GlobalLogic®

Security for the Internet of Things

Tzvi Kasten, AVP and Security Practice Head, GlobalLogic Inc.

The emerging Internet of Things (IoT) market is introducing new concerns around cyber security. Now that hackers can access connected devices in addition to pure data, they are affecting the physical world and breaching user privacy in brand new ways.

Although IoT is revolutionizing the way companies do business and the way people live their lives, it is crucial to secure all the various “things” in an IoT ecosystem. In this white paper, we will identify current IoT security challenges and address how they can be resolved.

www.globallogic.com

Table of Contents

What Is This IoT Thing That Everyone Is Talking About?

The Precursors to IoT

In the early days of the Internet, content was created and consumed by people on a static website. The website itself was merely a communication device, similar to a phone or newspaper. As technology improved, websites became dynamic objects powered by server side scripts. Websites could be created based on a request from the browser. This concept was further enhanced through client side scripting, wherein the JavaScript code interacts with the web server to update a website. So instead of a website being created by a person, it was created by a machine (i.e., Machine-to-Person).

This approach essentially automated the Internet. For example, a user could purchase goods from an e-commerce website without the seller being present during the transaction. To process the user's credit card, the website would simply gather financial data from a connected credit card system. Similar systems could gather data from sensors and other connected devices. When two computerized systems communicate with each other like this, it's called Machine-to-Machine (M2M).

Moving Beyond M2M

Now that the costs associated with connecting computerized systems to networks are decreasing, and as network availability and throughput improves, there is a growing trend to connect unconventional devices to the Internet. For example, utility providers can now remotely read customer meters through embedded sensors. Furthermore, by connecting these sensors to an automated billing system, utility providers can generate and distribute customer invoices without requiring a single person to access or manage any of this data.

Similarly, as server computing power becomes more available and accessible, businesses can manage and analyze huge amounts of data through new and better analytics applications. This combination of improved analytics and connected devices (or "things") has led to what is now known as the "Internet of Things" movement.

At GlobalLogic, we define IoT as a set of technologies that connects data from a variety of sources (including sensors) with the ability to intelligently drive context-aware actions in near real time. In this definition, sensors may be in a smart device or in a person acting in an observer role, and intelligence may be in the cloud, a local gateway, or the device itself (i.e., "ubiquitous computing). Regardless of how it's defined, IoT is disrupting nearly every market around us through innovative new technologies.

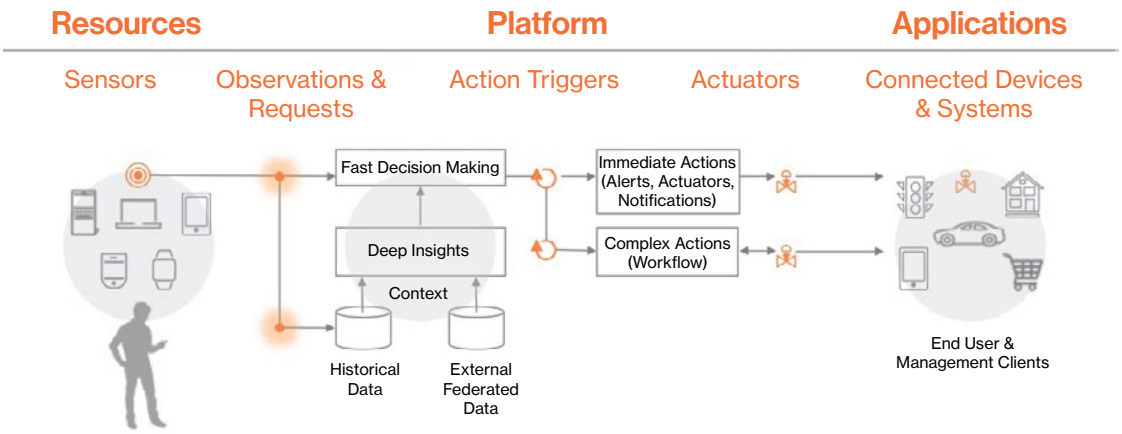

Figure 1: The Internet of Things ecosystem

Why Are We Hearing So Much About Cyber Security Lately?

