International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 12 | Dec 2019 www.irjet.net p-ISSN: 2395-0072

Securing IP Surveillance Cameras using Adaptive Security Appliance (ASA)

Hamed Sadiqzada[1], Prabhat Kumar Panda[2], Yaser Mowlawizadah[3], Bilal Ahmad Ayobi[4]

[1,3,4]Post Graduate Scholar, REVA University, Karnataka, India
[2]Asst. Professor, REVA University, Karnataka, India

Abstract - *IoT is growing rapid and it may cause that other technologies may look insignificant. IoT promises to connect everything from CCTV cameras, medical devices, smart home products to smart enabled vehicles and many more devices and the security in IoT devices is quite important, in this paper we are going to configure the IP security camera using the In Vehicle Monitoring System (IVMS) software. And also simulate the way to make the video transmission of security cameras out of hackers and sabotages hands, so for fulfill this goal we have been used Adaptive security appliance (ASA) in the GNS3 Network simulator. By which we can assign some roles inside our simulated network that only the authorized users can access to the data of security cameras.*

Key Words: in vehicle monitoring system, adaptive security appliance, security camera, simulation.

1. INTRODUCTION

IoT is growing rapid and it may cause that others technologies may look insignificant. Predictions are that by 2020 there will be some +20 Billion connected devices worldwide. The IoT promises to connect everything from CCTV cameras, medical devices, smart home products to smart enabled vehicles and many more devices. Connecting these devices is promising to revolutionize our lives today by bringing greater efficiencies, improved customer service, more effective products and services in an abundance of markets and sectors.

As the security for devices connected to the internet of things (IoT) has been a hot topic, and Internet Protocol (IP) surveillance cameras, in particular, have been the subject of growing scrutiny.

IP cameras have become a top target for hackers because of their relatively high computing power and good internet traffic throughput.

1.1 Motivation for targeting IP surveillance camera

One of the major motivations for hacking IoT devices is financial gain. And when it comes to monetization, IP surveillance cameras are distinct targets for the following reasons:

Constant connectivity: Like many other devices, IP cameras need to be internet-connected to function properly. However, exposure to the internet also makes it easy for hackers to find the cameras and potentially exploit the devices. Once hacked, the devices will be able to serve the hackers' needs.

Low hacking investment: Unlike with hacking a PC, once hackers see a way to break the security of an IoT device such as an IP camera, the same approach can usually be applied to other devices of similar models, resulting in a very low per-device hacking cost.

Lack of supervision: Unlike PCs, especially those used in offices, IP cameras have low user interaction and are not well-managed in terms of security. Installation of an aftermarket anti-malware application is not available either.

High performance: The idle computing power of an IP surveillance camera is usually good enough to perform hacking-related tasks such as cryptocurrency mining, and without being noticed by end users at that.

High internet-facing bandwidth: The always-connected, fast, and huge bandwidth designed for video communications makes for a suitable target for hackers to initiate DDoS attacks.

1.2 Related work

Roy Francis Navea et al. [1] purposed the Design and Implementation of a Human Tracking CCTV System Using IP Cameras this work represents the analysis that IP cameras were used to provide network flexibility focus on detection, recognition and tracking of a person of interest the logic behind this work was to firstly configure the camera and then analyze and process the picture captured by security camera The Haar feature-based cascade classifier was used for face detection. The Karhunen-Loeve transform was used for face recognition. And optical flow was used for tracking which was implemented in Processing. We also discussed about the configuration of the camera and its resolution in this work.

Setiya purbaya et al. [2] targeted the Design and Implementation of Surveillance Embedded IP Camera with Improved Image Quality Using Gamma Correction for Surveillance Camera This study is going to design a device such as IP surveillance camera which based on an embedded system, with improved image recording feature by using gamma correction and data storage feature which integrates with cloud service through a network based on IP (Internet Protocol).we went through this work to know the protocols

used in IP cameras. And know the protocols for security has been used in this work.

