Zmiana kodu identyfikującego UID w kartach Mifare jest możliwa tylko w przypadku kart specjalnie wyprodukowanych do tego celu. Zgodnie z zaleceniami standardu wprowadzonego przez NXP, blok 0 sektora 0 nazywany jest „Manufacturer block", w którym na etapie produkcji zapisywane są informacje o producencie oraz identyfikator karty UID. Po zakończeniu procesu produkcji ten blok jest zabezpieczany i nie ma możliwości zmiany danych w nim zawartych. Obecnie bez problemu można nabyć karty które nie zostały wyprodukowane zgodnie z tą normą i blok 0 sektora nie jest w żaden sposób zabezpieczony. Oznacza to, że możliwe jest wykonanie kart Mifare o identycznym UID.

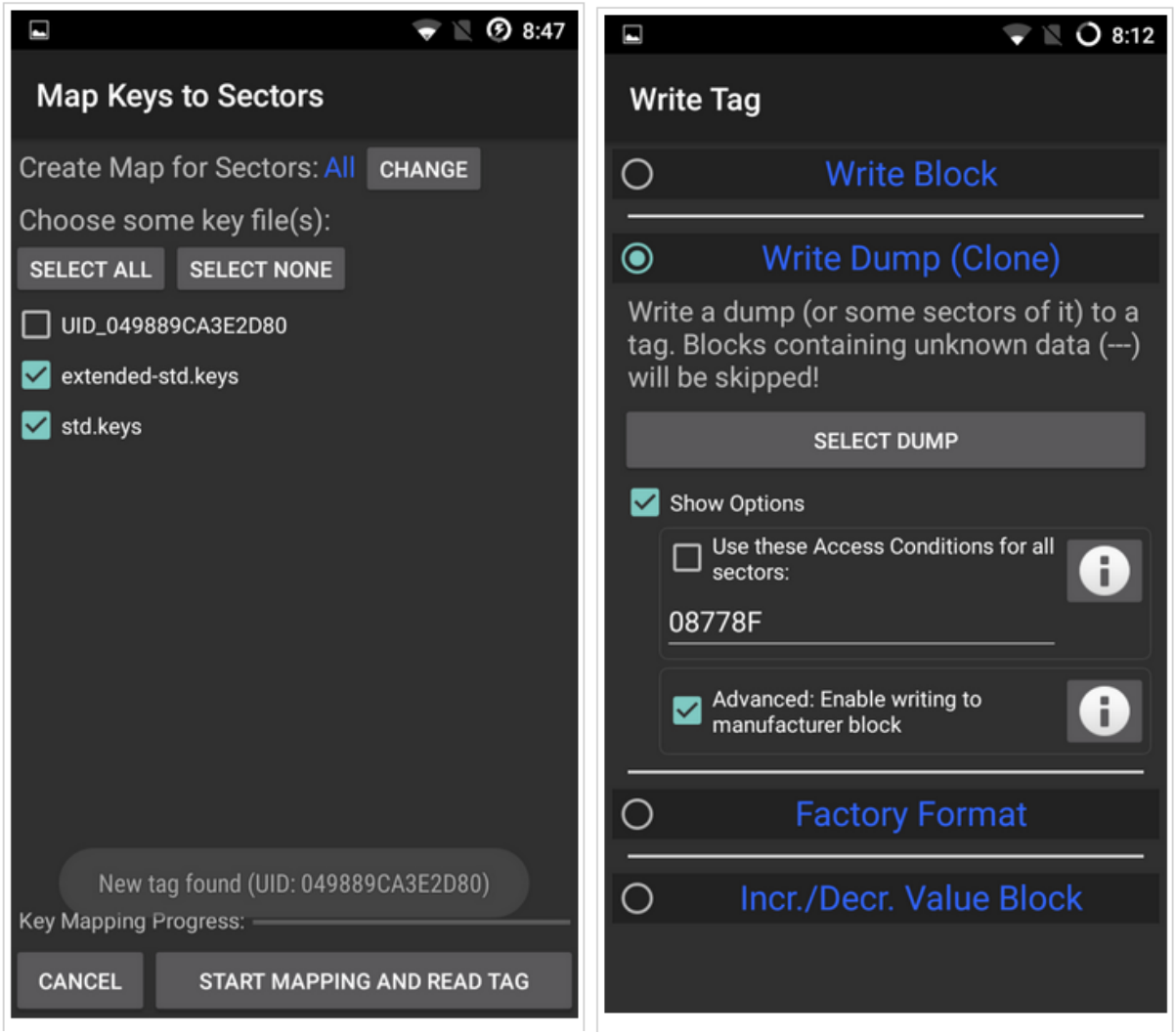
W sieci dostępnych jest wiele kart oraz breloczków pozwalających na zapis własnego UID. Istnieją również karty obsługujące zarówno częstotliwość 125 kHz i 13,56MHz. Karty 13,56 MHz można nabyć już w cenie około 2 zł za sztukę.

