A Survey On Improving Home Automation Security by Integrating Device Fingerprinting Into Smart Home

Athira Sankar[1] Lakshmi S [2]
PG Scholar[1], Asst. Professor[2]
[12] Sree Buddha College of Engineering, Alappuzha, India
Dept. of Computer Science & Engineering , Sree Buddha College of Engineering, Pattoor, Alappuzha

---***---

Abstract - Home automation involves automatic control of household features, activity and appliances. A home with an automatic control system is known as smart home. Automation system helps one's home to promote security, comfort and convenience. This paper is a survey on home automation by integrating device fingerprinting. This paper explains the importance of accessing modern smart home over the internet and highlights various security issues with it. The work explains the evolution of device fingerprinting approach and moreover, a two stage verification process for smart home, using device fingerprinting and login credentials, which verifies the user devices as well as the user accessing the home over internet.

Keywords: Home-automation, Device fingerprinting, Login credential

1. INTRODUCTION

Home automation is becoming popular due to its numerous benefits. With the advancement of technology and services, people's expectations of what a home should do or how the services should be accessed at home has changed a lot during the course of time, and so has the idea of home automation systems arises. If we look at different home automation systems over time, they have always tried to provide efficient and convenient ways for home inhabitants. This could be done when an attacker is within the proximity of the homes internal to access their homes. The change in user expectations, advancement of technology, or change of time, the role of a home automation system has remained the same.

A modern Home Automation System must alert and prevent an intrusion attempt in a home. Home Automation based on internet focuses on controlling home electronics devices, whether we are inside or outside home. Home Automation gives an individual the ability to automatically control things around the home.

Device fingerprinting is the collection of information which gives the remote computing devices for the purpose of identification. Fingerprints can be used to identify individual users or devices even when cookies are turned off. Objectives of the work is to successfully identify a device accessing the home over the internet using Device Fingerprinting. The second objective is to identify authorized user even when there are changes in location, browser or other browser specific features.

The third objective is to identify malicious devices, that consisting of fingerprints of those devices that will not be allowed access to home its called blacklist. Finally identify legitimate devices and develop a whitelist consisting of fingerprints of devices that are allowed access to the home. The rest of the paper is organized as follows, Section II discusses the Related Works on device fingerprinting and security issues associated with username and passwords. Section III describes the existing system and Section IV describes the proposed system.

2 Literature Survey

The advancement of technology has contributed to the changing concept of security in modern homes.

Here various home automation methodologies and techniques from a security perspective are discussed[1].Context-aware Home Automation Systems, Central Controller-based Home Automation System, Bluetooth-based Home Automation System, GSM or Mobile-based Home Automation System, SMS-based Home Automation System are the various techniques used for the home automation.
All the systems presented in this paper features to an ideal system for home automation with remote access.

This paper explains [2] generation of a privacy footprint on the Internet. Foot printing (also known as reconnaissance) is the technique for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system. This approach defines edges between the visible nodes, which are the servers that users directly access, and the hidden nodes, which are the servers that are accessed as a result accessing a visible node. Construct a privacy footprint, which monitors the diffusion of information about a user's actions by measuring the number of associations between visible nodes via one or more common hidden nodes. A privacy footprint provides us a basis on which to continue to monitor the diffusion of privacy information.

Ting-Fang Yen et al [3] proposed host fingerprinting and tracking on the web. The work performs a large-scale study to quantify the amount of information revealed by common host Identifiers. Here, this method analyzes month-long anonymized datasets collected by the Hotmail web-mail service and the Bing search engine, which include millions of hosts across the global IP address space. In this setting, compare the use of multiple identifiers, including browser information, IP addresses, cookies, and user login IDs.

This paper [3] demonstrates the privacy and security implication of host-tracking in two context. In the first context the causes of client churn and in the second context how the host tracking can be leverage to improve security.

This paper [4] proposed exploring the ecosystem of web-based device fingerprinting. Here examine web-based fingerprinting. Three popular browser-fingerprinting code providers reveals the techniques that allows websites to track users without the need of client-side identifiers. Among these technique, a commercial fingerprinting examines user's real IP address and the installation of intrusive browser plugins.

Keaton Mowery et al proposed [5] canvas fingerprinting using pixel map. Canvas fingerprint use a black box and white box .A website could render tests to a <canvas>, extract the pixel map. Then use a cryptographic hash to obtain a convenient fingerprint.

Here demonstrated the behavior of <canvas> text and webGL scene rendering on browsers which forms a new fingerprints. The new fingerprint is consistent, transparent to the users.

This paper [6] presents a techniques, remote device fingerprinting. Remote device fingerprinting is used to catalyze the anonymous network traces. This approach renders perfect security. This technique is applied to a number of different goals, ranging from remotely distinguishing virtual honey nets and real networks to counting the number of hosts behind a NAT.

This paper [7] proposes an enabling personalized search over encrypted outsourced data with efficiency improvement. This paper, addresses the problem of personalized multi-keyword ranked search over encrypted cloud data. Here this proposes a two PRSE scheme for evaluating the keyword priority and solved the limitation of the artificial method of measuring.

3. CONCLUSIONS

A smart home automation based on device fingerprinting improves the security. Device fingerprinting is used for fighting fraud on websites. The device fingerprint along with username/password based security enables the verification of user as well as the device used to access the home. This significantly improves home security when they are accessed over the internet.

ACKNOWLEDGEMENT

We are grateful to our project guide and PG Coordinator Prof. Minu Lalitha Madhav for her remarks, suggestions and for providing all the vital facilities like providing the Internet access and important books, which were essential. We are also thankful to all the staff members of the Department

REFERENCES

[1] A.C Jose, R. Malekian, ―Smart Home Automation Security: A Literature Review‖, Smart Computing Review, Vol. 5, No. 4, pp. 269-285, August 31, 2015

[2] B. Krishnamurthy and C. E. Wills, ―Generating a privacy footprint on the Internet‖, Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement, ser. IMC '06, New York, NY, USA, 2006, pp. 65–70

[3] T.-F. Yen, Y. Xie, F. Yu, R. P. Yu, and M. Abadi, ―Host Fingerprinting and Tracking on the Web: Privacy and Security Implications", Proceddings of the 19th Annual Network and Distributed System Security Symposium (NDSS), San Diego, California, USA, 5th February – 8th February 2012

[4] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens, G. Vigna, "Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting", Proceedings of the 2013 IEEE Symposium on Security and Privacy, 2013.

[5] K. Mowery and H. Shacham, ―Pixel perfect: Fingerprinting canvas in HTML5‖, Proceedings of W2SP 2012, M. Fredrikson, Ed. IEEE Computer Society, May 2012

[6] T. Kohno, A. Broido, and K. Claffy,- Remote physical device fingerprinting‖, IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 2, April-June 2005, pp. 93–108.

[7] Z. Fu, K. Ren, J. Shu, X. Sun, F. Huang, "Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement," IEEE Transactions on Parallel and Distributed Systems, Vol. 27, Issue. 9, 2015.