IoT Security: Penetration Testing of White-Label Cloud-Based IoT Camera Compromising Personal Data Privacy

Marlon Intal Tayag, Francisco Napalit and Arcely Napalit

School of Computing Holy Angel University, Angeles, Philippines

ABSTRACT

The Internet is driving force on how we communicate with one another, from posting messages and images to Facebook or "tweeting" your activities from your vacation. Today it is being used everywhere, now imagine a device that connects to the internet sends out data based on its sensors, this is the Internet-of-Things, a connection of objects with a plethora of sensors. Smart devices as they are commonly called, are invading our homes. With the proliferation of cheap Cloud-based IoT Camera use as a surveillance system to monitor our homes and loved ones right from the palm of our hand using our smartphones. These cameras are mostly white-label product, a process in which the product comes from a single manufacturer and bought by a different company where they are re-branded and sold with their own product name, a method commonly practice in the retail and manufacturing industry. Each Cloud-based IoT cameras sold are not properly tested for security. The problem arises when a hacker, hacks into the Cloud-based IoT Camera sees everything we do, without us knowing about it. Invading our personal digital privacy. This study focuses on the vulnerabilities found on White-label Cloud-based IoT Camera on the market specifically on a Chinese brand sold by Shenzhen Gwelltimes Technology. How this IoT device can be compromised and how to protect our selves from such cyber-attacks.

KEYWORDS

Network Protocols, Wireless Network, Mobile Network, Virus, Worms &Trojon, Internet of Things, Hacker, Smart Camera

1. INTRODUCTION

Privacy is the right to relationship and personal matters secret; it is the right to be alone [1]. The Philippines is a country that values personal privacy. With the advent of the Internet personal privacy is being invaded.

To protect every individual of their right to privacy, the government passed the Data Privacy Act of 2012. As stated on the said law "to protect the fundamental human right of privacy, of communication while ensuring the free flow of information to promote innovation and growth" [2]. We feel safe; we used everything the Internet has to offer, email for communication, social media sites such as Facebook. We post everything on Facebook from what eat and every accomplishment we have.

As we connect to the digital world, we are giving up part of our personal privacy without even knowing it. The Internet, as a whole, has affected everyone's lives and sometimes the Internet can be a dangerous place.

DOI: 10.5121/ijcsit.2020.12503

Moreover, as the Internet becomes a part of our life, we are connected to it constantly. Today everything is being connected, and security is now a concern. British visionary Kevin Ashton coined the term Internet of Things in 1999. It envisions the connections of objects with sensors. Currently, there are many definitions of the Internet of Things or IoT; its definition changes as technology evolved. One such define it as the Internet of Things (IoT) is a connection of different devices that uses the Internet as the medium for communication. Each device has sensors to analyze their environment and send those data to the Internet on a cloud-based server for further analysis.

The technology for the Internet of Things is rapidly evolving, by 2016 interconnected things will reach 6.4 billion and it is estimated that it will grow 30 times reaching 20.8 billion by the year 2020 [3].

Application of the Internet of Things is far and wide; there are now smart devices being used everywhere, from a smart thermostat, smartwatch, smart TV all connected to the Internet. As we grow accustomed to these devices we are letting our guards down, cyber-attacks on these devices are becoming common.

We, Filipinos love technology, we always are an early adopter. As the speed of the internet in the Philippines is becomin4g faster from 5 Mbps to 25 Mbps. The internet is now a medium used to protect our home. People are now buying Cloud-based IoT camera connected to the internet used to monitor our home. Using our smartphone, we can connect to this smart camera and see our house, view our loved ones. The risk of a cyber attacker who can hack the said camera and control it without even knowing it is unfathomable.

The concept and implementation of the Internet of Things arose in the mid-’80s and became more popular in the late 1990s. Any device connected on the internet, which integrates sensor or “smart function” can be classified as an IoT device. Smart devices are rapidly being integrated into all aspect of security monitoring. One such device is a Cloud-based IoT Camera.

Cloud-based IoT Camera or “Smart IoT Camera” are basically surveillance camera connected and accessible from the Internet thru web application or mobile application specifically designed for the said IoT device. Videos from the device can be viewed or stream to a mobile device application.