Rys. 1 Tagi umożliwiające zapis UID obsługujące częstotliwość 13,56 MHz i 135 kHz

Urządzenia do kopiowania kart zaczynają się od kwoty 40 zł. Najprostsze z nich obsługują tylko jedną częstotliwość i posiadają 2 przyciski: jeden do odczytu danych z aktualnie przyłożonej karty, a drugi do zapisu numeru z pamięci urządzenia. Bardziej zaawansowane posiadają klawiaturę do wprowadzenia numeru UID do zapisu, lub są wyposażone w złącze USB do współpracy z oprogramowaniem zewnętrznym.

Rys. 2 Przykład urządzenia zapisującego UID na kartę

Są również opisane przypadki kopiowania UID za pomocą telefonu z interfejsem NFC. Cały proces sprowadza się do wciśnięcia kilku przycisków w dedykowanej aplikacji.



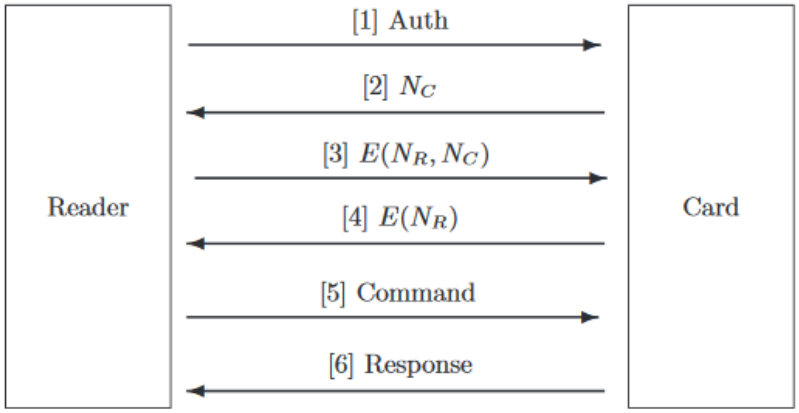
Rys. 3 Aplikacja służąca do kopiowania kart

Bardziej zaawansowanym urządzeniem do pracy z technologiami RFID są urządzenia typu proxmark3. Są to urządzenia dedykowane dla zaawansowanych użytkowników posiadających wiedzę z zakresu transmisji radiowych, elektroniki, układów FPGA oraz programowania. Proxmark3 to urządzenie wielkości talii kart pozwalające na działanie w trybach czytnika, emulatora karty oraz w trybie podsłuchu. Jest możliwość podłączenia do niego zewnętrznej anteny, co pozwoli na pracę zarówno w obszarze niskich częstotliwości (np. 125 kHz) i wysokich (13,56 MHz). Sygnał z anteny jest przetwarzany do postaci cyfrowej przez 8-bitowy przetwornik ADC. Za niskopoziomowe przetwarzanie sygnałów (modulacja, demodulacja) odpowiada programowalny układ FPGA Xilinx Spartan. Wstępnie przetworzone dane są następnie przekazywane do procesora ARM, który jest wykorzystywany do dalszych analiz danych. Cały projekt jest udostępniony na zasadzie open-source. Łatwo można znaleźć pliki Gerber części sprzętowej, aby samemu zlecić wykonanie urządzenia, oraz oprogramowanie do wgrania na urządzenie. Otwartość oprogramowania pozwala na dowolne modyfikacje zarówno w części FPGA jak i w oprogramowaniu

uruchamianym na CPU, przez co możliwe jest tworzenie własnych algorytmów filtrujących oraz przetwarzających dane przez zaawansowanych użytkowników. Domyślnie jest przygotowany zestaw podstawowych komend do pracy w trzech podstawowych trybach: odczytu danych, emulowaniu karty oraz podsłuchu transmisji. W oficjalnej dokumentacji jest wspomniane o około 30 obsługiwanych formatach kart.

