IP camera security: "Security Eyes"

Sultan S Alshamrani[1†]
susamash@tu.edu.sa
Department of information technology, college of computer science and information technology, P.O.Box 11099, Taif 21944, Saudi Arabia

Abstract
With the rapid growth of Internet of Things (IoT) applications and devices, there are still defects in safety and privacy. Current researches indicate that there are weak security mechanisms to protect these devices. Humans use the Internet of Things to control and connect their devices with the Internet. Using the Internet of things has been increased over time. Therefore, capture of sensitive user data has increased intentionally or not [1]. The IP Camera is a type of (IOT) devices. Therefore, in this paper we aim to create a "Security Eyes" application that protects IP Cameras from security attacks according to certain security mechanisms (increasing the strength of encryption and filling the usual security holes in IP cameras ... etc) and alerts the user when the live broadcast is interrupted or an error occurs.

Keywords:
IP cameras, internet of things, application security, IOT.

1. Introduction

1.1 Overview and Problem Background

The Internet of Things can be defined as the connection of multiple devices by communication protocols [2]. We can connect devices with each other and access things remotely [3], [4]. In the Internet of Things, there are two types of threats: a threat against the Internet of things and a threat from the Internet of things. An example of threats against IoT: A massive DDoS attack against DNS servers was published on October 21, 2016 and shut down many web services including Twitter [5]. Additionally, hackers exploited the usernames of the cameras, default passwords, and other IoT devices and installed the Mirai botnet [6] on compromised IoT devices. in addition, IP cameras can be compromised via buffer overflow attacks [7].

IP cameras today are one of the most important technologies that people rely on to monitor and protect their property and homes remotely from anywhere in the world. In addition, to know the perpetrators in case of crimes, God forbid, we can watch a live broadcast from these cameras. For Security, we enter the IP address, password and username or any other authentication process through the application on our phones or computers. However, this process can be dangerous at times.

So, don't forget that the increasing reliance of people on surveillance cameras will increase the exploitation of intruders to spy on homes and learn the lifestyle of their residents, thus facilitating crimes. In order to address camera violations, we will develop an application that increases the security of cameras so that they do not become a tool for spying on us.

Additionally, security camera vulnerabilities become an aid to criminals. In Japan, April 2018, the system was tampered through unauthorized access to a river water monitoring camera [8] [9].

In 2014, Mira botnet targeted surveillance systems and infected more than 600,000 devices worldwide [6] [10].

Through Censys.io and Shodan.io queries of well-known manufacturers, found over 1 million surveillance cameras and over 125,000 surveillance servers exposed to the Internet [10].

1.2 Problem Statement

Many surveillance cameras are subjected to vandalism due the ease of guessing passwords and the lack of extensive technical knowledge of the need to change the factory settings for security, and weak algorithms to achieve security.

To provide solutions for this problem, it is preferable to move away from any of these points [1]: (1) default login information does not change the default settings such as username and password. (2) Simple keys. (3) Weak authentication policy for choosing a password. (4) Low encryption method for confidential information and data, or sending data unencrypted. (5) No mechanism to lockout the IP camera account after several wrong password attempts to enter to the system by hackers. (6) Removable unencrypted memory that stores video and vulnerability in Android applications that are used to monitor devices.

Some potential attacks of IP Cameras **[1]:** Eavesdroppers: When a hacker eavesdrops on data that passes through the network plane.

Manuscript received February 5, 2022
Manuscript revised February 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.2.10

The Man in the Middle (MITM): Hackers attempt to improperly implement SSL to resend all. Correspondence in its channels (s): to spy on network traffic that is transmitted in the form of readable text. The man at the end (MATE): If the attacker searches for or disables the software or hardware of the physical device. The malicious code the hacker programs it to target a network. The Wi-Fi Sniffers: When an attacker tries to find the router's key and log in as a trusted user of the system and the network. The app developers: Search for user activity by hiding trackers in apps or by installing malware or leaking information.

1.3 Objectives

We have designed a surveillance camera application to increase its security that contains a strong encryption algorithm that protects the user from any attacks or piracy.

We aim to achieve the following goals:

Ease of use the application to save time and effort for the user. Protect the application from any hacking or interruption of recorded or permanent broadcasts. Protection when transferring video by increasing the strength of encryption. The application supported multiple cameras

1.4 Scope

IP Cameras are considered under the computer science and information technology, as Security eyes will combine these two departments from depth in programming to achieving security. Security eyes provides a high security service to protects IP cameras through increasing the strength of encryption and filling the usual security holes as it aims to design an easy-to-use application that features strong encryption policies and Ensure that the applications associated with the IP camera work in high efficiency and provide a two-step verification step when logging in to access its privacy information. It alerts the user when the live broadcast is interrupted, or an error occurs. Also, this application will save the user time and effort while fully protecting information by encrypting the live broadcast to prevent hackers from penetration. It will serve a large number of society and help them achieve safety, among the sectors that will be served by the project are the health, engineering, educational, national and personal sectors in general. The application can be used anywhere and anytime. It's used widely in homes for monitoring at 24\7.

