software design solutions

an applied visions company

IoT App Security

How To Protect Your Users and Your Bottom Line

IoT Application Security:

How to protect your users and your bottom line

By Sam Fahnestock

Executive Summary

The number of devices connected to the Internet of Things (IoT) is expected to reach 55 billion by 2025. Compare this to the 9 billion such devices in 2017, and you can see how quickly the number of IoT devices is growing. It is also estimated that the global IoT market will grow from $151 billion in 2018 to $1.567 trillion by 2025. Growth will be driven by the development of new IoT appliances, the movement of more data to the cloud, and increased usage of IoT devices.

But as IoT devices proliferate, security becomes a bigger issue. Each of these billion-plus devices can be a potential attack vector into a system. IoT attacks increased by 600 percent between 2017 and 2017, according to the *2018 Symantec Internet Security Threat Report*.

Fortunately, security is getting a much-needed piece of the IoT budget. Gartner estimated that global spending on IoT security will increase to $1.5 billion in 2018. This is a 28 percent increase from the $1.2 billion spent in 2017, with forecasts predicting IoT security spending will hit $3.1 billion by 2021.

As IoT devices continue to proliferate, we applaud the increased attention security is getting. History has shown how simple it is for vulnerabilities in IoT devices to be exploited, exposing your entire network to attack. Some of the most notable examples include the Mirai botnet, hackable cardiac devices from St. Jude's Medical Center, and the TRENDnet webcam hack.

In this white paper, we take a closer look at the predominant attack vectors and the steps you need to take to defend yourself against them. A proactive approach to IoT security is the best defense, and the only way to make sure your IoT applications do not expose your users or your business to irreparable damage.

Table of Contents

Why we should all care about IoT application security

When we think about IoT security, there is one glaring similarity with more traditional application security—it is often an afterthought tacked on at the end of the development process. This is a particularly big problem with IoT because these applications are largely dependent upon hardware, and much of security is hardware-centric.

If you're not thinking about security from the very beginning, your hardware designs can severely limit the level of security you can build into the associated software. It can become tempting to skimp on security or dumb it down.

At SDS, we integrate security into the design and development process from day one, and we recommend this approach for all IoT applications. This ensures that you have a secure product that has the necessary features for a safe deployment.

IoT applications do have a few unique issues to address when it comes to security:

- ### *NETWORK SECURITY*

  IoT devices are typically deployed onto unsecure networks, because often that is all that's available. This places a heavier burden on the IoT device itself to provide the required security functionality.

- ### *PHYSICAL RESTRICTIONS*

  Many IoT devices have physical restrictions such as low computing power and small memory capacity, which can create security blind spots. These limitations force developers to pick and choose which security capabilities to build in. For example, if you're building a $10 sensor for a smart thermostat, designers will be very limited by the security hardware they can add while keeping the price reasonable. In this three-way battle between security, functionality, and cost, security often takes a back seat. This leaves your IoT devices and applications open to attack.

The frightening five: The top IoT attack vectors

1 RANSOMWARE

You are probably familiar with ransomware attacks, thanks to two well-known occurrences from 2017:

- The WannaCry ransomware spread quickly in May of 2017 by infecting Windows computers. It exploited a Windows vulnerability that allowed the attackers to encrypt files on the hard drive. The attackers demanded a ransom to decrypt them. A patch was available, but many had not implemented it. High-profile systems were impacted by WannaCry, making it one of the worst ransomware attacks to date.

- NotPetya existed before the WannaCry attack, but an updated version hit the scene shortly after WannaCry and spread quickly, confirming the lack of attention being given to cyber security.

You may be surprised to learn that ransomware is growing in the IoT space as well. The Symantec report found that ransomware was one of the most prevalent forms of IoT attacks in 2017, and it continues to be a major threat. An example is the ransomware attack on the San Francisco Municipal Transportation Authority, in which more than 2,000 network computers were locked until a ransom was paid. All rail system payment terminals were down during the attack, allowing riders free access while causing the city to lose more than $1 million in revenue.

Businesses are becoming more dependent on networks of smart sensors and devices. IoT devices are taken “hostage” in a ransomware incident. The attacker demands a ransom from the owner (a company or an individual) as payment for releasing the device.

An even bigger threat looms for businesses that use armies of IoT systems to run daily operations. Imagine an entire production line being shut down if an attacker did not receive the demanded ransom payment.

There are, of course, additional complexities in a ransomware attack against IoT, ranging from communicating with the victim on a device that has no screen and overcoming the

many network layers of IoT systems (including the cloud, edge, and fog). Attackers will have to be more creative, but the threat is real and cannot be ignored.

