Securing the Architecture and Infrastructure of the IoT Ecosystem

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

If compromised, devices and systems connected via the Internet of Things (IoT) could cause serious harm – medical devices, automobiles, electrical power infrastructure, etc. It is critical that organizations working in IoT create an end-to-end security strategy that protects their devices, applications, architecture, and infrastructure.

In the white paper entitled "Protecting Smart Devices and Applications Throughout the IoT Ecosystem," we addressed device and application layer security. This document will address the equally important challenge of securing the IoT architecture and infrastructure.

- Architecture is the suite of components that enables deployment of applications that monitor, manage, control, and collect data from connected devices.
- Infrastructure is the computing, networking and storage that underlies the architecture.

IoT architecture security challenges

Compared to the cloud, which has a well-defined security model and limited points of access, IoT presents a much broader and more diverse attack surface. Any device, operating system, or protocol that is not properly secured can leave an organization vulnerable to attack.

The Shodan search engine, which crawls the Internet looking for connected devices, has cataloged 500 million connected devices. From factories to hockey rinks, car washes, traffic lights, security cameras, and even a nuclear plant – a high percentage possess only very limited security capabilities. Some companies are aware of these dangers but see little urgency in addressing them because they have yet to deploy IoT applications on a large scale. But, do they know how many of their devices are already connected to the Internet and potentially exposed to attack?

The limited size and processing power of many IoT devices makes them particularly sensitive to participating in Distributed Denial of Service (DDoS) attacks in which hackers compromise the device and then direct a flood of traffic at other infrastructure. On October 21, 2016, the DDoS attack on the domain name system (DNS) infrastructure that brought down Twitter, Netflix, and other sites provided a wakeup call to many organizations regarding the dangers of unsecured networked devices. Most of the malicious endpoints used in this attack were consumer-owned Internet of Things (IoT) devices such as digital video recorders (DVRs) and video cameras. The hackers used the Mirai botnet malware to recruit a network of slave devices that could be controlled as a group without their owners' knowledge. Even though the specific vulnerabilities that were targeted in this attack are likely to affect few, if any, enterprise IoT applications, the method of attack helps illustrate the potential dangers that enterprise IoT applications must secure themselves against.

Imagine discovering a serious security flaw in an IoT application deployed on tens of thousands of devices around the world. Your engineering team rushes to develop a patch to fix the problem, but what is the best way to push it out? Sending an email advisory to the individuals responsible for these devices will generate a tremendous amount of work without ensuring that the devices will be secured over a reasonable period of time. Yet, automating the process isn't any easier because of the many configurations, boards, chips, modules, software, etc. unique to each device – each of which could require a different patch. The automated process could be further complicated by the need to switch devices over to a safe state before the software patch can be installed and by the possibility that the device may be offline when the update is attempted.

IoT infrastructure security challenges

Cloud-based infrastructure provides the backbone for most IoT deployments. Companies already familiar with cloud security are familiar with the requirements for securing the IoT infrastructure, but the added scale and complexity of IoT connectivity, communications, and endpoints adds greatly to the challenge. Another factor to consider is the possibility that the infrastructure could fail in the event of a natural or man-made disaster which could cause your applications to go out of service or lose data.

IoT architecture security best practices

The responsibility for securing the architecture is shared among the various vendors that comprise a particular solution. For the pieces of your solution that you outsource, it's important to evaluate each vendor's capability to secure your connected products and processes. You should explicitly ask questions about security posture and what your vendors do to help secure their piece of the solution. You may also want to ask which parts of security they believe they own and where your responsibility lies. A mature security organization will be able to articulate the ownership of the various pieces of security.

You can simplify the process of securing your IoT architecture by using a commercial IoT platform that was built from the ground up with security in mind. A typical state-of-the-art platform is divided into two components: server and edge. The server handles user and device authentication, authorization, and auditing, brokers communication between systems, people, and things, transforms data and maintains data persistence, and manages the business logic of the application. The edge components provide secure communication between devices and the server while enabling intelligence and pre-processing of data at the edge.

An architecture that segments the various components of the network is critical for increasing the security posture of the deployment. For example, the infrastructure that terminates connections from devices should be in a demilitarized zone (DMZ) while the application server and database should be in a separate internal network. In this instance, even if a hacker successfully penetrates the DMZ, they will not be able to compromise the platform itself. More generally, segmenting your components minimizes the attack surface for an outside party to compromise the system.

The IoT platform should also have procedures in place to identify security vulnerabilities in current releases and provide updates for security flaws in standard product releases or maintenance updates. Remote software-management capabilities enable individual devices or device populations to be updated without costly software duplication and shipping. The IoT platform should also maintain in-depth information on the configuration of each device, enabling software releases to be correctly mapped while avoiding the need for manual intervention reducing costly support calls from customers.

IoT infrastructure security best practices

Cloud infrastructure that supports IoT technologies demands multilayer, multilevel security in order to ensure confidentiality, integrity, and availability. Communications between deployed endpoints, IoT hubs, and cloud management servers must be encrypted to prevent interception, while input to IoT application servers and back-end databases should be sanitized to weed out malicious traffic and application-based attacks.

Critical IoT assets must be safeguarded against man-made and natural disasters. Data center locations should be designed to withstand extreme weather events and prevent unauthorized persons from accessing data center space. Access to application servers and data should be secured by providing users with the least amount of privileges required to do their job. The physical security of the data center should be protected with assets such as security guards, cameras, bullet proof glass and walls, biometric systems, and portals that authenticate one person at a time.

Power availability should be assured by utilizing high-capability, redundant generators that provide power even during metro-wide outages. Data centers should provide cooling systems with redundant HVAC units at each location powered by normal and emergency electrical systems. Cold water tanks should also be installed to keep air conditioning units functioning when the data center transitions from direct power to generator power during emergencies.

The availability of IoT services must be ensured with proper data backup, disaster recovery, and resiliency planning. Disaster recovery capabilities should include a complementary, redundant environment that can rebuild and run the entire IoT service until the primary system is back online.

Conclusion

Compared with traditional cloud deployments, the scale and complexity of the IoT presents risks to valuable data and intellectual property. Organizations moving to capture the enormous opportunities presented by smart, connected products need to ensure that their IoT infrastructure and architecture are designed to meet stringent security requirements. With these measures in place, organizations can confidently build, deploy, and expand IoT products and services.

J9314_WhitePaper_ThingWorx_EN_0522