2nd National Level Students' Research Conference on
"Innovative Ideas and Invention with Sustainability in Computer Science and IT-2021"
In association with International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

eSIM: Security Aspects for Privacy and Protection of Users

Hrushikesh Walvekar, Mansi Chandak, Anuradha Kanade
Master of Computer Application , (Computer Science), MIT - World Peace University, Pune, Maharashtra, India

ABSTRACT

The developing world needs optimization of hardware components and higher performance of the devices. An innovative idea got implemented in 2012 which also provided additional range and storage benefits. But with advanced technology benefits, there are also cons of using it. The main con of eSIM was hijacking it and tampering it for gaining full access. eSIM has a specific encrypted link to a specific MNO which may give access to hackers to push a new profile in it but this has been already reported by GSMA. The security level of eSIM is as equal as a normal SIM[11][18][22]. The following security aspects have been elaborated in this paper.

Keywords - eSIM, GSMA(Global System Mobile Association), MNO, eUICC, SM-DP, SM-SR.

I. INTRODUCTION

The eSIM technology is an embedded-SIM or embedded universal integrated circuit card (eUICC) which is a form of programmable SIM card, it is embedded directly into a device[8]. eSIMs are re-programmable and can support multiple profiles[2]. eSIM technology provides the same level of security as that of regular SIM, with additional secure over-the-air (OTA) update capability. There is no physical SIM card involved and no physical swapping is required by the individual [21]. eSIM is a global specification by the GSMA which authorizes remote SIM available to any mobile device. GSMA defines eSIM as the SIM for the next generation of connected consumer devices[5]. This specification is used in various applications such as electronics, home IoT applications, industrial (IIoT) applications like smart metering or in logistics[9][19]. eSIM are simply SIM chips embedded in your device instead of having a simple physical SIM card[16]. eSIM can be used for both the consumer solution and Machine-to-Machine (M2M) solution as more capable devices are entering the market[1]. It is the next big thing in the telecommunication world which allows distant deployment of network details and connectivity on the phone containing eSIM [6].

II. EASE OF USING AN ESIM

A. Cell Network Personalization

eSIM enables users to change operators remotely, directly from their phone, without having to purchase a new SIM card, waiting for it to arrive and start functioning, and then inserting it into your phone. You also don't need to hunt for a SIM 'ejector tool' to remove the SIM and to insert the new one [22].

B. Freedom of Switching Network

eSIM allows users to store multiple profiles on a single device, upto five numbers, and switch between them at ease[22].

III. PROS OF ESIM

- eSIM gives instant connectivity. One doesn't need to wait for the new SIM to arrive or install it on the phone. You will be able to do it with just a few taps.
- Giving a range of 5 network options to choose from, eSIM helps users customise, personalise and a sense of freedom.
- In a world wherein thin phones are all the rage, eSIM enables a significant reduction in phone size. The absence of a SIM tray leads to visible physical reduction in size.
- eSIMs are more secure as it is programmed to request verification whenever someone tries to change the user profile [22].

IV. CONS OF ESIM

- E-waste is a global crisis. The concept of eSIM renders older phones waste as it does not work in older models. Thus the new technology creates much more debris and unnecessary waste.
- Data such as contacts are difficult to transfer as you will have to download and reupload that data.
- eSIM can only be used on a single phone. You cannot just take the SIM out and use it on a different phone[24].

V. SECURE ELEMENTS OF ESIM

A. Secured according to design

eSE(embedded Secure element) is a hardware component which is a tamper-proof chip and is available in all designs and sizes for every different device[14]. Security by device is checked by performing penetration testing at both the hardware and software levels. Hackers cannot push any new profile into the current existing profile of the eSIM[13]. Hence tampering of the information of current users cannot be done[13].

B. Trusted execution environment (TEE)

This environment amplifies the security of eSIM which runs on the handset/device memory or has a separate, secure element[3]. The communication is having end-to-end encryption with secure services and it also uses secured interfaces and drivers that link hardware security features to a particular trusted education environment [1].

C. Trusted environment (TRE)

This environment provides RoT(Root of Trust) and hardware security anchor. It contains all the necessary resources that establishes a reliable environment and protects the system behavior for the execution of software, and storage of sensitive data [1].