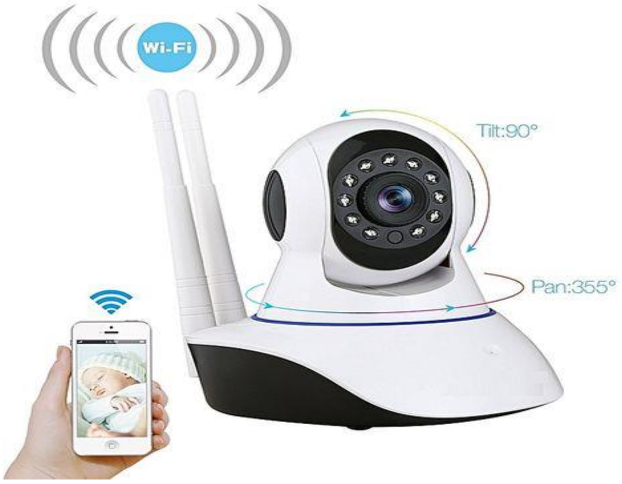


Figure 1. White Label Cloud-based Camera

In today’s market, this type of Cloud-based IoT Camera’s are becoming cheap, and anyone can buy one online Fig. 1 shows an example of a White-label Cloud-based IoT Camera. With a smart camera, sensitive data that reveals the habits of an individual can be captured [4]. Security concern thus arises when hackers compromise such an IoT device.

Most of the Cloud-based IoT Cameras on the market are White-label products; White-label items are created by a supplier to be re-branded, resold to a finished product to clients. With White-labeling, suppliers are provided access to an extensive distribution network through their reseller partners, and resellers will expand their product and repair line,only not having to manufacture their product from scratch. The key to white-label is obscurity, as shoppers obtain the product without aware that it had been originally created by a white-label supplier [5].

According to Gainor (2014, June 3) building, a customized solution from scratch is a setup from failure; this is where white-label products come in. They provide quick and easy branding, saves time and money. When time is of the essence. White-labelling offers the best answer to pre-made items for distribution [6].

With while-label products, the company’s selling the product can minimize its cost because it requires few resources. The product is already pre-made by another company, the next step is to rebrand it [8]. White-labelling is an accepted practice in the retail and manufacturing industry, especially on Chinese products.

As shown in Fig. 2 a White-label is a process in which a product or a service is rebranded under another company’s brand [7].

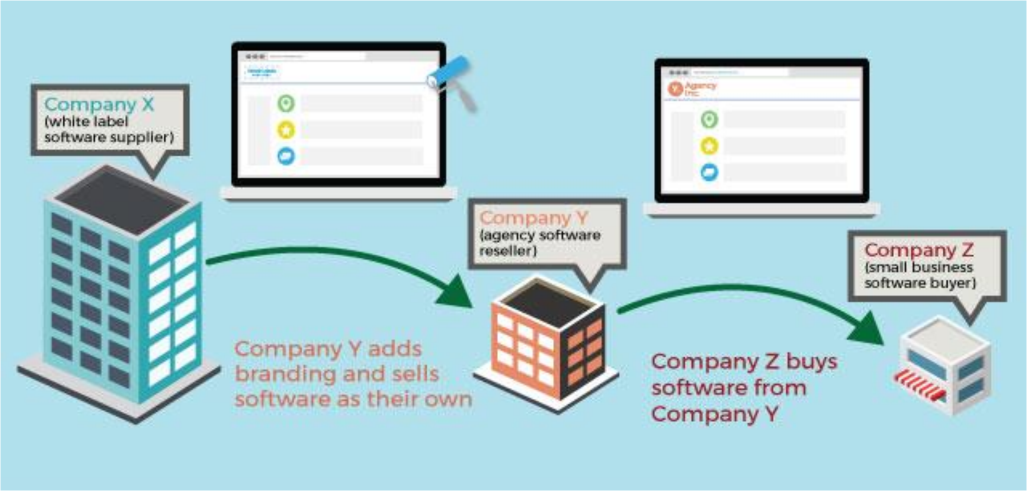

Company X (white label software supplier)
Company Y (agency software reseller)
Company Z (small business software buyer)
Company Y adds branding and sells software as their own
Company Z buys software from Company Y

Figure 2. White-label market process

This study focusses on the deployment of White-label Cloud-based IoT cameras at home and their vulnerability of being hacked in which personal data privacy is affected. A demonstration of an actual hack on IoT camera will be shown along with the different ways a person can protect himself from such an attack.

Objective of the Study

The main objective of the study is to identify vulnerabilities on White-label IoT Cloud-based Camera.

