

A Smart Home Automation Security by Integrating Device Fingerprinting

Athira Sankar¹ and Lakshmi S²

¹PG Scholar, ²Asst. Professor

Dept. of Computer Science & Engineering

^{1,2} Sree Buddha College of Engineering, Alappuzha, India

aadhis994@gmail.com¹, lakshmi.rnath@gmail.com²

Abstract: Nowadays home automation systems have become widespread in several industries by playing a vital role in dominating many process-related operations. We live in the world of automation wherein most of the systems have become machine-driven. Home automation involves automatic controlling of home appliances using completely different technologies and controllers over desktops, laptops, smart phones or tablets. 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, AES Algorithm, Device fingerprinting, login credential

I. 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. Identify authorized user even when there are changes in location, browser or other browser specific features. Identify malicious devices, that consisting of fingerprints of those devices that will not be allowed access to home it's called blacklist. Identify legitimate devices

and develop a whitelist consisting of fingerprints of devices that are allowed access to the home. 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.

II. Related works

Home automation systems are attractive target for an attacker, and the challenges faced by a home automation system from the point of view of the homeowner and security engineers. 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 presents in this paper features to possess an ideal system for home automation with remote access.

This paper explains [2] generating 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. Here 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. In this paper 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 this 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.

III . Existing System

The existing system consist of double verification process- device fingerprinting and logging credentials.

