Bezpieczeństwo w Komunikacja bliskiego pola (NFC)

Mocne i słabe strony

Ernsta Haselsteinera i Klemensa Breitfußa

Półprzewodniki Philipsa
Mikronweg 1, 8101 Gratkorn, Austria
ernst.haselsteiner@philips.com
klemens.breitfuss@philips.com

Abstrakcyjny. W artykule dokonano kompleksowej analizy bezpieczeństwa w kontekście NFC. Nie ogranicza się do określonego zastosowania NFC, ale wykorzystuje podejście systemowe do analizy różnych aspektów bezpieczeństwa za każdym razem, gdy używany jest interfejs NFC. Autorzy chcą wyjaśnić wiele błędnych przekonań na temat bezpieczeństwa i NFC w różnych aplikacjach. W artykule wymieniono zagrożenia, jakie czyhają na technologię NFC oraz opisano rozwiązania chroniące przed tymi zagrożeniami. Wszystko to podano w kontekście obecnie dostępnego sprzętu NFC, aplikacji NFC i możliwego przyszłego rozwoju NFC.

1. Wstęp

NFC oznacza komunikację bliskiego pola. Szczegóły specyfikacji NFC można znaleźć w normie ISO 18092 [1]. Główną cechą NFC jest to, że jest to interfejs komunikacji bezprzewodowej z odległością roboczą ograniczoną do około 10 cm. Interfejs może pracować w kilku trybach. Tryby różnią się tym, czy urządzenie wytwarza własne pole RF, czy też urządzenie pobiera energię z pola RF generowanego przez inne urządzenie. Jeśli urządzenie generuje własne pole, nazywa się je urządzeniem aktywnym, w przeciwnym razie nazywa się je urządzeniem pasywnym. Urządzenia aktywne zwykle mają zasilanie, urządzenia pasywne zwykle nie (np. bezdotykowa karta inteligentna). Gdy dwa urządzenia komunikują się ze sobą, możliwe są trzy różne konfiguracje. Są one opisane w Tabeli 1:.

Tabela 1: Konfiguracje komunikacji

Urządzenie A	Urządzenie B	Opis
Aktywny	Aktywny	Kiedy urządzenie wysyła dane, generuje pole RF. Podczas oczekiwania na dane urządzenie nie generuje pola RF. Zatem pole RF jest generowane naprzemiennie przez urządzenie A i urządzenie B
Aktywny	Bierny	Pole RF jest generowane wyłącznie przez urządzenie A
Bierny	Aktywny	Pole RF jest generowane tylko przez urządzenie B

Konfiguracje te są ważne, ponieważ sposób przesyłania danych zależy od tego, czy urządzenie nadawcze znajduje się w trybie aktywnym, czy pasywnym.

W trybie aktywnym dane przesyłane są przy użyciu kluczowania z przesunięciem amplitudy (ASK) [1], [2]. Oznacza to, że podstawowy sygnał RF (13,56 MHz) jest modulowany danymi zgodnie ze schematem kodowania. Jeżeli szybkość transmisji wynosi 106 kbodów, schemat kodowania jest tzw. zmodyfikowanym kodowaniem Millera. Jeśli szybkość transmisji jest większa niż 106 kbodów, stosowany jest schemat kodowania Manchester. W obu schematach kodowania pojedynczy bit danych jest wysyłany w ustalonej szczelinie czasowej. Ten przedział czasowy jest podzielony na dwie połowy, zwane półbitami. W kodowaniu Millera zero jest kodowane z przerwą w pierwszej połowie bitu i bez przerwy w drugiej połowie bitu. Jedynka jest kodowana bez przerwy w pierwszym bicie, ale z przerwą w drugiej połowie bitu. W zmodyfikowanym kodowaniu Millera stosowane są dodatkowe zasady dotyczące kodowania zer. W przypadku jedynki, po której następuje zero, dwa kolejne półbity będą miały przerwę. Zmodyfikowane kodowanie Millera pozwala uniknąć tego poprzez kodowanie zera, które bezpośrednio następuje po jedynce z dwoma półbitami bez przerwy.

