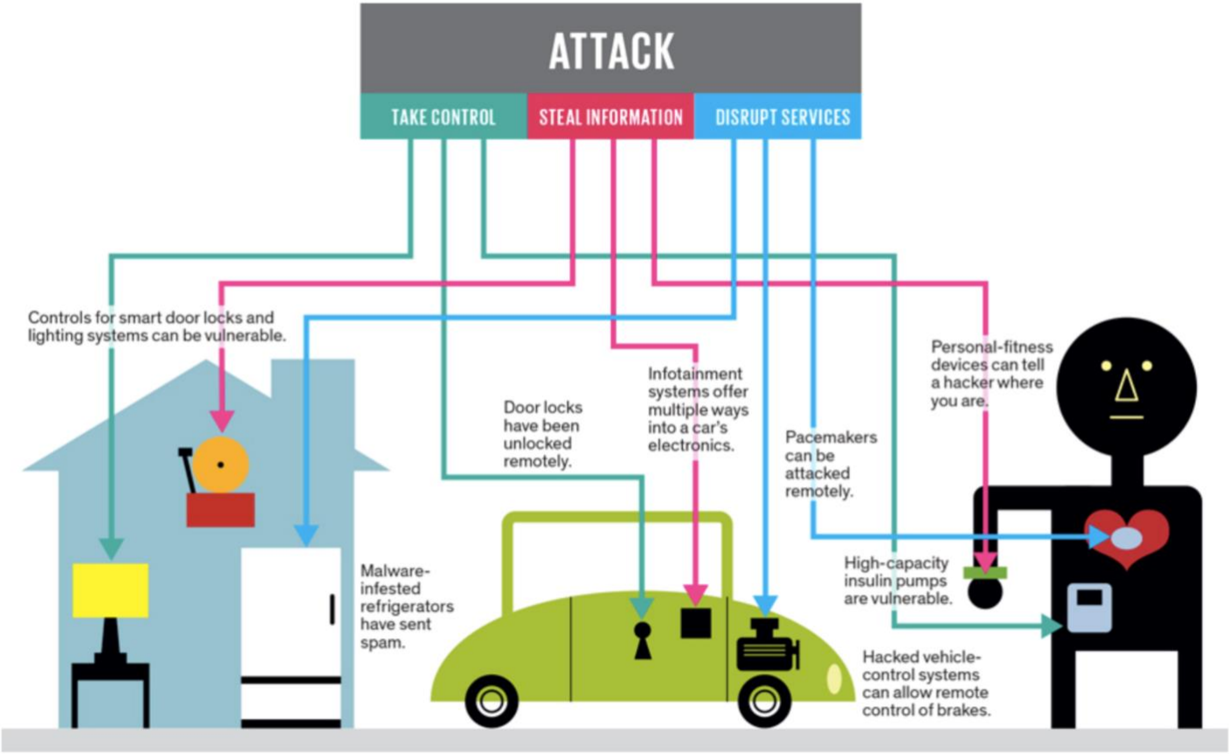
- The sensor data should be stored and processed securely.
- Data integrity, including checksums or signatures, can help to make sure that the original raw data is not modified during transmission.
- Data should be erased in a better way and should not be recovered in any part of the system.
- Maintaining compliance with legal and regulatory framework is necessary and challenging also.



Challenges in IoT Securities

Application and Services

- All applications and services should also be secured as they manage, process, and access IoT devices along with the sensor data.
- Security vulnerabilities and breaches are unavoidable but security measures need to be taken to avoid conflict of interest.



Controls for smart door locks and lighting systems can be vulnerable.

Malware-infested refrigerators have sent spam.

Door locks have been unlocked remotely.

Infotainment systems offer multiple ways into a car's electronics.

Pacemakers can be attacked remotely.

