2017

Evaluating IP surveillance camera vulnerabilities

Brian Cusack
Auckland University of Technology

Zhuang Tian
Auckland University of Technology

Recommended Citation

Cusack, B., & Tian, Z. (2017). Evaluating IP surveillance camera vulnerabilities. DOI: https://doi.org/10.4225/75/5a84efba95b46

DOI: 10.4225/75/5a84efba95b46
Cusack, B., & Tian, Z. (2017). Evaluating IP surveillance camera vulnerabilities. In Valli, C. (Ed.). (2017). *The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017*, Edith Cowan University, Perth, Western Australia. (pp.25-32).

EVALUATING IP SURVEILANCE CAMERA VULNERABILITIES

Brian Cusack, Zhuang Tian
Cyber Forensic Research Centre, Auckland University of Technology, Auckland, New Zealand
brian.cusack@aut.ac.nz, zhuang_tain@hotmail.com

Abstract

Hacking of IP surveillance camera systems came to public attention in 2016 when the high bandwidth and resources were exploited for a massive DDoS attack that affected one third of all US Internet services. A review of previous studies show that a vast number of IP cameras have been hacked because the default usernames and passwords have not been changed from the factory defaults. In this research we asked, What are the vulnerabilities of an IP surveillance camera? The purpose of the study was to provide identification of vulnerabilities and guidance for the protection of surveillance camera systems. The research shows that the tested surveillance camera had many vulnerabilities and that there is urgency for distributing alerts and best practice guidelines.

Keywords: Hacking, CCTV vulnerability, Evaluation, Security

INTRODUCTION

Closed Circuit Television (CCTV) systems have proliferated in businesses and for private use. The surveillance systems are relatively inexpensive and provide multiple sensors that feed information back to a centralised processing station and monitoring screens. The application is for monitoring assets and human behaviour for risk management. The sensors provide different data types that include visual, audio, infrared, and other spectrum data. Monitoring may proceed by human observation, automation, archival mapping, or a combination of these. Many systems have software to assist human decision-making, and resource management systems to optimise the cost of surveillance against the benefits it may deliver. Research has shown that these CCTV surveillance systems have critical points of failure (Costin, 2016). In addition, Ozkan (2016) shows that over 100,000 wireless Internet Protocol (IP) cameras in the research sample had little or no information security protection. Others show that surveillance cameras from 79 vendors are vulnerable to Remote Code Execution (RCE) (Kirk, 2016; Costin, 2016). The security problem is increased by vendors are selling IP cameras using the “white labelling” business model with the same firmware developed by the same company across the product range and with unprotected RCE. The vulnerability allows an attacker to seize control of the camera for manipulation. Manipulation can have several features, such as, data seizure, mechanical manipulation, anti-forensic data planting, exploitation of the bandwidth resource, end-user deception, and zombie exploitation (McKee, et al., 2017). A significant weakness is that most IP cameras only log authenticated requests and have no traces on the camera of user activity or unique identification. Hence, an attacker can be anonymous while acquiring real-time video streams, archived footage; email, FTP, other credentials, and access to the system resource controls. The significant vulnerability grants an attacker invisibility and the ability to host malware; run arbitrary software such as botnets, proxies and scanners; and create backdoors for future access. Consequently, a CCTV system is generally available to unauthorised control, and the system itself, can sponsor attacks on other systems (Coole, et al., 2012; Cuputo, 2014; Costin, 2016). In this paper, we test an out-of-the box camera to identify security vulnerabilities.

BACKGROUND

On 21 October 2016, a massive DDoS attack against Dyn, a domain name system (DNS) provider, broke a large portion of the Internet, causing a significant outage to hundreds of websites and services (CCTV, 2017). Although, Dyn did not disclose the actual size of the attack, but it has been speculated that the DDoS attack could be much bigger than the one that hit French Internet service and hosting provider OVH that peaked at 1.1 Terabytes per second (TBps), which is the largest DDoS attack known to date (Smith, 2013). The attack was caused by a botnet that consisted of 100,000 devices infected by malware named Mirai. The Mirai malware targeted Internet of Things (IoT) devices such as IP cameras and digital video recorders (DVR) that have weak default passwords, making them easy to infect (Wu, et al., 2010; Zanella, 2014; Kirk, 2016). A similar study by Minin (2015) found that a malicious attacker took control of the cameras remotely and controlled movement, redirected the video feeds, and worked out the password for the wireless network the device was connected. The owners of the surveillance camera systems were not aware of the system compromise and the use for a massive attack. A similar study analysed Motorola’s Focus 73 (Minin, 2015) outdoor security camera. Images and video taken by the camera can be delivered to a mobile phone application. One attack showed how it is possible to scan for cameras connected to the Internet and then to get a reverse root shell to forge control credentials. Additionally, by tampering with DNS settings, the attacker can intercept the alerts that the camera sends to its owner, as well as to see video clips that would be sent to a cloud storage service. Further analysis showed that the firmware is a generic and used in other kinds of IP cameras. The code is not encrypted or digitally signed leaving open a backdoor for malware to be uploaded to the camera (Gotham Digital Science, 2012).