This study aims to achieve the following objectives:

a. Identify the caused of the vulnerability
b. The effect on personal data privacy of the user as such devices are compromised
c. Mitigate and find a solution to the vulnerabilities

Scope of the Study

The study will focus on the testing of White-label IoT Cloud-based camera that is currently on the market; specifically, a camera that is manufactured by a Chinese company called Shenzhen Gwelltimes Technology. The test will involve scanning and comprising the IoT device. Upon gaining full access to the IoT device, as proof, a screenshot of the video stream will be saved. Plan mitigation will be implemented to harden the security of the device, and the user of the IoT device will be informed of the process of how the IoT device was compromised, along with the methods on how to protect from such attacks

2. Literature Review

As ubiquitous computing is becoming mainstream, the connected device is now part of our daily lives, cloud-based security devices are installed on homes to act as monitoring and protection. The problem arises when the question of security is implemented on these different types of devices. Engin Leloglu [8] stated in their paper, IoT devices are vulnerable to other kinds of network attacks such as sniffing and injections, concluding the need for strong encryption to protect data.

On their paper, Yogeesh Seralathan [9] demonstrated how IoT security camera collects data with no security in mind. Video coming from such devices are vulnerable and can be compromised, and malware such as Mirai can take advantage of these vulnerabilities. Their study monitored video streaming transmitted through the network, and capturing the streams using Wireshark, exposing the weakness of these devices – unencrypted data.The author Brian Cusack and Zhuang Tian tested surveillance cameras and found vulnerabilities, stating the urgency for best practice guidelines. The password of the camera where easily cracked, compromising the device.

Sublah Ullah tested smart cameras; smart cameras can capture confidential data and disclose the people they capture. As a result, protection and privacy have become a significant concern due to their broad implementation, the sensitive nature of the data collected, and the open infrastructure. The efficacy and reliability of security strategies is a particular challenge due to the resource limitations of smart camera systems [4].

As the security concerned in the IoT domain is evolving, IoT security touches on the most prevalent issue of privacy, identification, authentication, and lack of management. Authentication and authorization are currently the most missing component of IoT security. In the everyday lives of users, the growing number of IoT devices makes authentication and security-critical [10].

Finding a vulnerable camera connected to the Internet without any protection can easily be done using tools such as Shodan. Author Joseph Bugeja et al. conducted a vulnerability assessment on devices using Shodan, a search engine similar to Google. With the main feature of finding connected devices on the internet. They observed an alarming number of devices with poor configurations and lacking rudimentary security controls. The devices found represent serious privacy threats [11].

Williams et al. [12] conducted a large-scale vulnerability assessment of consumer IoT products on the Internet. The authors used Shodan and Nessus15 to search for vulnerabilities. The analysis included devices such as webcams, smart TVs, and printers, and then classified the security threats associated with each product category.

With this IoT device flooding the market, security is now a big concern. In an article published by Lisa Goeke, she explained IoT devices that use cloud-infrastructure sends their data to the "cloud" for reviews and analysis on users smartphones [13].The risk to personal data privacy issue arises when privacy is invaded, whether knowingly or unknowingly. People using compromised Cloud-based IoT Cameras deployed in homes to monitor, and a means of protection can be used to breach personal data privacy.

3. RESEARCH DESIGN

The researcher implemented a descriptive and quantitative approach is used to interpret the data collection and pen-testing result of the IoT Cloud-based Camera. Survey and questionnaire forms were distributed to participants along with interviews. A literature review was done to anchor the need for understanding the views of other authors on the topic and assessing the different technologies involved.

Implementing the penetration testing phase was done to find the vulnerabilities on the said IoT Cloud-based Security Camera. Results from the said test were evaluated and interpreted. Fig.4 shows the research methodology implemented.

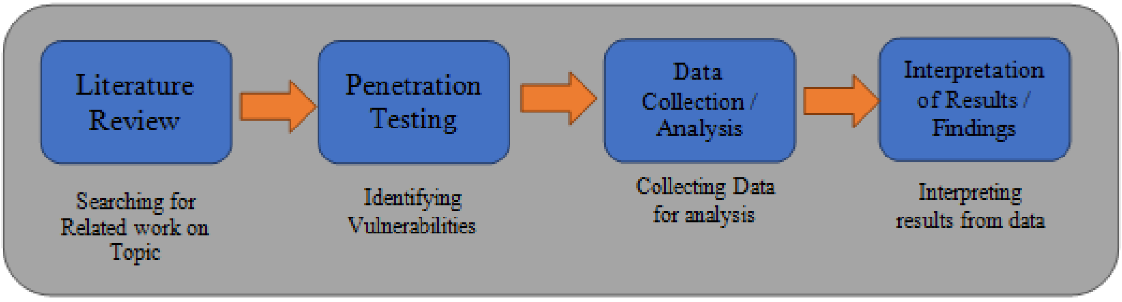

Literature Review
Penetration Testing
Data Collection / Analysis
Interpretation of Results / Findings
Searching for Related work on Topic
Identifying Vulnerabilities
Collecting Data for analysis
Interpreting results from data

Figure 3. Research Methodology

A. Participants

Selection of the participants of the study was done by means of purposive sampling. Five (5) families using the camera installed on their house were selected, one camera for each family, 2 (two) Car wash center installed on their garage for security purpose, and 1 (one) in a school for monitoring students security with five camera deployed. Bringing the total of nine IoT Cloud-based security camera running. Pre-survey was done to get the respondents to answer the need of installing surveillance camera on their premises. Testing of the device was done with their consent, this involved connecting to their WiFi network and implementing the penetration testing phase.

