2019

27. Security in Internet of Things (IoT)

Candidate number.: 15653
UNIVERSITY OF OSLO

Contents

Introduction

Imagine the potential of connecting everyday objects to the internet. Your fridge might alert your phone when you're out of milk, and by asking it, your speakers can answer every factual question you might be wondering. This phenomenon is better known as Internet of Things and it's growing bigger every day. How can this technology be beneficial for consumers and corporations? In this academic paper I will be addressing this topic. I will also be covering some of the most common risks that can occur in the world of IoT, and how to ensure safety against them, both as a consumer and as a bigger business.

What is Internet of Things?

The Internet of Things, IoT for short, is a recent phenomenon describing the implementation of connectivity to the internet in everyday objects. Essentially, everything that can benefit from sending and receiving information has the potential and will most likely end up becoming part of the Internet of Things. Today, consumers have the option of connecting their phones, TV's, security cameras and even their lamps to the internet.

Considering the potential of connecting lamps to the internet; Earlier it could only be switched on or off by a switch located in the same room. If a bulb would break, someone would have to notice it themselves and physically go to a store to buy a new one.

If one was to connect a lamp to the internet today, it could be remote-controlled from any device anywhere in the world where an internet connection is present. A single socket could notify your computer how much electricity is uses, whether it is turned on or off, and if its bulb needs to be replaced. Given the last scenario, it would then be easy to implement a way for the socket to automatically order a replacement bulb to your door from an online store.

If there exists a way a device can connect to the internet, the opportunities for that single device can go way beyond the initial function of that device. The potential is essentially limitless, and today we have only scraped the surface of what IoT has the potential of becoming in the future.

One could argue that owning a light source that automatically orders new lightbulbs using your own credit card would seem both scary and unnecessary. Therefore, it is both the responsibility of the provider and the consumer to preserve the integrity of both the device and its features. Even though the devices are created to increase productivity, they come with risks. It is therefore critical for developers to implement fail-secure systems. Consumers must be able to trust all devices, both in terms of hardware and software solutions. It is also important that communication between the devices and especially connectivity to the internet

uses good protocols that in practice should be impossible for attackers to break. This is especially true if the device stores or takes advantage of personal credentials such as credit card information.

The security issues and dangers of IoT

Today many of the manufactured IoT devices unfortunately have notoriously bad security solutions. This is usually due to manufacturers prioritizing producing quantity over quality. Many programmers write half-good code that rely on weak security solutions. The code is also not researched and tested thoroughly enough to be considered secure. For a long time, it didn't matter if potential attackers could breach the devices they sold. It was irrelevant, so long as the product was shipped as fast as possible. This is mostly due to saving the both expense of components used for making highly secure devices, and the extra time used to implement the required algorithms for each device. IoT security shows few signs of improvements, even though it is getting increasingly widespread. In a worldwide study, Kaspersky, a corporation focusing on security and antivirus solutions, created honeypots as bait to detect new attacks. Many of these honeypots were IoT devices made with different weaknesses for attackers to exploit and take advantage of. The statistics revealed that the number of attacks detected had increased by 9 times from 2018 to 2019.[1] This number suggests that the more types of IoT devices are made, the more ways attackers can go about targeting those devices. Essentially, more devices meant more attack methods.

The eye-opening attack

In October of 2016, one incident made the importance of security in IoT devices more apparent than ever. The incident is described as the first major outbreak of malware targeting the IoT. It is dubbed the "Mirai Malware", "Mirai" being the Japanese word for "Future". The attack made hackers able to access a range of personal devices using the basic username and password combinations they were shipped with. By misusing the devices, the hackers created botnets that could target a website and send massive amounts of data to it. Given the scope of infected devices, the information sent was too much for a targeted website to handle, resulting in it crashing temporarily. This specific type of attack is better known as a "DDoS", or

[1] Kaspersky honeypots find 105 million attacks on IoT devices in first half of 2019, Url: https://www.techrepublic.com/article/kaspersky-honeypots-find-105-million-attacks-on-iot-devices-in-first-half-of-2019/

Distributed Denial of Service attack. The attack also contributed to making botnets the third most dangerous threats businesses using IoT potentially must face. The first and second most dangerous threats concern attackers being able to access to sensitive data and attackers committing sabotage. Both of which closely relate to- or can be achieved using botnets. An attack can take on an unlimited amount of forms, but many of these resemble each other, taking advantage of many of the same things. Therefore, it is possible to prepare for many of these attacks. The first step in this preparation process is to identify what aspects can be targeted, using a method called risk assessment.

