The Internet of Things Requires Enhanced Security
Guidelines for the Future

Erik Miller, Treemont Haga and Chen-Chi Shing*
Department of Information Technology Radford University Radford Virginia, USA
*Corresponding author

Keywords: Internet of Things (IoT), OAuth, RFID, RIOT OS, Spark OS.

Abstract. The Internet of Things (IoT) is a relatively recent technological and economic trend that involves using computers, microcontrollers, and RFID to collect and analyze data, as well as perform tasks and services. An IoT device represents a real-world entity. These devices have the ability to create new business and employment opportunities, but they must be secure. These devices may serve a business function, or used on a consumer’s home network. There are various layers of security in an IoT system: Network, Interface, Authentication, and Physical. The device must not be vulnerable to attacks in these layers. Only authorized users should be able to access the device or the service. The device must also be protected from weather and theft. These four aspects serve as a baseline for securing an IoT device.

Introduction
The IoT is an economic event as well as a technological one. What started as a method of automation, grew into an industry built up around the collection and analysis of data. The IoT can be thought of as everyday objects that are made into wirelessly connected devices. These objects are given computing ability and sensors which record data. These data are used by companies to sell a service to consumers. Data are recorded autonomously, without the direct involvement of any person. Since these devices are connected to the internet they come with many security risks. These security vulnerabilities and weaknesses have the potential to cause personal damage to many consumers and that is why it is crucial that these devices are secure.

History
Definition and Background
The origin of the IoT can be traced back to the 1970s. Meters on the electrical grid could be monitored remotely through the telephone lines. During the 1990s, closed wireless networks were used on an enterprise-level to allow machines to talk to each other, using proprietary technology [1]. These machine-to-machine communication solutions were not designed for communication over the internet, but it was the next logical step.

In the early 1990s, people began to use Internet Protocol to connect devices other than computers to the internet. The first internet-enabled device was a toaster [1], which could be controlled over the internet. During the following years, many other devices and objects were internet-enabled, and this laid the groundwork for the IoT. In 1997, Kevin Ashton coined the term “Internet of Things”. He was describing the use of radio frequency identification tags (RFID) to fully-automate the process of tracking inventory. RFID requires three parts: a scanning antenna, a transceiver, and a transponder, which is programmed with information [2]. The transponder takes the form of a tag which is affixed to an object. The tag receives an electromagnetic signal from the broadcast, which it stores and converts
to energy. The energy is harvested to broadcast information back to the antenna using a process called inductive coupling.

Ashton has a vision: “We need to empower computers with their own means of gathering information, so they can see, hear, and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world -- without the limitations of human-entered data.” [3] To Ashton, computers are much more useful to humans when they are more autonomous, because humans are busy and less precise than machines. A computer, which is fast and accurate, could efficiently capture more data than a human can. The person could then focus on data analysis rather than data collection.

Another type of “smart device” may connect to a network using Internet Protocol. IP provides a unique address to a device, which contains information about an object. Information is encoded and decoded via data packets sent over the internet. Since IP is so robust, fast, and standardized, it has had a significant impact on the IoT. Unlike RFID, information can be requested and sent without the need of a sensor, and there is no need to be close to the receiver.

**Popularity and usefulness**

Using methods to fully-automate tasks with remote management isn’t new, so why is it so popular today? There are several probable reasons, most notably the widespread adoption of IP networking. Computers are now smaller, cheaper, and faster than ever before, and can be embedded in all sorts of things. The expectation of internet connectivity drives new demand and opens newer market opportunities. Data-collection algorithms and data-storage methods allow for companies to build new products and services around these data, gathered by sensors built into a “Thing”. According McKinsey & Company, there are nine settings of a Thing [1]: Factories, Cities, Human, Retail, Outside, Work sites, Vehicles, Homes, and Offices. Each of these classifications offer a unique angle to economic development using the IoT.

**Identifying Security Vulnerabilities and Weaknesses**

When it comes to the IoT, security should be a top priority. Since these devices are made up of computer systems and technologies that are already in use, these interconnected devices inherit the security vulnerabilities of today’s technology. Are we ready to trust a network of autonomous, connected devices? There are security flaws we need to address before deploying IoT devices.