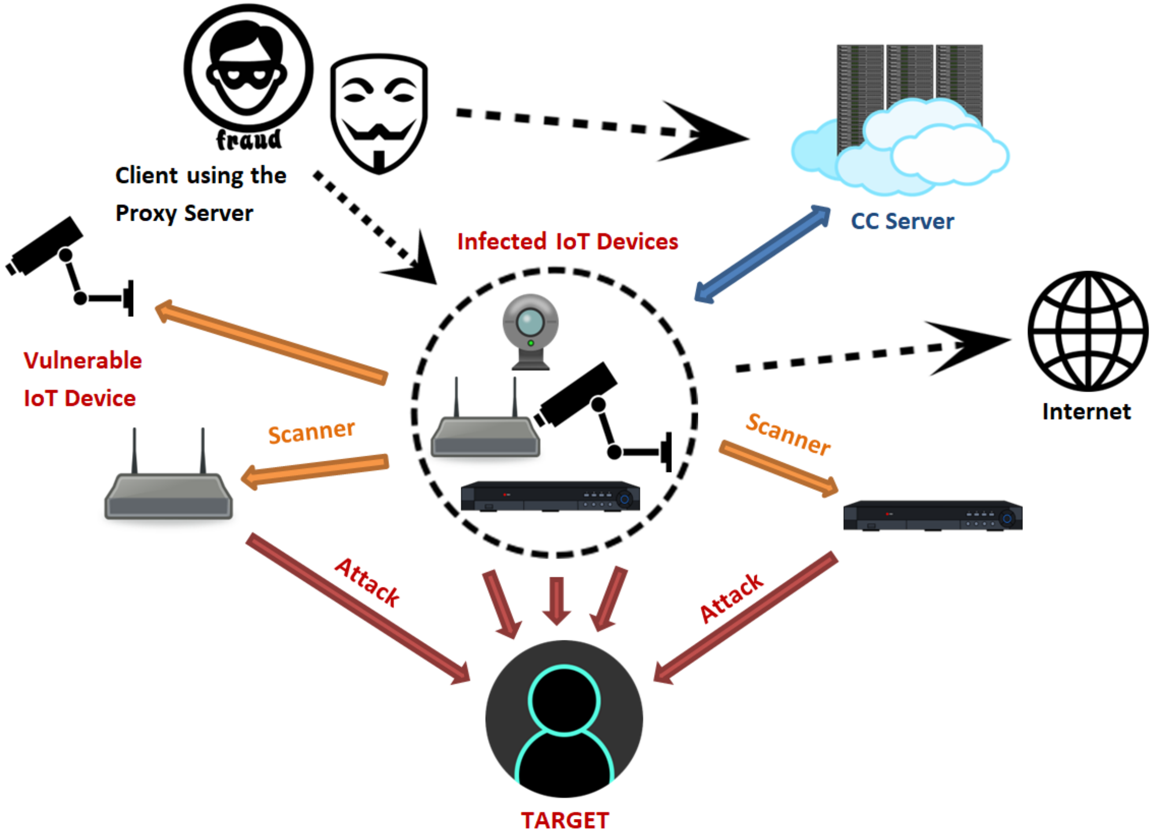
Personal-fitness devices can tell a hacker where you are.

High-capacity insulin pumps are vulnerable.

Hacked vehicle-control systems can allow remote control of brakes.