The Evolving Ecosystem of Cyber Crime

In the past, hackers were primarily motivated by ego. Now cyber crime is perpetrated for monetary gain and has become a significant sector in international criminal activity. These cyber criminals have established supply chains, are highly motivated to seek new opportunities, can react quickly when an opportunity is identified, and can easily recruit talent and technical resources to achieve their goals.

Since cyber criminals have time, money, and technology on their side — and since they can target zero day vulnerabilities that are unknown and therefore hard to protect against — it is virtually impossible to ensure 100% security against a persistent and targeted attack. Even engaging law enforcement is difficult because (1) attacks can be performed from anywhere in the world, and (2) the field of cyber forensic science is not yet developed enough to establish firm evidence against an attacker.

Security Concerns for IoT

Connecting systems and devices to the Internet introduces the risk of people potentially gaining unapproved access to private or sensitive data through a network.[1] For example, the popular "Bring Your Own Device" (BYOD) policy, wherein employees can connect their personal devices to the corporate network, opens up businesses to data theft or modification through a compromised network or dishonest employee.

Hacking threats are even more sinister in an IoT environment because attackers are trying to gain control of the devices themselves — devices such as traffic lights, door locks, automobiles, or even pacemakers. As more and more devices become connected to the Internet and each other, there is a greater potential for hackers to make a negative impact on the physical world.

Since these devices touch many details of our day-to-day lives, our privacy is also at stake. A smart TV with a built-in camera is great for Skyping with friends and family, but it's also a window into your home. Similarly, while wearable medical devices are a huge step in remote patient care, they also leave patients vulnerable to having their sensitive medical records breached. Before we can truly benefit from the amazing capabilities of a connected ecosystem, we must first ensure that our devices are safe from cyber attacks.

What Are the Challenges and Strategies for Building a Secure IoT System?

Although there are some special challenges to consider when building a secure IoT system, we can apply much of the same knowledge we have already learned from building secure information systems. Below is a breakdown of the security issues unique to IoT, along with strategies for securing each component of an IoT ecosystem.

Device Hardware

Challenges

Since IoT systems utilize many different devices, one of the most common attacks is to gain control of a physical device and then attempt to access the entire IoT platform through it. While this can be avoided for many devices with some common sense "lock the door" procedures, it can be a bit more complicated for devices that are in the public domain (e.g., traffic lights) or purposefully mobile (e.g., automobiles).

In some scenarios, IoT devices are operating under strict cost and power consumption constraints. Leveraging state-of-the-art processors with sophisticated security features such as encryption requires both additional costs at the hardware level and additional processing power. These higher costs and power consumption requirements can have a material impact on the device itself.

Strategies

When creating an IoT ecosystem, look for devices that have a secure booting process and that utilize hardware-

1 To learn more about the complex world of information security, we recommend you read GlobalLogic's white paper, "An Introduction to Information Security."

based security features such as tamper-proof secure areas for code and data. A secure booting process can be achieved if manufacturers properly configure their devices to ensure that each boot stage validates the cryptographic signature of the booted software. We also highly recommend cryptography acceleration because it enables encryption and decryption without significantly impacting a device's performance and/or power consumption. ARM's TrustZone technology and Intel's hardware-assisted security are both good examples of how to secure an IoT system.

Of course, due to the above-mentioned location and processing power constraints, an IoT system may not be able to ensure that all of its devices follow the above protocols. For this reason, companies should not rely solely on a virtual private network (VPN) to secure its IoT system. Any time a device is not located in a controlled environment, it cannot be trusted to connect to a network, even through a VPN. For example, if someone with the right technical skills acquires one of the "things" in a company's IoT environment, he/she could then join the network as a trusted entity.

System Software

Challenges

Most stand-alone devices utilize well-known operating systems and software applications, which means that vulnerabilities are often quickly identified and resolved through patches and upgrades. Think about the device you are using to read this whitepaper — how often do you receive notifications about new versions and/or security patches being available for your operating system or software applications? Often our devices download and install these patches and upgrades automatically without us even being aware of it.

However, deploying and installing patches and upgrades becomes much more complicated with IoT devices because they are part of a larger network. Often there is no automatic process for installing these updates or even notifying users that an upgrade or patch is available because:

- The developers of an integrated IoT solution have not considered comprehensive software updates as a security feature; instead, they provide general tech support tools to fix issues that individual users find.
- Updating devices that are remotely distributed across multiple locations is too challenging.
- It is not prudent for devices with critical functions to restart automatically after installing a patch or update.