**Network Security**

Think of a connected, automated device that has no defense against other entities on the Internet. Network security is a huge issue with the IoT that could put many lives at risk. Allowing a device to communicate by sending and receiving signals is a powerful thing that can be heavily abused and exploited. It is highly important that these devices are kept secure when in use over a network.

As devices connect to the Internet, new opportunities to exploit potential security vulnerabilities grow. Poorly secured IoT devices could serve as entry points for attack by allowing malicious individuals to reprogram a device. Poorly designed devices can expose user data to theft by leaving data streams inadequately protected. Failing or malfunctioning devices can also create security vulnerabilities [4].

Attackers are using Denial of Service and/or Brute Force attacks more often to gain access to networks[5]. The issue looking forward is that the IoT is ill-equipped to handle or mitigate such attacks. That should be the main focus for the future of network security when it comes to the IoT.
Interface Security

It is important that any kind of operating system or software on a device is highly secure so that data stays private. Software issues need to be addressed for the IoT to be successfully secure.

IoT devices can be different than standard computers. At times they are simply microcontrollers that respond to a RESTful API. Such is the case for the Particle.io platform. Particle’s cloud-based Spark OS handles the routing and flashes machine code to the device using an http PUT request. Each device is managed with Spark OS through the web and is given a unique id number. Users’ client applications must have an access token to use the API.

There are benefits and vulnerabilities to this approach. While it is secure to keep access to the resources bottlenecked with authentication, those resources are all shared by the servers. An attacker who breaks into Spark OS could theoretically generate a random id number and use a compromised access token to send a PUT request to a device with malicious code.

Authorization and Authentication

An automated device can communicate over the Internet without knowing the received data is from the intended entity. How does the device know it is not sending data to an attacker? Identifying the true owner of a device is critical to maintaining overall IoT security.

Authorization and authentication takes place in both the networking and software elements of an IoT device. However, both elements are lacking sufficient approaches to this issue and must be addressed. For this task, an IoT device is likely using OAuth. OAuth is an open-source authentication standard that is in use by many large companies such as Google, Twitter, and Facebook. An authentication middleware layer provides a means to filter out illegitimate clients.

OAuth relies on a few concepts: A Server that holds resources and restricts access to them, a User that will own resources on a server, a Client application will attempt to access the resources, Client Credentials, comprised of a public and secret key, and Token Credentials which are distributed to trusted clients. OAuth is achieved in a specific sequence of steps [7]. The user must sign up for a consumer key and secret on the server. A client requests access to the server’s resources. The server provides a temporary request token, which grants access to the server’s authorization end-point. The user must enter his or her credentials. The client is then verified and the temporary access token is traded for a user access token and secret. The token is passed to the client and used to access the resources on the server.

A client application is only granted access to a server’s resources if it can pass through two layers of access: one for temporary verification and one that checks the client’s credentials. Even then, the client must prove it has been verified with each subsequent request. However, this system does not guarantee that a client is not malicious, and its effectiveness relies on its implementation.

Physical Security

Consider a device that is physically durable but has exposed ports or other facets for optional attachments. Limiting a device to what it ultimately needs to function is another goal that needs to be met. You also want to make sure the device is durable enough to stand the tests of time. Giving your device the proper physical care against the elements and attackers will ensure the devices use and longevity. Depending on what kind of device it is, it may require unique physical defenses for that specific device.

The physical security industry must exercise caution in developing and manufacturing products for the IoT. More data sharing inevitably means that a security breach on one device or system could result in vast amounts of data from many systems and devices being compromised. In fact, HP recently reported that up to 70 percent of commonly used IoT devices are vulnerable to cyber-attacks. Another
point for the industry to consider is the likelihood of new laws being developed to protect the end user’s privacy, specifications to which the industry must adhere [8].

For example, it would be a huge risk to equip an IoT device with exposed USB ports or Ethernet ports with the only exception being a power port for battery life. That means all communication must be done wirelessly, even the transfer of data to and from a device. Figure 2 shows an example of how an IoT device should not look on the outside [9].

