Security of IoT Devices

The network of home devices is the concept of establishing a web of connections using SMART devices in the household. These devices, a part of the Internet of Things (IoT), have expanded the idea of interconnectedness on the internet. As technology progresses, more devices are given the capability of connecting to a network, creating convenience for users. Within a household specifically, SMART appliances such as washers, dryers, refrigerators, and TVs can connect to a network via Bluetooth, Ethernet, or Wi-Fi. Although the benefits of IoT devices are significant, so are the potential downsides that can be created when improper implementation of protocols used to communicate information among networks are used. As millions of devices connect to the Internet daily, it is important to measure the security of these connections. Not uncommon to find, a popular trade-off exists between security implementation cost and actual security levels. In this research, we study proper security implementation of connected household electronic devices and whether these SMART devices follow said protocols to safeguard transmitted data.

Keywords: Internet of Things, Lightweight Cryptography, Security Trade-off, Wireless Protocol

Introduction

The Internet of Things (IoT) is an expanding concept of interconnectedness. It allows small and medium sized devices to simplify and secure tasks typically done on a day to day basis. These devices have a wide range of uses in the field and often handle user data. Due to this, these devices must have a way of securing data while at rest and in transmission.

Over the past decade many breaches have happened at companies around the world, due to improper implementation of security. Although some of these breaches did not occur due to an IoT device, the ideas relate back to the concept of a connected device. If a device transmits sensitive data over the internet, through Wi-Fi or Ethernet, it must follow proper security channels to do so. However, there is a problem with using

traditional protocols and standards with IoT. Some of these devices have low resources that make it impossible or inefficient to use the standards specified by well-known agencies.

Research within this field is growing, highlighting several factors from hardware and software cryptology to operating system usage across different devices. This paper aims at consolidating a small portion of the ideas already presented out in the field.

It is important to mention the contributions of other researchers in this field. Although some of the concepts will be mentioned in the following sections, this piece will help identify the key concepts that helped push this paper forward. Regarding lightweight encryptions, McKay and partners created a NIST report that details the necessary standards lightweight encryptions should have [1]. Leander and partners details a lightweight variant of DES [2]. Bogdanov and partners detail PRESENT, a lightweight encryption available for use [3]. Katagi and partners created a general overview report regarding lightweight cryptography [4]. Russell and partners have a key management cheat sheet important for encryption key management [5]. Regarding protocols, there are a variety of sources that demonstrate both vulnerabilities and information. Valerio and partners talks about network risks and why data communication in IoT requires the proper protocol choice [6]. Kwon and partners talk about the proper protocol choice for the IoT device in use [7]. Beal presents definitions for Wi-Fi and what it means [8]. Mitchell breaks down the 802.11 protocol [9]. Aircrack presents information about de-authentication [10]. The definition of WPA is further explained by WhatIs [11]. Vanhoef details another attack, with key reinstallation [12]. Chacos breaks down Krack, a resent exploit project for the Wi-Fi protocol [13]. Press and Thomas talk about the security tradeoffs of IoT, and why it is important to consider such tradeoffs [14], [15]. Neagle talks about hacks for popular home devices

[16]. Alongside the security tradeoffs section, is also a discussion about endpoints, with two references by Heer and partners as well as Covington and partners [17], [18]. Regarding the SMART trend, Greenberg describes certain key aspects [19]-[33].

Lightweight Encryptions

As mentioned earlier, one of the key issues surrounding IoT devices is their capability to store data and transfer data over several types of networks. As data breaches become more common, it is important for data at endpoints to be secure. Alongside storage and transmission security, comes the idea of integrity and availability. Some attacks are not directed at stealing data, but rather corrupting the contents and bringing down services and devices. There are various methods used in the field to overcome these issues. For example, encryption can be used to secure data in transmission and at rest, while also maintaining its integrity. In terms of availability, systems are created to validate entries and restrict user input as much as necessary to protect the system.

