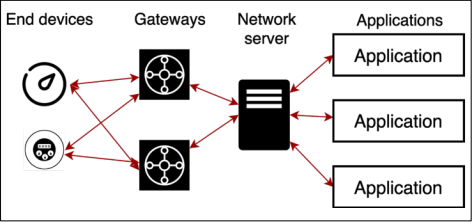
**Research on the Lora Network**

**Introduction:**

The long rang wide area networking (LoRaWAN) is one of the popular wireless, low-power WAN protocol that is used for IoT environment to design smart cities, smart home and industrial IoT, etc where millions of IoT devices are connected to communicate with interconnected applications over long rang (LoRa) wireless connections. LoRaWAN has built-in=encryption to making it secure by default, but implementation issues and the weaknesses can make it hackable as the cyber security vulnerabilities in LoRaWAN network are not well known which makes LoRaWAN deployments to be targeted by hackers.

**Architecture:**

**There four key elements that shape a LoRaWAN implementation:**



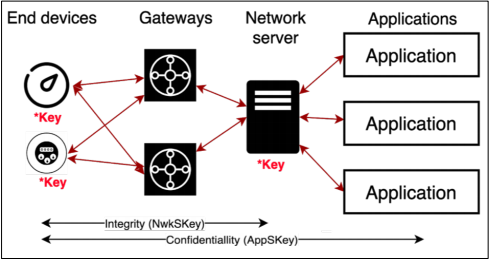
1. **Technology**

* **End devices:** such as sensors that communicate with gateway using LoRa protocol
* **Gateway:** The gateway is a device that act as a bridge between nodes/end devices and IP stack, in the LoRa network gateway exchange messages between end devices and network server.
* **Network Server:** is a software to manage and optimize the network and provide authentication and authorization of the devices to send data between end devices to the application.
* **Application server:** handles all application between users and backend devices, it’s the destination for device application data sent as a payload in LoRaWAN message.

In the LoRa network the devices exchange messages through the gateway by using LoRa physical layer (Wireless) and LoRaWAN and gateway exchange messages with the network server using different protocols such as TCP/IP or UDP/IP based on the implementation, so the traffic from devices to the server called uplink and the opposite way from the server to the devices called downlink.

1. **Security in LoRaWAN:** LoRaWAN consists of two security layer, **Network-level** security that ensures the authenticity of Nodes/devices to provide integrity between devices and network server and **Application-layer** security which ensures the confidentiality using end-to-end encryption between the devices and application server to prevent access to transmitted data by third parties. LoRaWAN uses device, network and application keys to transmit data securely at the network and application layers which are known the Network Session Key (NwkSKey) and Application Session Key (AppSKey) and both are 128 bits long.

**Fig: Session keys and functions in LoRaWAN**



1. **Vulnerabilities**

* **Compromising Device and Network Keys:** LoRaWAN provides end-to-end security using application and network keys.common issues and weaknesses in the LoRaWAN implementation are the Keys and their management, if an attacker have physical access to the end device and extract the keys which makes LoRaWAN network vulnerable because the keys are source of security mechanism encryption in the LoRaWAN network.
* **Reverse Engineering Devices:** The possibility of sniffing or spoofing the communication between the LoRa radio module and the microcontroller unit (MCU) that is over SPI (Serial Peripheral Interface) or UART (Universal Asynchronous Receiver/Transmitter) by extracting the keys from devices by attackers. Also, the attacker can copy the firmware of the device if flash security is not enabling or obtain the firmware online from the vendor.
* **Device Tags:** It's a tag that displays a QR code or text with the device’s DevEUI (64 bits number), AppKey (application Key), etc which need to be used in the commissioning prosses. These tags need to be removed before using the devices, otherwise if an attacker with physical access can use this information and generate a valid session key.
* **Network servers with default or weak password:** default credentials such as admin/admin or weak password can be easily guessed by a hacker, or the attacker can use Shodan for a quick search for LoRaWAN well-known server web headers to obtain default credential to login and stole the keys from the servers.
* **File Disclosure:** usually, device manufacturers share the keys with their clients through email, flash storage or online which can be obtained by third parties who can access these keys.
* **Service Provider Breach:** The LoRaWAN infrastructure that been offered by providers to route the message between devices and application which includes the gateway and servers that manages the LoRaWAN network whereas these servers needed AppKeys to join the network and these keys are stored in backups, databases, etc. if data breach happens through the service provider’s cloud by attackers, they can obtain all the keys used by clients.
* **Servers with security vulnerabilities:** network servers with poor security and miss configuration where hackers can access or exploit a software vulnerability to have access to the LoRaWAN network management and devices’ AppKey.
* **Compromised device manufacturers:** installing the firmware and setting the keys by the manufacturers on their devices can be an issue where if the hackers get access to the manufacturer’s system, they can easily compromise the keys on many devices which can be used on LoRaWAN network globally.
* **Offline key cracking:** attackers can perform a dictionary or brute-force attacks in order to crack the AppKey. this allows attackers to control, spoof or perform a denial of service attack to many devices or to whole LoRaWAN network where in many implementations the same keys are used for group of devices.
* **Cyber-attacks scenario on smart home**: LoRaWAN is used in home automation with the application such as smart looks, alarm and security system, smart lights, smart fridge, smart cooker, smoke detectors, smart windows and so on, if the attackers hack a smart home’s LoRaWAN network successfully, they would be able to control every thins within the network by disabling the alarm system and unlock doors and monitor a house remotely.

1. **Security Recommendation:**

* **Key Protection:** devices keys need to be protected to prevent attacks by hackers, if a key is compromised the whole LoRaWAN network can be hacked, to prevent this from happening:

1. We need to replace the default keys which provided by vendors with random keys.
2. On each different device using different key.
3. Audit the root keys used to detect the weak keys.
4. We need to be sure that service providers have a secure infrastructure and following the best security practice.

It is important that each device within the LoRaWAN network have their own unique AppKey that is not shared with other devices. Regular auditing to detect the weak keys where as the LoRaWAN network can be grow and new devices with a weak key can be added to the network.

* **Prevent. Detect and Monitor:** to prevent attacks from happening we need completely secure the LoRaWAN network ecosystem by securing all the individual components and technologies within this environment such as devices, gateway, application and network servers, applications and etc, this is the possibility of identifying and troubleshooting the problems which can be done regularly. The LoRaWAN network is subject to constant cyber-attack and can be hacked, it is important to monitor LoRaWAN network regularly in order to detect and react on time to any attacks by using third party software to monitor and analyse the network to prevent or stop the attack.