IJARIIT
INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 1)
Available online at www.ijariit.com

A Literature Survey on Smart Home Automation Security

Rohit Ragmahale
Dr. D. Y. Patil College of Engineering, Ambi, Pune University,
Maharashtra
rohitragmahale.mobile@gmail.com

Abstract: This paper presents a detailed description of different technologies and home automation systems from a security point of view. This paper highlights various security flaws in existing home automation systems and how the concept of security and the meaning of the word "intruder" have evolved over time. We studied the challenges in home automation security from point of view of home owner and security provider. This work considers home automation systems like central controller based home automation systems, context-aware home automation systems, Bluetooth-based home automation systems, Short Messaging Service-based home automation systems, Global System for Mobile communication or mobile-based home automation systems, and Internet based home automation systems. The work is concluded by giving future directions home automation Security Research.

Keywords: Access Control, Data Security, Smart homes, Intrusion Detection.

INTRODUCTION

Since last 4-5 decades, the concept of home automation has been there. People's expectations regarding home automation and security have changed to large extent during the course of time due to the advancement of technology and services. Different automation systems over the time tried to provide efficient convenient and safe way for home inhabitants to access their homes. Irrespective of the change in user expectations, advancement of technology, or change of time, the role of a home automation system has remained the same.

"*The tasks of a modern security system include identifying an intruder trying to gain access to the home, alerting the homeowner about the intrusion or intrusion attempt, preventing the intruder from gaining access to the home, and gathering or collecting evidence regarding the intrusion so that the perpetuators can be brought to justice.*" The changing concept of security in modern homes has an impact on the advancement of technology. Sophisticated security systems using microphones, proximity sensors, contact sensors, cameras, alarms etc. has been changed from a simple lock and key based security system. Today, users can access and control their homes remotely from anywhere and at any time in the world by connecting modern homes to the Internet which is very popular. Reduction in power consumption, cost, and size of new electronics devices due to an increase in processing power of newly-designed processors and the considerable enables people to know and control every aspect of their home. By using live video and audio feeds from different parts of their home people can keep an eye on their home, also can be aware of different environmental factors inside and outside their home, like temperature, humidity, light intensity etc. In a Wireless Sensor Actor Network, sensors gather information about the environment around them or the physical world. Actors perform the appropriate actions on the environment as directed by the user or any other party. Engineers, designers, researchers can come up with efficient methods to allow home inhabitants to access and control each and every aspect of their home, including the environment due to the popularity of the Internet and Wireless Sensor Actor Networks.

Challenges in Home Automation Security

- **From a Homeowner's Point of View**
  1. There is a huge difference between what user thinks is the implementation of access control and the access control and security measures that are actually implemented.
  2. The owner also has to consider the social implication of rejecting access to a guest. Though the owner may have to consider the guest's feelings, a guest may feel insulted. The owner may need to change user access control rules often which is a big security threat.

3. Along with home security system, there can be more devices connected to a home network like mobile phones which go with other user and connects to external other networks.
4. An attacker can compromise home automation system by using these devices as a gateway to home network when these devices get connected to home network because user are careless in this case.
5. Most of the times people are unaware, misinformed or careless about various security risks while choosing home automation system due to the money issue.

- **From a Security Engineer's Point of View**
  1. Unlike in companies, one can't enforce policies or security procedures that affect the convenience of people at home or their guests.
  2. People are careless about even simple security policies.
  3. Home may consist of people of different age groups e.g. Senior citizens which are not cable of understanding the technical aspect of the security system is more vulnerable to social engineering.
  4. An attacker who hacks a home automation network can cause a wide range of damage, including theft, vandalism, emotional harm, permanent damage to electronic devices, loss of reputation, financial damages, blackmail, environmental damages, physical harm to a home's inhabitants, granting unauthorised access to anyone.
  5. The mixed ownership of devices at home and guests with varying technical knowledge and different intentions compounds security issues at home.

