ISSN 2586-1816
Journal of Convergence for Information Technology e-ISSN 2586-4440
Vol. 8. No. 6, pp. 129-134, 2018 DOI : https://doi.org/10.22156/CS4SMB.2018.8.6.129

The Analysis of CCTV Hacking and Security Countermeasure Technologies: Survey

Sunghyuck Hong[1*], Sae-Young Jeong[2]
[1]Associate Professor, Div. of Information and Communnication, Baekseok University
[2]Student, Div. of Civil-Engineering Education, Chungnam National University

CCTV 해킹에 대한 분석 및 보안 대응책 연구: 서베이

홍성혁[1*], 정세영[2]
[1]백석대학교, 정보통신학부 부교수, [2]충남대학교, 건설공학교육과 학생

Abstract This is about the CCTV hacking which is one of the recently emerging privacy-spilling crime. Recently, the usage of CCTV is being increased, and Black Hat Hackers spill the individual's privacy by hacking it. However, That crime is being increased. However, most users rarely fulfill the security management ,and the government's measures are insufficient. Therfore, this research report implies some security technologies including user authentication protocols such as SSH Tunneling and Media Encryption Algorithm. and recently developed technologies including Wookyeong Information Technology's SecuWatcher for CCTV, Norma's CCTV Care App, and MarkAny's Password SAFERTM for CCTV.

Key Words : Privacy-spilling Crime, CCTV Hacking, User Authentication Protocol, SSH tunneling, Media Encryption Algorithm

요 약 최근 부각되고 있는 사생활유출범죄 유형 중 CCTV 해킹을 이용한 범행에 대한 것이다. 요즘 CCTV를 사용이 증가함에 따라 악의적인 해커들은 CCTV를 사생활유출수단으로써 이용하고 있다. 그러나 이러한 CCTV 해킹을 통한 범죄가 늘어나고 있는 반면 일반 사용자들의 보안의식 수준은 현저히 낮았고, 국가적 차원에서의 대응·대책 또한 부실한 상황이다. 따라서 이번 연구논문을 통해 CCTV 해킹을 방지할 수 있는 여러 보안기술에는 중 사용자 인증 프로토콜, SSH 터널링을 통한 원격접속, 미디어 암호화 알고리즘 등을 소개하고, 최근에 출시된 기술로는 우경정보기술사의 SecuWatcher for CCTV, 노르마사의 CCTV Care 앱, 마크애니사의 Password SAFERTM for CCTV 등을 분석하여 대응책을 제시하여 CCTV 해킹으로부터 피해를 줄이기 위한 제안을 하였다.

주제어 : 사생활유출범죄, CCTV 해킹, 사용자 인증 프로토콜, SSH 터널링, 미디어 암호화 알고리즘

1. Introduction

The content of the introduction is about the so-called privacy leakage crime, which is one of the issues that have become a big issue these days. Cyber crimes related to the leakage of personal privacy in the Korean society, such as the use of a stigma known as the ″ Particularly, it should be noted that privacy leakage using CCTV is increasing. In other words, the purpose of CCTV is to maintain personal and public safety and security, but CCTV is rather abused as another secret camera.

*This research is supported by Baekseok University fund in 2018.
*Corresponding Author : Sunghyuck Hong (shong@bu.ac.kr)
Received October 2, 2018 Revised November 7, 2018
Accepted December 20, 2018 Published December 31, 2018

The ongoing inspection of the state in 2018 has also raised concerns about the above. According to a survey conducted by the National Assembly Science and Technology Broadcasting Commission, Park Seong-jung revealed that 8 out of 10 personal information infringement cases in the National Human Rights Commission's "Human Rights Report" of March last year infringed privacy related to CCTV,), But the government's response was inadequate [1]. Analysis of the hacking method revealed that most of them use 'Shodan' site to access CCTV which is in a defenseless state and hack in real time. 'Shodan' is a site designed to allow hackers to search and penetrate all the Internet-connected devices around the world [2]. Fig. 1 shows high ratio of harmful devices on each country. US is highest and African countries are relatively low.

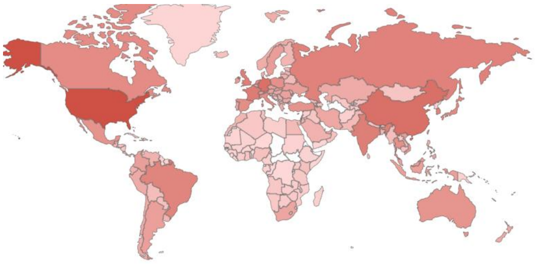

Fig. 1. Shodan Homepage

This hacked CCTV allows the citizens to see the realities of their private lives by hacking the CCTV installed in the house as well as the citizens who are walking on the streets. Moreover, even the major national key facilities and industrial facilities are managed using CCTV. If such a cyber attack is violated, national security will be hindered and economic losses due to the leakage of core technologies can result. Therefore, this research report presents the various causes of CCTV attack on hacking in Chapter 2, presents the related security technologies in the existing or under development in Chapter 3, and in the last chapter, what direction should the countermeasures be established in the future? I will conclude by presenting.

