SURVEY ON IP CAMERA HACKING AND MITIGATION

DEVANG THAKAR
Student
Department of Computer Engineering,
Marwadi University, Gujarat, India
devangthakar07@gmail.com

ABSTRACT

IP based cameras have been replacing the CCTV cameras as CCTV cameras cannot be used for monitoring and surveillance over the network. IP cameras can be used for monitoring and surveillance purpose over the network as they are connected with the network cable and can send their feeds to centralized server or monitoring system. Thus, the IP cameras are having security features implemented. IP cameras are not much secured as the manufacturers and the deployment organizations do not concern about the security of IP cameras and it surveillance system.

Survey conducted on various major vulnerabilities and mitigation to the particular vulnerabilities found in the IP cameras and surveillance systems. Studied existing vulnerabilities in IP cameras and surveillance systems and provided mitigation to the particular vulnerability. Hopefully findings of vulnerabilities and mitigations will be valuable to organization working with the IP cameras and surveillance systems and society as well.

Keywords: Hacking, IP camera, Network Video Recorder, Surveillance System, Mitigation

1. INTRODUCTION

The first ever CCTV Camera was used in 1942 to monitor V-2 rockets. This technology was designed by the engineer Walter Bruch. In 1949, his technology which was later launched on a commercial level. CCTV technology has been burgeoning briskly and has gotten better with time. Now cameras come equipped with high megapixels, stronger durability, weather resistant, infrared light with nigh vision equipped to it and even radio for voice transmission. This technology has been a major help for the authorities in crime prevention and monitoring [8]. IP cameras and surveillance systems consists of cameras, Digital Video Recorder (DVR)/Network Video Recorder (NVR), servers and network are becoming very common all around the world. Nowadays, IP cameras based surveillance systems are basic fundamental for most of the life areas of the modern society. Their use is immensely moving over wide areas such as law enforcement and crime prevention, to transport safety and traffic monitoring, and control of retail, to unauthorized, illegal and even criminal use.

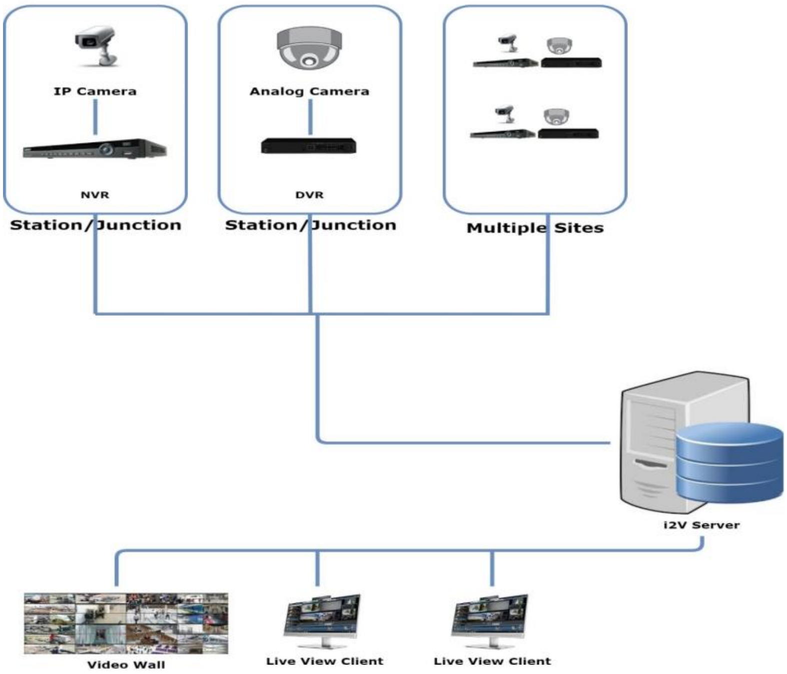
Usually, most of worries about IP camera and surveillance systems are related to privacy issues for obvious reason. The privacy impact of IP camera and surveillance system is notably important vital in the light of revelations about global IP camera surveillance programs. As progressively embedded devices are being analyzed at large scale for vulnerabilities, it is no amaze that IP camera and surveillance systems have recently boosted a dramatic increase of attention from security researchers. Those and similar studies led to more than a few vulnerabilities with large impact in real life. The assortment of vulnerabilities in those studies precisely implies the unhealthy state of cyber security of IP cameras and surveillance systems.

In this paper, conducted an organized review of the existing threats and vulnerabilities in IP cameras and surveillance systems based on found in research papers which are publically available. Additionally, we survey main risk and attack for IP cameras and surveillance systems. We also serve some remediation and mitigation that can benefit to enhance the security and privacy levels.