Risk assessment

On the surface, the potential risks considering IoT devices can be easily diminishable. Taking the light socket example, if a potential attacker was to break its security, what would he be able to do? The general functions of a connected IoT light socket might vary from device to device. In general, it would not exceed setting the light settings, and maybe also monitoring electricity use in more expensive devices. Both functions will usually prove unbeneficial for the attacker. What good would it do to switch off your neighbours' lights? However, the manufacturers might want to add a function for registering user information. This will make the socket able to communicate with an online shopping service, and in turn order a new bulb if the old one should break. If an attacker was to target a device that stored credit card information and other credentials, the potential damage of using that device without precaution would skyrocket. This proves that the risk lies not only within the device itself, but also in the access it provides.

The process of assessing risks

Long before manufacturers can start producing a function for an IoT device, they are required to compare the values this function presents, and the ways attackers can go about taking advantage of that functions. This process is critical for creating safe and secure functions for the device. Risk assessment is the process of identifying, estimating and prioritizing risks regarding the organisation and the end-users of the provided service. Long before starting development of a new function, developers must ask themselves "what can go wrong?", "what's the likelihood of that happening?", and "what might the consequences of it be?" The risk-assessment team will also have to enter the attackers head and look for ways it would be beneficial for the attacker to attack certain parts of their devices. After completing the risk assessment, the team should develop a clear strategy of actions for each risk based on both the likelihood and impact level of that threat scenario. These strategies will be to either reduce the

risk by implementing good security solutions, to share or transfer the risk to another subject, to tolerate the risk and its potential consequences, or to avoid the risk completely by dropping implementation of the planned function. Today more than ever before, focus on keeping the security of the IoT devices are one of the most central parts of developing any IoT device. As of May 2018, new laws were taken into effect to ensure the safety of users' personal information. These laws are formally known as the General Data Protection Regulations (GDPR). Specifically, in article 34, section 3b, it states

"The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise." [2]

We could interpret this as if there exists any known possibility of an attack materializing, the developers are required by law to decrease or completely remove the likelihood of it ever happening. If a company fails to follow guidelines in article 34 of GDPR, they might be fined up to 10 million euros, or 2% of annual global turnover, which can be devastating to a company. In addition to the GDPR, NISTR 8228, is a publication from June 2019 that specifically describes the risks and dangers of using IoT devices. It identifies three main considerations that may affect both the management of cybersecurity and privacy risks for IoT devices compared to conventional devices. The considerations are described as the following:

1. *Many IoT devices interact with the physical world in ways conventional IT devices usually do not.*
2. *Many IoT devices cannot be accessed, managed or monitored in the same ways conventional IT devices can.*
3. *The availability, efficiency, and effectiveness of cybersecurity and privacy capabilities are often different for IoT devices than conventional IT devices.*[3]

As every IoT device are built differently than both the conventional computers and other IoT devices, the ways to go about both attacking and protecting will most definitely also appear as very different then what we are used to. Managing risks for IoT devices will therefore never be a one-and-done thing. Developers must constantly look out for new attack patterns and develop ways to handle them in a never-ending game of cat and mouse.

[2] GDPR article 34, Url: https://gdpr-info.eu/art-34-gdpr/
[3] NISTR 8228, pages 4-5, Url: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

Security Implementations

Device Security

There exists a plethora of different IoT devices, and as time passes, the list is only increasing. The definition of a smart car might be completely different in five years compared to today's definition. Is therefore critical for every new device to be implemented with its own personally tailored security solutions. In his article "The Basics of IoT Device Security", Alan Grau describes the most common weaknesses in the IoT devices themselves can be divided into three categories. The first being "Deployment or use vulnerabilities", which occur from a user's lack of knowledge when installing or operating the devices. These vulnerabilities may be but are not limited to not changing the default- or using weak passwords, and not enabling recommended security features. The second category is "Implementation vulnerabilities." Strictly from a software perspective, the device has been provided with bad code that itself poses as a danger to the security. This category includes Buffer Overflow, which is an anomaly where a program overrun the buffer's boundary, causing it to overwrite memory. The last category is "Design vulnerabilities", which stem from programmers failing to implement updated and proper security measures during development. This category includes vulnerabilities stemming from not encrypting credentials or passwords during communication with the servers. Even though IoT devices are made differently, all these three categories prove to be relevant for every IoT device. Therefore, they can be helpful in recognizing different types of flaws regarding the making- and use of IoT devices.

