# A Study on Security of IP Cameras and Its Awareness

*Adam Motowidlo*[1], *Timothy Adatsi*[2],
*Alvin Jackson*[3], *and Shushan Zhao*[4]

## Abstract

IP/smart cameras or Internet of Things (IoT) have become a popular trend over the years thanks to their many capabilities. They can automate, make tasks more manageable and monitor your home efficiently, and at the same time, make you feel safer. However, because these devices can connect to the internet, there is a possibility that they can become a security risk to the users. Whenever a smart device is accessible on the internet, it is possible for other individuals, or hackers to access the device. This research aims to identify and analyze consumers' basic knowledge about network security and the dangers of unsecured IP cameras. The research comprises of a survey on security awareness on these devices, and experiments on exploitation of known vulnerabilities. With the results, we can understand and learn major issues about security of these devices.

***Keywords :*** **Internet of Things, IoT, IP camera , network camera**

## I. INTRODUCTION

With the ongoing advances of network devices and IP cameras (also known as smart cameras, or network cameras), more and more smart devices are being integrated into other networks, hence becoming an Internet of Things (IoTs). An IoT is a device or a group of devices that are connected to the internet for the purpose of exchanging data or are used for other purposes. Thanks to internet access, users can easily access their IP cameras from far, one example, using a smartphone. Thanks to these smart devices, tasks and security have become more automated, and they have made our lives more comfortable, but there is a major concern when it comes to security. When owning an IP camera, or any device that connects to the internet, those devices can potentially expose your network. These devices can become backdoor entryways for intruders or threat actors from the internet, hence become a security risk and this is not being managed or handled properly.

IoTs have become a trend in the past decade, thanks to their ease of use and practicality, but how certain are you that the camera you own is secured or safe to use? Especially, as time progresses, new hardware and devices replace the older ones, while the older devices become obsolete or "outdated". It may come as no surprise, but new vulnerabilities are found daily, and manufacturers are liable for patching these vulnerabilities nearly every

Manuscript Received : December 20, 2021 ; Revised : January 10, 2022 ; Accepted : January 15, 2022. Date of Publication : February 5, 2022.

A. Motowidlo[1] is *Master Student*;
Email : motowidlo@my.ccsu.edu ; ORCID iD : https://orcid.org/0001-9404-2946
T. Adatsi[2] is *Master Student*;
Email : tadatsi@my.ccsu.edu ; ORCID iD : https://orcid.org/0000-0002-8763-9610
A. Jackson[3] is *Master Student*;
Email : alvinjackson@my.ccsu.edu ; ORCID iD : https://orcid.org/0000-0002-0381-5489
S. Zhao[4] is *Assistant Professor* ;
Email : shushanz@ccsu.edu ; ORCID iD : https://orcid.org/0000-0002-3142-3626

Department of Computer Electronics & Graphics Technology, Central Connecticut State University, 1615 Stanley Street, New Britain, CT 06050, USA[1,2,3,4]

**DOI : https//doi.org/10.17010/ijcs/2022/v7/i1/168956**

day, but not for a lifetime. An attack targeting a vulnerability in a system or device that has been disclosed but is not yet patched is known as zero-day attack. Any product that is connected to the internet can and will be prone to hacking and your privacy can be invaded. As Murphy's law dictates, “If anything can go wrong, it will”, and certainly, this has become a fact.

As of now, IP cameras are known to be one of the most known exploitable and favored tools for hackers to use to this day. The number of exploited devices continue to soar, and cameras are only one means of intrusion. “Upto 30 billion devices will come online by 2020, including insecure webcams, baby monitors, and other devices that can be enslaved and collectively wielded as a weapon.” [1]. The market for IP cameras is increasing and so are the unsecured ones. Many consumers are unaware of how or why this isn't being managed properly.

IP cameras and other IoT devices may receive updates from their manufacturers, but users are also responsible for managing and securing their own network. If users fail to update their devices and fail to understand the risks of using outdated equipment, then they are responsible for the security of their network. If a hacker is able to take hold of a smart device without the owner's knowledge, the device could forever be used as a backdoor to your network. In the end, both manufacturer and consumers alike must uphold practices to protect their networks.

Our hypothesis is that we believe that most consumers are unaware of potential security risks of carrying outdated/unsecured IP cameras and are unknowingly putting their networks in risk. One proof to support our hypothesis is the continuous rise of hacked devices and cybercrimes. The purpose of our research is to help identify these unsecured devices and spread awareness in the community. Through our research, we can estimate the number of people at risk and find a general reasoning.

The rest of this paper is organized as follows: Section II reviews related work in the area of IP camera security in literature. Section III shows overview of our research. Section IV presents survey results. Our experiments and techniques employed to exploit the vulnerabilities are explained and demonstrated in Section V. Section VI discusses our thoughts to improve security of IP cameras. Section VII concludes the paper.

## II. LITERATURE REVIEW AND RELATED WORK

There is an extensive literature on various aspects of security of IP cameras.

In [2], Abdalla and Varol study and analyze security elements of an IP camera. The authors explain the most common security problems that are found within an IP camera. The authors include examples such as leaving the default login credentials, simple-to-imagine keys, poor authentication methods, and low or no encryption methods. Not only are these common security problems found within an IP camera, you will also find many other IoTs today. For this experiment, the author will use several penetrating tools such as Wireshark, Kali-Linux, Arpspoof, and others to discover flaws within the selected IP camera. From their findings, it seems that the IP camera has more vulnerabilities than initially anticipated. The IP camera has two default login credentials for identification and password, in this case, they already found a back door or another entry way into the IP camera. The fact that there is another entry way is concerning since it is an entry way not known to common users and it was configured with a weak password, making this device even more vulnerable than it should have been.

These days, cloud-based systems have proven to be useful for IP cameras when large amount of storage is needed to store recordings. Although they are useful, cloud-based networks are at risk because of IP cameras. In [3], the authors investigate how an IP camera's traffic could be sniffed and possibly expose a cloud network. For this research, the authors have chosen an easy plug-in-play IP camera called NetCam. The goal of this research was to expose IP camera devices and other IoT from possible threat actors, a single or group of people who can take action to cause harm on certain devices. The authors of this research claim that IP cameras are highly unsecured devices even if they are placed in a private network, they can still be found. Despite what some might think, as long as your network has access to the internet, hackers can still detect these cameras. Another reason why these devices can be easily targeted is that the devices can be connected to a cloud or server. With experiment the researchers prove that they are able to gain access to the device and demonstrate how weak the security that NetCam possessed was. This further proves that manufacturers are partially responsible for placing weak security standards on their devices. At this point, a patch may not fix this device if these ports remain open, making this device obsolete.

Closed Circuit Television (CCTV) systems, IoT, and IP cameras have proliferated in businesses and for private use. In [4] it is shown that cameras from 79 vendors are vulnerable to Remote Code Execution (RCE), or more commonly known as remote hacking. The purpose of the study was to provide identification of vulnerabilities and guidance for the protection of surveillance camera systems. The authors completed their research study in six phases that "include literature review, system setup, pilot testing, data collection, data analysis and its comparison with results of previous research". Of note, the authors created a pilot study and experiment conducted by testing an internet camera by trying different exploits. They used multiple tools including Angry IP Scanner, WireShark, Ophcrack, Burpsuite, Nmap Hydra, Nikto, Metasploit, and Cain & Abel for data collection while using Windows Explorer, DMMultiview, and GvIP Device Utility to access and remotely manage a target camera.

In [5] the authors' objectives were to understand what kind of data is publicly accessible from internet connected smart cameras, whether that data could be used to cause privacy and security risks in home, and the approximate number of network cameras on a worldwide scale that could be potentially accessed using known vulnerabilities by unauthorized users. Using a tool called Shodan, the authors discovered thousands of smart connected cameras broadcasting at different locations. It was noted by the authors that the tools used such as Shodan and NMap could be used by an individual with little experience in programming or coding knowledge.

In [6] the researchers provide engineers a better way to harden or secure modern video surveillance systems. They describe several known facts, methods of attacks, and tools to find these devices online by using search engines like Shodan and Censys. Moreover, of these devices, 90% do not have secure login portals and use HTTP which is not encrypted, whereas HTTPS is. The researcher gave numerous reasons why devices like IP cameras can be attacked by threat actors. These devices can be attacked through different channels and can be used for different purposes. One reason why threat actors would take over a video surveillance system is that they are looking to sabotage a certain individual. A threat actor would be able to watch a live or pre-recorded video footage for either spying, blackmail, searching for valuables and/or to study the individual's behavior. The fact that the threat actor has taken over the device is already a violation of privacy.

Kim and Han [7] identify the security model of today's internet cameras, the threats they face, and outline methods of securely implementing such devices. The security threats include eavesdropping, interruption, modification of data, unauthorized access, repudiation, and illegal monitoring. Functions of a secure network camera include privacy masking, user/device authentication, security tunneling, access control, intrusion prevention, prevention of forgery, and prevention of misuse. The functions of a secure network previously mentioned by the authors are essential for ensuring the safety of modern video surveillance networks. Each function of a secure network presented above must be implemented in relation to each specific network requirement. The authors go into extensive details to illustrate and explain how a secure network should be pursued. Their study and models illustrate a technical outline that provides the reader with in-depth knowledge of inner workings of video surveillance and security structure.

Costin [8] presents each type of visual or online attack and demonstrate a solution or means of ways to counter each attack; some of these attacks can be obscure. Other than exploiting a camera through physical or hacking methods, there are different variety of visual attacks on CCTVs through obscuration and steganography. The author explains how steganography can be used to insert malicious code within an image, like hiding a URL within an image which can exploit the camera to run malicious code. These types of attacks are useful for our knowledge and give us insight on how hackers can easily gain access to an IP camera or CCTV.

In [9], a way to detect cameras through encrypted connections further proves that creating a system detects these smart cameras in those environments. "The goal of our work therefore, is to present a novel service discovery framework for remote access of smart cameras with NAT traversal and SSL/TLS." The research has given us further insight about detecting smart cameras through some of these techniques, such as IP filtering, heartbeat flow extraction and device identification. Other than using search engines like Shodan to search for open smart cameras, the author of this research employs CAMHUNTER, a detection system that was created for this research. By using a certain set of algorithms and techniques, this software can discover IP/smart cameras through the internet through SSL/TLS protocols, these are connections that are encrypted. After studying their models, they employed CAMHUNTER and from their results, they have shown that CAMHUNTER has an accuracy of 100% for detecting smart cameras behind NATs. This paper further proves that smart cameras are still detected through encrypted protocols, which means that they can be exposed on the internet.

As for reasons why IP or smart cameras have become so favored or sought out, in [10] some explanation is given. The authors explain how smart cameras are easily exploitable and produced, as well as how large a risk they are within a cloud-based system, and give us more understanding of how IP cameras can become more intrusive than we initially thought of when a cloud-based network is involved. When a network camera is placed within a cloud system, you can expect the intrusion to be devastating since the network is more spread out within a cloud-based network. If a smart camera is placed within a cloud, the hacker could easily traverse from one network to the next. The author stresses how dangerous these smart cameras can become when placed within a home cloud network, the security or firewalls placed in that network would be irrelevant in this case.

To enhance security of IP cameras and IoT devices, Koo and Kim [11] point out that security compliance is one of the largest factors when protecting private data. By following such practices, consumers would be able to authenticate themselves and protect their information at the same time. Lee [12] suggests that the government should create a backed certification or protection for privacy of all consumers or citizens when handling IoT. An unsecured IoT can become intrusive in one's personal life and must be prevented by additional means. The government should aid with deploying IoT with more care since unsecured devices can also greatly affect the economy.

There is not much work in literature on users' awareness of security of IP cameras or IoT devices.

## III. OVERVIEW OF OUR RESEARCH

This study comprises of a survey and a series of experiments. The survey is to collect data of a user's common knowledge about network security practices and their behavior. The means will involve sending surveys to students attending Central Connecticut State University and they must be owners of IP cameras. The survey will also help us identify what percentage of students secure their IP cameras or network. We can then determine how vulnerable a student's network is. The survey consists of two segments of questions, the first section is a simple yes and no portion which questions users about their own network and how they manage it. The second set of questions is a five-point Likert scale survey, from one to five: strongly agree (1) to strongly disagree (5). The questions also base the user's personality or concerns about their network, giving us and idea of what kind of users they are. These questions include whether users have taken precautions on their home devices/networks and how they manage it. At the same time, the survey serves as a basis of awareness, providing them basic security practices and how they can secure their own network.

To understand more, this research explores these objectives to understand the gap:

**(1)** Identify and determine which IP cameras can become exploitable by hackers and how they become intrusive.

**(2)** Establish what measures or standards should be taken to secure a homeowner's smart camera and network.

**(3)** Identify the most secured and weakest smart camera brand.

**(4)** Identify the average lifespan of a smart camera and determine how long manufacturers support their products.

There is a limitation in this research. One is that we must respect the privacy of an owner's home network as well as the number of people who are willing to take the survey. It would be prudent not to force those who do not understand the core concept of the survey and other technical terms. Furthermore, the responses that we collected were anonymous to protect the identity of the people who answered the survey.

The period of the present research was August 2021 to December 2021.As a part of our project, we experiment on known risks and vulnerabilities of IP cameras and demonstrate how they can be exposed on a network and how they can become intrusive devices. We purchased a few modern IP cameras from a reputable market and tested their security functions. We then simulated a regular home network and exhibited how these cameras can become intrusive back doors and how they can be used against homeowners.

With the results of our data, we prove our hypothesis and establish an optimal way of securing a home network.

## IV. THE SURVEY ON SECURITY AWARENESS OF IP CAMERAS

The survey that we created was developed in Google Forms. Not only was the survey accessible online, we were able to present our surveys online via email and Teams provided by the university also. The purpose of our survey was to help gain a bit of insight on how camera owners and users manage their IP cameras or other IoTs. By asking directly, we were able to understand more about how concerned or wary users are. For this project, we presented our surveys to the students attending Central Connecticut State University and for approximately two months we gathered 117 responses. The demographics of this survey was mainly filled out by students in the campus, ranging from the age of twenty to late thirties, all of whom own IP cameras and other networking devices. With this survey, we can have a clear idea how students are managing their devices.

The survey is separated into two segments, the first being a simple yes and no answer regarding general internet security. Many of these questions ask students whether they have taken precautions for their IP cameras, set basic security functions and/or other preventative measures. The second segment of the survey is designed in a Likert Scale. In this section the questions ask about the student's personality and behavior with regard to their concerns about online security and network management. By gauging these questions, we can understand how students feel about their privacy concern when owning an IP camera.

In the first segment of the survey, we first asked, “Do you have a password set on your IP/smart camera(s)?”. A simple question that should obviously yield a high result of “yes”, but surprisingly, a staggering 63.2% of students answered “No” (Fig. 1). To many, setting a password may not seem important, but it should and must be taken on priority. A device that has no password means that anyone can access it without permission. One theory is that students may believe that the device can only be accessed in person, but if connected to the internet, it can be accessed remotely. Earlier, in the literature review, research has shown us that many smart cameras are vulnerable because of not having proper passwords for devices. This data has already shown that many of the students are unaware how this can lead to intrusion.