Due to the nature of IoT devices, following the cryptography standards already in place for traditional devices such as computers, servers and tablets are at times impossible or inefficient. IoT devices have limited resources that cut the computing and processing power significantly. Some of the limiting factors include power consumption, memory availability, and often even physical size constraints. For a lightweight cipher to be successful, it must consume a small amount of energy and efficiently go through the process of encryption and decryption. Although there are numerous factors that affect how ciphers are processed, some of the most crucial factors, as defined by NIST, include key sizes, round process, key generation, and cipher block sizes [1].

Key sizes vary depending on the algorithm and the use, but for most standard algorithms key sizes range from 64 bits to 256 bits. The cryptographic community

agrees that a bigger key, when paired with a standard algorithm, leads to increased security. Unfortunately, for IoT devices that have limited power or memory this option cannot be exercised. Although a key size for lightweight encryptions has not been standardized, some lightweight ciphers have been known to use a 56-bit key. One of these ciphers, DESL, is a recreation of the DES algorithm with new security methods to work efficiently under low resource availability. To overcome the issue of a shorter key, a process known as key whitening is used to reduce the effects of cryptanalysis and add an extra layer of security [2].

For processing to be quick and efficient, the number of rounds within a lightweight encryption must be proportional to the resources available. As the S-box shrinks, so does the number of gates necessary in hardware to perform a round. Following both DESL and PRESENT, S-boxes can shrink down to use 4-bit values, versus the 8-bit seen in traditional encryptions. The number of rounds necessary to complete the process also shrinks, depending on implementation and key usage [3]. By using an implementation like this in IoT devices, the number of gates and power necessary are decreased. It also makes it easier for devices to have some form of security once deployed, without having to manage or patch it often.

For ciphers and data to remain secure, proper key management must be in place. If a cipher uses the same key for an extended period, the data becomes vulnerable to cryptanalysis and breaking, nullifying the security effect encryption provides [4]. Different agencies, such as OWASP, NIST, and FIPS have identified certain guidelines to follow depending on implementation and the data being handled. However, there are still general guidelines that everyone should follow [5].

- Generation – Based on the FIPS 140-2 standard, a key can be generated with hardware or software. There are 4 levels of security, with Level 4 being the most

secure. Key generation must have its own separate module, with a random bit generator.

- Distribution - Based on the FIPS 140-2 standard, distribution, when necessary, must be done through secure channels. Some devices do not transport keys over the air.
- Storage - An essential element to security, storage must meet a variety of requirements to be considered secure. There should be a vault, where the key is stored in an encrypted state and where all encryption, decryption should happen. Key integrity should be verified often to ensure keys have not been altered.
- Backup - For devices that have long term data storage, some form of key backup should be included. There are diverse ways to achieve this, if they meet the FIPS 140-2 standard.
- Rotation - Although it preferable that no person see clear text keys, if someone has that access, a system must be in place to track viewing and access. Keys should never be reused and should be changed, at a minimum, every 6 months.

Cipher block sizes affect the amount of memory needed to complete the process. Traditional ciphers like AES and 3DES use block sizes 128-bit and 64-bit, which may or may not work with smaller devices. NIST released a publication that mentions 64-bit and 80-bit blocks are still useable in certain IoT devices [1]. PRESENT, an ultra-lightweight cipher, uses 64-bit blocks with small rounds and small S boxes. This makes it possible to implement with even the smallest of devices.

Lightweight encryptions are a possible solution for devices that require small power consumption and efficient data output with small memory available. Some IoT devices already use these encryptions on the field and have seen promising results. To

further compare these algorithms, an analysis was conducted between AES and PRESENT. These results can be found in a later section.

Protocol Choice and Implementation

Another solution for solving the security issue is the improvement of protocol implementation. Most devices are created to use primitive protocols to speed up the data communication where herein lies the problem. Companies today don't fully understand the entirety of theses protocols and simply use them as a low cost, easy to implement method. The different Wi-Fi 802.11x standards are the protocols that are widely used that have the most security flaws. This is prevalent in the rapid progression of the cellular era as Valerio states "cellular hardware is challenged by new low-cost Wi-Fi and Bluetooth-enabled devices using wireless technologies, including standards such as Wi-Fi 802.11ah. While these new standards offer the possibility to connect many more devices at low cost, they pose bigger security challenges by operating in frequency bands that everyone can access and exploit" [6]. So, the idea here is to implement the more expensive/time consuming protocols that will ensure and safeguard IoT devices.