Related Work

- **Central Controller-based Home Automation System**

  A central controller based home security system can be implemented by combining many homes into a security network with a control node dedicated to each locality depending on the number of users. There are few central or chief control nodes with high processing power which controls these nodes.

  Central Controller-based Home Automation System Challenges:

  There must be a considerable number of homes in the locality to implement this system. So that it will be cost effective and maintainable.

  A person having central control and its data will be able to know about a home's intimate and private information from the data at its disposal, like if a home's room AC is off or on, or if a person in a home is taking a shower. This may cause serious privacy concerns.

  A home automation Security System called SmartEye using GPRS also uses a central controller, to which many individual home controllers are connected [5]. This system proposes a real-time monitoring system and home automation. The user can view the home using live camera feeds. The system notifies the homeowner by mobile phone using GPRS.

  SmartEye uses video cameras for security. This proposed system is also not suitable for securing single homes, but suits for a group of homes.

  This central controller-based security system is difficult to implement and can cause some very serious privacy concerns.

- **Bluetooth-based Home Automation System**

  The work of N. Sriskanthan et al. [6] shows the implementation of a home automation system using Bluetooth. They use a host controller, which is implemented on a PC, is connected to a micro-controller based sensor and device controllers. Home Automation Protocol (HAP) is proposed to make the communication between devices possible. The system allows more than one device controller to be connected to the host controller.

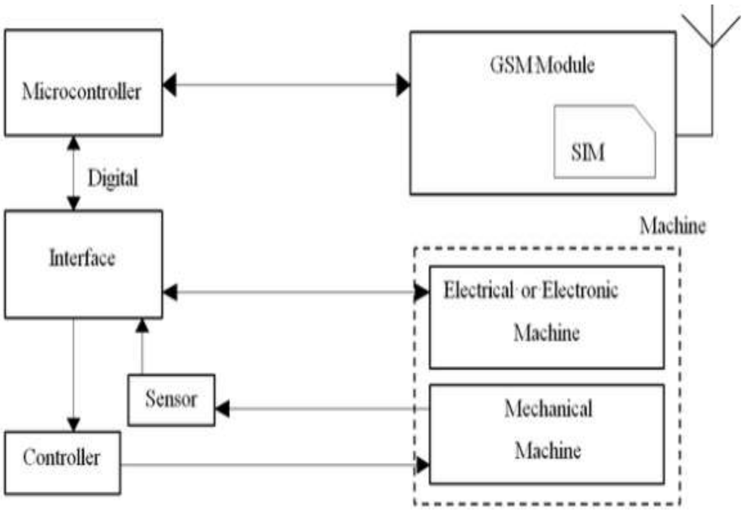
  The work of H. Kanma et al. [7] also proposes a home automation system using Bluetooth that can be accessed remotely through GPRS. The paper discusses controlling and updating home devices along with fault detection and diagnostics remotely. The work also talks about providing an electronics user manual on the phone using Bluetooth and Internet.

  Issues of using Bluetooth
  1. Bluetooth has a maximum communication range of 100m in ideal conditions. More may be needed in a home environment.
  2. Bluetooth communication has comparatively high power consumption, so the batteries of devices need to be frequently recharged or replaced.
  3. Bluetooth technology has advanced and improved to Bluetooth Low Energy (BTLE), which provides the same range of communication. However, it has serious security concerns such as eavesdropping and weak encryption as discussed by M. Ryan [8].
  4. Bluetooth communication should only be used on occasions where there is a need for quick short-lived network communication with little concern for security.

Bluetooth looks like an attractive communication technology for creating smart homes. Bluetooth is cheap, easy, and quick to set up. People are already familiar with the technology. The hardware required for establishing

Bluetooth communication is readily available and the technology also provides the necessary bandwidth for the operation in a home.

- **GSM or Mobile-based Home Automation System**



Mobile based home automation is attractive to researchers because of the popularity of mobile phones and GSM technology. We mainly consider three options for communication in GSM, namely SMS-based home automation, GPRS-based home automation, and Dual Tone Multi Frequency (DTMF)-based home automation. Each of these three technologies is discussed below, along with their shortcomings.