Other than setting password for IP cameras, it is also imperative to set passwords for the rest of network devices or other IoTs, including the owners of Wi-Fi network. The next question we asked was whether the students had placed passwords on their devices, and stats show that nearly 26.5% had not. (Fig. 2). Having an open network or an IoT without a password is the same as leaving your car door open and having your keys in the ignition which anyone can take. Another example of this would be an infamous case where a casino was hacked because an open fish-tank thermometer was left without a password. Here, 64.1% of students have not taken precautions, meaning many of the students are carrying risk of an attack.

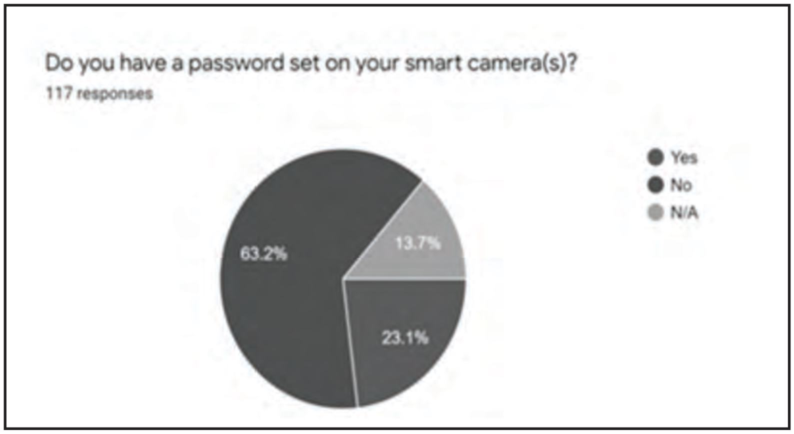


**Fig. 1 Result of Survey Question 1**

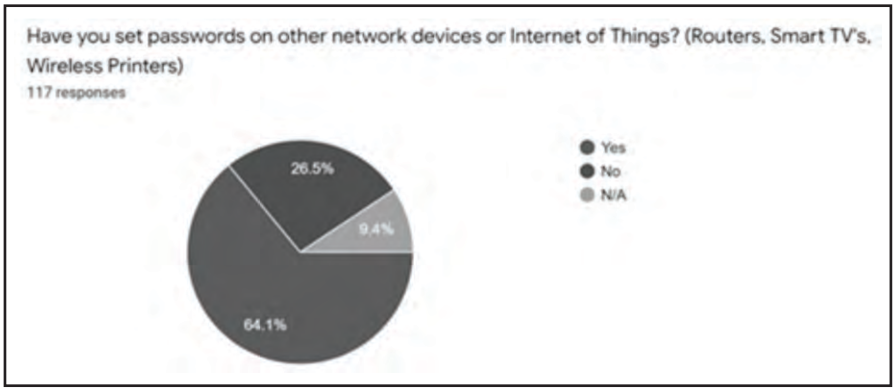


Fig. 2 Result of Survey Question 2

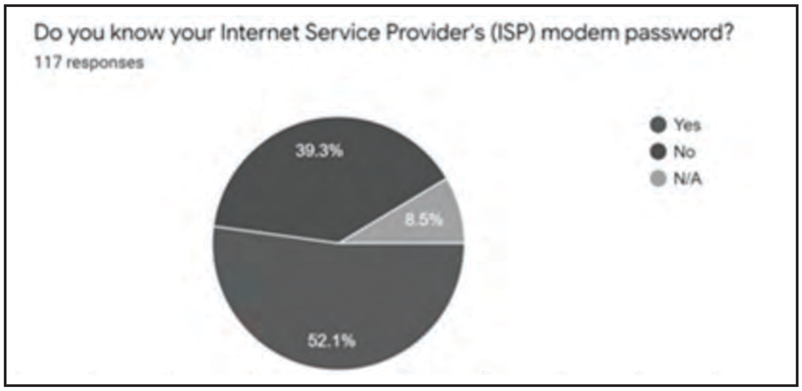


Fig. 3 Result of Survey Question 3

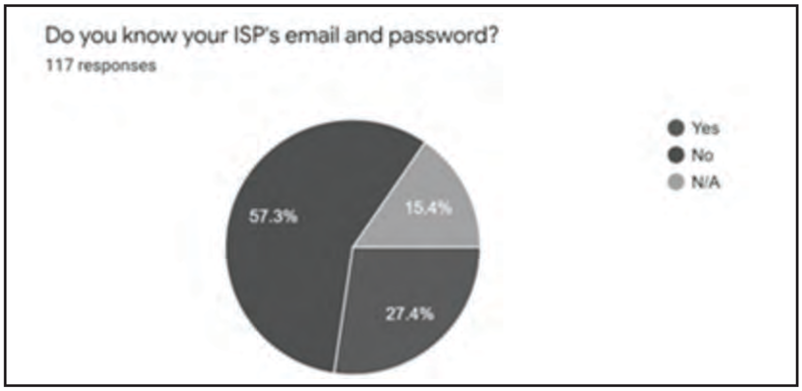


Fig. 4 Result of Survey Question 4

The next set of questions asked students about their Internet Service Provider (ISP) modem. This can vary as there are many ISPs and they all supply different routers. Many supply customers with routers that may have default credentials, which can be found online. We asked students if they have set a password or know their account passwords. The survey revealed that around 40% have not set a password and 57% do not know their account password (Fig. 3 and 4). The ISP modem is the device that governs and communicates with the internet, hackers can easily access this device and can intrude a user's network. The data continues to show that nearly half of the students who have taken this survey were not familiar with this practice and did not know how dangerous this is.

To further prove this, we asked the students the next question, “Do you have a firewall installed in your

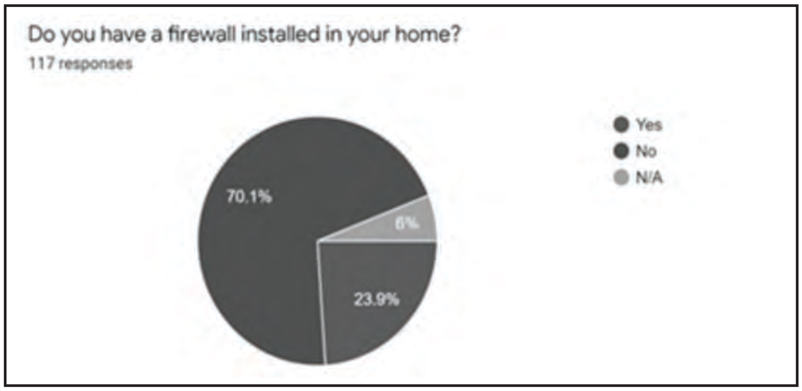


Fig. 5 Result of Survey Question 5

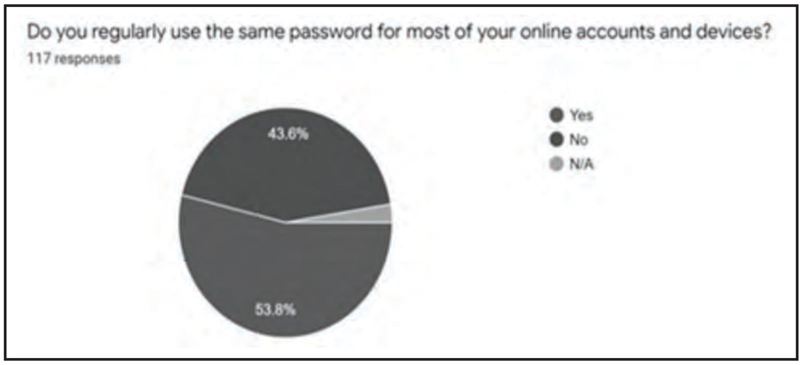


Fig. 6. Result of Survey Question 6

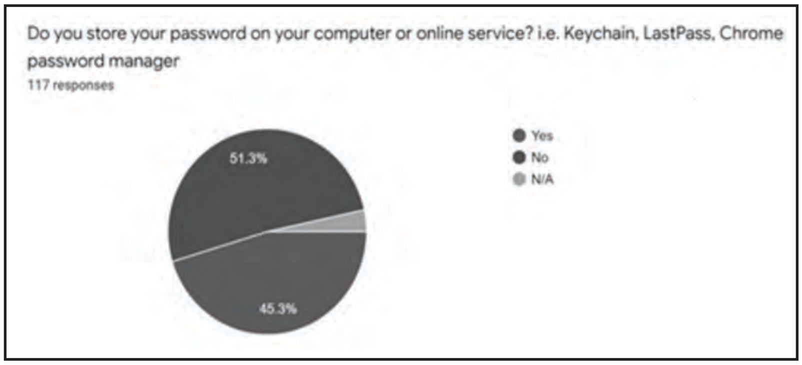


Fig. 7. Result of Survey Question 7

home?". This is technically a trick question as the ISP modem acts as a firewall if properly configured by the ISP. Out of all the questions, this question has the largest "No" ratio of 70.1% (Fig. 5). This shows us that nearly a quarter of the students who have taken the survey understood the question or are possibly not aware of what a firewall is. Today, firewall modems can be purchased in many different varieties, and they can be configured easily to protect your network.

For the next set of questions, we asked users a series of questions regarding strong password, password storage services, and security questions (Fig. 6, 7, and 8). The responses show that 40-60% of students have been using the same passwords, security answer, and password services. It may seem a bit personal to ask such questions, however, these are important when it comes to online privacy. Hackers would essentially use reverse social engineering and targeting techniques to gather as much information of a user as they can. If users rely on the same passwords or store them for easy access, hackers could

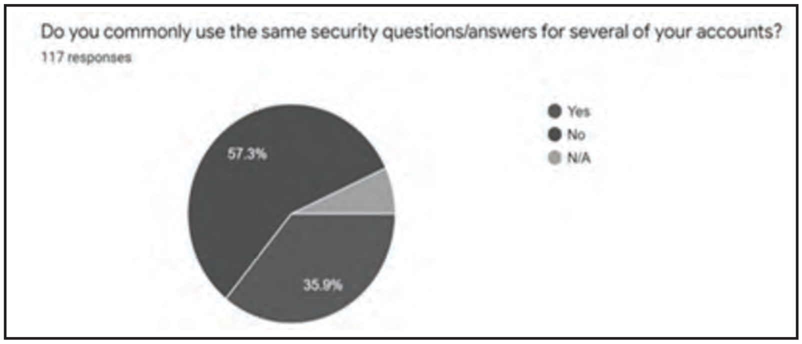


**Fig. 8. Result of Survey Question 8**

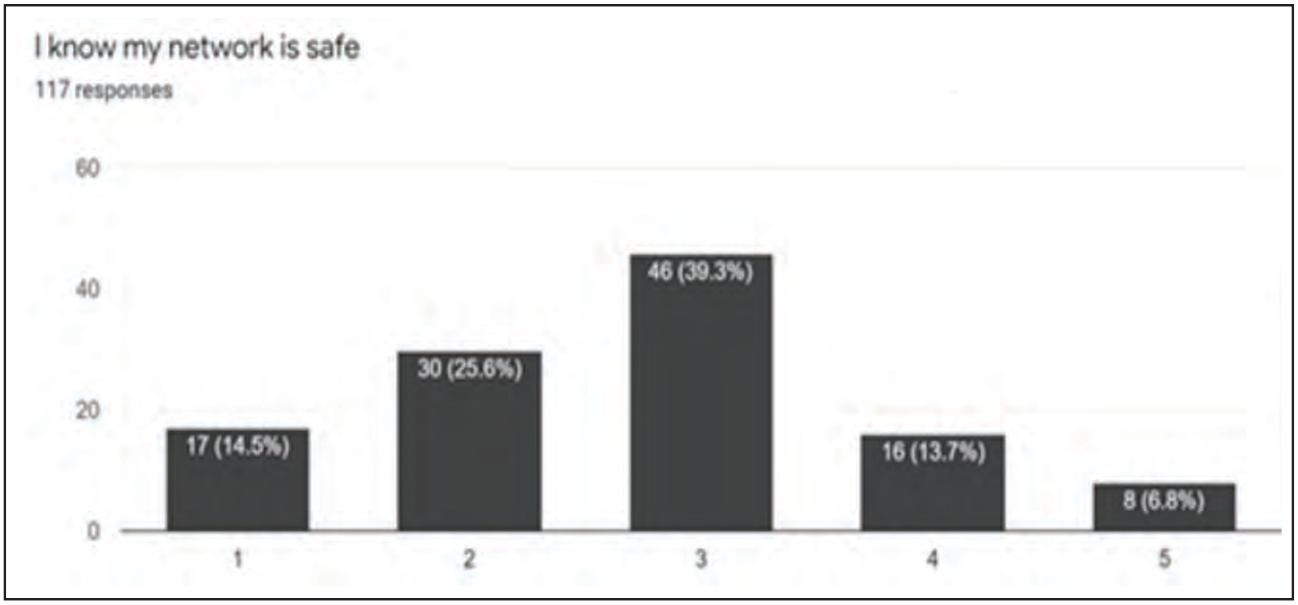


**Fig. 9. Result of Survey Question 9**

easily guess other accounts with the same password. Generally, users are responsible for managing their own passwords and security questions. Yet, if hackers try to gain more information of a user, they try to gain as much information for malicious means, even going as far as stealing a user's personal bank information. This survey reveals that most students are unaware of this danger.

The next segment of our survey has behavioral questions, it is structured in the form of a Likert Scale from 1-5, from ‘Strongly Agree’ to ‘Strongly Disagree’. These questions help provide an insight into how students feel about common internet practices and how much concern they have about their IP cameras and network. Not only were we able to have a more diverse answer, many of the responses had many different ratios.

The very first question we asked the users was the following: “I know my network is safe”. This behavioral response is partially a trick question, as no one can assume that his network is safe. Hackers can intrude your network without your knowledge unless precautions are set. The responses we received varied, although the majority agreed that they were unsure if their network was safe (Fig. 9). Around 40% of the students have answered that their network is safe, which is most likely wrong, as any device in a network could be prone to attacks without the user’s knowledge.