The argument for protection when the surveillance system is on a dedicated network without access to other client systems, is shown to be false (Tekeoglu et al., 2015). The experiment was performed on MicroDigital, HIVISION, CTRing and a substantial number of other rebranded devices. The result shows the tested surveillance systems transmit the user name and password in clear text over port 5920 transmission control protocol (TCP) during authentication stage. The experiment also used a Metasploit framework to perform brute-force and dictionary attacks on the tested devices. The sample showed that 70% of the instances utilised had the default vendor passwords that had not been changed.

The list of known CCTV vulnerabilities have been published in a database (CCTV Calculator, 2017). They list vulnerabilities existing in the vendors product range including Siemens, ZoneMinder, Zhuhai RaySharp, Samsung, Grandstream, WESPMonitor, WebGate, D-link, Panasonic, Cisco, Hikvision, FOSCAM, Y-Cam, TRENDnet, CIPCAMPTIWL, Dahua, TVT, AVTECH, Brickcom, TP-LINK, AirLive, Axis, Sony, QNAP, Arecont Vision, GeoVision, March Networks, Canon, FlexWATCH, Mobotix and Linksys. The vulnerability discovered in GeoVision DVR systems allows a remote attacker to execute arbitrary code by calling the GetAudioPlayingTime method with arguments. Tian (2014) shows more detailed vulnerabilities in GeoVision include directory traversal in geohttpserver and SanpShotToFile in GeoVision LiveX. Weak encryption schemes for passwords allows attackers to obtain the password via sniffing (Wu, et al., 2010). The sysinfo script in GeoHttpServer allows remote attackers to cause a DoS via a long password, and triggering a buffer overflow. When GeoHttpServer is configured to authenticate users, it allows attackers to bypass authentication and access unauthorised files via a URL that contains %0a%0a – code injection (Bruschi, et al., 2003; Bojinov, et al., 2009). These examples indicate the GeoHttpServer has several vulnerabilities that gives access for an attacker to perform unauthorised activities within the surveillance system. Nonetheless, these vulnerabilities were discovered in the period between 2004 and 2011 and no information is provided regarding whether or not these vulnerabilities have been fixed by the manufacturers since. Further research (Gotham Digital Science, 2012; Kyaw, et al., 2016) shows a remote file disclosure vulnerability in GeoHttpServer. The code has no authentication requirement and hence an attacker can exploit this vulnerability to retrieve and download stored files on the server such as ‘boot.ini’ and ‘win.ini’.

RESEARCH METHODOLOGY

The aim of this research was to answer the research question: What are the vulnerabilities of an IP surveillance camera? To answer the question, the research has six phases (Figure 1). These phases include literature review, system setup, pilot testing, data collection, data analysis and its comparison with results of previous research. Different research phases employ different research methods. The literature review section, for example, provided understanding for the work of different authors and their recommendations for future research. This phase constitutes the qualitative part of the study. The data collection, on the other hand, included a pilot study and experiment conducted by testing the camera by trying different exploits. The system setup phase set up the equipment for the field trials. These rational phases constitute the quantitative part of the study. The final phase compares the results obtained from both parts of the study in a mixed methods approach (Bryman, 2012).

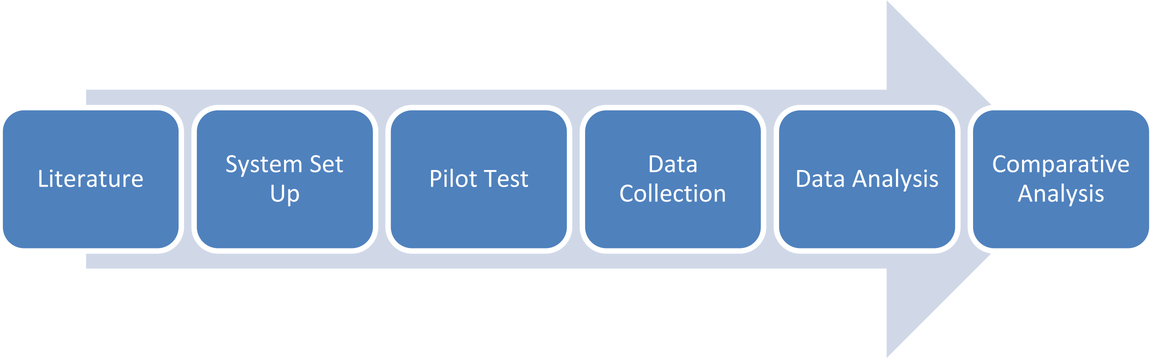


Figure 1. Research Phases

System Design

The following devices are used in the research, and the system design is in Figure 2:

- *Target IP surveillance camera (10.0.0.2): GeoVision GV-FD220D 2MP H.264 IR fixed IP Dome camera*
- *Network switch: Thomson TG585 v8 ADSL2+ wireless gateway*
- *Client (10.0.0.5): Lenovo laptop Thinkpad X200 Table with Intel Core 2 Duo CPU L9600 2.13GHz ×2, 242.9 GB HDD and Windows 7 32-bit*
- *Attack device 1(10.0.0.6): Lenovo laptop Thinkpad X200 Table with Intel Core 2 Duo CPU L9600 2.13GHz ×2, 242.9 GB HDD and Kali Linux Rolling 2016.2 32-bit*
- *Attack device 2 (10.0.0.3): Acer laptop Aspire V3-371-501P with Intel Core i5-4210U 1.7GHz, 4GB DDR3, 500 GB HDD and Windows 8.1 64-bit*

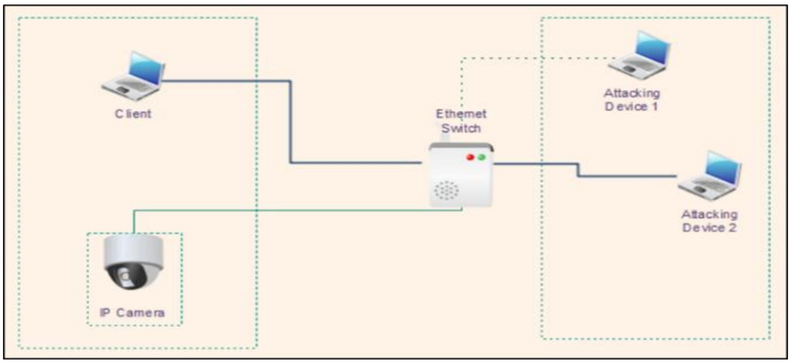
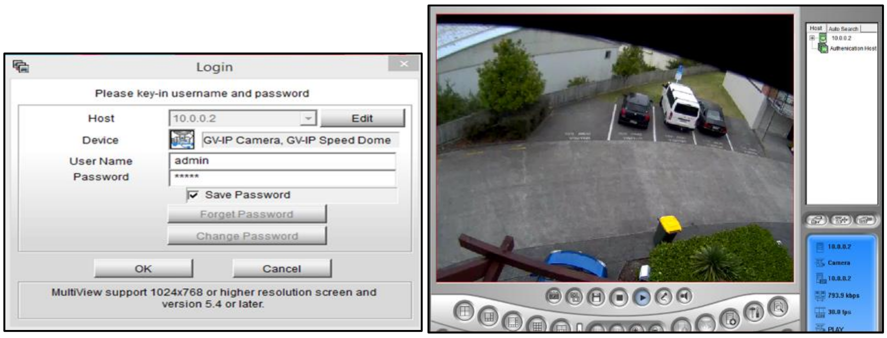


Figure 2. System Design

Pilot Test

After setting up the IP surveillance system network, a pilot run was made to configure and test the camera functionalities as well as network connections amongst all the devices. The user can connect to the IP camera either through *Windows Explorer* by entering its IP address in the URL field; or use GeoVision *DMMultiView* client software to connect the camera's DVR by selecting the host IP address and type of device. A User can use *GvIP Device Utility* to find the IP camera IP address. *GV IP Device Utility* is an application software to help the user to manage IP cameras, update their firmware, identify them by their IP addresses within a local area network (LAN) or backup and restore their settings (Figure 3).



Login

Please key-in username and password

Host: 10.0.0.2 [Edit]
Device: GV-IP Camera, GV-IP Speed Dome
User Name: admin
Password: *****
☑ Save Password

MultiView support 1024x768 or higher resolution screen and version 5.4 or later.