Without including a way to identify known vulnerabilities, alert users of those vulnerabilities, and automatically distribute and install updates/patches, hackers can use the same techniques and tools to corrupt an IoT system over and over again. At the same time, attackers could use an automatic software update tool to compromise an entire network by loading his/her own special software version onto a device. So while enabling devices to stay up-to-date with the latest OS and software versions is crucial to avoiding known vulnerability attacks, product developers must also consider the security aspects of the software update tools themselves.

Strategies

Securing an IoT system's software and operating system requires a three-prong approach: (1) developing software through a secure development lifecycle process, (2) identifying software vulnerabilities and alerting system operators of available patches/updates, and (3) installing patches/updates across the entire system.

First and foremost, IoT software developers must follow a secure development lifecycle (SDLC) process when

creating embedded software for IoT devices or system applications. Security should be baked into the system requirements, design, and implementation testing, and there should be a plan for supporting the product's security after deployment.

The process should enable developers to identify and build to the product's required security levels while facilitating a rational level of security investment in terms of cost so that organizations aren't left with an all-or-nothing approach. The below figure illustrates GlobalLogic's own SDLC process, which is based on Agile methodology and defines specific security activities for specific sprints.

The second step to securing software is creating a unified process for identifying vulnerabilities within specific devices/applications and alerting system administrators when a software patch or update is available. While developing these processes will vary across different businesses, Oracle and Timesys offer some excellent alert services that identify when critical patches exist.

Finally, let's talk about how to remotely install software patches and updates across system devices. Although updates are typically installed through a network or USB interface, this approach makes it possible for a hacker to insert malicious code. Ideally, any software updates should be performed through an authenticated connection using a digitally signed binary file that can be authenticated by the device. Furthermore, companies must assess whether operating system updates are critical, as they can be much more costly, complicated, and even risky to deploy.

