Protecting smart devices and applications throughout the IoT ecosystem

By: Rob Black, CISSP, Senior Director of Product Management PTC

The Internet of Things (IoT) presents security challenges that left unmitigated could pose serious risk to organizations. For example, consider the lack of human supervision of thousands upon thousands of connected devices which precludes using some of the most effective security methods that have been developed for and proven out in cloud applications.

Many connected devices – such as automobiles, power plants, and medical devices -- could cause serious damage if they are hacked. Even companies that have not consciously deployed IoT applications are at risk because many of their devices may already be intentionally or inadvertently connected to the Internet. Completely securing IoT solutions requires collaboration among several players including the infrastructure provider, the IoT platform provider, the application developer and the company that controls the devices. This white paper will address IoT security best practices at the device and application level such as data and network traffic encryption, audit trails, granular permissions and visibility and a secure software development life cycle (SDLC). Following these best practices will make it possible to develop smart, connected products that deliver real business value to your company and its customers while protecting against unauthorized and malevolent intruders.

IoT security challenges

At first glance, IoT is just an expansion of the cloud, which sometimes leads to the misperception that as long as the IoT application runs on a cloud system that has been secured then it will inherently possess the same level of security. However, the inherent interconnected characteristics of IoT applications present special security challenges that are not present in traditional cloud systems and are therefore not addressed by existing cloud security practices. As a case in point, user management in the cloud is simplified by the fact that permissions are typically granted to one human being using one application. The presence of that human puts firm boundaries around the authentication and authorization process. With IoT, on the other hand, devices may authenticate as themselves, as a human or on behalf of a human, requiring a much more complex permissions and trust model. For instance, the absence of a human user for the vast majority of IoT devices eliminates the possibility of using techniques that rely upon the human user for authentication, such as entering a user name and a password or for authorization, such as by clicking OK to permit a software update.

Another difference between the cloud and IoT is that IoT typically has many more devices, often several orders of magnitudes more, and these devices typically come in many different flavors and use many different operating systems and protocols. In order to do serious damage, a hacker typically does not need to penetrate all or even many of these devices but rather can focus on a small number of or even a single weakly protected device. Another element of the IoT security challenge is the variety of types of devices that must be managed and secured. In many applications it's necessary to assume that IoT endpoints deployed in the field can easily be scanned and probed, disassembled and studied by a potential hacker in an effort to identify their weaknesses. As a result, organizations that are designing new connected products need to ensure that all of their devices and applications are secure even from an attacker that has perfect knowledge of the operation of their IoT endpoints.

The security challenges of IoT are heightened by the increasingly critical types of devices that are connected and the potential damage that could be produced by taking control over them. For example, security researchers recently demonstrated that they could remotely disable the wheels and brakes of a popular sports utility vehicle (SUV).[1] Students remotely took control of the pacemaker implanted in a robotic dummy patient used to train medical students and showed they could cause life-threatening injuries to or even kill a real patient if it had actually been implanted in one.[2] Hackers demonstrated the ability to take control of a Wi-Fi connected rifle in order to aim it at a different target or prevent it from firing.[3] One of the most damaging real-world IoT hacks to date is the attack on the Ukrainian power grid in late 2015 that left 230,000 homes and businesses in the dark for up to six hours during the cold Ukrainian winter.

Application vulnerabilities present another serious security issue. Hackers can potentially gain instant, high-level access to IoT deployments by targeting security weaknesses in the firmware and applications running on embedded systems. If your IoT implementation is not properly managed a single compromise of one device could potentially lead to compromise of your entire system. This is particularly important in environments where the devices are deployed in other organizations' networks. Your organization's ability to mitigate security issues for these devices can be difficult as you don't control the environment. For this reason, among others, avoiding application vulnerabilities in your IoT solution is extremely important.

You may be connected and not know it

Many companies that haven't yet developed a single IoT application are already exposed to these risks. The Shodan search engine, which crawls the Internet looking for connected devices, has already cataloged more than 500 million connected devices including control systems for factories, hockey rinks, car washes, traffic lights, security cameras and even a nuclear plant. These devices were typically connected to the Internet through an internal application provided by the manufacturer or by third parties so in some cases the owner of the device may not even be aware that it is connected. As you might expect, these devices often possess only rudimentary security capabilities. Many of these devices need no password to connect to them and many others use "admin" as their user name and "1234" as their password. 70% of the devices communicate in plain text so breaking in is easy even if they use a secure password. Furthermore, millions of device are running very old versions of their operating systems with many known vulnerabilities that a hacker could use to gain access to the system.

[1]https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[2]http://www.computerworld.com/article/2981527/cybercrime-hacking/researchers-hack-a-pacemaker-kill-a-man-nequin.html
[3]http://www.usatoday.com/story/tech/2015/08/06/computer-controlled-rifle-black-hat-trackingpoint/31239637/

Digital data protection

A definition of the three states of digital data can be useful in defining security requirements for IoT. These three states are data at rest, data in use and data in motion. Data at rest refers to data stored on a device such as a hard drive or offsite cloud backup that is not currently being transmitted, read or processed. Data in use, on the other hand, is data that is in the process of being generated, updated, appended or erased by one more applications. Data in motion is defined as data that is in the process of traveling across a network.

Confidential data at rest should be encrypted on IoT applications and cloud services to prevent data leaks and limit the downstream impact of a compromised application. In particular, system passwords and keys should always be stored encrypted and user passwords must be hashed both at the edge components and at the IoT platform.