Ransomware is becoming more common among smaller companies, and even individual homes. An attacker can take control of personal IoT devices and block their use or alter the data captured by the device. This can have serious consequences for such devices as connected cars, smart home controls, and medical wearables.

2 CRYPTOCURRENCY ATTACKS AND BLOCKCHAIN TECHNOLOGY

Many people equate Blockchain technology with Bitcoin, but there's a lot more to it than just cryptocurrencies. Blockchain has many characteristics attractive to IoT designers, such as tracing provenance of data, and there are even those who see a role for cryptocurrency in IoT (micro payments at the device level, for example). Blockchain is believed by many to be "unhackable" (which is debatable), creating a false sense of security.

The reality is attackers frequently target the software that is running the Blockchain network, wreaking havoc through:

- Cryptomining attacks (also known as "cryptojacking"), in which "miners" (software that uses special algorithms to mine for coin) are used to gain access to someone else's mining software and reroute data or currency to their own account.

- Attacking cryptocurrencies by flooding the network with extra coin to devalue the currency.

Cryptomining only requires a few lines of code, making it difficult to detect. It is seeing a huge jump in occurrence rates, with a staggering 8,500 percent increase in coin mining detections in 2017, according to the 2018 Symantec Internet Security Threat Report.

Blockchain technology is also assisting with the management of IoT devices by creating a decentralized system that provides scalability and security. Several companies are already putting the union of Blockchain and the IoT to work. Waltonchain uses Blockchain, IoT, and RFID to manage the supply chain. Internet Token Node (ITN) is a decentralized system that uses Blockchain technology to assist IoT devices and machines to connect.

3 PIVOT POINTS

In this type of attack, the IoT device is not what is valuable. Rather, the attacker uses the IoT device to gain access to the larger network, which may contain sensitive data.

An example is the breach suffered by the Target retail store chain, in which the HVAC system was attacked to infiltrate the point of sale system containing customers' debit and credit card information.

IoT applications built for seemingly insignificant functions such as heating and cooling systems can let developers slack on security measure. It's just an HVAC system after all, right? Wrong. This is a major threat to the rest of the network.

4 SUPPLY CHAIN ATTACKS

A supply chain attack is a cyber attack that infiltrates your network by exploiting a less-secure point in your supply chain. They come in two forms—hardware and software—and Symantec found they increased by 200 percent in 2017. Companies often do not realize supply chain partners have been compromised until it is too late and damage has already been done.

Hardware supply chain attacks are important if you get any of your hardware from a third party. This is more prevalent in high-end devices such as servers and routers, and less so in lower-level devices for IoT, but it can happen. And when it does, it is significantly more dangerous because it is harder to detect and protect against.

The hardware supply chain attack launched by China that affected a number of large American companies (including Amazon and Apple) is an example of how far-reaching and serious this type of attack can be. This was discovered almost by happenstance: Amazon detected tiny microchips that had been added to server circuit boards, as a result of in-depth (and expensive) due diligence it was conducting on a company it was looking to acquire. However, most companies cannot afford to do this level of testing and investigation.

Software supply chain attacks are also of concern when an IoT system uses third-party libraries or frameworks as part of the software development. These are also difficult to detect if proper security testing is not performed.

5 OVER-THE-AIR UPDATE ATTACKS

Over-the-air (OTA) update capabilities allow you to remotely update hardware settings, software, or firmware. They are great for adding new features to IoT applications, and in fact this capability is critical for sending out necessary security patches.

But an OTA capability can also open your IoT system to attack. Attackers can use the over-the-air update mechanism to get into your system and change the way your IoT device works.

The necessary nine: IoT security solutions

1 MAKE SECURITY A PRIORITY FROM DAY ONE

Use chips and board components that are capable of increased security functionality, such as Intrinsic ID and ARM. Only add pieces to the board that are necessary. Anything in excess is just another piece open to attack.

Use secure coding practices, running frequent software scans and security tests. This can be accomplished within the Agile Continuous Integration process with the right tools.

Proper scanning and security testing require the use of a combination of testing tools, such as Static Application Security Testing (SAST) tools and Dynamic Application Security Testing (DAST) tools. Sorting through the results from all of these tools can be cumbersome and slow development down—unless you can quickly correlate them into a single report that is easy to digest. We use an automated application vulnerability management tool called Code Dx.

Code Dx processes the results from all of your scans and removes the duplicates. It identifies which vulnerabilities were found by more than one tool and allows you to set priorities based on severity. Code Dx already includes a number of open source SAST tools and supports many commercial tools as well.

Even more importantly, it integrates with the environments our developers are already using. We have integrated Code Dx with our Visual Studio development environment and our Continuous Integration servers, Jenkins and TeamCity.

