Securing the smart and connected home

Tang Yiming, Eric Seow, Sarah Woo

www.infineon.com/Smart-Home-Security

Contents

1. The smart and connected home 3

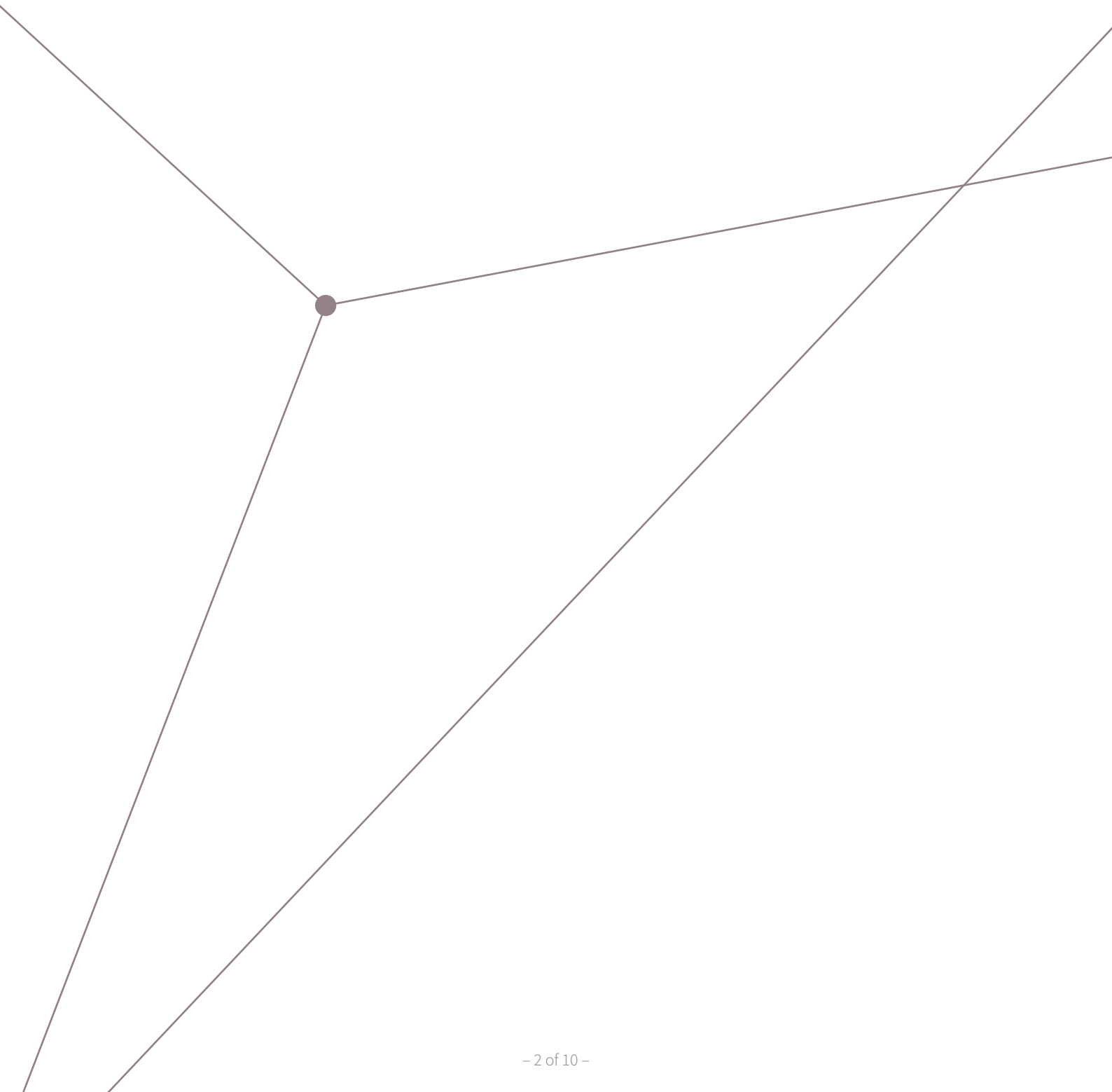
2. Major Security Threats in Smart Home 5