Next, we asked the students about their privacy concern when using social media such as Facebook (Fig. 10). The data shows us that most students have a some mistrust of sharing their privacy online and only around 15% of students have no concern. This shows us that the majority of students are atleast wary of privacy concern when

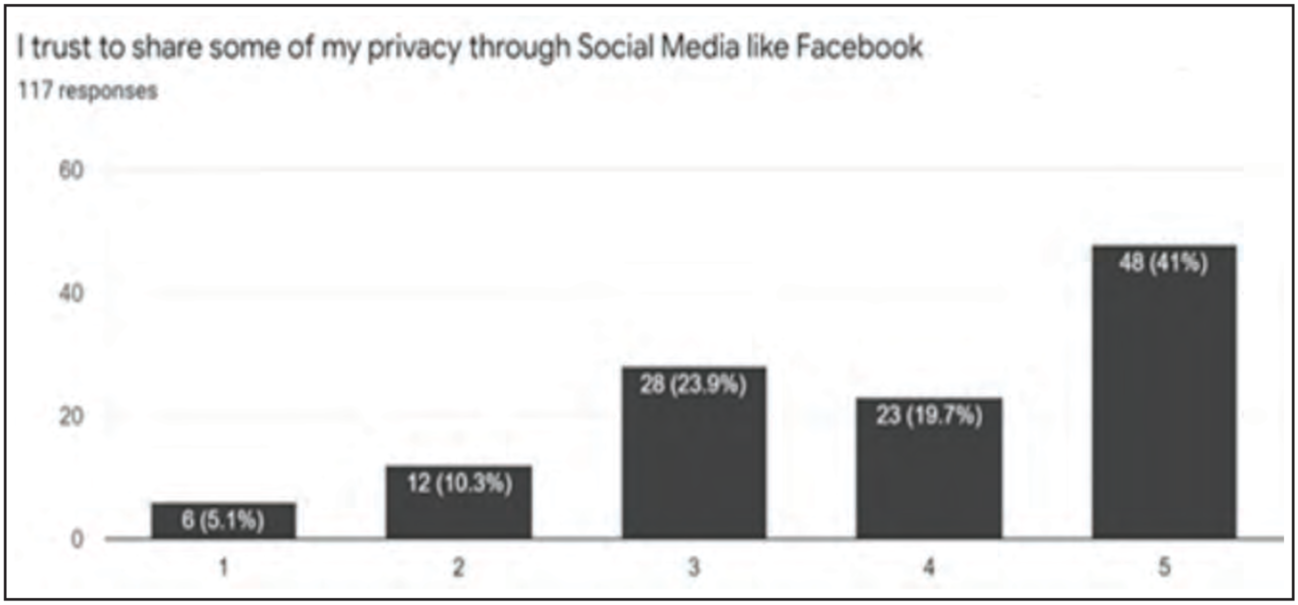


**Fig. 10. Result of Survey Question 10**

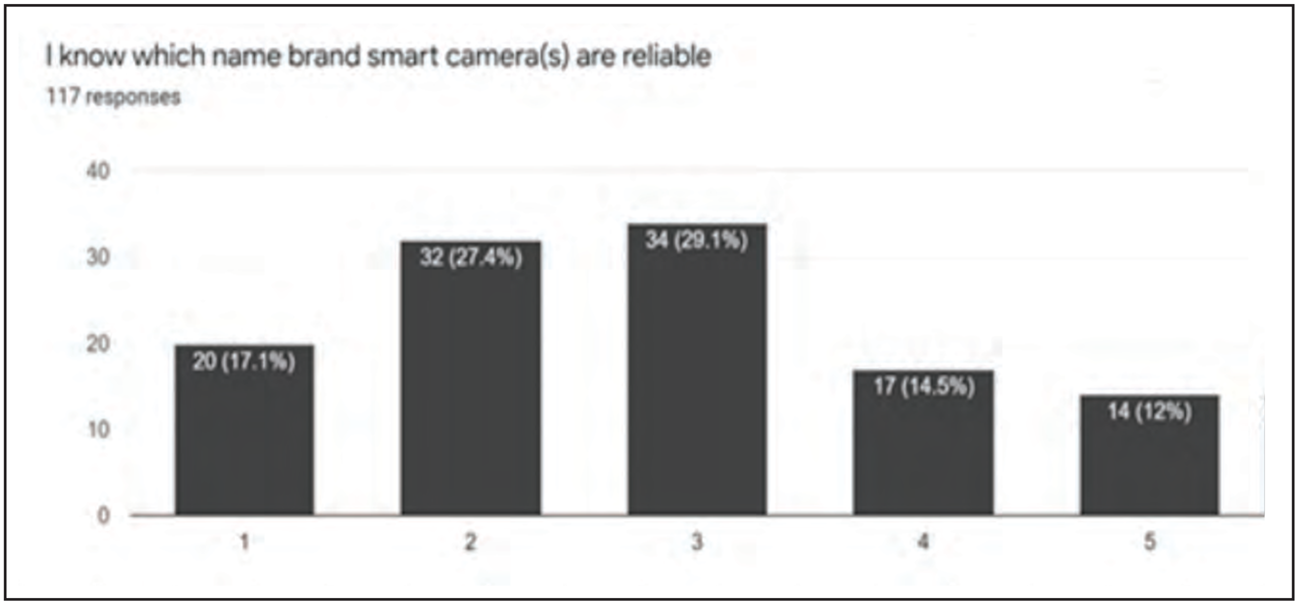


**Fig. 11. Result of Survey Question 11**

using social media. Today, reverse social engineering is one favored attack for hackers to gain access of user information. One infamous example would be Donald Trump's Twitter account being exposed in December 2020, when his Twitter account password was guessed as "maga2020!" [13] .

For the next question, we asked students about reliable name brands for IP cameras. The data has shown that the answers were diverse across the board (Fig. 11). This means that many of the students are evenly sure or unsure of which name brands to purchase or which smart cameras are trustworthy. Name brands today can be associated by attribute and promises made by the company, but quality is not one of them. Purchasing a product due to pricing is not considered good quality, a name brand's reputation is what is important. Our literature review has revealed that many of the IP cameras made by Chinese name brands are inferior and have little network security implemented. Sadly, many of these products can be found on today's market and their name brands can be changed at times.

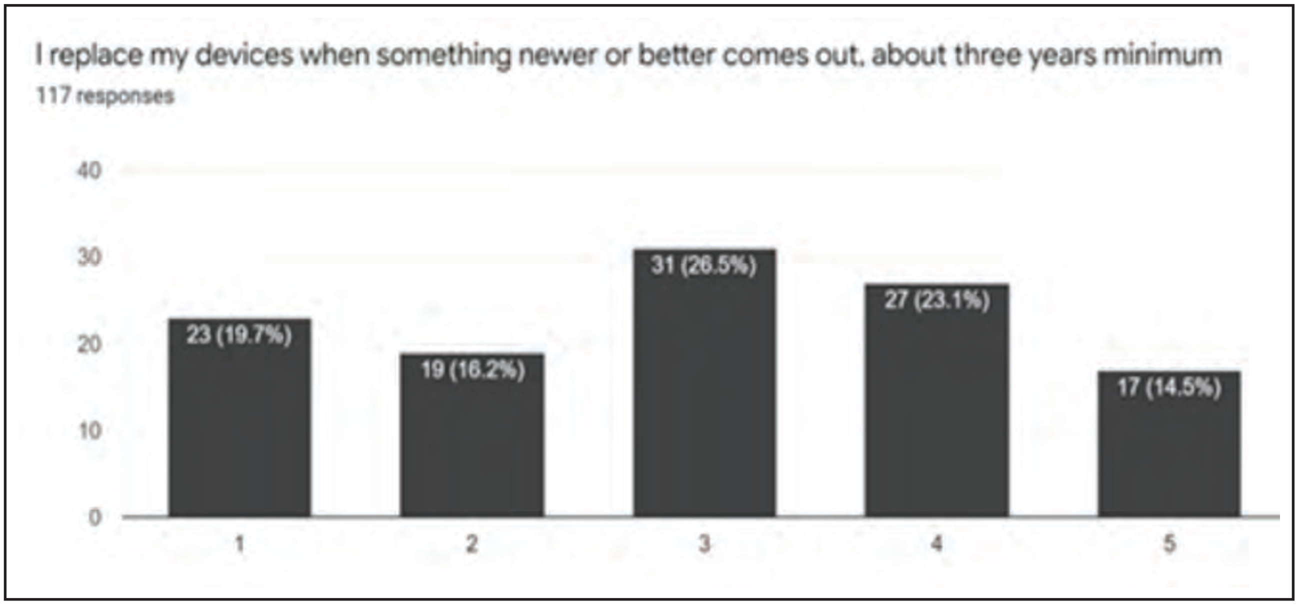


Fig. 12. Result of Survey Question 12

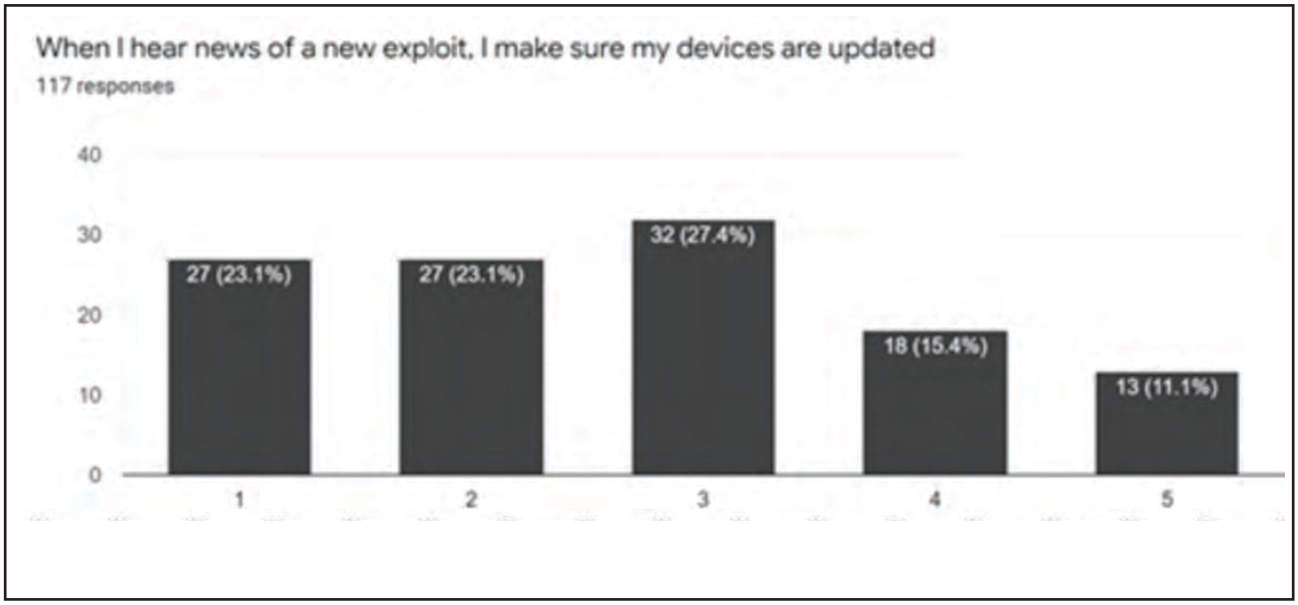


Fig. 13. Result of Survey Question 13

Another important question that we asked the students was if they would replace their devices for a new one for atleast three years . Our results show that nearly 38% of respondents disagree with this, which is a bit concerning (Fig. 12). From time to time, smart cameras and IoT have a short life cycle, depending on the make and brand. At best, many devices have support for atleast five years. The reason the life cycles are short is new advances and programming human society has created every day. From analyzing this data, we can conclude that many of the students are unaware that older devices could become exploitable over time (Fig. 13). It may not be discovered yet, but if hackers were given ample amount of time, they would eventually find an exploit. The same could be applied to any IoT, any device could be reverse engineered and eventually be used for malicious means.

Having safeguards can be beneficial in a home network, such has having VPN or an anti-virus program. For the next couple of questions, we asked students if they had applied such safeguards (Fig. 14 and 15). Again, the

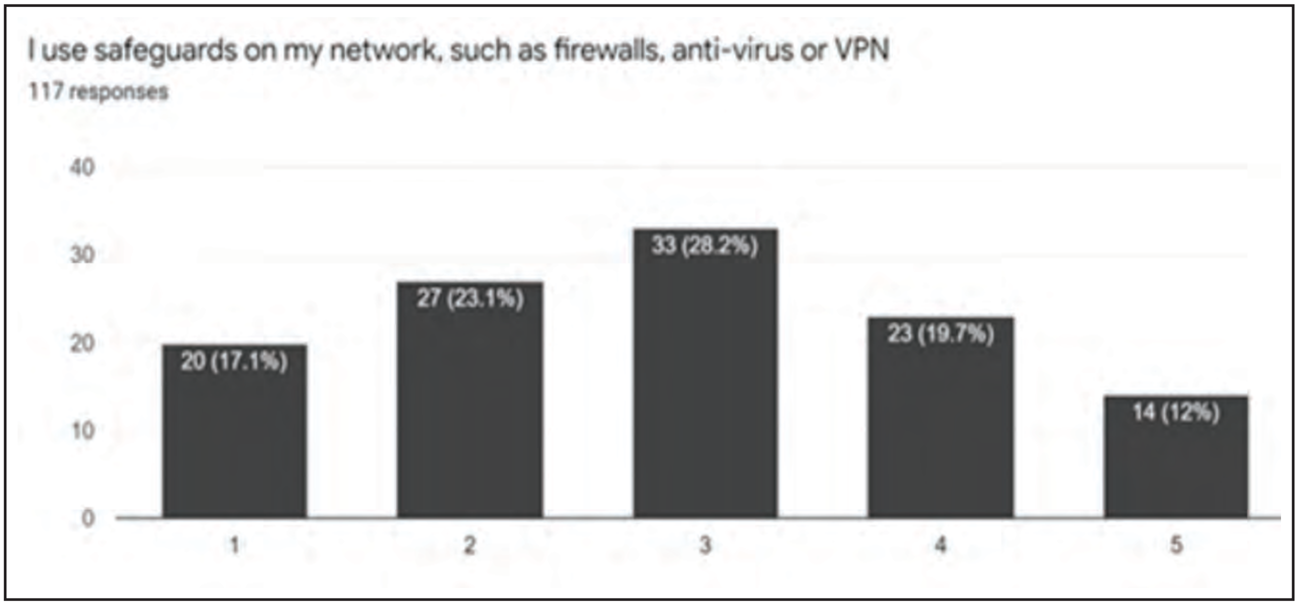


Fig. 14. Result of Survey Question 14

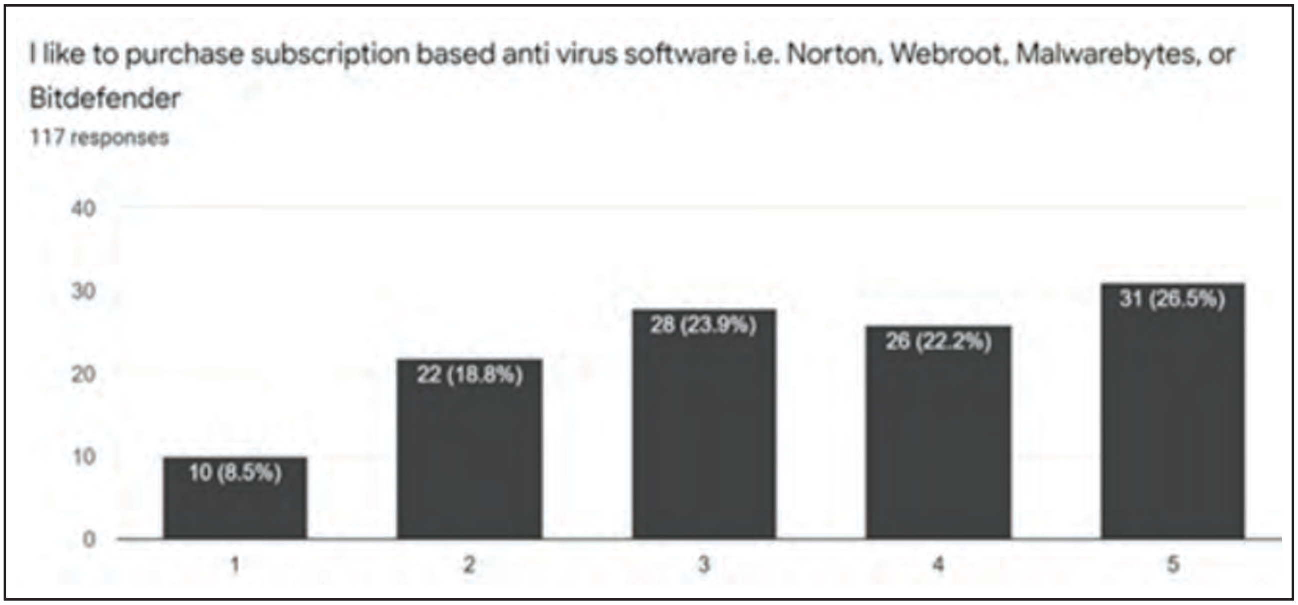


Fig. 15. Result of Survey Question 15

data shows a diverse answer and nearly half the students are not adopting such security guards. Having an anti-virus can protect users from malware and sometimes can prevent ransomware from occurring. VPN also provides secured connections over the internet, preventing hackers from accessing your network. It is true that both services are not free, but having such safeguards can become beneficial when data needs to be protected.

