[TYPE THE COMPANY NAME]

Network Video Recording and Their Challenges

AIT 685: Capstone

Thomas "T.J." Blot, Loc Duong, and Douglas Kim

Spring 2020

You may have come across the term, “Internet of Things” (IoT) while browsing the Internet, or may have heard an advertisement offering management services for IoT on television or the radio; but what really is the IoT? With the increasing availability and necessity of Internet access at home, often provided through local internet service providers (ISPs), mobile phones, and dedicated hotspots, the desire to connect more devices to the Internet has also increased. IBM defines an IoT as a “concept of connecting any device (so long as it has an on/off switch) to the Internet and to other connected devices. The IoT is a giant network of connected things and people—all of which collect and share data about the way they are used and about the environment around them.” (Clark, 2016) As the Internet and devices have evolved, the types of devices that can be added to an IoT has also evolved. Some may be commonly used by all people, such as a smartphone or a computer, while some may be slightly more obscure to the non-technical user, such as newer automobiles, some types of medical equipment, and home security systems. An IoT device gives the user the ability to monitor and collect data remotely, no matter what type of device it is, provided that the device is able to connect to the Internet at that time.

One IoT device that has been rapidly growing in popularity is video recorders for home security. Video recorders can come in a number of different types, including video doorbells, indoor cameras, and external cameras. A video doorbell is similar to typical doorbells, which can produce a chime inside the house when run by a visitor, but also include a built-in camera. Many widely used models now also feature a microphone and speaker. This entire doorbell camera

connects back to the Internet. The doorbell camera provides the user with the ability to answer the door from anywhere with an Internet-connected device. The users who own the doorbell camera typically will receive a notification on their computer or smartphone when someone pushes the doorbell button, or if the camera senses motion. The users can talk with the person at the door through the built-in speaker and microphone without having to go to the door. This can be done from anywhere, including outside the home, with a second Internet-connected device. For example, a person can check on their smartphone who is at their door, even if the owner of the house is busy elsewhere in the house, down the street, or all the way around the world, and all they would need is access to the Internet. The silent motion-sensing notifications can be used to see what is going on outside, and record and possibly even deter potential criminals. Many doorbell camera companies, e.g.: Ring, tout that if a burglar sees a specific type of camera at a house, they may think twice about trying to rob it. (Owoseje, 2018)

While home video recorders undeniably have many upsides for the user, they also come with potential issues concerning security and privacy. To simplify the install process, for instance, manufactures may not be security-focused, instead streamlining the installation for ease of use. Per Popular Mechanics, in the past few years, there have been multiple incidents with home video recorders. (Blum, 2019) For example, in the case of Google Cam, there has been an increase in exploits which led to unauthorized users having the ability to view and communicate through the cameras. During one incident, an unauthorized

user gained access to a camera and used the built-in microphone to berate the owners with offensive language. In another incident, an unauthorized user was able to view the feed of a baby's room, learn the habits of the homeowners, and even learn the layout of the house. These exploits indicate a significant issues with respect to security and the configuration of the network to which these devices connect. These companies' failure to properly secure and configure a system can cause great stress and the loss of peace of mind for the owners of the cameras.

To prevent the possibility of security and privacy issues, it is advisable to use multiple layers of security. However, many people with non-technical backgrounds do not know exactly what that means. One exercise to better convey this idea is to imagine your home Internet network as an onion. Onions have many different layers; so does your network. Different layers of your network will have different security settings, letting certain information pass through. The goal is to only allow the information that you want to be processed fully to pass through. If this is implemented carefully and successfully, a malicious person trying to gain access to your home network or network-connected devices will be unable to do so. Unfortunately, no system is ever completely fool-proof. There are new exploits developed every day, and the "bad guys" are often working just as hard to exploit the Internet as the "good guys" are trying to keep it safe and secure. Your goal should be to make your network difficult for hackers to penetrate, increasing the likelihood that they give up out of frustration, or, if they do get in, delaying the breach so much that the information

they have obtained is no longer relevant to them. However, one must also refrain from locking down the network too much, as doing so may keep you from accessing your own cameras remotely, even though you are the trusted and intended user.

There are three layers of security that the common user should keep in mind to lessen the possibility of a malicious person gaining access to your system. They are (1) always keeping and regularly updating a strong password; (2) understanding and fixing any security vulnerabilities; and (3) understanding the manufacturer's privacy policy and recommended configuration settings. By leveraging all three security measures, gaining unauthorized access to your network becomes significantly more difficult and time-consuming.