Our team members do not need to go to an additional location for security issues. They receive alerts on issues within the tools they are already using, and we can continuously monitor security as we work. Using this tool allows us to keep security as a main concern without slowing down development time.

2 IoT AUTHENTICATION

Authentication can be as simple as a username and password or a more complex two-factor verification process. IoT authentication is often done through embedded sensors, removing the need for human interaction.

There are many secure IoT authentication methods that are easy to implement. The caveat is that many—such as Secure Boot and Trusted Platform Module (TPM)—require more powerful hardware or special chips. This increases the cost of your end product, but the risk it eliminates is worth the investment.

A cheaper product that is easily attacked will cost your business more money in terms of lost customers, legal fees, and a tarnished reputation. A more secure device can be marketed as such, educating the buyer to the dangers of cheaper, less secure alternatives.

3 IoT ENCRYPTION

Encrypting data between IoT devices and back-end systems keeps data safe from attackers. Encryption (as with authentication) requires more computing power. It is worth the extra cost to add more security to your IoT device.

Earlier this year, researchers at MIT developed a tiny chip suitable for IoT devices that can perform public-key encryption using 1/400 of the power required by software execution.

The National Institute of Standards and Technology (NIST) developed an initiative for lightweight cryptography to address the challenges of securing data in IoT devices with limited computing power. In April of 2018, NIST called on software developers to help compose guidelines and standards for IoT encryption. With standards on the way, developers should consider quality encryption a requirement.

4 IoT NETWORK SECURITY

The network that connects IoT devices to back-end systems must be secure. Network security is more challenging with IoT applications because there is a wide variety of standards, devices, and communication protocols involved. The result is that IoT devices are often placed on less-secure networks that do not provide enterprise-level protection.

There are also, typically, other IoT devices on the same networks, creating more opportunities for security vulnerabilities. One device may be used as a pivot point to get into other networks, as in the Target case previously mentioned.

IoT network security demands in-depth attention during design and deployment. Developers need to create more-secure IoT devices, but deployment cannot be based on the assumption that the device itself is secure. In fact, deployment should be based on the understanding that the device may not have been developed in the most secure manner.

Firewalls, antivirus, and intrusion detection and prevention systems should be used to create a secure IoT network. If the device is successfully attacked, it should not compromise the entire network. This is how you achieve in-depth, compartmentalized security.

5 IoT PKI

As cloud-based communications and data storage continues to rise, more data is traveling between the cloud and IoT devices. Customers expect that their personal data will be safe during transit. This includes data confidentiality (access is limited to authorized users) and integrity (data is accurate and consistent).

Public Key Infrastructure (PKI) delivers this transit security. PKI is a digital certificate that provides encryption and authentication via a third party. Each digital certificate is issued by a Certificate Authority and is based on cryptographic keys to create a unique and strong credential without the need for passwords, tokens, or other clunky verification.

PKI is needed to make sure the data is encrypted properly. Usage is on the rise thanks to IoT, with a recent survey finding that 44 percent of IT and security employees identify IoT as the main driver behind PKI adoption. Again, this is worth the investment for secure communications between IoT devices and platforms.

6 IoT SECURITY ANALYTICS

IoT security analytics involves thinking about not only how to create a secure device, but how to monitor and fix it when something goes wrong. This is starting to receive more attention at the enterprise level, but it needs to trickle down to commercial devices.

More exploits could be avoided if more attention was devoted to IoT security analytics. We expect this area to grow in the coming years. In its *Internet of Things Security, 2017* report, Forrester stated that IoT security analytics will be necessary for detecting threats and attacks missed by more traditional network security solutions.

Developers need to build in the ability to monitor security, so that an alert is generated in real-time when something goes awry. Alerts and reports can help developers correct issues quickly and prevent them from happening in the future.

It is also important to avoid "alert fatigue." This occurs when your team gets too many notifications of potential threats, is unable to handle them, and ends up feeling overwhelmed and doing nothing.

Proper IoT security analytics requires gathering and analyzing data from IoT devices, networks, and the cloud. A baseline must be formed so that anomalies can be properly identified. This allows you to isolate aberrations that may be a threat to your IoT applications and network. You may discover that a device is not functioning as intended, or that the network is suffering from poor performance.

Adding Machine Learning (ML) and automation to your analytics speeds up the process, and helps identify which potential vulnerabilities pose the highest threats and should be investigated further. You can, for example, decrease the time required for analytical processing by using advanced ML algorithms to identify "bad" files, which can be flagged for further investigation.

7 IoT API SECURITY

Representational State Transfer (REST) Application Programming Interfaces (APIs) connect devices to the internet. APIs are another way for an attacker to connect to your device and access data.