The figure above is from the work of A. Alheraish [3]. It shows the logical diagram of how a home's sensors, electrical, and mechanical devices interact with the home network and communicate through the GSM module using a Subscriber Identity Module (SIM). The system converts the machine functions into electrical signals through a transducer, which goes into a micro-controller. A transducer converts physical quantities like sound, temperature, and humidity into some other quantity like voltage; here, a sensor does that function. For electronic devices, their reading goes directly into the micro-controller. The micro-controller analyses these signals and converts them into commands that can be understood by the GSM module. Based on the received commands, the GSM module selects the appropriate communication method (SMS, GPRS or DTMF).

- **SMS-based Home Automation System**
  The work of A. Alheraish [3] proposes a home automation system using SMS. The proposed system detects illegal intrusions at home and allows legitimate users to change the passkey for the door and control lights in the home. The illegal intrusion into the home is identified by monitoring the state of the home door, which is done using Light Emitting Diode (LED) and infrared sensors. The passkey to the door can be any 4 digits, which can be set either by using the keypad or by using SMS from a registered user's mobile number. A user can control the lights in their home remotely using SMS from their registered mobile number; by turning the lights on in different rooms at random intervals of time, one can give the impression that the home is occupied, even when it is not.

The work of M.S.H Khiyal et al. [9] proposes an SMS-based home security system called SMS-based Wireless Home Appliance Control System (HACS). In their work, a homeowner can control their home using SMS messages from a preset registered mobile number. If the SMS is not from a legitimate mobile number, the system ignores the message. In the case of an intrusion, the appliance control subsystem and security subsystem in the proposed system informs the owner through SMS.

The work of U. Saeed et al. [10] also proposes an SMS-based home automation system. The system has a Java application running on the phone. Legitimate users can log in to the application using their username and password and can select the building/floor/room/device that they wish to remotely control along with an appropriate action from the list of available user actions. The Java application will compose the appropriate SMS message and send it to the home's GSM modem. The GSM modem will receive the SMS message, decode it, and pass it to the home network to perform the action specified. The researchers use a 4-digit passkey and facial recognition for security.

In the work of A.R Delgado et al. [11], GPRS communication is used as a backup for an Internet-based home automation system. This adds to the fault tolerance of the system. The homeowner will be able to get alerts on their mobile phone about the unusual state changes in the sensors. The user could then react either by messaging or using a web interface. In any case, there will be two possible ways to access the home, so if one fails the user can rely on the other.

Security concerns about SMS-based home security systems:

1. The 4 digit security passkey (used by A. Alheraish [3] and U. Saeed et al. [10]), in itself, proposes a security vulnerability. An attacker could wait outside the home and peep through the window to learn the passkey. One can't expect the owner to be careful every time he or she enters the passkey. The user punches in the passkey routinely, so the probability of the user being careless is high.
2. The passkey used in the work of U. Saeed et al. [10] is different for each individual at home, which improves the odds of hacking the keypad. Moreover, these passkeys are chosen by users who are vulnerable to social engineering and other hacks.
3. Most of the proposed systems don't consider sophisticated attackers or are no match for a sophisticated attacker. The systems don't consider any other entry points into the home apart from the front door. The LED and IR sensors used by A. Alheraish [3] to identify intrusions could easily be spoofed by a sophisticated attacker.
4. Informing the homeowner about an intrusion at home through an SMS message is never a good practice. Users may not frequently check their phones for SMS messages, or may not be near enough to the phone to hear a message received tone, so they could easily miss the intrusion alert.

Simple facial recognition systems could be hacked using a photograph of an authorized person, as the system can't distinguish between a picture and a real human.

- **GPRS-based Home Automation System**
  There are a lot of home security systems implemented using GPRS. Most systems use the word security in the traditional sense, and only address the threat put forth by old fashioned intruders in the home.