Rys. 4 Proxmark3

Dane na kartach Mifare są szyfrowane za pomocą algorytmu CRYPTO1, który został stworzony przez firmę NXP. Wszelkie informacje na jego temat były tajne, co zapewniało bezpieczeństwo komunikacji. Szybko stał się celem ataków i prób złamania. W 2007 roku Karsten Nohl i Henryk Plötz za pomocą inżynierii wstecznej i analizy szyfrujących układów scalonych ujawnili procedurę inicjalizacji szyfrowania oraz układ generujący liczby losowe wykorzystywane przy inicjalizacji szyfrowania (LFSR). Generowany losowy numer jest zależny od czasu. Kolejnym krokiem do złamania CRYPTO1 było podsłuchanie komunikacji pomiędzy kartą a czytnikiem przy użyciu urządzenia proxmark3. W tym ataku wykorzystano odtwarzanie strumienia szyfrującego bez poznania kluczy szyfrujących. Poprawna procedura autoryzacji przebiega jak na poniższym rysunku.



Rys. 5 Procedura uwierzytelniania Mifare

Czytnik przesyłał żądanie autoryzacji, karta odpowiada losowo wybranym numerem – noncją. Następnie czytnik generuje własną noncję, szyfruje obie wartości za pomocą klucza i odsyła do karty. Jeśli karta po zdekodowaniu tej wiadomości otrzyma noncję którą wygenerowała, to czytnik potwierdza w ten sposób, że zna klucz i metodę szyfrowania. Następnie karta potwierdza znajomość klucza i algorytmu szyfrującego przesyłając do czytnika jego zaszyfrowaną noncję. Cała dalsza komunikacja jest szyfrowana. Do szyfrowania, po stronie czytnika jak i karty są wykorzystywane te same strumienie szyfrujące, które bit po bicie są poddawane operacji XOR z danymi do zaszyfrowania. Pierwszym krokiem ataku było podsłuchanie poprawnej komunikacji karty z czytnikiem. Następnie czytnik przesyłał żądania autoryzacji, aby karta odpowiedziała taką samą noncją jak w podsłuchanej, poprawnej komunikacji. Jest to możliwe ze względu na słabość generatora liczb pseudolosowych - generowane przez kartę noncje zależą od momentu przesłania żądania. Gdy karta odpowie taką samą noncją jak w zapisanej transmisji, czytnik przesyła zarejestrowaną wcześniej odpowiedź. W tym momencie modyfikując przesyłane komendy i wiedząc jaka powinna być odpowiedź karty jesteśmy w stanie wydobywać kolejne bity strumienia szyfrującego. Znając cały strumień szyfrujący i potrafiąc wymusić na karcie odpowiedź określoną noncją możliwe jest przesyłanie dowolnych komend do karty i deszyfrowanie odpowiedzi.

	INCREMENT	ACK	VALUE	TRANSFER	ACK
Plaintext	c1 04 f6 8b	0a	01 00 00 00 bb 4a	b0 04 ea 62	0a
Ciphertext	4c 88 31 bc!	0a!	e2 79!2a!14 35!6f!	04!81 2d!1e!	0c!

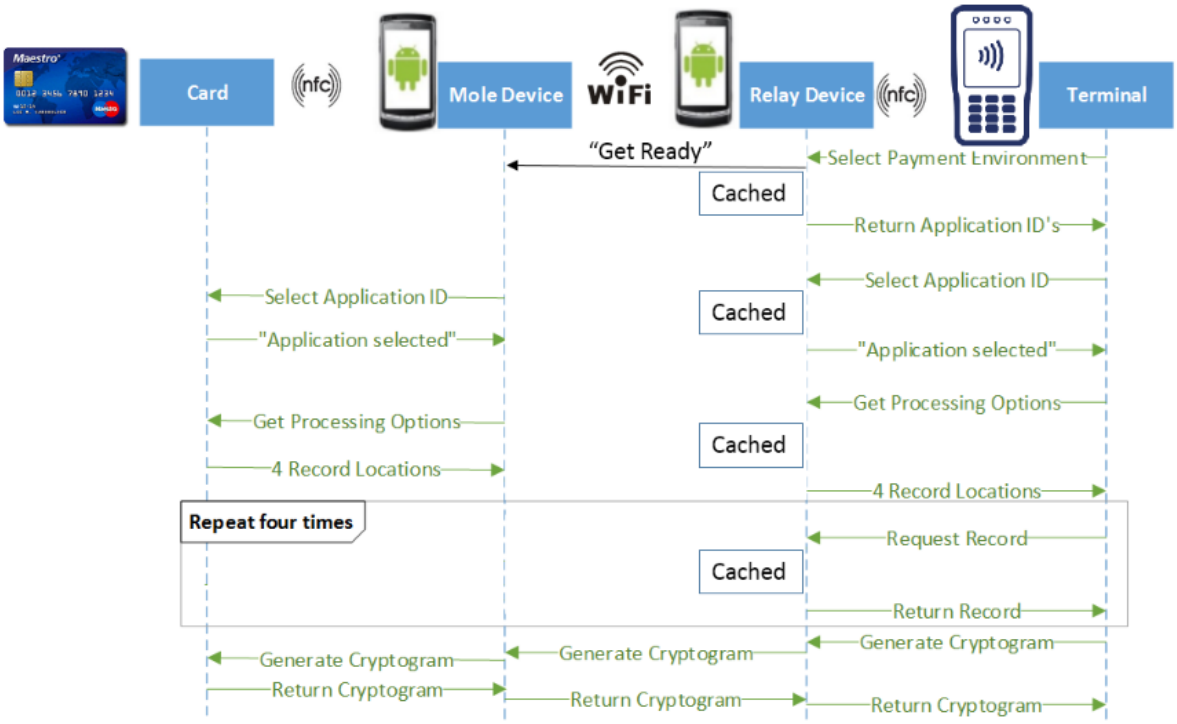
Rys. 6 Przykład odzyskiwania strumienia szyfrujqcego