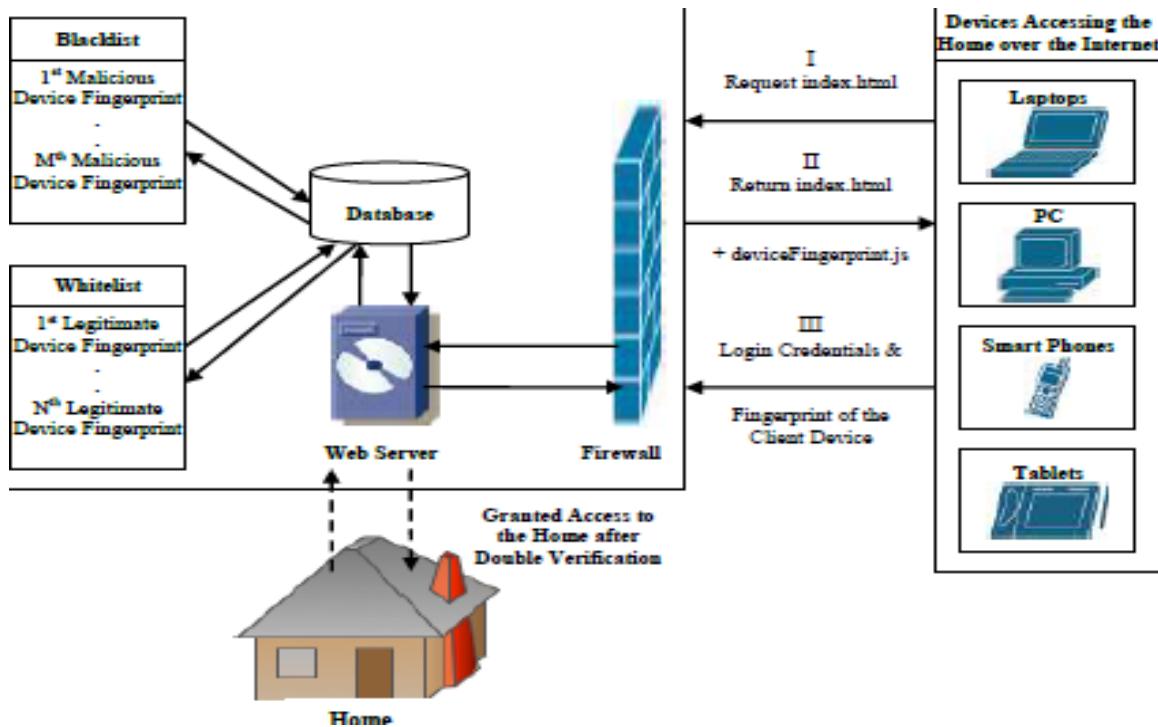


Fig 1: Logical diagram of existing system

Fig.1 shows the Device Fingerprinting process in the existing system. When a user wishes to access the home over the internet, he requests the login page from the server, the server then returns the login page along with the fingerprint. The user provides the login credentials along with the fingerprint of the device he is using. The login credentials are verified, if the verification is passed, then the gathered device fingerprint is being analyzed. There are two fingerprint lists in database, whose entries are accumulated over time. The whitelist is a list of authorized device fingerprints belonging to authorized users. Fingerprints in the whitelist allowed the client to access the home after login credential verification. The blacklist is a list of unauthorized or malicious device fingerprints belonging to potential attackers or intruders who tried to gain access to the home. Fingerprints in the blacklist denied

the access to the home even if the login credentials are correct. If the login credentials are matched and there are sufficient fingerprinting parameters and the Device Fingerprint is not in our 'whitelist' and 'blacklist', then the client should be verified by some other more direct method in order to assure legitimacy. Hash function can be used to encrypt the device fingerprinting parameters to protect against eavesdropping attack or man in the middle attack attempts. The authenticity for fingerprinting can be verified by self-evaluation using Message-Digest algorithm 5 (MD5) checksum.

Device Fingerprint Algorithm

Device fingerprinting parameters mainly include device identification algorithm are —:

User Agent Parameters: These are parameters obtained from Browser name, Browser version, OS name, OS Bits.

Screen Parameters: These are parameters obtained from Screen maximum width, Screen maximum height, Screen available width, Screen available height, Screen color depth, Screen pixel depth, Taskbar position, Taskbar size.

Lesser Bit Parameters: Lesser bit parameters provide very little identifiable information about a client's device.

MIME Parameters: These parameters are obtained from Mime length, Mime type.

Geo-Location Parameters: Geo-Location parameters can be obtained from the client's current latitude and longitude and the country name corresponding to the latitude and longitude obtained from the Google API.

Device Fingerprinting Algorithm

Step 1: Begin

Step 2: Obtain the device fingerprint from the client

Step 3: If at least 7 out of the 9 device fingerprinting parameters are available, then, Step 4 else, Step 10.

Step 4: Analyze and compare each device fingerprinting parameter with the fingerprints in the whitelist and generate the parameter score corresponding to each of the available parameters.

Step 5: Compute the probabilities corresponding to each of the parameters based on the parameter score from Step 4.

Step 6: Analyze each probability score and compute the total probability score corresponding to the client's fingerprint.

Step 7: If (total probability score \geq threshold probability) then, Step 8 else, Step 9.

Step 8: Device Fingerprint match found. Do Step 11.

Step 9: No Device Fingerprint match found, check the blacklist for malicious device's fingerprint match. Contact the user if fingerprint not in the blacklist. Do Step 11.

Step 10: Ask user to enabled JavaScript, Flash and Geo-Location so that parameters for device fingerprinting can be gathered and return to login page.

