International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Device Fingerprinting for Secure User Enrollment using TEE

Prathamesh Raut[1], Bhushan Patil[2]

[1]M.E CNIS Student, Mumbai University, Rajiv Gandhi Institute of Technology, Mumbai

[2]Assistant Professor, Computer Engineering Department, Mumbai University, Rajiv Gandhi Institute of Technology, Mumbai

Abstract: ***Mobile phone user's access content from web-sites using their browsers and nowadays as the power of mobile devices gone to high level compared to old handsets, every service provider wants to provide their service to users by using various ways. To provide better service, service providers need to know their potential customers and the services in which they are interested. Sometimes tracking without users concern could create security issues. This paper presenting, options for secure user enrollment using device fingerprinting with trusted execution environment. In this paper presenting software-based and hardware based approach with the help of Trusted Execution Environment that would enable the secure and practical enrollment, which could enable more widespread secure deployment of various mobile and web security services.***

Keywords: Device Fingerprinting, Trusted Execution Environment, Secure Enrollment

1. Introduction

If we look back in recent years, then we can say that current mobile devices are much more powerful in the aspect of features they provide. We call today's mobile devices are ‗Smart devices'. Nowadays, our lives are increasingly dependent on smart connected devices. We use them to conduct business, maintain social relationships, make purchases, and enjoy media content. Mobile computing devices such as tablets and smart phones enable a high degree of connectivity and productivity that employees now expect in their jobs and daily usage[5]. There are number of mobile Oss available in the market like Android, iOS, windows, blackberry etc. Recent research provides the following insights: Android has taken a surprising lead as the most common mobile operating system supported for organization-owned devices (at 56%); followed by iOS (41%); Windows Mobile (30%); and BlackBerry (28%). The landscape is changing dramatically in this industry [1], [2]. Every service provider wanted to provide better service to its customer and for that they wanted to know their user. So, to find out user base companies started tracking user by using various techniques like browser fingerprinting, sensor-value etc [3], [7]. There are many components available in mobile devices which can be use to find authenticated device by service providers.

1.1 Device Fingerprinting

With personal identity information, such as credit cards and login passwords now a commodity on the black market, companies need to look to alternative methods for verifying identities and transactions online. This problem is compounded by the fact that fraudsters now routinely evade IP Address Blacklisting and IP Address geolocation tools using proxies. Fingerprinting is a new way of differentiating between a valuable customer and a professional fraudster online. Today, the prevalence of identity theft and hackers has meant that it is much harder to verify that the person you are doing business with is who they say they are. That new customer could be a compromised computer transacting on behalf of a sophisticated eastern European crime gang or an opportunistic thief that has lifted personal details from Facebook. It's clear that online identity verification is a significant challenge and concern to all business owners [4], [3].

1.2 Trusted Execution Environment

Trusted Execution Environment plays very important role in mobile devices nowadays. The TEE provides features which can be used to identify user, store any secret information of user such as private keys, fingerprints etc. The TEE is a separate execution environment that runs alongside the Rich OS and provides security services to that rich environment. The TEE isolates access to its hardware and software security resources from the Rich OS and its applications [2], [4]. TEE guaranties that the sensitive information stored inside it will remain safe, processed and protected in an isolated environment. TEE provides security against the attacks that have been generated in Rich OS. TEE helps to application developers to utilize features of TEE and make applications which does not only satisfy users need but it also guaranty about security.

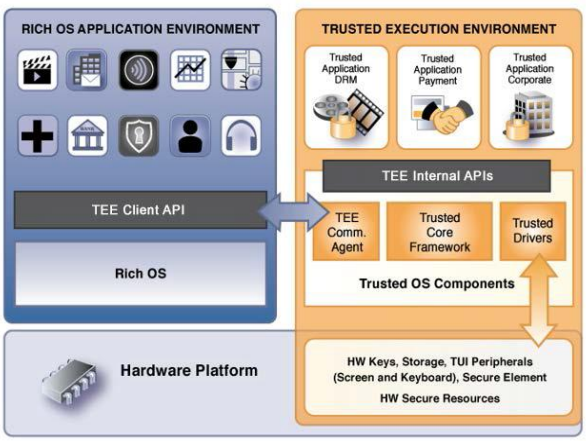

Figure 1: Architecture of TEE [3]

1.3 Benefits of TEE

The TEE is a unique environment that is capable of increasing the security and assurance level of services and applications requiring security, including the following [3]:

- **User Authentication**: Through its Trusted User Interface feature, the TEE makes it possible to securely collect a user's password or PIN code that will then be verified locally, on a remote server, or within a Secure Element. This trusted user authentication can be used to verify a cardholder for payment, confirm a user's identification to a corporate server, attest to a user's rights with a content server, and more.
- **Trusted Processing and Isolation**: Any processing that needs to be executed on a device can be isolated from any untrusted software attack by being run in the TEE; this is possible while still leveraging any of the device's resources. Examples include processing a payment, decrypting premium content, reviewing corporate data, and more.
- **Transaction Validation**: Through its Trusted User Interface, the TEE makes it possible to ensure that the information displayed accurately portrays the application's request—as opposed to displaying misinformation offered by a rogue application. This is useful for a variety of functions, whether validating payment, protecting a corporate document, or other.
- **Abstraction of Usage of Secure Resources**: By using TEE APIs, application developers can easily leverage the complex security functions available from a device's hardware instead of using less safe software functions. Such hardware security resources include hardware cryptography accelerators, Secure Elements, biometric equipment, key materials handling, secure clock, and more.
- **Certification**: Trusted certification is only achievable through standardization of the TEE; an appropriate evaluation scheme improves stakeholder confidence that the security-dependent applications are running on a trusted platform (comprised of the TEE and its underlying hardware) that has been deeply evaluated and certified.

