Attacks against GSMA's M2M Remote Provisioning

Maxime Meyer[1,2], Elizabeth A. Quaglia[2], and Ben Smyth[3]

[1] Vade Secure Technology Inc., Paris, France
[2] Information Security Group - Royal Holloway, University of London, UK
[3] Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg

Abstract. GSMA is developing and standardizing specifications for embedded SIM cards with remote provisioning, called eUICCs, which are expected to revolutionize the cellular network subscription model. We study GSMA's "Remote Provisioning Architecture for Embedded UICC" specification, which focuses on M2M devices, and we analyze the security of remote provisioning. Our analysis reveals weaknesses in the specification that would result in eUICCs being vulnerable to attacks: we demonstrate how a network adversary can exhaust an eUICC's memory, and we identify three classes of attacks by malicious insiders that prevent service. We disclosed our findings to GSMA; GSMA confirmed the validity of these attacks and acknowledged their potential to disrupt the cellular industry. We propose fixes, which GSMA is incorporating into its specification. Thus, we improve security of next generation telecommunication networks.

1 Introduction

Machine to Machine (M2M) devices (i.e., machines communicating together without human intervention) are ubiquitous. Some of these devices communicate using cellular networks. To access such networks, a device authenticates using an embedded SIM, which is issued by a Mobile Network Operator (MNO). Authentication is established with the AKA protocol [4]. AKA algorithms and keys are embedded in SIMs, which physically ensures their confidentiality and integrity. Limitations of SIMs include being neither re-programmable (hence, restricted to a *single* subscription during their lifetime) nor remotely personalizable (hence, installation requires physical access).

ETSI [6] specified requirements for re-programmable and remotely personalizable embedded SIMs to overcome the aforementioned limitations. Following ETSI's specification, industrial researchers, e.g., [2, 7, 17], and academic researchers, e.g., [20], proposed remote provisioning schemes. Moreover, building upon ETSI's specification and GlobalPlatform's smart card standard [8], GSMA released a specification for a next generation SIM, namely, an *embedded UICC*, which supports multiple operators simultaneously. Profiles are remotely provisioned and installed into eUICCs. For M2M devices, remote provisioning proto-

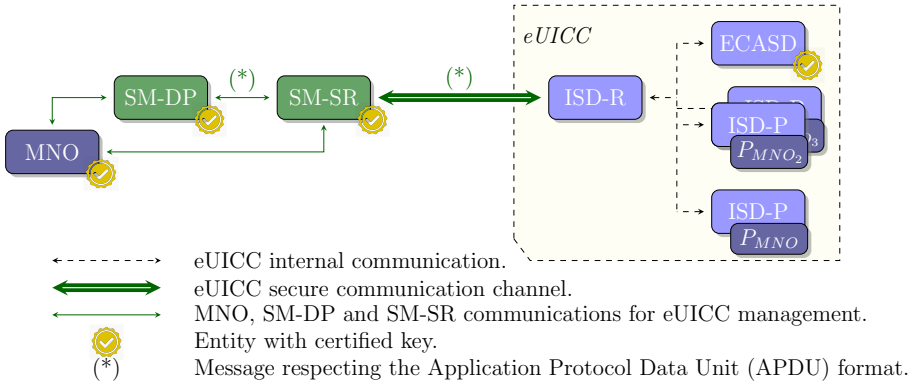

Fig. 1: Remote provisioning interfaces and communication channels, adapted from [18]

cols and management mechanisms are described by GSMA's *"Remote Provisioning Architecture for Embedded UICC"* specification [12].[1] (We adopt GSMA's terminology for consistency with their specification.)

Unlike SIMs, which are restricted to a single subscription from a single operator, eUICCs support multiple subscriptions and multiple operators. Subscriptions are defined by *Profiles* (P_{MNO} in Fig. 1), which encapsulate subscription data. Each profile is stored inside a separate *Security Domain* (ISD-P in Fig.1) and an interface (ISD-R in Fig. 1) is defined for communication between ISD-Ps and remote entities. Authentication of that communication is managed by an application (ECASD in Fig. 1). Internal communication between eUICC components exploits the underlying GlobalPlatform framework, which is reliant on the Application Protocol Data Unit (APDU) message format.

