Securing the Smart Home

1) How will the advent of 5G impact security in the Smart Home?

The advent of 5G is likely to lead to much wider use of IoT devices in the Smart Home. Analysts like Gartner predict that there will be over 20 billion connected devices by 2020, although obviously not all of these will be in the home – industrial IoT is set to boom too.

If these devices and the network are inadequately secured, that will open the owner of the Smart Home up to a much wider range of security threats including data and identity theft. However, if security is built into 5G technical standards from the outset, then device manufacturers will have to build in security too to make their products function on 5G. In that scenario the Smart Home may potentially be more secure than it is today given that currently many IoT devices are rushed to market with an emphasis on low pricing rather than adequate security.

2) Is there too much focus on mass market appeal in the Smart Home or is there still a place for high-end products?

SIMalliance does not comment on suitable price points for types of IoT product but we would like to emphasise that there is a danger that suppliers may fail to invest in security for low cost devices, in order to keep bill of materials costs low. This is a mistake. Simple devices do not necessarily require simple security. In fact, simple devices are often at higher risk of attack.

The security requirements of an IoT device do not correlate with its cost and complexity but instead with the value of the data being stored/transferred, the threats and risk it faces. Therefore, it is important to understand that low cost devices should not mean low cost security. Across the entire Massive IoT sector, a level of security proportional to the data being stored/transferred is required. Trying to save money on security today may incur hidden costs tomorrow.

3) What types of security threat does the Smart Home create?

The Smart Home can create two types of security threat. The first is to the consumer. Inadequate security could for example see the consumer have their data stolen or otherwise tampered with. Their credentials could be accessed, leading to identity theft. A denial of service attack could see them lose access to their service.

The second and potentially more serious is to the network. Inadequately protected IoT devices allow attackers an entry point to the network. In this case, while the consumer data or device is in itself of little interest to the attacker, it provides them with the opportunity to cause damage on a much wider scale.

This is why it's so important that even low cost, simple IoT devices must be adequately secured.

4) How can security and privacy concerns (in the Smart Home) be overcome?

The key to meeting security and privacy concerns in Massive IoT, be it in the home or in industrial uses, is to ensure that security is in proportion to the value of the data being stored or transferred, and the threats and risk it faces.

A compelling security concept for IoT must also provide a solid proposition for the end-to end security. That means not just focusing on device security but considering security at all points of the chain – the consumer themselves, the device, the application, the service and the network.

Security must also consider lifetime value. In some areas of IoT, devices have a very long lifespan, so both the device and its security must be designed for a lifetime of at least 15 years.

5) What is the technology key to protecting the Smart Home?

SIMalliance believes that a hardware based approach in Massive IoT provides a proven secure platform, offering the best protection from physical tampering and subscription/identity cloning. The tamper-resistant hardware element industry can bring a great deal to use cases within the IoT space that require robust security mechanisms, including its neutrality, the trust it has created in different ecosystems, as well as the security, interoperability and diversity of the hardware element.

However, there is no one size fits all approach and multiple layers of security solutions and approaches will be needed, based on a thorough assessment of risk and a clear understanding of the value of the data being stored or transferred.

For more information about SIMalliance and its activities in IoT, please visit the SIMalliance website.