IoT Security

By Thomas Rind, ECE '18

Introduction

Devices with Wi-Fi capabilities are becoming more widespread and cheaper which is providing the opportunity for this industry to bloom. But security for these devices has sometimes been largely ignored. It will be harder to scale to the level of security needed as more devices come online. Any device that can connect online is susceptible. Hackers can gain control of a device and use it for their own purpose. This in fact happened in 2016 when DNS provider Dyn was hit by a distributed denial of service (DDoS) attack. Normally these attacks are windows desktop PCs infected with malware, but in this case it was a botnet of IoT devices (Sims, 2017). This attack brought down sites like Twitter® and Spotify® and many more all because the security on these devices was not good enough. What makes IoT security not as modernized as it should be is because it involves many different devices with different protocols, all of which have limited memory and power. There is usually three layers when talking about IoT security. The perception layer, the network layer, and the application layer.

Architecture of IoT Security

Perception Layer

The perception layer is the physical hardware and communication over wireless channels. This layer contains 3 main security issues; the strength of the wireless signals can be affected by other signals, the sensor nodes can be tampered with, and the inherent nature of the network topology (Mahmoud 2016). A device can be disconnected from the network by moving it around or blocking it with interfering signals. Alternatively, someone can physically affect the sensors. The sensors can be broken or given false data. Systems will develop incorrect behavior models because they are learning from incorrect data (Green 2016). Machine Learning depends on correct information and small changes to the data can corrupt a learned behavior.

For our project the physical shelf and accompanying raspberry pi are in this layer. While shelf must be able to learn from the food placed on it, the bigger vulnerability is the raspberry pi. Most devices come with a default password and username which must be changed. In addition, someone could insert a USB with malicious code that grant them access to the raspberry pi.

Network Layer

The network layer is responsible for connecting all devices and transmitting data to other layers.

The most common attack to this layer are DDoS attacks, but this layer is also responsible for protecting confidentiality and privacy of users. (Mahmoud 2016). An attacker with access to a network can use sniffing applications to steal data (O'Gorman, 2017). The whole system can be compromised if the keying material is eavesdropped (Mahmoud 2016). An attacker with privacy keys can act as the device to other devices and receive and send data. Securing this layer is also tough because devices need to be compatible, and older devices are less secure. Current network protocols are made from many old and new components which make securing this layer even more difficult (Mahmoud 2016).

For our project we are on an unsecure network so we are at a large risk here. While the raspberry pi is password protected, the data can still be sniffed. Private home networks only have to worry about the network being brought down or its identity being spoofed.

Application Layer

The application layer is responsible for passing messages to other devices through protocols like MQTT, COAP, RESTFUL, etc. (Asim, 2017). The Application Layer has many issues do to the lack of a standard. There are different authentication mechanisms between applications, if many devices are connected then the application will have trouble staying available online and allowing users to control the data they want to show and hide (Mahmoud 2016).The many different authentication methods makes communication across applications difficult, The application must also be able to scale with the devices connected to it. A server can crash from too many devices sending data to it. Finally, the users need to have the tools to control their data, so they can protect their own privacy.

The protocols used all require different resources and power usage which can limit what devices use them. The MQTT protocol uses publisher/subscriber architecture and has lightweight CPU and memory usage (Asim, 2017). This allows more devices to use it and since it is publisher/subscriber architecture, a single device can easily send a message to many devices. The issue about this protocol though is that the MQTT subscriber must support TCP and have a connection open at all times with a broker (the server that the publisher sends data to) (Asim, 2017). Data sent with MQTT can be encrypted, but the protocol itself does not do that. On top on that MQTT protocol doesn't provide authorization, which is instead handled by the MQTT server (Mendez, 2017). The data's integrity can be in question when handled by the MQTT server. CoAP (constrained application protocol) is low power and memory and uses UDP instead of TCP. CoAP uses client server architecture so it cannot communicate to many devices at once.

The raspberry pi microcontroller has a significant amount of processing power and is always plugged in. It can use MQTT which integrates with Amazon AWS IoT. Amazon AWS requires devices to have credentials which are stored on the device and need to be protected in the perception layer. AWS also requires the data be encrypted using TLS (AWS IoT, 2018). By using TLS data from a device can be securely transferred to an AWS lambda function or database while maintaining its privacy and integrity.