2. Literature Review

Secure enrollment of user is very important as many services like mobile payment; enterprise applications etc. are available on mobile devices. These services are part of daily life for users, which makes it very important for service providers to enroll user securely. There are so many organizations like GlobalPlatform, FIDO alliance etc., also many expertise working on device fingerprinting for secure enrollment of user using TEE. Below table 2.1 shows various work done on TEE for device fingerprinting.

Table 2.1: Comparative Study of TEE

Author Name	*Paper Title*	*Characteristics*
Kari Kostianinen et.al	The Untapped Potential of Trusted Execution Environment on Mobile Devices	Study about TEE and its security features
Claudio Marforio et. al	Secure Enrollment and Practical Migration for Trusted Execution Environments	Use of ARM TrustZone with Software-based approach
Hristo Bojinov et.al	Mobile Device Identification via Sensor Fingerprinting	Using Sensor(Accelerometer)-based fingerprinting
Andreas Kurtz et.al	Fingerprinting Mobile Devices Using Personalized Configurations	Used user's apps and user's music taste to identify user
Vimal K. Khanna	Remote Fingerprinting Of Mobile Devices	Devices unique id, browser, mobile app and its effect on OSI model
P. Eckersley	How unique is your web browser?	Shows difference in browser fingerprinting on PC and mobile devices
Mohamed Sabt et.al	Trusted Execution Environment: What it is, and What it is not	Comparative study on properties and core concepts of TEE

Kari Kostianinen et.al, worked on hardware-based Trusted Execution Environment. Suggested TEE for application developers to improve the security and usability of their applications. Also described why TEE is widely deployed in mobile devices and its capabilities.

Claudio Marforio et.al, suggested use of software-based device fingerprinting. Authors developed mobile application which collects data generated while using application. Also they have discussed about the challenges in identifying mobile devices and argued on the current architecture of mobile devices.

Hristo Bojinov et.al, suggested that, mobile devices comes with many sensors in it. Authors perform operations on Accelerometer specifically. Data collected are analysed carefully and pattern of data is identified. On the basis of pattern gathered from the accelerometer they found out sensor based device fingerprinting. Authors showed the possibilities of device fingerprinting using sensors on smart phones. Sensors can be used to construct reliable hardware based fingerprint of the phone.

Andreas Kurtz et.al, perform analysis and iOS SDK to find out various API available which help applications developers to access various factors of iOS devices. They collect data of users using iOS app developed by them to gather data of devices so user identification can be perform.

Vimal K. Khanna, suggested the concept of remote fingerprinting by various factors using browser and mobile applications and its effect on OSI layer.

P.Eckersley, is the pioneered of browser fingerprinting. He showed the difference of browser fingerprinting on PC/Desktop devices and mobile devices. The results generate the interest in the field device fingerprinting for mobile devices.

Mohamed Sabt et.al did comparative study on TEE and analyzes core properties of TEE. Also discussed some known

attacks on deployed TEE as well as its wide use guarantee security in diverse applications.

3. Conclusion

As the devices are become more and more powerful in terms of computing power, memory and latest mobile processor architecture are responsible for increase in mobile era where everyone, everything wants go mobile. Mobile security architecture such as, ARM TrustZone are widely available in current devices. This provides opportunity for service implementation with high security assurances. This paper highlighted the problem of secure enrollment and practical migration for services that leverage such security architectures. Also, need more open architecture to access TEE environment for developers then only developers can utilize the untapped potential of TEE.

References

[1] Andreas Kurtz, Hugo Gascon, Tobias Becker, Konrad Rieck, and Felix Freiling, ―Fingerprinting Mobile Devices Using Personalized Configurations" in Proceedings on Privacy Enhancing Technologies; 2016(1) : 4 – 19

[2] Mohamed Sabt, Mohammed Achemlal, Abdelmadjid Bouabdallah." Trusted Execution Environment: What It is, and What It is Not." 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Aug 2015, Helsinki.

[3] GlobalPlatform Inc , ―Trusted Execution Environment: Delivering Enhanced Security at Lower Cost to Mobile Market", White Paper , June 2015

[4] Vimal Khanna, ―Remote Fingerprinting of Mobile Devices", IEEE Wireless Communications 22(6):106-113 December 2015

[5] Frank Dickson ―Hardening Android : Building Security into Core Mobile Devices", Secure Networking in Frost & Sullivan , Volume 2, Number 4, May 2014

[6] Claudio Marforio, Nikolaos Karapanos, Claudio Soriente, ―Secure Enrollment and Practical Migration for Mobile Trusted Execution Environments".[Online].Available:https://www.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/publications/pub2013/spsm_marforio.pdf

[7] P.Eckersley, ―How unique is your web browser?" [Online]. Available: https://panopticlick.eff.org/static/browser-uniqueness.pdf

Author Profile

Prathamesh Raut received the B.E. in Information Technology in year 2012 and pursuing M.E. in Computer Network and Information Security from Rajiv Gandhi Institute of Technology, Mumbai.

Bhushan Patil, Assistant Professor in Computer Engineering Department of Rajiv Gandhi Institute of Technology, Mumbai.