POLITECHNIKA POZNAŃSKA

Wydział Informatyki i Telekomunikacji
Internet Przedmiotów

DESFire - podatności

Systemy Automatycznej Identyfikacji

Sprawozdanie

144456

Semestr: lato-2024

1 Karta DESFire - wprowadzenie

DESFire to seria układów scalonych montowanych w kartach bezkontaktowych. Należą one do rodziny układów MIFARE. Zostały opracowane i wprowadzone do sprzedaży przez firmę NXP Semiconductors w 2002 roku jako bardziej zaawansowana i bezpieczna alternatywa dla MIFARE Classic. Wykorzystywane są głównie w systemach kontroli dostępu, płatności bezdotykowej i transporcie publicznym. Oparte są na standardzie ISO/IEC 14443. Pierwszą wersją wprowadzoną na rynek było MIFARE DESFire MF3ICD40 (w skrócie oznaczane jako DESFire D40). Najnowsze karty oparte na DESFire charakteryzują się między innymi:

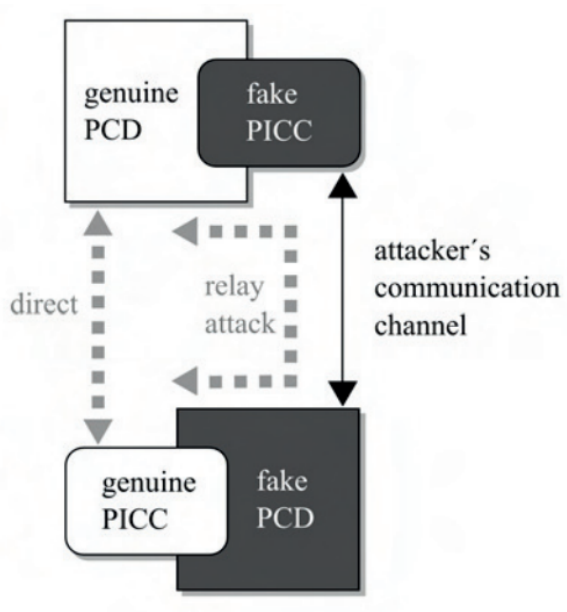
- wysokim poziomem zabezpieczeń przechowywanych danych (dokładniej jest to opisane w punkcie 3),
- możliwością obsługiwania teoretycznie nieograniczonej liczby aplikacji (ograniczenie jest jedynie pamięciowe), gdzie w pierwszych iteracjach karta mogła obsłużyć do 28 aplikacji),
- zapewnieniem interoperacyjności aplikacji dzięki Virtual Cards Architecture, co pozwala na stworzenie karty o wielu zastosowaniach,
- wymianą danych z czytnikiem na odległości do 100mm (według niektórych źródeł karty z serii DESFire EV2 i DESFire EV3 charakteryzują się większym zasięgiem).

2 Przegląd podatności kart DESFire

Ze względu na małą popularność badań nad kartami DESFire, a szerzej patrząc MIFARE (w repozytorium IEEE dla frazy "MIFARE" wyników jest 53, dla "DESFire" - 8), w celu przedstawienia przykładowych podatności i ataków z ich wykorzystaniem należało sięgnąć do zasobów internetowych.

2.1 Relay attack

Najczęściej występującym atakiem pojawiającym się w zasobach literaturowych jest "relay attack", w którym dane pomiędzy oryginalna kartą, a czytnikiem (np. służącym do uzyskania dostępu do pomieszczenia) są przekazywane za pomocą "przedłużenia", którego właściciel karty nie jest świadomy. Przekazanie takich informacji może nastąpić bezpośrednio przy pomocy przewodu albo drogą radiową.



Rysunek 1: Konfiguracja ataku typu relay, pomiędzy oryginalną kartą (na obrazku PICC - ang. proximity inductive coupling card) a oryginalnym czytnikiem (na obrazku PCV - ang. proximity coupling device). Grafika z artykułu 5.

Według firmy Nedap [6], która jest autorem jednego ze znalezionych materiałów, można wyznaczyć 3 warianty tego ataku, które różnią się medium służącego do przekazania danych pomiędzy oryginalną kartą, a czytnikiem:

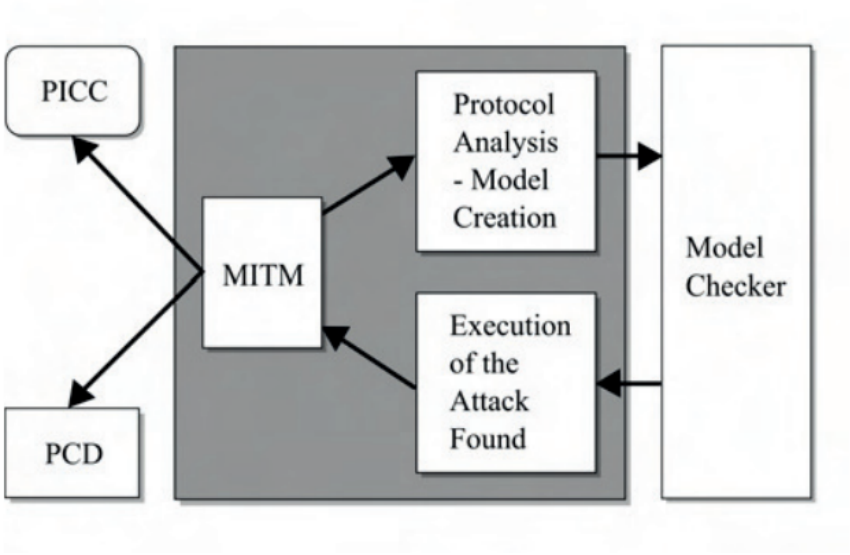
1. Przekazanie przy pomocy przewodu - charakteryzuje się niskim kosztem i niskimi opóźnieniami, ale ma bardzo ograniczony zasięg (10-100 m).

2. Przekazanie przy pomocy bezprzewodowego systemu superheterodynowego (radio zmieniające częstotliwość odbieranego sygnału poprzez generowany przez siebie sygnał o niskiej częstotliwości) - charakteryzuje się niskimi opóźnieniami, ale ma ograniczony zasięg i wymaga dedykowanego sprzętu.

3. Przekazanie przy pomocy sygnału radiowego (np. telefonii komórkowej) - charakteryzuje się łatwością implementacji (mogą to być nawet dwa telefony z obsługą NFC) i nieograniczonym zasięgiem, ale ma największe opóźnienia, co może być wykryte przez karty nowszej generacji.

Został on opisany między innymi w podanych poniżej artykułach i zasobach:

- "A concept of automated vulnerability search in contactless communication applications" [5] i "Modeling of Contactless Smart Card Protocols and Automated Vulnerability Finding" [7] - dwa artykuły z odpowiednio 2012 i 2013 roku, w których Henzl M. i inni opisują stworzenie i eksploatację stanowiska do automatycznego wyszukiwania podatności w systemach bazujących na kartach bezprzewodowych przy pomocy ataku typu relay, podsłuchiwania danych przekazywanych pomiędzy kartą a czytnikiem, a także zmieniania przesyłanych danych po przechwyceniu ich (działanie Man-in-the-Middle (MitM)).



Rysunek 2: Konfiguracja opisanego stanowiska. Grafika z artykułu 5.

- "An investigation of possible attacks on the MIFARE DESFire EV1 smartcard used in public transportation" [4] - artykuł z 2019, w którym Flynn R. opisuje 3 przykładowe ataki na infrastrukturę używaną w komunikacji miejskiej poprzez przechwycenie przesyłanych komend i ich manipulację bądź wstrzymanie. Jeden z ataków opiera się o retransmisję ramki odpowiedzialnej za doładowanie karty transportowej, w wyniku czego na karcie wartość doładowania jest wyższa niż zostało to zaznaczone przy pierwotnym doładowaniu.

- "The danger of relay attack within the physical security domain" [6] - dokument przygotowany przez firmę Nedap opisujący wcześniej przytoczone typy ataków relay, a także informujący o tym jakie kroki można podjąć, aby się przed nimi ochronić. Zabezpieczeniem wykraczającym poza konstrukcję samej karty jest chowanie jej podczas nieużywania do ochronnego opakowania, które miałoby charakterystykę klatki Faradaya, czyli ekranowałoby promieniowanie elektromagnetyczne wysyłane przez atakującego, co uniemożliwiłoby mu odczyt danych. Inne propozycje, takie jak ograniczenie czasu oczekiwania na transakcję albo wykrywanie obecności karty zostały wprowadzone w nowszych iteracjach karty DESFire i są opisane w punkcie 3.

2.2 Złamanie szyfru 3DES poprzez Side Channel Attack

Drugim atakiem szczegółowo opisanym w literaturze jest ten autorstwa Davida Oswalda i Christopha Paara, w którym łamią oni szyfr 3DES używany w kartach MIFARE DESFire MF3ICD40 poprzez odczytanie klucza prywatnego przy pomocy ataku typu SCA (ang. Side Channel Attack), który polega na obserwacji oddziaływania karty na środowisko podczas wymiany danych. W przypadku tego artykułu wykonywana jest CPA (ang. Correlation Power Analysis), czyli analiza poboru energii przez kartę pod kątem jej korelacji z wysyłanymi danymi. Autorzy stwierdzają, że w momencie przesyłania poszczególnych bitów pomiędzy