W kodowaniu Manchester sytuacja jest prawie taka sama, ale zamiast przerwy w pierwszej lub drugiej połowie bitu, cała połowa bitu jest albo pauzą, albo modulowana.
Oprócz schematu kodowania również siła modulacji zależy od szybkości transmisji.

Dla 106 kbodów stosowana jest modulacja 100%. Oznacza to, że podczas przerwy sygnał RF ma w rzeczywistości wartość zerową. W przerwie nie jest wysyłany żaden sygnał RF. Dla szybkości transmisji większych niż 106 kbodów stosowany jest współczynnik modulacji 10%. Zgodnie z definicją tego współczynnika modulacji [1] oznacza to, że w przerwie sygnał RF nie wynosi zero, ale stanowi około 82% poziomu sygnału nieprzerwanego. Ta różnica w sile modulacji jest bardzo ważna z punktu widzenia bezpieczeństwa, co opiszemy w dalszej części analizy bezpieczeństwa.

W trybie pasywnym dane są przesyłane przy użyciu modulacji słabego obciążenia. Dane są zawsze kodowane przy użyciu kodowania Manchester z modulacją 10%. Dla 106 kbodów do modulacji używana jest częstotliwość podnośnej, dla szybkości transmisji większych niż 106 kbodów modulowany jest podstawowy sygnał RF o częstotliwości 13,56 MHz.

Oprócz trybu aktywnego i pasywnego, urządzenie może pełnić dwie różne role w komunikacji NFC. NFC opiera się na koncepcji wiadomości i odpowiedzi. Oznacza to, że jedno urządzenie A wysyła wiadomość do innego urządzenia B, a urządzenie B odsyła odpowiedź. Urządzenie B nie może wysłać żadnych danych do urządzenia A bez uprzedniego otrzymania wiadomości od urządzenia A, na którą mogłoby odpowiedzieć. Rolę urządzenia A, które rozpoczyna wymianę danych, nazywa się inicjatorem, rolę drugiego urządzenia nazywa się celem.
Poniższa tabela 2 przedstawia wszystkie możliwe kombinacje tej roli w odniesieniu do trybu aktywnego lub pasywnego. Niemożliwa jest tylko kombinacja Inicjatora i Pasywności.

Tabela 2: Możliwe kombinacje Aktywne/Pasywne z Inicjatorem/Celem

	Inicjator	Cel
Aktywny	Możliwy	Możliwy
Bierny	Niemożliwe	Możliwy

Ponadto należy wspomnieć, że komunikacja NFC nie ogranicza się do pary dwóch urządzeń. W rzeczywistości jedno urządzenie inicjujące może komunikować się z wieloma urządzeniami docelowymi. W tym przypadku wszystkie urządzenia docelowe są włączone jednocześnie, ale przed wysłaniem wiadomości urządzenie inicjujące musi wybrać urządzenie odbierające. Komunikat musi następnie zostać zignorowany przez wszystkie niewybrane urządzenia docelowe. Tylko wybrane urządzenie docelowe może odpowiedzieć na otrzymane dane. Dlatego nie jest możliwe przesyłanie danych do więcej niż jednego urządzenia w tym samym czasie (tzn. nie jest możliwe rozsyłanie komunikatów).

2 aplikacje

Nie da się dać pełnego obrazu zastosowań NFC, gdyż NFC to tylko interfejs. W poniższych podrozdziałach przedstawiono trzy przykładowe zastosowania. Należy je postrzegać jako typowe przypadki użycia i wybrać je w celu uzasadnienia listy możliwych zagrożeń podanej w następnej sekcji.

2.1 Token zbliżeniowy

Dotyczy to wszystkich aplikacji, które wykorzystują NFC do pobierania niektórych danych z tokena pasywnego. Tokenem pasywnym może być bezdotykowa karta inteligentna, etykieta RFID lub breloczek do kluczy. Ponadto token może być fizycznie umieszczony w urządzeniu bez żadnych połączeń elektrycznych z tym urządzeniem.