Remote provisioning is a core aspect of GSMA's specification. Motivated by business cases [11, §3], GSMA introduces Subscription Managers which act as intermediaries between operators and eUICCs. Subscription managers are separated into two roles: Data Preparation roles (SM-DPs) oversee eUICC profile formatting and installation, they may be controlled by an individual operator; and Secure Routing roles (SM-SRs) oversee remote eUICC management, they may be operated by an independent organization, e.g., a regulator.

GSMA is promoting their specification for standardization [23, 10]. Any weakness or flaw in the specification or subsequent standard could have disastrous consequences on the secure deployment of eUICCs. As such, security of remote provisioning must be analyzed. Indeed, finding and fixing specification flaws is paramount, because the cost of fixing problems increases exponentially once production commences.

Contribution & Structure. We study version 3.1 of GSMA's M2M remote provisioning specification and present the first analysis of remote provisioning. Our

[1] Meyer, Quaglia & Smyth provide a detailed introduction to GSMA's specification [18].

analysis reveals flaws which would make eUICCs vulnerable to attacks and we present fixes to eliminate those flaws. We proceed as follows: Section 2 describes creation of a profile and its associated security domain Section 3 presents a memory exhaustion attack against eUICCs. The attack works by dropping an acknowledgement message sent during ISD-P creation, which causes the creation of an empty and undeletable ISD-P, and can be repeated to exhaust an eUICC's memory. Section 4 presents attacks by malicious insiders that exploit remote management messages to prevent operators from installing new profiles on eUICCs. Section 5 shows how a malicious operator can lock an eUICC to their profile and block other operators. Section 6 documents our disclosure of the aforementioned attacks to GSMA and explains how GSMA is revising its specification.

2 Preliminaries

2.1 Profile Download and Installation

GSMA's eUICC specification defines a remote provisioning procedure, called `Download&Install`, which transmits profiles from an operator to an eUICC, and installs them. The procedure can be summarized as follows (see Fig. 2):

1. An operator initiates the process with a `DownloadProfile` request to an SM-DP containing a profile description (e.g., profile size, network capabilities).
2. The SM-DP uses the `GetEIS` function to obtain data about the target eUICC, including mutable (e.g., remaining memory, SM-SR identifier, installed profiles description) and immutable (e.g., production date, platform version) information about the eUICC. The SM-DP checks the validity of the profile description against the characteristics of the eUICC and creates a profile according to the operator's profile description.
3. The SM-DP makes a `CreateISDP` request to the SM-SR responsible for the target eUICC (procedure `CreateISDP` detailed in §2.2). The SM-SR receives the request (labelled 3a in Fig. 2) and creates an ISD-P on the eUICC to hold the profile (labelled 3b).
4. The SM-DP establishes a secure channel with the ISD-P (labelled 4a), and sends the profile to the ISD-P over that channel (labelled 4b).
5. The ISD-P installs the profile, and relays acknowledgments to the operator.

2.2 ISD-P creation

ISD-P creation (Step 3 in §2.1) precedes the upload of the profile onto the eUICC. At the end of this phase, the profile container's unique application identifier (`ISD-P AID`) has been set, and memory has been reserved for the future profile onto the eUICC. The creation proceeds as follows (see Fig. 3):

1. The SM-DP sends a `CreateISDP` request to the SM-SR containing the following payload: the identifiers of the target eUICC and the operator that requested profile creation, along with memory requirements.

