White Paper

Security and the Internet of Things (IoT): Should Developers Worry?

Lon W. Schiffbauer, Ph.D. Consultant
Unlocked Communications, LLC

October 07, 2014

Windows Embedded

The emerging technology of the Internet of Things (IoT) has the potential to profoundly improve many aspects of our lives. However, as with any other technology that trades in personal data, security risks pose significant concerns. With hackers all over the world looking for ways to steal important data from the Internet, it's important that we carefully consider the security risks inherent in IoT.

There can be no doubt that when designing an intelligent system—connecting edge products (peripheral devices or components) to remote servers (for example, connecting a wearable device to the cloud so that remote caretakers can download vital data)—there are many security concerns a developer must consider. This paper will examine the question of data security when designing intelligent systems in an IoT ecosystem. It will also explore a variety of solutions that address these challenges, not only at each layer of the IoT ecosystem, but in aggregate as well.

Contents

What is IoT?

IoT is the ability for devices to connect, communicate with, and remotely manage other networked peripherals over the Internet. It transforms "things" into Internet-enabled edge devices or components, capable of generating data that can then be analyzed. Whereas in the past, technology generally required a human catalyst—a user to access a computer system to pull data, for example—the new IoT megatrend enables edge devices to communicate with one another and provide the user with important information when and where it is needed. Today the cloud, social media, mobile devices, and information sharing are driving early adoption of IoT. Wearable technology, smart home appliances, and intelligent medical equipment are just a few examples of how IoT is starting to work its way into everyday life.

IoT connectivity begins with sensor-equipped edge devices on either a wired or wireless network. These devices then send data to a public or private cloud via a gateway. From there the data can be pulled and analyzed by an approved individual or organization with the appropriate access. For example, consider an individual suffering from diabetes. This person can wear a wristwatch-type of devise (often termed a "wearable") that can monitor blood glucose levels, track food intake, measure activity levels, and even deliver insulin. This device can also access the appropriate gateway and transmit the data to a physician's cloud server for later evaluation.

Where are the Vulnerabilities of IoT?

In a report issued on September 11, 2014, Earl Perkins, research vice president at Gartner, said that over 20-percent of enterprises will recognize the need to protect business units that use IoT devices by the end of 2017. As a result, according to Gartner, companies will be required to make significant investments in security—security that will span and blend approaches, such as securing mobile and cloud architecture, industrial control, automation, and physical security. Blending these approaches, while necessary, exposes the system to vulnerabilities.

As with any other system, there are many security layers designed to safeguard against hacking. But while these measures are intended to provide increasingly rigorous levels of security, the savvy security developer understands that each level also exposes the system to different risks. This is compounded by the connective nature of IoT. For instance, access control and device authentication present unique challenges to the security developer. Access controls set strict parameters on privileges, allowing them to access only those devices and resources needed to do what they're designed to do. If the security of any component is compromised, access to the entire system is potentially at risk. Then, when the device is connected to the network, it has to authenticate itself before it can receive or trans¬mit data. The challenge presented by IoT is that it requires multiple sensors and devices to connect and share data seamlessly—preferably with as little intervention on the part of the user as possible. Yet this ease of sharing creates vulnerabilities.

Another factor to consider when assessing vulnerabilities is the nature of the target system. Some gateways may be on the device itself and be built specifically to enable IoT technology. These are called "greenfield" gateways. Other gateways, such as "brownfield" gateways, may be built over legacy devices. This has important implications when it comes to designing data security systems. The most effective security systems are not plugged in as post-deployment add-ons, but rather are an integral feature of the device's OS and leverage hardware security capabilities currently available. For this reason, developing in "greenfield" and "brownfield" gateways carries with it different sets of challenges and opportunities. This principle applies not only to the edge devices in the IoT ecosystem but equally to the cloud servers as well. Servers that run an OS developed specifically to fully leverage the hardware's security capabilities will allow the developer to deliver a more robust, comprehensive, and embedded security solution.

What Should you Consider when Designing a Robust Intelligent System?

After you've thought about your overall IoT architecture—or better you've worked with an expert partner to develop one—the next angle to look at is actually connecting the "Things" that make up your In the report issued by Gartner, Earl Perkins admitted that "At this time, there is no 'guide to securing IoT' available that provides [CIOs] with a framework for incorporating IoT principles across all industries and use cases. What constitutes an IoT device is still up for interpretation, so securing the IoT is a 'moving target.' However, it is possible for [CIOs] to establish an interim planning strategy, one that takes advantage of the 'bottom up' approach available today for securing the IoT." Simply put, this means that while there is no best practices playbook to draw upon, we are not left completely to our own devices. There are strategies we can follow.