For the most part memory processing on a computer is not protected for data in use. The mitigating controls protecting the machine are considered adequate for data processing. Cryptographic function processing sometimes is run in a Trusted Platform Module (TPM) which is a dedicated microcontroller for secure crypto computation. Your organization should determine if the costs of such a solution are necessary for the application that you are designing.

Data in motion should also be encrypted so it cannot be intercepted or manipulated while traveling to its destination. The current industry standards are AES 128 or 256 for symmetric key encryption and RSA 2048 for asymmetric or public key encryption. Data in motion encryption should be considered for both data transmitted across networks and for data within a network for instance between a device and gateway or maybe even between a sensor and device. Of course there are some instances where the hardware does not have the processing power to be able to perform encryption activities. In these cases, network monitoring and other mitigating security controls should be put in place.

Authentication

Encryption is the beginning of data protection, not the end. Your valuable IoT data and systems should also be protected through security best practices such as Authentication-Authorization-Auditing (AAA). The large number of ways in which devices may need to authenticate requires considerable versatility in the IoT platform. The IoT platform should be able to support HTTPS authentication which requires a user to establish a web session with a user name and password. Some platforms simplify the setup process by delegating the authentication of credentials to an LDAP system that manages password policies such as password expiration, account lockout, password dictionary use, password history and password strength. One interesting approach is a pluggable authentication model that enables companies to implement their own business process specific user authentication model. Leading edge IoT platforms also support industry standard authentication mechanisms and integration with authentication modules provided by leading enterprise software providers such as Salesforce.com and SAP.

One of the simplest and most powerful best practices to address the vulnerabilities of IoT devices is to configure devices so that the device itself initiates all communications using a secure protocol and the device communicates only with a single, predetermined cloud server. This approach supports communications over a local area network (LAN), Wi-Fi, or cellular network while eliminating the need for the device to possess a public IP address. The result is that the devices' access to applications, devices and data can be controlled with a fine level of granularity. The use of TLS end-to-end encryption and authentication prevents interception and device or service impersonation. Security is further improved by the use of a stateless connection that is only on when in use and that opens remote sessions only on specific ports of the target device.

Authorization

State-of-the-art IoT platforms provide a highly granular system of permissions and visibility that can be implemented without coding. These platforms make it possible to grant or deny both design time and run time permissions at a range of different levels. In the case of a conflict, the most restrictive security setting is honored. Access control can be granted at the most granular level such as specific read or write access to a single property of a single thing. Or, the ability to read all properties of all things in the system can be granted much more broadly at the collection level. Likewise, multiple property services, subscriptions and events can be combined in a template to which permissions can be granted. Another approach is to structure things and people into hierarchical structures which might be based on organizational units, function, geography or business process and assign permissions and visibility based on this structure.

Auditing

Auditing can also make an important contribution to IoT security. Employing systems that allow for close monitoring of deployed devices, including logging of inbound communications, device configuration changes and local authentication attempts can ensure that efforts to compromise IoT devices in the field don't escape notice. If an attack takes place, the audit trail can be used to understand how the attack was performed, establish accountability and even potentially prosecute the wrong-doers. State of the art IoT platforms provide a full set of logging services including the application, the script engine, and the security system. All logins, successful or not, are logged. File transfers between edge devices and the server and remote desktop sessions to edge devices can also be monitored. Data that is typically logged includes the initiator, receiver, time, data size, bytes transferred, event type, error message if any, plus additional transport information. Authorized users can subscribe to specific types of logging data.

Securing the software development lifecycle

IoT security can't be bolted on but rather must be built into an application from the ground up. This can be accomplished through the use of industry standard secure Software Development Lifecycle (SDLC) coding practices that minimize the risk of application related attacks. Leading edge IoT platforms are designed with the use of frameworks such as the Open Web Application Security Project's (OWASP's) Open Software Assurance Maturity Model (OpenSAMM), Microsoft's Security Development Lifecycle (MSDL) and Cigital Software Security Touchpoints that provide the building blocks for effective software security assurance. These frameworks can be used to evaluate an organization's existing software security practices, build a balanced software program, and define and measure security-related activities.

IoT platforms developed using these frameworks have a more mature security posture and not only are more secure but have the ability to adapt to an ever changing security landscape. For example, OpenSAMM guidelines provide a framework for security governance, construction, verification and deployment. Each of these business functions have a subset of security practices associated with them. Verification for instance includes design reviews, code reviews and security testing. While many evaluations focus on the pen testing aspect of security testing, one can see how the OpenSAMM framework has a much broader set of considerations and thus pushes organizations to holistically develop their IoT applications. Not only do these frameworks help to mitigate security issues but they also can help to lower development costs. It's much less expensive to fix issues early in the development process than after the software has been deployed into the field.

Finally, IoT platforms commonly rely upon third party hardware and software so these components must be scrutinized for security issues on a regular basis. Vendors that do a good job tracking, maintaining and managing these components demonstrate their security maturity. IoT platform customers should ask their vendors for a list of third party components. If the vendor is unable to produce the list, then their ability to manage the security of their solution should be questioned.

This is the first of two white papers. Be on the look out for the second white paper:

- Securing the Architecture and Infrastructure of the IoT Ecosystem

Conclusion

The potential for substantial performance and cost improvements is motivating many organizations to develop thousands of new smart, connected products. With the the number of connected devices and applications increasing at an exponential rate, it goes without saying that the security risks associated with these devices and applications is also skyrocketing. The number and variety of these devices presents a broad attack surface that combined with the absence in many cases of human operators poses critically important security challenges. This white paper has outlined security best practices that can be applied at the device and application level by organizations that are planning or designing smart connected products to ensure the security of their IoT devices and deployments.

J7952–ProtectingSmartDevices–EN–1016