It should be obviously clear that devices that have been compromised or are too old to be considered secure anymore are recalled and the services for them shut down completely. This way, attackers have no way for repeating attacks using the same methods as earlier, or even on the same devices they already compromised. The devices that still can be considered useable will need secure firmware- and software updates. A new and improved file format for storing and sending video footage might prove itself useful for an IoT security camera. A firmware update can then allow for the camera to film videos in that new format. Even though the hardware for the camera was created before the new file format, it still has the potential of using the new format with a firmware update. Both firmware and software updates also often include new functions providing protection from the newest types of discovered attacks.

One specific way attackers go about targeting IoT devices is by trying to run their own code directly on the devices. If the developers are not careful about this, it could lead to fatal consequences. Most smart cars will eventually have functions for detecting and avoiding

potential dangers. An attacker might then write rogue code, hacking into a car and causing the car to actively drive towards that danger, increasing the potential for collision. One way to protect against this is a method called Secure Booting. It limits the devices to only be able to execute code provided by the original equipment manager, the company that manufactured and sold the device. This is achieved by implementing cryptographically signed code. The device will then ignore all code that is not encrypted in the same way. This method might require more work from the developer's side, but it proves to be very useful in practice.

Moving away from the device itself, and onto the subject of communication, it is important for all device communication to be encrypted. Every device should be provided with a valid certificate, unique for it and no other device. This is achieved by using unique certificate, and common protocols for key transferal, like Public Key Infrastructure (PKI). This makes the server able to authenticate all non-rogue devices and establish a safe connection to them, and vice versa.

Router Security

The potential dangers are not only important to consider for the end-devices, but also the devices in between, such as the Router. Most every IoT device is connected to the internet through a router, and if the router should be compromised, the connected devices could consequently also be considered compromised. Anyone with a router can choose to enable password-protected encryption to increase the security of all communications with the router. It is highly advised against having a password-free router, as everyone can connect to it, and in turn see the files on your personal devices. Having an encryption-free router widens the options attackers can go about attacking said router. It is important to recognise that routers have been using different types of Wi-Fi encryption throughout their lifespan. As time passes, newer technologies are being introduced, needing more advanced algorithms to be considered secure. In turn, the routers must keep up with these changes as well. The oldest router encryption still being used in 2019 is Wired Equivalent Privacy (WEP). This algorithm was introduced in 1997 and was superseded by Wi-Fi Protected Access (WPA) in 2003. If a router only supports WEP, WPA, or both, it is highly advised to consider buying a new router. These algorithms are easy for attackers to break, and don't provide the security needed for today's standards. Today, the most common encryption is Wi-Fi Protected Access 2 (WPA-2). However, WPA-2 is in general still susceptible to some devastating attacks.

One attack is dubbed the 2017 KRACK attack. As the name suggests, KRACK, or Key Reinstallation Attack is an attack that directly takes advantage of the handshake used in

communications between a client and a server. In the third step of the handshake, the server sends a nonce, a randomly generated key used in establishing a secure connection between the client and the server. Attackers misused this nonce, repeatedly resetting it to gradually match the encrypted packets. The information was then used to learn the full keychain used for encryption, essentially breaking it. This attack directly takes advantage of the WPA-2 encryption, so every device using WPA-2 is in theory vulnerable. The newest Wi-Fi encryption, introduced in 2018, is WPA-3. It will likely gradually be taking over WPA-2's place as the leading standard for Wi-Fi encryption. It fixes many of the problems WPA-2 introduced and is a more secure encryption in general.

In addition to establishing encrypted connection to the end-devices, almost every new router provides a firewall. A firewall can provide features such as NAT filtering, port forwarding and -filtering and services blocking. All the mentioned features add new layers of security on the network, securing against attackers in their own way. A firewall controls and monitors all incoming and outgoing network traffic based on its rules and protocols. One could picture a firewall as a barrier, only letting safe and authenticated information pass through on either side of it. This feature will prevent attackers from getting their hands on some sensitive information like your router's location and IP address.

Some routers have the option of using a Virtual Private Network (VPN), which can prove useful. A VPN is good when multiple devices are connected to one single network. This is especially useful for bigger corporations that wishes to deliver a robust, consistent and secure experience for their employees. A VPN creates point-to-point connections through the internet. These connections are often referred to as tunnels and are usually encrypted. This type of connection is useful when connecting to otherwise unencrypted or weakly encrypted networks, making connecting to them secure and private regardless of their own level of encryption.

