Rodzaje ataków w komunikacji NFC

Atak eavesdropping

Atak polega na użyciu specjalnego urządzenia NFC, które jest w stanie odczytać sygnały radiowe przesyłane między dwoma innymi urządzeniami NFC.

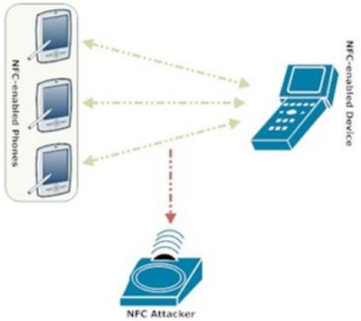
Atakujący może zbliżyć się wystarczająco blisko, aby przechwycić sygnały radiowe, a następnie zdekodować je, aby odczytać przesyłane dane.

Może to obejmować informacje takie jak numer karty płatniczej, dane osobowe, identyfikatory dostępu czy inne poufne dane.

Atak eavesdropping

Podstawową metodą zapobiegania podsłuchiwaniu jest korzystanie różnych metod szyfrowania.

Jednocześnie odległość urządzeń komunikujących się stanowi dodatkową przeszkodę dla przeprowadzenia ataku.

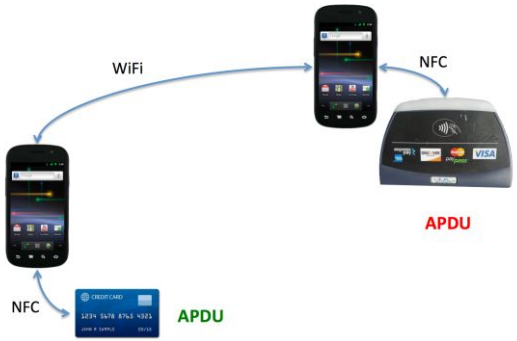


Atak typu Relay

W przypadku ataku relay w NFC, atakujący wykorzystuje dwa urządzenia.

Pierwsze urządzenia, zbliża się do ofiary, która posiada urządzenie NFC, takie jak smartfon, karta płatnicza lub identyfikator dostępu

Drugie urządzenie, znajduje się w miejscu, do którego ofiara chce uzyskać dostęp lub nawiązać komunikację, na przykład terminal płatniczy lub zamek drzwi.



Atak typu Relay

Przykładowa sytuacja z przekazaniem sygnału do otwarcia zamka

Dużą wadą jest opóźnienie które można łatwo wykryć

Atak DoS

Atak typu DoS (Denial of Service) polega na zakłóceniu lub utrudnieniu funkcjonowania urządzeń NFC, uniemożliwiając tym samym prawidłowe wykonanie pożądanych operacji.

Atak DoS może być przeprowadzany na różne sposoby:

- Atakujący może wysłać zakłócające sygnały radiowe w pobliżu urządzenia NFC, co może prowadzić do zakłóceń w komunikacji NFC między dwoma urządzeniami. Może to uniemożliwić prawidłowe wykonanie operacji, takich jak odczyt lub zapis danych.

Atak DoS

- Atakujący może manipulować protokołem NFC, np. poprzez generowanie błędów w komunikacji lub wysyłanie nieprawidłowych pakietów danych. To może prowadzić do awarii w procesie komunikacji i uniemożliwiać prawidłowe wykonanie operacji NFC

- Atakujący może próbować przekroczyć pojemność bufora w urządzeniu NFC, wprowadzając zbyt wiele danych na raz. Może to spowodować przeciążenie systemu i tym samym zakłócić lub uniemożliwić działanie urządzenia NFC.

Atak DoS

Metody ochrony:

- Kontrola dostępu
- Limitowanie częstotliwości transakcji
- Mechanizmy detekcji anomalii
- Odpowiednie zarządzanie zasobami

Atak typu replay

Atak typu replay polega na przechwyceniu i późniejszym powtórnym przesłaniu wcześniej zarejestrowanych danych NFC

Atakujący przechwytuje dane NFC, które zostały wcześniej wysłane między dwoma urządzeniami NFC. Następnie atakujący wysyła te przechwycone dane ponownie do urządzenia docelowego, tak jakby pochodziły one od prawidłowego nadawcy.