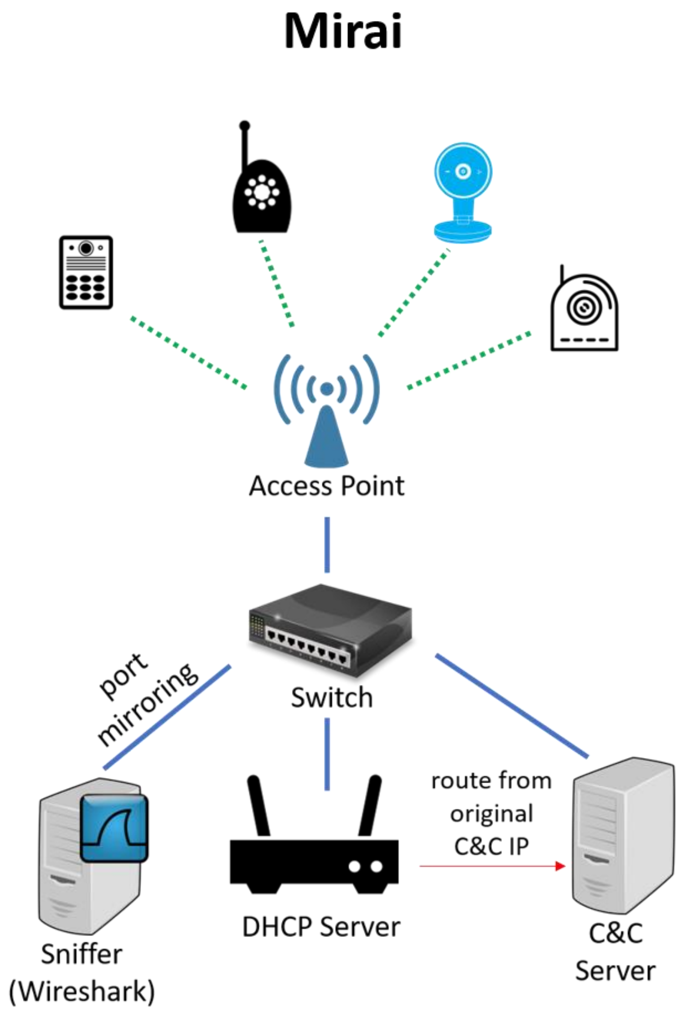
Mirai Botnet and the Algorithm

- Mirai Trojan is the main reason of creation of Mirai Botnet.
- A research group determined that it had evolved from a previously-created Trojan also known Gafgyt, Bashlite, Lizkebab, Bashdoor, Bash()day, and Torlus.
- It was created using Executable and Linkable Format (EFL) binaries which is a common file format for Unix and Linux based Systems
- Mirai malware uses a uniform scanning strategy where it randomly scan public IP addresses and selects a pair of username/password from a hardcoded dictionary list for the attack.



Mirai Botnet and the Algorithm

- Devices that are infected by Mirai will continuously scan for IP address in the internet of the IoT devices.
- Mirai then identifies the IoT devices that are vulnerable using the common factory default usernames and passwords.
- Infect them with Mirai malware.
- There are over a hundred of thousands IoT devices using default settings and making them vulnerable to infection.
- It is also reported that a successor of Mirai is designed to hijack crypto currency mining operations.
- The source code for the Mirai is made open-source and the techniques have been adapted in other malware projects.



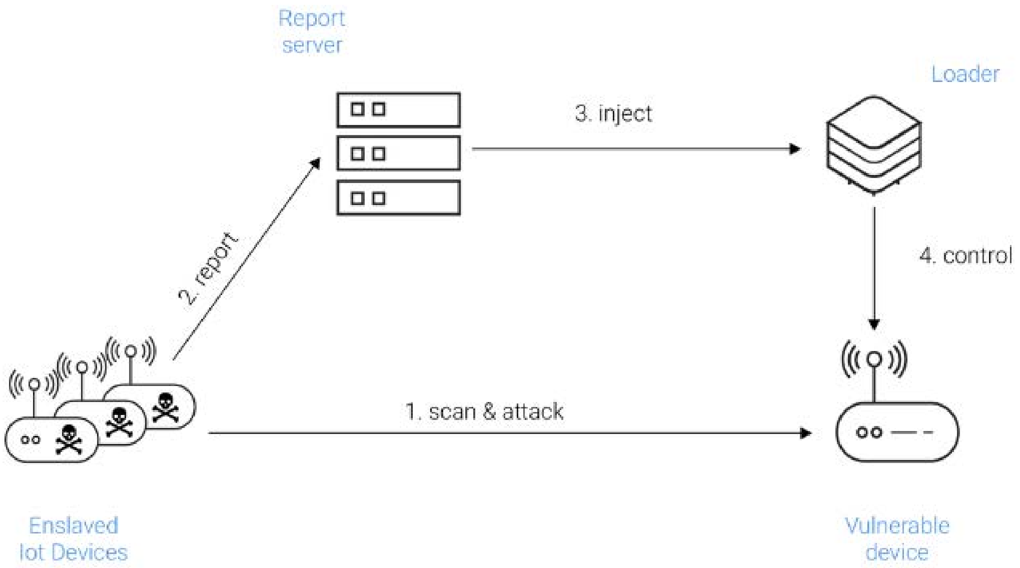
Summary

- A multi layered security design approach is most needed for managing IoT devices, sensor data, mobile and cloud related application
- This enables us to maintain data privacy and integrity while also delivering IoT data, apps and services without any compromises.
- In short, IoT development and advancement will bring more security related issues, which is always going to be the research focus in coming years.

How Mirai works

At its core, Mirai is a self-propagating worm, that is, it's a malicious program that replicates itself by finding, attacking and infecting vulnerable IoT devices. It is also considered a botnet because the infected devices are controlled via a central set of command and control (C&C) servers. These servers tell the infected devices which sites to attack next. Overall, Mirai is made of two key components: a replication module and an attack module.