3. Basic Security Cornerstones 6

4. Hardware based trust anchors for Smart Home Security 7

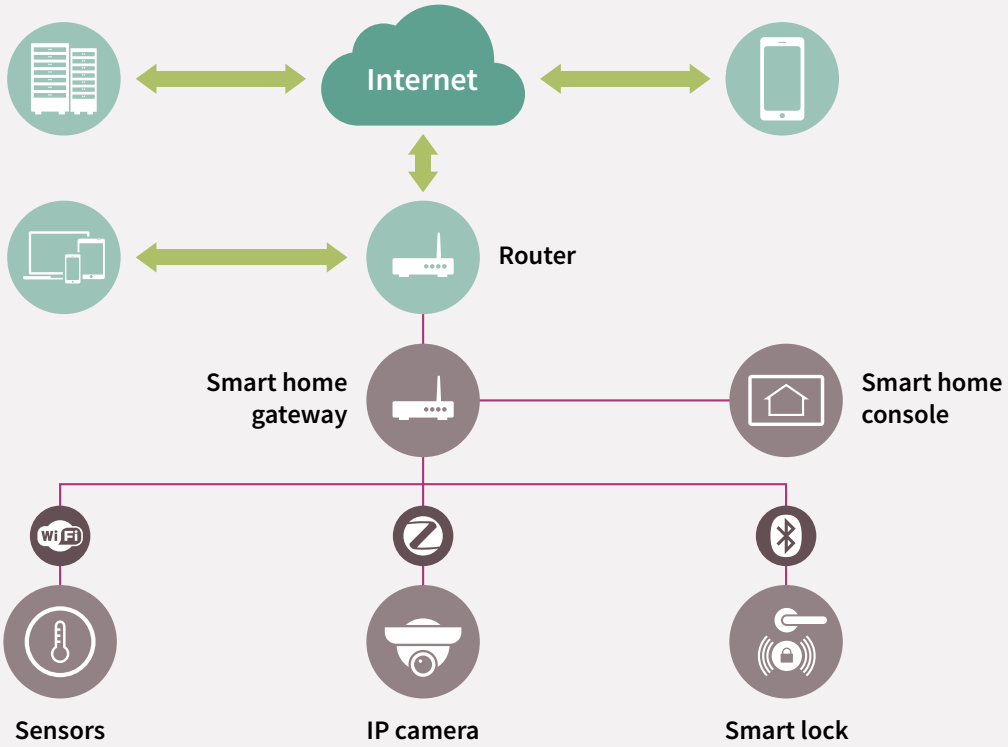
5. How hardware trust anchors address the most important use cases 8

6. Conclusion 10



1. The smart and connected home

With the fast growth of IoT applications, our home environment has been changed dramatically in recent years. Today, a typical home network environment consists of a router/ gateway with many home appliances being connected to the internet using various wireless communication protocols such as WIFI, BLE, ZigBee etc. Such a home network can be illustrated as in below diagram:



For instance, smart sensors like thermostats need to be connected to the internet for data logging and remote control. Voice assistants such as smart speakers are sending voice commands to the cloud and 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. In addition, home appliances such as Air-cons, washing machines, rice cookers and refrigerators are offering remote access possibilities to bring about greater conveniences to home owners.

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 interactions. 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.

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[1] and Germany[2] 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.

[1] source:www.pcworld.com/article/3134056/hacking/an-iot-botnet-is-partly-behind-fridays-massive-ddos-attack.html
[2] source: www.pcworld.com/article/3145449/security/upgraded-mirai-botnet-disrupts-deutsche-telekom-by-infecting-routers.html

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.[3]

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.