B. Ethical Consideration

The penetration testing phased involves the actual hacking of the participants IoT Cloud-based Camera. To protect the personal data privacy of the participants, written consent was first asked in the agreement of what the actual test will be. The penetrating testing was clearly explained and the reason for the study. Anonymity and confidentiality of all personal data or information from the participants were preserved.

C. Sources of Data

To anchor the need for the research. The researcher reviewed the literature pertaining to the research topic. Interviews, survey, online research and utilization of library resources was also conducted. Listed below are the detailed process is done for the data collection method.

a. Interviews Results

Using the interview results, the research learned of the participants need in using the IoT Cloud-based Camera as a surveillance system to protect and monitor their home premises or business location. The feeling of safety knowing everything in their location is monitored and recorded

b. Survey Results

With the pre-survey results, the researcher learned of the needs of the participants in implementing a surveillance system of their premises, why they choose to buy IoT Cloud-based Camera instead of CCTV Cameras

c. Penetration Testing Results

With the result of the penetrating testing, the researcher identified the vulnerabilities on the IoT Cloud-based Camera. Using findings mitigation method were implemented to hardened security of the IoT devices.

d. Internet and Library Research

The researcher made use of book, articles and online resources/material related to the security implementation and vulnerabilities of Internet of Things devices. The said materials and resources served as references in developing the study.

D. Research Instruments

The researcher used two instrument in this study. First is the pre-survey questionnaire which was used to gather information on respondents usage of their IoT Camera. With the pre-survey, it allowed the researcher to understand the need of the participants in using such a device, specifically the Cloud-based IoT Camera for security purposes.

Using the results of the post-survey, after the penetrating testing phased was done, the lack of security of the IoT device was shown. This allowed the researcher to recommend mitigation that will prevent hacking of the IoT device which in term breach the personal data privacy of the participants.

E. IOT Security Penetration Testing Framework

As part of the study, a penetration testing model will be followed to test the security of the IoT Cloud-based Camera. Three stages of the pen-testing model will be used.