But before the protocol suggestions are made, it is important to understand the diverse types of connections used in IoT devices:

(1) Device to device
(2) Device to gateway
(3) Gateway to device
(4) Data system to data system

Device to device will be the focus as this type of communication deals with end to end communication with individual devices. Some examples of this communication are from television to remote, smart pad to alarm sensor and computer to computer.

According to Kwon, “TCP’s point-to-point streams often do not meet the requirements because its reliable data transmissions require multiple retries until an acknowledgment is received. That’s why a non-TCP transport layer such as UDP is desired here” [7]. In addition, using the UDP and other related UDP protocols, MQTT-SN, CoAP, DDS, eliminate header based and protocol based attacks right away making a major improvement to many devices. This point is only a small example of the idea of improving weak protocols. In the big picture, every device has very specific needs and by using specific protocols instead of cheap general all-purpose ones, will take a major step to improving the security of IoT devices.

From all the current protocols that IoT devices implement, Wi-Fi is the most common. Beal states that Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections [8]. This requires the use of an access point, or commonly known as a hotspot, which serves as the gateway between device and network. So as convenient as this may be, security takes a big hit. This data link protocol is subject to many vulnerabilities and weaknesses in today’s IoT world. Two prime examples are denial of service attacks and security protocol vulnerabilities.

Speaking first on the denial of service attack, it’s important to understand the Wi-Fi standards first. The Wi-Fi protocol abides by the IEEE 802.11x standards which today, the latest to be published is 802.11ac. With this latest standard, Mitchell describes the newest generation of Wi-Fi signaling in popular use, 802.11ac utilizes dual-band wireless technology, supporting simultaneous connections on both the 2.4 GHz and 5 GHz Wi-Fi bands. 802.11ac offers backward compatibility to 802.11b/g/n and bandwidth rated up to 1300 Mbps on the 5 GHz band plus up to 450 Mbps on 2.4 GHz [9]. This may sound great as it is an upgrade; however, there is a

problem that continues to get ignored in these new implementations. In the datagram itself, there are management frames that allow for the maintenance of communication. On in particular named the de-authentication frame, continues to get exploited with the intention to de-authenticate users from wireless networks. Unfortunately, these attacks occur quite often because this attack is very easy to implement. Aircrack-ng is a complete suite of tools to assess network security. The tool used to attack is named aireplay-ng. This is used to send broadcast or targeted de-authentication datagrams to clients effectively cutting their connection from the access point. To be more specific, this attack sends disassociate packets to one or more clients which are currently associated with an access point [10]. Many attackers continue to abuse this exploit for many several reasons. To name a couple, attackers use this to redirect users to a rouge access point that connects them to an unencrypted, or open, network to sniff or monitor traffic. Another reason used in the hacking community is for password attacks. De-authentication forces users to reconnect which gives attacks the opportunity to sniff the four-way handshake. This capture is needed to mount a brute-force or dictionary attack based on WPA password cracking.

Although this attack is dangerous, there is a solution. Depending on the device being used, Wi-Fi standard IEEE 802.11w, or the Protected Management Frames standard, may or may not be enabled or supported. This standard encrypts management frames which protects from deauthentication notices. This has already been implemented in Linux as a part of the 802.11mac driver code base but as for Windows, only Windows 7 and up have the support. Even with one of these devices, it is important to always verify. For example, typing the command “netsh wlan show driver” in a Windows command prompt, will show if the device has it enabled.