Network Security

Now that we have covered both the devices and the routers they are connected to, it is logical to ask ourselves what comes next? After a safe connection is achieved between all devices, is safety ensured? The final part to consider is whether internet is safe in general. Can you trust the servers that the IoT devices are connected to? And how is the information transmitted through the internet? There are many dangers lurking on the internet. In this paper I'll only be focusing on the ones most likely to target IoT devices. One type of malicious software that poses a danger to your personal IoT devices are backdoors. Backdoors refer to any method an

unauthorized user may be able to bypass normal security measures and gain a root access to a device. Backdoors are notorious for being discreet and often invisible if you don't know what to look for. Considering IoT devices, backdoors can potentially be used to create a botnet, like the botnet that originated from the Mirai malware mentioned earlier. This has lead to IoT devices being called a modern day "trojan horse", as neither you, nor the servers they are connected to have a way of knowing that the devices have been compromised.

There exist many measures to protect against different types of attacks over the internet. Specifically regarding IoT devices, you want to both protect your own devices, but also protect your own assets from rogue IoT devices. The easiest way to do this is to acquire an anti-virus (AV). AV's are a type of software made for detection and removal of viruses on a device. This is achieved in two ways. The first way scans the filesystem, trying to detect known malware from a dictionary of already detected dangers. There exists no way for an AV to detect never-before-seen malware, so another smart method it uses is to look for suspicious activities within the programs stored in a device. If the AV detects anything it would deem dangerous, it will alert the users and prompt a way to delete or quarantine the malicious files in question. This way, even though an attack might have happened successfully, there is a way to reverse it.

A new feature introduced to the world of IoT is Universal Plug and Play (UPnP). This feature allows for many devices to discover each other's presence on the network for data sharing and communication between them. This feature makes it easier to configure the devices, but also poses a threat. If every device is connected to each other via IP, it would be easy to target multiple devices by using their communication. To preserve security for all your devices, it is therefore recommended to disable UPnP. In a business setting, this proves especially beneficial, as attacks on their devices might do a lot of damage to their infrastructure.

As mentioned earlier, most every IoT devices need to send and receive data trough the internet. This can be achieved in a matter of ways. One way is to annually send the data needed. Perhaps a lamp only needs to send its information every 24 hours, once an hour or every time a user demands it to. In which case, it can use common handshake protocols for establishing contact with its servers. On the other hand, there exists devices that have a need to constantly send information. One safe solution to this is the use of continuous data streaming. One could visualize a river of information. There is no beginning or end, but a constant stream of information flowing through the internet in real-time. This proves beneficial as information is processed as it is created and made available on-demand with no

delay. Streaming data flows are different than regular batch-based flows. They are more time-sensitive, meaning that if a device fails to constantly send or receive data, it might not be able to work properly. As the information is constantly flowing, it tends to typically be larger, and require a big processing memory on both ends of the flow. Also, a decision must be made for how long information is being stored before deletion. Much of the information in the flow may prove to have low or no long-term value after processing and might be deleted instantly. It is therefore important to research whether it would prove beneficial to use real-time dataflow before implementing it.

How to ensure safety when using IoT devices

As a business

IoT devices help in improving automation and efficiency in a work environment but can in turn expose it to many new security threats. It is important to evaluate what benefits may come from investing in IoT devices compared to the new risks occurring from using them. It is important to remember that IoT devices are a luxury and might not prove to be as useful in every setting. If a business can afford to buy tamper-proof devices, that would be the optimal option. A device with built-in-security solutions like it being patchable is preferred. A patchable device can receive both software and firmware updates, making its potential lifespan longer before it needs to be replaced. If the developers do a good job with updating their IoT devices, they will annually release secure updates to prevent never-before-seen attack patterns. For example, they can remove the potential for older devices becoming part of the Mirai Botnet mentioned earlier.