Atak typu replay

Sposoby ochrony:

- Zastosowanie unikalnego identyfikatora transakcji
- Wykorzystanie czasowych ograniczeń
- Używanie szyfrowania danych

Atak MITM

Atak Man In The Middle (MITM) polega na tym że atakujący umieszcza swoje urządzenie między czytnikiem a kartą.

Przykładowo użytkownik posiada ukradzioną lub zagubioną kartę płatniczą. Mimo iż została ona zablokowana użytkownik za pomocą specjalnego sprzętu który znajduje się między kartą a terminalem może wysłać sygnał aby terminal przyjął płatność.

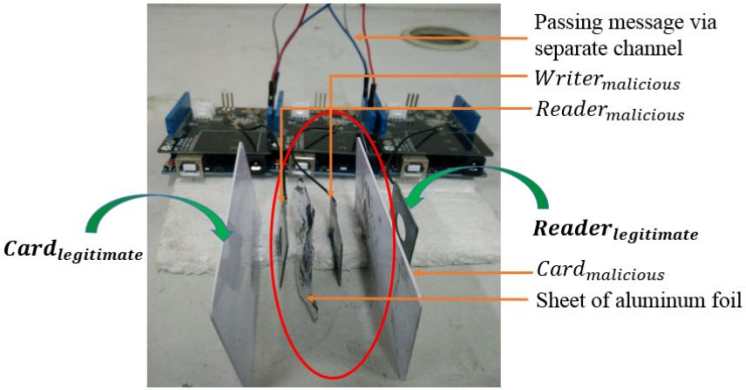
Sprzęt można schować np. do portfela.

Atak jest możliwy tylko w przypadku płatności offline

Atak MITM

Dopiero po dłuższym czasie gdy dochodzi do rozliczenia banku ze sprzedawcą, okazuje się że płatność nie powinna zostać przyjęta. W zależności jak jednostki się umówią, stratny będzie bank lub częściej raczej sprzedawca.

W celu ochrony przed atakiem oprogramowanie odbiornika NFC (terminalu) musi zostać odpowiednio zabezpieczone. Przykładowo opóźnienie przesyłania wiadomości jest dużo większe w przypadku przeprowadzania ataku.



Atak typu spoofing

W ataku spoofing na NFC, atakujący podszywa się pod inną jednostkę w celu wprowadzenia w błąd użytkownika, aby zbliżył swoje urządzenie do tagu NFC.

Przykładem takiego ataku może być skompromitowany tag NFC na inteligentnym plakacie, który przekierowuje nas na nieodpowiednią stronę.

Niektóre urządzenia mobilne są skonfigurowane do automatycznego wykonywania poleceń - bez wcześniejszego potwierdzenia użytkownika.

Atak typu spoofing

Aby skutecznie przeciwdziałać temu rodzajowi ataku, ważne jest odpowiednie skonfigurowanie urządzenia.

Powinno być wyświetlone ostrzeżenie lub potwierdzenie przed wykonaniem jakichkolwiek poleceń otrzymanych z tagu NFC. Użytkownik powinien otrzymać informację o tym, co zostanie wykonane i mieć możliwość zaakceptowania lub odrzucenia danego polecenia.

Ważne jest również, aby korzystać z urządzeń i tagów NFC zaufanych i sprawdzonych.

Literatura

S. Akter, S. Chellappan, T. Chakraborty, T. A. Khan, A. Rahman and A. B. M. Alim Al Islam, "Man-in-the-Middle Attack on Contactless Payment over NFC Communications: Design, Implementation, Experiments and Detection," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 6, pp. 3012-3023, 1 Nov.-Dec. 2021, doi: 10.1109/TDSC.2020.3030213.

Pierluigi Paganini, Near field communication (NFC) technology, vulnerabilities and principal attack schema, https://resources.infosecinstitute.com/topic/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/

Fahrianto, Feri & Lubis, Muhammad & Fiade, Andrew. (2016). Denial-of-service attack possibilities on NFC technology. 1-5. 10.1109/CITSM.2016.7577582.