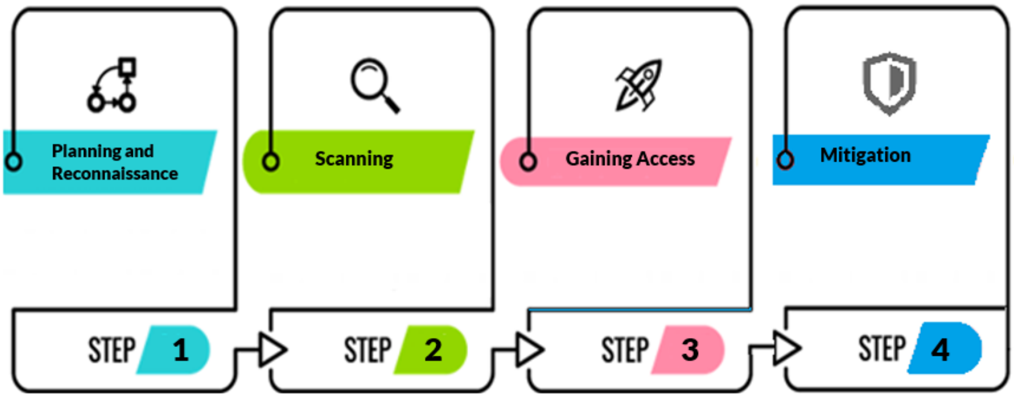


Figure 4. IoT Security Penetration Testing Framework

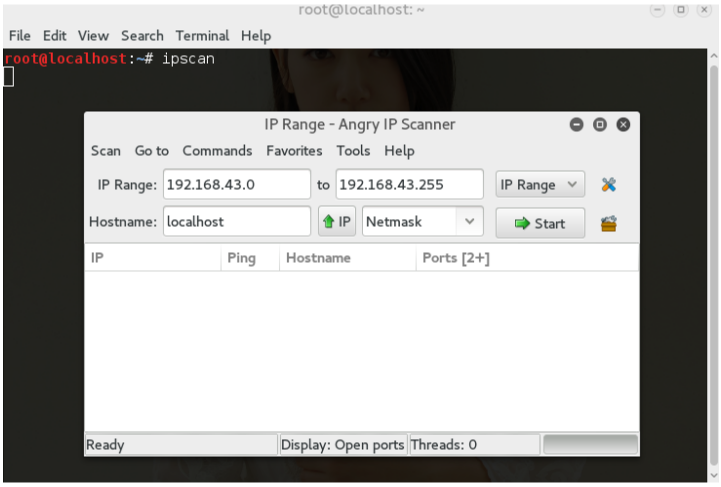
Using the above framework (Fig.3), testing the IoT security of the Cloud-based Camera will be done. Kali Linux will be the primary tool for the security testing phase. Kali Linux is a Debian operating system, use for penetration testing. It has the latest tool every hacker can use to hack into systems, including IoT devices.

Penetration Testing Procedures

To comprised the system,the following steps were done using the Penetration Testing Framework. To proceed with the Penetration Testing, the authors use Kali Linux as the primary Operating System (OS) of choice for penetration testing. Kali Linux is a Debian OS with pre-installed software tools for a security audit.

Step 1-Reconnaissance

The first step will be identifying the target by implementinga ping sweep to determine the IP address [14].Using Kali Linux as the Pen-testing operating system, the researcher uses AngryIP Scanner to scan the network for the IP address (Figure 4) of the IoT device. Angry IP Scanner is a cross-platform network scanner tool use to scan active IP address on the network. The program can run either in Windows or Linux operating system [15]. The result was to find active devices on the network (Fig. 5).


root@localhost: ~
File Edit View Search Terminal Help
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range
IP
Start
IP
Ping
Hostname
Ports [2+]

```
root@localhost:~# ipscan
```

IP Range: 192.168.43.0 to 192.168.43.255

Hostname: localhost Netmask

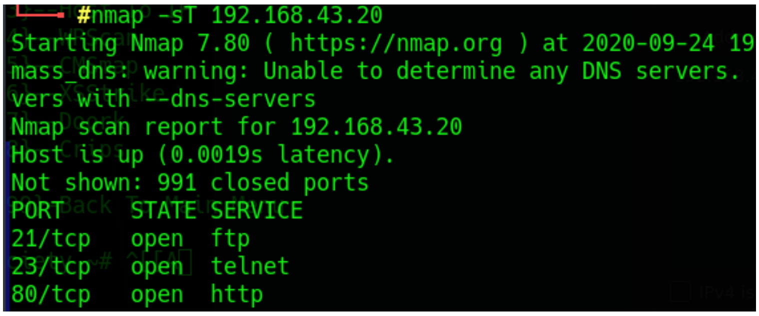
Ready | Display: Open ports | Threads: 0

Figure 5. Using Angry IP Scanner to find active devices on the network

Step 2- Scanning

The second steps involve finding open ports services on the IoT device. Every active service runs on a device usinga port with a corresponding number or port number to communicate. Identifying each active port can point out to what service is running on the device. As an example, port 80, by default, is the web service for each device running on the Internet.

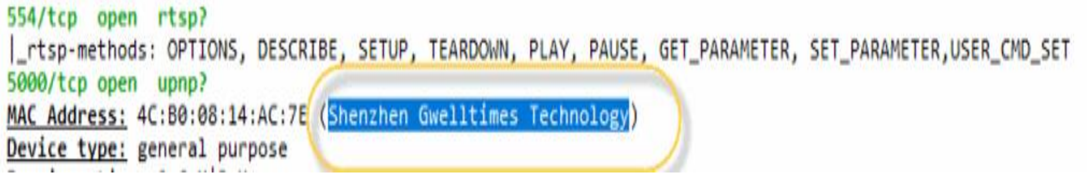
To the port scanning, Nmap was used. Network Mapper or nmap for short is an open-source tool for network and vulnerability scanning installed in Kali Linux. Used for network discovery and auditing. It can be used not only to identify open port but also identify security risk[16]. Nmap is designed to rapidly scan large networks, identify host, operating systems, services and firewalls. Fig.6 shows the open ports found on th devices. Services running on port 80-HTTP indicates the devices has a built-in web server for web application control.



```
└──╼ #nmap -sT 192.168.43.20
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-24 19
mass_dns: warning: Unable to determine any DNS servers.
vers with --dns-servers
Nmap scan report for 192.168.43.20
Host is up (0.0019s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
23/tcp   open  telnet
80/tcp   open  http
```