Integrity is an important security practice in which data has been secured, have not been modified or destroyed. For the next two questions, we asked users if they have backed up their data either through a cloud-based system or using a flash drive. When asking users how they backed up their data, we found that most of the students do not back their data physically (Fig. 16 and 17). In fact, more than 50% of the students have backed up their data on a cloud-based system rather than physically, this is another concern.

Even if users were to opt for a cloud-based backup, a cloud-based system is never fully secure. From literature

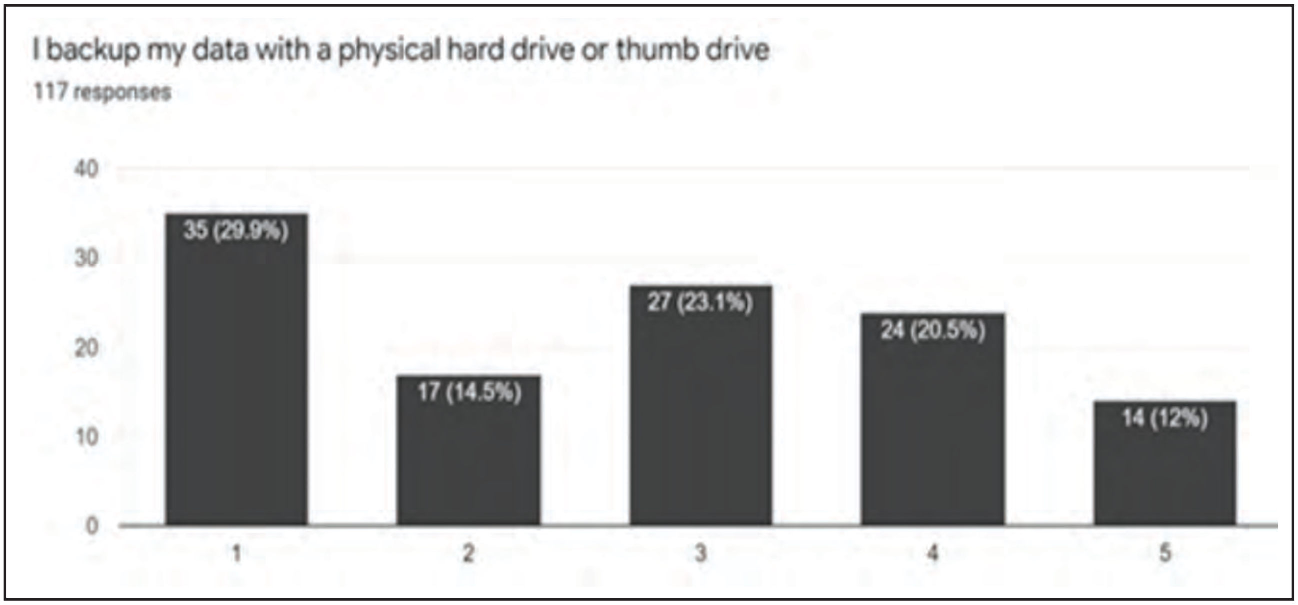


Fig. 16. Result of Survey Question 16

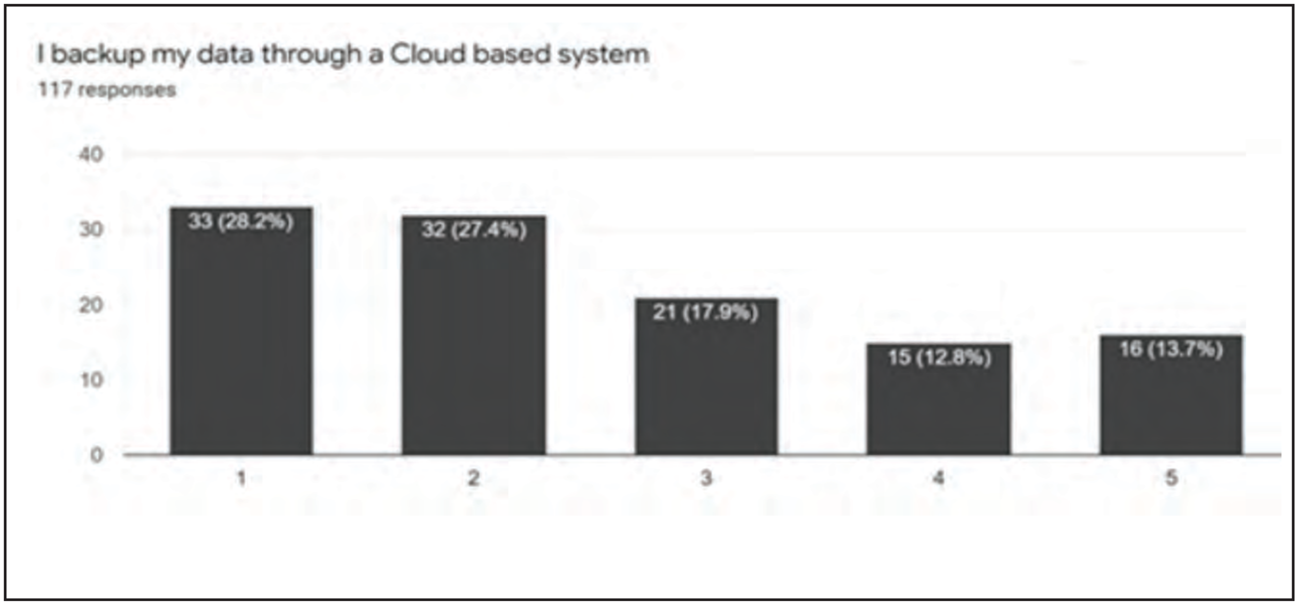


Fig. 17. Result of Survey Question 17

review, we found that many cloud-based systems are favored to be attacked by hackers and owning an unsecured IP camera adds to this risk. Any device or software that is linked to the internet can be attacked, meaning that data that is placed in a cloud is also in jeopardy. If data on a cloud has been altered, then the integrity has been compromised. The data could be destroyed or worse, it could be prone to ransomware in which users must pay to retake their data back. This further proves that the majority of students are unaware of security risks to cloud-based products.

Next, we asked students about connecting to unknown or unfamiliar Wi-Fi signals in their homes. From the responses, we see that nearly 24% of students do connect to Wi-Fi that they are unfamiliar with (Fig. 18). Similarly, we also asked the students about connecting to a public Wi-Fi area, in which case, more than half the students agreed that they did (Fig. 19). This is proof that most of the students are unaware about monitoring attacks, a method in which hackers can intercept Wi-Fi traffic between two devices such as MITM. Not only can

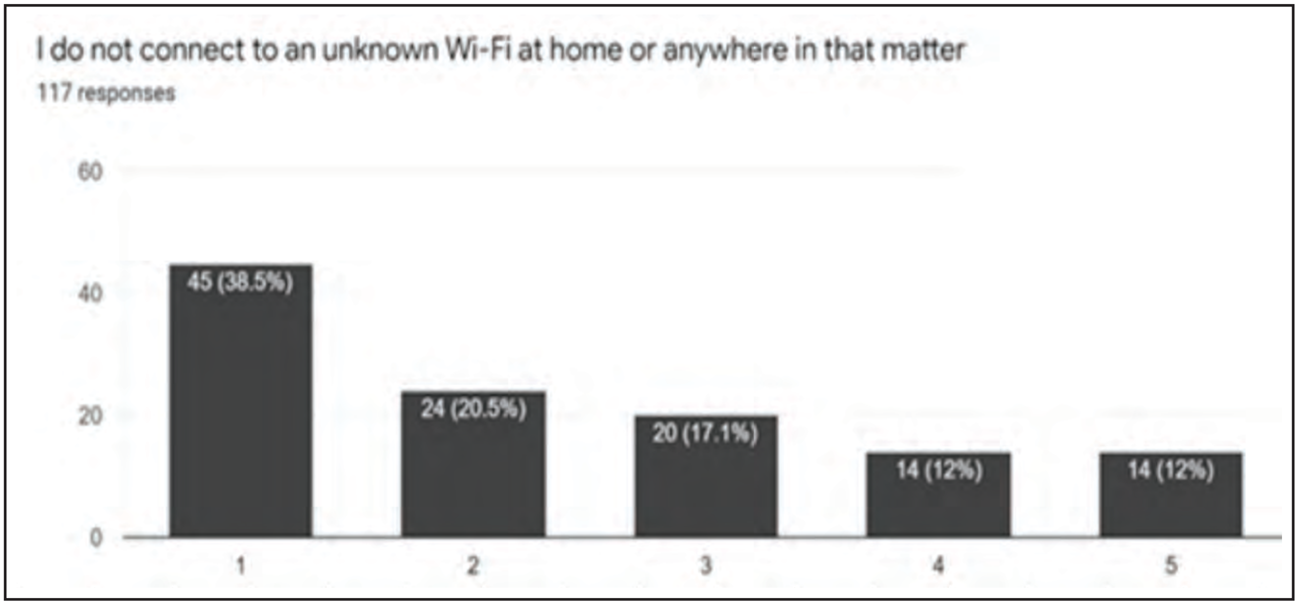


Fig. 18. Result of Survey Question 18

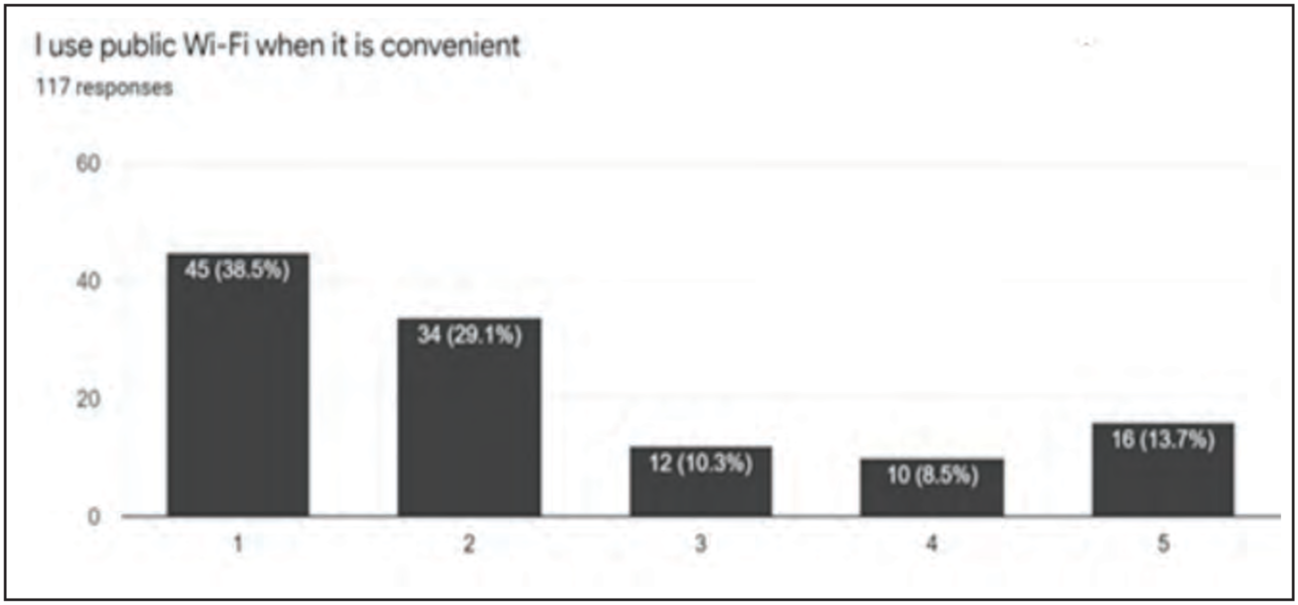


Fig. 19. Result of Survey Question 19

information and data be intercepted, but something as valuable as passwords can be seen by hackers.

Hackers today are known to mostly target large corporations for big game or for more valuable data. Even though the survey responses we have received are all from students, we can also assume that some of the students also have full-time or part time jobs. So, for the next question, we asked if students separate their work from their personal computer. The responses show that more than half the students often use their personal computers for work, another concern as this could jeopardize their employer's data (Fig. 20). This shows us that most of the students are unaware how a personal computer can compromise their employers' network.

