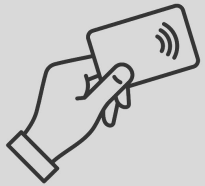
DESFire - podatności

Autor: 144456

Plan prezentacji

1. Czym jest karta DESFire
2. Przegląd podatności kart DESFire
3. Opis przykładowego ataku nr1 na karty DESFire
4. Opis przykładowego ataku nr2 na karty DESFire
5. Usprawnienie odporności na ataki w poszczególnych generacjach DESFire (DESFire, EV1, EV2, EV3)

Czym jest karta DESFire



Karty bezdotykowe bazowane na standardzie ISO/IEC 14443

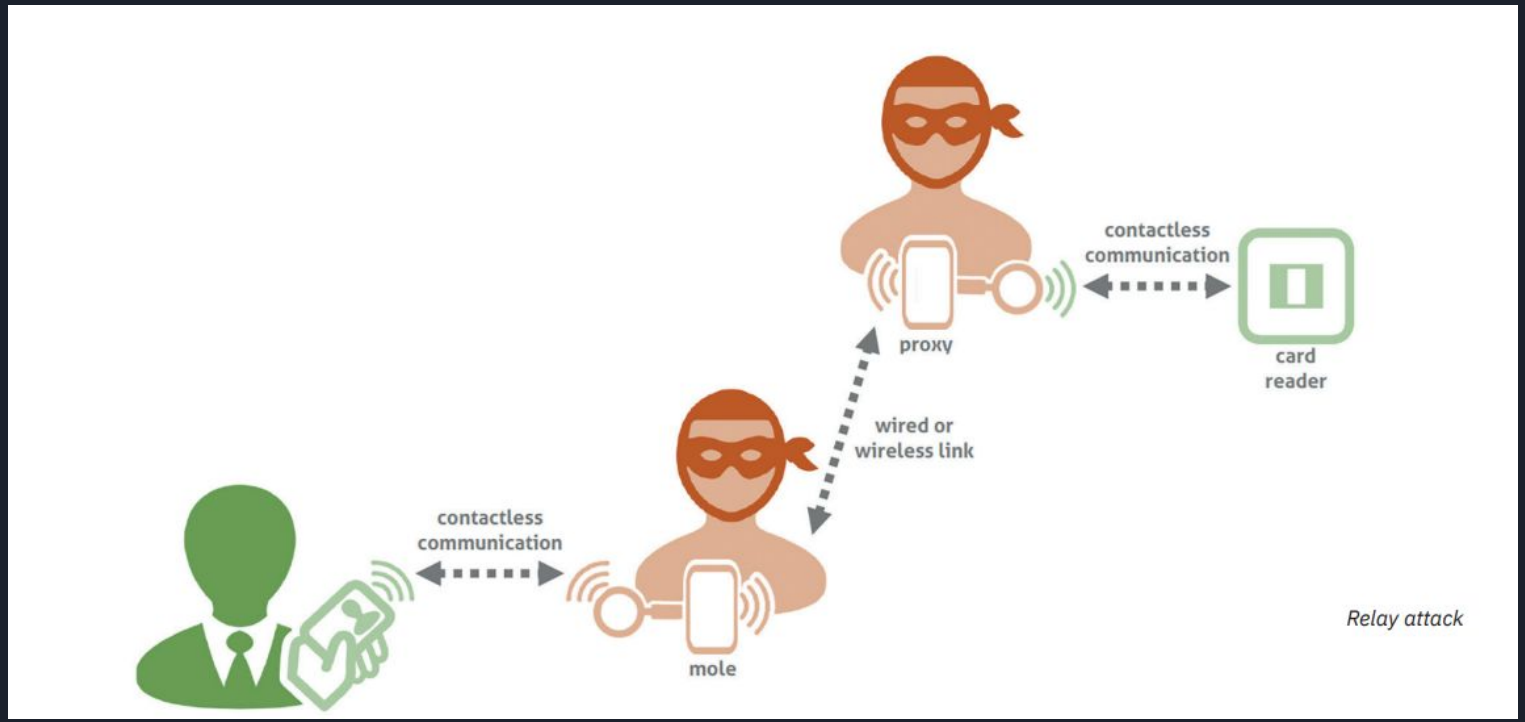
Wykorzystywane w systemach kontroli dostępu, płatnościach bezdotykowych i transporcie publicznym

