Investigating Privacy Concerns of Wi-Fi Cameras in the Context of Smart Home Security

Muhammad Khuram Khalil[1], Zahraa Al Ajmi[1], Zahraa Al Ajmi[1], Hadi Al Ajmi[1] and Vikas Rao Naidu[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

The popularity of smart home technology has led to increased use of Wi-Fi cameras, which provide real-time video streaming and remote access. However, the wireless transmission of video and audio data raises privacy and security concerns, including unauthorized access and data breaches. This study employs a qualitative research approach to investigate privacy concerns associated with Wi-Fi cameras in smart homes. This study investigates privacy concerns related to Wi-Fi cameras in smart homes. While these cameras offer convenience and security, they also raise privacy issues. The study explores potential risks and aims to provide insights and solutions through a qualitative analysis of user experiences. Semi-structured interviews with Wi-Fi camera users will explore experiences and perceptions of privacy risks and strategies for managing them. Thematic analysis of the data collected will identify patterns related to privacy concerns and user experiences. The study aims to contribute to literature on smart home security by informing strategies for addressing privacy concerns and promoting responsible use of smart home technology.

Introduction

Since the 1970s, there has been home automation, offering consumers quick and secure access to their residences. A modern home relies on multiple services for infrastructure support, including internet and electricity. Home automation systems deal with services, space planning, and stuff. Early home automation systems faced challenges like high costs, lack of standards, and unfamiliarity with technology. Standards for communication were established, nevertheless, as technology developed. Complex user interfaces, high pricing, and a lack of dependable components are still issues with modern home automation systems.

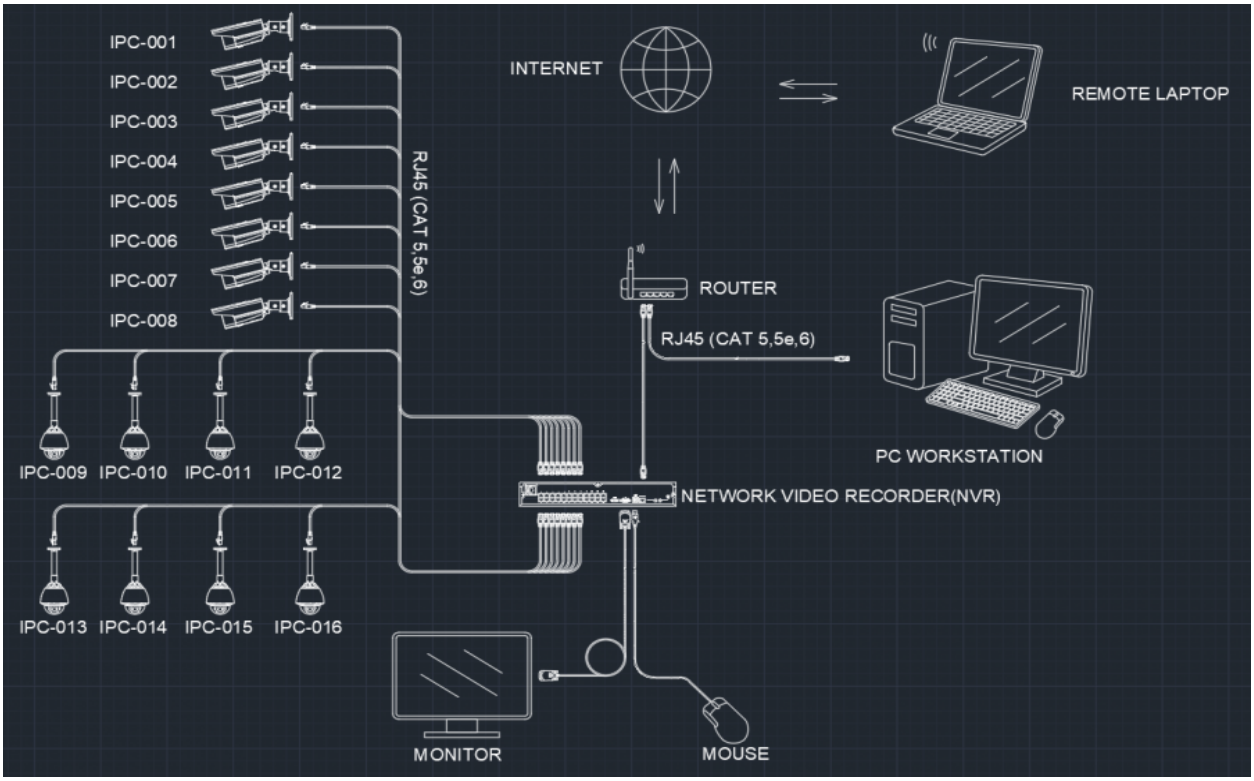
Security Risks of Modern Home Automation Systems