In most cases, companies offer to lend their own computers to their employees to mitigate or prevent data leak, such as using a company VPN and anti-virus software. Methods like these are a standard in most organizations, although not everyone adopts this method. In the worst case scenario, if an employee had a personal

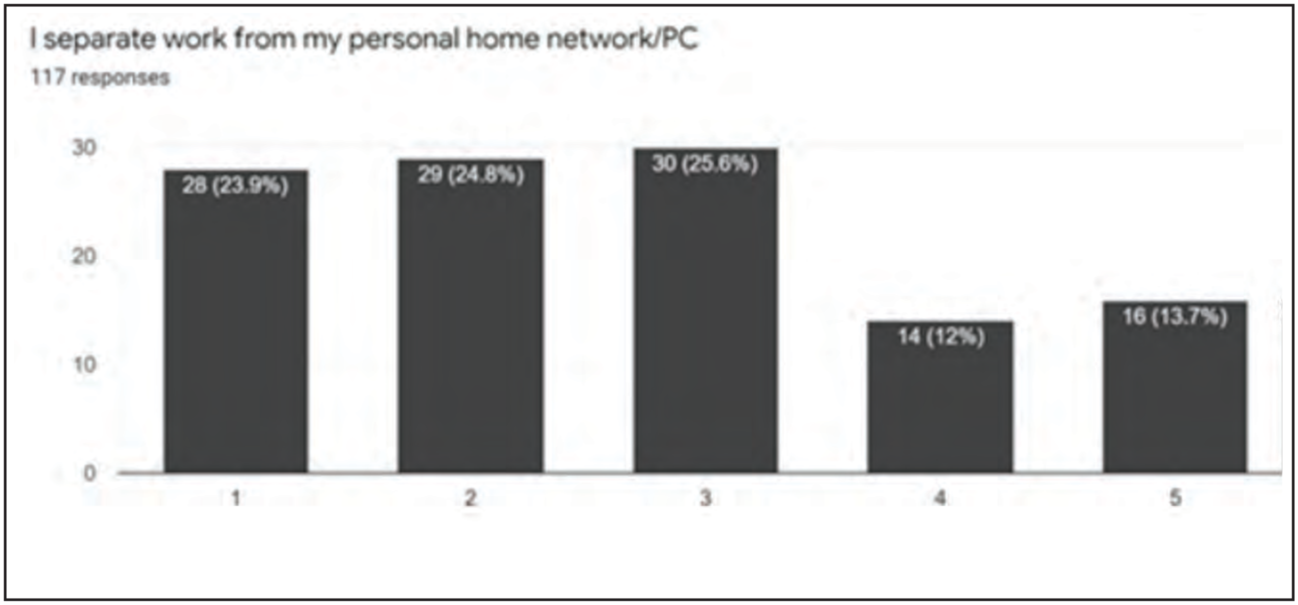


**Fig. 20. Result of Survey Question 20**

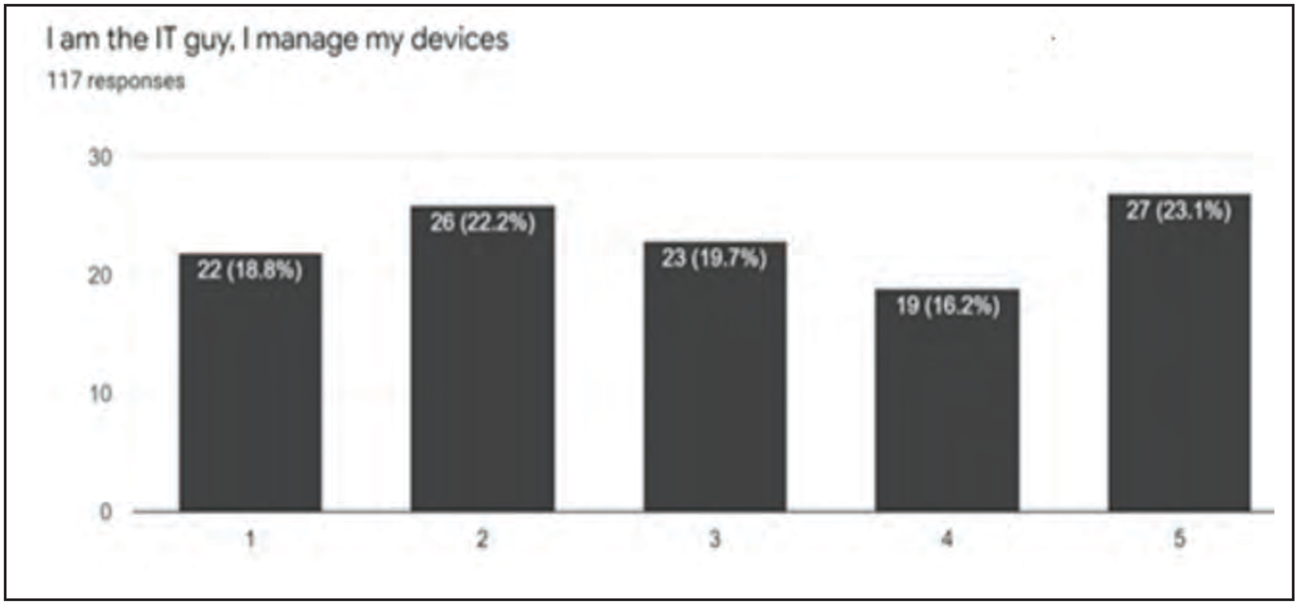


**Fig. 21. Result of Survey Question 21**

computer that was installed with malicious software, that computer could infect everything it connects to. If that computer were to be connected to their employer's servers, it would lead to a server compromise and everything that the employer owns could be infected, resulting in catastrophe for the company.

For the next set of questions, we asked students if they managed their own network or devices or if they had someone else manage it for them. From our responses, it seems more than half of the students have someone they know manage their own devices while the other half or lesser percentage manage it themselves (Fig. 21 and 22). This is another concern as less than half of the students are aware of online security practices when it comes to managing devices. Hence, revisiting the first question of the survey, "Do you have a password set on your smart camera(s)", this means that half the students have no clue why not setting a password is a security risk because they trust someone else to watch their network. Another security risk with having someone managing your

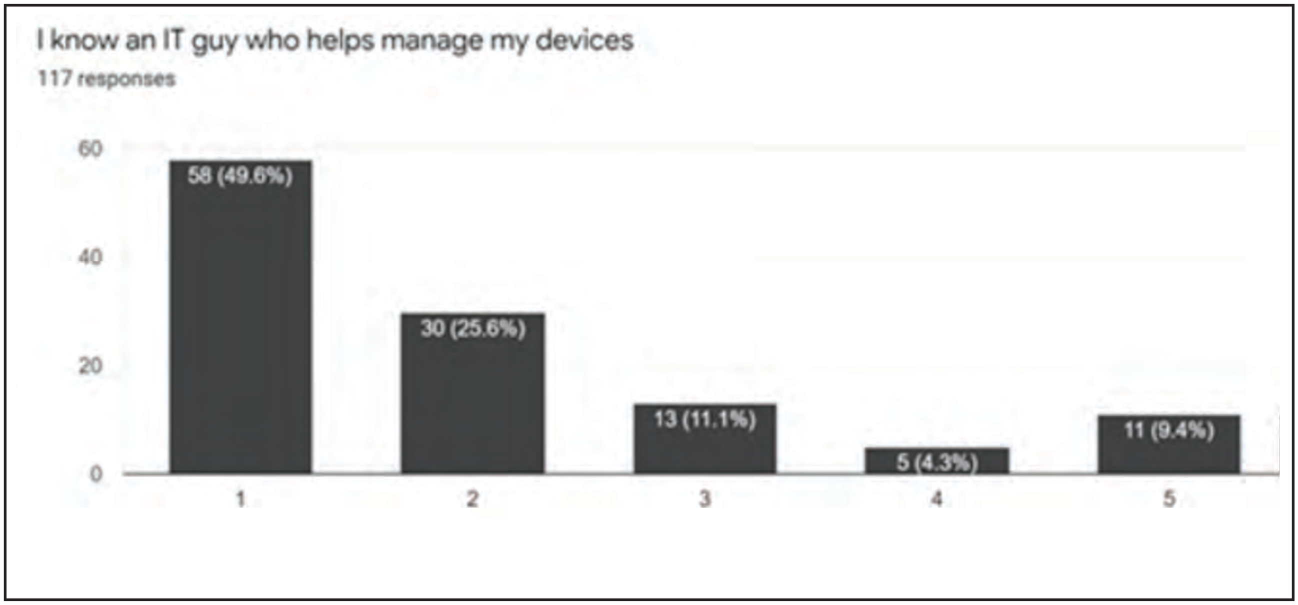


Fig. 22. Result of Survey Question 22

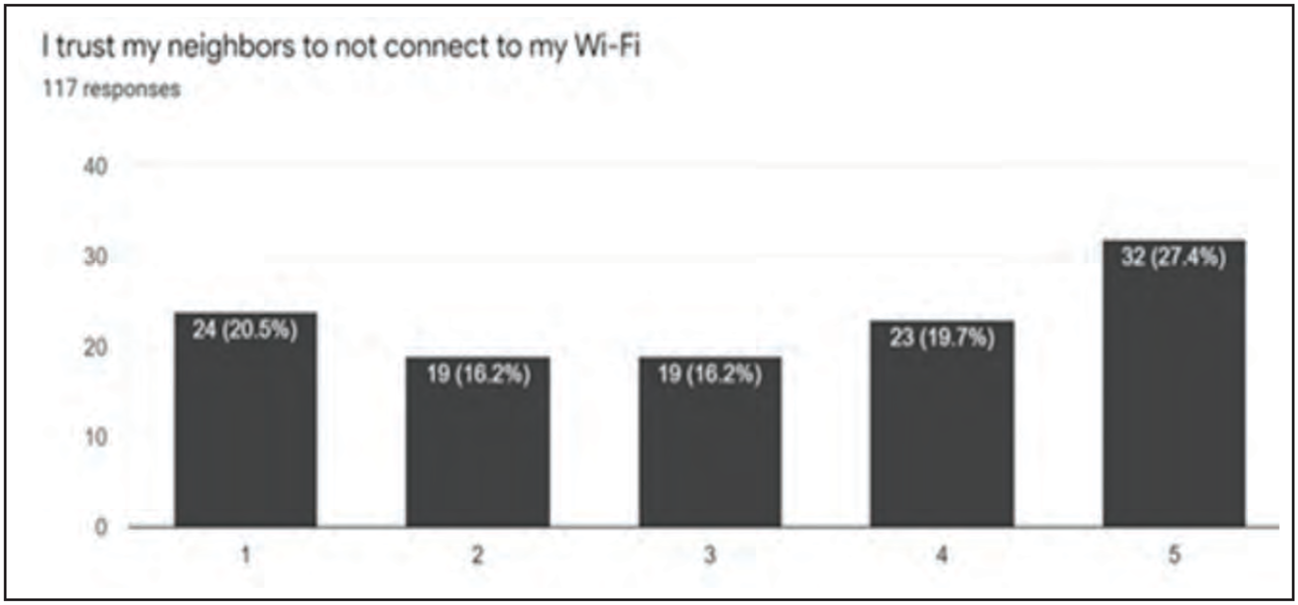


Fig. 23. Result of Survey Question 23

devices is whether that person can be trustworthy. Users should atleast know what their devices do, who and what has access to them.

For the next question, we asked the students if they trust their neighbors to not connect to their Wi-Fi. Depending on the area they live in or how close they are to one another, their answers can vary. Our results show very diverse answers as many of the responses we have are almost even across the board (Fig. 23). This question's real aim is to know whether users have atleast secured their own Wi-Fi from others joining in. As stated earlier, this is a concern because wireless signals can be intercepted easily if someone has a sniffing tool. Another concern would be if a neighbor has an infected computer, he can also jeopardize the home-owner's network as well.

For the next set of questions, we asked users if they were aware of phishing. Phishing is a practice of social engineering where users receive fraudulent claims about their account details. This type of email is almost seen occasionally like spam, yet if the email contains user information, you would think it were authentic. This would sometimes scam users to follow a link to leak their

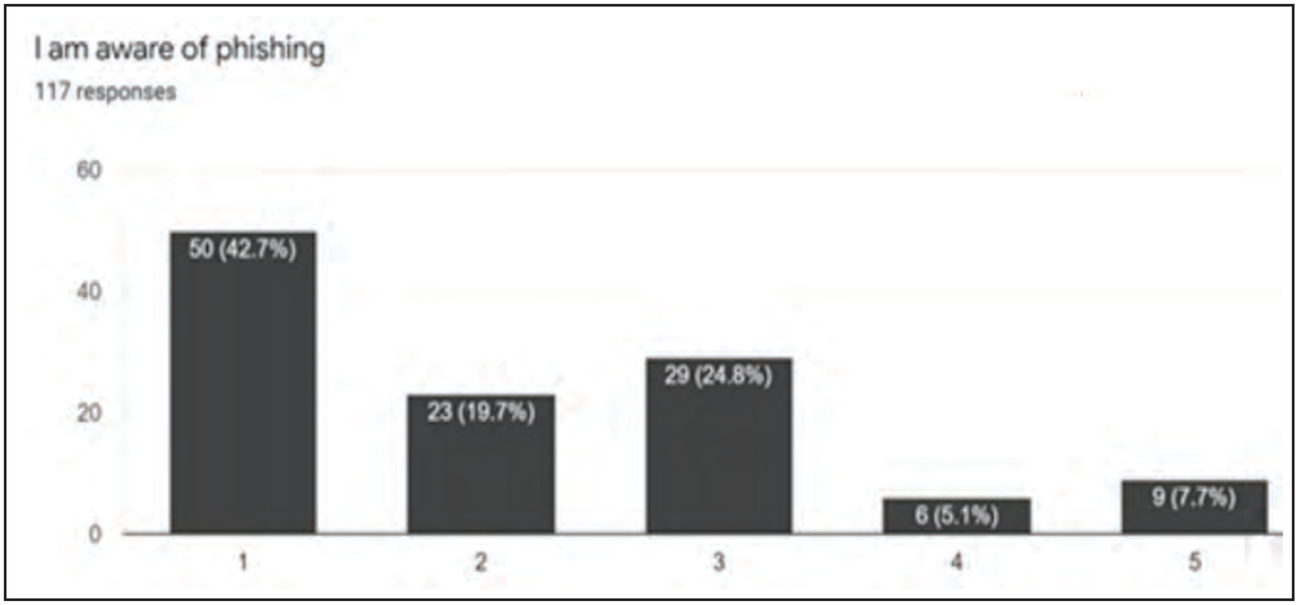


**Fig. 24. Result of Survey Question 24**

credentials to hackers. Surprisingly, most of the students in the survey have answered that they are aware of phishing (Fig. 24). It seems that roughly 30% of the students are unsure what phishing is. As for our last question, we asked the students if they practiced common online security practices. As seen before, nearly 50% of the students answered evenly across the scale which supports most of the other charts we have seen thus far (Fig. 25). Truthfully, one can never assume one has practiced online security practice without proper credentials or certification.

After analyzing all our data and charts (Table I and II), we can assume that more than half of the students who have taken this survey are not aware of proper security protocols or are aware of the risks when owning an outdated smart camera. From what we have seen thus far, the certainty levels are roughly 50:50. Yet, some questions show high concerns, such as the first question of not setting a password on a smart camera. Therefore, we can also assume that nearly 70% of the students are truly unaware of actual security practices. After reviewing the data and charts, we can reach our conclusion.

## V. EXPERIMENTS ON VULNERABILITY EXPLOITATION

To better support our research, we carried out a series of experiments to showcase how simple it is for hackers to exploit an IP camera and gain access to a network. In the experiments, we simulated a regular home network using the following tools: a laptop installed with the latest version of Windows 10 named Host, a NETGEAR Nighthawk router to act both as the default gateway and wireless access point, and an IP camera. During literature review, we learned that most IP cameras sold online were mostly unsecured and easily found. For IP cameras, we tested a Boavision Wireless Surveillance Dome and an AXIS M1034-W Network Camera. Our experiment revealed that the IP camera had poor security function and could possibly be used as a back door by hackers.

