International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 04, April 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

RECENT STUDY OF CLOSE CIRCUIT TELEVISION (CCTV) IN HACKING

Mohammed Farook Bin Rafiuddin[1], Prethpal Singh Dhubb[2], Hamza Minhas[3]

[123]*Student, Bachelor of Forensics Computing & Security, Asia Pacific University (Malaysia)*

ABSTRACT

This paper comprises of research done on various aspects of CCTV Hacking. A research was conducted to study the history of CCTV, the fields in which CCTV is commonly used in e.g. crime prevention etc. This research is focused more on How to hack a CCTV step by step and how easy it is. Also this paper shows and outlines the hardware and software needed to hack this technology and the main components being used in this hacking. The process that takes place in hacking CCTV is explained in this article. The advantage and differences between public IP and private IP is explained. The models and types of camera often used and preferred has also been analyzed and diagnosed in this paper.

Keywords: Close Circuit Television, IP Scanner, Crime Prevention, Hacking

I. 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 [1]. CCTV technology has been growing rapidly 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. Also, CCTV technology has helped the police departments in many cases to identify criminals who were caught on camera. For instance, in 2014, group of armed robbers were caught on CCTV camera while putting on their disguise [2]. Massive cyber-attack on Russian bank allows hackers to access 24,000 CCTV and home video cameras in 30 different countries including the U.S [3]. According to the daily mirror of UK, the attackers saw as many as 660,000 request being sent every second using a network of more than 24,000 hijacked devices which also allowed these hackers to gain access office CCTV's as well as home digital cameras. An attack of such high scale left the banks losing more than USD31 million in the attack. Cyber-attacks and hacking has become so widespread that critical attacks happen so frequently. Despite all that, how easy is it to hack CCTV Cameras? While there is no clear documented evidence to claim the first CCTV hacking done historically; research has shown recently based on real time incidents that, popular surveillance camera is open to hackers [4]. While the CCTV cameras in Washington DC were hacked just few days before Donald Trump's inauguration which left the 123 out of the 187 cameras crippling in the network due to a cyber-attack and with other similar attacks globally [5]. It is made to look that having CCTV's may not be as safe as it used to be once

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

upon a time. With that in mind, this research investigates the question as to "How easy is it to actually hack intoa CCTV system and if so how to do it?." With that as the primary objective of the research, the document provides the results in a step by step approach.

II. PHYSICAL SECURITY

What is physical security? Physical security refers to any kind of security measures designed to prevent unauthorized access to facilities, equipment, and resources and to protect personnel or industrial property from external or internal breach, terrorism and any kind of disasters. Physical security has three major layers: access control, surveillance and testing. Access control refers to the amount of allowed activity of legitimate users towards the amount of privilege the user is given to access resources in a system [6]. Physical security brings about many importance especially in Crime Prevention through Environmental Design (CPTED) [7]. According to the physical security report, Close-circuit television or surveillance systems utilize camera in areas where surveillance is needed 24 hours which are known as high-risk areas [8].

III. IP ADDRESS

We hear the term or expression "IP address" more and more on television, news and movies. That's right, Your PC has an IP address, your smartphone has an IP address, even a coke machine will have an IP address. But what exactly is an IP Address?IP address or in its full form "Internet Protocol Address" is a unique identifying number assigned to every single device that's connected to the internet. Just like a car license plate, or your street address, an IP address is a special, globally unique serial number used for identification [9].

3.1 There are 2 Types of IP Addresses, Private IP and Public IP

A public IP address is an IP address that can be accessed over the internet. Just like the way postal addresses are used to deliver a postal mail to your home, a public IP address is a globally unique IP address assigned to a unique computing device. In layman terms, a public IP address is an address that is assigned to a computing device in order to allow direct access over the internet. An email server, web server or any server device that is directly accessible from the internet are candidate for a public IP Address.Private IP addresses on the other hand is used to assign computers or network devices an identification that will not directly expose them to the internet. For example, if you have multiple devices on your own network, you may want to use the private IP address to address each device within your network. In such a scenario, your router gets the public IP address, and each of the devices that are connected to your router (either via Wi-Fi or wired) gets a private IP address from your router using the DHCP (Dynamic Host Control Protocol). In a layman example, a network printer that is residing in your home or office is assigned a private address so that only devices within your network can communicate and print to your local printer (IP Location). The Internet Assigned Numbers Authority (IANA) is the sole organization responsible for registering IP address ranges to organizations and ISPs (Internet Service Providers). In order to allow organizations to freely assign private IP addresses, the Network Information Centre (InterNIC) has specially reserved certain IP address blocks for private use. The following is an example of IP address blocks reserved for private IP addresses.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Class	Starting IP Address	Ending IP Address	Number of Hosts
A	10.0.0.0	10.255.255.255	16,777,216
B	172.16.0.0	172.31.255.255	1,048,576
C	192.168.0.0	192.168.255.255	65,536