2. CCTV Hacking Reasons

2.1 User Management Fault

CCTV hacking vulnerabilities used by individuals and small groups are, above all, in the lull of security management of their own. With the recent development of IoT technology, it has made a great contribution to the prevention of theft and the safety management of children and companion animals by confirming the home CCTV image in real time from a remote location with a smart phone. Fig 2 shows IoT Home CCTV.

Fig. 2. IoT Home CCTV

However, even though the use of CCTV is increasing, the recognition level of CCTV information security is not enough. Because most home CCTVs are based on Wi-Fi, Wi-Fi, where many hosts share the network, is able to penetrate easily by hacking IDs and passwords, not just the original users, but also third parties. It is said that it is most likely to be hacked because it does not change the password of the router and leaves it with the initial number which can be very easily found such as 1234 and 0000 [3]. Of course, users with professional hacking techniques may be hacked, but basically, if you are interested in basic security management, such as changing your password periodically, you will not be easily hacked.

2.2 Usage of Made in China CCTV

Nowadays, as cheap Chinese CCTV is circulated, anyone can easily buy CCTV, which means that the use of CCTV from China will serve as a means for personal information leakage by Chinese hackers. Although it is not all about Chinese products, Chinese hackers have applied backdoor hacking technology to products exported to South Korea and leaked the privacy of female users to unauthorized distribution on their adult sites [4]. Backdoor is a hidden door, and it is used in the IT field to refer to the system without going through security procedures. However, the more serious problem is that not only individuals but also public institutions use Chinese products. In particular, half of the CCTV installed at the Gwacheon government building was found to be made in China, and it was revealed that the Kori nuclear power plant also uses Chinese products. However, the government is not responding properly [5].

3. Related Security Technology

So far, I have analyzed the causes of hacking in CCTV. Though most of the causes are in the user's management mismanagement, technical measures to prevent professional hacking, such as information leakage from China, are also needed. Therefore, this chapter describes CCTV security related technologies which are present or under development.

3.1 User Authentication Protocol

The basic principle of IP CCTV is the connection method through user ID and password, which is a very common and common access method. Conventional analog CCTV which exchanges information through coaxial cable is easy to be intercepted by malicious user during information exchange, installation is very complicated, and there is also problem with image quality. Nowadays, installation is simple, image quality is excellent, I use a wireless IP CCTV which can easily check the image anytime and anywhere. However, in case of wireless CCTV, most of them send and receive real-time information based on Wi-Fi. Therefore, the technology that is introduced to improve the problem of simple connection method which is vulnerable to security is user authentication protocol. The user authentication protocol is used to authenticate the user during the user registration process. In addition, the user authentication is strengthened by using the R number, which is a random number given at the time of login, in addition to the unique number concept of the CCTV, and prevents unauthorized access due to the unlock crack It is designed. The user is accessed through the Integrated Management System (VMS) to be authenticated. The following is the procedure of user authentication protocol.

1. The user makes a service request to VMS.
2. The VMS requests information from the user.
3. User logs in using ID, password and SN.
4. Perform user authentication and provide IP address and one time R value.
5. The user connects to CCTV and sends ID, password, SN, R value to request service.
6. CCTV sends authentication information to the VMS.
7. VMS performs authentication and notifies service availability if it matches.
8. CCTV notifies the user of the authentication completion message and starts to provide the service.

Fig 3 shows procedure of current user authentication protocol in CCTV system.

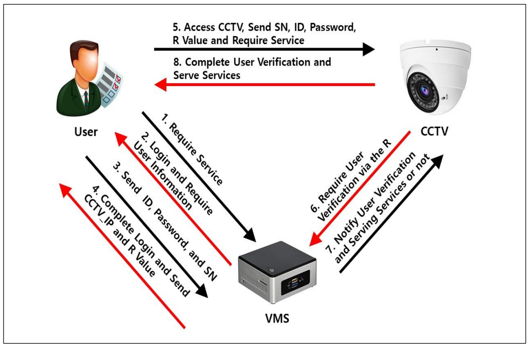
5. Access CCTV, Send SN, ID, Password, R Value and Require Service
8. Complete User Verification and Serve Services
User
CCTV
1. Require Service
2. Login and Require User Information
3. Send ID, Password, and SN
4. Complete Login and Send CCTV_IP and R Value
6. Require User Verification via the R
7. Notify User Verification and Serving Services or not
VMS