The first step in our simulation was to create the simulated home network. We paired the IP camera with Host laptop which was already managed by the router. The three devices were then linked together via Wi-Fi and the router was able to handle the DHCP protocol for the devices since it was the main default gateway. The router utilizes an 802.11n wireless signal and emits at a 2.4 Ghz bandwidth, the same frequency that supports the IP camera.

We tested the following exploitations:

### *A. Connecting to an IP Camera*

Connecting to an IP camera means after knowing the IP address of the camera, sending connection request to

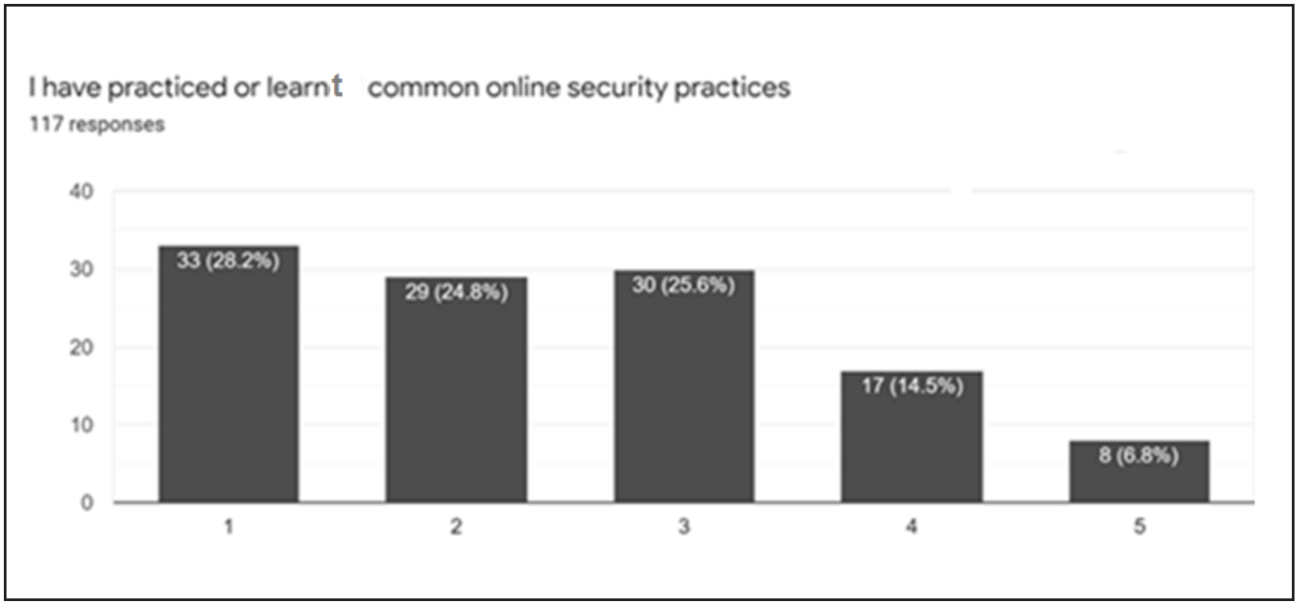
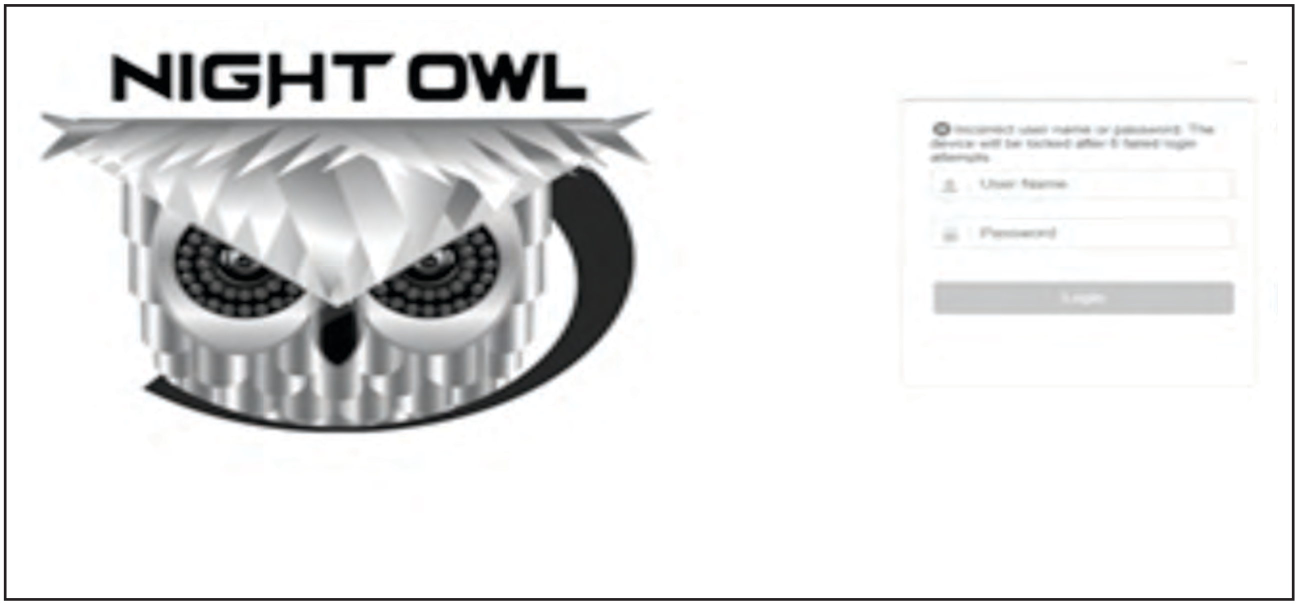


**Fig. 25. Result of Survey Question 25**



Incorrect user name or password. The device will be locked after 5 failed login attempts.

**Fig. 26. A Login Page to Access the Camera**

HTTP/HTTPS service running there and establishing connection. From Shodan or Censys, we can search and find many IP cameras. If we try to connect a detected IP camera, we are presented a login page similar to the one shown in Fig. 26.

To attack a specific IP camera that is not detected by Shodan or Censys, like the one in our case, we need to get into the local network first. A wired Ethernet has so-called perimeter security, and we need physical access to the router or switch or cable to get into. If the camera is in a wireless network, it is much easier to get into the same network.

There are many attacks against wireless routers. The first thing to try is WPS attack. Wi-Fi Protected Setup (WPS) is an optional means of configuring security on wireless networks. It is created to make connecting to Wi-Fi easy. WPS has design and implementation flaws:

⇘

TABLE I.

YES/NO QUESTIONS OF THE SURVEY

| The Questions from the Survey | Yes | No | N/A | Yes Percentage | No Percentage | N/A Percentage |
|---|---|---|---|---|---|---|
| Do you have a password set on your smart camera(s)? | 27 | 74 | 16 | 23% | 63% | 14% |
| Have you set passwords on other network devices or Internet of Things (Router, Smart TV's, Wireless Printers)? | 75 | 31 | 11 | 64% | 26% | 9% |
| Some devices are not updated automatically, do you update them manually? | 62 | 52 | 3 | 53% | 44% | 3% |
| Do you know your Internet Service Provider's (ISP) modem password? | 61 | 46 | 10 | 52% | 39% | 9% |
| Do you know your ISP's email and password? | 32 | 67 | 18 | 27% | 57% | 15% |
| Do you commonly use strong password on your devices and other online accounts (i.e. using combination of numbers, letters, and symbols, e.g. P@$$w0rD)? | 74 | 27 | 16 | 63% | 23% | 14% |
| Do you also have a strong password placed on your home Wi-Fi? | 91 | 21 | 5 | 78% | 18% | 4% |
| What about Multi-Factor Authentication, do you have one enabled (i.e. using a smartphone to receive a textcode in order to access your account)? | 87 | 28 | 2 | 74% | 24% | 2% |
| Do you have a firewall installed in your home? | 28 | 82 | 7 | 24% | 70% | 6% |
| Do you have a VPN service? | 38 | 70 | 9 | 32% | 60% | 8% |
| Do you regularly use the same password for most of your online accounts and devices? | 63 | 51 | 3 | 54% | 44% | 3% |
| Do you store your password on your computer or online services (i.e. Keychain, LastPass, Chrome password manager etc.)? | 53 | 60 | 4 | 45% | 51% | 3% |
| Do you have a lock screen on your computer which requires a password to log in? | 99 | 17 | 1 | 85% | 15% | 1% |
| Are your files or valuable information encrypted on your computer? | 42 | 73 | 2 | 36% | 62% | 2% |
| Do you commonly use the same security questions/ answers for several of your accounts? | 42 | 67 | 8 | 36% | 57% | 7% |

↳ There is no lockout limit for entering PINs.

↳ The PIN is 8-digit numerical, and the last digit is only a checksum.

↳ The wireless router reports the validity of the first and second halves of the PIN separately.

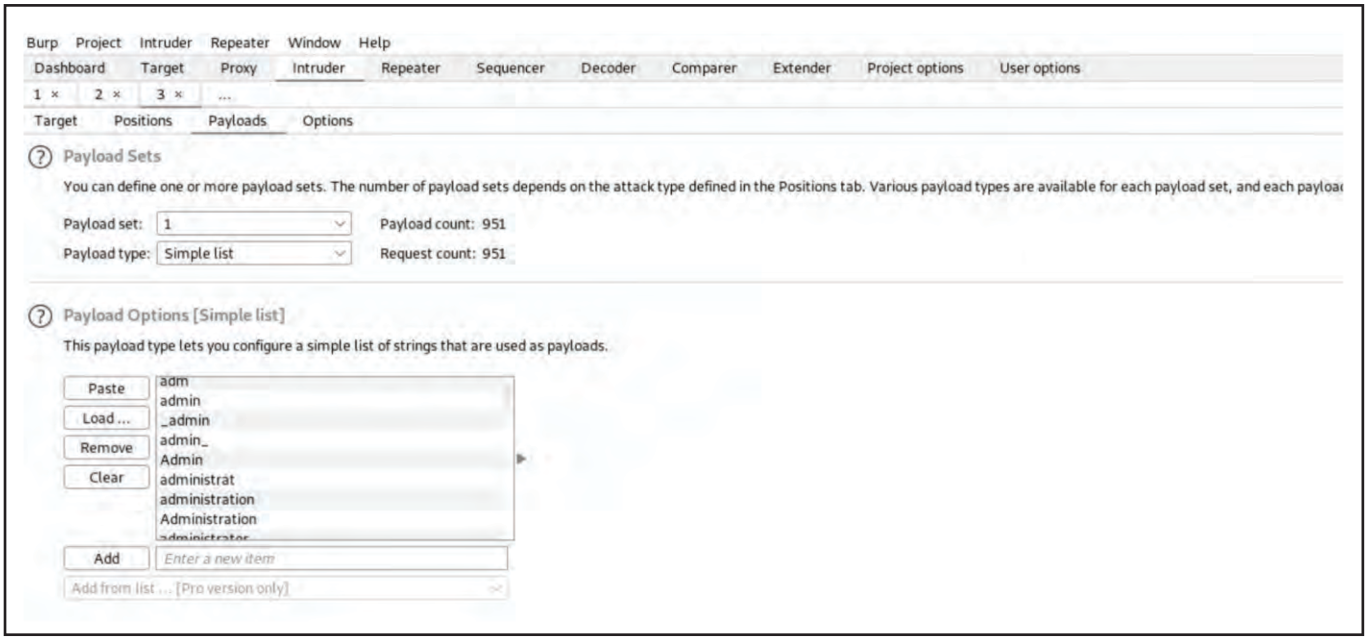
These features lead to the fact that it could take about 4 hours to brute force the WPS PIN.

If WPS is not enabled, we can try to break the encryption password to connect to the wireless router. The encryption method could be either WEP or WPA/WPA2. There have been plenty of works in literature on how to break WEP or WPA/WPA2. We are not elaborating it here. Briefly, we use *Airodump-ng* and *Aircrack-ng* to dump and analyze the traffic to crack the password.

In our experiments, we could break any WEP password in less than 1 hour; we could break weak to medium difficulty WPA/WPA2 passwords in a few hours

## TABLE II.
## LIKERT SCALE QUESTIONS OF THE SURVEY

| The Questions from the Survey | Strongly Agree | Agree | N/A | Disagree | Strongly Disagree | Strongly Agree % | Agree % | N/A % | Disagree % | Strongly Disagree % |
|---|---|---|---|---|---|---|---|---|---|---|
| I know my network is safe | 17 | 30 | 46 | 16 | 8 | 15% | 26% | 39% | 14% | 7% |
| I trust to share some of my privacy through social media like Facebook | 6 | 12 | 28 | 23 | 48 | 5% | 10% | 24% | 20% | 41% |
| I know which name brand smart camera(s) are reliable | 20 | 32 | 34 | 17 | 14 | 17% | 27% | 29% | 15% | 12% |
| I use hard to guess passwords that don't involve my personal life | 37 | 25 | 27 | 11 | 17 | 32% | 21% | 23% | 9% | 15% |
| I replace my devices when something newer or better comes out, about three years minimum | 23 | 19 | 31 | 27 | 17 | 20% | 16% | 26% | 23% | 15% |
| When I hear news of a new exploit, I make sure my devices are updated | 27 | 27 | 32 | 18 | 13 | 23% | 23% | 27% | 15% | 11% |
| I use safeguard on my network (such as firewalls, antivirus or VPN) | 20 | 27 | 33 | 23 | 14 | 17% | 23% | 28% | 20% | 12% |
| I like to purchase subscription based antivirus software (such as Norton, Webroot, Malwarebytes, or Bitdefender) | 10 | 22 | 28 | 26 | 31 | 9% | 19% | 24% | 22% | 26% |
| I use an adblocker when surfing the web (such as ublock, Adblocker plus or AdGuard) | 29 | 25 | 21 | 15 | 27 | 25% | 21% | 18% | 13% | 23% |
| I backup my data with a physical hard drive or thumb drive | 35 | 17 | 27 | 24 | 14 | 30% | 15% | 23% | 21% | 12% |
| I backup my data through a Cloud based system | 33 | 32 | 21 | 15 | 16 | 28% | 27% | 18% | 13% | 14% |
| I do not connect to an unknown Wi-Fi at home or anywhere in that matter | 45 | 24 | 20 | 14 | 14 | 38% | 21% | 17% | 12% | 12% |
| I trust my neighbors to not connect to my Wi-Fi | 24 | 19 | 19 | 23 | 32 | 21% | 16% | 16% | 20% | 27% |
| I separate work from my personal home network/PC | 28 | 29 | 30 | 14 | 16 | 24% | 25% | 26% | 12% | 14% |
| I am aware of phishing | 50 | 23 | 29 | 6 | 9 | 43% | 20% | 25% | 5% | 8% |
| I am the IT guy, I manage my devices | 22 | 26 | 23 | 19 | 27 | 19% | 22% | 20% | 16% | 23% |
| I know an IT guy who helps manage my devices | 58 | 30 | 13 | 5 | 11 | 50% | 26% | 11% | 4% | 9% |
| I have practiced or learned common online security practices | 33 | 29 | 30 | 17 | 8 | 28% | 25% | 26% | 15% | 7% |
| I use public Wi-Fi when it is convenient | 45 | 34 | 12 | 10 | 16 | 38% | 29% | 10% | 9% | 14% |