Figure 6. Nmap scan identifying open ports/services

From the scan output, port 554 used for Real-Time Streaming Protocol (RSTP) is open along with port 5000. RTSP is a protocol used for real-time transmission of media. It can be used to deliver continuous video stream which can be viewed [17]. The manufacture of the device is also identified as Shenzhen Gwelltimes Technology (Figure 7).



```
554/tcp  open  rtsp?
|_rtsp-methods: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, PAUSE, GET_PARAMETER, SET_PARAMETER,USER_CMD_SET
5000/tcp open  upnp?
MAC Address: 4C:B0:08:14:AC:7E (Shenzhen Gwelltimes Technology)
Device type: general purpose
```

Figure 7. Manufacturer information found on the nmap scan

Step 3 – Gaining Access

There are several ways in which the researcher gain access to the IoT devices. The first method is looking the history of the company who made the Cloud-based IoT camera. Doing a simple Google search gave the researcher the necessary step in compromising the IoT devices.

Shehzen Gwelltimes Technology Co., Ltd is a white-label vendor that produces Cloud-based camera. Their cameras are being sold around the world, label as a different product from a different vendor. All of their cameras use the default accounts admin as the main user and 123 as the password. Another security risk implemented by Shenzen is sequentially numbering their devcice ID. Any attacker who enumerate the device ID and use the default accounts (Fig.8).

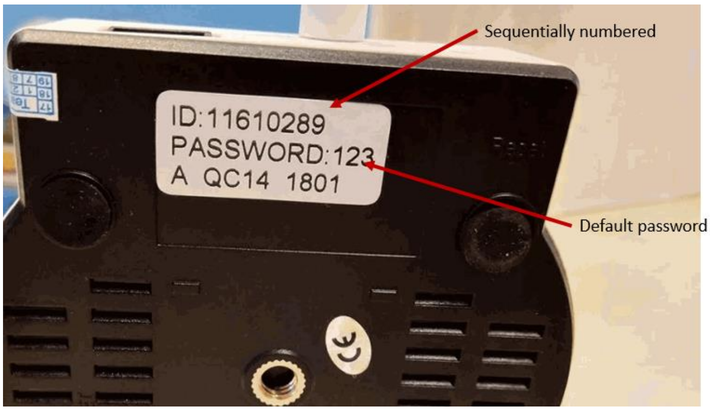
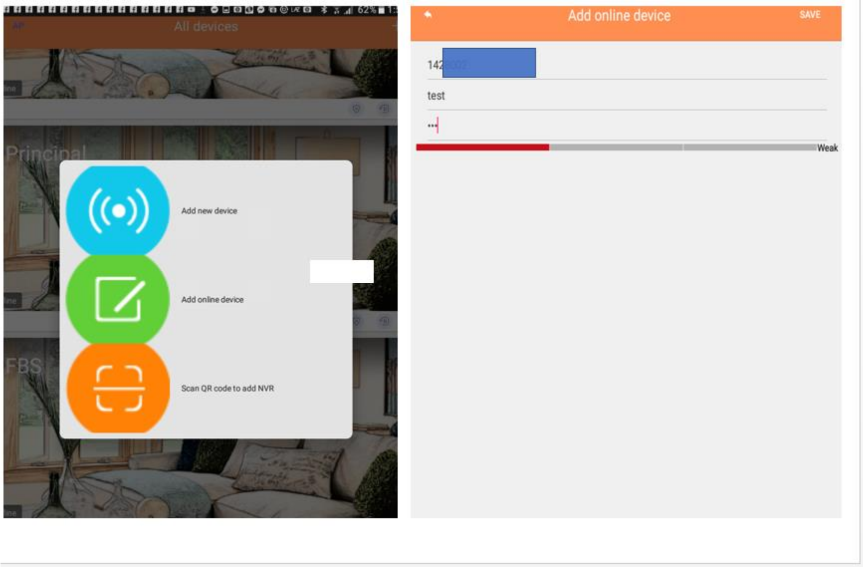


Figure 8. Default accounts and device ID

To use the Cloud-based camera, the user needs to install a mobile app called YYP2P, which is freely available on Google Play Store and Apple Apps Store (Figure 9).

Figure 9. YYP2P app

Fig.10 shows by just enumerating sequential device ID and using default accounts, several Cloud-based IoT



142[redacted]

test

•••

Figure 10. Device ID enumeration using sequential ID

Camera where compromised. Without the user knowing that their personal digital privacy has been invaded, as shown in Fig.11.