Fig. 3. Procedure of User Authentication Protocol

The strength of the user authentication protocol is that, even if an external intruder finds out the ID and password of the user, the CCTV hacking is virtually impossible if the SN given at the time of membership registration can not be found, and moreover, the disposable R value This is the best technology in terms of security because it changes every time [6]

3.2 SSH Tunnelling

Next, it is about CCTV remote access technology through SSH tunneling. The first principle is that the user receives the information through the tunneling system with secure connection and creates the encrypted tunnel between the CCTV cameras. Data transmitted through this tunnel is subject to security encryption and can not be hacked through sniffing. The procedure and configuration are similar to the previous user authentication protocol, but in this case the tunneling system replaces the VMS.

The second principle is that if the CCTV camera exists in a firewall or a VPN, the tunneling server acts as an intermediary for the CCTV camera to solve the connection problem in order to improve the situation that the connection from the outside is impossible. Fig 4 shows the configuration of SSH.

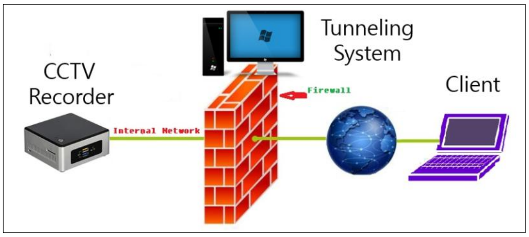

Fig. 4. SSH Tunneling System

The disadvantage of the SSH tunneling technology is that the encryption / decryption process for the system security is delayed. However, it is the ultimate advantage of the technology that the security performance can be improved while bypassing the firewall and the network obstacle [7]

3.3 Media Cryptographic Algorithm

The next method is to encrypt video media to prevent unauthorized distribution due to external intrusion when mainly distributing CCTV images for black box video or incident / accident analysis. Especially, it is applied to embedded system which has low computing ability like CCTV.

Such a system requires an H.264 codec. The codec has a NAL structure. In the NAL structure, it is possible to convert compressed video data without directly accessing the codec. There are several block encryption algorithms for encryption, such as SEED, AES, and TDES. The procedure first detects the byte to be encrypted. In the reference paper, we do not encrypt all parts, but encrypt only the screen related parts so that the screen is not exposed to the outside. The following table summarizes the types of NAL structure types. Table 1 describes NAL unit type classes.

Table 1. NAL unit type Classes

NAL unit type	Content of NAL unit
0	Unspecified
1	Coded slice of a non-IDR picutre
2	Coded slice data partition A
3	Coded slice data partition B
4	Coded slice data partition C
5	Coded slice of an IDR picture
6~31	-

Next, the algorithm for detecting the byte to be encrypted is as follows. There is also an encryption method using the HIGHT algorithm, but it will be omitted. The ultimate advantage of the media encryption algorithm is that it saves time because it detects only the parts that need to be encrypted rather than encrypting the whole screen, and it does not burden the embedded system with low computation ability like CCTV[8].

3.4 Recently developed security technology

SecuWatcher for CCTV is a product launched by

Woo Kyung Information Technology, a security solution company in 2017. The feature of this product is to encrypt and transmit images transmitted from CCTV in real time, and to protect user authentication and image file by applying image forgery prevention technology when exporting image data to the outside. The dynamic object privacy management technology based on face recognition is a unique technology of this company and it can be applied to all images generated in real time by providing customized privacy[9].

3.4.2 CCTV Care App

The CCTV Care App is useful for individual users who do not have a separate security system. It first diagnoses the security risks, detects vulnerable CCTV devices or networks, analyzes the vulnerabilities, and presents solutions. In addition, it measures and manages security passwords, viruses, and security vulnerabilities of the device itself. This program is freeware and anyone can easily download it[10]. Fig 5 shows detectiing algorithm.