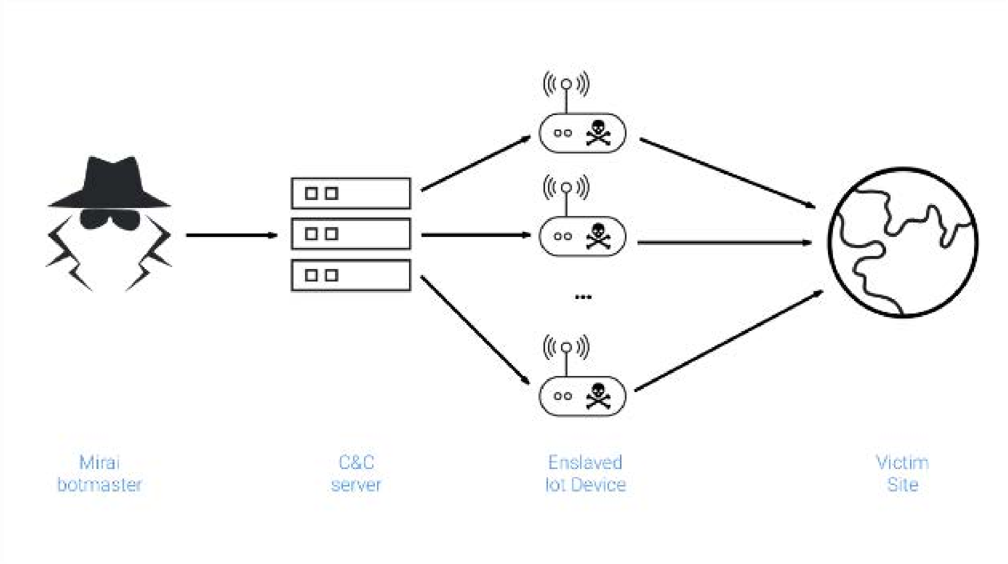
Replication module



The replication module is responsible for growing the botnet size by enslaving as many vulnerable IoT devices as possible. It accomplishes this by (randomly) scanning the entire Internet for viable targets and attacking. Once it compromises a vulnerable device, the module reports it to the C&C servers so it can be infected with the latest Mirai payload, as the diagram above illustrates.

To compromise devices, the initial version of Mirai relied exclusively on a fixed set of 64 well-known default login/password combinations commonly used by IoT devices. While this attack was very low tech, it proved extremely effective and led to the compromise of over 600,000 devices. For more information about DDoS techniques, read this Cloudflare primer.

Attack module



The attack module is responsible for carrying out DDoS attacks against the targets specified by the C&C servers. This module implements most of the code DDoS techniques such as HTTP flooding, UDP flooding, and all TCP flooding options. This wide range of methods allowed Mirai to perform volumetric attacks, application-layer attacks, and TCP state-exhaustion attacks.

