The topic of Internet of Things (IoT) Security is both very popular right now and also quite broad. In this article, we'll focus our attention on security of devices: the things running in the world and our known universe that are rapidly being connected to networks, and from there to one another and to other computing systems.

IOT SECURITY FOR DEVICES

BY **TIM HAHN** / DISTINGUISHED ENGINEER, CHIEF ARCHITECT, CONNECTED VEHICLE & IOT, IBM

BUILDING SECURE DEvices takes experience, dedication, hard work, and ongoing support, well after these devices are deployed into their operating environments. The considerations device makers must cover include Designing for security and privacy, Testing for security, Adopting and following a continuous delivery model, and Ensuring integrity in the supply chain, during manufacturing, and through delivery.

Device registration is also a heated topic and is related to maintaining the security and integrity of devices. As device makers move towards providing their offerings as a service themselves, device makers must also take on more responsibilities for secure deployment and operations of these devices. Secure operations, is a topic for another article.

There are several unique considerations for security in IoT solutions. One aspect that differentiates IoT solutions from traditional computing environments is that the devices are used in harsh operating environments and conditions. The physical security of the device cannot always be ensured. There are also going to be many, devices. Far more than there are mobile devices such as smartphones. Devices will operate under several constraints such as CPU, memory, and network capacity. While these constraints are common with any computing environment, there are some additional constraints as well such as power consumption and heat dissipation. IoT devices are also used in situations that are much closer to the physical environment and exert control over physical objects. As such, they must be able to operate in mission-critical and safety-critical situations, and do so even when disconnected. These devices must have fail-safe modes of operation.

"ONE ASPECT THAT DIFFERENTIATES IOT SOLUTIONS FROM TRADITIONAL COMPUTING ENVIRONMENTS IS THAT THE DEVICES ARE USED IN HARSH OPERATING ENVIRONMENTS AND CONDITIONS."

One aspect that differentiates IoT solutions from traditional computing environments is that the devices are used in harsh operating environments and conditions. Even with these differences there is much existing security technology to extend from.

SECURE DEVICE DEVELOPMENT

It is possible to create a secure-able computing device. Note the use of the term secure-able rather than secure. This is intentional, since, like many tools, it is always possible for the user of the tool (or computing system) to set things up in such a way that the tool is dangerous or the computing device is insecure. So, let's consider the creation of secure-able computing devices.

THE BUILDING BLOCKS FOR DOing this are well known and come from years of experience in computer security. Don't invent new security algorithms or protocols. Use proven encryption/decryption, signing, hashing, and random number generation techniques and algorithms. Better yet, use toolkits and implementations that have been well tested, analyzed, stressed, and vetted.

By using well known algorithms and protocols, authentication, authorization (access control), auditing, and administration operations can be deployed for the IoT computing system, resulting in a secure-able system. In the case of devices, this usually means that there is both a local and a remote form of handling each of these security topics.

Most importantly, consider security at all stages of development. Security needs to be addressed during design, implementation, testing, deployment, maintenance, and even in the retirement of the device. →

ARM mbed IoT Starter kit

element14.com/community/docs/DOC-74945

Internet of Things Made Simple. The ARM mbed IoT Starter kit is a hardware development platform for IoT applications with no specific experience in cloud or web developments, connect your ARM mbed device and application to the IBM Internet of Things Foundation Bluemix Service, and visualize the data in real time, designed to spur on the invention of internet-connected gadgets.

CONSIDERATIONS FOR DEVICE MAKERS

WHAT THEN, SHOULD DEVICE MAKERS BE DOING TO BUILD SECURE-ABLE IOT DEVICES? THERE ARE MANY EXISTING TECHNIQUES TO APPLY AND USE.

FIRST, DEVICE MAKERS should be considering security from the very start of their creation of the device, starting at the design stage. By including threat modeling techniques as a part of the design process, device makers can identify threats, find solutions or mitigations, and provide details on what threats must be handled at later stages of device use. An important part of designing for security is to use a secure by default mindset when designing and implementing the device. While this can mean a bit more attention and work during device deployment, the alternative of having in-secure and widely deployed devices is no longer acceptable.