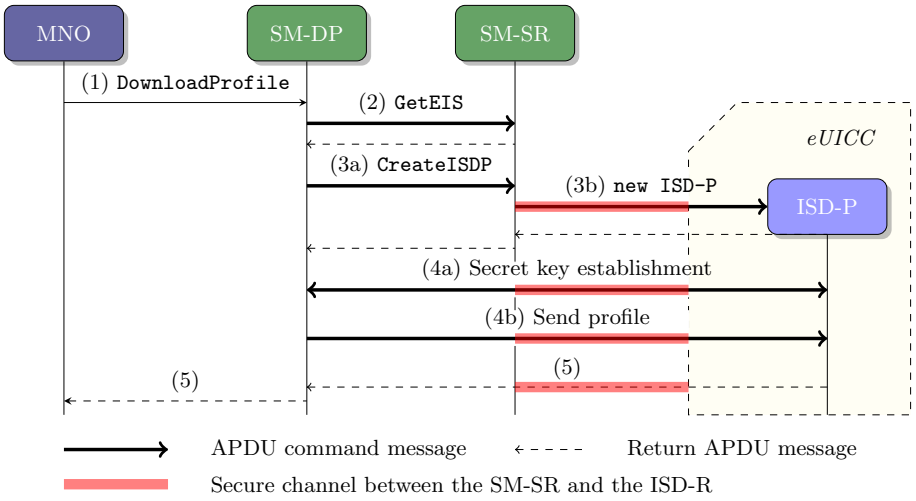

Fig. 2: Profile download and installation flow (high level)

2. The SM-SR establishes a secure channel with the eUICC, via its ISD-R interface.
3. The SM-SR instructs the ISD-R to create an ISD-P, specifying its creation parameters (e.g., ISD-P identifier (AID), profile size, etc.).
4. The command is processed by the smart card (labelled 4a in Fig. 3) which creates the ISD-P (4b) and returns (4c).
5. The ISD-R reports the success of the ISD-P creation to the SM-SR.
6. The SM-SR updates the eUICC Information Set (EIS) file.
7. Finally, the SM-SR returns the ISD-P identifier to the SM-DP.

3 Memory exhaustion attack by network adversary

We analyzed the security of GSMA's remote provisioning protocol [12] by considering potential adversaries and their motivations. In this section, we consider a network adversary, i.e., an adversary that is able to read, modify and delete messages sent over wireless networks. In practice, such an adversary can intercept a signal simply by being close enough to the signal transmitter or receiver.

3.1 Memory exhaustion attack

It is possible to launch an attack that fills part of an eUICC's memory with an empty ISD-P by exploiting error handling during ISD-P creation, and the ISD-P deletion mechanism. Moreover, the eUICC's memory could be exhausted by repeating the attack. Indeed, an adversary could drop the ISD-R's response to the SM-SR (see (5) in Fig. 3) as is common in denial of service attacks [27, 28].

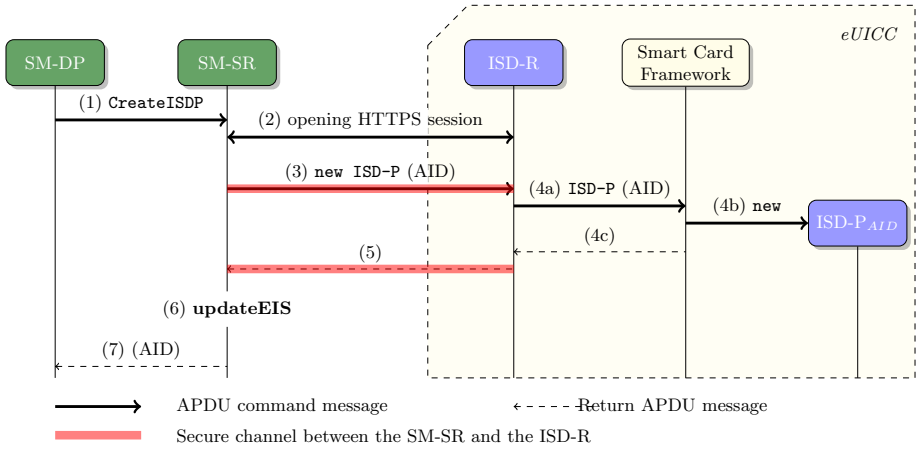

Fig. 3: ISD-P creation flow

(The adversary can identify and drop the response, even when it is encrypted, using truncation attacks [3, 24].) As a result of the dropped message, the SM-SR, unaware of the ISP-D creation status, cannot update the `EIS` file, and after waiting some time, sends a timeout response message to the SM-DP. The ISD-P created remains on the card, neither associated to an SM-DP nor operator, thus the ISD-P is *orphaned* and memory space on the eUICC has been reserved for its profile.