3.2 Angry Ip Scanner

Angry IP Scanner is a network scanner that has been designed to be fast and simple to use. It scans IP addresses and ports and is cross-platform and Open Source.Angry IP scanner simply pings each IP address to check if it's alive, then optionally it is resolving its hostname, determines the MAC address, scans ports, etc. The amount of gathered data about each host can be extended with plugins. With help of plugins, Angry IP Scanner can gather any information about scanned IPs. Anybody who can write Java code is able to write plugins and extend functionality of Angry IP Scanner. In order to increase scanning speed, it uses multithreaded approach: a separate scanning thread is created for each scanned IP address shown in "Fig.1".

3.3 Features of Angry IP Scanner

- Scans local networks as well as Internet
- IP Range, Random or file in any format
- Exports results into many formats
- Extensible with many data fetchers
- Provides command-line interface
- Free and open-source
- Works on Windows, Mac and Linux

It also has additional features, like NetBIOS information (computer name, workgroup name, and currently logged in Windows user), favorite IP address ranges, web server detection, customizable openers, etc.

3.4 Hacking Steps

3.4.1 ANGRY IP

Figure.1 Angry IP Scanner

The screen of the software where user should set preferences for the timing and port selection of the IP is shown below "Fig.2".

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

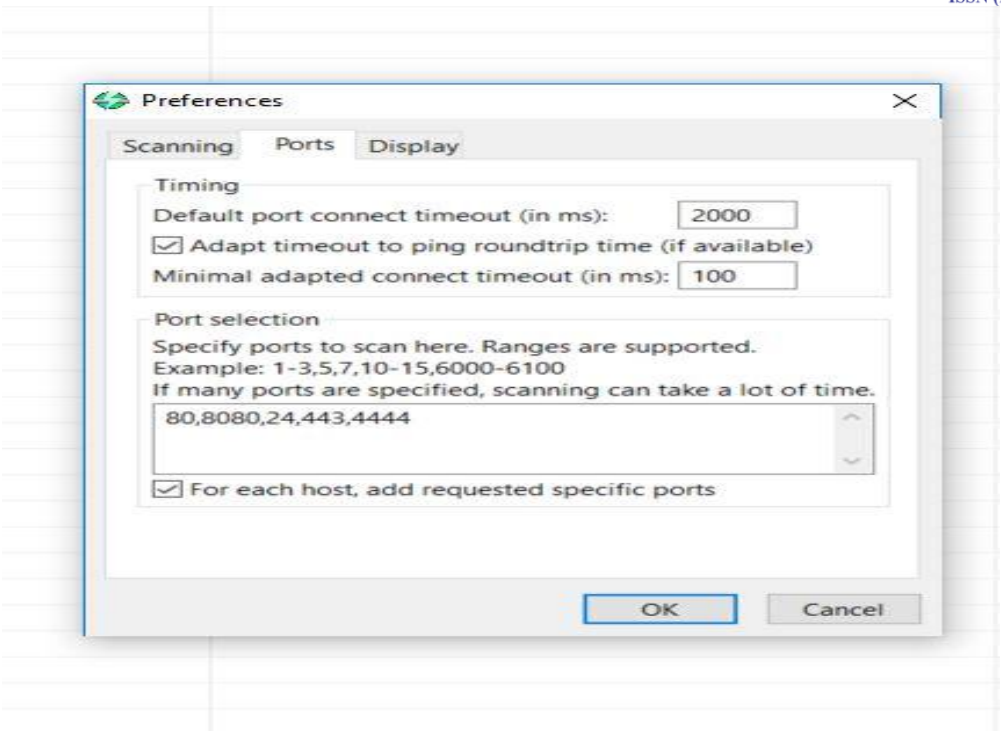

Figure.2 IP preferences

Before proceeding to scan the network IP range, be sure to manually key in the ports interested. The ports scanned were 80,8080,24,443, and 4444.