As for the security protocols, there are three main encryption standards. Wired Equivalent Privacy, or (WEP), Wi-Fi Protected Access, or (WPA), and Wi-Fi Protected Access 2, or (WPA2) which is the current standard. Sadly, as of October 16, 2017, even WPA2 has been exploited. WhatIs.com defines Wi-Fi Protected Access is a subset of, and is compatible with, IEEE 802.11i -- sometimes referred to as WPA2 -- the security standard that superseded it in 2004. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). It is based on the obligatory Advanced Encryption Standard algorithm, which provides message authenticity and integrity verification, and it is much stronger and more reliable than the original TKIP protocol for WPA [11]. Unfortunately, on October 16, Belgian researchers Mathy Vanhoef and Frank Piessens of the University of Leuven published details of a new WPA2 attack called “KRACK”, or Key Reinstallation Attack, that exploits the four-way handshake allowing the traffic to be sniffed leading to man-in-the-middle-attacks. This new exploit is rooted in the standard itself meaning that any implementation is vulnerable. If your device supports Wi-Fi, it is most likely affected. With that kind of range, attackers can now use this exploit for many different motivations. Such motivations can be directed towards sniffing out cookies for logins and passwords or hijacking TCP sequence number and connections for injecting malicious data into unencrypted HTTP sites [12]. Either could potentially have harmful effects towards users but luckily, there are some mitigations that can be implemented. Chacos and Simon urge to keep your devices up to date. Vanhoef says “implementations can be patched in a backwards-compatible manner” [12]. That means that your device can download an update that protects against KRACK and still communicate with unpatched hardware while being protected from the security flaw. Given the potential reach of KRACK, patches are coming quickly from many major hardware and operating

system vendors. Up-to-date Windows PCs, for example, are already protected [13]. But for all you other devices, update them as soon as possible. If that is not feasible at the current time stick to websites that use only HTTPS encryption. Those sites are protected even though your security protocols are not. Finally, using a virtual private network, or VPN, that takes advantage of the IPSEC protocol, will allow you to hide all data over the network.

Security Tradeoff

A secondary key issue in the industry creating IoT devices is the tradeoff between cost of security and implementation of security. There are multiple fallacies that only add to this issue, such as security through obscurity and the widespread belief that a breach will never happen to that company. Some devices work with personal data that can be harvested, and protecting it despite the cost is important. If a company fails to protect data, lawsuits, government investigations, and other actions might be brought against said company. In terms of responding to the tradeoff, research was conducted to demonstrate the rising cost of implementing security at various stages of development.

One of the most effective methods of security for data is encryption. Encryption takes clear text and transforms it into cipher text, with either one key or a set of keys two endpoints use. One issue with not always using encryption is the range of IoT devices and their capabilities. It becomes difficult to standardize a process that works universally [14]. With so many encryption schemes available, it may sometimes be difficult to figure which is the best fit for a device. Some encryptions, such as AES and 3DES, offer algorithms with a variety of key sizes for increasing security. If a device does not have much memory to work with, an algorithm with a smaller key size can be an option. A second issue that comes from devices that do use encryption is key rotation. For data to remain secure, scheme keys must be changed often, to maintain the

data in a safe state. This process can be time consuming and expensive, leading to issues seen in the tradeoff discussed earlier. One solution to this are smart chips embedded within devices. They can contain certificates or adapted encryption schemes to protect stored data and software.

The security level of an IoT device needs to match the level of valuable information that device is handling. With household IoT devices, the vital information is not just things like credit card numbers. Household IoT devices contain a great amount of information on the user habits. Data mining the information from fitness wristbands, fridges, and AC can reveal the user's daily routine. Many companies would pay for those profiles [15]. Protecting the device itself is not the only security consideration as household IoT devices are connected to a cellphone or a Wi-Fi network. Even if the devices don't contain any information worth protecting, they can become a vector of attack on the network it connected to [15].