1.5 Contributions/Significance of the Project

Significance of the Project.	Contributions.
For help increase the security of surveillance cameras.	For help increase the security of surveillance cameras.
Educating users, the importance of changing the default values of passwords and choosing strong passwords that contain large and small letters, numbers, and symbols.	Security information in the users systems.
Facilitating the advantage of monitoring the property at any time and place.	-
Data protection during transmission.	Cryptography and Encryption.
• Provides the most important requirements for security, confidentiality, authentication, access control, integrity, intrusion detection and prevention.	Encryption and 2 Step Authentication.
Limit intrusions and attacks on surveillance cameras.	Encryption and 2 Step Authentication.

1.6 Realistic Constrains

- The size of the application, it must be suitable for the devices, and this is difficult due to the images and encryption processes for the data and the continuous updates of the application. Most users delete the application after a while, either because they don't understand how to use it or because there is not enough space for the device.

- Updates and maintenance on the application, changes and modifying bugs in the mobile applications is very difficult.

- The way of use (interfaces). Dealing with the screens of small devices is one of the obstacles to designing mobile applications, so it must be easy, understandable and clear to the user.

- The environment in which the application will be published, so that determining who will "promote" or use the application in beginning is importance in the success and spread of the application.

We have discussed in this point the most prominent problems that face users of surveillance cameras and the threat of vulnerabilities. In the next topic we will discuss literary reviews of scientists in the security of surveillance cameras.

2. Related Work

The security and privacy of IoT recently is important. The number of IoT devices is growing quickly around the world according to researches and studies [11] [12]. it's reported that a hundred and eight million network security cameras dispatched internationally around the world in 2019 according to a research report by HIS Markit [12] [1].
In fact, most of IP Cameras are known to weak security mechanism or send their data unencrypted via the internet which leads to many privacy and security concerns from hackers [14].
Many researchers for Example Tekeoglu and Tosun [15] performed a study of a Belkin IP Camera and its Android Netcam application they able to modify programs, use a backend account, or change the password of the current admin without his knowledge, which enabled them to carry out a Man-in-the-middle (MITM) attack and hack IP camera live broadcasts[14] .
Authors [16] whose topics are mentioned in the scientific paper entitled "The Security of IP-based video surveillance systems" focus on physical attacks such as data extraction, covert channels, and concealment of information. The aim of this study is to make the reader have a strong background on the attack of the IP-based surveillance system so that he can understand and analyze the objectives and techniques of the attacker in the context of these systems [10].
These studies Basically analyzed the Security of IP CAMERAS and accessible to its internet-users and their application [1]. According to the current studies and research carried out by the two researchers, Alharbi and Aspinall [13] where they have an experiment with five IP cameras. They shed light on the categories of vulnerabilities in their devices that are used for monitoring and explained the effect of these things on users' privacy and security. Therefore, they cause a threat due to poor security and easy penetration [1].
The study of Alharbi and Aspinall [13] Concluded several vulnerabilities of these cameras include poor encryption policy, easy default passwords, no mechanism to lockout the IP camera account after several attempts to enter to the system with the wrong password, unsecure video stream, bad key management encrypted video stream, user-sensitive leakage of details, unencrypted removable memory which stores videos and weaknesses in android applications that used to monitor devices [1].
Authors [15] whose topics are mentioned in the scientific paper entitled "The Security of IP-based video surveillance systems" systems were able to extract JPEG images that were recorded by a NetCam IP camera by eavesdropping on network traffic as an authorized user due to weak algorithms [10].
The proposed paper will aim to design an easy-to-use application that features strong encryption policies and Ensure that the applications associated with the IP camera work with high efficiency with provide a two-step verification step when logging in to access its privacy information. Also, the agreed application will aim to implement the system shutdown feature when trying to log in with several unsuccessful attempts, as this feature will provide high security and protect privacy, which makes it a protection shield against hackers.
We researched extensively to choose a good encryption algorithm for the videos and we read several papers with the following titles:
A New Algorithm for MPEG video encryption [17], An efficient MPEG video encryption algorithm [18] , Comparison of MPEG video encryption algorithms [19]. Accordingly, we chose a VEA encryption algorithm, which is short for (Video Encryption Algorithm), Because there is a useful feature during video transmission in networks, the transmission is not reliable. Noise is present in most transmission media and this noise results in bit or frame loss, but VEA allows re-sync for users to decode only certain parts of the video. In VEA, the encryption and decryption key is the same.