Current Issues and Solutions

Data Confidentiality, Integrity, and Availability

When messages are sent between devices, they need to be properly encrypted to ensure confidentiality. Maintaining confidentiality as grown increasingly tougher as different types of devices, networks, protocols, etc. have been introduced. Each node in an IoT network is susceptible. If the data sniffed is authentication data, the whole system becomes compromised. On top of encrypting data, the physical device needs to be in a tamper proof area. An attacker with physical access to the device can damage or break into it (Khan, 2018). If the default password and username are not changed, then it's only a matter of time the confidentiality is broken.

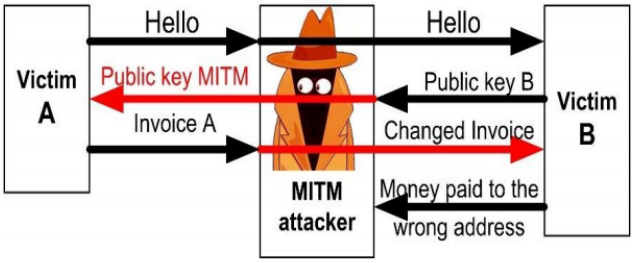
The integrity of the data is also important. Data can be faked, but also authentication can be denied. The end node will not grant access to a device with an altered certificate, which is good because it protects from other threats but denies the device access to the nodes services.

Data can be lost when a system is not available . A system could be brought down by physically breaking it, DDoS attacks, or signal interference. A jamming attack could be done on our interface, that could prevent the raspberry pi from communicating with AWS (Khan, 2018). There must be a way to save a downed systems state to send out an update once the it's brought back up. Since IoT devices need to have low power and low CPU usage, they cannot always be broadcasting.

Authentication

Nodes authenticate themselves to other nodes to establish trust and ensured data reaches its destination safely. Authentication must happen at each layer for each device. A problem that has occurred involving authentication include Man in the Middle (MITM), Sybil, and spoofing attacks. MITM attacks network communications protocols by posing as a legitimate node (O'Gorman, 2017). A MITM consists of an attacker circumventing normal authentication by intercepting an encrypted message from side A asking side B for its public key. The attacker forwards the message to B and

then B sends the attacker its public key. The attacker forwards B's response to A and A thinks the line is secure. A then sends its encrypted data to B (Cekerevac, 2017).



(Cekerevac, 2017)

MITM attacks can happen because of several reasons. Several reasons include that a connection is unsecure, the embedded system is not updated, or the device has root privileges when it shouldn't (Cekerevac, 2017). Our raspberry pi needs to be moved to a password protected network with updated account privileges because it is currently on an unsecure network with root privileges on its main account.

An attacker can spoof an RFID signal to read and record data transmission from an RFID tag (O'Gorman, 2017). This could used to gain access to buildings and devices by faking an identity. Ways to prevent this is to use RFID with encryption and avoid getting RFID tags scanned by questionable scanners. Another spoofing attack is signaling attacks. A malicious node overwhelms other nodes with messages which increases processing time (Zhang, 2017) or falsifies data (Li, 2017). Sybil attacks are similar to spoofing except in a Sybil attack the attacker acts as multiple nodes while in spoofing the attacker acts as a single node (Chen, 2010). An attacker can be refused authorization once they are detected. Some ideas that have been brought forth are measuring a signals strength for their mac address, deploying detector nodes to determine a sender's location (Khan, 2018). Our raspberry pi needs to be physically protected so attackers can not take the certifications stored on the pi.

Future of IoT Security

New techniques will be made because hackers will always find ways around all security techniques. Since the security of today is repurposed from older standards, newer IoT security will take a more systematic approach. The architecture will need to change using microservices for lightweight containers instead of virtual machines. This will allow workloads to be more efficient and resources easier to deploy (Radovan 2017). This technique will scale better to help deal with large amounts of traffic that devices might occasionally send. IoT standards will need to be set so communication between applications, devices, and users can be more secure (Mahmoud 2016). A standard authentication across many devices makes it easier to establish trust across many devices.