After proper research has been made into whether it would prove beneficial to acquire IoT devices, the local network needs to be prepared in the best way possible. IoT includes a group of network protocols that work on different layers. Both the network and transport-layer need to be protected with encryption. A secure Intranet usually translates to secure communications between the devices connected to it. It would be a smart move to purchase AV-programs to every computer connected to their internet. The IT-department should also secure the databases containing their employees' credentials, preventing SQL-injections and other known attacks to their databases. One employee should only be able to access the assets concerning his position in the corporation. For example, an intern should not be able to directly access the databases containing information about every employee's salaries, but it might prove useful for an accountant. If the corporation stores sensitive data, they must have strong authentication-, and access control solutions. One way to achieve this is to use two-

factor authentication. Two-factor authentication makes logging into the corporation's servers harder, as you require more than just a username and password. This can be achieved in many ways. A common way is to use a second device, a token, that can receive a one-time login password for access to their servers. Regardless of how much security is implemented within a corporation's intranet solutions, the biggest danger still lies in how well equipped their employees are in handling their devices. Every employee needs training in both how to operate the devices and how to preserve their integrity. Understanding how data is stored and processed it vital to come up with good strategies on how to efficiently use IoT devices. In conclusion, a corporation needs to research both the benefits and dangers of using IoT devices. Planning and preparation of both staff and their own security solutions in the intranet is key to make the transition go smoothly. Invest only if the corporation can both afford it and have a practical use for it, and don't settle for half-good devices, as they often lack the security needed.

Privately

A private consumer doesn't have to worry about a lot of the risks that bigger corporations can face. This is due to their intranet being much smaller, usually only consisting of one router and the personal devices connected to it. Also, the calculated value of one private consumer's information and devices is much lower that a big corporation with a big infrastructure. Taking the Mirai botnet attack into consideration, attackers wouldn't gain much from DoS-ing only one household with no more than ten devices compared to a big corporation consisting of hundreds of devices and servers. As a private consumer, preparing their own intranet is a much easier task compared to what it's like for big corporations. Many devices have implemented Access Control and User interfaces that are easy to follow. Setting up a firewall and an AV should also be a small task for one possessing a little knowledge on the subject.

The most important task regarding acquiring an IoT device is to check whether the device itself proves to be safe and useful. Consumers should only buy from trusted websites and stores. They should also familiarize themselves with what features the device provides. When the features are clear to them, consumers should ask themselves how this device can help in making their lives easier. If the answer is an obvious yes, then there is no problem in trying it out. On the other hand, if the answer is unclear, maybe the solution is to do more research, or speak to a professional on the subject. As mentioned earlier, it is important to have secure and unique passwords on every device in the household allowing it. Most IoT devices are made to be secure and easy to use from the get-go, but it is important to understand the basics on how

they work. If a person new to technology was to acquire an IoT device, it might prove difficult to use. That might in turn make the device prove to be more of a nuisance then helpful for the buyer, resulting in regret.

Summary

It is apparent that The Internet of Things has come to stay. Being able to create a network of most every home appliance, essentially creating a what's commonly known as a smart-home is revolutionizing how the modern human is living. It also brings with it a lot of new threats that are hard for inexperienced people to handle and prepare for. IoT is a new idea, and for it to stay, it is important that every connected device can get its work done in a secure and safe manner. We are living in a technological world and it is important to familiarize ourselves with how technology is evolving, and what benefits new technology provide. This also includes getting to know how to stay securely connected to the internet via a router. One should know what risks can arise in the different parts their own intranet, and how to assess these risks. Only then you can safely benefit from the ever-increasing world of IoT.

Sources

(Every link is tested November 13. 2019)

Jacob Morgan, Forbes, (May 13 2019), A Simple Explanation Of 'The Internet Of Things', Url: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#1beafbd91d09

Margaret Rouse, (October 2018), IoT security (internet of things security), Url: https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

Jayshree Pandya, Founder of Risk Group, (June 27, 2019), Investing In The Internet Of Things Security, Url: https://www.forbes.com/sites/cognitiveworld/2019/06/27/investing-in-the-internet-of-things-security/#b4fafb43d590

Christopher S. Yoo, University of Pennsylvania (2019), The Emerging Internet of Things – Opportunities and Challenges for Privacy and Security, Url: https://www.cigionline.org/articles/emerging-internet-things?gclid=Cj0KCQjwuZDtBRDvARIsAPXFx3BUyIFx_Cb7MlANkwqza6nt1s0I6gy_szrrsTVww6K0azQ_mNpUOZAaAk-QEALw_wcB

Avast Busiiness Team (February 12, 2019), What risks do IoT decurity issue pose to businesses? Url: https://blog.avast.com/iot-security-business-risk

Richard van Hooijdonk, (March 7, 2019), The hidden dangers of IoT devices, Url: https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/The-hidden-dangers-of-IoT-devices

