GSJ: Volume 10, Issue 9, September 2022, Online: ISSN 2320-9186

www.globalscientificjournal.com

A Generic Tool For Auditing Smart Homes From A User Perspective

Metto S. Kimutai [1], Omieno K. Kelvin[2] and Ondulo M. Jasper[1]

Masinde Muliro University of Science and Technology, Kakamega, Kenya,

Kaimosi Friends University College, Kaimosi, Kenya.

Contact: ksmetto@gmail.com

Abstract

With the rapid development of information technology and the increasing popularity of information and communication technology, the information age has come. There are many characteristics of a smart home but key of them is the ability to obtain information from the environment and respond accordingly. However, little work has studied ways in which smart home users can do evaluation of their own homes. Vendors have developed large-scale information system for smart homes which should is a concern in audit work. The objective of this paper is to develop a tool that can help any user to evaluate their homes before, during and after leaving a smart home with an objective to promote awareness and personal safety. It extracts some actionable activities from existing security models of auditing and best practices for conducting security audits of Internet of Things devices. The paper provides a tool to use in ensuring all devices installed in the smart home have control features, access controls provide confidentiality, authentication and authorization, which is comprehensive and effective. This tool is part of the effort to make more audits in smart homes easier and understandable to the users on what needs to be addressed. The paper also identifies some challenges that is often the decision of devices when there are false positives and false negatives.

Keywords: Security, Auditing, Smart homes

Introduction

The development of innovative technologies that have artificial intelligence within them is a normal occurrence currently in technological developments. This has led to development of smart devices and incorporated into almost every aspect of life. Smart homes have not been left behind in this development too. A Smart Home is a living environment with an objective of comfort living, life safety, efficiency of consumables and security. Smart homes therefore incorporates the appropriate technology within them to support achievement [1]. The key characteristics of a smart home is the ability to obtain information from the environment and respond accordingly [2]. These smart homes support desirable features, such as voice-controlled lights and remote-controlled door locks, but they also raise new security and privacy risks [3]. There are risks that are inherent to the structures and therefore a way of providing assurance to the inhabitants of these homes is required.

As part of providing assurance to home occupiers over information systems in smart homes it is cautious that audit activities be carried out to evaluate risk exposures and contemplate the adequacy of controls related to living in these smart homes.

Information Systems audit in smart homes involves assessing the control environment with an objective of making stakeholders more aware of the risks accompanying the use of smart devices.
Auditing is a favourable solution that has been practiced successfully in other domains. However, auditing of Internet of Things devices is a challenge due to the fact that manufacturers implement a high-level security recommendation provided by standards and best practices and are not readily applicable to auditing data found in the low-level device such as sensor readings, sensor configurations and logs [4]. The outcome will be a more robust security control being put in place.

BACKGROUND AND RELATED WORK

Risks related to smart devices used in smart homes can be categorized as either compliance, privacy, physical security, or information security [5]. The heterogeneous nature of IoT devices and their domains increase the complexity of the audit procedure. The heterogeneity requires integration of security policies, collection, classification and interpretation of audit data and following appropriate audit procedures [6].
For audits in smart homes to be successful, the adopted approach is to assess risks and controls associated with smart devices as other technologies emerge and as the assortment of devices increase in number and complexities [4]. Home users are conscious of possible security and privacy issues but may not largely concerned, for those who take a personal initiative of ensuring they have control over their devices, tensions may arise between many residents in a smart home [3]. Previous research on end users of smart homes has mostly focused usability matters, such as installation, inspirations and use cases, and the interfaces for control and automation [7].
Security Risks in Smart Homes in smart homes include:- the risk of personally identifiable information which is increasingly being stored on a smart devices, Technical Risks such as connectivity disruptions either wireless or cellular networks, Power failures, changes in human resources, leaving security features on default settings, Device vendors and manufacturers may also share data collected through their devices and apps, Devices are accessible through online connections, there is also a large number of devices that lack authentication or encryption [8]. All these issues need to be taken care of when evaluating the security posture of a smart home.