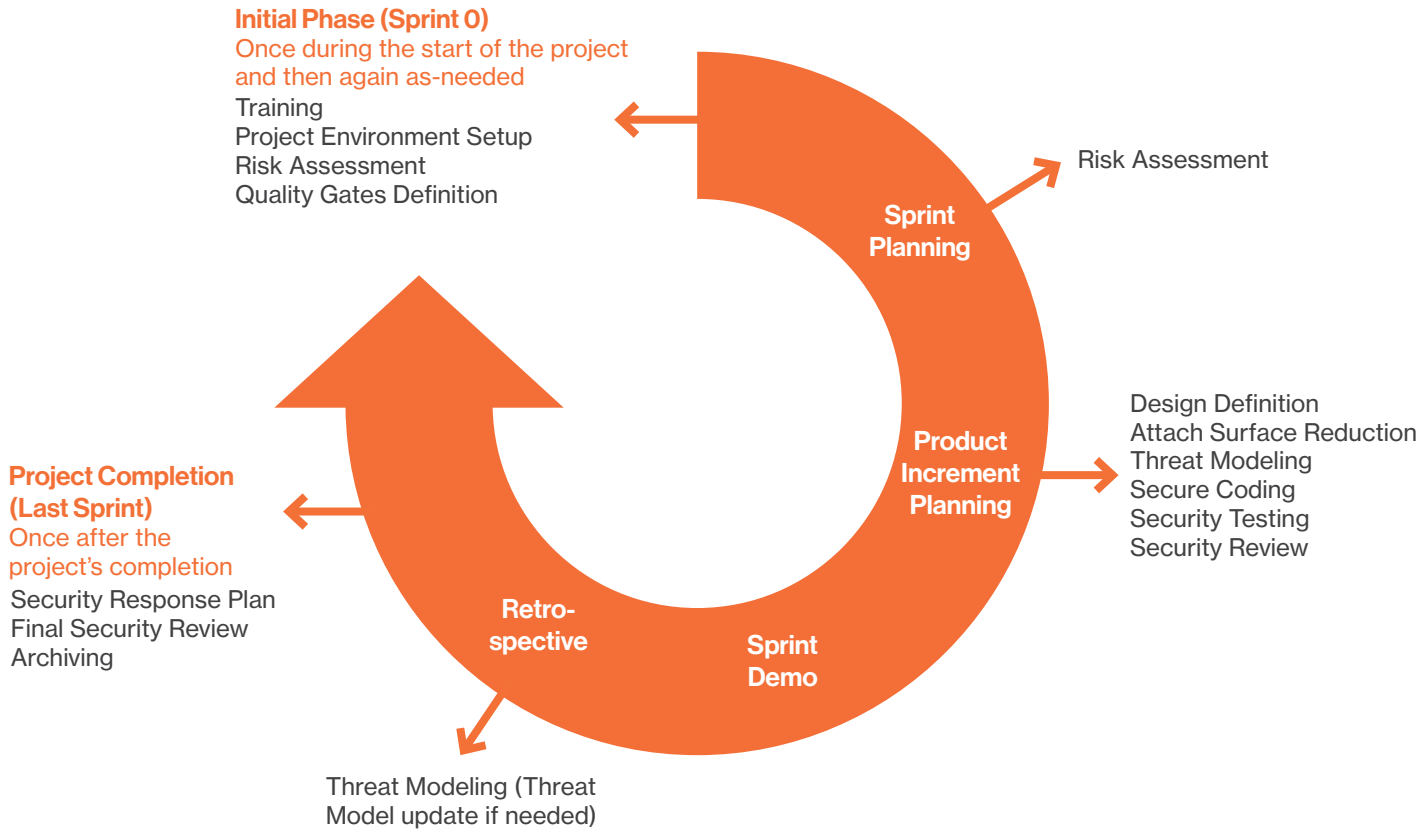

Figure 2: GlobalLogic's Secure Development Lifecycle (SDLC) Process

Device Authentication

Challenges
A single IoT ecosystem can utilize multiple devices developed by multiple vendors, along with multiple systems to manage these devices. With so many different technologies involved, there is not a single way to authenticate all devices. Each device may use its own authentication approach, and some devices may (by their very nature) be less secure than others. All these factors make it a challenge to ensure that authenticated devices are what they claim to be. However, if device authentication is not handled properly, an attacker could potentially sniff the network and "play back" the login session without the other server or device even being aware that it is talking to a simulator.

Strategies
Authentication is a crucial step for ensuring that external devices are interacting with a legitimate IoT platform and not a hacked system that is pretending to be the IoT platform. The platform also needs to authenticate that the device requiring access is legitimate. The best way to achieve device authentication is for the manufacturer to embed a unique certificate on the device. This would enable the IoT platform to validate the device, and vice versa. We also suggest encrypting dynamic, random information within the authentication process itself to eliminate hackers from recording and playing back the authentication sessions.

Furthermore, businesses should be utilizing state-of-the-art standard cryptology algorithms for authentication. Using obsolete cryptology standards results in well-known security flaws that can be used to attack a system, and using non-standard cryptology is risky because it often results in design flaws. System developers may assume that proprietary encryption is preferable because it is not a commonly used tool like standard cryptology, but the reality is that hackers can and will unravel non-standard encryption. It is much more preferable to use standard cryptology approaches like Transport Layer Security (TLS) because of the very fact that they are widely used and therefore well-tested.

System Network

Challenges
By its very nature, an IoT network is distributed across multiple locations and connected through the public Internet. This setup expands the network attack surface area because it allows multiple entry points into the system. A hacker can use the network to compromise the entire IoT system without actually attacking the system itself.

Using firewalls to protect the devices and the network that connects them is not practical. In the past, organizations have used VPNs to ensure secure connectivity between distributed networks. However, as we mentioned earlier, VPNs are not helpful in an IoT ecosystem because the devices may be located in public areas or in networks that are not under the control of trusted users.

Strategies
A good encryption strategy is the most effective way to secure an IoT network, as it prevents hackers from accessing the messaging interface, gathering information on the network protocols, and identifying ways to attach the entire system. Examples of encrypted communication protocols include using TLS-based HTTPS and using MQTT over TLS. System administrators should also secure the XMPP, and they should utilize a valid X.509 PKI architecture to ensure that certifications are properly validated.

Furthermore, it is important to segregate communication channels so that even if one network channel is compromised, the other channels will remain secure. For example, it is important to separate the remote provisional and control channel to the device from the statistics and information reporting channel. This approach will also help if a device is on more than one IoT network, such as being on a vendor's network (i.e., for software updates, support, and licensing) and being on an organization's IoT network (i.e., for applications). It is important to separate the two communication channels and not allow devices to jump from one to the other.