Recovery from this attack by deleting the created ISD-P is not possible, because deletion of an ISD-P and its profile is restricted to operators or SM-DPs and requires the ISD-P's identifier. Restricting deletion to operators and SM-DPs was motivated by a operator's requirements. An exceptional procedure called *Master Delete* is defined in the specification to allow an SM-SR to delete a profile correctly installed on an eUICC for which the operator owning the profile has given its approval for deletion and for which the subscription period is elapsed [12, §3.10]. Consequently, the master delete procedure cannot be applied. In fact, there is no mechanism defined in the specifications for the SM-SR or the eUICC to delete orphaned ISD-Ps. If the attack is repeated to exhaust the eUICC's memory, only profiles existing on the eUICC before the attack can be used later.

This attack causes financial loss, as it prevents operators from providing service. Moreover, recovery is impossible and any trace of the attack is minimal. An operator, with a profile on an eUICC, could, for example, collude with a network adversary and deliberately fill the eUICC memory.

Countermeasure. The attack can be prevented by creating a mechanism on the card to manage ISD-P creation. Once an ISD-P is created, the mechanism awaits the next logical instruction of the `DownloadProfile` process, i.e., the APDU command for the key exchange between the SM-DP and the ISD-P. If the awaited instruction is not received on time, the ISD-P is automatically deleted

by this mechanism and a notification is sent to the SM-SR. As such, even if the notification is dropped too, the orphaned ISD-P is deleted. This mechanism could be implemented as an extension of the GlobalPlatform framework.

4 Payload exploitation by malicious insiders

GSMA does not formally define the trust model between the different network entities. In this section, we exploit this and we present two attacks that can be performed by a malicious entity, behaving as a *malicious insider* [22, 15]. Such an adversary is dishonest, perhaps due to greed. Malicious entities have the capabilities of their honest counterparts, plus they will try to modify the protocol or the messages sent without being suspected of being dishonest as they could face sanctions otherwise [9, 25], resulting in what is considered as low cost attacks (see [1] for further information on such attacks).

4.1 Undersizing memory attack

A malicious SM-SR could, after receiving a `GetEIS` request from the SM-DP (§2.1), return the EIS file with the value of field `remainingMemory` set to a random value under the minimal size of a profile. (This cannot be detected because the field is not signed). By doing so, the SM-SR prevents an SM-DP from creating an ISD-P required for uploading a new profile on the eUICC, because the `Download&Install` process would halt, and the eUICC would be considered by the SM-DP as unable to receive a new profile. Therefore, an SM-SR can deny operators from installing profiles on an eUICC.

This attack is feasible as mutable fields from the EIS file, including the `remainingMemory` field, are not signed.[2] Such an attack is likely to be detected if the eUICC has been recently created but, for an old eUICC, the SM-SR will likely probably not be detected.

Countermeasure. This attack can be prevented by having eUICCs sign the values sent back to the SM-SR during an `AuditEIS` request. Such a request updates the value of an eUICC's mutable characteristics present in the EIS file, ensuring the SM-DP of their integrity. To prevent replay attacks, the signature should also contain a timestamp.

4.2 Inflated profile attack

A malicious operator could request, during the `DownloadProfile` protocol (§2.1), a profile almost exhausting the eUICC's remaining memory. (The operator can learn how much memory is available from using the getEIS function). This prevents other operators from installing profiles on the eUICC. This attack can similarly be initiated by an SM-DP during the `createISDP` request.

[2] Immutable characteristics of eUICCs, set at manufacture time, are signed by the manufacturer and stored, with other mutable information, into the *EIS* file. The *EIS* file is issued by the manufacturer to the first SM-SR responsible for the eUICC.

Countermeasure. This attack can be avoided by defining a profile size upper bound. During a profile creation, the operator's profile request would be verified by the subscription managers.[3]

5 Locking profile attacks by network operators

5.1 Profile Policy Rules and eUICC lock

GSMA's specification defines policy rules for managing the life cycle of profiles. These rules are initialized by the operator during profile creation, and are stored inside each profile. An unsynchronized copy of these rules, maintained by the operator, is in the EIS file stored by the SM-SR. They specify whether a profile can be disabled, can be deleted, or should be deleted once it is disabled. A profile's rules can only be modified when the profile is enabled by the operator owning the profile.