The first layer of security we will discuss is the use and application of passwords. Almost all types of devices use passwords. Per the National Institute of Standards and Technology (NIST), a password is defined as an authentication method that "is a secret value intended to be chosen and memorized by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value." (National Institute of Standards and Technology, 2020) Devices use passwords to authenticate whether you are an authorized user in determining whether to grant access to a device.

Many people who install IoT devices, such as video recorders, get excited while installing their new device and skip some of the non-mandatory configuration settings in order to get the device running more quickly. However,

these are necessary to help secure the device. For example, many people forget (or may not even be aware of) the importance of updating the default password on a device. However, updating the passwords on your cameras alone is not enough to completely resolve potential problems; the default passwords should be updated on all networked devices, as a malefactor can gain access to one device on a network by first compromising a different one. Heimdal Security states, “By regularly changing your password(s) you reduce those hacking odds by more than 50 percent.” (Unterfingher, 2019)

One of the biggest challenges of using passwords as an authentication method is the vast number we have to remember. People tend to forget their passwords often, which sometimes leads to users developing bad habits in their password selections. In order to avoid forgetting her password, a use might choose one that is easy to remember. Some common examples include the word “password”, the individual’s name, their address, or other easily accessible public information about them. As a result, these passwords are easy for a malicious person to guess. When creating a password, the FBI states, per NIST guidance, that passwords should “include uppercase letters, lowercase letters, numbers, and special characters.” (Federal Bureau of Investigation) Further, it is good practice to change your password periodically in case an undisclosed data breach has occurred.

While following this guidance is a great start to having more secure passwords, this may not be enough to keep everyone out of your devices. A more secure approach is to also implement additional recent guidance from NIST

advising that password length is even more beneficial than complexity. (National Institute of Standards and Technology, 2020) A user is safest when using a password that is both long and complex.

There are further challenges in using passwords. Users often have different logins for different websites or devices on the Internet. If the user has chosen to use the same password across many different media, she could be exploited multiple times due to a single initial breach. Per the FBI 2018 Internet Crime Report, there were 50,643 different victims of a personal data breach in that year alone. (Gorham, 2018) In addition to using a different password for every unique website or device, another layer of security that users can implement is multi-factor authentication. The two primary types of authentication methods that devices support are (1) something you know and (2) something you have. An example of something you know is your password. To safeguard this authentication method, you should never share your password with anyone, and each user should have their own unique login, rather than sharing accounts. An example of something you have is using your smartphone to receive a temporary verification code that you use in combination with your password. When using two-factor authentication, the device or application you are trying to access will request both your password and the verification code; both factors are required to gain access. Two-factor authentication provides an extra layer of security if your password is ever compromised.

As home recording systems evolve, more and more people want to incorporate high-level recording systems for their homes, but also potentially for

their businesses. While attaching business cameras to the Internet can increase physical security, if they are not properly secured, they can lead to greater vulnerability if unauthorized users are able to gain access. Some examples of what an unauthorized user watching a feed could be: a combination to a safe over someone's shoulder, when security changes shift, or when staffing is lightest, leading to the best time to plan a robbery.

As IoT home security devices become more widespread and common around households, the number of targets for hackers or people with malicious intent also goes up. Since these devices are designed with built-in cameras, microphones, speakers, and access to the internet via Wi-Fi, this makes them a prime target for hacking, especially since connecting to the Internet via Wi-Fi is more exploitable than a standard cabled connection.

However, WiFi connectivity is not the only vulnerability IoT devices have. In November 2019, cybersecurity company Bitdefender discovered a vulnerability in Ring video doorbell software. (Ng, 2019) The issue occurs during the set-up process for the doorbell, when the user links the doorbell to the Ring application. The user has to input their Wi-Fi information to connect the application to the doorbell. This information gets sent through an unencrypted network, which means that anyone viewing the data at this time would be able to see the user's username and password for their Wi-Fi network. This is a huge issue because with the login information to one's Wi-Fi network, a malicious user could gain access to all connected computers and devices within one's network, including

the doorbell camera. Ring stated that this vulnerability was patched automatically three months after it was discovered. (O'Donnell, 2019)

In December of 2019, further issues were discovered with the Ring video devices. The vulnerabilities discovered were that the doorbell was not notifying owners of suspicious login attempts when the devices were accessed from new IP addresses, and that the software did not have a set limit on failed login attempts. There are many ways that malicious users can gain login information to devices, including data breaches, buying information on breached accounts, email phishing attempts, and others. As stated previously, many users have the bad habit of sharing the same password and login information across many, if not all, of their devices, so if a malicious user gains access to one account they could gain access to them all.