Main contributions are:

- Present the various types of vulnerabilities and various types of attacks found in and against the IP cameras and surveillance systems.
- Discuss in-depth novel and specific vulnerabilities and attacks on IP cameras and surveillance systems.

Fig 1: IP camera and surveillance system



2. RELATED WORK

At one side researchers approached the security and threat modelling of different parts of IP camera and surveillance system. Haitao Xu, Fengyuan Xuy, and Bo Chenz [7] have observed and investigated IP cameras with no password protection on the online directory of IP cameras. They have found large number of IP cameras without password protection and also gathered information about IP cameras such as open ports and web servers. Where some researchers had developed the infrastructure for testing the wireless IP cameras on their own and found some vulnerabilities in the wireless IP cameras [6]. Jungho Kang, Jaekyung Han and Jong Hyuk Park [5] have designed the access control protocol for IP cameras using hierarchical group key.

On the other side some researchers tried to find the vulnerabilities based on the taxonomies. Thomas Doughty, Nauman Israr and Usman Adeel have found the different vulnerabilities in IP cameras and surveillance system using ARP poisoning method; they have found vulnerabilities such as DDOS attack, MITM attack, and ARP poisoning attack vulnerabilities. They have also done brute force attack and packet sniffing as well on their own developed environment of IP cameras and surveillance system [1]. Brian Cusack and Zhuang Tian have setup the system of IP camera and surveillance system and performed pilot test to find out the vulnerabilities on the IP cameras and surveillance system. They evaluated vulnerabilities of IP cameras [2].

Based on above related work, survey what are the common vulnerabilities found in the IP cameras and surveillance systems and what is the mitigation have been provided for the particular vulnerability.

3. REVIEW OF VULNERABILITIES, ATTACKS AND MITIGATIONS

Determined the common vulnerabilities found in the IP cameras and surveillance system by surveying. On the basis of particular vulnerability determined attacks that can be happened using specific vulnerability. At last noticed some of the mitigation provided by the researchers to mitigate some of the vulnerabilities in IP cameras and surveillance systems. Commonly found vulnerabilities are weak passwords, poorly protected credentials, insecure configuration management, and more [9].

In below sub sections presented the vulnerabilities and mitigation that were determined from the different white papers in which the researchers have found those vulnerabilities and possible attacks and provided mitigation for that particular vulnerability.

3.1 Discussion on specific vulnerability and attacks

3.1.1 Denial of Service

Denial of Service is a prime goal for the attacker, as this can set back the raising of the alarm, and deny the gathering of evidence after the incident has been detected [1].

In this kind of attack, attacker tries to gain access of the DVR/NVR of the IP camera and surveillance system and tries to get down IP camera or the whole surveillance system by sending large number of requests to the DVR/NVR or to the IP cameras. Sending large number of requests to the system causes shut down or hanging problem of the system due to the unable to handle the large number of requests.

Attacker can shut down the whole surveillance system by performing this attack on the system. These systems are very much vulnerable for this attack as IP cameras and surveillance system are open to access and their servers are not able to handle the huge amount of traffic at the same time.

3.1.2 Man in the Middle

Man in the Middle attack is very dangerous attack for the IP cameras and surveillance systems. Attacker sits between client and server of the surveillance system using ARP poisoning method and tries to capture the traffic between client and server and attacker can also alter the data packets and can change the data in between client and server.

Performing this attack on the IP cameras and surveillance systems is very easy for attackers as there are not much security measures concerned by the manufacturers and the client who implement these systems. As the No/weak encryption algorithms are used to transfer the data and feed of the IP cameras to the DVR/NVR and to the server as well, therefore all the data packets are going unencrypted and anyone can view and alter the data or feed from the data packets.

This is one of the major vulnerability found in the IP cameras and surveillance system which can cause the whole system and can impact will affect the common people of society.

3.1.3 Weak Authentication or Authorization

Weak authentication or authorization of the IP cameras and surveillance system is the major problem till date. Login portals are still using weak authentication mechanism and the clients are not aware of changing or removing default password to access IP cameras and surveillance systems.

Authentication mechanism provided by manufacturers is weak in terms of accessing the system. Clients or the users are still using the default user names and password to access the IP cameras and surveillance systems. As the weak authentication has been provided by the manufacturers, attackers can easily get into the system by brute forcing on login portals and can easily get access the IP cameras and the surveillance systems. Attacker can do anything by getting into the system and can damage the whole system.

Weak authentication or authorization is very basic and crucial vulnerability in the IP cameras and surveillance systems. Manufacturers need to make the login portals strong for authentication and users also need to be aware of to remove or disable default user name and password.