The policy rule `CannotBeDisabled` locks an eUICC to a profile, forcing the device to connect to a specific network. It is a feature of the existing subscription model [26], typically used to subsidize subscriptions. However, contrarily to eUICCs, for 4G networks, once unlocked, a device cannot be locked again.

At a high level, rule `CannotBeDisabled` is either *true* or *false* for the enabled profile. We show that this rule introduces a weakness that can result in an eUICC being locked to an undesirable operator's profile, without regard for the initial value of the rule. We demonstrate that a malicious operator can launch an attack when rule `CannotBeDisabled` is false (§5.2.1) and that an opportunistic operator can take advantage of its position when the rule is true (§5.2.2).

5.2 Locking profile attacks

5.2.1 Rule `CannotBeDisabled` is *false*. Suppose all of an eUICC's profiles have set the policy rule `CannotBeDisabled` to *false*. Further suppose a malicious operator is interested in blocking other operators' profiles. For this, the malicious operator installs its profile (§2.1), enables it and sets policy rule `CannotBeDisabled` to *true*. This disables the enabled profile, which is possible given its policy rules. The eUICC is locked to the malicious operator's profile which cannot be disabled and, consequently, cannot be deleted. Thus, even upon receiving a notification from the SM-SR about the disabling of its profile, the operator owning the previously enabled profile will be unable to re-enable it. The following examples present scenarios whereby eUICCs might be locked:

- **Cyberwarfare.** Assuming conflict between countries, one country could use a national operator to remotely attack the other country's eUICCs [21].
- **Hackers.** Hackers might steal valid certificates, as previously observed [19, 16]. Thus, it is feasible for hackers to pose as insiders.

[3] The SM-SR should perform the check to prevent a similar attack by the SM-DP.

– **Supply chain attack.** Assuming devices are powered-on once manufactured, and then shipped to their destination, and further assuming that devices are passing along the border of a country where operators have an aggressive market strategy, one operator could install a profile on all devices inside the container. Such attacks could also occur while devices are in production or in storage.

5.2.2 Rule `CannotBeDisabled` is *true*. An issue might arise when a subscriber wants the operator to unlock devices. Indeed, device owners are likely to initiate the remote unlocking of eUICCs. This setting, where the client ask the operator to unlock devices, is problematic in the presence of an opportunistic operator. Such an operator can delay the unlocking process, thus preventing other operator's from enabling their profile on the locked eUICC. Furthermore, the locking profile cannot be deleted without the operator's approval.

Countermeasure. We present several countermeasures that can be combined, if desired. First, a mechanism to automatically unlock the eUICC, once a lock expires. Secondly, specifying an upper bound on the locking period (e.g., two years), to prevent abuse. Finally, permitting locking only once during the life of an eUICC. This can be achieved by using a counter set to a specific value once a lock is used on a profile.

6 GSMA response

We reported our findings to GSMA under their Coordinated Vulnerability Disclosure Programme. GSMA's experts investigated our findings, acknowledged our attacks and confirmed their ability to impact the mobile industry. GSMA publicly recognized our work and contribution by adding our names to their Hall of Fame. Moreover, GSMA is working with us to incorporate our fixes into their specification. So far, GSMA has released an updated specification [14], which includes the fix described in §3 (see §3.1.1_(7) of the updated specification). They have also released a document detailing non-technical trust model and dependencies between the different parties needed for remote provisioning [13], which covers attacks initiated by malicious insiders by claiming that certification will solve the problem. Furthermore, GSMA is still integrating technical countermeasures, including our suggestions, to appear in the next releases of the specification.

7 Conclusion

GSMA is striving towards standardization of remotely provisioned, embedded SIMs. Its efforts have resulted in specifications for remote provisioning, in particular, for M2M devices. This evolution towards next generation telecommunications is exciting, but not without risk. Indeed, we have studied release 3.1

of GSMA's specification and discovered that the proposed evolution is insecure. More issues might well exist and it is crucial that the specification is studied further to ensure security of next generation telecommunications, ideally resulting in formal security proofs.

Acknowledgments. This work was largely conducted at Huawei's Mathematical and Algorithmic Sciences Lab in France.