> "DEVICE MAKERS SHOULD BE CONSIDERING SECURITY FROM THE VERY START OF THEIR CREATION OF THE DEVICE, STARTING AT THE DESIGN STAGE."

Along with designing for security, device design and development should consider data privacy as well. Depending on the information collected and transmitted by the device, different privacy concerns will need to be addressed. As an example, the privacy concerns related to measured brake temperature by itself may be very small but when brake temperature is coupled with time and location there could be more issues to resolve. This could impact how data is collected, transmitted, stored, and segregated, as well as the settings for providing access to the data.

Software development teams in more traditional computing systems have been adopting agile and continuous delivery methodologies quite rapidly. For these teams, they have found that getting very quick feedback from their user community and also being able to deliver changes and new features quickly has made them much more effective in delivering useful and usable solutions. The same is true for IoT device development. Adopting a continuous delivery model impacts security in several ways:

- When there are security-related changes that must be deployed, there is already a delivery path in place to make these available.
- The delivery path itself needs to be built with security in mind so that devices are not susceptible to applying an incorrect, corrupt, or rogue-developed update.
- Security-related testing and evaluation must be addressed as a part of the continuous delivery processing so that it becomes part of the quick develop-test-deliver cycle rather than a ceremonial event which happens infrequently.

Because of the nature of IoT devices and the conditions in which they operate, the entire supply chain from procuring parts, to assembling the device, to loading firmware and applications onto the device, through delivery to the user must be secured. There are several examples of comprised devices being delivered to customers where the devices were tampered with during manufacturing or shipping, thus pointing out the need to consider the entire supply chain. With Internet-connected devices, this supply chain extends beyond physical device delivery into the electronic delivery of software and firmware updates, including the vetting of toolkits from other vendors that are packaged into software updates which will run on the device.

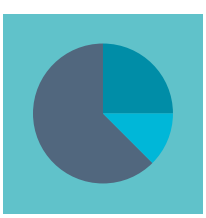
An emerging and important area for all parties working with IoT devices, from CPU and chip fabricators, through device manufacturers and assemblers, extending into owners and users of the devices is device registration and device identification. As devices include more and more security-related technology, the issue of key generation and storage, certificate generation and device identification, and the ability to verify device identity (to varying levels) becomes possible and also required. Work is underway to establish device registries which allow for chip fabricators, device manufacturers, and device users to all take part, securely, in maintaining the identification of and current status of devices used in IoT solutions. Device registries will factor heavily in the ongoing monitoring, maintenance, and support of IoT devices.

NEXT ARTICLE

Securing the operations of devices is a large and interesting topic itself. Look for a future article discussing this important area of IoT Security, that of security for operators of devices.

In the meantime, learn more about IBM's point of view on IoT Security at www.ibm.com/IoTSecurity

CHANGING BUSINESS MODELS



In the past, many device manufacturers would build their devices, sell them to a user or consumer, and then hope for the warranty period to end before they heard from the consumer again. With IoT devices connected to the Internet, this is no longer possible.

AT THE SAME TIME, DEVICE manufacturers now realize that customer satisfaction and ownership experience factors heavily into ongoing usage of and repeat purchase of devices by consumers. There is a growing need for device makers to pay more and more attention to the care and management of devices post-sale.

In addition to customer satisfaction, there is a growing trend in device usage which resembles more and more a rental-style model or pay as you go format rather than device ownership by the user. In the computing industry this started with outsourcing and has now moved into a model of "as a service" style offerings covering infrastructure, platform, software, and now services available on a pay-per-use type of deployment. The same is happening with devices as well. Businesses are now paying device manufacturers for the time they are using devices rather than for the devices themselves, with the device manufacturer taking on the responsibility for deployment, maintenance, and security of the devices. This change in business model implies that device makers must now consider "operations management" of their devices. ■