Zhaoyu Liu et al. [3] purposed the Communication Protection in IP-based Video Surveillance Systems. . In this work, they address the security threats to the data communications in IP-based video surveillance systems. They first analyze the current approaches, mainly naive and selective methods, to secure real-time video data, and identify their limitations to IP-based video surveillance systems. Then we propose a system design of secure internetworking video surveillance systems. All we got from this work is one of the ways to secure the video transmission inside the network.

Nitin Naik et al. [4] designed Fuzzy Logic Aided Intelligent Threat Detection in Cisco Adaptive Security Appliance 5500 Series Firewalls. This work presents a fuzzy logic aided intelligent threat detection solution, which is a cost-free, intuitive and comprehensible solution, enhancing and simplifying the threat detection process for all. In particular, it employs a fuzzy reasoning system based on the threat detection statistics, and presents results/threats through a developed dashboard user interface, for ease of understanding for administrators and users. We also got to know what Adaptive Security Appliance (ASA) is and how it works. That configured to apply security policies in our simulated network.

Prerna Arote et al. [5] purposed on Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting in this work in proposed mechanism of detection, initially traffic over the network is sniffed by Central Server (CS). Then, CS sends trap ICMP ping packet, analyze the response in terms of ICMP reply and successfully detects attacker. And we understand the way ICMP works and it defends attackers from malicious actions.

Hina Uttam Keval [6] targeted effect, design, configuration, and use of digital Security camera in this work the various aspects of an IP security camera has been discussed how to design a camera and configure in a proper way what are the effect of a security camera and how to use this camera in the environment the way for controlling the security camera has been discussed in this work and This research was undertaken in response to a number of changes taking place within the field of CCTV: 1) changing social perceptions and attitudes towards security; 2) an increase in CCTV technological developments; 3) an increase in the number and variety of CCTV users; and 4) an increase in the utility of CCTV. And we understand how security camera is important how it works and what the effect of these systems is in daily life.

Gron-Woo kim et al. [7] designed the security Model for video surveillance System. The work have done to identify the security Model for video surveillance system, ensuring reliability, safety and privacy detection. The problem in this work is that the implementation of this model in real time is costly and difficult and we understood that there are some model for making the surveillance systems more secure.

Sushant Kumar et al. [8] studied and design Remote Home surveillance System This work presents a novel solution that makes the surveillance of home from anywhere with the help of internet. Remote home surveillance with the help of internet, mobile robot and an IP camera is presented. The security of the robot in this systems are the issue for this work and we also perceive the impact of security surveillance cameras in the Home.

Ming-Jiang Yang [9] designed the Cost effective IP camera for video surveillance. This work introduces a cost effective, power efficient and low profile IP Camera. The camera consists of a video preprocessing unit, an H.264 encoder, and an embedded streaming server that make a good surveillance environment with low cost for the users and our contribution from this work is the way they followed for making such environment for make the camera more cost effective and reliable.

Dimitrios N. et al. [10] targeted the study on security and privacy in Distributed Smart Cameras they describe security requirements, possible attacks, and common risks, analyzing issues at the node and at the network level and presenting available solutions for the possible attacks and so we will know which attacks are possible in the network over the security camera and how to prevent these attacks in this work they didn't show the way for some new attacks and we should analyze that and give good solution in our own work.

2. Typical attack chain

Initial Infection

After locating a device with open ports — such as Telnet, Secure Shell, and Universal Plug and Play (UPnP) — the attacker uses the device's default credentials.

Command and Control

After gaining control of the device, the attacker downloads and executes malicious scripts or samples that report to the command-and-control (C&C) server. That server issues commands instructing the affected IP camera to perform malicious activities such as cryptocurrency mining or DDoS attacks on other devices via User Datagram Protocol floods.

Propagation

Depending on its kind, the malware used can scan the network and employ the same infection methods to propagate itself to other vulnerable devices.

A layered defense IP

A complete functionality offered by an IP camera often consists of the camera itself, the network capability, and the cloud services. To offer a secure product, manufacturers need

to implement security strategies in an overarching approach from the device to the cloud.