3.1.4 Remote Code Execution

Remote Code execution vulnerability is also found in the IP cameras and surveillance systems. This vulnerability allows attacker to remotely access the system and to execute the arbitrary code on IP cameras and surveillance system.

This vulnerability causes due to the non-updated firmware and using old versions of software/firmware in the IP cameras and surveillance system. Using this vulnerability attacker can get the access of the whole system along with the DVR/NVR and the servers and by exploiting this vulnerability attacker will cause damage to the whole system performing arbitrary codes on the system or servers.

Remote Code Execution is also one of the dangerous vulnerability found in the IP cameras and surveillance systems.

4. MITIGATIONS PROVIDED

In this part, stated some mitigations provided by the researchers for the various vulnerabilities of the IP cameras and surveillance systems.

One of the mitigation provided by the researchers is strong user authentication using steganography. Researchers have developed a protocol named as “User Authentication Protocol” to block the malicious users [3]. Design of IP camera access control protocol utilizing hierarchical group key is also mitigation provided by researchers [5].

Above provided both the mitigations are for access control or user authentication utilizing which we can secure IP cameras and surveillance systems from unauthenticated user and attackers.

MITM vulnerability mitigations provided are to make the communications secure between client and servers by using the encryption algorithm for safe and secure communication. So the attackers not able to get the clear texted data.

5. RECOMMENDATIONS

Apart from the mitigations provided by the researchers in this part we will try to give some solutions in brief to the above stated vulnerabilities.

Below we summarize a set of recommendations that we hope can help enhance the security of the firmware and network communication of IP cameras and video surveillance systems. With enhanced security, we hope that a safer operation and an increased privacy of the entire IP camera and surveillance system could be achieved.

- Users of the IP camera and surveillance system have to change the default user ID and passwords or remove it from system.
- Another way is to regularly update firmware of the IP camera and system.
- Use the strong passwords for login.
- Use encryption algorithms for communication over network.
- Properly configure the IP camera network and surveillance system.

6. CONCLUSION

This paper provides a systematic review of security of IP camera and surveillance systems by describing in detail vulnerabilities, attacks, and mitigations. Based on publicly available data and existing classifications and taxonomies, the review presented in this paper provides comprehensive information on how video surveillance systems can be attacked and protected. This knowledge can then be used to better understand and identify the security and privacy risks combine with the development, deployment and use of these systems. Moreover, this paper presented a set of recommendations that can enhance the security and privacy aspects of IP cameras and surveillance systems.

7. REFERENCES

1. B. Cusack, Z. Tian “Evaluating IP surveillance camera vulnerabilities”, 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia
2. C. Moon, K. Ryoo, “Control System for Security Enhancement of CCTV Camera Maintenance Devices”, International Journal of Engineering & Technology, 7 (3.24) (2018) 104-109
3. C.H.M. van den Bogaard, “Security Analysis of Cloud-Based Video Cameras” Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on.
4. Checkmarx Application Security Research Team, Jaekyung Han and Jong Hyuk Park, “Exposing Wireless IP Camera Security Flaws”.
5. Costin, “Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations”, 6th International Workshop on Trustworthy Embedded Devices, Vienna, Austria — October 28 - 28, 2016

6. Haitao Xu*, Fengyuan Xuy, and Bo Chenz, “Internet Protocol Cameras with No Password Protection: An Empirical Investigation”, International Conference on Passive and Active Network Measurement PAM 2018

7. J. Bugeja, D. Jönsson, and A. Jacobsson, “An Investigation of Vulnerabilities in Smart Connected Cameras”, Second International Workshop on Pervasive Smart Living Spaces, Internet of Things and People Research Center and Department of Computer Science and Media Technology, Malmö University, Malmö, Sweden

8. J. Park and S. Kim “Study on Strengthening Plan of Safety Network CCTV Monitoring by Steganography and User Authentication”.

9. Jungho Kang, Jaekyung Han and Jong Hyuk Park, “Design of IP Camera Access Control Protocol by Utilizing Hierarchical Group Key”.

10. M. Rafiuddin, P.S. Dhubb, H. Minhas “RECENT STUDY OF CLOSE CIRCUIT TELEVISION (CCTV) IN HACKING”, 3rd international conference on latest trends in engineering science, humanities and management, Indian Federation of United Nation Association, New Delhi (India), 8th April, 2017

11. T. Doughty, N. Israr and U. Adeel “VULNERABILITY ANALYSIS OF IP CAMERAS USING ARP POISONING”, 8th International Conference on Soft Computing, Artificial Intelligence and Applications (SAI 2019), June 29-30, 2019, Copenhagen, Denmark