Wprowadzone przez NXP Semiconductors w 2002 roku

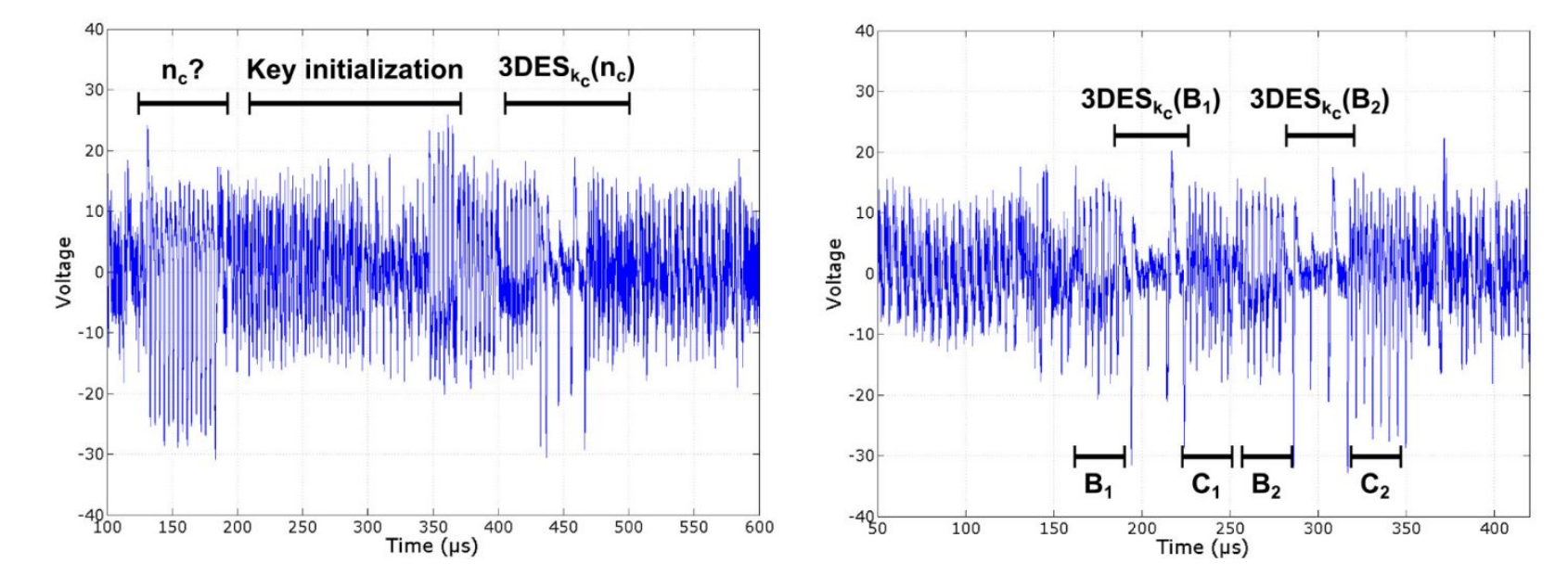
Przegląd podatności kart DESFire

- 2011 - David Oswald, Christoph Paar - złamanie algorytmu szyfrującego 3DES wykorzystywanego w kartach MIFARE DESFire MF3ICD40,
- 2012 i 2013 - Martin Henzl et al. - przedstawienie zautomatyzowanego systemu wyszukiwania słabych punktów w protokołach kart bezprzewodowych,
- 2019 - Rory Flynn - relay attack, opisanie 3 ataków na urządzenia wykorzystywane w komunikacji miejskiej,
- 2020 - Nedap - relay attack, uzyskanie dostępu do pomieszczeń/systemów poprzez utworzenie tunelu czytnik-karta

Opis przykładowego ataku na karty DESFire (relay attack)



Opis przykładowego ataku na karty DESFire (złamanie szyfru 3DES)



Usprawnienie odporności na ataki w poszczególnych generacjach DESFire

D40 (2002)	EV1 (2006)	EV2 (2016)	EV3 (2020)
- DES/3DES	- AES128 -EAL4+	- proximity check (anty relay) - EAL5+	- transaction timer (anty MitM) - DES/3DES/AES

Dziękuję za uwagę

Źródła

- https://en.wikipedia.org/wiki/MIFARE#MIFARE_DESFire_family
- https://www.digitalid.co.uk/blog/mifare-desfire-ev1-vs-ev2
- https://www.shopnfc.com/en/content/37-mifare-desfire-ev1-ev2-ev3
- https://www.researchgate.net/publication/344479867_An_investigation_of_possible_attacks_on_the_MIFARE_DESFire_EV1_smartcard_used_in_public_transportation
- https://ieeexplore.ieee.org/document/6393556
- https://www.nedapsecurity.com/wp-content/uploads/2020/03/Nedap-Whitepaper-Relay-Attack-EN.pdf
- https://ieeexplore.ieee.org/abstract/document/6597681
- https://www.iacr.org/archive/ches2011/69170208/69170208.pdf