IP Camera Hardware

Since finding a system vulnerability is one of the most critical factors for hackers to penetrate into an IP camera, leading manufacturers in the industry pay close attention to monitoring the firmware and patching the vulnerable system components of products. However, to raise the bar on security, further enhancements can be applied, such as:

- Enforcing the changing of default credentials.
- Applying secure boot to prevent compromised devices from functioning.
- Implementing firmware over-the-air (FOTA) updates to patch issues if necessary.
- Employing the principle of least functionality by minimizing open ports on the device if not necessary.

Networking

Deploying IP cameras within a closed network is already a highly adopted mechanism to ensure a better level of security. Virtual private networks (VPNs) can be used to enable remote access with a secure connection. Other network-related security implementations include:

- Encrypting connections to deter attempts at compromise.
- Connecting with a security tunnel.
- Using a hardware component to store encryption keys.

Cloud

The more features provided by cloud services there are, the more critical cloud security becomes. On the upside, many, if not most, service providers are already aware of this. Most leading service providers have adequate protection on their cloud infrastructures. Highly integrated security products including those from Trend Micro also play an important role for cloud environments.

3. Configuration

For this purpose one of the best choices is using of In Vehicle Monitoring System (IVMS) Application that is a software with its all configuration details for IP cameras. So first the camera should set physically then connect it to the NVR (Network Video Recorder) after configuring that it will be able to access camera with the Default IP that is assigned in backside of cameras. To connect to the camera the Computer want to access to camera should have the same range of IP as IP camera. Then it's possible to open the software and go through configurations,

Setting user name and password and port number are the beginning steps for log in to the application.

Log in to the IVMS and selecting the Device management will shows the various fields of the camera that are configurable that are

Main view: help to see all the cameras picture

Remote Playback: possibility of access to the previous recorded videos by the camera

Time and Date: accurate time and date being set for cameras.

Real time Alert: if any unauthorized access come.

Human body retrieval: recognizing people body

Face Recognition: recognizing people faces

E-map: feature to provide graphic map information for users to overview entire CCTV layout.

The options for user log in is shown in Figure 1.

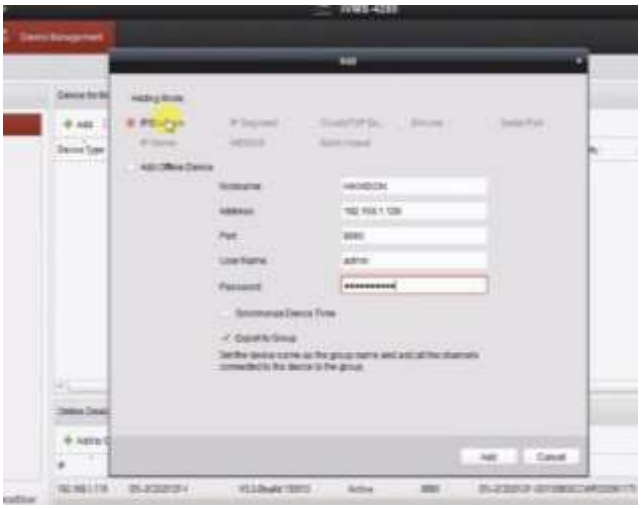

Fig -1: Adding IP Camera and defining Network Settings

The camera into the software that is Add Client by clicking on that we can configure the network portion of the camera as shown on Figure 1. in this screenshot mode and Network configuration of camera are visible Adding Mode should be set of IP Domain that assigning the network setting being applied here.

Nickname, Address, Port, User Name, Password, Synchronize device time, and Export to Group that will allow access to a group of users.

Next step is Remote Configuration of the camera being configured the network part.

In Remote Configuration various fields are configurable:

Device Management: Reboot the device, Restore the Default settings, Import configuration Files and Export configuration Files are included.

General: Network interface cable (NIC) type, configuration of the network settings, HTTP port are configured.