Figure 3. GeoVision DMMultiview User Authentication and GeoVision DMMultiview Live Capture

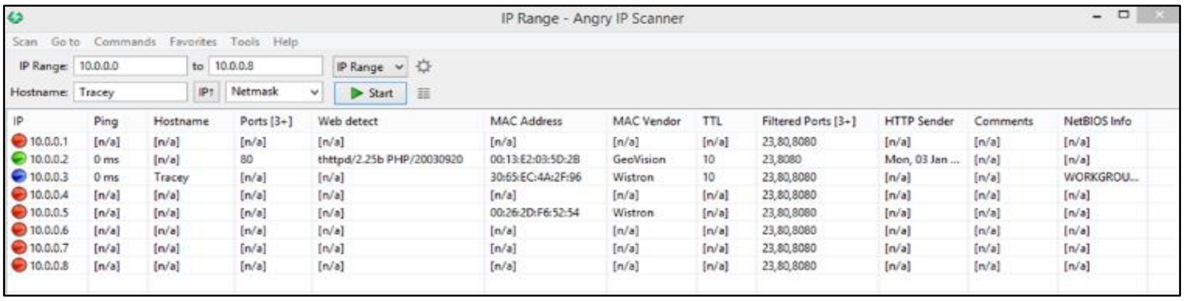
The attacking device ran *Kali Linux*, so we also needed to test whether it can connect to the IP camera in the pilot study, and to ensure a penetration test is possible using preinstalled tools from the attacking device.

Data Management

The tools *Angry IP Scanner, WireShark, ophcrack, Burpsuite and Cain & Abel*, were tested in the pilot study for performance and functionality. Each has their own built-in data processing ability as specified by the distinct features and functions of the tool. Others tested, such as *Nmap Hydra, Nikto and Metasploit,* are command-line based and are relevant for data collection from IP cameras. The collected data are automatically processed and analysed by these tools. The results can be saved to a file; analysis performed, and a report generated. Data collection was undertaken with website and IP camera DVR penetration testing tools and techniques. For result accuracy, the same tools are used 3 times and then the collected data compared to identify any variations. Data dump files are created for each penetration tool used, and the collected data analysed.

RESEARCH FINDINGS

Angry IP Scanner and Nmap were used to collect information about the target system, such as its IP address, media access control address (MAC), manufacturer and server information. The *Angry IP Scanner* is a fast lightweight cross-platform IP address and port scanner; used to scan IP addresses in any range. It includes information on any of the ports by simply pinging each IP address to check if it is alive, then optionally resolving its hostname, determining MAC addresses and the vendor (Figure 4).



IP Range: 10.0.0.0 to 10.0.0.8

Hostname: Tracey

Netmask

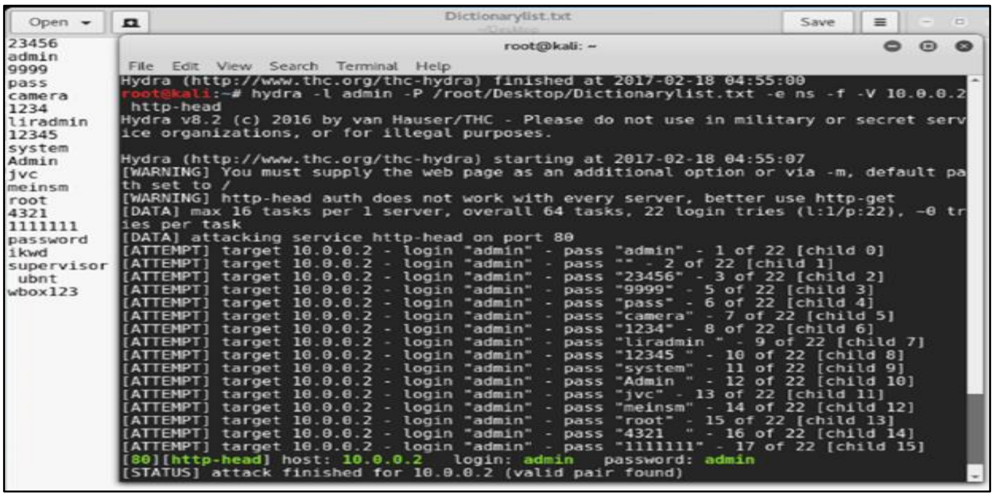
IP	Ping	Hostname	Ports [3+]	Web detect	MAC Address	MAC Vendor	TTL	Filtered Ports [3+]	HTTP Sender	Comments	NetBIOS Info
● 10.0.0.1	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	23,80,8080	[n/a]	[n/a]	[n/a]
● 10.0.0.2	0 ms	[n/a]	80	thttpd/2.25b PHP/20030920	00:13:E2:03:5D:2B	GeoVision	10	23,8080	Mon, 03 Jan ...	[n/a]	[n/a]
● 10.0.0.3	0 ms	Tracey	[n/a]	[n/a]	30:65:EC:4A:2F:96	Wistron	10	23,80,8080	[n/a]	[n/a]	WORKGROU...
● 10.0.0.4	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	23,80,8080	[n/a]	[n/a]	[n/a]
● 10.0.0.5	[n/a]	[n/a]	[n/a]	[n/a]	00:26:2D:F6:52:54	Wistron	[n/a]	23,80,8080	[n/a]	[n/a]	[n/a]
● 10.0.0.6	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	23,80,8080	[n/a]	[n/a]	[n/a]
● 10.0.0.7	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	23,80,8080	[n/a]	[n/a]	[n/a]
● 10.0.0.8	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	[n/a]	23,80,8080	[n/a]	[n/a]	[n/a]