Step 11: End

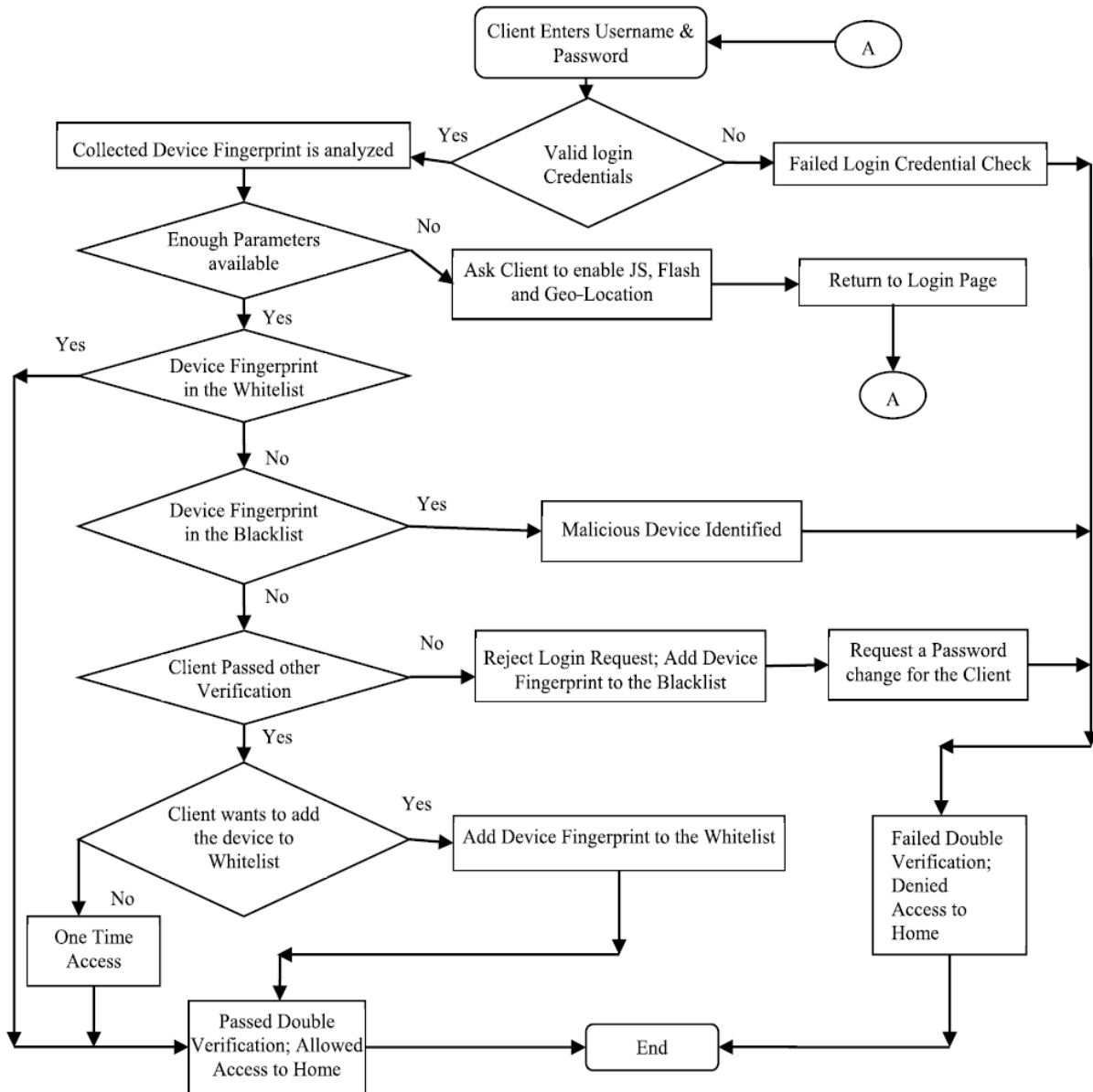


Fig 2: Flowchart of double verification process

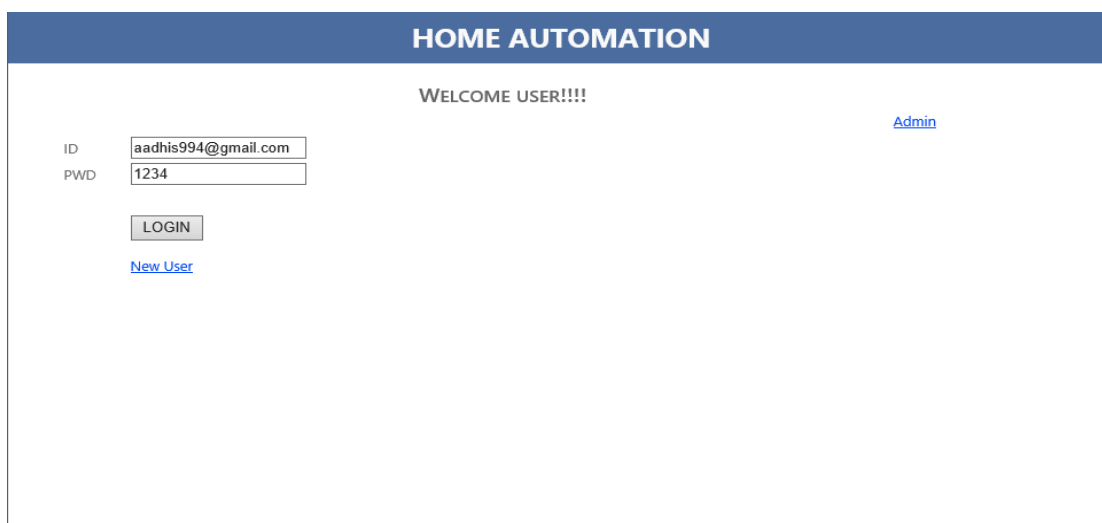
IV. Proposed System

The existing system explains the double verification process- device fingerprinting and login credentials. In the device fingerprinting different parameters are used. Each parameter information are encrypted by hash based algorithm that is an MD5 checksum algorithm is used. The parameter entries stored in a MD5 hash table cannot be enumerated efficiently, but only in some pseudo-random order. Therefore, there is no efficient way to locate an entries. Hash tables become quite inefficient when there are many collisions. To avoid this problem, instead of using AES algorithm can be used.

The advanced Encryption standard (AES) is used in order to protect against unauthorized access and to encrypt this. The cryptographic process key of varying lengths is utilized for this purpose. AES is more secure. AES supports larger key sizes than DESs 112 or 168 bits. AES is faster in both hardware and software. Advanced Encryption Standard not only assures security but also improves the performance in a variety of settings in the home automation. The AES algorithm is designed for home automation systems with security as the primary objective. This work attempts to identify the person operating the device as well as the user access the device in the home. Comparing and verifying different parameters like OS name in user agent string, and screen maximum width and height in Screen parameter helps us to establish the legitimacy of user agent and screen parameters. Moreover, getting the country name from Google API latitude and longitude obtained from Geo-Location. Comparing the country name with the country name in the date object helps us to determine the validity of the date object and time zones. By AES algorithm, device fingerprinting parameter validation is used to defend against parameter spoofing. In the proposed work, user agent, screen parameters, date object and flash parameters are validated, which increases the authenticity of the generated fingerprint.

V. Result