Macy Bayern, Security in TechRepublic, (October 15, 2019), Kaspersky honeypots find 105 million attacks on IoT devices in first half of 2019, Url: https://www.techrepublic.com/article/kaspersky-honeypots-find-105-million-attacks-on-iot-devices-in-first-half-of-2019/

Norton Youtube Channel, (August 15, 2017), Mirai Botnet Malware Outbreak, Url:
https://www.youtube.com/watch?v=MBIvEdkkzAg

Dan Demeter, Marco Preuss, Yaroslav Shmelev, (October 15, 2019), IoT: a malware story, Url:
https://securelist.com/iot-a-malware-story/94451/

Prasanna Bidkar (2019), How Do Routers Provide Security? Url:
https://smallbusiness.chron.com/routers-provide-security-70778.html

Anastasios Arampatzis, (August 15, 2019), IoT Devices – Why Risk Assessment is Critical to Cybersecurity, Url:
https://www.tripwire.com/state-of-security/security-data-protection/iot/iot-devices-risk-assessment-critical/

Unknown publisher, brightline IT (November 8, 2017), IoT Security: Threats, Risk Assessment, and best Practices, Url;
https://brightlineit.com/iot-security-threats-risk-assessment-best-practices/

Various contributors, intersoft consulting, (May 25, 2018), General Data Protection Regulation – GDPR, Url:
https://gdpr-info.eu/

It governance (2019) – GDPR penalties and fines, Url:
https://www.itgovernance.co.uk/dpa-and-gdpr-penalties

Nist, Information Technology Laboratory, (February 14, 2018), Draft Interagency Report, NISTIR 8200, Summarizes International Efforts to Standardize Internet of Things Cybersecurity, Url:
https://csrc.nist.gov/News/2018/Report-International-IoT-Cybersecurity-Standards

Various contributors, NIST, (June 2019), NISTIR 8228 – Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks, Url:
https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

Alan Grau, (September 20, 2019), The Basics of IoT Device Security, Url:
https://www.machinedesign.com/iot/basics-iot-device-security

Kim Komando, (March 23, 2019), 5 essential router security setting you need to check now, Url:
https://www.foxnews.com/tech/5-essential-router-security-settings-you-need-to-check-now

Various contributors, (September 19, 2019), Wired Equivalent Privacy, Url:
https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

Various contributors, (September 24, 2019), KRACK, Url:
https://en.wikipedia.org/wiki/KRACK

Various contributors, (October 23, 2019), Wi-Fi Protected Access, Url:
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

Various contributors, (November 5, 2019), Cryptographic nonce, Url:
https://en.wikipedia.org/wiki/Cryptographic_nonce

Michael Horowitz, (October 31, 2019), Router Security
https://routersecurity.org/

Linksys, (2019), What is a VPN Router?, Url:
https://www.linksys.com/us/r/what-is-a-wifi-access-point/vpn-router/

Various contributors, (May 2, 2017), Virtual private network, Url:
https://no.wikipedia.org/wiki/Virtual_private_network

Various contributors, (November 7, 2019), Firewall (computing), Url:
https://en.wikipedia.org/wiki/Firewall_(computing)#:~:targetText=In%20computing%2C%20a%20firewall%20is,network%2C%20such%20as%20the%20Internet.

Biz4Intellia, (2018), Trending: IoT Malware Attack, Url:
https://www.biz4intellia.com/blog/iot-malware-attack/

EDITOR (Unnamed), (November 26, 2018), Protect your IoT devices with these tips, Url:
https://www.techadvisory.org/2018/11/protect-your-iot-devices-with-these-tips/

Adrian Bridgwater, (February 13, 2018), Why data streaming matters in the IoT, Url:
https://internetofbusiness.com/data-streaming-matters-iot/

Todd Greene, (June 17, 2014), 5 Challenges of Internet of Things Connectivity, Url:
https://www.pubnub.com/blog/5-challenges-of-internet-of-things-connectivity/

Various contributors, (March 15, 2016), UPnP, Url:
https://no.wikipedia.org/wiki/UPnP

Xu, Zou, Co-founder and CEO, ZingBox, (2019), IoT devices are hard to patch: Here's why – and how to deal with security, Url:
https://techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security

Adam Justine, Grid Connect, (October 2, 2014), 6 things to consider before buying your first home IoT product, Url:
https://www.embedded-computing.com/embedded-computing-design/5-things-to-consider-before-buying-your-first-home-iot-product