Protecting the device itself is not the only security consideration as household IoT devices are connected to a cellphone or a Wi-Fi network. Even if the devices don't contain any information worth protecting, they can become a vector of attack on the network it connected to [15]. There been a case where email password was stolen because its calendar was sync to a smart fridge [16]. Some IoT device needs to also be secured again a false central node. Car and door lock connected to a cellphone need to able to differentiate between the real phone and an emulated clone. Compromised IoT device can also be a part of a larger DDOS attack. Information of the device and its network would not matter in this case. Because of this, even the most innocuous IoT device requires careful consideration when it comes to security level.

One of the problems in securing an IoT device is that it is difficult to update the protection. IoT systems are not always designed with an update system as security was

not a major feature of the current systems. For hardware-based system, the security components are often not connected to the network to protect them from attacks. Updating these kind systems would require technician come to update them or the system would need to be replaced. Even if they have away to update, IoT system often uses components from different manufacture which use proprietary driver [17]. The component manufactures don't always keep their driver up-to-date, so any patch need to work around that. If there are updates, then the IoT companies also need to have a system to distribute the update. Either alert the device owner to download and install the update or have the devices update themselves. IoT companies need to consider the cost of replace a system versus creating a maintenance structure.

An endpoint is a connection to a TCP/IP stream where either a user or a system has access. This notion of an endpoint is a crucial factor to security. The number of IoT endpoints in a system directly correlates to the security of transmissions. With the rapid increase in IoT device usage, there is more and more access point for attackers [18]. Having two cameras provide a better coverage but also a higher probability at least one of them will fail. For system that use hardware-based protection, having more IoT devices mean a higher material cost. IoT devices in a system might not have the same manufacture, which make patching security holes become more difficult. Any patch to a device need to keep it compatible with the rest of the system or the entire system need to be updated together. This can leave the system open to a specific attack for a longer period. At the same time, devices having different manufactures mean an attack that work on one device might not able to propagate through the system [18].

SMART Device Trend

SMART devices are a central part of IoT. These devices are made to control and simplify various tasks, such as control over AC units, lighting, and vehicle maintenance,

among other things. There are two trends that have emerged from the use of SMART devices.

The first, is the creation of a central hub to interact with the data from these devices. Mobile devices have become a crucial point in the communication of IoT devices. Development companies such as IBM and Amazon have developer information on how to use a cellphone as a hub between a server and another device. Due to the higher processing power found in mobile devices, this is an alternative for IoT to communicate with servers.

The second trend revolves around devices such as Amazon Echo and Google Home. These devices are built to control a variety of apps and external devices through voice commands. This means that built in microphones are always active and listening. Recently, it was discovered that Amazon Echo models sold before 2017 had a vulnerability that allowed them to be used as wiretap devices. Although it required direct access to the device, no sign of intrusion would be left [19]. As this trend continues, it is important to note that these devices must be safeguarded and require bigger privacy contracts due to potential recording.

Examination and Results

As part of this research project, experiments were conducted to further compare the results between traditional approaches and new IoT solutions. The first experiment relates to the efficiency of traditional encryptions versus lightweight algorithms. Using Python 2.6 on a Windows 10 machine, running an Intel Core i7-7500U CPU @ 2.70GHz, AES and PRESENT were tested to measure CPU consumption as data size grew.

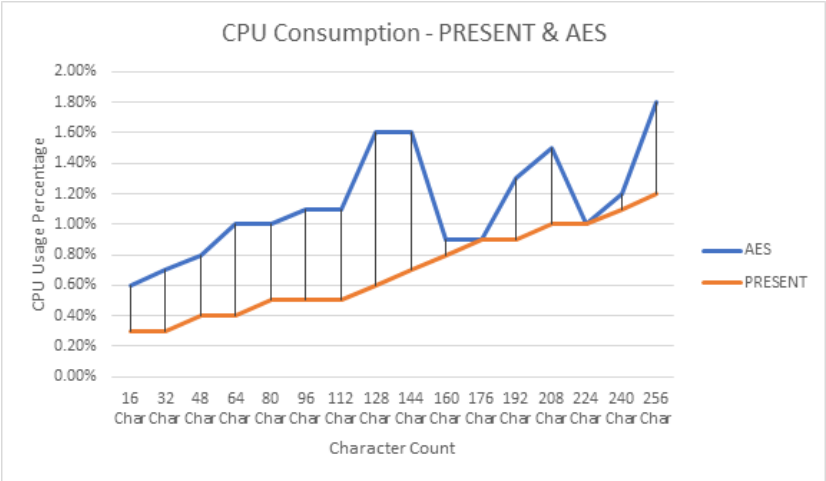

Figure 1. CPU consumption between two algorithms, AES and PRESENT. Conducted over increasing data sizes.