Modern homes now have complex security systems that make use of different sensors, cameras, and alarms rather than a basic lock and key system. Because these systems are online, owners can access and manage their houses remotely from any location in the world. However, increasing connectivity also brings with it security dangers like Cross Site Scripting (XSS) vulnerabilities in home automation systems, routing attacks on wireless sensor networks, and replay attacks. Many designers and businesses have placed little emphasis on security in favor of enhancing functionality and consumer ease. This strategy presents challenges because homes are places where individuals should feel safe and secure, and any psychological harm can result from a compromise. It is crucial to take into account the flaws in home automation systems as well as the potential dangers of connecting them to the Internet. Home automation systems are attractive to attackers because:

- They frequently include information and personal data.
- They are typically accessible from any place because they are online constantly.

- They are less secure because they don't have a specialized system administrator.
- It's possible that homeowners are unaware of required updates or patches.
- The systems are frequently complicated and challenging for non-tech aware homeowners to secure.
- Devices made by many manufacturers could each have unique security flaws..
- Attackers might search the internet for particular holes in home automation equipment.

Basic Design Security Camera System[11]



Home Automation's Risks and Difficulties as Seen Through the Eyes of a Homeowner

When choosing home automation equipment, homeowners frequently put price over security, which puts their properties at risk of theft and intrusion. When choosing home automation equipment, homeowners frequently put price over security, which puts their properties at risk of theft and intrusion. People of all backgrounds utilize homes, thus it is unreasonable to expect visitors to be aware of security dangers. This could be an issue since mobile gadgets, such as mobile phones and PDAs connected to home networks, could be utilized as a doorway into the house by attackers. This implies that even a minor security vulnerability may have detrimental effects. Homeowners might attempt to construct elaborate and challenging access control methods. Additionally, they might regularly need to modify access control settings, which can be tedious and annoying. Clairvoyant Access Right Assignment (CARA) is a technique that lessens the workload associated with assigning each resource to specific visitors. This approach, meanwhile, is not always reliable and is susceptible to social engineering and hacking.

When end users think about access control, their expectations rarely match the practical execution of access control and security systems. In other words, even though homeowners have some awareness of security measures, they might find it difficult to put them into practice successfully.

When it comes to the implementation of access control and security measures, end users frequently have expectations that are different from what is actually happening. This suggests that householders may experience difficulties trying to put security measures into effect even though they are aware of them.

Security Challenges in Home Automation

- Ubiquitous computing in a home environment is complex and unpredictable from a security standpoint.
- It might be difficult to enforce security rules or regulations when they interfere with residents' or their guests' convenience.
- Homes consist of people of all ages with different behaviors, and some are more vulnerable to social engineering.
- Breaches in home automation networks can cause physical, emotional, financial, and environmental harm, as well as unauthorized access, theft, blackmail, vandalism, or voyeurism.
- Security concerns at home are exacerbated by guests' different technological skills, mixed ownership of equipment, and malicious intentions.

Challenges of Context-Aware Computing in Home Automation Security

The modern home's computing environment is constantly changing, making it difficult for users to be security conscious when accessing their home from outside. Although it can be difficult to pinpoint a user's location and activity, context-aware home automation systems attempt to increase security by recognizing the context in which a user makes a decision. Additionally, context-aware computing raises serious privacy concerns as it requires sharing intimate information about the user. The author contends that rather than letting residents make decisions on their own, smart home devices should help them make judgments that are more security- or energy-conscious.

Factors to Consider for Successful Implementation of Context-Aware Systems at Home

- System should be transparent about its knowledge, methods, and actions
- User must be informed when system's actions affect others
- Context-aware computing adds complexity and is difficult to accurately interpret
- Contextual computing increases manufacturing, implementation, and maintenance costs
- System requires constant user intervention and expert assistance if malfunctioning
- Context-aware systems are challenging to implement and are fraught with privacy issues.

Central Controller-Based Home Automation System

Because a central controller-based security system gives a single point of control and access to sensitive information about residences and their occupants, it can in fact provide privacy and security problems. In addition, the effectiveness of such a system depends on the number of homes participating, making it less suitable for securing individual homes. The proposed SmartEye system using GPRS and video cameras may also have security issues that need to be addressed, and the importance of communication and network setup should not be prioritized over security considerations. Ultimately, any home security system must balance the need for convenience and accessibility with the need for privacy and security, and carefully consider the risks and benefits of centralized versus decentralized approaches.

Bluetooth-Based System for Home Automation

With a host controller running on a PC, N. Sriskanthan et al. constructed a Bluetooth-based home automation system. sensors, device controllers, and the new Home Automation Protocol (HAP) protocol that are all based on microcontrollers.