Figure 4. Angry IP Scanner Network Scanning Result

The result shows that our target IP surveillance system's IP and MAC address, its manufacturer information as well as its active ports. Once, we obtain the target IP address, we used *Nmap* for further reconnaissance. Nmap is a free and open source utility for network discovery and security auditing. It uses raw IP packets to determine available hosts on the network, services offered, operating system (OS) they are running, type of pocket filters and firewalls in use as well as other user characteristics. From the Nmap scanning results, the target IP camera has TCP port 80, 111 and 10000 open. Hence, it is shown again that a user can login to the target IP surveillance system through Windows Explorer via port 80, and port 10000 is the virtual switch system (VSS) port for video streaming. Thus, to further the research IP packets were collected, and packet sniffing and spoofing performed to identify any vulnerabilities in the system. Packet sniffing and spoofing are methods that identify the weak points of network system, particularly on a layer 2 switched network. A LAN uses address resolution protocol (ARP) with holes enabling the attacker to sniff packets and lodge ARP spoofing attacks.

WireShark was put into monitoring and capturing mode to authenticate to the target surveillance system website application, in order to capture the user name and password either in clear text or in hash values. The captured packets were then analysed and by following the TCP packet streams, other matters for further investigation were discovered. Firstly, we were able to find the user name and password; and the two MD5 hash values. There were also two groups of 50 bits assigned to two variables, namely *gUserName* and *gPassword*. Finally, we saved both MD5 hash values to be decrypted. Similarly, *Cain & Abel* was used to recover passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force and cryptanalysis attacks, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analysing routing protocols. *Cain & Abel* sniffs the network for the target device, and then launches attacks. We used ARP poisoning to perform a man-in-the-middle (MITM) attack. During a MITM attack, the attacking device secretly intercepts, replays and potentially alters the communication between two parties who believe they are directly communicating with each other – in this case the camera and its control. The ARP poisoning feature caught the username and password when a client computer authenticated with the target IP surveillance system. There were 9,652 packets transmitted between the target IP surveillance system and its client were captured. The two MD5 hash values captured when logging into the target IP surveillance system from Windows Explorer browser, were sent to a hash value cracker – *ophcrack* to decrypt the hash values. *ophcrack* is a free open source program that cracks hash values, and Windows log-in passwords by using Lan Manager hash (LM) through a rainbow table. After entering both captured MD5 hash values into Wireshark, it returned the results as "*empty*". Thus, *WireShar*k did not capture any packets related to the user name and password in either clear text or hash values. Thus, we required the alternative software for hash value cracking and to gain the user name and password for the target IP surveillance system. Two cracking techniques were used, namely: brute-force and dictionary.

To identify the range of vulnerabilities a IP camera may have we used many cracking tools including Hydra. It is also called THC-Hydra, and is a command-line-based network logon cracker that can use a dictionary attack to decrypt passwords from many protocols and applications. Before using Hydra to run a dictionary attack on the target IP surveillance system, we needed to generate a word list. Based on the previous research reviewed, we formed a dictionary of possible default passwords, including *admin* as a common user name. Previous studies show that *GeoHttpServer* have several vulnerabilities; and HTTP header contains much useful information. Thus, we used these clues to run *Hydra* with the *http-head* command (Figure 5).



```
23456
admin
9999
pass
camera
1234
liradmin
12345
system
Admin
jvc
meinsm
root
4321
1111111
password
ikwd
supervisor
 ubnt
wbox123
```

```
Hydra (http://www.thc.org/thc-hydra) finished at 2017-02-18 04:55:00
root@kali:~# hydra -l admin -P /root/Desktop/Dictionarylist.txt -e ns -f -V 10.0.0.2
 http-head
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret serv
ice organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-02-18 04:55:07
[WARNING] You must supply the web page as an additional option or via -m, default pa
th set to /
[WARNING] http-head auth does not work with every server, better use http-get
[DATA] max 16 tasks per 1 server, overall 64 tasks, 22 login tries (l:1/p:22), ~0 tr
ies per task
[DATA] attacking service http-head on port 80
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "admin" - 1 of 22 [child 0]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "" - 2 of 22 [child 1]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "23456" - 3 of 22 [child 2]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "9999" - 5 of 22 [child 3]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "pass" - 6 of 22 [child 4]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "camera" - 7 of 22 [child 5]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "1234" - 8 of 22 [child 6]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "liradmin " - 9 of 22 [child 7]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "12345 " - 10 of 22 [child 8]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "system" - 11 of 22 [child 9]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "Admin " - 12 of 22 [child 10]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "jvc" - 13 of 22 [child 11]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "meinsm" - 14 of 22 [child 12]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "root" - 15 of 22 [child 13]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "4321  " - 16 of 22 [child 14]
[ATTEMPT] target 10.0.0.2 - login "admin" - pass "1111111" - 17 of 22 [child 15]
[80][http-head] host: 10.0.0.2   login: admin   password: admin
[STATUS] attack finished for 10.0.0.2 (valid pair found)
```