Time: Time zone is crucial aspect in security camera because if any occurrence determined then to access to that the camera should has the exact time of accident.

System Maintenance: Ability of system n term of any failure.

RS232: Serial communication Protocol

Log: Users are able to search logs by type, group, user and camera. And Export log is for bucking up the logs.

User: As shown in Figure 2. Possibility of adding users and modifying the setting and permission for users are configurable.

Service and Security: The security for camera is the password defined for, and also to access to the IVMS it's possible to assign change and remove the password for Application,

For completing the camera configuration in IVMS it should be tested and this is what we worked on.

Fig -2: Modifying, editing and deleting users for camera

The IP camera has been configured and as it is clear the IP cameras are working with IP and inside the network. The main Question is how to secure Transmission of the video captured by the IP camera to the clients inside the network? For that purpose one way is that applying security module on security camera and apply some algorithm on it that every user would not be able to access the data of camera, but it is difficult and costly to improve such idea. Another way is to simulate the data transmission inside the network using Simulation in this simulation the idea is that every security camera inside a network is a node and every node can transmit and receive data inside the network, then how is possible to secure the data transmitted from IP camera (node) to the client has access to. The IVMS environment is shown in figure 3.

By using GNS3 simulation software this idea can be promoted. Requirement for fulfill this demand are Router In the simulated network as it is optional that is possible to use other network equipment's such as Switch. The most important device is needy for this purpose is Adaptive Security Appliance (ASA) that the image of this device should be downloaded and installed in the GNS3 simulator after installation is completed it needs configuration to start working as a security policy between nodes inside the network

Fig-3: IVMS environment

4. Analysis:

Simulation Analysis

In the simulation analysis now come to the purpose of this work in here ASA used to control communication between nodes, that which nodes can access each other in the network and which node doesn't have access to any specific node inside the network even though nodes are in the same network as well as outside of the network or different ranges of network. In above example there are 4 nodes that one can play the role of IP camera inside the network, by using the ASA it is possible to limit the access of any node from outside as well as inside of the network to the specific node. For example in Figure 4 consume that the PC1 is the IP camera and other nodes are the computers inside the network, the nodes that are administrators and want to have access to the PC1 are PC3 and PC4 other node (PC2) is the node that video of the IP camera should not being shared with and it should not has accessibility to PC1, although the data from PC1 should not be accessible to the nodes outside of the network so the ASA helps to reach this goal and limit the access to the video or any data of the PC1 inside the network. The simulation in GNS 3 shown in Figure 4.

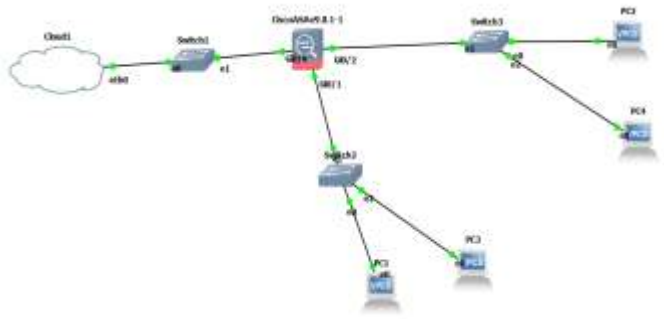

Fig.4: Adaptive security Appliance using GNS3

Performance Analysis

The aim is to limit or cut the connection between PC1 and PC2 inside the network first assigning the same range of IP addresses to all of the nodes inside the network separately and assign IP address to the ASA device by using command prompt in GNS3. Check the connection between the nodes and ASA by using ping command that if the IP ranges assigned accurately nodes will have connection with the ASA that was the configuration of the ASA in the network using GNS3 simulator and now PC1 in the network can has access to the PC 2 through ASA, other PC's cannot have access to the PC1 and no one of them can ping the PC1.By pinging PCs we will understand that which PC will be in access and which will not be able to ping our device.