As shown in Figure 1, as data size grew, so did CPU consumption on average. However, the AES implementation consumed more CPU over a constant amount of trials than PRESENT. This could be due to the round process or S-box configuration of each algorithm. These trials were done with the same key size of 128 bits, input as "0123456789abcdef". The AES algorithm used the same key input for the IV. The input data was a repetition of the 16 characters of the key.

Although the changes range from 0% to 1%, a noticeable change is seen merely with CPU consumption. With bigger data or different keys, more changes can separate the performance of these two algorithms. Further experimentation with memory use, disk use, and energy consumption could also be good factors to determine the appropriate algorithm to use for a specific situation. Figure 2 below shows the values for all characters counts from Figure 1.

Character Count	AES	PRESENT	Percent Change
16	.6%	.3%	.3%
32	.7%	.3%	.4%
48	.8%	.4%	.4%
64	1%	.4%	.6%
80	1%	.5%	.5%
96	1.1%	.5%	.6%
112	1.1%	.5%	.6%
128	1.6%	.6%	1%
144	1.6%	.7%	.9%
160	.9%	.8%	.1%
176	.9%	.9%	0%
192	1.3%	.9%	.4%
208	1.5%	1%	.5%
224	1%	1%	0%
240	1.2%	1.1%	.1%
256	1.8%	1.2%	.6%

Figure 2. Values corresponding to CPU consumption in Figure 1.

As testing continued, the number of endpoints was also measured. Endpoints play a key role in security, from programming to data transmission.

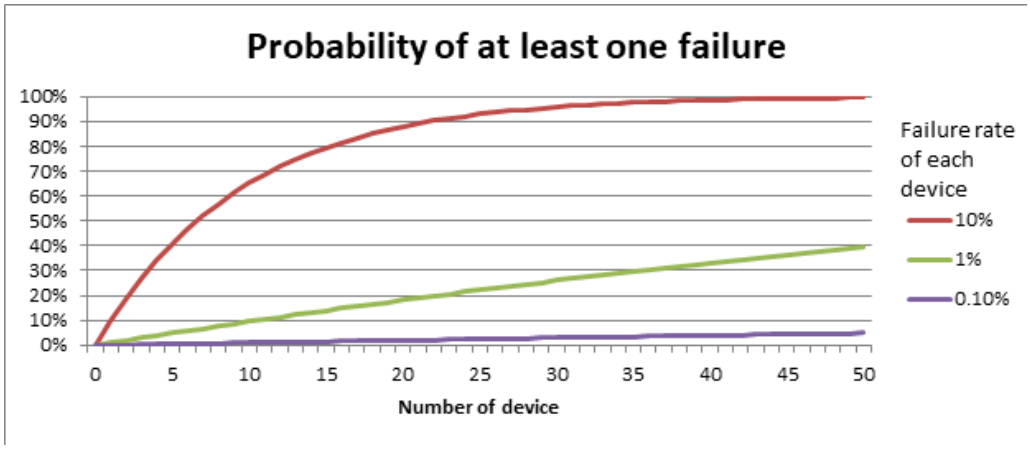

Figure 3. Failure probability based on endpoints.

For systems that use hardware-based protection, having more IoT devices mean a higher material cost. IoT devices in a system might not have the same manufacture, which make patching security holes become more difficult. Any patch to a device need to keep it compatible with the rest of the system or the entire system need to be updated together. This can leave the system open to a specific attack for a longer period. At the same time, devices having different manufactures mean an attack that work on one device might not able to propagate through the system [18]. As more and more

household device become connected, the failure rate of each endpoint must be lowered to keep the whole system failure rate at an acceptable level.