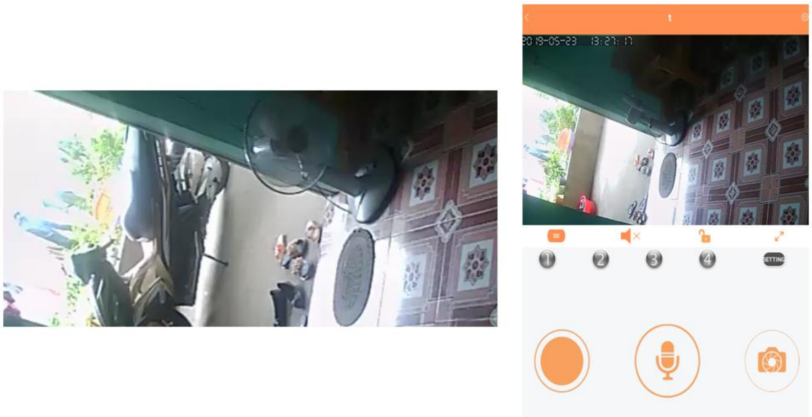


Figure 11. Compromised Cloud-based IoT Camera

Step 4- Mitigation

With the IoT cloud-based security camera compromised. Remote viewing the home of the user is possible without them knowing about it. As part of the mitigation phase, the user is informed of the breach of their device. A proper security update was implemented, the update of the firmware, and changing the user default password to a stronger one.

4. Results And Discussion

The researchers used a quantitative method to analyze the data, using a statistical treatment such as frequency and weighted mean. Based on the participant's response and the result of the vulnerability assessment and penetration testing. Statistical was used to analyze the data collected, focussing on (a) security of the device, (b) knowledge of the user in deploying the devices, and (c) the need for deploying such devices a means of protecting the premises.

A safety test was done to ensure privacy of the target device data. The scope of the test focusses only on the IoT cloud-based camera. Any other devices found on the network being attack were not the target of attack. During the process of scanning, devices such as PC, Smart TVs, laptops and tablets were also found. With the IoT cloud-based security camera compromised the device itselft can be used as a jumping point on the network to attack other devices.

Table 1 shows the primary reason why individual users and organizations are opting to deploy or install IoT Cloud-based security cameras. With 4.80 as the highest mean respondents saw the device as a way to protect their premises from intrusion, along with 4.70 in monitoring the premises. Accessing the camera from the internet and how easy it does it garnered 4.50 and 4.40, respectively

Table 1. Assessment for the need for deploying IoT Camera based on functionality

Indicators	Weighted Mean	Description
1. IoT Camera can protect the premises from intrusion	4.80	Exceedingly Functional
2. IoT Camera can be a tool to monitoring the premises	4.70	Exceedingly Functional
3. IoT cloud-based Camera is accessible from the internet using mobile app	4.50	Exceedingly Functional
4. IoT cloud-based Camera are easy to used	4.40	Very Functional
General Mean	**4.60**	**Exceedingly Functional**

Testing the security of the IoT Camera during deployment was done using the Penetration Testing Framework and on the knowledge of the user on the need for adequately securing the device employing changing the default user name and password. Table 2 shows the majority of the devices deployed by users are still using their default credentials with 4.80 highest mean. At the same time, 4.70 focuses on user knowledge on how to change the default credentials.

Table 2. Security of the IoT Cloud-based Camera – Default Credentials

Indicators	Weighted Mean	Description
1. Default credential still in used	4.80	Not Secure
2. Changing of default credential is not to the user	4.70	Not Secure
General Mean	**4.75**	**Not Secure**

5. CONCLUSION AND RECOMMENDATION

In this paper, we showed how vulnerable white-label IoT cloud-based security camera on the market today. Using the Penetration Testing Framework, the device was compromised with eased. Factors from default configuration and little knowledged of the user on how to change the default configuration of the device can lead to data privacy breach. The proliferation of mass produced and cheap IoT cloud-based security camera in the market today have become a means of securing everything from a store to a home. People are buying the devices and setting them up using default credentials can lead to personal data breach with their video stream being monitored by threat actors. With most of the devices in need of critical updates on their firmware, they are open and vulnerable from attacks. Proper security mitigation must be implemented on the manufacturer and on the user side.

6. REFERENCES

[1] "PRIVACY | definition in the Cambridge English Dictionary." [Online]. Available: https://dictionary.cambridge.org/us/dictionary/english/privacy. [Accessed: 23-Jun-2019].

[2] "Summary: Philippines Data Privacy Act and implementing regulations." [Online]. Available: https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/. [Accessed: 23-Jun-2019].

[3] D. G. Aneela, I. A. Anusha, K. Malavika, and R. Saripalle, "Research Trends of Network Security in IoT," vol. 4863, no. September, pp. 6–10, 2017.

[4] S. Ullah, L. Marcenaro, and B. Rinner, "Secure smart cameras by aggregate-signcryption with decryption fairness for multi-receiver IoT applications," Sensors (Switzerland), vol. 19, no. 2, 2019.