Methodology

The approach here is to give the home user or owner an idea of what he is engaging in when moving into a smart home on matters security and privacy. This first step in this security auditing methodology is to identify the areas which are of interest as an information systems auditor in a smart environment such as a home. The second step is to establish a bridge between policy in information systems security and best practices which leads to the development of a list of areas which need to be addressed in each of the identified areas. The next step is to develop a tool that will cover all areas in the smart home hence inform the approximate level of information security in the home. The design of the tool is subdivided into three sections:- before occupation, when living in the smart home and while relocating or leaving.

The Tool For Auditing

Some of the audit objectives derived from the tool include but not limited to:-
Ensuring all devices installed in the smart home have control features, access controls provide confidentiality, authentication and authorization. This should be comprehensive and effective. The controls should provide reasonable assurance that the smart home processes actions and output which is complete and accurate.

		Yes	No	N/A
Hardware Installation				
1	Is there a comprehensive list of all connected devices to the home? • Access points • Smoke detectors • Connected access door locks • Water systems • Home Appliances (Refrigerator, Washing Machines) • Energy systems • Lighting systems • Security alarms, • CCTV monitoring systems			
2	Is there a documentation of device vendor contacts?			
3	Are there procedures addressing controls on upgrades?			
4	Is there documentation for all hardware and software installed?			
5	Are there any active vendor warranties?			
6	Are there backups for devices data?			
Physical Access				
1	Does the facility allow access for only authorized users?			
2	Are the procedures for issuing one time passwords functional?			
3	Are procedures in place to terminate users who are no longer authorised?			
4	Are there satisfactory procedures for resetting access credentials?			
5	Are access rights classified?			
6	Are there logs in the devices?			
7	Is there a limit for passwords lock out?			
8	Is there a mechanism to report password attempt failure?			
9	Are there procedures if a security violation occurs?			
10	Are there default configuration settings for access?			
11	Is encryption supported by the devices?			
12	Have previous owners (if any) confirmed that they no longer have administrative or user access?			
13	Are there devices that are no longer maintained by vendors?			
Output And Processing				
1	Are devices giving the right responses as programmed? • Smoke detectors • Door locks • Water systems			

	• Home Appliances • Energy systems • Lighting systems • Security alarms • CCTV monitoring systems			
2	Are there adequate controls for data inputs (Limits on inputs, ranges)			
3	Is there a way to reconcile input and output and differences investigated?			
Upgrades				
1	Is there any formal written upgrade policy from vendors?			
2	Is the policy effectively communicated to home owners?			
3	Have all staff been informed of the upgrade procedures?			
4	Are updates from the internet controlled to prevent the virus?			
Internet Access				
1	Is there any proper policy regarding the use within the home?			
2	Does the policy identify the specific assets that the firewall is intended to protect and the objectives of that protection?			
3	Does the policy support the legitimate use and flow of data and information?			
4	Is information passing through firewall monitored?			
5	Is the policy properly communicated to the users?			
6	Is anti-virus inspection enabled?			
7	Is there physical protection of communications lines ?			
Physical Security				
1	Check the safety against fire in the following ways: Are building materials resistant to fire? Are floor and Wall coverings resistant to fire? Is there a separation from risky environments (e.g. Kitchen areas)? Is there a separation from materials prone to fire (e.g. paper, fuel)? Is there a smoking area if need be? Are there fire resistant safes (e,g for documentation storage)?			
2	Check the appropriate arrangements of fire detection devices: Are the smoke detectors placed strategically? Are fire alarm systems linked properly? Are there portable extinguishers? Is it easy to access fire extinguisher services? Are there fire instructions which are clearly posted? Incase of fire emergency, what is the order of alert? Are fire alert and alarm buttons visible? Is there an emergency power-off procedure? Is there an evacuation plan incase of a fire dissaster?			