VI. ESIM SECURITY ARCHITECTURE

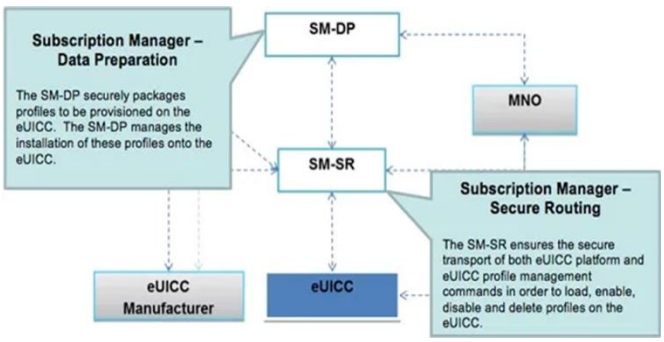

Fig.1. eSim Security Architecture

SM-DP (Subscription Manager-Data Preparation) : It stores,
prepares and protects the operator's profile (including the operator credentials)[10]. It also downloads as well as installs the profile of eUICC(Embedded Universal Integrated Circuit Card)[6][7].

eUICC (Embedded Universal Integrated Circuit Card) : It is a secure element which contains more than one subscription Profiles[6][7].

SM-SR (Subscription Manager-Secure
Routing) : It manages the statuses of the Profiles of eUICC. It secures communication links between eUICC and SM-DP which is used for delivery of the user Profiles[6][7].

VII. SECURITY ASPECTS

The eSIM security aspects are majorly focused by the companies as many frauds are taking place as well as the tampering of the eSIM is done.

eUICC (Embedded Universal Integrated Circuit Card) has an independent security realm. MNO(Mobile Network Operator)[17], SM-DP (Subscription Manager-Data
Preparation) and SM-SR (Subscription Manager-Secure
Routing) also consider the approach of the security realm which is based on the commercial as well as regulatory impact[7][12]. Secure Channel Protocol(SCP) is used for maintaining the security between the eUICC (Embedded Universal Integrated Circuit Card) and the eSIM infrastructure and also provides confidentiality of the messages which have been exchanged[7][8].
Four cryptographic algorithms are used for the security of the eSIM namely:

- Advanced Encryption Standard (AES) - 128 bits.
- SHA-256.
- Elliptic curve (ECC) - 256 bits.
- Rivest Shamir Adleman (RSA) - 3070bits.

WIB(Wireless Internet Browser) which is a SIM toolkit application which allows users to customise dynamic menus for the value added services of that particular subscriber. This process can be done using OTA(Over the Air) messages which are controlled by the central server. This WIB vulnerability is similar to the simjacker[4].

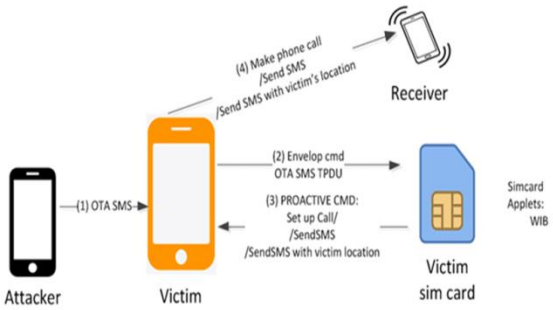

Fig.2. Using WIB(Wireless Internet Browser) for attacking victim

Simjacker exploit which has been fixed 2013 but there are still many eSIM which are non-certified and do not follow the GSMA standards and can be affected. The binary message which is used in eSIM management can be handled without any acknowledgement of the receiver's device/user[15]. Due to this SIM toolkit command gets executed and is sent back to the attacker by using another binary message.

VIII. IS TAMPERING OF ESIM DURING DEVICE REPAIRS POSSIBLE?

The tampering of the hardware can be done when the device is given for repairs as the hardware of the eSIM will carry the information of the user. If that embedded eSIM is replaced by some other hardware then that information could be transferred or swapped just like normal sim card swapping but in this case there would be a hardware swap. The eSIM has eUICC embedded software which has been deployed on the embedded SIM hardware like MFF2 (Machine-to-Machine Form Factor). Once the hardware is ready it can be deployed in any device. So hardware swapping from one device to another can be easily done.

IX. IS IT POSSIBLE TO CAMOUFLAGE ESIM TO HACK USER INFORMATION?

When an attacker takes control of the mobile phone that person can take control of the eSIM signal strengths and could manipulate the users calls. The users might see signals of their mobile operators on their mobile phones but in the background it would have no signal and spoofing of wrong signals could be a possibility. This would create problems for the users while talking on the phones. Also the whole conversations as well as texts would be tracked by the hackers. The attackers/hacker may not be able to swap the eSIM information but could manipulate the eSIM by re-rooting the phone softwares.