Figure 5. Hydra Http-Head Dictionary Attack Result

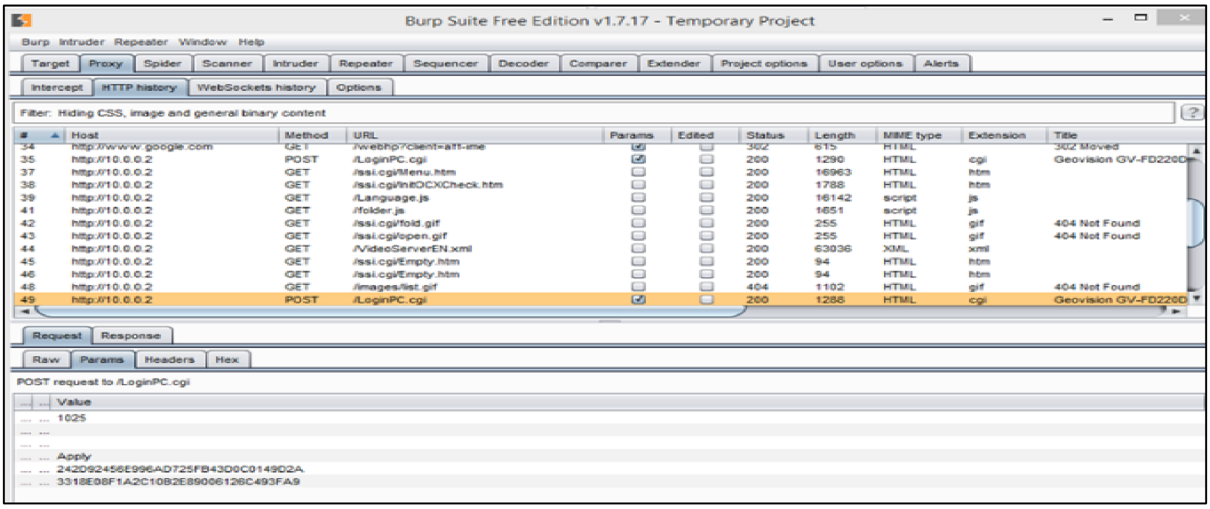
The results showed, 17 tries on 22 possible passwords; and one pair valid user name and password found. To confirm the result, we used the identified user name and password to login on the target surveillance system through Windows Explorer. The result confirmed they were correct. *Hydra* with *http-get* command was run to compare the results.

DVR is the heart of IP surveillance system network and has a weak default password. Therefore, we evaluated how well the target IP surveillance system can resist such an attack. *Metasploit* was chosen for the task of developing and executing exploit code against the remote target machine. The results showed the attacking computer was not able to establish connection with 10.0.0.2 on port 5920 - the port used by most IP surveillance systems. We also tried the ports 4550, 5550, 6550 and 10000, which are the system's data port, audio port and VSS port. Metasploit did not provide the option for a user to specify which port to exploit so we tried other tools. Nikto was used to perform web server scanning on the target IP surveillance system. *Nikto* is an open source web server vulnerability scanner, which performs comprehensive tests against web items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1,250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. The following vulnerabilities were identified:

- *The anti-clickjacking X-Frame-Options header is not present*
- *GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS*
- *GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type*
- *OSVDB-2119: GET/shopexd.asp?catakigud='42:VP-ASP Shopping Cart 5.0 contains multiple SQL injection vulnerabilities. CVE-2003-0560, BID-8159*
- *OSVDB-3092: GET /htpasswd: This might be interesting...*
- *OSVDB-3268: GET /tmp/: Directory indexing found.*
- *OSVDB-3092: GET /tmp/: This might be interesting...*
- *OSVDB-3268: GET /images/: Directory indexing found*
- *OSVDB-3268:GET /images/?pattern=/etc/*&sort=name: Directory indexing found*