Co ważne, jedynym interfejsem tokena jest interfejs zbliżeniowy.
Oznacza to, że nie może działać jako łącze komunikacyjne z głównym procesorem urządzenia, ponieważ nie może połączyć się z głównym procesorem urządzenia poprzez interfejs kontaktowy. Załóżmy też, że token ma dość ograniczoną moc obliczeniową, więc nie może obsługiwać żadnych skomplikowanych protokołów. Podstawowym zastosowaniem byłoby przechowywanie niektórych danych, które następnie można wygodnie odczytać za pomocą aktywnego urządzenia NFC. Przykładami takich danych może być adres URL przechowywany w tagu produktu konsumenckiego lub podręcznik użytkownika takiego produktu. Użytkownik może następnie przeczytać tag i automatycznie uzyskać łącze do strony pomocy technicznej tego produktu. Innym przykładem byłoby przechowywanie danych konfiguracyjnych niezbędnych do uzyskania dostępu do sieci Wi-Fi. Nowi użytkownicy będą mogli wówczas łatwo skonfigurować swoje laptopy do podłączenia do sieci.

2.2 Bilety/mikropłatności

w tej przykładowej aplikacji interfejs NFC służy do przesyłania cennych informacji. Dane biletu lub mikropłatności przechowywane są na bezpiecznym urządzeniu. Może to być bezdotykowa karta inteligentna, ale równie dobrze może to być telefon komórkowy. Gdy użytkownik chce dokonać płatności lub skorzystać z zapisanego biletu, przedstawia urządzenie czytnikowi, który sprawdza otrzymane informacje i przetwarza płatność lub akceptuje/odrzuca bilet.

W tym przykładzie zastosowania urządzenie użytkownika musi być w stanie wykonać określony protokół z czytnikiem. W większości przypadków prosta operacja odczytu nie będzie wystarczająca. Ponadto urządzenie użytkownika prawdopodobnie będzie wyposażone w drugi interfejs, który służy do ładowania pieniędzy lub kupowania biletów. Ten drugi interfejs można na przykład połączyć z procesorem telefonu komórkowego. Dane dotyczące biletów można następnie załadować do telefonu komórkowego za pośrednictwem sieci komórkowej.

W tej aplikacji czasami używany jest termin „Bezpieczny NFC”. Nie oznacza to jednak wcale, że łącze NFC jest w jakiś sposób zabezpieczone. Faktycznie, nazwa jest raczej błędna

prowadzący. Nazwa oznacza po prostu konfigurację wykorzystującą chip sprzętowy NFC w połączeniu z chipem karty inteligentnej. Powinna nazywać się „Bezpieczna karta inteligentna i NFC”, ale niestety dość często używana jest krótsza nazwa.

2.3 Parowanie urządzeń

W tej aplikacji dwa komunikujące się urządzenia będą należeć do tej samej grupy urządzeń. Przykładem może być laptop i aparat cyfrowy. Użytkownik chce nawiązać połączenie Bluetooth między dwoma urządzeniami w celu wymiany danych obrazu. Połączenie Bluetooth jest ustanawiane poprzez zbliżenie dwóch urządzeń do siebie i uruchomienie między nimi określonego protokołu przez NFC. Dzięki temu użytkownik staje się oczywisty, które dwa urządzenia są faktycznie połączone, i odciąża go od poruszania się po menu i wybierania odpowiednich urządzeń z list możliwych partnerów komunikacyjnych.

Należy zauważyć, że samo połączenie NFC w tym przykładzie służy wyłącznie do nawiązania połączenia Bluetooth. Dane obrazu nie są przesyłane przez NFC, ponieważ szerokość pasma NFC jest po prostu zbyt mała, aby przesyłać duże ilości danych.

3 zagrożenia

3.1 Podsłuch

Ponieważ NFC jest interfejsem komunikacji bezprzewodowej, oczywiste jest, że podsłuchiwanie jest ważną kwestią. Gdy dwa urządzenia komunikują się za pośrednictwem NFC, do komunikacji wykorzystują fale RF. Osoba atakująca może oczywiście użyć anteny do odbioru przesyłanych sygnałów.