A home automation system employing Bluetooth that can be accessed remotely via GPRS has been presented by H. Kanma et al., using a smartphone with Bluetooth as the host controller and a GSM modem for Internet connectivity. and talked about updating and remotely controlling home appliances.

Issues with using Bluetooth for home automation include limited range in home environments, high power consumption, and serious security concerns with Bluetooth Low Energy (BTLE).

Bluetooth communication should only be used for hurried, transient network connection that gives minimal thought to security.

Due to its low cost, simplicity of installation, and availability of hardware, Bluetooth is a popular technology for smart homes, however there are some drawbacks.

SMS-Based Home Automation System

These are four different research works on SMS-based home automation and security systems. A. Alheraish suggests a system that recognizes unauthorized entrances and enables authorized users to operate the door passkey and house lighting through SMS. et al., M.S.H. propose an SMS-based system that enables homeowners to control their appliances and receive intrusion alerts through SMS from a registered mobile number. U. Saeed et al. propose a Java-based system that allows users to remotely control their home devices by sending SMS messages with the appropriate user actions. Last but not least, A.R. Delgado et al. provide a GPRS-based backup system for an Internet-based home automation system that adds fault tolerance, permits alarms, and allows access through both a message interface and a web interface.

- Using a 4 digit passkey for home security is vulnerable to attacks, as it can be easily learned by someone watching the owner enter it, and users may not always be careful.
- Additionally, having different passkeys for each person at home raises the danger of hacking.
- SMS-based alerts may not be effective as users may miss the alerts or not check their phones frequently.
- A photo of a legitimate person can be used to hack facial recognition software, and it is also easy to copy the SIM card from a legitimate smartphone.
- The use of remote access and cameras in a home automation system, as proposed by A.R
- Delgado et al. [37], may increase the chances of vulnerabilities being exploited by attackers

GPRS-Based Home Automation System

The article discusses several home security systems that use GPRS, with varying levels of functionality. Some of the proposed systems include video streaming and surveillance using webcams and mobile phones, remote control of home devices via mobile phones, and monitoring of home status through mobile phones. Some systems also use motion sensors and infrared sensors to detect intrusions or other emergencies and notify the homeowner via email, text message, or phone call. The proposed systems use different architectures and technologies, such as client/server models and embedded systems. Overall, the systems aim to provide improved security and automation for homes and offices using GPRS.

GPRS-based home security systems raise security issues:

- A number of studies (M. Danaher and D. Nguyen [13], B. Wu et al. [38], L. Yang et al. [39], and S.R. Das et al. [42]) use cameras in home security systems, which can be exploited by knowledgeable attackers to provide them access to real-time video feeds of the inside of the home.
- Video feeds can be looped if not installed and maintained properly.
- In order to protect against invasions, GPRS-based intrusion detection systems demand ongoing monitoring of phones.
- Skilled intruders are capable of spoofing the infrared sensor-based intrusion detection systems described by B. Wu et al. [38].

- The research by L. Yang et al. [39] uses ambiguous terminology and permits valid mobile numbers to be faked, potentially enabling attackers to influence or monitor home devices and ascertain occupancy.
- Email alerts for intrusion attempts may be easily missed by users.
- Home security systems can now be accessed via a web browser, according to researchers S.R. Das et al. [42], however, this poses extra security risks.
- The majority of GPRS-based home security systems use simple methods to identify intruders and do not take technologically adept attackers into account.

DTMF-Based Home Automation System

A DTMF-based home automation system is presented by the work of L. Muhury and A.H.M.A. Habib [44], allowing users to operate items by tapping numbers on their phone's keypad. The system receives and decodes the DTMF tone using a GSM module and a decoder and implements the user's commands at home. However, DTMF-based systems are not commonly used due to better communication options available. Moreover, they are vulnerable to "fuzzing attacks," where unusual input data can cause the home network to crash by triggering an exception in the DTMF processing algorithms.

System for A**ut**omating Homes Over the Internet

Researchers frequently choose Internet or IP protocol-based communication in home automation systems because of its scalability, flexibility, popularity, availability, and affordability. For end customers who already own devices like laptops, cellphones, and tablets, it is also practical and simple. A user interface (UI), web pages, or Android/iOS/Windows applications are common elements of an Internet-based home automation system that use a login and password as the only authentication method to provide access to the home.

This Raises Some Security Concerns

- People often write down passwords and usernames in easily accessible places, making them vulnerable to theft.
- Reusing the same passwords and usernames across different platforms makes users vulnerable to phishing attacks.
- Logging in from different networks, including public Wi-Fi networks, increases the risk of man-in-the-middle attacks and credential theft.
- Human behavior may lead to the use of easily guessable passwords, and social engineering attacks can be effective in obtaining login information.
- Accessing a home through a web browser can introduce security issues, and convenience may override security considerations for users.