Another tool used was the *Burp* suite, which is a Java based software platform of tools for performing security testing of web application. The suite of products combines automated and manual testing techniques and consists of a number of different tools, such as a proxy server, web spider, scanner, intruder, repeater, sequencer, decoder, collaborator, extender, and to brute force a login page. After installing the attacking device with *Burp*, Internet

Explorer is then configured to work with *Burp*. It can operate as MITM between the web browser and the target IP surveillance system web server, and it intercepts the traffic exchanged between the browser and the server. *Internet Explorer* (*IE*) was used to connect to the server and enter the correct user name and password. The interception and capture of the POST request gave the username and password that is supplied to the server. This can occasionally be a GET request also. The result shows that both the username and password are MD5 hash values (Figure 6).


Burp Suite Free Edition v1.7.17 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request Response
Raw Params Headers Hex

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
34	http://www.google.com	GET	/webhp?client=aff-ime	☑	□	302	615	HTML		302 Moved
35	http://10.0.0.2	POST	/LoginPC.cgi	☑	□	200	1290	HTML	cgi	Geovision GV-FD220D
37	http://10.0.0.2	GET	/ssi.cgi/Menu.htm	□	□	200	16963	HTML	htm	
38	http://10.0.0.2	GET	/ssi.cgi/InitOCXCheck.htm	□	□	200	1788	HTML	htm	
39	http://10.0.0.2	GET	/Language.js	□	□	200	16142	script	js	
41	http://10.0.0.2	GET	/folder.js	□	□	200	1651	script	js	
42	http://10.0.0.2	GET	/ssi.cgi/fold.gif	□	□	200	255	HTML	gif	404 Not Found
43	http://10.0.0.2	GET	/ssi.cgi/open.gif	□	□	200	255	HTML	gif	404 Not Found
44	http://10.0.0.2	GET	/VideoServerEN.xml	□	□	200	63036	XML	xml	
45	http://10.0.0.2	GET	/ssi.cgi/Empty.htm	□	□	200	94	HTML	htm	
46	http://10.0.0.2	GET	/ssi.cgi/Empty.htm	□	□	200	94	HTML	htm	
48	http://10.0.0.2	GET	/images/list.gif	□	□	404	1102	HTML	gif	404 Not Found
49	http://10.0.0.2	POST	/LoginPC.cgi	☑	□	200	1288	HTML	cgi	Geovision GV-FD220D

POST request to /LoginPC.cgi

...	...	Value
...	...	1025
...	...	
...	...	
...	...	Apply
...	...	242D92456E996AD725FB43D0C0149D2A
...	...	3318E08F1A2C10B2E89006126C493FA9

Figure 6. Burp Network Packet Capture Result

We then used *Intruder* and *Sniper* to perform dictionary attacks on the MD5 hash values captured. Instead of trying to decrypt the captured hash values, *Intruder* and *Sniper* allows the attacker to perform a dictionary attack precisely on the captured MD5 hash value fields. The dictionary attack is performed, and a valid user name and password will be shown. Based on the word list used for the attack, there are 27 words used, 54 requests tried and responses in total. Table 1 summarises the vulnerabilities identified in the research and the software used.

Table 1 Summary of vulnerabilities

Software	Functionality	Attack
Pilot Study		
Windows Explorer	Get Camera IP address	Vector
GeoVision DMMultiView	Connect the camera's DVR	Vector
GvIP Device Utility	Manages IP camera, firmware updates, IP addresses within a local area network (LAN), backup records and restore settings	Vector
Main Study		
Angry IP Scanner	Collects IP address, media access control address (MAC), manufacturer and server information	Reconnaissance
WireShark	Collects IP address, media access control address (MAC), manufacturer and server information; packet capture	Reconnaissance
ophcrack	Hash value cracker	Analysis
Burpsuite	Performs security testing of web applications	Reconnaissance
Cain & Abel	Recovers passwords, cracks encrypted passwords using dictionary, brute-force and cryptanalysis attacks, recovers wireless network keys, passwords and routing protocols	Analysis
Nmap	Collects IP address, media access control address (MAC), manufacturer and server information, and system characteristics	Reconnaissance
Hydra (THC-Hydra)	A network logon cracker that can use a dictionary attack to decrypt passwords for many protocols and applications	Analysis
Nikto	Web server scanning for the target IP surveillance system	Reconnaissance
Metasploit	Develops and executes exploit code against a remote camera	Active agency

