# Securing the smart and connected home

Author: Tang Yiming, Eric Seow, Sarah Woo

**Abstract:**

Smart devices including mobile terminals, wearables and all kinds of sensors, smart nodes and platforms with connectivity and critical information processing capabilities are fast growing into billions of pieces. These billions of smart devices have at least one external connectivity interface which potentially becomes the entry point for attackers to bring down the entire system. Smart home is one such example of a connected system with intelligence. To prevent attacks, a robust, market proven and certifiable hardware security solution becomes a key ingredient of such systems that communicate and process critical or sensitive information. In this article, we will look into the various security threats in connected smart home devices and discuss the necessary security measures that should be utilized, in particular leveraging on the values of hardware trust anchors. We will also present specific use cases on Smart home environment as a good reference for the audience to gain a better understanding.

## Introduction:

With the fast growth of IoT applications, our home network environment has been changed dramatically in recent years. A typical home network setup 5 years ago consists of a wireless/wired router with ADSL/cable connection to the internet, and the devices are connected to the router are mainly desktop computers, laptops and smartphones. These devices have one commonality, which is that they are operated by human beings, and they are not powered up 24/7 in many cases except the smartphone.

Today, the home network setup is undergoing a complete revolution. A typical home network environment can be described as in below diagram:
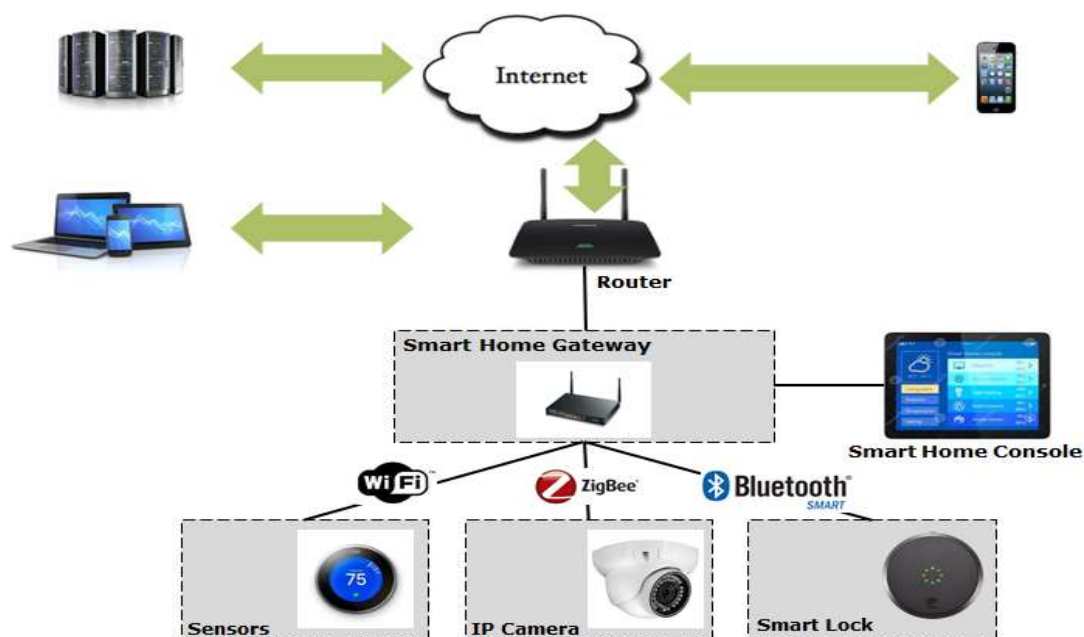


There are few important new characteristics of a smart home network environment

First, there are more devices in the home today (beyond computers and phones) that are becoming smarter and connected. For instance, smart sensors like thermostats need to be connected to the internet for data logging and remote control. IP cameras need to be connected to internet for real time monitoring. Even door locks have evolved to include connectivity options to allow remote monitoring and to allow opening of the door remotely.

The dramatic increase of smart devices in the network increases the potential entry point of attacks from a security point of view. And all these smart devices have very minimal direct

human operations. They all have built-in intelligence to collect data and information, make decisions based on the programmed algorithms and in many cases they need to have data communication capability with either the home gateway or the cloud server. End users mainly control or monitor these devices via external consoles or smart phones. Therefore in case of an occurrence of a security breach, end users have very minimum way to detect, prevent the issue and make corrective actions because these devices operate on their own.

Secondly, wireless connectivity solutions are not only limited to Wi-Fi in today's smart home environment. Connectivity solutions, such as Bluetooth, ZigBee and Z-Wave have evolved and are adopted quickly. With the increase of the connected devices via different wireless connectivity solutions, the attack surfaces of smart home devices have greatly increased and the number of attacks has been rising steadily. Additional protection at system level is thus strongly needed.

