The secure foundation for IoT

By Sherry Zameer

11 Sep 2018

The low-cost, low-power nature of the IoT can cause security considerations to be deferred until much later in the product implementation stage, or sometimes, indefinitely. However to realise IoT's true potential, it is critical that security be considered at the very early stages, and even take pole position in some applications.

Sherry Zameer is vice president of IoT at Gemalto

Luckily, there are some simple frameworks that we can follow to improve the security mindset and build a secure foundation for the IoT system from the start.

First, be paranoid

Due to the sheer number of moving parts in an IoT system, there are numerous vectors that hackers can use to attack. A healthy dose of paranoia during the examination of the entire IoT system can ensure that the system is thoroughly explored and that appropriate security controls are selected. However, IoT security, like any other system, should be driven by business risk. Thus, things like privacy laws, compliance, and business value should all balance the paranoia with pragmatism.

Most IoT devices are valued in terms of the nature of their function, e.g. temperature, telemetry, video stream. Since the data is often used upstream for higher-order decision making, there is an implicit value that affects the outcome of the system at large. For example, temperature from IoT devices might drive the fire suppression systems, or facial recognition from video feeds may alert physical security services.

Consequently, the takeover of the IoT device could be used to conduct data integrity attacks that change the behavior of the upstream system(s).

For instance, information regarding the energy consumption from your home or business to your utility provider could be altered, in order to manipulate billing, services and status. All threats of this nature jeopardize the trust in the information being transmitted and ultimately in the overall infrastructure.

Cryptojacking - a silent threat

11 Sep 2018

Attacks against device manufacturers, cloud service providers, and IoT solution providers have the potential to inflict the widest degree of harm. These parties will be entrusted with large amounts of data, some of it highly sensitive in nature. This data also has value to the IoT providers because of the analytics it enables, which represents a core, strategic business asset - and a significant competitive vulnerability if exposed.

Second, use a persona-based approach

IoT systems are made up of many vendors, each one focusing on their core strength, whether it's manufacturing, connectivity, data warehousing, analytics or some other function. Thus, security in the IoT system can only be achieved through collaboration of all the vendors, but remains the responsibility of the system provider.

An effective way to design and review security needs of the system is by borrowing the persona-based approach used in product development. This involves identifying every distinct persona involved in an IoT system, including the buyer, the device manufacturer, the cloud provider, developers and other vendors, and then analysing all interactions between these parties and installing relevant security controls.

These controls should be driven by a defense-in-depth strategy, whilst minimising friction, especially for human personas. Any friction imposed by security controls motivates humans to find ways to circumvent them (all in the name of productivity and efficiency), so this process can help ensure that security controls are applied that maximize both security and empathy for the user.

Each persona should be assigned an appropriate level of authentication for their digital identities, for example certificates assigned to machines and multi-factor authentication for humans. The level of assurance of authenticity should be directly proportional to the business value of the data the persona can access.

Further authorised access to the data should be based on the principle of least privilege, so any given persona is able to access only the data that it needs to deliver or consume business value.

All data related to the system should be categorised as well, and then given the appropriate level of protection it requires. Encryption should be used on all sensitive data and communications to maintain highest levels of integrity.

Finally, special attention must be paid to the basics – network monitoring, vulnerability patching, the use of tamper detection

for the devices and code signing to validate what they're doing.

Applying a healthy level of paranoia and preparing for the worst, from the very beginning, is key to building a secure foundation for the IoT.

ABOUT SHERRY ZAMEER

Sherry Zameer is Vice President IoT at Gemalto.
- Creating a better, conveniently secure tomorrow with IoT - 20 Feb 2019
- Silent authentication: a seamless customer experience - 11 Feb 2019
- The secure foundation for IoT - 11 Sep 2018
- Prepare for the 5G revolution - 7 Sep 2018
- 4 reasons why identity verification matters for African mobile operators - 31 Jul 2018

View my profile and articles...