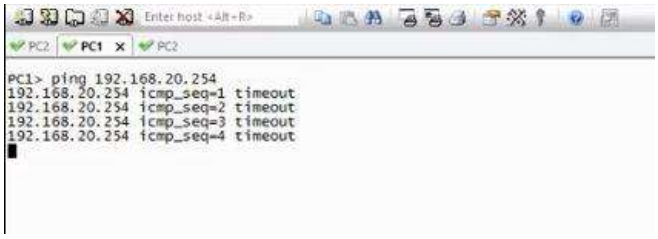

Fig.5: Result of the Simulation

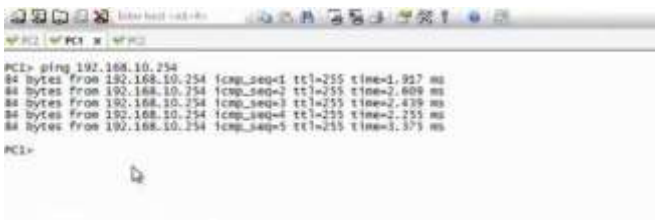

Fig.6: Result of the Simulation

In Figure 5 we will be able to see the timeout that means there is no connection with this IP. The devices that have permission to access to the IP camera will be able to ping that and start exchanging data with the camera inside the network. ASA (Adaptive Security Appliance) is configured in the way to have policies for nodes as ICMP will check weather connection between nodes are alive or not.

In Figure 6 we will see that the destination node is accessible and we can communicate and exchange data with. The policies assigned inside the ASA (Adaptive Security Appliance) shows us that some node restricted to access the IP camera and they will not be able to ping and exchange data.

5. CONCLUSION

As the importance of IP camera for surviving people works and life's became mass topic in this work firstly configuration on IP camera is discussed and As the network is working based on IP, each node inside the network has an IP, although the equipment for applying this system in real world was costly to fulfill this project it simulation is affordable idea, so in this work the idea of making secure the transmissions between nodes are Simulated by a simulator named GNS3, one of the nodes assumed as an IP camera and by using ASA the transmission of the traffic and accessibility of other node to the IP camera was limited by configuring the (ICMP inspect) in ASA that make able the nodes to (echo) ping each other and can communicate to each other. This made the system became more reliable and secure. The future scope for this work is to implement the work in real time environment and also the face detection for the video captured by the camera should be analyze by sing some image processing application.

REFERENCES

[1] Navea, R. F. (2018). Design and Implementation of a Human Tracking CCTV System Using IP. IEEE, 11-17.

[2] Setiya purbaya, Dodi, wisaksono Sudiharto , Catur Wirawan Wijiutomo. (2017). Design and Implementation of Surveillance Embedded IP Camera with Improved Image Quality Using Gamma Correction for Surveillance Camera. IEEE, 4-6.

[3] Zhaoyu Liu; Dichao Peng; Yuliang Zheng; J.liu. (2005). Communication Protection in IP-based Video Surveillance Systems. IEEE, 2-5.

[4] Nitin Naik ; Paul Jenkins ; Brian Kerby ; Joseph Sloane. (2018). Fuzzy Logic Aided Intelligent Threat Detection in Cisco Adaptive Security Appliance 5500 Series Firewalls. IEEE, 8-10.

[5] Prerna Arote ; Karam Veer Arya. (2015). Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting. IEEE, 11-23.

[6] Keval, H. U. (2016). Effect, design, configuration and use of digital security camera. california: IEEE.

[7] Grom-Woo kim. (2009). Security Model for the Surveillance System. IEEE.

[8] Sushant Kumar,Nora Hassin. (2010). Remote Home Survveillance System. IEEE.

[9] Ming-Jiang Yang. (2016). Cost effective IP camera for video Surviellance . IEEE.

[10] Dimitrois N. Halarin , juck D. (2006). Security and Privacy in didtribution smart cameras. IEEE.

[11] (cisco, 2015) usage of Adaptive Security Appliance.

[12] (Koushesh, 2015) How to implement security in GNS3 (2015)