

Università degli Studi di Roma Tor Vergata

DIPARTIMENTO DI INGEGNERIA CIVILE E INGEGNERIA DELL'INFORMAZIONE

Corso di Laurea Magistrale in Ingegneria Informatica

Titolo della tesi

Candidato:

Matteo Fanfarillo

Matricola 0316179

Relatore:

Giuseppe Bianchi

Correlatore:

Francesco Gringoli

[Citazione]

Indice

1	Introduzione	6
1.1	Panoramica sulla eSIM	6
1.2	Obiettivo del lavoro	6
1.3	Definizioni preliminari	6
1.4	Panoramica sui capitoli successivi	6
2	Interfacce e funzionamento della eSIM	8
3	Analisi della sicurezza della eSIM a run-time	9
4	Analisi della sicurezza della eSIM a boot-time	10
4.1	Funzionamento del boot della eSIM	10
4.2	Potenziati vulnerabilità	10
4.3	Prove sperimentali	10
5	Conclusione	11

Elenco delle figure

Elenco delle tabelle

Introduzione

1.1 Panoramica sulla eSIM

La eSIM (embedded-SIM) non è altro che una SIM virtuale: grazie a lei, quando l'utente vuole cambiare operatore, non deve più acquistare fisicamente una nuova SIM card presso un negozio del nuovo operatore, bensì gli è sufficiente ricevere via e-mail un profilo, ossia una "SIM digitale" che può essere caricata subito sul telefono mediante la scansione di un QR code. Si tratta di una soluzione molto più pratica rispetto a recarsi fisicamente presso il negozio dell'operatore, tant'è vero che negli ultimi anni si sta diffondendo sempre di più: uno studio di Juniper Research stima che il numero di telefoni che utilizzano la connettività eSIM aumenterà dai 986 milioni attuali ai 3.5 miliardi entro il 2027 [1]. Per questi motivi, e poiché le informazioni associate alla comunicazione tra eSIM sono sensibili, è fondamentale garantire un livello di sicurezza sufficientemente elevato per il funzionamento della eSIM sia a run-time che a boot-time.

1.2 Obiettivo del lavoro

La presente trattazione si propone di effettuare un'analisi di sicurezza e delle vulnerabilità della eSIM e del suo funzionamento e, successivamente, di tentare di sfruttare, anche con delle attività di laboratorio, le eventuali vulnerabilità trovate.

1.3 Definizioni preliminari

- **eUICC (embedded Universal Integrated Circuit Card):** è un chip utilizzato all'interno dei telefoni all'interno del quale è embeddato il software della eSIM. È integrato direttamente nei dispositivi (i.e. non è rimovibile) ed è progettato per essere programmato a distanza. Può contenere uno o più profili SIM.
- **SM-DP+ (Subscription Manager Data Preparation plus):** è un protocollo che rappresenta una tecnica di provisioning usata per configurare le eSIM in modo automatico e remoto. Rispetto alla versione base SM-DP, offre delle funzionalità aggiuntive come un sistema di crittografia più avanzato e un'architettura di rete più flessibile.
- **LPA (Local Profile Assistant):** è un'applicazione che vive nel telefono dell'utente ed è responsabile della gestione dei profili all'interno della rete mobile, incluse la creazione, l'aggiornamento e la cancellazione.

1.4 Panoramica sui capitoli successivi

Nel capitolo 2 verrà svolta una trattazione dettagliata sull'architettura e sulle interfacce della eSIM, con lo scopo di fornire al lettore gli strumenti per comprendere appieno le tematiche centrali del lavoro. Nel capitolo 3 verrà effettuata un'analisi della sicurezza della eSIM a run-time, mentre nel

capitolo 4 si procederà con l'analisi della sicurezza della eSIM a boot-time (i.e. durante la fase di configurazione).

Capitolo 2

Interfacce e funzionamento della eSIM

[TODO]

Capitolo 3

Analisi della sicurezza della eSIM a run-time

[TODO]

Capitolo 4

Analisi della sicurezza della eSIM a boot-time

4.1 Funzionamento del boot della eSIM

[TODO]

4.2 Potenziali vulnerabilità

[TODO]

4.3 Prove sperimentali

[TODO]

Capitolo 5

Conclusione

[TODO]
[2] [3]

Bibliografia

- [1] Corcom. *"Telefonia mobile, cosa sono le eSim? E perché sono più sicure?"*, 2023. <https://corrierecomunicazioni.it/telco/telefonia-mobile-cosa-sono-le-esim-e-perche-sono-piu-sicure/>.
- [2] GSM Association. *"RSP Technical Specification Version 2.0"*, 2016. https://gsma.com/newsroom/wp-content/uploads/SGP.22_v2.0.pdf.
- [3] Team di Android. *"Implementing eSIM"*, 2023. <https://source.android.com/docs/core/connect/esim-overview>.

Ringraziamenti

[TODO]