References

1. Anderson, R., Kuhn, M.: Low cost attacks on tamper resistant devices. In: International Workshop on Security Protocols. pp. 125–136. Springer (1997)
2. Berard, X., Gachon, D.: Method for remotely delivering a full subscription profile to a uicc over ip (2013-12), US Patent App. 13/991,846
3. Berbecaru, D., Lioy, A.: On the Robustness of Applications Based on the SSL and TLS Security Protocols. In: Public Key Infrastructure. LNCS, vol. 4582, pp. 248–264. Springer (2007)
4. Blom, R., Norrman, K., Naslund, M., Rommer, S., Sahlin, B.: Security in the Evolved Packet System. Tech. rep. (2010-02)
5. Cimpanu, C.: New Malware Intentionally Bricks IoT Devices. `goo.gl/06gwr5` (2017-04), accessed: 2017-04-11
6. ETSI: Smart Cards; Embedded UICC; Requirements Specification (V. 12.0.0). Tech. Spec. 103 383 (2013-09)
7. Girard, P., Proust, P.: Method for managing content on a secure element connected to an equipment (2013-11), US Patent App. 13/991,823
8. GlobalPlatform: Card Specification (V. 2.3). Tech. Spec. GPC_SPE_034 (2015-10)
9. Gow, D.: Telefónica hit by record €152m anti-trust fine. `goo.gl/Dvx6kk` (2007-07), accessed: 2016-12-06
10. GSMA: GSMA announces mobile industry initiative to create a global remote provisioning specification for consumer devices (March 2015)
11. GSMA: Business Process for Remote SIM Provisioning in M2M (V.1.0). Tech. Spec. CLP.05 (2015-02)
12. GSMA: Remote Provisioning Architecture for Embedded UICC (V. 3.1). Tech. Spec. SGP.02 (2016-05)
13. GSMA: M2M IoT Trust Model (V. 1.0). Tech. Spec. SGP.15 (Novembre 2017)
14. GSMA: Remote Provisioning Architecture for Embedded UICC (V. 3.2). Tech. Spec. SGP.02 (2017-06)
15. Jiang, S., Smith, S., Minami, K.: Securing web servers against insider attack. In: Annual Computer Security Applications Conference. pp. 265–276. IEEE (2001)
16. Langley, A.: Further improving digital certificate security. `goo.gl/kRHHD6` (2013-12), accessed: 2017-01-16
17. Merrien, L., Berard, X., Gachon, D.: Method for transmitting a SIM application of a first terminal to a second terminal (2014-05), US Patent App. 13/991,542
18. Meyer, M., Quaglia, E.A., Smyth, B.: Overview of GSMA Remote Provisioning Specification (2017), `https://bensmyth.com/publications/2017-eUICC-overview/`
19. Microsoft: Fraudulent Digital Certificates Could Allow Spoofing. `goo.gl/bLbSQM` (2011-08), accessed: 2017-01-16

20. Park, J., Baek, K., Kang, C.: Secure Profile Provisioning Architecture for Embedded UICC. In: International Conference on Availability, Reliability and Security. pp. 297–303. IEEE (2013)
21. Schneier, B.: Cyberwar. goo.gl/SJW3oU (2007-06), accessed: 2016-10-12
22. Schultz, E.E.: A framework for understanding and predicting insider attacks. Computers & Security 21(6), 526–531 (2002)
23. Sierra Wireless: The eUICC opportunity: harness the power of IoT eSIMS. White paper (2017)
24. Smyth, B., Pironti, A.: Truncating TLS Connections to Violate Beliefs in Web Applications. In: USENIX Workshop on Offensive Technologies. USENIX Association (2013), see also INRIA tech. rep. hal-01102013 (2015)
25. Thomas, D.: France hits Orange with €350m antitrust fine. goo.gl/B8z1Xf (2015-12), accessed: 2016-12-06
26. Vermeulen, J.: Why it is legal for FNB to SIM-lock its smartphones. https://goo.gl/xbX5zn (2016-09), accessed: 2017-01-16
27. Wood, A.D., Stankovic, J.A.: Denial of service in sensor networks. computer 35(10), 54–62 (2002)
28. Xie, L., Zhu, S.: Message dropping attacks in overlay networks: Attack detection and attacker identification. ACM Transactions on Information and System Security 11(3), 15 (2008)