During an investigation, Ireland-based information technology company Motherboard logged into Ring accounts via the Ring app and website from various IP addresses worldwide; no suspicious login attempts were flagged by the software and sent to the owners of the devices, even when multiple logins occurred simultaneously. (Cox, 2019) Motherboard also found that once they were logged into the Ring account, they were able to access a wide array of information that wasn’t protected or encrypted. This information included the user’s Wi-Fi network information, home address, saved video footage, and saved audio. Once inside the account, the malicious user could also listen in on the devices live, which allows them to spy on the users in real time.

There have been many reported incidents of Ring device hijacking, such as one from early December 2019, reported by a couple in Grand Prairie, Texas. (Howerton, 2019) The hackers set off their Ring device alarms and started speaking through their Ring devices, threatening the users' lives and demanding ransom in untraceable bitcoin. The hacking of these devices has gotten so widespread that hackers have created their own podcast called "NulledCast" where they record themselves taking over people's devices.

While we used the Ring device vulnerabilities as an example, they are not the only surveillance devices susceptible to such vulnerability. Published research from the security firm Tenable discusses a vulnerability in software made by NUUO, a global video surveillance vendor. (Hatmaker, 2018) The software is used in cameras in all environments around the world such as banks, hospitals, schools, and homes. The vulnerability was named "Peekaboo." This vulnerability provides malicious users control of the video surveillance cameras that use the NUUO software, and allows the hackers the ability to monitor the feed, tamper with it, and also access the camera feed of any other device that the camera is connected to on the network.

While these devices were designed as a way to help monitor and protect homes and businesses, users should be aware that these devices can also give hackers and malicious users a way into them as well. Many users overlook potential vulnerabilities when setting up any type of device, focusing instead on the features and potential uses and benefits of the device. As shown above, if a hacker or malicious user is able to gain access to the IoT device, they have

access to not only view your video footage, but to tamper with the device itself, and potentially gain access to all devices on your network and linked accounts as well.

Overall, network video recording devices have made life easier for a number of people and their businesses. However, it can also be trivially easy for hackers to exploit if one does not take proper precautions. To secure IoT devices like network video recorders, always make sure to do your due diligence in setting up your network's security network; set up a strong, unique password for every device; and consider adding two-factor authentication. Lastly, check in on the device and its manufacturer periodically to make sure that no patches, changes, or unusual activities have occurred. While this won't make you immune to a hacker breaking in, working to make it as hard as possible for the bad guys might be what saves your system.

Works Cited

Blum, S. (2019, February 6). *Popular Mechanics*. Retrieved from https://www.popularmechanics.com/technology/security/a26214078/google-nest-hack-warning/

Clark, J. (2016, November 17). *International Business Machines*. Retrieved from https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

Cox, J. (2019, December 17). *Vice*. Retrieved from https://www.vice.com/en_us/article/epg4xm/amazon-ring-camera-security

Federal Bureau of Investigation. (n.d.). Retrieved from https://www.fbi.gov/video-repository/protected-voices-passphrases-and-mfa-102319.mp4/view

Gorham, M. (2018). *Federal Bureau of Investigation*. Retrieved from https://pdf.ic3.gov/2018_IC3Report.pdf

Hatmaker, T. (2018, September 17). *Tech Crunch*. Retrieved from https://techcrunch.com/2018/09/17/nuuo-peekaboo-tenable-vulnerability/

Howerton, M. (2019, December 11). *WFAA ABC Texas*. Retrieved from https://www.wfaa.com/article/news/hacker-says-pay-bitcoin-ransom-or-get-terminated-through-couples-ring-security-cameras/287-226c535c-c765-4b29-91b6-d849fb315e94

National Institute of Standards and Technology. (2020, March 3). *NIST*. Retrieved from https://pages.nist.gov/800-63-3/sp800-63b.html#memsecret

Ng, A. (2019, November 7). *CNet*. Retrieved from https://www.cnet.com/news/ring-doorbells-had-vulnerability-leaking-wi-fi-login-info-researchers-found/

O'Donnell, L. (2019, December 18). *Threat Post*. Retrieved from https://threatpost.com/ring-plagued-security-issues-hacks/151263/

Owoseje, T. (2018, November 5). *Independent*. Retrieved from https://www.independent.co.uk/news/world/americas/homeowner-burglars-doorbell-camera-video-edmonton-canada-clem-ho-a8618486.html

Unterfingher, V. (2019, December 6). *Heimdal Security*. Retrieved from https://heimdalsecurity.com/blog/home-security-cameras-safety/