**Safeguards Against Security Threats**

**Network Security Safeguards**

The IoT needs to have a more secure approach to communication over the Internet, otherwise data could be compromised. Specific network security safeguards should be put in place to protect data. These devices must be equipped with the most modern network security provisions and must defend against the most common attacks. Firewalls or multiple firewalls would be an excellent start to protect an IoT device.

Another measure is to ensure that a device is able to use SSL. However, there is a problem depending on the IoT device in use. There is a memory requirement to using SSL, because long certificate chains will take up potentially more memory than the device can allocate.

Without securing the data transmission, attackers can learn about specific implementation details of the system. Certain parameters passed along the query string may be viewed without encryption.

**Interface Security Safeguards**

An up and coming operating system called RIOT has become a promising vision of what software security stands for. From the ground up, the developers set out to make the most secure operating system for the IoT. The RIOT operating system uses an advanced real-time Kernel for wireless sensor networks to detect potential threats as they happen to allow for quicker reaction time. It houses the FireKernel, which is designed as a true microkernel, providing it with only essentially necessary features like scheduling, inter-process communication and synchronization [10]. This allows devices to make quicker decisions, therefore stopping and preventing attacks.

**Authorization and Authentication Safeguards**

While OAuth is a good method to deflect a malicious client, there are some vulnerabilities. Firstly, the authorization layer is only as effective as its implementation. Second, OAuth’s goal is to verify a user, not to verify a server. Third, a token is encrypted, but any other request parameters may not be. An eavesdropper may be able to learn vital information about the implementation of the authentication layer, which could in-turn provide a means to brute-force attack the server [7].

It is good practice to make sure that tokens and secrets stored on the server are long and random. OAuth was designed primarily for insecure communications, and pairing with SSL is an ideal way to prevent eavesdropping. Utilizing a nonce (a number used only once) can help add more variability to the signature of the client’s requests. This would mean adding a random number to the request that is regenerated after a certain period of time [7]. The system could even generate random tokens that are used as a mask for a user access token, but are linked to the token bearer. The user’s client would be issued a new, random, temporary token after a certain period of time.
Physical Security Safeguards

Physical location plays a vital role in securing an IoT device. It restricts possible entry points to an IoT device by keeping communication between devices wireless. This allows us to focus effort into making sure wireless communications are protected.

To solve this problem, we need to make sure all IoT devices have only one physical connection. The only physical connection a device should have is the power supply or a battery recharge port, limiting potential damage and accessibility. However, that does not mean all physical attacks can be prevented.

A system needs to be in place that sends a warning or alert to the owner of the device if it were to become damaged or manipulated without the owner’s authority. A series of sensors could be in place to check for suspicious activity around a device once it has been deployed.

Management of Interconnected Devices Moving Forward

The constant stream of new, connected devices is overwhelming. Discovering a method to effectively monetize and manage IoT devices, keep track of their data, and maintain security is going to be a serious, monumental task. However, maintaining and securing IoT devices has the potential to create millions of new jobs in the IT industry.

In a recent survey done by DevicePilot, fifty companies planning to deploy IoT applications were polled to see if they had the proper device management resources. “It is clear that most IoT companies are currently managing their connected products manually or by a mixture of manual and automatic processes,” said Pilgrim Beart, CEO at DevicePilot. “But as projects move from pilot to deployment at scale, the time and operational cost of manually logging-in to each device to perform an upgrade or check if it is working becomes a major barrier. Automatic asset management, monitoring and lifetime support are essential for the long term success of the IoT.” [11]

Not only will this impact the IT industry but it will impact the entire world. A security research and software development engineer at Tripwire named Lane Thames wrote, “The Industrial Internet of Things will drastically change the future, not just for industrial systems, but also for the many people involved. If we can achieve the full potential of the Industrial IoT vision, many people will have an opportunity to better their careers and standards of living as a result of countless value creation opportunities.” [12]

Conclusion

Since these devices are connected to the Internet they come with many inherent security risks. These security vulnerabilities and weaknesses have the potential to cause personal damage to many consumers and range from network security to the device’s own physical layout. That is why it is crucial that we secure every aspect of these devices moving forward. These guidelines would greatly improve and make using smart devices a lot smarter.

References


