Bezpieczeństwo kart SIM

Jakub Olejnik

Wprowadzenie do kart SIM

SIM = Moduł identyfikacji abonenta

Struktura:

- Mikroprocesor (CPU)
- Pamięć programu (ROM)
- Pamięć robocza (RAM)
- Pamięć danych (EPROM lub E2PROM)

Typy:

- Pełnowymiarowa karta SIM
- Mini SIM
- Mikro SIM
- Nano SIM
- Karta eSIM

Ataki na COMP128

COMP128 – algorytm implementowany na kartach SIM

Nieoczekiwany wyciek kodu źródłowego

Przykłady ataków:

- Atak czarnej skrzynki
- Atak szyfrogramem

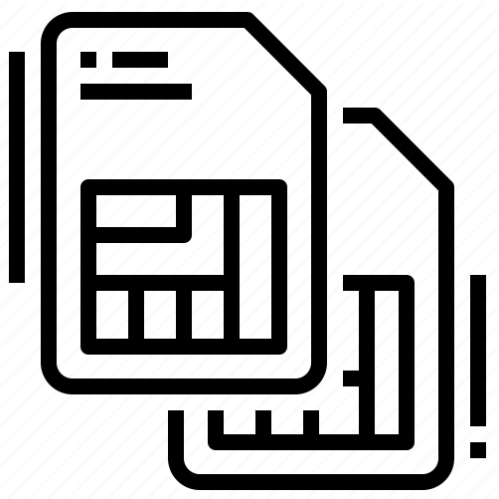
Klonowanie kart SIM

Klonowanie – duplikacja kart SIM

Obecnie trudne w realizacji

Wymagania:

- IMSI – identyfikator karty
- Ki – klucz uwierzytelniający



Funkcjonalności związane z bezpieczeństwem kart

Atrybuty bezpieczeństwa obsługiwane przez SIM:

- Algorytm uwierzytelniający (A3)
- Algorytm szyfrujący (A5)
- Algorytm generowania klucza szyfrującego (A8)

Ewolucja kart SIM

- USIM – aplikacja używana w UMTS
- UICC – uniwersalna karta z układem scalonym która może zawierać kilka aplikacji

Źródła

- He, Sheng, and Ing Christof Paar. "SIM card security." *Seminar Work, Ruhr-University of Bochum*. 2007.
- Anwar, Nuril, Imam Riadi, and Ahmad Luthfi. "Forensic SIM card cloning using authentication algorithm." *International Journal of Electronics and Information Engineering* 4.2 (2016): 71-81.
- Brumley, Billy. "A3/A8 & COMP128." T-79.514 Special Course on Cryptology (2004): 1-18.
- https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/sim?fbclid=IwAR37Bz1gjEni-PDb-ubduYSRHPrCAdMNit18GloNuXVrFNJbEW9Mp7D_LC8
- https://en.wikipedia.org/wiki/SIM_card