DESFire, a czytnikiem można zauważyć znaczny skok pobieranej mocy. Na podstawie odległości pomiędzy takimi skokami w czasie istnieje także opcja zidentyfikowania częstotliwości z jaką działa magistrala, po której są wymieniane informacje. Zebrane dane umożliwiają także zauważenie, że istnieją wahania okresach pomiędzy kolejnymi ramkami. Jest to spowodowane przez zabezpieczenia, które powodują, że czas pomiędzy wykonaniami kolejnych operacji w ramach 3DES nie jest jednostajny (zabezpieczenie to działa na zasadzie losowania, w pewnych ramach, opóźnienia, z jakim wysyłane są bity). W celu wyłuskania danych z tak przesuniętych w czasie odczytów należy zastosować jedną z metod dostosowania danych. Przykładem takiej metody jest DTW (ang. Dynamic Time Warping), czyli metoda matematyczna pozwalająca dopasować do siebie dwie sekwencje czasowe, mimo różnić w szybkości ich przebiegu. Inną, poczynioną w artykule obserwacją było to, że amplituda napięć podczas procesu szyfrowania jest niższa niż przy innych operacjach, co wskazuje na to, że moduł do tego wykorzystywany jest low-power, co pokrywa się z informacjami zawartymi w karcie katalogowej MIFARE DESFire MF3ICD40. Autorzy stwierdzają, że pełne wyłonienie prywatnego klucza 3DES może zająć około 7h, przy pobraniu ok. 250 tys. próbek sygnałów wysyłanych przez kartę w środowisku sprzętowym, kosztującym około 3000$, stworzonym na potrzeby eksperymenty. We wnioskach autorzy zaznaczają, że karty DESFire EV1, bazujące na algorytmie szyfrującym AES, mają zaimplementowane kolejne zabezpieczenia przed atakami typu SCA.

3 Usprawnienie odporności na ataki w poszczególnych generacjach DESFire

Artykuł opisany w punkcie 2.2 był powodem, dla którego firma NXP nakłaniała użytkowników swoich produktów do przejścia na kartę o wyższym poziomie zabezpieczeń, którą na tamten moment było MIFARE DESFire EV1. DESFire D40 charakteryzowało się wykorzystywaniem jedynie algorytmów szyfrujących bazujących na DES (DES/2K3DES/3K3DES) i nie posiadało zabezpieczeń umożliwiających uchronienie się przed atakami opisanymi wcześniej. Każda z nowszych iteracji karty wprowadzała kolejne usprawnienia, mające na celu zwiększenie ochrony przesyłanych danych. Zestawienie zmian zostało pokazane w tabeli poniżej. Pod nazwą każdej z kart widnieje także rok jej zapowiedzenia przez NXP

	D40 (2002)	**EV1 (2006)**	**EV2 (2016)**	**EV3 (2020)**
Algorytm szyfrujący	warianty DES (2K3DES, 3K3DES)	warianty DES + AES128	warianty DES + AES128	warianty DES + AES128
Ocena EAL	-	EAL4+	EAL5+	EAL5+
Inne	-	-	proximity check VCA	transaction timer proof of transaction

Wyjaśnienie pojęć znajdujących się w tabeli:

- ocena EAL - ang. Evaluation Assurance Level - ocena zabezpieczeń danego produktu teleinformatycznego, wystawiana na podstawie spełnienia warunków zawartych w normie ISO 15408, zwanych Common Criteria, skala EAL jest w zakresie 1-7,
- proximity check - zabezpieczenie pozwalające na wykrycie czy uzyskiwane informacje są przekazywane z karty znajdującej się blisko czytnika czy z urządzenia osoby wykonującej relay attack,
- VCA - ang. Virtual Card Architecture - opisano w punkcie 1,
- transaction timer - zabezpieczenie przed atakami typu MitM, które wykrywa opóźnienia związane z przesyłaniem danych niebezpośrednio pomiędzy kartą, a czytnikiem (wskazuje to na udział urządzeń trzecich w komunikacji),
- proof of transaction - potwierdzenie wymiany danych pomiędzy kartą, a czytnikiem przy pomocy generowanego przez kartę kody potwierdzającego MAC (ang. Message Authentication Code).

4 Źródła

1. https://en.wikipedia.org/wiki/MIFARE#MIFARE_DESFire_family
2. https://www.digitalid.co.uk/blog/mifare-desfire-ev1-vs-ev2
3. https://www.shopnfc.com/en/content/37-mifare-desfire-ev1-ev2-ev3

4. https://www.researchgate.net/publication/344479867_An_investigation_of_possible_attacks_on_the_MIFARE_DESFire_EV1_smartcard_used_in_public_transportation
5. https://ieeexplore.ieee.org/document/6393556
6. https://www.nedapsecurity.com/wp-content/uploads/2020/03/Nedap-Whitepaper-Relay-Attack-EN.pdf
7. https://ieeexplore.ieee.org/abstract/document/6597681
8. https://www.iacr.org/archive/ches2011/69170208/69170208.pdf