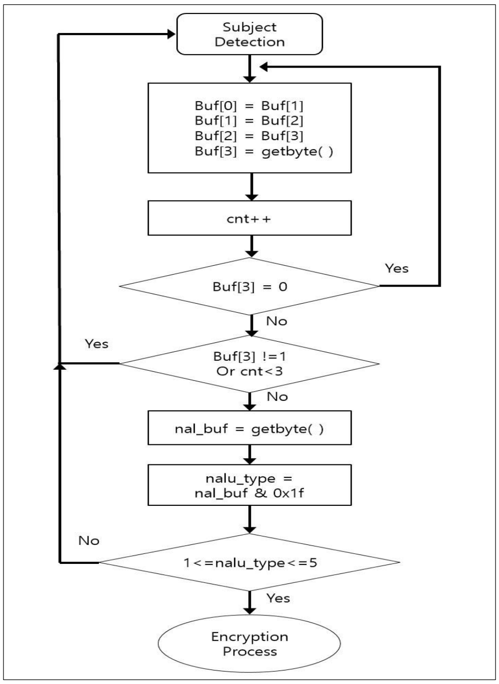

Fig. 5. Algorithm for Detecting bytes to encrypt

3.4.3 Password SAFERTM for CCTV

Password SAFERTM for CCTV is a password security management technology developed by domestic security solution company, MarkAny. You need to change the password periodically and store and manage its history. Passwords are encrypted in real time and stored in the database, designed to be automatically applied to VMS. In addition, fingerprint recognition technology has been introduced to enhance convenience, and it has become possible to issue OTP, a one-time password for external users [11].

4. Conclusion

It is also important for governments and companies to apply IP filtering techniques, VPN tunnel techniques, a method of separating the CCTV video surveillance network from the general network, and a method of mounting a CCTV dedicated certificate. In addition, by strengthening the certification system of information security management system, which is a system for certifying the security reliability of information system, it is necessary to make efforts to prevent CCTV hacking at the national level [12-14].

REFERENCES

[1] M. C. Yim. (2018. 10. 10.). *Congressman Seong-Jung Park says “Most of the CCTV Hacking is Defenseless state”.* ZDNetKorea. *.http://www.zdnet.co.kr/news/*news_view.asp?artice_id=20181010140028&type=det&re=zdk

[2] Y. S. Go. (2016. 2.). *Study of Security vulnerability IOT device IP exposure threat prevention system.*. Bukyeong National University, Busan.

[3] J. Y. Byeon. (2017). *'IP camera' hacked 'clumsy'... Clear outflow immediately.* Sanup News. http://www.kidd.co.kr/news/199010

[4] K. T. Lee. (2018. 8. 22). *Chinese CCTV Hackes Korean Privacy.* Digital Times. http://www.dt.co.kr/contents.html?article_no=2018082302100351041002&ref

[5] B. S. Jeon & H. C. Yang. (2018). *Chinese CCTV hacking*

is defenseless. MBN News. http://www.mbn.co.kr/pages/vod/programView.mbn?bcastSeqNo=1194180

[6] T. S. Park. (2011). *Design and Implementation User Authentication Protocol to Prevent Malicious User in IP CCTV Enviornment.* Sungsil University, Seoul.

[7] G. J. Hwang, J. P. Park & S. M. Yang. (2016). *Security Technique using SSH Tunneling for CCTV Remote Access.* Sungsil University, Seoul.

[8] S. C. Hwang. (2012). *Development of Media Crypto Algorithm for anti-hacking into CCTV.* Indeok University, Seoul.

[9] N. I. Heo. (2017). *CCTV Video Hacking Protection Solution "SECUWATCHER".* Money Today. http://news.mt.co.kr/mtview.php?no=2017121109240835573

[10] N. I. Heo. (2018). *Norma released CCTV Security App "CCTV Care".* ETNews. http://www.etnews.com/20180717000198

[11] S. Hong. (2017). Research on IoT International Strategic Standard Model. *Journal of the Korea Convergence Society, 8(2),* 21-26. DOI : 10.15207/jkcs.2017.8.2.021

[12] G. W. Lee. (2012). *A Study on Public Institutions CCTV Information Security Management System.* Dankook University, Yongin.

[13] S. Hong. (2014). Analysis of DDoS Attack and Countermeasure: Survey. *The Journal of Digital Policy and Management, 12(1),* 423-429. DOI : 10.14400/jdpm.2014.12.1.423

[14] S. Hong. (2013). Disconnection of Wireless LAN Attack and Countermeasure. *The Journal of Digital Policy and Management, 11(12),* 453-458. DOI : 10.14400/jdpm.2013.11.12.453

홍 성 혁(Sunghyuck Hong) [정회원]

- 1995년 2월 : 명지대학교 컴퓨터공학과 (공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2007년 9월 ~ 2012년 2월 : Texas Tech University, Office of International Affairs, Senior Programmer
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : Network Security, Hacking, Secure Sensor Networks
- E-mail : shong@bu.ac.kr

정 세 영(Jeong, Saeyoung) [학생회원]

- 2015년 2월 : 제천고등학교 졸업
- 2015년 3월~ 현재 : 충남대학교 건설공학교육과 재학
- 관심분야 : 정보통신, 데이터 분석
- E-Mail : oph5932@naver.com