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × 3 × ...
Target Positions Payloads Options
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ... [Pro version only]

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payloa

Payload set: 1 Payload count: 951

Payload type: Simple list Request count: 951

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
adm
admin
_admin
admin_
Admin
administrat
administration
Administration
administrator
```

Fig. 27. A Screenshot of Using Burp Suite to Break Password

(The time needed depends on password difficulty and dictionary quality).

### *B. Logging Into the Control Page*

Logging into the IP camera means that we pass the username/password authentication on the login page, and get access to the control page and the content provided by the camera.

As for username/password authentication, all cameras have an "admin" username and a default password for it in factory settings. Most users do not change either of them, and only a few users change the password. The first thing to pass the authentication is to search the internet for the default username/password for the specific brand and model of camera.

If there is no search result, or the user has changed default username/password, we can run some brute-force tools to discover username/password. We have tested *medusa*, *hydra* and *Burp Suite* included in Kali Linux. Fig.27 is a screenshot of using *Burp Suite* to break the password of a specified username, where we use a file of password dictionary.

We have also tested another way to break the username/password in Wi-Fi environment. Many outdated IP cameras use HTTP protocol to login in which the traffic is unencrypted. We can capture and decrypt the Wi-Fi traffic (using the Wi-Fi password when we connect to the network if any), and see the username/password. For us to capture the traffic from both the host laptop and IP camera, we had to set the Kali laptop in monitoring mode. Monitoring mode is a function that would allow us to sniff, or pickup, wireless traffic without joining into the host's network,. meaning that whatever is being signaled in the air can be easily intercepted without anyone noticing our presence.

After configuring the wireless card to enter Monitoring mode, we can begin using Wireshark to collect IP packets. IP Packets or packets are structures that carry network data when it is transmitted from device to device; in this case, we are collecting the packets from the three devices. We then used Wireshark's capture command to collect the transmission of the wireless signals. As this was happening, we then used the Host Laptop to log into the IP camera. Doing so would allow the Kali Laptop to "listen" or eavesdrop as the Host Laptop logs into the IP camera. After logging in, the Kali laptop was able to collect the entire transmission.

Within a minute, Wireshark was able to sniff over a thousand packets from the devices. The reason there are so many packets is that the IP camera is known to exchange hundreds of packets per second as it is transmitting a live feed to the laptop. For each frame, the IP camera is sending constant data to the laptop and back,

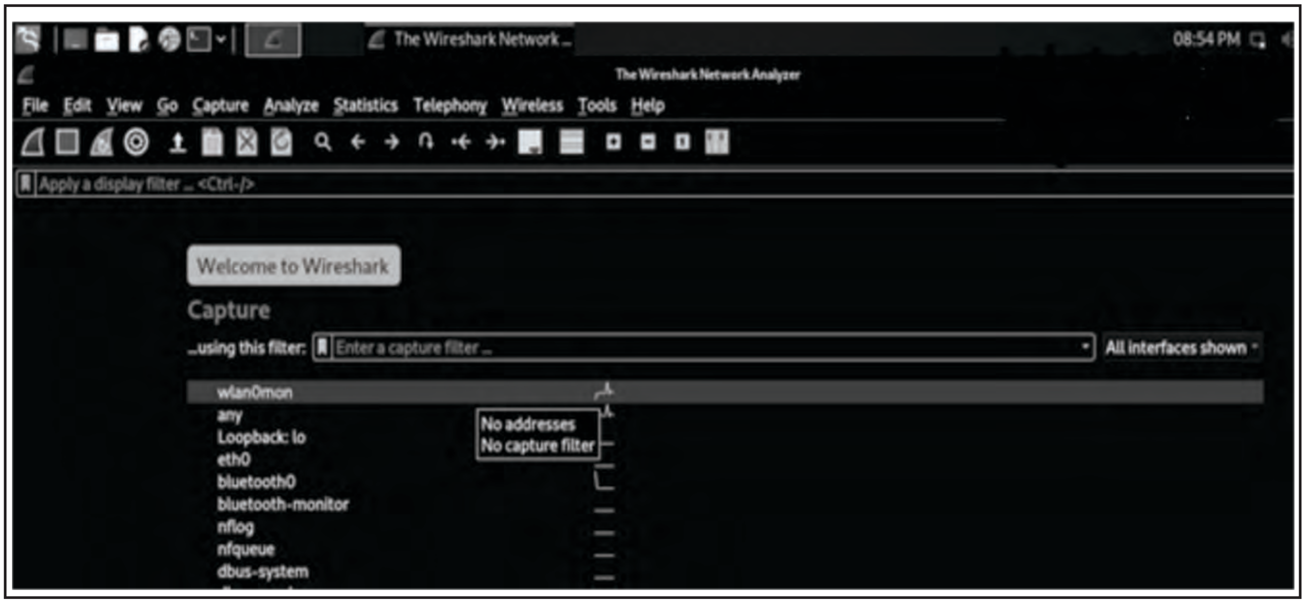

The Wireshark Network ...
08:54 PM
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
wlan0mon
any
Loopback: lo
eth0
bluetooth0
bluetooth-monitor
nflog
nfqueue
dbus-system
No addresses
No capture filter

**Fig. 28. Capturing IP Camera Traffic With Wireshark**

creating a large number of packets. Wireshark was then able to list the packets accordingly within milliseconds. The results show that the IP camera mostly uses TCP and HTTP packets. As we learned from our literature review, whenever a packet is in HTTP, the packets are easily readable because they are not encrypted. Therefore, the IP camera is utilizing HTTP port. IP cameras that utilize HTTP traffic are known to be exploitable, and this IP camera was sold with this feature.

Next, with all of the packets we captured, we used Wireshark's filter feature to categorize the packets. This feature allows us to search for any specific types of packets or streams that we want to search for. By following these streams, we can see what the camera is sending from order, we then can view certain information (Fig. 28). In the first captured TCP packet, we were able to follow it and view the IP camera's full description. The packet listed the camera's make, model, ID, IP address, firmware, program, and associated devices. Next, we followed the HTTP packet associated with the IP camera and soon enough, we found a packet which listed the IP camera's authentication credential in plain text (Fig. 29). With this credential, we can now log into the smart camera.

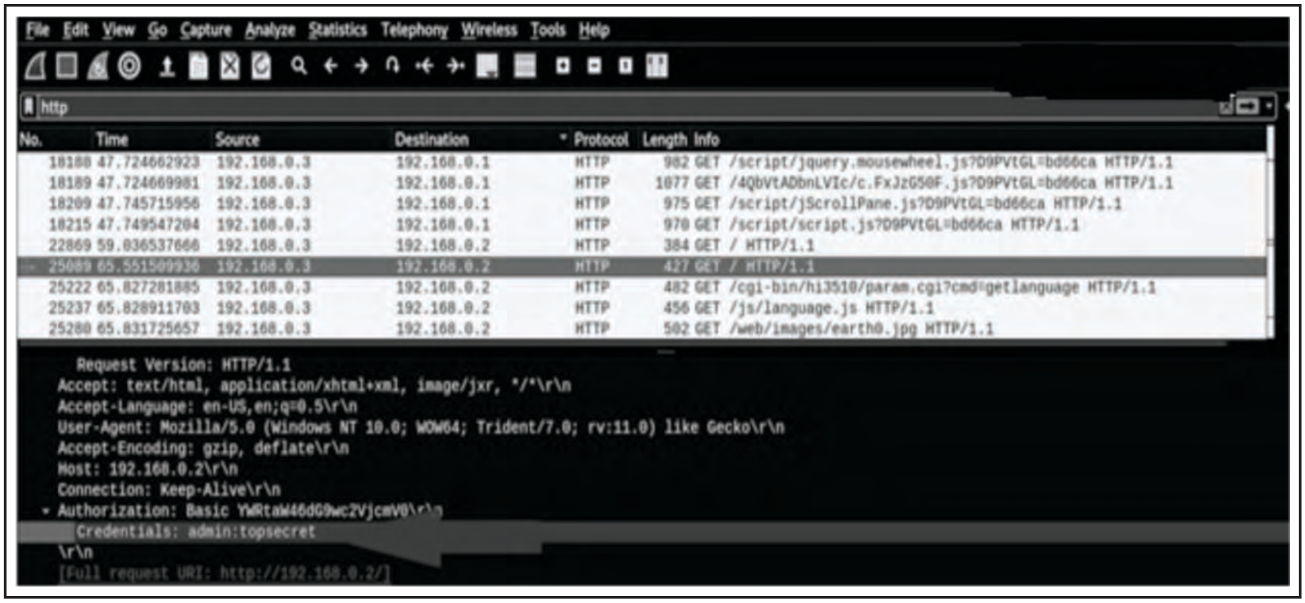
The final step in our experiment is to log into the IP camera and take control of it. Thanks to Wireshark, we were able to have full access to the smart camera (Fig. 30). Not only were we able to view the live feed, but we could also change the camera’s settings, take control of the smart camera's movement, or even input our own voice into the audio channel. With these functions, hackers could exploit this smart camera for their own malicious means such as blackmail, privacy intrusion or alter the IP camera for DDoS attacks just as our literature review has proven.

### C. Getting Root Privilege

Even if the host or user can change his password, once a hacker is able to install a malicious firmware into the smart camera, the hacker will always have a back door to the smart camera. “The code is not encrypted or digitally signed leaving open a backdoor for malware to be uploaded to the camera” [4]. The highest level of attack on an IP camera is to replace its firmware and leave a backdoor. This requires root privilege to the device. We have tested reverse engineering techniques for this purpose.

We first searched from Internet the firmware of our IP cameras. It is available to download from the manufacturer's website, and many other websites. We then used the tools called *binwalk* and *jeffereson* included in Kali to analyze the firmware. Fig. 31 shows the files extracted from the firmware.

We can see the */etc/passwd* file and its content. The line “*root:AiADGkJIfIlXk:0:0:root:/root:/bin/sh*” indicates that the root password is encrypted using *crypt(3),* and *“AiADGkJIfIlXk”* is the ciphertext. A little


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time            Source        Destination   Protocol Length Info
18188 47.724662923    192.168.0.3   192.168.0.1   HTTP      982 GET /script/jquery.mousewheel.js?D9PVtGL=bd66ca HTTP/1.1
18189 47.724669981    192.168.0.3   192.168.0.1   HTTP     1077 GET /4QbVtADbnLVIc/c.FxJzG50F.js?D9PVtGL=bd66ca HTTP/1.1
18209 47.745715956    192.168.0.3   192.168.0.1   HTTP      975 GET /script/jScrollPane.js?D9PVtGL=bd66ca HTTP/1.1
18215 47.749547204    192.168.0.3   192.168.0.1   HTTP      970 GET /script/script.js?D9PVtGL=bd66ca HTTP/1.1
22869 59.036537666    192.168.0.3   192.168.0.2   HTTP      384 GET / HTTP/1.1
25089 65.551509936    192.168.0.3   192.168.0.2   HTTP      427 GET / HTTP/1.1
25222 65.827281885    192.168.0.3   192.168.0.2   HTTP      482 GET /cgi-bin/hi3510/param.cgi?cmd=getlanguage HTTP/1.1
25237 65.828911703    192.168.0.3   192.168.0.2   HTTP      456 GET /js/language.js HTTP/1.1
25280 65.831725657    192.168.0.3   192.168.0.2   HTTP      502 GET /web/images/earth0.jpg HTTP/1.1

    Request Version: HTTP/1.1
  Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: 192.168.0.2\r\n
  Connection: Keep-Alive\r\n
▾ Authorization: Basic YWRtaW46dG9wc2VjcmV0\r\n
    Credentials: admin:topsecret
  \r\n
  [Full request URI: http://192.168.0.2/]
```

Fig. 29. IP Camera's Authentication Credential Captured

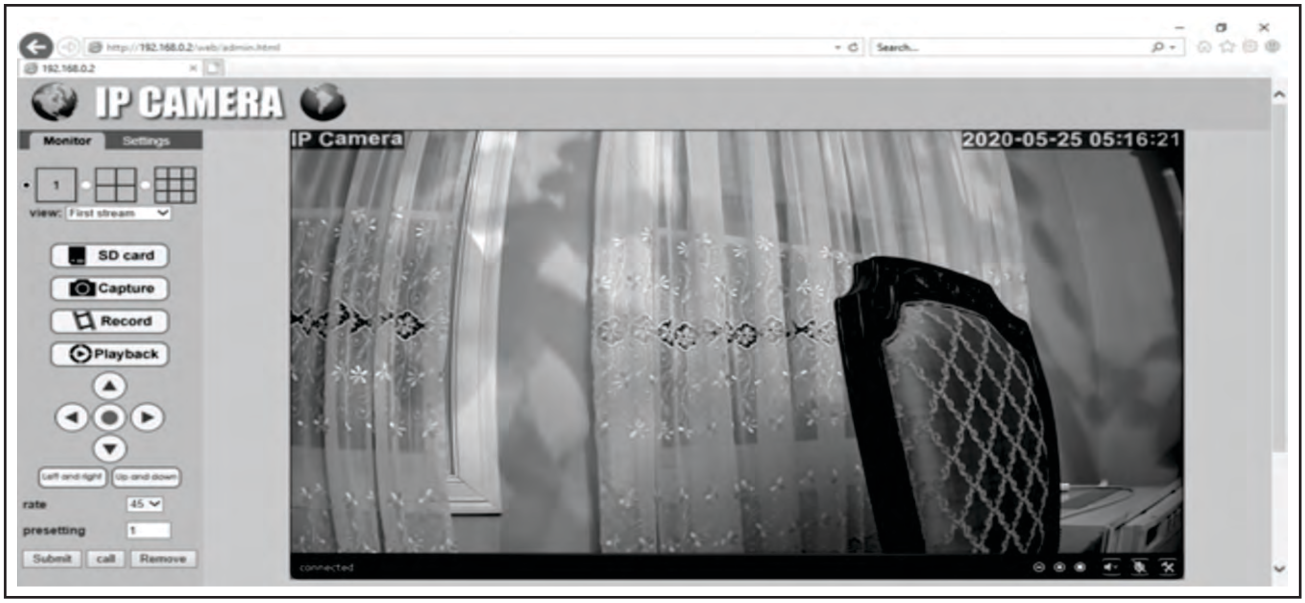
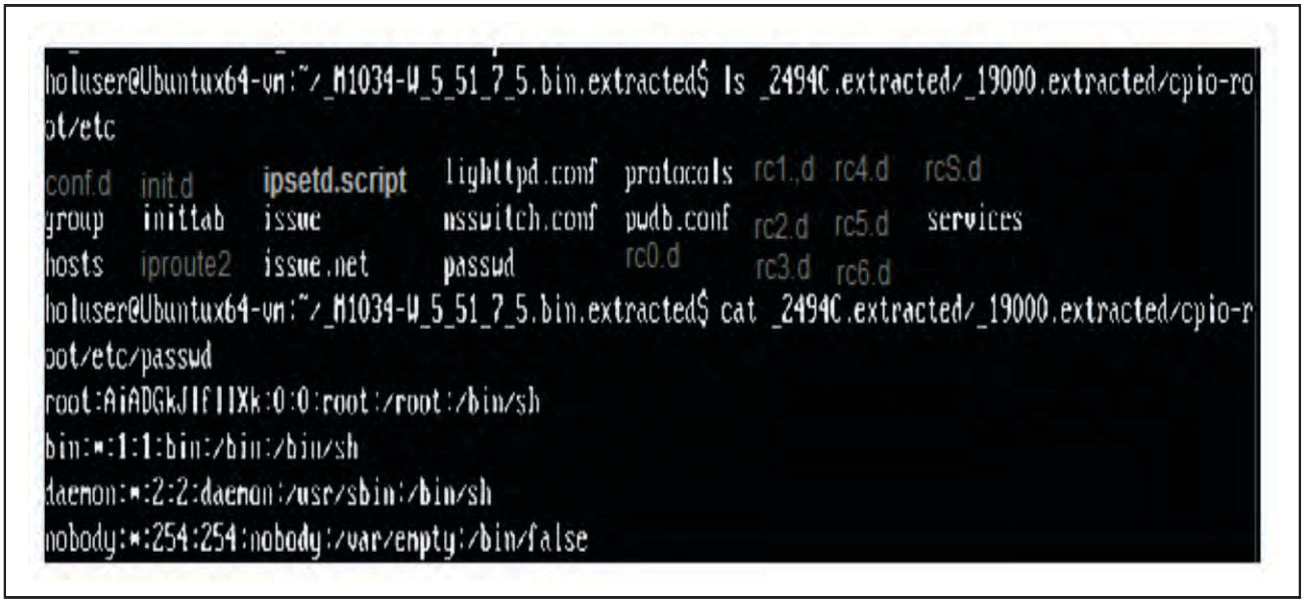