3.4.2 Fetchers

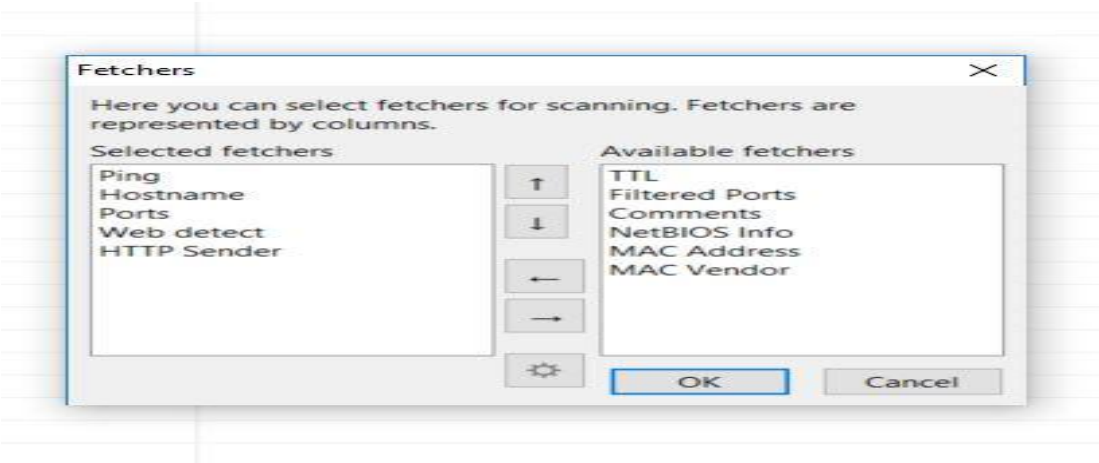

Figure.3 Fetchers

Make sure to select Ports, Web Detect and HTTP Sender. The above “Fig.3” shown the fetchers for scanning IP.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 04, April 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

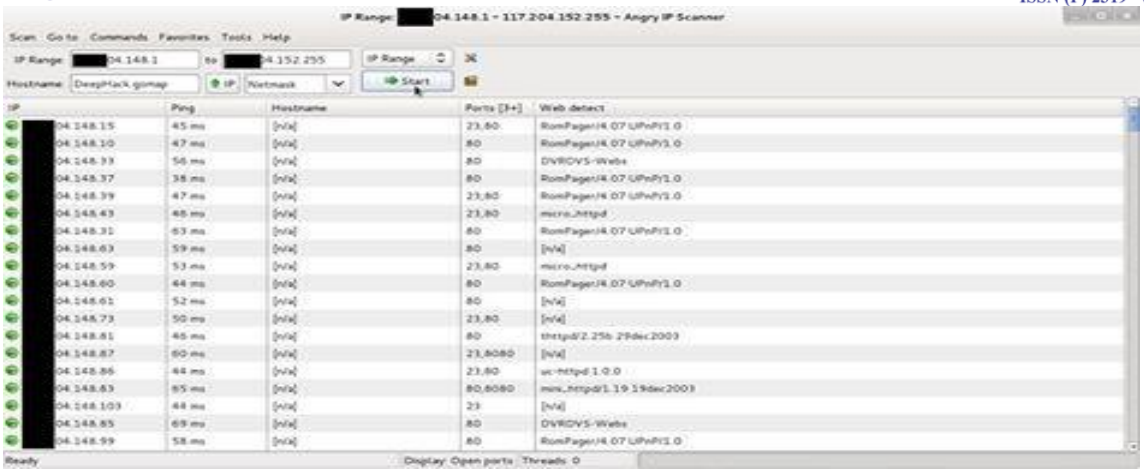

Figure.4 Angry IP Scanner

The above "Fig.4" shown the list of active IP address and following is the list of available active IP addresses that are available between the selected Target IP. The one with https and web detect are those with active CCTV connection. The most common username and passwords identified during the research are as follows:

Username: "admin' Password: "admin'

Username: "" Password: "12345

Username: "admin Password: "12345"

Username: "admin" Password: "9999"

Username: "admin123" Password: ""

Username: "admin" Password: "password"

Username: "user" Password: "123456789"

Username: "user" Password: "user"

Username: "user" Password: "user12345"

