How to Create, Deploy, & Operate Secure IoT Applications

TELIT WHITEPAPER

by Dr. Mihai Voicu, CISO, Telit

INTRODUCTION

As IoT deployments accelerate, an area of growing concern is security. The likelihood of billions of additional connections and the proliferation of endpoint devices in the form of IoT modules, sensors and other equipment is radically increasing the threat surface that organizations need to defend. We're now in a world in which a tire pressure sensor on a vehicle can be hacked, enabling cyber criminals to gain control of vehicle systems.

However, it's important to not get swept away by a wave of paranoia even while recognizing threats are real and therefore they need to be prevented and controlled. We're at a stage now where organizations are acknowledging that security attacks are a fact of life and breach occurrences are a case of when, not if. Knowing how to handle an attack is growing in importance over learning how to prevent attacks themselves.

Security is the most important barrier affecting the wider deployment of IoT solutions, as detailed in the recent Voice of the Enterprise: Internet of Things, Q1 2016 Survey, conducted by 451 Research. This survey uncovered that security concerns are seen by respondents as the greatest impediment to deploying an IoT initiative (Figure 1).

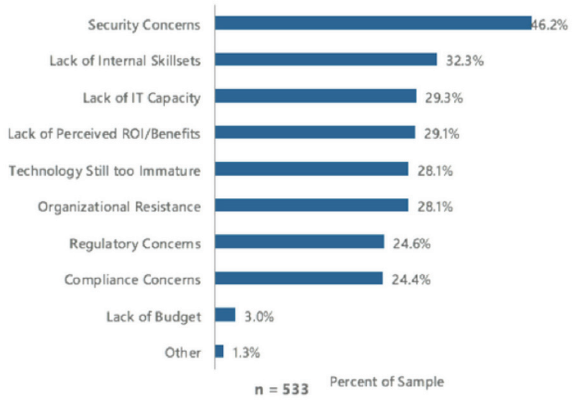


Figure 1. Impediments for IoT deployments
Source: 451 Research, Voice of the Enterprise: Internet of Things, Q1 2016 Survey

Contents

SERIOUS ABOUT SECURITY

It's clear therefore that the IoT industry needs to get serious about addressing security concerns. For some, IoT security is little more than an extension of traditional internet security, but the reality might be different. Endpoint devices need to be secure, the network itself needs to be secure and the servers and IT architecture at the other end must also be secure.

There are two core aspects to security in IoT: securing endpoint devices and securing the control plane of IoT solutions. A key aspect of the security focus is on how to secure the data from sensors and the collection of information that is relevant to a particular customer. At the same time, equal or greater focus is devoted to the security of the control plane of IoT solutions.

The majority of insights into IoT vulnerabilities today that are publicly available are related to how the criminals got to the data. The issues do not concern how they actually gained control of the data because just getting to the data today means that you have the ability to utilize it. It's therefore important that IoT security addresses how to prevent criminals getting to the data as a priority. After all, if they can't get to it, they can't steal it. Prevention may be better than the cure after all.

ENDPOINT DEVICE SECURITY

One of the most relevant aspects of IoT security is the multiplicity of endpoint devices and the strength of their security. The majority of security penetrations are coming from vulnerabilities that result in compromised devices. This is partly because many IoT devices are considered novelty items and the pricing does not support inclusion of security.

However, it's important to consider that hacking an endpoint doesn't offer much value to a criminal. When you look at an endpoint device, it may be easy to get into but what can you do once you have access to it? The device may be just an entry point.

Organizations should be aware, that the control plane of the platform can also be compromised at the device level. Such back end security technologies are robust but, if the correct policies and processes are not put in place by the enterprise, criminals can get round them by hacking devices and fooling the back end into believing that the devices have not been taken over and remain legitimate.

Secure Boot

Endpoint devices present a huge attack surface for cybercriminals to exploit. Telit has been working with the GSMA to create security guidelines for endpoint devices. Efforts have focused first on what is put on the endpoint device, which is the interface with the cloud or network. A secure boot capability – which ensures that a trusted, secure environment is created when an endpoint device's communications module is booted – has been developed by Telit to ensure a secure anchor into an endpoint device exists.