[5] "The Ultimate Guide to White-Label Products &amp; Solutions - Vendasta." [Online]. Available: https://www.vendasta.com/blog/the-ultimate-guide-to-white-label#how-white-label-works. [Accessed: 09-Jul-2019].

[6] "Why A White Label Solution Is Easier Than Building Your Own." [Online]. Available: https://www.forbes.com/sites/theyec/2014/06/03/why-a-white-label-solution-is-easier-than-building-your-own/#748a2186dd9e. [Accessed: 09-Jul-2019].

[7] "What is White Labeling? Pros and Cons of White Labeling Software | CallRail." [Online]. Available: https://www.callrail.com/blog/what-is-white-labeling/. [Accessed: 24-Jun-2019].

[8] K. Olha, "An investigation of lightweight cryptography and using the key derivation function for a hybrid scheme for security in IoT," p. 42, 2017.

[9] Y. Seralathan et al., "IoT security vulnerability: A case study of a Web camera," Int. Conf. Adv. Commun. Technol. ICACT, vol. 2018-Febru, pp. 172–177, 2018.

[10] J. Porras, J. Pänkäläinen, A. Knutas, and J. Khakurel, "Security In The Internet Of Things - A Systematic Mapping Study," Proc. 51st Hawaii Int. Conf. Syst. Sci., pp. 3750–3759, 2018.

[11] J. Bugeja, D. Jönsson, and A. Jacobsson, "An Investigation of Vulnerabilities in Smart Connected Cameras," 2018 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2018, pp. 537–542, 2018.

[12] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, “Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach,” 2017 IEEE Int. Conf. Intell. Secur. Informatics Secur. Big Data, ISI 2017, pp. 179–181, 2017.

[13] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, “Security challenges of the Internet of Things,” Internet of Things, no. 9783319507569, pp. 53–82, 2017.

[14] J. N. Goel and B. M. Mehtre, “Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology,” Procedia Comput. Sci., vol. 57, pp. 710–715, 2015.

[15] “Angry IP Scanner - the original IP scanner for Windows, Mac and Linux.” [Online]. Available: https://angryip.org/. [Accessed: 10-Jul-2019].

[16] “What is Nmap? Why you need this network mapper | Network World.” [Online]. Available: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html. [Accessed: 10-Jul-2019].

[17] “What is Real Time Streaming Protocol (RTSP)? - Definition from Techopedia.” [Online]. Available: https://www.techopedia.com/definition/4753/real-time-streaming-protocol-rtsp. [Accessed: 10-Jul-2019].

AUTHORS

Dr. Marlon I. Tayag is a full-time Associate Professor at Holy Angel University and teaches Cyber Security subjects on Ethical Hacking and Forensic. He earned the degree of Doctor in Information Technology from St. Linus University in 2015 and is currently taking up Doctor of Philosophy in Computer Science at Technological Institute of the Philippines – Manila. Dr. Tayag is Cisco Certified Network Associate, 210-250 CCNA Understanding Cisco Cybersecurity Fundamentals and Fluke CCTTA – Certified Cabling Test Technician Associate. Microsoft Certified Professional and Microsoft Certified Educator.

Dr. Francisco D. Napalit, is a result driven IT professional who got a doctoral degree in Information Technology, with experience in the administration and support of information systems and network systems. Experienced in implementation, analysis, optimization, troubleshooting LAN/WAN network systems. Strong hands-on technical knowledge in CyberSec OPS, Cyber Crime Incidence Response, MCP, CCNA, Fluke Networks certifications. Proven ability to lead and motivate project teams to ensure success. Track record for diagnosing complex problems and consistently delivering effective solutions.A solid 24 years work experience in diff. companies, institutions, organizations and currently the Dean of School of Computing at Holy Angel University. He is one of the founders and former vice president of Information Systems Security Association of the Philippines with direct experience in corporate and professional training, education and consulting in the field of I.T. and network systems. A subject matter expert (theoretical and practical), who got a hands-on experience in curriculum design and syllabus design in his varied work in different universities and colleges here and abroad. He is an individual who got strong business insight and passion for training and development, and with a good training and facilitation skills.

Prof. Arcely Perez-Napalit is a full-time faculty under the Computer Science Department of Holy Angel University. She’s been teaching for almost two decades. One of her motto in teaching is to help students develop their logical and critical thinking and develop the character of a student as a whole. She also shared her passion for teaching overseas for six years. She is currently pursuing her post-graduate studies under the Ph.D. in Computer Science. She is also the coordinator representative in the outreach project and became a research facilitator of the School of Computing.