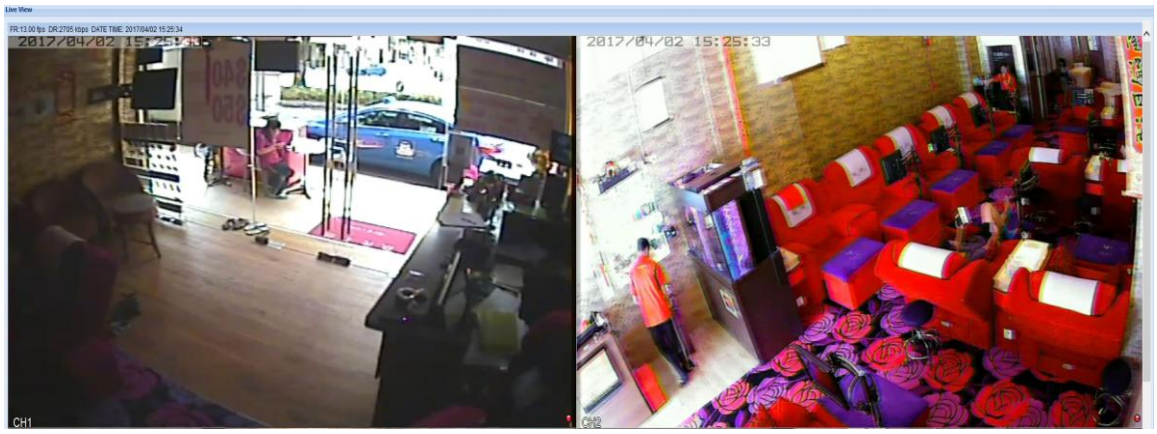

Figure.5 Output Images

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 04, April 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Figure.6 Output Images

Figure. 7 Output Image

The above "Fig.5, Fig.6, Fig.7 and Fig.8" was taken from 4 active CCTV cameras belonging to a massage parlor. When access has been granted, the above are some few settings which allows you to Play and pause capture moments, save videos, capture images, turn on their Mic and to hear their surroundings. The mic icon refers to turning on user microphone to connect with victim. Therefore, when this is activated, user may establish a open mic connection with the victim. The pic below shows the option for Mic and Speaker.

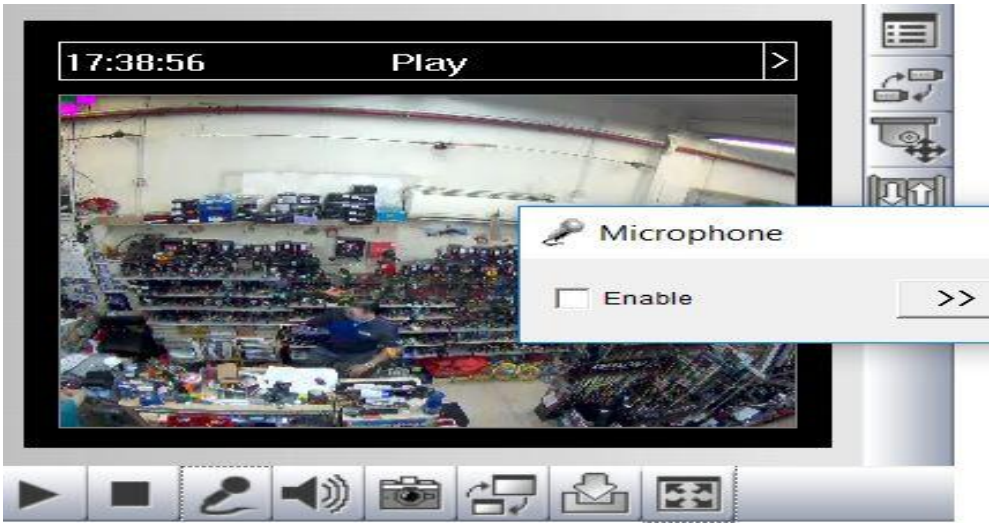

Figure.8 Output Images

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 04, April 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