System Data & Users

Challenges

IoT systems are often used to gather sensitive data such as medical biometrics, personal schedules, inventory and supply chain information, etc. Even when systems do not gather information that is explicitly sensitive, there is often enough contextual data that — given the right analytics tools and cross-reference systems — someone could deduce further information.

To prevent potential data leaks or thefts, it is crucial that IoT system developers identify which types of data can be shared with which systems and which users. However, this can be complicated in a distributed IoT ecosystem because of the many types of users and their roles within a system (example below):

- Platform system operator
- Platform tenant operator (only uses specific component of IoT platform)
- System IT administrator
- Hardware/application/service provider
- Hardware/application/service consumer

Ensuring that each of these users can access everything they require from an IoT system, while simultaneously limiting their access to any other parts of the system, is quite complex. Furthermore, a user may hold more than one role or have roles that change, meaning a system must be able to dynamically update user access rights in real-time. Furthermore, each of these user roles may interface with the IoT platform differently. Securing multiple interfaces that need to be both easily available and high-performing is an additional challenge.

Strategies

The security of an IoT system's data and users relies entirely on good policymaking. For example, organizations should use mask keys (i.e., arbitrary data) instead of information like names or identity numbers whenever possible. By masking data this way, organizations can more effectively obscure content that is sensitive or that becomes sensitive when correlated with context. It also enables organizations to comply with certain regulatory requirements regarding cloud-based storage and enables them to more easily share data with third-parties without disclosing information about their patients/customers/etc.

The next step is to have a well-defined user map that identifies a system's various users, their roles, and their relationships with the IoT system.[2] Similarly, an organization must define policies for which users can access which data or systems, how the data and systems can be accessed, and how users can utilize the data and systems.

It is also important to rate an IoT platform's various interacting systems along a "trustworthiness" scale, as some systems may be less secure than others. For example, a user who tries logging into his/her email account from a personal laptop in a hotel lobby is naturally less "trustworthy" than a user who accesses his/her email account over a corporate network using a biometrics-enabled device. The first user should only have limited access to the system until he/she connects in a more secure way. By treating each system according to its own unique level of trustworthiness, organizations can balance their often opposing requirements of accessibility and security.

This policy-making may sound tedious, but it will prevent unintentional data loss, leakage, or unauthorized access. Understanding — and limiting — who can access which data or systems also ensures that if there ever is a security breach, only that specific user or system will be affected.

Finally, consider giving responsible hackers and cyber experts an opportunity to challenge a system's security. Although this may seem at first counterintuitive, it is often very effective to "use a thief to catch a thief." After all, while processes and tools are useful for building a wall, there is no match for human intuition and innovation.

2 Gartner and the Kantara Initiative provide useful examples of how to create user maps.

Conclusion

The Internet of Things will touch nearly every sector in the near future, from connected homes to connected cars. Because of its pending widespread reach, businesses need to implement IoT very carefully with an eye towards security. Although there is no silver bullet that can ensure the 100% security of an IoT system, both organizations and individual device and application developers can use the above-mentioned strategies to make an IoT ecosystem as secure as possible, to identify security threats as quickly as possible, and to adapt to these attacks as agilely as possible.

References

https://www.globallogic.com/blog/the-internet-of-things-part-i/

http://www.globallogic.com/wp-content/uploads/2013/12/An-Introduction-to-Information-Security.pdf

About the Author

Tzvi Kasten is GlobalLogic's Associate Vice President of Business Development and leads the company's Security Practice. He has been integral in developing security-based products for many of GlobalLogic's customers, and he previously develop one of the first encrypted IP-based video conferencing solutions. Tzvi also provides security consultation for the company's Goliath platform for IoT product development.

About GlobalLogic Inc.
GlobalLogic is a full-lifecycle product development services leader that combines deep domain expertise and cross-industry experience to connect makers with markets worldwide. The company works with both start-ups and industry leaders in the digital media, electronics, healthcare, infrastructure, finance, retail, and telecom industries.

Headquartered in the United States, GlobalLogic operates design and engineering centers around the world and leverages its global pool of security experts to facilitate a leadership role in the sector. This expertise facilitates the company's ability to develop security-oriented products and services that meet both industry standards and customer requirements.

For more information, visit www.globallogic.com