Physical Layer Solutions

One proposed way to detect jamming is by measuring the signal strength and location of the nodes (Khan, 2018). Issues that may arise from this is that it requires some extra computation from the device, which may not be able to give the resources. Devices must be initialized properly which means changing default logins and removing debugging tools. To ensure there is no eavesdropping there must be a minimum data rate (Khan, 2018).

Physically a device needs to have few interfaces. The raspberry pi's USB ports are a vulnerable point. If a device needs to have a USB port, then there should be ways to lock and unlock it when necessary.

Network Layer Solutions

Attacks that trick devices to repeat sending important data in 6LoWPAN can be alleviated by including timestamps and nonce options in fragmented packets to prevent redundant responses. (Khan, 2018). In order to prevent insecure neighbor discovery Elliptic Curve Cryptography(ECC) can be used (Khan, 2018). This will encrypt the data and use smaller packets compared to non-ECC methods. A social graph could be made of the network to detect Sybil attacks (Khan, 2018). This would have to be implemented on a device that can handle this and not the specific IoT device.

Application Layer Solutions

Interfaces need strong passwords and should be tested against injection attacks (Khan, 2018). Data should follows certain formats and cannot be altered. Detecting if data is in the form of a cross site scripting for SQL injection attack can prevent

the layer from being compromised.
A middleware server could also act to communicate between many heterogeneous devices to standardize communication (Khan, 2018). A standard gives many layers of security.

Conclusion

IoT is an ever-expanding field and provides many opportunities to integrate various applications.
The security of this industry should not be ignored. There has already been a major botnet attack using IoT devices, and issues from this attack still exist. In addition, devices are limited to their memory, power, and CPU usage. Security can currently be improved by making sure the device is on an encrypted password protected network, is using protocols that include encryption, has ways to authenticate other nodes if it needs to communicate, and is only accessible to trusted users.

References

1. Asim, M. (2017). A Survey on Application Layer Protocols for the Internet of Things. *International Journal of Advanced Research in Computer Science*, 8(3). https://doi.org/10.5281/ZENODO.51613.

2. AWS IoT. (2018). Retrieved from https://docs.aws.amazon.com/iot/latest/developerguide/iot-security-identity.html

3. Mendez, D. M., Papapanagiotou, I., & Yang, B. (2017). Internet of Things: Survey on Security and Privacy, 1–16. Retrieved from http://arxiv.org/abs/1707.01879

4. O'Gorman, T. (2017). A Primer on IoT Security Risks. Retrieved from https://securityintelligence.com/a-primer-on-iot-security-risks/

5. Cekerevac, Z., Dvorak, Z., Prigoda, L., & Cekerevac, P. (2017). Internet of things and the man-in-the-middle attacks - Security and economic risks. *MEST Journal*. https://doi.org/10.12709/mest.05.05.02.03

6. Zhang, P., Nagarajan, S. G., & Nevat, I. (2017). Secure Location of Things (SLOT): Mitigating Localization Spoofing Attacks in the Internet of Things. *IEEE Internet of Things Journal*, *4*(6), 2199–2206. https://doi.org/10.1109/JIOT.2017.2753579

7. Li, S., Xu, L. Da, & Li, S. (2017). Security Requirements in IoT Architecture. In *Securing the Internet of Things* (pp. 97–108). Elsevier. https://doi.org/10.1016/B978-0-12-804458-2.00005-6

8. Chen, Y., Yang, J., Trappe, W., & Martin, R. P. (2010). Detecting and localizing identity-based attacks in wireless and sensor networks. *IEEE Transactions on Vehicular Technology*, *59*(5), 2418–2434. https://doi.org/10.1109/TVT.2010.2044904

9. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395–411. https://doi.org/10.1016/J.FUTURE.2017.11.022

10. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2016). Internet of things (IoT) security: Current status, challenges and prospective measures. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 336–341. http://doi.org/10.1109/ICITST.2015.7412116

11. Radovan, M., & Golub, B. (2017). Trends in IoT security. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1302–1308. http://doi.org/10.23919/MIPRO.2017.7973624

12. Sims, G. (2017). IoT security – what you need to know (Gary explains). Retrieved November 12, 2017, from https://www.androidauthority.com/iot-security-gary-explains-72