VI. CCTV CAMERA AND SPECIFICATIONS

Closed Circuit Television (CCTV) is a system where the circuit in which the video is transmitted is closed and all the elements (camera, display monitors, recording devices) are directly connected. (Brickhouse Security). Any camera that is able to broadcast signals can be attached to a CCTV system, whether wired or wireless. Before the advances to wireless CCTV, every system had used wires to send and receive images from the CCTV system. A wired CCTV, used a high-quality wire between the camera and the monitor or recording equipment. Some of the benefits of wired CCTV include exceptional picture quality, high quality cabling type such as Cat5 which allows the camera image to be seen or recorded without any interference and also that the system is almost impossible to Jam with frequency blockers [10].Whereas on the other hand, Wireless CCTV is used to send images through analogue signals. The latest technology in wireless CCTC systems include high-speed, highly-encrypted and a very secure data transfer to get images from the camera to the receiving unit. Some of its benefits include that their cameras can send images through wi-fi signal, but can also utilize 3G or 4G and even satellite signals to send data which results in them being used anywhere and even the most remote site or area can be protected. The latest technology utilizing wireless IP camera CCTV system ensure an exceptionally high quality picture with less chances of interference from car alarms, baby monitors or microwave ovens. IP camera systems will also allow for a multitude of cameras on a single system without the fear of any interference.In this article, we will be featuring two big brands of CCTVs—Panasonic and Geovision, however, there are much more other brands offering similar models and functions as well. Both of these brands have a wide range of products that specializes on different purposes. Some of the types/models of CCTV cameras offered by these brands are explained as follows:

4.1DOME CCTV CAMERA

Dome CCTV cameras are most commonly used for indoor security and surveillance applications. These cameras

get their name after the shape of their housing. These housing are designed to make the CCTV cameras unobtrusive, i.e. not covert or hidden [11]. The dome shape of the camera makes it difficult to tell whatdirection these cameras are facing, thus are ideal for deterring criminals. Some units that allow the CCTV camera to pan/tilt/zoom and spin quickly within the housing are often referred to as speed domes, which gives the operator the ability to move the camera.

4.2 BULLET CCTV CAMERA

Bullet CCTV Cameras have a long, cylindrical and tapered shape, which is similar to that of a rifle bullet, often used in applications that require long distance viewing. This camera is not typically designed to have pan/tilt/zoom control, but instead it can capture images from a fixed location, pointing at a particular area. A bullet CCTV camera will be wall mounted or ceiling mounted that is typically designed for indoor use, although it can also be used for some outdoor applications. Many bullet cameras can also be waterproof by being installed inside protective casings, which will protect against dust, dirt, rain and other environment harmful elements.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 04, April 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

4.3 DISCREET CCTV CAMERA

Discreet CCTVs are cameras in disguise in such a way that they could look like a fan, freshener, smoke alarm or any other thing that would not seem suspicious in the area [12].

4.4 DAY/NIGHT CCTV CAMERA

The Day/Night CCTV camera has a very distinctive advantage of being able to operate in both normal and poorly-lit environments. These cameras do not have infrared illuminators because they can capture clean and clear video images in varying light conditions and in dark. This type of camera is ideal for outdoor surveillance applications where the infrared CCTV cannot function optimally. These CCTVs can have a wide dynamic range to function in glare, direct sunlight, reflections and strong back light 24/7 [11].

4.4.1 INFRARED/NIGHT VISION CCTV CAMERA

These types of CCTV cameras have the ability to see images in pitch black conditions using infrared LEDs surrounding its Lens and are ideal in outside conditions where lighting is poor to zero. They are basically designed for evening lookouts [12]

4.4.2 NETWORK/IP CCTV CAMERA

These types of cameras come in both hardwired and wireless that transmit images over the internet, often compressing the bandwidth so that it doesn't overwhelm the web. IP cameras are much easier to install than analogue cameras because they do not require a separate cable run or power boost to be able to send images over a longer distance [11].

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

4.4.3 WIRELESS CCTV CAMERA

One thing to keep in mind: Not all wireless cameras are IP-based. Some wireless cameras use alternative modes of wireless transmission. But, no matter what the transmission method, the primary benefit of these cameras is still the same, and that is flexibility in installation. These cameras also may or may not be connected to the internet. They use signaling devices to transmit images from camera to viewing area [12].

4.4.4 HIGH-DEFINITION CCTV CAMERA

High Definition cameras are often relegated to niche markets such as the casinos. These allow the operator to be able to zoom in with extreme clarity, especially to look at poker players, for example, who might have something up their sleeve. In the past days, these cameras were tube-based analog cameras, but today's era of digital technology has displaced those older units. These cameras can also transmit their images using HDcctv [13]

4.4.5 PTZ/SPEED DOMES CCTV CAMERA

PTZ (Pan/Tilt/Zoom) cameras give the surveillance in charge operator the ability to move the camera left or right (pan), up and down (tilt), and zoom the lens closer or farther. These are all relegated to surveillance situations where there is an on the spot live guard or surveillance specialist monitoring the images. However, there are cameras that have automated PTZ functionality where the camera is moving on a times basis. These cameras are many times used to cover a wide area with only one camera, or to avoid poor light conditions, such as a setting sun [13].