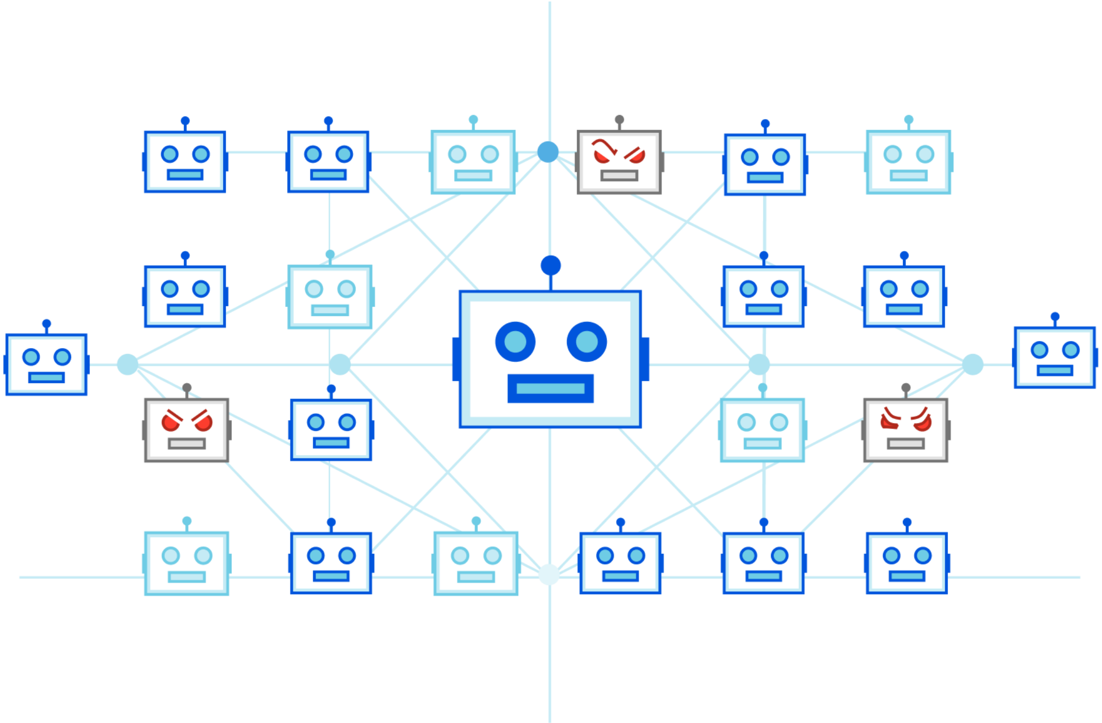
What is the Mirai Botnet?

cloudflare.com/learning/ddos/glossary/mirai-botnet

The Mirai malware exploits security holes in IoT devices, and has the potential to harness the collective power of millions of IoT devices into botnets, and launch attacks.

What is Mirai?

Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots or "zombies". This network of bots, called a botnet, is often used to launch DDoS attacks.



Malware, short for malicious software, is an umbrella term that includes computer worms, viruses, Trojan horses, rootkits and spyware.

In September 2016, the authors of the Mirai malware launched a DDoS attack on the website of a well-known security expert. A week later they released the source code into the world, possibly in an attempt to hide the origins of that attack. This code was quickly replicated by other cybercriminals, and is believed to be behind the massive attack that brought down the domain registration services provider, Dyn, in October 2016.

How does Mirai work?

Mirai scans the Internet for IoT devices that run on the ARC processor. This processor runs a stripped-down version of the Linux operating system. If the default username-and-password combo is not changed, Mirai is able to log into the device and infect it.

IoT, short for Internet of Things, is just a fancy term for smart devices that can connect to the Internet. These devices can be baby monitors, vehicles, network routers, agricultural devices, medical devices, environmental monitoring devices, home appliances, DVRs, CC cameras, headset, or smoke detectors.

The Mirai botnet employed a hundred thousand hijacked IoT devices to bring down Dyn.

Who were the creators of the Mirai botnet?

Twenty-one-year-old Paras Jha and twenty-year-old Josiah White co-founded Protraf Solutions, a company offering mitigation services for DDoS attacks. Theirs was a classic case of racketeering: Their business offered DDoS mitigation services to the very organizations their malware attacked.

Why does the Mirai malware remain dangerous?

The Mirai is mutating.

Though its original creators have been caught, their source code lives on. It has given birth to variants such as the Okiru, the Satori, the Masuta and the PureMasuta. The PureMasuta, for example, is able to weaponize the HNAP bug in D-Link devices. The OMG strain, on the other hand, transforms IoT devices into proxies that allow cybercriminals to remain anonymous.

There is also the recently discovered - and powerful - botnet, variously nicknamed IoTrooper and Reaper, which is able to compromise IoT devices at a much faster rate than Mirai. The Reaper is able to target a larger number of device makers, and has far greater control over its bots.

What are the various botnet models?

Centralized botnets

If you think of a botnet as a theatrical play, the C&C (Command and Control Server, also known as the C2) server is its director. The actors in this play are the various bots that have been compromised by malware infection, and made part of the botnet.

When the malware infects a device, the bot send out timed signals to inform the C&C that it now exists. This connection session is kept open till the C&C is ready to command the bot to do its bidding, which can include sending out spam, password cracking, DDoS attacks, etc.

In a centralized botnet, the C&C is able to convey commands directly to the bots. However, the C&C is also a single point of failure: If taken down, the botnet becomes ineffective.