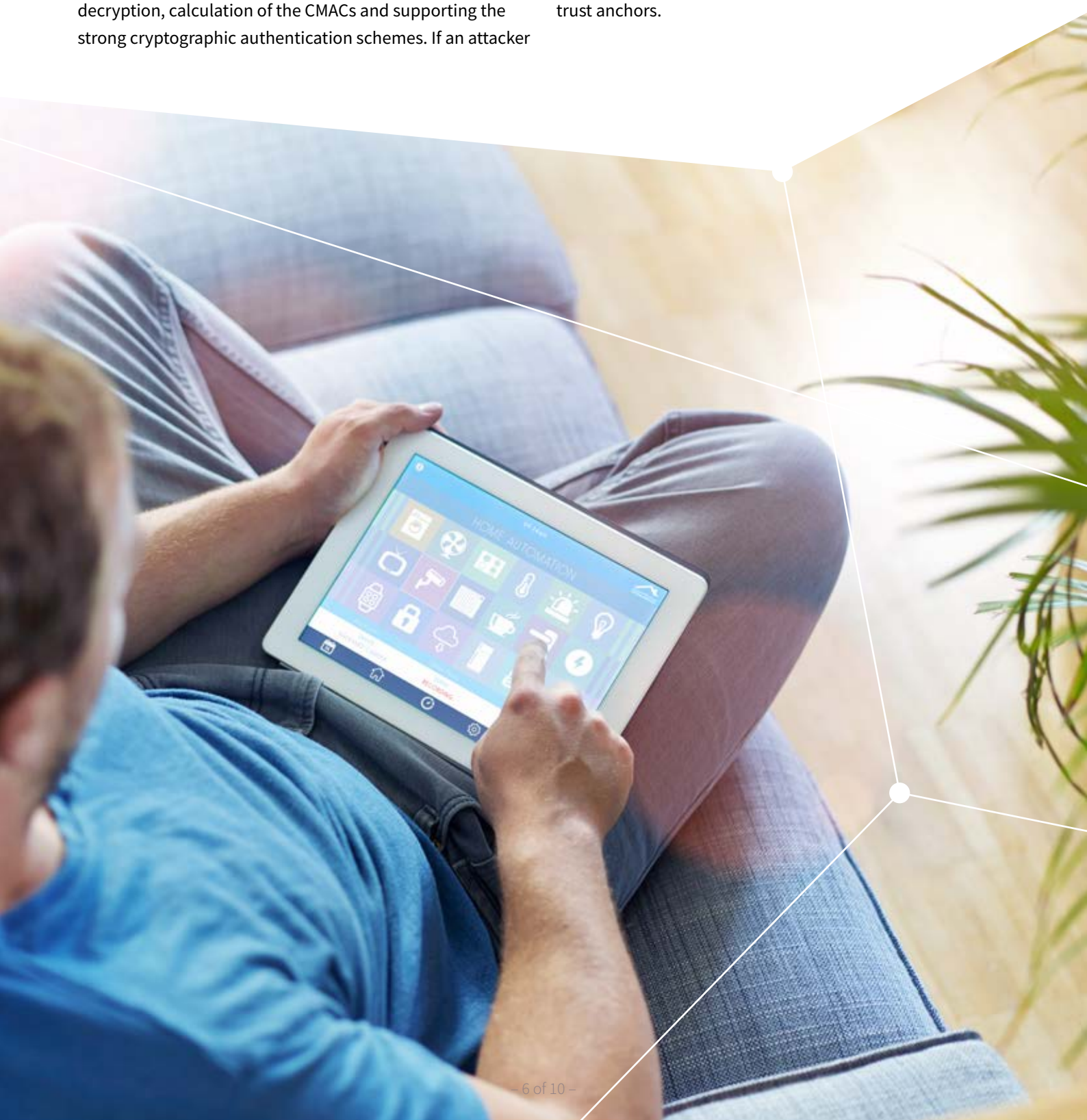
[3] source: techxplore.com/news/2014-07-experts-reveal-weakness-wifi-lifx.html

3. Basic Security Cornerstones

The 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.