3. Methodology

Here we will explain how to protect the IP camera in modern ways such as Face ID and the devices authorized to enter the camera application. We will create an application for IP Camera and this application helps protect against hacking.

3.1Waterfall Model

We used waterfall model to design our system (Security Eyes). The waterfall is the sequential design process, used in software development, in which progress is seen as flowing steadily downwards through the phases of conception initiation, analyze, design and maintenance. And This approach is called "the traditional approach", and is considered one of the simplest, oldest and most used models.
It consists of several stages:

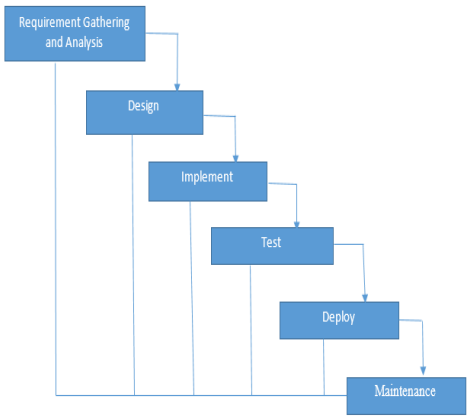

Figure 3.1: waterfall model (Security Eyes).

3.2 system Security Eyes

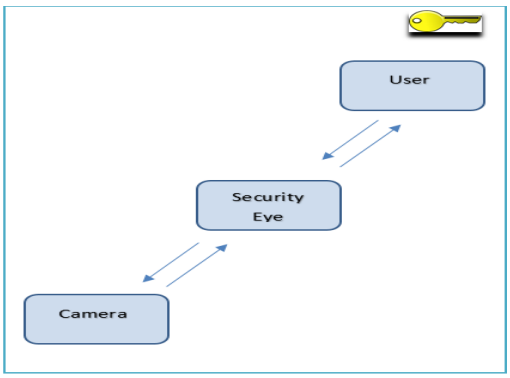

Figure 3.2: system Security Eyes.

33.3 Involved Technologies

Python , kivy , VEA

Why python?

Python is an easy-to-learn yet powerful programming language with excellent functionality for processing linguistic data, used to build programs [20]. We use this language in our system (Security Eyes).

Tools:
Some tools and software are used in the experiment part to reveal the vulnerability types in the IP camera [1]:
Kali Linux: Well-known platform for checking security threats and vulnerable discoveries.
Wireshark: for analysing packets in network level.
Nmap: network discovery tool, it's also known as network mapper.
Arpspoof and Mitmproxy: to the aim of implement MITM attacks.
Netdiscover: to collect information in detail about the network devices.
Bettercap: used for sniffing and spoofing.

7 3.4 Expected Benefits:

This project aims to provide safety and security in cameras using the " Security Eyes " application.
Using this app by stakeholders (e.g., parents in home, companies, schools, governments, traffic) will have largely protected them while using the cameras. They will know about breakthroughs as soon as they happen and respond to them.
The application will keep the information it uses from the cameras confidential.
The application provides innovative and reliable protection mechanisms that are not present in other applications. While many applications overlook simple aspects, hackers may exploit them to penetrate; we cover all aspects of security.
The app gives you multiple security options for your camera, you don't have to choose just one.

- The application provides remote control by designing interfaces that enable the user to enter camera information and enables us to control remotely (e.g., camera name, ip camera, password).

The application enables you to give the powers to control the
camera to other individuals (such as for the father to give control to the mother).
The application gives you space to save videos and pictures and back up them without the need for external memory or other applications to save them. You can save remotely by the application.
The application enables you to discover errors and malfunctions, not just intrusions.
The application makes continuous updates every period to fill new gaps and develop security methods.

4. conclusion and future work

Cameras are a kind of different types of IOT that are used in a wide range of applications and essential uses, so our goal in this project is to implement "security eyes" that provide protection for IP cameras from attacks, security breaches, loopholes, espionage and other harmful uses that threaten the safety of the camera and the user. Using methods and techniques to increase safety.
We believe that “security eyes” will provide high security to the user by providing two-way authentication to the user via e-mail and face ID to increase the verification of the user’s identity. It also provides a strong encryption algorithm that encrypts the videos and protects them from unauthorized people spying. It also provides monitoring of usage when the user uses the application and stops for five minutes or more from controlling or working on the application, his exit will be recorded automatically.