Tiered C&Cs

Botnet control may be organized in multiple tiers, with multiple C&Cs. Groups of dedicated servers may be designated for a specific purpose, for example, to organize the bots into subgroups, to deliver designated content, and so on. This makes the botnet harder to take down.

Decentralized botnets

Peer-to-peer (P2P) botnets are the next generation of botnets. Rather than communicate with a centralized server, P2P bots act as both a command server, and a client which receives commands. This avoids the single point of failure problem inherent to centralized botnets. Because P2P botnets operate without a C&C, they are harder to shut down. Trojan.Peacomm and Stormnet are examples of malware behind P2P botnets.

How does malware turn IoT devices into bots or zombies?

In general, email phishing is a demonstrably effective way of infecting the computer - the victim is tricked into either clicking a link that points to a malicious website, or downloading infected attachment. Many times the malicious code is written in such a way that common antivirus software is not able to detect it.

In the case of Mirai, the user doesn’t need to do much beyond leaving the default username and password on a newly installed device unchanged.

What is the connection between Mirai and click fraud?

Pay-per-click (PPC), also known as cost-per-click (CPC), is a form of online advertising in which a company pays a website to host their advertisement. Payment depends on how many of that site’s visitors clicked on that ad.

When CPC data is fraudulently manipulated, it is known as click fraud. This can be done by having people manually click on the ad, by use of automated software, or with bots. Through this process, fraudulent profits can be generated for the website at the expense of the company placing those ads.

The original authors of Mirai were convicted for leasing their botnet out for DDoS attacks and click fraud.

Why are botnets dangerous?

Botnets have the potential to impact virtually every aspect of a person's life, whether or not they use IoT devices, or even the Internet. Botnets can:

- Attack ISPs, sometimes resulting in denial-of-service to legitimate traffic
- Send spam email
- Launch DDoS attacks and bring down websites and APIs
- Perform click fraud
- Solve weak CAPTCHA challenges on websites in order to imitate human behavior during logins
- Steal credit card information
- Hold companies to ransom with threats of DDoS attacks

Why is botnet proliferation so hard to contain?

There are many reasons why it is so difficult to stop the proliferation of botnets:

IoT device owners

There is no cost or interruption in service, so there is no incentive to secure the smart device.

Infected systems may be cleaned out with a reboot, but since scanning for potential bots happens at a constant rate, it's possible for them to be reinfected within minutes of the reboot. This means users have to change the default password immediately after reboot. Or they must prevent the device from accessing the Internet until they can reset the firmware, and change the password offline. Most device owners have neither the know-how, nor the motivation to do so.

ISPs

The increased traffic on their network from the infected device typically does not compare to the traffic that media streaming generates, so there is not much incentive to care.

Device manufacturers

There is little incentive for device manufacturers to invest in the security of low-cost devices. Holding them liable for attacks might be one way of forcing change, though this might not work in regions with lax enforcement.

Ignoring device security comes at great peril: Mirai, for example, is able to disable anti-virus software, which makes detection a challenge.

Magnitude

With over a billion-and-a-half ARC-processor-based devices flooding the market each year, the sheer number of devices that can be conscripted into powerful botnets means that these malware variants have grown in possible impact.

Simplicity

Ready-to-go botnet kits obviate the need for tech savvy. For $14.99-$19.99, a botnet may be leased for an entire month. Refer to What is a DDoS Booter/Stresser? for more details.

Global IoT Security Standards

There is no global entity, or consensus, to define and enforce IoT security standards.

While security patches are available for some devices, users might not have the skill, or the incentive, to update. Many manufacturers of low-end devices don’t offer any kind of maintenance at all. For ones that do, it is often not long term. There is also no way to decommission devices once the updates are no longer maintained, making them indefinitely unsecure.

Global Law Enforcement

The difficulty in tracking down and prosecuting botnet creators makes the containment of botnet proliferation difficult; There is no global Interpol-equivalent (International Criminal Police Organization) for cybercrime, with corresponding investigative skills. Law enforcement across the globe is commonly not been able to keep up with cybercriminals when it comes to latest technology.

Many botnets now employ a DNS technique called Fast Flux in order to hide the domains they use to download malware, or to host phishing sites. This makes them extremely hard to track, and take down.

Does botnet infection degrade performance for IoT devices?

It might. Every once in a while, infected devices might perform sluggishly, but they mostly work as intended. Owners have no great motivation to find ways to clear out the infection.