Niemal równolegle Nicolas Courtois stworzył algorytm, który zaimplementowany na komputerze pozwalał na złamanie klucza w ciągu 200 sekund. Następnie powstały narzędzia MFOC i MFCUK, które pozwalają na odczyt całej zawartości karty bez konieczności posiadania zaawansowanej wiedzy o zabezpieczeniach kart Mifare.

Najbardziej spektakularnymi atakami na karty elektroniczne są te skierowane w karty płatnicze. Szczególnie podatne są karty z możliwością płacenia zbliżeniowego. Popularną metodą jest atak typu relay, polegający na stworzeniu tunelu przekierowującego komunikację pomiędzy kartą a terminalem. Zasada ataku jest bardzo prosta. Wymagane są dwa urządzenia, które umożliwiają pracę w trybie

czytnika i emulatora kart. Jedno urządzenie działa w pobliżu terminala płatniczego. Odczytuje ono komunikat inicjujący płatność zbliżeniową. Następnie za pomocą dowolnego kanału komunikacji (np. Bluetooth) ten komunikat jest przesyłany do drugiego urządzenia znajdującego się w pobliżu karty ofiary wymuszając odpowiedź z karty. Do wykonania transakcji potrzebna jest wymiana kilku wiadomości pomiędzy urządzeniami. Cały atak polega na przekazywaniu niezmienionych komunikatów pomiędzy kartą, a terminalem, czyli atakujący nie musi posiadać zaawansowanej wiedzy na temat kart elektronicznych i ich zabezpieczeń.

Bardzo ciekawe testy przeprowadził Jordi van den Breekel w 2015 roku. Dokonał on przekierowania komunikacji pomiędzy kartą zbliżeniową, a terminalem za pomocą telefonu z systemem Android i interfejsem NFC. Dzięki analizie komunikacji udało się wybrać komunikaty które są identyczne dla każdej transakcji. Przesyłając te komunikaty bezpośrednio z pamięci urządzeń atakujących, nie oczekując na żądania ze strony karty czy terminala udało się uzyskać zbliżone czasy całej transakcji, niwelując opóźnienie związane z przekierowywaniem komunikacji. Obala to pomysł zabezpieczenia przed tymi atakami poprzez odrzucanie transakcji trwających zbyt długo.



Rys. 7 Relay attack z wykorzystaniem pakietów przechowywanych w pamięci

Literatura:

https://timdows.com/projects/using-a-mobile-phone-to-clone-a-mifare-card/

https://github.com/Proxmark/proxmark3/wiki

http://www.blackhat.com/docs/asia-15/materials/asia-15-VandenBreekel-Relaying-EMV-Contactless-Transactions-Using-Off-The-Shelf-Android-Devices-wp.pdf

https://fc15.ifca.ai/preproceedings/paper_85.pdf

http://modsec.zimmerle.org/wireless-sec-papers/Practical%20Relay%20Attack%20on%20Contactless%20Transactions%20by%20Using%20NFC%20Mobile%20Phones.pdf

http://www.proxmark.org/documents/mifare_weakness.pdf