The multiple layers of IoT protocols make the security developer's job more complicated than when simply working with basic HTTP Web app security. There is just no one simple security protocol to manage all of the communication protocols involved in IoT (such as CoAP, XMPP, AMQP, and MQTT, to name a few). Security developers have to develop strategies that address the needs of not only the individual communication protocols but how they operate and connect in aggregate. Server OSs that provide a wide variety of solutions when tackling this issue will have an advantage over those that have no choice but to try and develop disparate solutions. Furthermore, initiation models have to be thought of in light of the unique attributes of IoT. The Internet Request/Response model should not be relied upon for all message exchanges when it comes to edge devices sharing data over the gateway. There are alternatives available to the IoT security developer, but selecting the best one for the need will be the challenge for creating a secure system.

How does Windows Embedded Address Some of These Security Concerns?

As discussed earlier, IoT edge devices include smart home devices (such networked appliances, lighting, heating, and security systems), industrial components (such as sensor networks for industrial automation), and an array of other embedded devices, all connected and sharing data. Many of these IoT edge devices, components, or nodes, operate without any sort of user interface. They operate autonomously as part of the larger IoT network, feeding data to the cloud via a gateway. This means that securing IoT cloud servers has to be the cornerstone of any security effort.

In response to this need—a need that is only going to become more and more vital as the demand for IoT capabilities grows—Windows Embedded solutions provide forward-looking security capabilities. These solutions provide integrated layers of security throughout the entire IoT ecosystem, starting from the edge devices, continuing on to the gateway, and ending at the cloud servers. Furthermore, this suite of security capabilities protects not only each layer of the ecosystem but the link as well. This security solution goes well beyond any postdeployment add-on that many companies feel they need to plug into their systems. It provides a comprehensive security solution at the OS level.

Windows Embedded solutions offer robust intelligent system capabilities for retail, manufacturing, and health. For example, Windows Embedded solutions in the area of healthcare can improve patient care, drive smarter operations, increase team collaboration, and gain better patient insights, all while providing a high level of security across the entire IoT ecosystem. Windows Embedded solutions extend the power of Windows to intelligent systems,such as those that connect edge devices to remote servers via gateways. For instance, Windows Server allows you to build a secure cloud infrastructure in support of your IoT needs. The process of building a cloud infrastructure uses a combination of Hyper-V, failover clustering, storage, and networking technologies. Windows Server delivers features and functionality that provide everything required to build an effective and secure cloud infrastructure. Another example, coming to market soon, will be the Microsoft Azure Intelligent Systems Service (Azure ISS). This solution will allow companies to fully leverage the potential offered by IoT by securely connecting and managing data from a variety of sensors and edge devices. Microsoft Azure ISS marks a significant leap forward of the Microsoft cloud data platform, developed specifically for developing and maintaining intelligent systems. Companies using the Intelligent Systems Service to extend the Microsoft Azure cloud across connected edge devices and sensors will be able to capture vital data, transmit it safely to where it is needed, analyze it, and make stronger data-informed decisions that will move business objectives forward. Though still in testing, the Azure ISS has the potential of being the most integrated enterprise solution for heterogeneous IoT environments to date.

Security and the Internet of Things (IoT):
Should Developers Worry?
White Paper | October 07, 2014

A Company's Future will Depend on its Ability to Provide Secure IoT Services.

As discussed earlier, IoT edge devices include smart home devices (such networked appliances, lighting, heating, and security systems), The emerging technology of IoT opens up a brave new world for businesses and individuals, both today and in the future. Companies that are able to provide robust, comprehensive, and embedded security solutions to their customers will lead the vanguard in this new technological revolution. While dreaming up new ways of embedding IoT capabilities in an ever-growing list of edge devices is sexy, companies that give equal consideration to securing their customers' data will win the day. Windows Embedded solutions are the cornerstone upon which successful companies can build this future.

Live link the report above:
http://www.gartner.com/newsroom/id/2844317

Five Years Out

Arrow Electronics, Inc.
Arrow Intelligent Systems (AIS)
9201 East Dry Creek Road
Centennial, CO 80112, USA