4 4.1 Future Works

In the future of this project, we will present the "security eyes" application for surveillance cameras with good security standards. That is for protecting the safety of the user and his information. In addition to this point to maintain the live broadcast of the cameras from being interrupted.

References

[1] P. A., Abdalla & C.,Varol (2020, June). “Testing IoT Security: The Case Study of an IP Camera.” In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.
[2] Z. Ling, K. Liu, Y. Xu, Y. Jin, & X. Fu., (2017, December). “An end-to-end view of iot security and privacy.” In GLOBECOM 2017-2017 IEEE Global Communications Conference (pp. 1-7). IEEE.
[3] L. Atzori, A. Iera & G. Morabito (2010).” The internet of things: A survey. “Computer networks, 54(15), 2787-2805.
[4] J. Gubbi, R. Buyya, S. Marusic, & M. Palaniswami, (2013). “Internet of Things (IoT): A vision, architectural elements, and future directions.” Future generation computer systems, 29(7), 1645-1660.
[5] S. Hilton, (October 2016) , Dyn analysis summary of friday october 21 attack [online] Available: http://dyn.comlblog/dyn-analysis-summary-of-friday-october-21-attack/
[6] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J.A Halderman, L. Invernizzi, M. Kallitsis, et al. “Understanding the mirai botnet.” In Proceedings of the USENIX Security Symposium, Vancouver, BC, Canada, 16–18 August 2017.
[7] R. Chirgwin, Get pwned: Web cctv cams can be hijacked by single http request - server buffer overflow equals remote control, November 2016, [online] Available: http://www.theregister.co.uk/2016/11/30/iot_cameras_compromised_by_long_url.
[8] August (2019) ,"Information and Security White Paper 2019 (in Japanese)", white paper Information-technology Promotion Agency.
[9] S. Shin, & Y. Seto, (2020, June). “Development of IoT Security Exercise Contents for Cyber Security Exercise System.” In 2020 13th International Conference on Human System Interaction (HSI) (pp. 1-6). IEEE.
[10] N. Kalbo, Y. Mirsky, A. Shabtai, & Y. Elovici, (2019). “The Security of IP-based Video Surveillance Systems.” arXiv preprint arXiv:1910.10749.
[11] M. Swan, (2012). “Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0.” Journal of Sensor and Actuator networks, 1(3), 217-253.
[12] Markit (2019) "The top trends of 2019: powered by transformative technologies".
[13] R. Alharbi, & D. Aspinall (2018). “An IoT analysis framework: An investigation of IoT smart cameras vulnerabilities.”
[14] J. Liranzo, & T. Hayajneh, (2017, October). “Security and privacy issues affecting cloud-based IP camera.” In 2017 IEEE 8th Annual Ubiquitous

Computing, Electronics and Mobile Communication Conference (UEMCON) (pp. 458-465). IEEE.
[15] A. Tekeoglu, & A. S. Tosun, (2015, August). "Investigating security and privacy of a cloud-based wireless IP camera: NetCam." In 2015 24th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-6). IEEE.
[16] A. Costin, (2016, October). "Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations." In Proceedings of the 6th international workshop on trustworthy embedded devices (pp. 45-54).
[17] L Qiao,., & K Nahrstedt,. (1997, July). "A new algorithm for MPEG video encryption." In Proc. of First International Conference on Imaging Science System and Technology (pp. 21-29).
[18] C shi,., & B Bhargava. (1998, October). "An efficient MPEG video encryption algorithm." In Proceedings seventeenth IEEE symposium on reliable distributed systems (Cat. No. 98CB36281) (pp. 381-386). IEEE
[19] U Potdar,., K. T Talele,., & S. T. Gandhe, (2009, January). "Comparison of MPEG video encryption algorithms". In Proceedings of the International Conference on Advances in Computing, Communication and Control (pp. 289-294)
[20] S. Bird, E. Klein, & E. Loper, (2009). "Natural language processing with Python: analyzing text with the natural language toolkit." " O'Reilly Media, Inc.".

Dr Sultan S Alshamrani is currently working as an associate professor at Taif University in Saudi Arabia and he is the head of the department of Information Technology and the Chairman of the committee of faculty members affairs. DR. Sultan got his PhD from the University of Liverpool in UK and a master‟s degree in Information Technology (Computer Networks) from the University of Sydney in Sydney, Australia. DR. Sultan finished his bachelor's degree in computer science from Taif University in 2007 with General Grade" Excellent" With first honor and an accumulative GPA of (4,85) out of (5,00) where considered the highest GPA in the collage