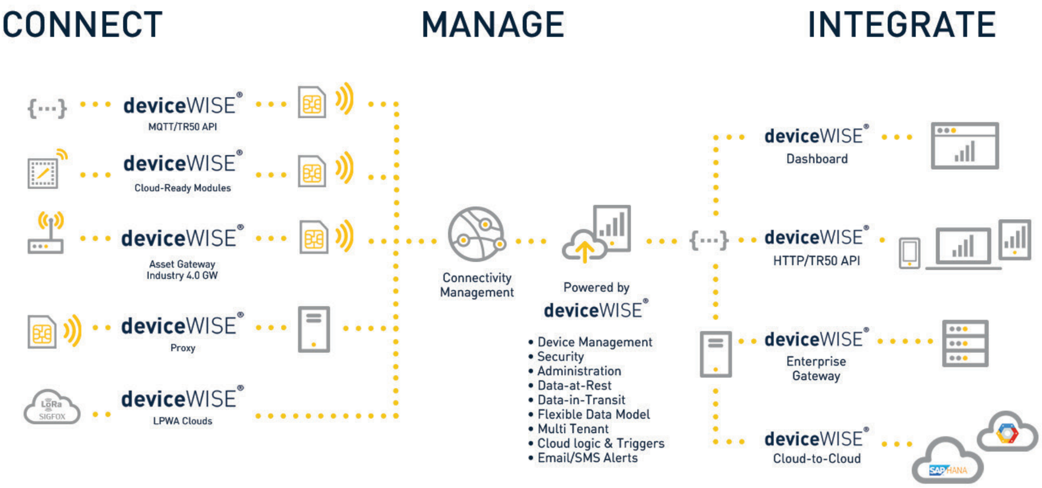
This secure anchor means that as soon as the chip fires up and the firmware initiates, every single line of code is assured to be from a trusted source. Firmware has many different inputs including those from cellular operators, from chip developers and from module providers. Telit's secure boot capability ensures that these, plus the customer firmware, are trusted. This comes together to assemble a series of firmware that users know is trusted and has no possibility of allowing or enabling any malicious code to be injected. Secure boot capability helps strengthen the endpoint device and is available today.

Once this trusted firmware environment exists it becomes less important whether an endpoint device is a high- or low-end product. High-end endpoint devices are typically operating systems with microcontrollers that allow the application additional security protection. However, the majority of endpoint devices in deployment are low-end devices without operating systems that might include a microcontroller. It's not uncommon to see a module that has the capability to support a microcontroller and that opens up security threats.

AGGREGATION POINT SECURITY

Beyond the module and the network, the next points of security weakness are the aggregation points at which data from modules are brought into the systems of an enterprise. First comes the gateway but the major aggregation point is the IoT platform which makes the connection into the enterprise. This point of aggregation is where all the gateways connect and, from there, multiple ways of getting data out exist.

The data itself is coming in from a multitude of inputs, as illustrated in Figure 2. below.



An asset gateway on the left hand side of Figure 2, for example, provides a gateway from a hardware perspective into the cloud. At the same time, Telit offers an agent in specific gateways that creates a secure bridge into the cloud so the enterprise can receive information in a secure way.

An enterprise gateway on the right hand side of Figure 2 has a similar agent that securely connects into the cloud so, once the data is aggregated in the cloud, an enterprise will want to extract it and deploy it into enterprise systems such as ERP. The gateway can enable a secure bridge from the cloud into the interfaces of each enterprise systems.

In essence, data can be encrypted by agents in an asset gateway and decrypted by agents in an enterprise gateway ensuring data is secure in the cloud.

CONNECTIVITY MANAGEMENT

Another aspect is connectivity management. Customers need to have secure connectivity but this is a complex situation. If, for example, a Telit platform resides in an Amazon Web Services environment in which it can operate securely, the asset gateways that are deployed -- on an oil pipeline or in fleet vehicles, for example -- also have to be considered carefully. The challenge is how to bridge the two situations, one of which is a secure environment and one of which is composed of the multiple remote endpoints which need to be specifically secured. This can sometimes be easily addressed with on-device security but it is often unclear who is responsible for securing the assets.

Cellular modules used by customers, for example, often need a data subscription, and a SIM card with a subscription, that also needs to be managed effectively so that the connectivity is attached to the proper carrier and the proper module to ensure security is maintained. Telit is able to operate this aspect so it not only provides a secure module to the customer but also offers SIM cards that are managed by Telit in a secure way. To achieve this, when the data comes out of the carrier it needs to go to the Telit cloud where it can be operated securely. This connectivity management is done by Telit in a secure fashion and is another important part of how Telit produces a secure solution for enterprises.