Researchers M. Danaher and D. Nguyen [2] propose a home security system using GPRS. The work uses a webcam to stream video and pictures of the home to its owner's mobile through GPRS. The webcam detects movement by comparing frames for differences, including light intensity. Video streaming of the proposed work is done using the home Internet connection, not the GSM modem.

U. Ali et al. [12] proposes another home and office automation system using GPRS in mobile phones. The user interacts with the home via a client/server architecture implemented at home using a PC and a micro Java application. Home devices are controlled by a device controller, which is connected to the PC's parallel port. The proposed system allows users to remotely control and inquire the status of the devices that are connected to the device controller.

The researchers J. Jin et al. [13] discuss a home automation system based on WSNs and GPRS. It allows it, users, to control equipment in their home, and collect data about a device's status and weather conditions at home through their mobile devices. The authors' custom-made the application for China, as users receive information about home intrusions and fire through the Chinese Instant Message Mobile Service. Unlike other GPRS-based home automation, the proposed system uses an embedded system-based central controller.

Researchers S.R. Das et al. [14] developed an iOS-based home automation security system using GPRS. The proposed system uses the client/server model for communication. The authors develop an iOS application that runs on a user's mobile phone and acts as the client and the cloud to which the home devices are connected acts as the server. The authors use video cameras, microphones, and motion sensors for providing security at home. When a motion sensor is triggered, the video cameras in the vicinity start to record. A user can view these live feeds on a mobile device through GPRS. The proposed system can also be accessed using a web browser.

Security concerns in GPRS-based home security systems:

1. The works of M. Danaher and D. Nguyen [2], S.R. Das et al. [14] both implement cameras at home. Streaming live video feeds over the Internet is never a good idea, especially when it is from inside the home. If these implemented cameras are compromised, then the attacker will have an eye inside the home. Moreover, people do not like to be watched; it affects their normal behaviour and makes them uncomfortable.
2. Video feeds could be looped by skilled attackers if the cameras and the system are not installed and maintained properly.
3. In a GPRS-based intrusion detection system, the user will have to monitor his or her phone constantly to successfully defend against intrusion.

Researchers S.R. Das et al. [14] provide users access to the home using a web browser, which opens the home to a different set of browsing-related security issues like session hijacking, cookie stealing, and cross-site scripting.

The work of M. Danaher and D. Nguyen [2] provides limited security, as they only use cameras and no other security mechanisms.

- **Internet-based Home Automation System**
  Internet or IP protocol-based communication in home automation systems is always a popular choice among researchers. The Internet is easily scalable, flexible when it comes to access and use, and very popular as a communication method in today's world, so the hardware and the network required for access is readily available, offers high bandwidth and very low communication cost, and devices can connect to and disconnect from the network easily.

These are some of the features that make the Internet such an attractive choice for researchers. Utilising the Internet as a means to access and control the home seems to be the next logical step forward for home automation systems.

From an end user's point of view, using the Internet to access their home is easy, convenient, cheap, flexible, and offers no complication of an added technology to learn. User interface devices like laptops, smartphones, PCs, and tablets are easily available in the market, and these devices are already a part of people's daily lives. So, incorporating home automation into these already-popular user devices seems to be the natural progression.

In most Internet-based home automation systems, a username and password seem to be the only authentication method used.

This raises some security concerns:

1. People are generally careless in nature. They tend to write complicated passwords and usernames on paper near their workstations or underneath their keyboards, thinking "who bothers to look there?"
2. People often repeat the same passwords and usernames on different websites and forums. This behaviour makes them vulnerable to phishing attacks.
3. During the course of time, a homeowner will have to log in to the home from different networks like from the office, from their friend's house, from public Wi-Fi networks such as coffee shops, even parks, sometimes using untrusted devices. The network chosen by the user to access the home may be vulnerable. This could result in the user being exposed to a variety of attacks like man-in-the-middle attacks. Moreover, when accessing the home from a compromised device, legitimate user credentials could be stolen by the use of simple software tools such as a key logger.
4. Researchers should also be aware of the human factor when depending only on passwords for security. The human factor means normal people tend to choose passwords that have some sort of significance to them like their pet's names, the name of their favourite movie, music artist, sports team, etc. Moreover, we should never underestimate the most powerful hack of all, social engineering, which could prove to be very effective when trying to obtain a person's password and username.