Fig. 30. We Get Access to the IP camera

research shows us when using crypt(3), the text is set to null and the password is the key. A salt used in the encryption is a two-character string chosen from the set *[a-zA-Z0-9./]* (64 characters) which has 4096 (64*64) possibilities [14]. We can run a brute force attack with a password dictionary, testing each password with 4096 possible salt values. This is feasible cost-wise and time-wise but in most cases, there is a better solution --- the ciphertexts for many popular passwords are already available online. In our case, we searched the string *"AiADGkJIfIlXk"* online and found the answer for the plaintext ("*pass*") immediately from the website: "*http://firmware.re/keys-n-pass/"*.

With root privilege, we could locally connect or *ssh* into the camera and change configurations and insert malware into it. That will be our future work to do.



```
holuser@Ubuntux64-vm:~/_M1034-W_5_51_7_5.bin.extracted$ ls _2494C.extracted/_19000.extracted/cpio-ro
ot/etc
conf.d   init.d    ipsetd.script   lighttpd.conf   protocols   rc1.d   rc4.d   rcS.d
group    inittab   issue           nsswitch.conf   pwdb.conf   rc2.d   rc5.d   services
hosts    iproute2  issue.net       passwd          rc0.d       rc3.d   rc6.d
holuser@Ubuntux64-vm:~/_M1034-W_5_51_7_5.bin.extracted$ cat _2494C.extracted/_19000.extracted/cpio-r
oot/etc/passwd
root:AiADGkJIfIIXk:0:0:root:/root:/bin/sh
bin:*:1:1:bin:/bin:/bin/sh
daemon:*:2:2:daemon:/usr/sbin:/bin/sh
nobody:*:254:254:nobody:/var/empty:/bin/false
```

**Fig. 31. Encrypted Password of Root is shown**

## VI. DISCUSSION

After completing our research and analyzing our survey responses, we can accept our initial hypothesis. Most consumers are unaware of potential security risks of carrying outdated/unsecured IP cameras and are unknowingly putting their networks at risk. In our literature review, we found that the most common network intrusions can be caused not by only smart cameras, but by several other factors. Managing smart devices is one large factor of having a stronger security and owning an IP camera holds a lot of responsibilities. If consumers do not secure their devices, it would become an intrusion point for hackers. One of the most leading causes of network intrusions is caused by these unsecured IP cameras.

After evaluating all the responses, we determined that more than half the students were not aware of common security practices and protocols, we can assume that most of the students were not familiar with the risks. To better combat this or mitigate security risks, we believe that the students and consumers alike should adopt a proper security policy. This is why consumers should learn about the Confidentiality, Integrity and Availability model (CIA). The CIA security model is a policy that has been adopted by many well-known organizations and is a great foundation when it comes to building strong security.

Revisiting our first objective, identifying and determining which IP cameras can become exploitable by hackers and how they become intrusive. We have determined that this is caused by several factors and not just by certain IP cameras. In fact, any smart/IP cameras can become exploitable over time due to either reverse engineering or newly found vulnerabilities. If anything, our research shows that the most reliable cameras are those with newer security models and protocols. Over time, IP cameras will become obsolete as technologies continue to evolve.

Continuing from earlier, another factor for a camera to become exploitable is if it is not placed with proper security measures. Our literature review has explained that many poor-quality IP cameras are built with weak or no security functions. One example would be having a camera with "HTTP" protocols enabled. In our experiment, we have shown that such protocols are prone to monitoring and can be easily intercepted, thus posing a risk for the network. Improper security protocols or unencrypted communication is what can lead to a compromised network.

Another factor is lack of support from the manufacturer. When a product is made, the manufacturers are responsible for supplying their products with newer firmware or software to improve their product or combat newly found vulnerabilities. As explained earlier, what creates good reputation is when a product continues to improve even after selling it in the market. If a product has been sold with weak security features and receives no support, it is most likely that the product's lifecycle was short or temporary. If that is the case, the camera may have been sold to you as-is, it would not be covered in any warranty and is dangerous to own.

Our second objective was to find ways to establish what measures or standards should be taken to secure a homeowner's smart camera and network. Going back earlier, we have already found the solution and that would be the CIA model. The CIA model is based on the three principles: confidentiality, integrity, and availability. If homeowners were to follow these principles, they could be able to set a stronger network security or harden their network.

Reviewing CIA, confidentiality means only one person would be authorized to view or modify data. To increase confidentially, there has to be a method to increase authentication, one other way to authenticate yourself other than knowing a password. One other method could be through the use of a smart phone, such as receiving a text to enter an email address, a standard of two-factor authentication for students attending Central Connecticut State University. Integrity is the data that has not been altered or touched by other users. One example of integrity would be having a bank account and double checking all withdrawals unless you found a discrepancy. For data, another idea could be having data as read-only, making it virtually impossible for data to be altered or modified, keeping its integrity. Availability is when a user can use or access data without trouble. One example would be accessing your favorite site or server without trouble. When a server or site receives a DDoS attack, that availability has failed. By implementing the CIA models, we can assure that one's privacy can be maintained.

Other than adopting the CIA model, another method to reduce exploitable devices on the market is to enforce policies for manufacturers. In one of the earlier literature reviews, the author of this research suggests that the federal government should enforce new policies and place better security protocols when manufacturers sell an IoT. This is a sound statement, as the number of exploitable and unsecured devices is still rising to this day. A prime example would be our demonstration where we purchased an exploitable smart camera from Amazon only a few months ago before this paper was written. If the government were to enforce such policies, they would be able to reduce the number of unsecured IoTs on the market.

One idea of enforcing a security policy can be that manufacturers must set different passcodes for all their products, not just a product line, but every single one. Usually, when a manufacturer produces a certain product line, many of those devices do share the same credentials by default. If every device sold on the market were to have complex passwords or complex default credentials, it would better secure the device, making it impossible for hackers to guess or search online for passwords.

Our third objective was to identify the most secure and weakest smart camera brand; this has become impossible to answer. The reason why is that there are far too many exploitable or unsecured IP cameras on the market. As explained earlier, many IoT's and IP cameras are sold cheaply in the market and many of the manufactures could have different aliases or brand names. Some manufacturers change their name brands to either hide their history or try to sell unsecured IoTs for quick monetary gain. As for the most secured smart cameras, these can be easily found if you recognize name brands such as Hikvision, Axis or Dahua. Manufacturers with reputable names are the most secured because of their reputation.

In our earlier research, we found that most of the exploited cameras that are sold are produced by third party vendors or non-reputable manufacturers. We purchased a brand-new smart camera from Amazon. The default credentials for this product were both "admin" and it was using HTTP protocol, an unsecured protocol. Going back to enforcing policies on manufacturers, if governments or law makers were to impose stricter rules of selling IoTs, we may be able to prevent unsecured devices being sold. Furthermore, if they were enforcing laws, a federal agency should test a manufacturer's device before it is sold in the market. Much like how the FDA approves of certain drugs before selling them in the market, the government should create an agency to monitor such products.

As for our last objective "Identify the average lifespan of a smart camera and determine how long manufacturers support their products," we have determined that the average life span of IP cameras can last for ten years, but this does not include support. Today, most digital IP cameras can last a very long time depending on the model and function. However, keeping such products for a long time is not a sound idea. In our survey, we asked the students about replacing their devices and most students were not willing to replace their devices after three years. Generally, IP cameras are best used for atleast five years before they are replaced with better ones because they continue to improve and become more secure.

It is a fact that every year technology advances and newer and better products are produced by well-known manufacturers. At that time, technologies such as Wi-Fi securities can also change. Currently, we employ WPA and WPA2 protocols to secure wireless devices from intruders. Before WPA, there was WEP, a wireless protocol which today is now obsolete and hackable, which means that cameras that are only pairable with WEP are vulnerable. Even though the software of a device can change, its hardware cannot, which is why it is considered common practice to replace devices every five years.

## VII. CONCLUSION

To conclude, we have determined that unsecured smart cameras are found almost every day and their use must be minimized. Our research has shown and proven that many users are uneducated about the standard security protocols, and this fact can lead to security risks and various attacks. It is also important that users and homeowners manage their own devices from possible intrusions. After all, we live in the age of data and information that can identify oneself must be protected. If nothing is done, the number of unsecured IoTs will continue to increase, when in fact we should start focusing on decreasing this number.

## AUTHORS' CONTRIBUTION

Adam Motowidlo, Timothy Adatsi, and Alvin Jackson were a group in their M.Sc. capstone project. They did the literature review, survey design and result collection, network & IP camera setup and experiment. Shushan Zhao was the advisor of the project, conceived the idea, and finally wrote the manuscript based on their project report.

## CONFLICT OF INTEREST

The authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest, or non-financial interest in the subject matter, or materials discussed in the manuscript.

## FUNDING ACKNOWLEDEGEMENT

The authors did not receive any financial support for the research, authorship, and/or for the publication of this article.

## REFERENCES

[1] Tiagosantos, "How healthy is the internet?", 2018. https://internethealthreport.org/2018/introduction/how-healthy-is-the-internet/ (accessed December, 2021).

[2] P. A. Abdalla and C. Varol, "Testing IoT Security: The Case Study of an IP Camera", in *8th Int. Symp. Digit. Forensics Secur. (ISDFS),* 2020, pp. 1–5, doi: 10.1109/ISDFS49300.2020.9116392

[3] A. Tekeoglu and A. S. Tosun, "Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam," in *24th Int. Conf. Comput. Communication Netw. (ICCCN),* 2015, pp. 1–6, doi: 10.1109/ICCCN.2015.7288421

[4] B. Cusack and Z. Tian, "Evaluating IP surveillance camera vulnerabilities," in Valli, C. (Ed.). (2017), *The Proc. 15th Australian Inf. Security Manage. Conf.*, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia (pp.25-32).

[5] J. Bugeja, D. Jönsson and A. Jacobsson, "An investigation of vulnerabilities in smart connected cameras," in *2018 IEEE Int. Conf. Pervasive Comput. and Commun. Workshops (PerCom Workshops),* 2018, pp. 537–542, doi: 10.1109/PERCOMW.2018.8480184

[6] N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The Security of IP-Based Video Surveillance Syst.," *J. \Sensors,* vol. 20, no. 17, 4806, 2020, doi: 10.3390/s20174806

[7] G. Kim and J. Han, "Security model for video surveillance system," in 2012 *Int. Conf. ICT Convergence (ICTC),* 2012, pp. 100–104, doi: 10.1109/ICTC.2012.6386789

[8] A. Costin, "Security of CCTV and video surveillance syst.: Threats, vulnerabilities, attacks, and mitigations," in *TrustED '16: Proc. of the 6th Int. Workshop Trustworthy Embedded Devices,* October 2016, pp.

45–54, doi: 10.1145/2995289.2995290

[9] B. Li, Y. Zhu, Q. Liu, Z. Zhou, and L. Guo, "Hunting for invisible SmartCam: Characterizing and detecting smart camera based on netflow analysis," in *IEEE Int. Conf. Commun. (ICC),* 2019, pp. 1–7, doi: 10.1109/ICC.2019.8761517

[10] J. Liranzo and T. Hayajneh, "Security and privacy issues affecting cloud-based IP camera," in *2017 IEEE 8th Annu. Ubiquitous Comput., Electronics Mobile Commun. Conf. (UEMCON),* 2017, pp. 458–465, doi: 10.1109/UEMCON.2017.8249043

[11] C. J. Koo and J. Y. Kim, "Enforcing high-level security policies for Internet of Things", *J. Supercomputing,* 2018, 74, pp. 4497–4505, doi: 10.1007/s11227-017-2201-9

[12] G. Lee, "What roles should the government play in fostering the advancement of the Internet of Things?," *Telecommun. Policy,* vol. 43, no. 5, pp. 434–444, 2019, doi: 10.1016/j.telpol.2018.12.002

[13] M. Berger, "Man really did hack Trump's Twitter account by guessing password, 'maga2020!,' Dutch prosecutors say," *The Washington Post,* 2020. https://www.washingtonpost.com/world/2020/12/17/dutch-trump-twitter-password-hack/ (accessed December 2021)

[14] B. Schneier, "Applied cryptography: Protocols, algorithms, and source code in C 2nd Ed," Wiley, 1996.

## About the Authors

**Adam Motowidlo** is currently a Masters student at Department of Computer Electronics & Graphics Technology at Central Connecticut State University. He is supposed to receive his M.Sc. degree in 2022 Summer.

**Timothy Adatsi** is currently a Masters student at Department of Computer Electronics & Graphics Technology at Central Connecticut State University. He is supposed to receive his M.Sc. degree in 2022 Summer.

**Alvin Jackson** is currently a Masters student at Department of Computer Electronics & Graphics Technology at Central Connecticut State University. He is supposed to receive his M.Sc. degree in 2022 Summer.

**Dr. Shushan Zhao** is Assistant Professor with Department of Computer Electronics & Graphics Technology at Central Connecticut State University. He received his Ph.D. degree in Computer Science from University of Windsor, Canada, in 2012.