Air Conditioning				
1	Is there a facility for monitoring temperature and humidity Are sensitive parts of the air conditioning facility well protected? IS there a back-up air conditioning tools in place?			
Power Supply				
1	Is there a reliable source of power ?			
2	Is there monitoring of line voltage?			
3	Is power supply regulated?			
4	Do we have uninterrupted power supply in place?			
5	Is there an alternative power supply? (e.g Emergency lighting system)			
Visitor Control				
1	Positive identification is always a requirement for all visitors?			
2	All physical entries logged in and logged out?			
Insurance				
1	Does adequate insurance exist to cover: Equipment? Software and documentation? Storage media? Replacement and associated costs? Loss of data? Interruption of critical systems?			
Disaster Recovery Plans				
1	Is there an all-inclusive contingency plan developed, documented and tested to guarantee continuity?			
2	Does the emergency plan provide for recovery of risky applications if there is a disaster?			
3	Are all recovery plans official and tested to ensure their competence if a disaster occurs?			
4	Are there operations procedures for use of equipment and software back-up?			
5	Has any of the vendors developed and implemented adequate plan maintenance procedures?			
6	Does a facility or device maintenance contract exist?			
7	Are there any priorities set for critical systems?			
8	Are recovery plans regularly tested?			

DISCUSSION

The use of the tool is to collect the data to verify the security levels of the smart home of interest. The focus is on avenues of internet-connected appliances, lighting, sensors, door locks, and other objects designed for the home environment. The use of smart devices in homes exposes home residents to risks, these risks are best isolated in layers of the Information architecture as identified in the tool designed above. Many smart home devices

have inbuilt memories, processing power and energy restrictions which makes them rigid to audit individually. Smart home devices communicate in low level languages which make them difficult to audit effectively. The audit is supposed to cover all aspects including governance of the home, device policies, best practices, standards, procedures continuous user training and awareness, disaster recovery plans, smart device and app management; and data protection. The tool therefore addresses all areas, which will be of concern to the user before occupancy, during occupancy, upgrade processes and during transitions. There are however some areas which will need technical assistance or experience during this audit.

CONCLUSION

In this paper, we presented areas of concern in a smart home which users should be aware of especially before entering into an agreement of smart home occupancy. We have identified areas where users need to pay attention and hence when making a decision it will be based on knowledge and significant risk assessment. This tool is part of the effort to make more audits in smart homes easier and understandable to the users on what needs to be addressed in audit. Despite this, there are areas which may be of concern especially on positive identification of visitors and the decision of devices when there are false positives and false negatives. As such this is still an area which needs further research. Such challenges are very many and focussed in the smart home domains heavily and are also shared on other IoT application spaces.

References

[1] D. L. N. K. Georgios Mantas, "Security in Smart Home Environment," *IGI Globa*, 2010.

[2] S. P. E. A. Davit Marikyan, "A systematic review of the smart home literature: A user perspective," *Elseveier*, pp. 139 -154, 2018.

[3] S. M. a. F. R. Eric Zeng, "End User Security and Privacy Concerns with Smart Homes," in *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).*, Santa Clara, CA, USA, 2017.

[4] T. I. o. I. Auditors, "Auditing Smart Devices: An Internal Auditor’s Guide to Understanding and Auditing Smart Devices," 2016. [Online]. Available: www.globaliia.org. [Accessed 01 June 2022].

[5] A. J. a. P. D. Joseph Bugeja, "On Privacy and Security Challenges in Smart Connected Homes," in *2016 European Intelligence and Security Informatics Conference* , Sweden, 2016.

[6] D. B. &. A. S. Suryadipta Majumdar, "Security Auditing of Internet of Things Devices in a Smart Home," in *IFIP International Conference on Digital Forensics*, 2021.

[7] T. a. C. W. Hargreaves, "Introduction: Smart homes and their users. In Smart homes and their users," *Springer, Cham*, pp. 1-14, 2017.

[8] D. a. H. P. Herrmann, "Basic concepts and models of cybersecurity." In The Ethics of Cybersecurity,," *Springer, Cham*, pp. 11-44, 2020.