X. CAN ESIM HARDWARE BE TAMPERED BY UPGRADING IT?

As the eSIM is embedded in the SIM hardware like MFF2 (Machine-to-Machine Form Factor) it could be changed by anybody. The information will not get deleted even if the eSIM hardware is changed by any repairer. Afterwards this information could be accessed by installing this hardware into some other device which will have the same device compatibility.

XI. SOLUTIONS

The eSIM hardware should be given a security code, once a user information gets registered in it. This will help in securing the information of the user even though the hardware is changed or swapped. Secondly the hardware should only accept the manufacturer's software updates and not any third-party updates. If any third party updates are taking place in the eSIM software then it should get locked.

XII.CONCLUSION

After observing the possibilities, causes and solutions we can conclude that the security of the eSIM is a major factor. eSIM tampering can be done in many ways and the solutions which are suggested can be implemented with a possibility of being successfully. There may be many more ways for saving the eSIM from leaking user's information and the hardware as well as the software part of the eSIM could be more sophisticated to break through its security in order to prevent frauds and thefts of the bank information which is connected to that particular eSIM phone number.

ACKNOWLEDGMENT

Dr. Shantanu Kanade: Help in Domain knowledge, Paper writing & review, Dr. Anuradha Kanade and Dr. Barnali Goswami: Help in paper review, help in paper formatting.

XIII. REFERENCES

[1]. Evolution of the SIM to eSIM by Elaheh Vahidian in 2013.
[2]. eSIM IoT Integration for IoT Devices by Mikaël DUBREUCQ – Director, Global Strategic Marketing.
[3]. Analyzing trusted elements in mobile devices by Saurabh Kulkarni.
[4]. Threats and Protection on E-Sim by Threats and Protection on E-Sim by Alex R Mathew.
[5]. E-SIM for consumers—a game changer in mobile telecommunications? by Markus Meukel, Markus Schwarz, and Matthias Winter.
[6]. eSIM on IoT : An Innovative Approach Towards Connectivity by Ms.Sayali Krishna , Mr. Bhaskar Mondal and Ms. Surabhi Thatte.

[7]. M2M embedded subscriber identity module provisioning in networks without SMS service by Ken-Tristan Peterson.
[8]. Accelerate celular IoT deployment with eSIM, ARM Limited 201 , whitepaper.
[9]. Securing solutions Ensuring your peace of mind, life.augmented, whitepaper.
[10]. eSIM, Whitepaper, 2018.
[11]. eSIM: The Global Market Report, whitepaper, 2019.
[12]. Kigen-How-Remote-SIM-Provisioning-Works-ebook, whitepaper.
[13]. SIMs, eSIMs and Secure Elements, whitepaper, www.simalliance.org.
[14]. https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/secure-elements/embedded-secure-element, 6 Feb 2021, 13:20 IST.
[15]. https://mobile-security.gi-de.com/esim 6 Feb 2021 13:20 IST.
[16]. https://hellofuture.orange.com/en/how-increasing-the-confidence-in-the-esim-ecosystem-is-essential-for-its-adoption/ 6 Feb 2021 13:20 IST.
[17]. https://www.gi-de.com/en/spotlight/connectivity/esim-technology-applications 6 Feb 2021 13:20 IST.
[18]. https://www.truphone.com/us/about/newsroom/how-safe-is-the-esim/ 6 Feb 2021 13:20 IST.
[19]. https://www.fiercewireless.com/tech/could-esim-technology-make-your-smartphone-less-secure 6 Feb 2021 13:20 IST.
[20]. https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/secure-elements/embedded-secure-element 6 Feb 2021 13:20 IST.
[21]. https://www.forbes.com/uk/advisor/mobile-phones/esims/ 6 Feb 2021 13:20 IST
[22]. https://www.usmobile.com/blog/esim/ 6 Feb 2021 13:20 IST
[23]. Fig.1. eSim Security Architecture : https://i0.wp.com/www.gsma.com/esim/wp-content/uploads/2019/08/sim1.jpg?w=590&ssl=1.
[24]. https://www.twilio.com/blog/what-is-esim 12 Feb 2021 17:15 IST.
[25]. Fig.2.Using WIB(Wireless Internet Browser) for attacking victim https://thehackernews.com/images/-wDLPnOEOjik/XY5Yv_wLctI/AAAAAAAA1PA/jh8nreQjdrQPsANIk2SQB2Br8Ig0JcoOwCLcBGAsYHQ/s728-e100/sim-browser-toolkit-simjacker-vulnerability.png 18 Feb 2021 20:49 IST