Last but not least, most of these smart devices run on various microcontrollers with proprietary Real-Time Operating System (RTOS). The security level of such implementations can vary from vendor to vendor. Also, very often there is a need for field firmware upgrade for these devices which opens up another highly potential attacking entry point because malware can be injected during firmware upgrade without sufficient protection mechanisms in place. The recent distributed denial of service (DDoS) attack from connected devices in US (source:http://www.pcworld.com/article/3134056/hacking/an-iot-botnet-is-partly-behind-fridays-massive-ddos-attack.html) and Germany (source: http://www.pcworld.com/article/3145449/security/upgraded-mirai-botnet-disrupts-deutsche-telekom-by-infecting-routers.html) are very good examples of the importance of firmware protection in connected home devices.

For the manufacturers of these devices it is essential to understand the threats and protection mechanisms that are present and available today.


**Major security threats in smart home**

We can broadly categorize security threats for smart home applications into 4 main categories. These security threats are identified and discussed as follows:


Fake Identity of Devices:

Most of the smart home devices possess some form of device identifiers as a unique ID or certificate. However, unique identifier without cryptographic protection can be easily cloned as soon as the attackers gain the knowledge of the generation process.  Once the unique identifier can be cloned without authorization, the attacker is able to gain immediate access to the network via the cloned device, and from there subsequent attacks can be deployed. E.g. critical

information can be stolen, bandwidth of the network can be misused, or malware and virus can be injected. On the other hand, validation of the server identity is equally important. If a home device is connected to a malicious server, critical user data can be stolen or in a very worst case, entire home network can be attacked.

Eavesdropping of Data:

Most of the communication interfaces used in smart home environment are based on wireless technologies, e.g. Bluetooth, ZigBee, Wi-Fi etc. Although most of the wireless technologies have some form of security protection mechanisms, they are not robust enough due to the constraints of the use cases. For instance, Bluetooth typically relies on simple passphrase to do pairing. It increases the risk of eavesdropping of the critical and sensitive user data over the communication interfaces.  It is also common to employ encryption of the communication data using cryptographic keys to protect the confidentiality and integrity, however, the protection of the cryptographic keys against stealing and extraction are then of great importance.

As an illustration of a real life attack, three years ago, experts from Context Security demonstrated the security weaknesses of certain smart-bulbs. These LED bulbs were connected to a Wi-Fi___33 enabled circuit board and the experts found that when the bulbs "talked" to each other across a mesh network (6LoWPAN powered), the messages contained a username and password. As the underlying pre-shared key was never changed, all the white-hat guys had to do to gain access was to set up a similar circuit board simulating one of the smart bulbs asking to join the network. That allowed them to steal credentials and eventually gain control of all the lights on the network. They reported that a potential attacker could have easily gained access in private homes or businesses if they could have gotten as close as 30 meters to the bulbs. Even worse they note also that such a attack would have gone undetected by the owner of the network. (source: https://techxplore.com/news/2014-07-experts-reveal-weakness-wifi-lifx.html)

Manipulation of Data:

Besides the risk of eavesdropping, there is possibility of critical data being manipulated/changed by malicious attacks, therefore data integrity protection is another important aspect of security in Smart home environments. Critical information like billing information, sensitive configuration data or resource usage cannot be communicated and stored as manipulated value.

Malware Infection:

One typical attack after gaining access to the network is to install malware so that the affected device becomes the source of next level attack. The recent cases happened in some of the major telecommunication networks are typical examples of such attacks. Once the connected home devices are breached with malware installed, such devices could be added to a botnet and start issuing DDoS attack. As a result many smart home devices - not only computers - become potential source of DDoS attacks. The amount of such smart home devices (e.g. smart cameras, home routers etc.) is much more than the amount of computers connected to the net, therefore the scale and speed of damage due to botnet DDoS attack can be also much more significant.

## Basic Security Cornerstones

The above mentioned security threats in the smart home environment can be addressed by 3 basic security aspects: "Confidentiality" by encrypting the sensitive data; "Integrity" by protecting data with cryptographic Message Authentication Code function or digital signature; "Authenticity" by using strong cryptographic authentication schemes.

At the center of these 3 security cornerstones are the cryptographic keys which are used for the encryption/decryption, calculation of the CMACs and supporting the strong cryptographic authentication schemes.  If an attacker manages to steal or clone these cryptographic keys, then these security cornerstones ("Confidentiality", "Integrity" and "Authenticity") can no longer be enforced since the attacker is now able to successfully eavesdrop and/or modify the communication data and fake itself as the real device.

Therefore, it is of paramount importance to protect these cryptographic keys by using a tamper-resistant hardware trust anchors.