Remarks and Conclusions

Encryption methods exist across many platforms, however lightweight versions of schemes could be used for handheld devices and IoT devices that use minimal energy and power. The practice of using lightweight encryptions with deployed devices helps ensure consumer privacy is maintained across all connected platforms. Although these lightweight encryptions have already been employed in the field, further research is still needed to test the strength and durability of lightweight encryptions.

One of the main points that should be emphasized for the future is the implementation of security early on. Whether data is valuable or not, some form of security should be added to protect the device. It is also worth noting that another thing to focus on in the future is the security behind always-on devices, such as SMART home controls. Devices that also carry data, such as TVs and refrigerators should also implement the same level of security as SMART home control devices. If they can maintain a microphone on, then extra security must be implemented to avoid compromising the privacy of the user.

IoT devices currently deployed have a spectrum of protocols in use. While some devices already employ lightweight encryption, others are not using these measures at all. To improve day to day security, minimum standards should be created for IoT devices that transmit data, whether they connect to the internet or not. Consumers should also carefully read privacy acknowledgements of devices they purchase, as companies may release themselves from lawsuits if data breaches or data mining attempts occur.

References

[1] McKay, K., Bassham, L., Turan, M. S., & Mohua, N. (2017, March). Report on Lightweight Cryptography. National Institute of Standards and Technology Internal Report, 8114, 5-10. Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf

[2] Leander, G., Paar, C., Poschmann, A., & Schramm, K. (2007). New Lightweight DES Variants. N.p.: Horst Gortz Institute for IT Security. Retrieved from https://www.iacr.org/archive/fse2007/45930197/45930197.pdf

[3] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A. q., Robshaw, M. J., Seurin, Y., & Vikkelsoe, C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. Retrieved from http://lightweightcrypto.org/present/present_ches2007.pdf

[4] Katagi, M., & Moriai, S. (2011). Lightweight Cryptography for the Internet of Things. Retrieved from https://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf

[5] Russell, B., Van Duren, D., Amador, V., & Bezold, S. (2016, June 4). In Key Management Cheat Sheet. Retrieved from https://www.owasp.org/index.php/Key_Management_Cheat_Sheet

[6] Valerio, P. (2016, May 13). Weak IoT Security Puts Networks At Risk. Retrieved October 15, 2017, from https://www.networkcomputing.com/iot-infrastructure/weak-iot-security-puts-networks-risk/708297483

[7] Kwon, Y. (2017, April 21). Understanding IoT Protocols – Matching your Requirements to the Right Option. Retrieved October 15, 2017, from https://solace.com/blog/use-cases/understanding-iot-protocols-matching-requirements-right-option

[8] Beal, V. (n.d.). Wi-Fi (wireless networking). Retrieved November 4, 2017, from https://www.webopedia.com/TERM/W/Wi_Fi.html

[9] Mitchell, B. (n.d.). What's 802.11? What These Wireless Standards Mean. Retrieved November 4, 2017, from https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553

[10] Aircrack-ng. (n.d.). Retrieved November 4, 2017, from http://www.aircrack-ng.org/doku.php?id=deauthentication

[11] What is Wi-Fi Protected Access (WPA)? - Definition from WhatIs.com. (n.d.). Retrieved November 4, 2017, from http://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access

[12] Vanhoef, M. (n.d.). Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse. Retrieved November 4, 2017, from https://www.krackattacks.com/

[13] Chacos, B., & Simon, M. (2017, November 8). KRACK Wi-Fi attack threatens all networks: How to stay safe and what you need to know. Retrieved November 9, 2017, from https://www.pcworld.com/article/3233308/security/krack-wi-fi-security-flaw-faq-tips.html

[14] Press, G. (2017, March 20). 6 Hot Internet of Things (IoT) Security Technologies. In Forbes. Retrieved from https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-things-iot-security-technologies/#1f5747f61b49