Accessing a home through a web browser opens the home up to a variety of browser-related security issues mentioned earlier. Researchers have to assume that when accessing their home over the Internet, people will choose convenience over security if given the choice.

FUTURE WORK

Our work focuses on the study of the security aspect of existing home automation system and find out the flaws. This paper shows pros and cons of existing home automation system. For future work in home automation system we are are focusing on making home automation system more robust and economical. We can develop techniques that can analyse user behaviours and can predict and analyse the result to identify and prevent intrusion.

ACKNOWLEDGEMENT

The authors would like to thank the publishers, researchers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure support. Finally, we would like to extend heartfelt gratitude to friends, family members.

REFERENCES

1. A. ElShafee, K. A. Hamed, "Design and Implementation of a WiFi Based home automation System," World Academy of Science, Engineering and Technology, vol. 6, 2012.
2. M. Danaher, D. Nguyen, "Mobile Home Security with GPRS," in proceedings of the 8th International Symposium for Information Science, Oct. 2002.
3. A. Alheraish, "Design and Implementation of Home Automation System," IEEE Transactions on Consumer Electronics, vol. 50, no. 4, pp.1087-1092, Nov. 2004
4. Michelle L. Mazurek, "Access Control for Home Data Sharing: Attitudes, Needs, and Practices," in CHI'10 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 645-654, 2010.
5. K. Atukorala, D. Wijekoon, M. Tharugasini, I. Perera, C. Silva, "SmartEye - Integrated solution to home automation, security, and monitoring through mobile phones," Third International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST '09, pp. 64-69, Sep. 2009.
6. N. Sriskanthan, F. Tan, A. Karande, "Bluetooth based home automation system," Microprocessors and Microsystems, Elsevier, vol. 26, pp. 281-289, 2002.
7. H. Kanma, N. Wakabayashi, R. Kanazawa, H. Ito, "Home Appliance Control System over Bluetooth with a Cellular Phone," IEEE Transactions on Consumer Electronics, vol. 49, no. 4, pp.1049-1053, Nov. 2003.
8. M. Ryan, "Bluetooth: With Low Energy comes to Low Security," WOOT'13 Proceedings of the 7th USENIX conference on Offensive Technologies, pp. 4-4, 2013.
9. M. Sikandar, H. Khiyal, A. Khan, E. Shehzadi, "SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security," Issues in Informing Science & Information Technology, vol. 6, Jan. 2009.
10.U. Saeed, S. Syed, S.Z. Qazi, N.Khan, A. Khan, M. Babar, "Multi-advantage and security based home automation system," 2010 Fourth UKSim European Symposium on Computer Modeling and Simulation (EMS), pp.7-11, Nov. 2010.
11. A. R. Delgado, R. Picking, V. Grout, "Remote-Controlled home automation systems with Different Network Technologies," Centre for Applied Internet Research (CAIR), University of Wales, 2009.

12. U. Ali, S.J. Nawaz, N. Jawad, “A Real-time Control System for Home/Office appliances automation, from the mobile device through GPRS network,” 13th IEEE International Conference on Electronics, Circuits, and Systems, ICECS '06, pp. 854-857, 2006.
13. Jian-she Jin, Jing Jin, Yong-hui Wang, Ke Zhao, Jia-jun Hu, “Development of Remote-Controlled home automation system with Wireless Sensor Network,” Fifth IEEE International Symposium on Embedded Computing, SEC '08, pp. 169-173, Oct. 2008.

14. S.R. Das, S. Chita, N. Peterson, B. Shirazi, “home automation and Security for Mobile Devices,” IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 141-146, 2011.