In 2016, Nissan's electric car—the Leaf—was easily attacked through a poorly secured API. All an attacker needed was the VIN number to control functions of the car, all because the API endpoint was not secure. This is not good for customers, and certainly not good for sales.

Only authorized devices and applications should be communicating with APIs. An attack (or a potential threat) needs to be detected immediately.

Authentication, encryption, and PKI can all be used to enhance API security. We also recommend incorporating security into the design, development, and management of APIs. API security policies and procedures must be enforced. Version management is also important: aging and redundant versions of your firmware should be identified and removed through an API audit process.

8 IoT SUPPLY CHAIN SECURITY

Exercise caution when using third-party hardware suppliers for your IoT applications and devices. Make sure they have a reliable reputation.

Do not always opt for the cheapest provider. Ask questions about the supplier's security policies and procedures, so you can determine if they meet your standards. You should still validate the parts you receive, of course. If you have the means to inspect every piece of hardware, then do it. Otherwise, randomly select a percentage of components and inspect them to make sure there are no extra pieces on them. They should be identical to the specifications you submitted to the vendor. You're probably doing this anyway for quality control, so you might as well check for security issues while you're at it.

Software supply chain security is achieved only when using trusted third-party libraries and frameworks, and scanning all third-party components for security vulnerabilities. This is where application vulnerability management tools such as Code Dx keep development moving along while keeping security well-integrated in the entire process.

9 OVER-THE-AIR UPDATE SECURITY

Over-the-air updates must be fully controlled by the developer and the customer. One way to exert this control is to require the customer to physically press a button on the device to allow an update to happen.

Another approach is through Virtual Private Networks (VPN). VPNs can create an encrypted tunnel between the device and the network for transmitting the software update.

All updates should be done though encrypted communication channels. Cryptography can be used to make sure the updates are from a verified author, and have not been altered in any way during transit.

We recommend using Secure Boot. This is a hardware feature that is set up to authenticate code using security credentials and cryptography. It makes sure that only verified and legitimate changes are made to the device, and establishes what is known as a "root of trust."

Practice makes perfect: Practical tips for IoT device security

The Online Trust Alliance (OTA) is an Internet Society Initiative dedicated to improving online trust and user empowerment through best practices relating to ethics, privacy, and data. OTA developed a checklist to help enterprises more securely manage consumer IoT devices.

There are several items on the checklist worth mentioning, and we have a few additional tips to add as well.

- Change all passwords to strong passwords, and use multi-factor authentication where possible.
- Never use default passwords when deploying an IoT system.
- Place IoT devices on a separate network that is firewalled and monitored. This will help protect against pivot point attacks.
- Disable unnecessary functionality, such as cameras. The more things you add, the more you need to protect. You're just creating more doors to welcome attackers into your system.

- Encrypt data that is being transferred when possible. Many IoT devices are not capable of encrypting data while it is sitting on the device. It just requires too much power and space. However, an increasing number of chips and boards are becoming capable of encrypting data while it is in transit, and this is where the data is exposed to attack. Data being sent up to the cloud or across internal networks must be protected through encryption so it can only be read by the intended recipient.

- Update firmware and software automatically, or as frequently as possible. Frequent updates are particularly important when it comes to zero-day attacks: those that exploit a vulnerability that was not previously known to exist. You can't afford delays when it comes to security patches and updates. It is just not worth the risk.

The full OTA checklist is available here for further reading.

Conclusion

The best protection is prevention. Integrate security into your design, development, and deployment process so that your IoT devices, applications, and networks are secure from the start.

Investment in IoT security has a strong return, translating to increased revenue and a positive reputation in the marketplace. If your team lacks the expertise needed when it comes to IoT security, reach out for help. An experienced group of professionals can make sure your IoT application is secure from end to end, providing the comprehensive coverage you need for success.

Software Design Solutions (SDS) provides embedded system and Internet of Things (IoT) software development, desktop application development, and software process improvement consulting. Software Design Solutions is also able to provide temporary software engineers for projects greater than the scope of its clients' abilities and to provide experienced programmers to companies who need to focus on other lines of business.

Sam Fahnestock is the Engineering Manager and lead security engineer for Software Design Solutions. As engineering manager, Sam coaches all team members across the company on implementing the Agile mindset, and as the lead security engineer Sam plays a vital role in incorporating security into projects across SDS. Prior to working for Software Design Solutions, Sam spent 9 years working in cyber security for the Air Force.

software design solutions

an applied visions company

Software Design Solutions, Inc.
4091 Saltsburg Rd. Suite S
Murrysville, PA 15668
412-282-8700
info@softwaredesignsolutions.com