KORE®

www.korewireless.com

IoT SECURITY

A White Paper by KORE | *We Make It Easy*

The Internet of Things (IoT) has taken center stage in our increasingly technological world. Connected devices are becoming more practical and affordable for mainstream consumers, as well as an integral part of many businesses. We trust M2M applications to transmit confidential and personal information, monitor valuable assets, and control mission- critical devices.

However, as we are beginning to witness the limitless potential to save time, cut costs, increase efficiency, and improve quality of life, we are also made aware that with all these potential benefits, there is also potential for new instances of data vulnerability and security breaches.

90% of M2M devices collect some kind of personal information

A recent study released by HP Security Research reviewed 10 of the most popular IoT devices that included some form of cloud service and mobile applications. The results revealed that an alarming 70% were subject to serious security vulnerabilities. Some of these concerns included insufficient authentication/password strength, lack of transport encryption, weak web interface credentials, and insecure software updates.

As a growing number of players enter the market with new connected devices and applications, security will not be viewed as a point of differentiation – it will be an expectation. We want you to understand what you can do to meet, and even exceed that expectation. The following are five questions to consider prior to deployment that can help secure a connected application:

1. Data Encryption - Is your data protected?

The aforementioned report suggests that up to 90% of M2M devices collect some kind of personal information, which makes it critical that applications are able to keep this information confidential. Encryption is necessary for any M2M application transmitting confidential information through the network such as POS system (credit card information), mHealth (patient data) or Usage Based Insurance (GPS coordinates & vehicle information).

While encryption may be widely practiced in many internet applications, M2M presents some unique challenges. At a glance, many developers may be inclined to use SSL for secure communications. However, this can be problematic in an M2M application due to the additional processing power and memory required in a device to support SSL, and the increased wireless data costs that are a product of the increase in network communications overhead.

One might also attempt to create a VPN tunnel from the device side in devices running a fully featured operating system like Linux. Unfortunately, device side encryption may not always be practical in M2M.

The most practical solution is to create a site-to-site VPN tunnel from the M2M operator to the backend server's network. This allows for encrypted data transmission across the most vulnerable segment of the network path – the Internet. Site-to-site VPN also creates efficiencies by not increasing the amount of wireless data consumed and by offloading all encryption and decryption processing to powerful network appliances.

Before choosing a site-to-site VPN tunnel, a developer must assume that the networks of the MNO and M2M operator are trusted (more on that later) and be comfortable with the encryption algorithms used to secure wireless communications between the connected endpoint and the MNO's systems.

2. Controlling Access - Who can access your data/system?

While encryption is demanded for private information, in some instances, confidentiality maybe far less important than access and authentication. For example, the data transmitted with a wireless command to open your car door may not be confidential, but it is critical that no unauthorized parties have access to unlock the door through that system.

Security requires a methodical approach that leverages every element in the technology stack. Beginning with the operating system and down through the hardware level, it is critical to understand that no single line of defense is sufficient for complete protection.

M2M hardware should be designed with internal components that allow for wireless connectivity to be enclosed and protected. Ensure that devices with a removable SIM card have taken measures so that the SIM is not easily accessible. A stolen SIM could result in unexpected wireless data charges, or even worse, allow a hacker to have direct access to your backend application servers.

In addition to secure hardware, you should also take steps to prevent access to your software systems. Consider using secure over-the-air application updates. Data signing can also be used to ensure authenticity and integrity of transmitted data.

3. Monitor at Every Layer – Do you know when something goes wrong?

Even the best preventive security systems are not foolproof. It is important to have monitoring systems in place when an event has occurred. Once the event has been detected, a responsive action must be triggered to prevent any malicious use of the device or active SIM.

A backend application should have functionality in place that can log abnormalities in the data it is receiving. If, for example, a device is programmed to intermittently send sensor data but inexplicably breaks pattern, the system should notify administrators and, if possible, block the device from communicating with the server. One advantage of having the site-to-site VPN tunnel in place between the application server and the M2M operator is that the misbehaving device will have a fixed IP address, making it easier to isolate & block.

Your M2M operator should offer alerting tools that can be used by the solution provider to assist with fraud detection and prevention. You may choose to correlate GPS with location and timestamp information to verify positioning data received in the backend system.

You might also consider monitoring for malicious interference using digitally signed data messages between a mobile device and an M2M server to identify altered messages, scanning frequency spectrum for IMSI catchers, or setting tampering alerts on hardware to trigger a server notification.

Even the best preventive security systems are not foolproof

4. Network Partners – Are your network partners secure?

A successful and secure M2M application requires quality partners. The majority of M2M applications that rely on cellular connectivity transmit data over three networks: the mobile network operator (MNO), the M2M operator, and the Internet – which are usually managed by three separate organizations. Application developers should perform their own due diligence to verify any networks managed by third parties meet the necessary security requirements.

Some possible questions that should be asked as part of the security due diligence for an MNO or Internet provider:

1. Are all servers and network components within the organization's network updated with the latest security patches and updates?
2. Is there a process in place to apply new patches and updates in a timely manner?
3. What model firewalls are used?
4. Is there an Intrusion Prevention System (IPS) in place?
5. Is there a DDoS defense system in place?
6. Are background checks performed on all individuals with root access to servers and network devices?
7. Are all security events logged? How long are those logs kept?
8. Is there a SIEM solution in place to provide analysis and correlation of security events?
9. How often are root passwords changed?
10. What systems are in place to secure & authorize access to physical servers and network components (PIN code, ID badge, biometrics, etc)?

5. Secure Foundation – Are you building with security in mind?

Make sure your M2M application has a strong foundation by building with security in mind. Decide early that security will be a priority. If possible, assign at least one member of the development team to be focused on the security of the application. This person should work to identify risks and recommend solutions to avoid them. It is recommended that this individual obtain an industry standard security certification such as the Certified Secure Software Lifecycle Professional (CSSLP).

It is also important to establish good protocol for internal security and regular testing. Testing might include scanning of your web interface, reviewing your network traffic, analyzing the need of physical ports, as well as assessing authentication and interaction of devices with the cloud and mobile applications.

Security should be a key element of your product design and management. If you have any questions on how to improve your overall level of IoT security, you can reach us at **info@korewireless.com**.