[15] Thomas, A. (2015, November 28). Understanding the convenience of IoT and the security trade off. Retrieved September 14, 2017, from ITProProtal: http://www.itproportal.com/2015/11/28/understanding-the-convenience-of-iot-and-the-security-trade-off/

[16] Neagle, C. (2015, August 26). Smart refrigerator hack exposes Gmail login credentials. Retrieved 10 12, 2017, from Network World: https://www.networkworld.com/article/2976270/internet-of-things/smart-refrigerator-hack-exposes-gmail-login-credentials.html

[17] Heer, T., Garcia-Morchon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security Challenges in the IP-based Internet of Things. Wireless Personal Communications, 527–542. Retrieved from http://iotsecuritylab.com/wp-content/uploads/2014/08/Security-Challenges-IP-Based-Internet-of-Things.pdf

[18] Covington, M. J., & Carskadden, R. (2013). Threat implications of the Internet of Things. 2013 5th International Conference on Cyber Conflict (CyCon). Retrieved from https://pdfs.semanticscholar.org/a4a2/e111da3e558b2c4d54671683ad8a24cb0fea.pdf

[19] Greenberg, A. (2017, August 1). A Hack Can Turn An Amazon Echo into a Wiretap. In Wired. Retrieved from https://www.wired.com/story/amazon-echo-wiretap-hack/

[20] Ashton, K. That ‘Internet of Things’ Thing. RFID J. 2009, 22, 97–114.

[21] Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A Survey. Comput. Netw. 2010, 54, 2787–2805.

[22] Giusto, D.; Lera, A.; Morabito, G.; Atzori, L. The Internet of Things; Springer: New York City, NY, USA, 2010.

[23] Federal Trade Commission. Internet of Things—Privacy and Security in a Connected World; FTC: Seattle, WA, USA, 2013.

[24] Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020; Gartner Inc.: Stamford, CT, USA, 2013.

[25] Newman, M. BACnet: the Global Standard for Building Automation and Control Networks; Momentum Press: NY, USA, 2013.

[26] Aberer, K.; Hauswirth, M.; Salehi, A. Infrastructure for Data Processing in Large-scale Interconnected Sensor Networks. In Proceedings of the IEEE International Conference on Mobile Data Management, Mannheim, Germany, 7–11 May 2007; pp. 198–205.

[27] Shelby, Z.; Hartke, K.; Bormann, C.; Frank, B. RFC7252: The Constrained Application Protocol (CoAP); IETF Standards; CoRE Working Group: Fremont, CA, USA, 2014.

[28] Lee, C.T.; Yang, C.H.; Chang, C.M.; Kao, C.Y.; Tseng, H.M.; Hsu, H.; Chou, P.H. A Smart Energy System with Distributed Access Control. In Proceedings of the IEEE International Conference on Internet of Things, Cambridge, MA, USA, 6–8 October 2014.

[29] Cirani, S.; Picone, M.; Gonizzi, P.; Veltri, L.; Ferrari, G. IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios. IEEE Sens. J. 2015, 15, 1224–1234.

[30] Blazquez, A.; Tsiatsis, V.; Vandikas, K. Performance Evaluation of OpenID Connect for an IoT Information Marketplace. In Proceedings of the 81st IEEE Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015; pp. 1–6.

[31] Seitz, L.; Selander, G.; Gehrmann, C. Authorization Framework for the Internet-of-Things. In Proceedings of the 14th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Madrid, Spain, 4–7 June 2013; pp. 1–6.

[32] Fotiou, N.; Kotsonis, T.; Marias, G.F.; Polyzos, G.C. Access Control for the Internet of Things. In Proceedings of the International Workshop on Secure Internet of Things (SIoT 2016), Crete, Greece, 27 September 2016; pp. 29–38.

[33] Gerdes, S.; Bergmann, O.; Bormann, C. Delegated CoAP Authentication and Authorization Framework (DCAF); IETF Internet Draft: Fremont, CA, USA, 2015.