## Hardware based trust anchors for Smart Home Security

Secured identities are established using secret keys and cryptographic processes that utilize secret keys. Secret keys are fundamental root of trust for the entire chain of security measures required to protect smart home systems. Hardware-based security solutions provide the robust levels of security required to protect secured identities and deliver a greater level of trust than pure software based implementation.

Software-only solutions often have common weaknesses such as software bugs or malware attack. Typically, it is also relatively simple to read and overwrite software, which, in turn, makes it easy for attackers to extract secret keys. In contrast, hardware based security solutions can

be used to store access data and keys on the same level as a safe is used to store confidential documents.

| | Main CPU | Software | Main CPU | Software | Hardware |
|---|---|---|---|---|---|
| Crypto functionality | | ✓ | | ✓ | |
| Strong isolation | | ▬ | | | ✓ |
| Security-certified | | ▬ | | | ✓ |
| Tamper-resistant | | ▬ | | | ✓ |
| Manufactured using security-certified processes | | ▬ | | | ✓ |
| Resistant to IP theft | | ▬ | | | ✓ |

There is no one-size-fits all solution when it comes to cyber-security and very often the effective approach is to adopt a defense-in-depth approach where the security countermeasures are built into various layers such as devices, software and application, processes and user education.

On the device and hardware level, the best-of-both-worlds can be achieved by adopting tamper-resistant hardware trust anchors to complement the software security implementations. The hardware trust anchors can be used to provide a secured storage of cryptographic keys and provide a strong level of trust to support the software implementations. By achieving the spatial separation of the software applications and cryptographic keys, this provides a cost-efficient and highly effective barrier against the leakage of the keys and certificates in the event of malware infections.

Based on the earlier discussion on the security threats to a Smart Home – Fake device, Eavesdropping, Manipulation and Malware attacks, the hardware trust anchor should then address the 4 use cases – Authentication, Secured Communication, Secured Data Store and integrity and Secured Firmware update respectively.

In this section, we will share how Infineon's OPTIGA Family of products will adequately address these use cases.

Use case 1: authentication

Authentication is the process of identifying users, computers, devices and machines in networks and restricting access to authorized persons and non-manipulated devices. Hardware-based security can support authentication by providing secured storage for a device's credentials (cryptographic keys or passwords). Infineon has developed a broad portfolio of OPTIGA™ products that build a root of trust in hardware devices to allow the secured authentication of devices and systems

Use case 2: secured communication

In typical embedded system architectures, devices and systems are connected across heterogeneous networks employing various standard and proprietary protocols. To protect communication against eavesdropping and message falsification, for instance, it must be secured between these systems. Infineon's OPTIGA™ family enables secured communications by storing the keys and certificates used in communication protocols as well as supporting cryptographic operations.

Use case 3: Stored data encryption and integrity protection

Embedded devices often store sensitive user data. The integrity and confidentiality of this data can be protected by encrypting or signing it. The challenge lies in securely storing cryptographic keys. Data can be easily decrypted if an attacker manages to read out the keys. Infineon's OPTIGA™ Trust and OPTIGA™ TPM families overcome this problem by encrypting data and storing cryptographic keys securely. The OPTIGA™ Trust and TPM family products also support software and hardware integrity checks

Use case 4: secured firmware update

Software and firmware in embedded systems often need regular updates. However, it can be challenging to protect both the software itself as well as the system that is being updated. Updates protected by software only are at risk as software can be read, analyzed and modified to compromise the update or system. However, software can become trustworthy by combining it with secured hardware. Secured hardware from Infineon's OPTIGA™ family protects the processing and storage of code by means of encryption, fault and manipulation detection, and secured code and data storage.

**Conclusion**

With the advent of the Internet of Things and Smart Home technology, more and more devices are becoming connected.  Attacks are made possible as these smart devices are able to run source codes for applications and that they are mostly connected to the internet without any secured connection. These can potentially become entry points for malicious hackers to break into the system to steal, manipulate confidential information (e.g. passwords) or even to inject malware.

In most of these cases, the users are unaware of the vulnerabilities and potential security exposure (e.g. ref the DDOS attack) of the products they purchase. Hence it is imperative that device makers include security measures from the design of their products.

In  this paper, we have highlighted 4 main attack scenarios namely  Fake device, Eavesdropping, Manipulation and Malware attacks and how through the use of a hardware trust anchor, we can better address the 4 use cases – Authentication, Secured Communication, Secured Data Store and integrity and Secured Firmware update respectively.

In addition to other security measures in the operating system or software, a hardware trust anchor provides the secured basis for the system. By relying on such a specialized device, the manufacturers of embedded devices can reduce their efforts for creating a secured basis while still getting a strongly secured s