V. CONCLUSION

Based on the research it can be concluded that CCTV Hacking or Penetration is indeed mind boggling yet simple to achieve. Hacking has played a major role in the growth of the Information Technology positively and negatively which has open about many good and bad in the industry.While CCTV is always a good option to have when it comes down to security. Sometimes even CCTV which is meant to be the source of confidence to the public eyes may at times fall prey to those who seek vision for negative purposes. This documentation highlights the fact that it is rather easy to hack into a CCTV system for the simple fact that it wasn't kept in a secure environment and the username and passwords were not changed from its default passwords. In a nutshell, all CCTV providers and major company distributors should come up with a solution to solve the very simple issue with hand. This can be solved by deploying a simple hotfix whereby it requires every CCTV owners to update their system username and passwords which would make it hard and tougher for hackers to penetrate the system. Hacking into a CCTV should be not taken lightly for it might just lead the attacker into something very valuable. Most crime can be prevented with the likes of having cameras around, but when cameras can now be

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

accessed by those who wish to commit crimes, it makes it a lot easier to plan a blind spot to carry out a successful criminal activity. Greater awareness should be brought to light to all CCTV distributors and users about the importance of having strong username and passwords and how easy it is to hack into a CCTV if such default usernames and passwords are not changed.

VI. ACKNOWLEDGMENT

The authors would like to share gratitude to Mr Umapathy Eaganathan, Lecturer in Computing, Asia Pacific University, Malaysia also Miss Angel Aron for her constant support and motivation helped us to participate in this International Conference and also for journal publication.

VII. REFERENCES

[1] PCR-UK's PC & Tech Industry , 2014. The history of CCTV. [Online]
Available at: http://www.pcr-online.biz/news/read/the-history-of-cctv-from-1942-to-present/034658
[Accessed 30 3 2017].

[2] Sunday Express , 2014. Armed robbers caught on CCTV putting on their disguises. [Online]
Available at: http://www.express.co.uk/news/uk/529050/Armed-robbers-CCTV
[Accessed 25 3 2017].

[3] Davies, G., 2016. Cyber attack on Russian banks. [Online]
Available at: http://www.dailymail.co.uk/news/article-3926598/Massive-cyber-attack-Russian-banks-allows-hackers-access-24-000-CCTV-home-video-cameras-30-different-countries-including-U-S.html
[Accessed 29 3 2017].

[4] Wired, 2012. Popular Surveillance Cameras Open to Hackers, Researcher Says. [Online]
Available at: https://www.wired.com/2012/05/cctv-hack/
[Accessed 26 12 2016].

[5] Holmes, S., 2017. CCTV cameras in Washington DC were hacked just days before Donald Trump's inauguration. [Online]
Available at: http://www.dailymail.co.uk/news/article-4191080/British-man-woman-arrested-CCTV-Washington-DC-hacked.html
[Accessed 28 2 2017].

[6] Vincent C. Hu, D. F. F. D. R. K., 2006. Access Control System. Maryland, National Institute of Standards and Technology , pp. 12-15.

[7] Queensland Government , 2007. Crime Prevention Through Environmental Design (CPTED). [Online]
Available at: https://www.police.qld.gov.au/programs/cscp/safetyPublic/Documents/CPTEDPartA.pdf
[Accessed 30 3 2017].

[8] Hutter, D., 2016. Physical Security and Why It Is Important, Sultan Link : SANS Institute .

[9] Gil, P., 2016. IP Address Explained. [Online]
Available at: https://www.lifewire.com/how-ip-addresses-work-on-the-web-2483446

[10] DCUKADMIN, 2016. CCTV Systems Explained. [Online]
Available at: http://www.dcukltd.co.uk/blog/cctv-systems-explained/

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[11] Wilson, J., 2015. CCTV Cameras. [Online]
Available at: http://www.sonitrolwesterncanada.com/blog/what-type-of-cctv-camera-should-i-buy

[12] cosmotechph, 2014. 10 Different Types of CCTV Cameras and Their Purposes. [Online]
Available at: https://cosmotechph.wordpress.com/2014/09/08/10-different-types-of-cctv-cameras-and-their-purposes/

[13] Knott, J., 2011. 12 Common Types of Security Cameras. [Online]
Available at: http://www.cepro.com/article/12_common_types_of_security_cameras