System for Automating Homes Over the Internet

According to researchers and end users, this paragraph explains the benefits of utilizing Internet-based communication in home automation systems. Researchers find the Internet an attractive choice due to its scalability, flexibility, availability of hardware and network, high bandwidth, low communication cost, and ease of connection and disconnection

of devices. End users find it easy, convenient, cheap, flexible, and compatible with devices they already own, such as laptops, smartphones, PCs, and tablets. Figure 3 illustrates the elements of a typical Internet-based home automation system, including a user interface (UI) that may be accessible via web pages or mobile applications. For authentication, the majority of Internet-based home automation systems just require a login and password.

This raises some security concerns:

People frequently write down complicated usernames and passwords close to their workstations, leaving them open to attacks.

The likelihood of phishing attacks increases when users use the same usernames and passwords across numerous websites and discussion groups.

Logging in to a home from different networks, such as public Wi-Fi networks, may expose users to various attacks like man-in-the-middle attacks.

Depending solely on passwords for security may not be enough because people tend to choose easily guessable passwords, and social engineering can also be used to obtain them.

Accessing a home through a web browser can pose security risks, and people may prioritize convenience over security

Decentralized Home Automation System Approach

The article discusses a decentralized approach to home automation systems, It does away with the requirement for a central controller. This strategy, suggested by M. Gauger et al., uses a distributed control or process architecture and incorporates actuators into the home's wireless sensor network (WSN). One or more control nodes receive data from sensors, process it, and start the relevant actuators to regulate the environment in accordance with the user's instructions. This approach avoids the problem of a single point of failure in a centralized system.

Issues with home automation systems' decentralized design:

- Without any built-in alarm systems, an attacker with knowledge of the network and actuator positions can quickly disconnect them.
- Communications are done in clear text, which means an attacker can eavesdrop on them with the right hardware.
- Home automation systems must do intricate tasks that demand processing power and storage, which actuator nodes are now unable to supply.

Role of User Interface in Security

The rising use of smartphones and other mobile devices to operate home automation systems is mentioned in this text. The significance of creating user interfaces that are clear and safe is also covered.

Some key points include:

- According to a survey, 2.50 billion of the 5.13 billion individuals who will be using mobile phones by the end of 2017 will be doing so with smartphones.
- User interfaces are important for allowing users to interact with home automation systems.
- According to a survey, consumers choose using PCs to schedule pre-planned activities or manage behavior patterns and mobile phones for instant control.
- Human error accounts for over 65% of the economic losses associated with information security breaches..
- Home automation systems are made to be used by people, so user interfaces must be effectively developed and take into account the users' level of technical expertise.
- Interface designers should consider users' habitual actions and mental models when developing security-critical interfaces.

Conclusion

This essay underlines the necessity to solve the issues with identifying and preventing sophisticated intruders in a home environment while concentrating on the security problems in current home automation systems. In order to stop skilled and sophisticated attackers, the article recommends that future research take into account the full home automation system and develop behavior prediction and enhanced sensing parameters. The efficient implementation and development of home automation systems depend on security, which gives residents a sense of security and eases their worries.

References

[1] Brand, S. (1994). *How buildings learn: And fail to learn*. Viking.
[2] Gellersen, H.-W. (2005). *ECSCW 2005 proceedings of the ninth European Conference on computer- supported cooperative work, 18-22 September 2005, Paris, France*. Springer.
[3] *IEEE Transactions on Consumer Electronics*. (1992). Institute of Electrical and Electronics Engineers.
[4] Krumm, J., & Krumm, J. (2007). *UbiComp 2007: Ubiquitous computing: 9th International Conference, Innsbruck, Austria, September 16-19, 2007: Proceedings*. Springer Berlin Heidelberg.
[5] Sobh, T., Elleithy, K., Mahmood, A., & Karim, M. A. (2008). *Novel algorithms and techniques in telecommunications, automation and Industrial Electronics*. Springer Netherlands.
[6] Gislason, D. (2008). *Zigbee Wireless Networking*. Newnes.
[7] Newman, H. M. (2013). *BACnet: The Global Standard for Building Automation and control networks*. Momentum Press.
[8] (N.d.). *Specification for Standard Cells*. https://doi.org/10.3403/00001252u
[9] *Combined proceedings, volume 67, 2017*. (2018). International Plant Propagators' Society.
[10] *Smart computing*. (2004). Sandhills Pub. Co.
[11] Draftman. (2021, January 29). *Security camera system*. Free CAD Block And AutoCAD Drawing. https://www.linecad.com/security-camera-system/?ssp_iabi=1682929584134