4. 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		
Restitant to IP theft		

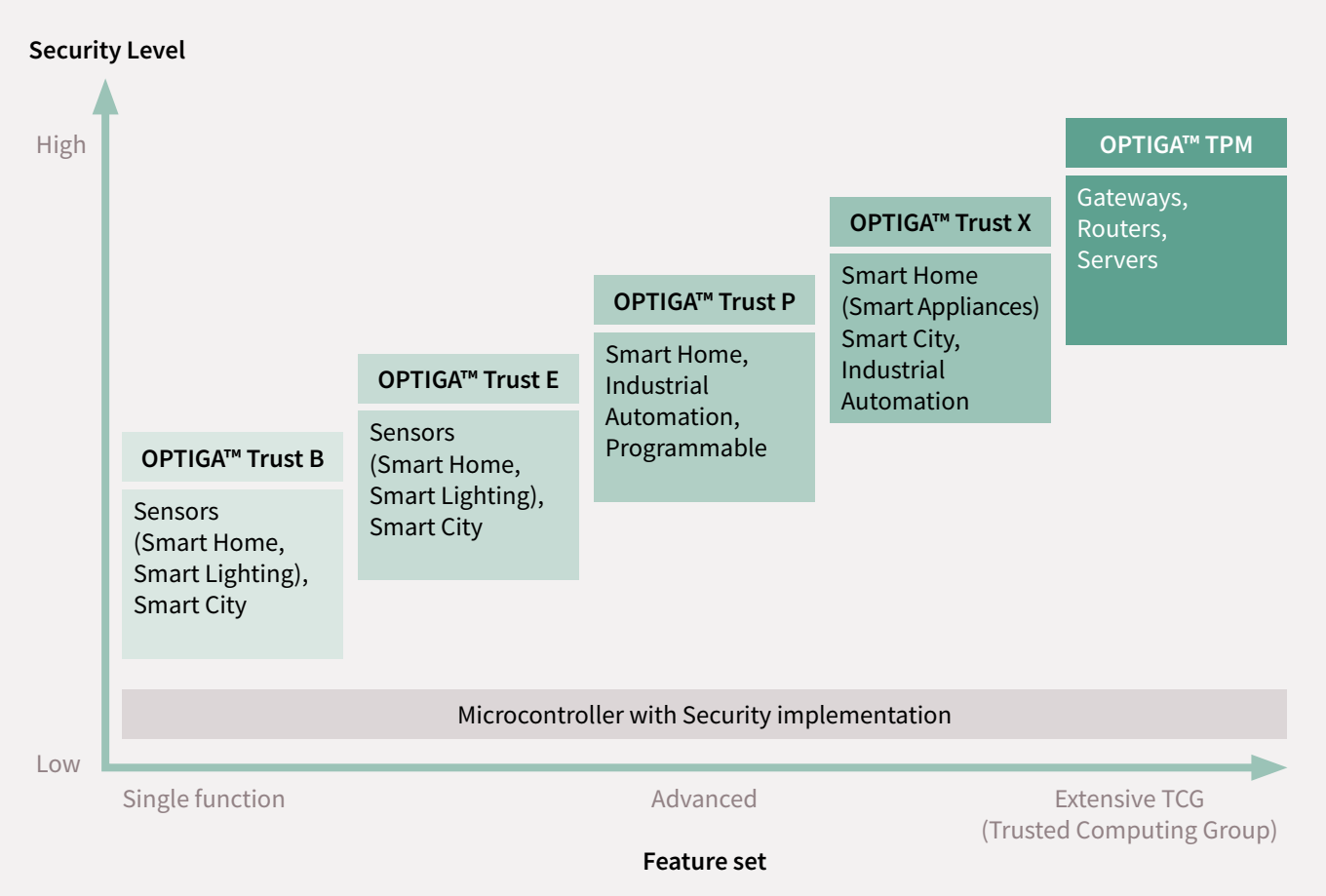
There is no one-size-fits all solution when it comes to cyber-security and very often the effective approach is to adopt a defense-in-depth approach where the security countermeasures are built into various layers such as devices, software and application, processes and user education.

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.

5. How hardware trust anchors address the most important use cases

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. For example, OPTIGA™ Trust B and E can be used to implement one-way authentication for branding and accessories protection, whilst the Trust X and TPM can be used for Mutual Authentication).

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. For example, it is important to secure the communication between the voice assistants and the cloud to protect the user's privacy and the protection of these keys for establishing the secure communication is crucial. Infineon's OPTIGA™ family (e.g. OPTIGA™ Trust X and TPM) enables secured communications by protecting 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 to detect any manipulations to the firmware or infection by malware.

Use Case 4: Secured Firmware Update
Software and firmware in embedded systems often need regular updates to roll out new features or to patch existing security vulnerabilities. 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. This can be overcome by combining it with secured hardware as the keys for verification and decryption of the firmware can be secured by using the Infineon's OPTIGA™ Trust X or TPM In addition, further security policies pertaining to secure firmware update, such as prevention of firmware version rollback, can be enforced securely using the OPTIGA™ Trust X and TPM.

6. 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 system.

Where to buy

Infineon distribution partners and sales offices:
www.infineon.com/WhereToBuy

Service hotline

Infineon offers its toll-free 0800/4001 service hotline as one central number, available 24/7 in English, Mandarin and German.

- Germany ..... 0800 951 951 951 (German/English)
- China, mainland ..... 4001 200 951 (Mandarin/English)
- India ..... 000 800 4402 951 (English)
- USA ..... 1-866 951 9519 (English/German)
- Other countries ..... 00* 800 951 951 951 (English/German)
- Direct access ..... +49 89 234-0 (interconnection fee, German/English)

* Please note: Some countries may require you to dial a code other than "00" to access this international number. Please visit www.infineon.com/service for your country!

Mobile product catalog

Mobile app for iOS and Android.

www.infineon.com

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 08 / 2018