Eksperymentując lub przeglądając literaturę, atakujący może uzyskać wymaganą wiedzę na temat sposobu wyodrębnienia przesyłanych danych z odebranego sygnału RF.
Należy założyć, że sprzęt wymagany do odbioru sygnału RF oraz sprzęt do dekodowania sygnału RF będą dostępne dla atakującego, ponieważ nie jest konieczny żaden specjalny sprzęt.

Komunikacja NFC odbywa się zwykle pomiędzy dwoma urządzeniami znajdującymi się blisko siebie. Oznacza to, że nie są one oddalone od siebie o więcej niż 10 cm (zwykle mniej). Główne pytanie dotyczy tego, jak blisko musi znajdować się atakujący, aby móc odzyskać użyteczny sygnał RF. Niestety, nie ma prawidłowej odpowiedzi na to pytanie. Powodem jest ogromna liczba parametrów decydujących o odpowiedzi. Na przykład odległość zależy od następujących parametrów, a jest ich o wiele więcej.

- Charakterystyka pola RF dla danego urządzenia nadawczego (tj. geometria anteny, ekranowanie) wpływ obudowy, płytki drukowanej, środowiska)
- Charakterystyka anteny atakującego (tzn. geometria anteny, możliwość zmiany pozycji we wszystkich 3 wymiarach)
- Jakość odbiorcy atakującego
- Jakość dekodera sygnału RF atakującego
- Konfiguracja miejsca, w którym przeprowadzany jest atak (np. bariery, takie jak ściany lub napotkane al, poziom hałasu)
- Moc wysyłana przez urządzenie NFC

Dlatego dowolna podana dokładna liczba będzie ważna tylko dla pewnego zestawu podanych powyżej parametrów i nie może być wykorzystana do wyprowadzenia ogólnych wytycznych dotyczących bezpieczeństwa.

Dodatkowo istotne jest w jakim trybie pracuje nadawca danych. Oznacza to, czy nadawca generuje własne pole RF (tryb aktywny), czy też nadawca wykorzystuje pole RF generowane przez inne urządzenie (tryb pasywny).
W obu przypadkach inny jest sposób przesyłania danych i znacznie trudniej jest podsłuchać urządzenia wysyłające dane w trybie pasywnym.

Aby nie pozostawić czytelnika bez pojęcia, jak duże są odległości podsłuchu, podajemy następujące liczby, które, jak stwierdzono powyżej, w ogóle nie są ważne, ale mogą jedynie służyć przybliżonemu wyobrażeniu o te odległości.

Gdy urządzenie wysyła dane w trybie aktywnym, podsłuch można wykonać do odległości około 10 m, natomiast gdy urządzenie wysyłające znajduje się w trybie pasywnym, odległość ta ulega znacznemu zmniejszeniu do około 1 m.

3.2 Uszkodzenie danych

Zamiast po prostu słuchać, atakujący może również spróbować zmodyfikować dane przesyłane za pośrednictwem interfejsu NFC. W najprostszym przypadku atakujący chce po prostu zakłócić komunikację w taki sposób, aby odbiorca nie był w stanie zrozumieć danych przesyłanych przez drugie urządzenie.

Uszkodzenie danych można osiągnąć poprzez transmisję prawidłowych częstotliwości widma danych we właściwym czasie. Prawidłowy czas można obliczyć, jeśli atakujący dobrze rozumie zastosowany schemat modulacji i kodowanie. Atak ten nie jest zbyt skomplikowany, ale nie pozwala atakującemu na manipulację rzeczywistymi danymi. Zasadniczo jest to atak typu „odmowa usługi”.

3.3 Modyfikacja danych

Modyfikując dane, atakujący chce, aby urządzenie odbierające faktycznie otrzymało pewne ważne, ale zmanipulowane dane. To bardzo różni się od zwykłego uszkodzenia danych.