CONCLUSION

In this research, we tested an out of the box GeoVision GV-FD220D 2MP H.264 IR fixed IP Dome camera for security vulnerabilities. Although the code injection and directory traverse exploitation techniques were rebuffed, many other points of vulnerability were identified. The two points of entry to the camera system were openly accessible through Windows Explorer or the GeoVision DMMultiView client. The password to the system was easily cracked (the factory default) and the GvIP Device Utility entry gained to control the IP camera. A fuller exploration of the whole surveillance system demonstrated the scope of a number of tools and the ability to gain control of critical information. Countermeasures are required to protect the IP camera from hacking and exploitation of the communication resources. Strong advice is to change the access password from the default, and then to change the password regularly. Detection of surveillance activity is required on a moment-by-moment basis and layers of protection are required to satisfy an attacker but also to maintain system integrity. Similarly, critical information requires encryption, protection by tunnelling, and cryptographic complexity to confuse analysis. The defeat of active agency can come by change management controls, benchmark auditing on a moment-by-moment basis, and the regular updating of IP Camera anti-virus software. Our research suggests that IP cameras are vulnerable to exploitation and we advocate for a greater urgency in distributing countermeasures.

REFERENCES

Bojinov, H., Bursztein, E. & Boneh, D. (2009). XCS:Cross channel scripting and its impact on web applications. The 16 ACM Conference on Computer and Communication Security (pp. 420-431). Chicago, IL, USA.

Bruschi, D., Ornaghi, A. & Rosti, E. (2003). S-ARP: a secure address resolution protocol . The 19th IEEE Annual Computer Security Applications Conference (pp. 66-74).

Bryman, A. (2012). Social research methods. Oxford: Oxford University Press.

Caputo, A. (2014). Digital video surveillance and Security second edition. London: Elsevier.

CCTV Calculator. (2017). Vulnerability database. Retrieved from CCTV Calculator: https://www.cctvcalculator.net/en/knowledges/vulnerability-database/

Coole, M., Woodward, A. & Valli, C. (2012). Understanding the vulnerabilities in Wi-Fi and the impact on its use in CCTV systems. The 5th Australian Security and Intelligence Conference (pp. 36-43). Perth, WA, Austrailia : Edith Cowan University.

Costin, A. (2016). Security of CCTV and video surveillance systems; Threats, vulnerabilities, attacks, and mitigations. The 6th International Workshop on Trustworthy Embedded Devices (pp. 45-54). Vienna, Austria: ACM.

Gotham Digital Science. (2012). Using metasploit to access standalone CCTV video surveillance systems. Retrieved from Gotham Digital Science: https://blog.gdssecurity.com/labs/2012/5/15/using-metasploit-to-access-standalone-cctv-video-surveillanc.html

Kirk, J. (2016). Security camera riddled with flaws that let attackers hack your video and your network. Retrieved from PC World: https://www.pcworld.com/article/3030014/security/study-of-another-ip-camera-reveals-serious-problems.html

Kyaw, A., Tian, Z. & Cusack, B. (2016). Wi-Pi: a study of WLAN security in Auckland City. International Journal of Computer Science and Network Security, 16(8) 68-80.

McKee, D., Clement, S., Almutairi, J. & Xu, J. (2017). Massive-scale automation in cyber-physical systems: Vision & challenges. IEEE 13th International Symposium on Autonomous Decentralized System (pp. 5-11). Bangkok, Thailand.

Minin, V. (2015, June 10). GeoVision (GeoHttpServer) webcams - Remote file disclosure. Retrieved from Exploit Database: https://www.exploit-db.com/exploits/37258/

Őzkan, S. (2016). Geovision: Security vulnerabilities. Retrieved from CVE Details: https://www.cvedetails.com/vulnerability-list/vendor_id-2385/Geovision.html

Smith. (2013). Hacks to turn your wireless IP surveillance cameras against you. Retrieved from CSO Online: http://www.networkworld.com/article/2224469/microsoft-subnet/hacks-to-turn-your-wireless-ip-surveillance-cameras-against-you.html

Tekeoğlu, A. & Tosun, A. (2015). Investigating security and privacy of a Cloud-based wireless IP camera: NetCam. The 24th IEEE International Conference on Computer Communication and Networks (pp. 1-6), Las Vegas, NV, USA.

Tian, Z. (2014). Digital forensics in the cloud: Encrypted data evidence tracking. Auckland, New Zealand: Auckland University of Technology.

Wu, H., Ding, Y., Winter, C. & Yao, L. (2010). Network security for virtual machine in cloud computing. In Proceedings of The 5th IEEE International Conference on Computer Science and Convergence Information Technology (pp. 18-21).

Zanella, A., Bui, N., Castellani, A., Vangelista, L. & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things, (1), 22-23.