The algorithm successfully identified 97% of the device that access the home. Firstly the client enters the username and the password. Then check for the valid login credentials. If the login credential is true then collected device fingerprint is analyzed, otherwise failed to login. If there are enough parameters available in the whitelist, then passed a double verification process that allowed the client user to access the home. If device fingerprint are available at the blacklist, then a malicious device is identified. So the client passed another verification. After the verification client add it to the whitelist. Then an OTP is send .Double verification process is done. Then the client can access the device in the home.



The screenshot shows a web interface for 'HOME AUTOMATION'. At the top, there is a blue header with the text 'HOME AUTOMATION'. Below the header, the text 'WELCOME USER!!!!' is displayed in the center. On the right side, there is a blue link labeled 'Admin'. On the left side, there is a login form with two input fields: 'ID' containing 'aadhis994@gmail.com' and 'PWD' containing '1234'. Below these fields is a 'LOGIN' button. At the bottom left of the form area, there is a blue link labeled 'New User'.

HOME AUTOMATION

OS PARAMETERS

OS Platform	Win32NT
OS Version	Microsoft Windows NT 6.2.9200.0
OS Name	Windows 10 Enterprise
OS Bit	32 bits.
Screen Maximum width	1366
Screen Maximum Height	768
Screen Current Width	1366
Screen Current Height	728
Screen Color Depth	32
Country Name	
Time Zone	US Eastern Standard Time
Task Bar Location	BOTTOM
Task Bar Size	40
Latitude	
Longitude	

BROWSER PARAMETERS

Browser Name	InternetExplorer11
Browser Version	11.0
Java Script Enabled	True
Flash Enabled	True
Cookie Enabled	True
Local Storage Enabled	
Mime Type	text/html<>application/xh
Mime Length	

SAVE

VI. Conclusion

The device fingerprint along with username/password based security enables the verification of user as well as the device used to access the home, which significantly improves home security when they are accessed over the internet. Unlike any previous approaches to device fingerprinting, AES algorithm which improves the fingerprint accuracy.

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 Web: Privacy and Security Implications”, Proceedings 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, "Cookies 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.