PLATFORM SECURITY

The notion of end-to-end security is an attractive concept in IoT but so far it remains just a concept, with pockets of security interlinking to create a semblance of end-to-end security. The idea of platform security is central to end-to-end security. On platforms such as Telit's deviceWISE IoT Platform, there is an intrinsic list of security features available but, in some cases they are also dependent on the policies of organizations operating the platform.

Humans typically have access to the platform but devices have different ways of being identified and authorized to connect. Each user and device has unique features when it comes to accessing the data itself. A device will basically publish information and the only way this can be done is through the use of APIs (application programming interfaces). Security is placed on top of APIs to enable devices and users to have access based on their roles. API roles and security controls are encapsulated into an abstract concept called "organization".

For example, in the fleet management industry, the majority of customers own a fleet of trucks but sets of those trucks are operated by different companies. Users want the ability to segregate trucks based on which company is operating them so there is a different level of security. This is why Telit offers so many layers of segregation: the owner of the fleet can see all its trucks but individual operators can only see the vehicles they manage. Access to data in this scenario is required for devices and humans but it is only provided according to their roles and privileges.

Telit's platform approach emphasizes the importance of being able to secure the control plane. For Telit, it's critical how access to the underlying capabilities, rather than the platform itself, is given and managed. Totally different levels of segregation for user access are enabled as well as a very strict approach to what needs to be added with change management control in place. Requests, approvals and execution are not performed by the same person and it's vital to ensure that the impact of infrastructure on operations from a security point of view is minimal.

CONCLUSION

The concept of end-to-end security is attractive and important for creating comfort among organizations that IoT will not be a back door for criminals. However, there are different categories of users in IoT and there is a broad layer of companies and users that are in the discovery phase of IoT. They haven't fully established what IoT means to them yet, nor what they will do with IoT. These organizations pick a platform and download sets of APIs and start playing with them, which makes the situation more of an experimental environment than a production one.

Even in this experimental phase, though, organizations need to pay close attention to security. Very quickly trials can expand and suddenly data from different entities is aggregated in the cloud and security becomes an issue that needs to be addressed.

It's important to bear in mind that security is regulated but such regulation can only be complied with if the data is secure end-to-end and data can be proven to be secure. This lowers the barriers for organizations and enables efficient compliance with regulations rather than requiring compliance to be demonstrated for each situation.

Telit is working on this now because it is one of the vital parts that IoT continues to be missing at the moment. Telit is working closely with GSMA, for example, to develop security guidelines that will help organizations establish their approaches to achieving secure IoT deployments and operation.

Telit can help you assess and address security vulnerabilities in your IoT application and provide you with a solution to bolster critical security attributes. Contact IoTSecurity@Telit.com.

REFERENCES

Beecham Research expects that revenues from device authentication, device management, data management, billing and security will exceed $3 billion by 2020. Out of these, the firm sees security and data management services generating $1.8 billion alone.

Worldwide spending on Internet of Things (IoT) security will reach $348 million in 2016, a 23.7% increase from 2015 spending of $281.5 million, according to Gartner.

Spending on IoT security is expected to reach $547 million in 2018. Although overall spending will initially be moderate, Gartner predicts that IoT security market spending will increase at a faster rate after 2020, as improved skills, organizational change and more scalable service options improve execution.

A survey conducted recently by Current Analysis among 1,000 enterprises on their investments in IoT technology disclosed that security is still a key concern. One-third of the businesses surveyed listed security as their top worry, and 17% of the companies surveyed that had evaluated but chosen not to implement an IoT project cited security concerns as the primary reason.

Gartner predicts that by 2020, more than 25% of identified attacks in enterprises will involve IoT, although IoT will account for less than 10% of IT security budgets. By the same year, the firm predicts that more than half of all IoT implementations will use some form of cloud-based security service.

The IoT security market is driven by rising security concerns in critical infrastructures and strict government regulations and is expected to grow from $7.9 billion in 2016 to $36.95 billion by 2021 at a Compound Annual Growth Rate (CAGR) of 36.1%, reports research from MarketsandMarkets.

Concern about the security of early IoT deployments has emerged as the leading impediment to new IoT projects, with 46.2% of 533 respondents to a 451 Research survey expressing concern.

Telit