Wykonalność tego ataku w dużym stopniu zależy od zastosowanej siły modulacji amplitudy. Dzieje się tak dlatego, że dekodowanie sygnału jest inne dla modulacji 100% i 10%.

W przypadku modulacji 100% dekoder zasadniczo sprawdza dwa półbity pod kątem włączenia sygnału RF (bez przerwy) lub wyłączenia sygnału RF (pauza). Aby dekoder zrozumiał jedynkę jako zero lub odwrotnie, atakujący musi zrobić dwie rzeczy. Najpierw należy wypełnić przerwę w modulacji częstotliwością nośną. Jest to wykonalne. Ale po drugie, atakujący musi wygenerować pauzę w sygnale RF, który zostanie odebrany przez legalnego odbiorcę. Oznacza to, że atakujący musi wysłać sygnał RF taki, aby sygnał ten idealnie pokrywał się z oryginalnym sygnałem na antenie odbiornika, dając w odbiorniku sygnał zerowy.
Jest to praktycznie niemożliwe. Jednakże, dzięki zmodyfikowanemu kodowaniu Millera w przypadku dwóch kolejnych, atakujący może zamienić drugi na zero, wypełniając pauzę kodującą drugą. Dekoder nie zauważyłby wówczas żadnej przerwy w drugim bicie i zdekodowałby to jako prawidłowe zero, ponieważ jest poprzedzone jedynką. Dlatego w modulacji 100% atakujący nigdy nie może zmienić bitu o wartości 0 na bit o wartości 1, ale atakujący może zmienić bit o wartości 1 na bit o wartości 0, w przypadku gdy ten bit jest poprzedzony bitem o wartości 1 (tzn. z prawdopodobieństwem 0,5).

Przy modulacji 10% dekoder mierzy oba poziomy sygnału (82% i pełny) i porównuje je. Jeśli znajdują się w prawidłowym zakresie, sygnał jest ważny i zostaje zdekodowany.
Osoba atakująca może spróbować dodać sygnał do sygnału 82% w taki sposób, że sygnał 82% pojawi się jako sygnał Pełny, a rzeczywisty sygnał Pełny stanie się sygnałem 82%. W ten sposób dekodowanie zdekoduje prawidłowy bit o wartości przeciwnej do bitu wysłanego przez właściwego nadawcę.
To, czy atak jest wykonalny, zależy w dużej mierze od dynamicznego zakresu wejściowego odbiornika.
Jest bardzo prawdopodobne, że znacznie wyższy poziom zmodyfikowanego sygnału przekroczy możliwy zakres wejściowy, ale w niektórych sytuacjach nie można tego całkowicie wykluczyć.

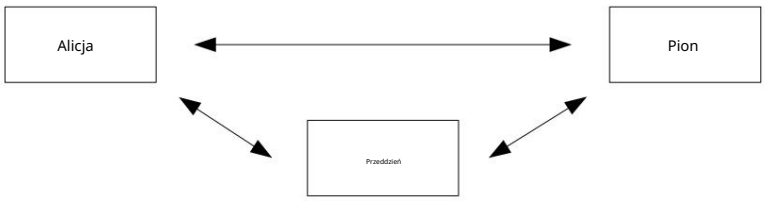
Wniosek jest taki, że dla zmodyfikowanego kodowania Millera ze 100% ASK atak ten jest wykonalny dla niektórych bitów i niemożliwy dla innych bitów, natomiast dla kodowania Manchester z 10% ASK ten atak jest możliwy na wszystkich bitach.

3.4 Wprowadzanie danych

Oznacza to, że atakujący wstawia wiadomości do wymiany danych pomiędzy dwoma urządzeniami. Jest to jednak możliwe tylko w przypadku, gdy automatyczna sekretarka potrzebuje bardzo dużo czasu na odpowiedź. Osoba atakująca mogłaby wówczas wysłać swoje dane wcześniej niż prawidłowy odbiorca. Wstawienie zakończy się sukcesem tylko wtedy, gdy wprowadzone dane będą mogły zostać przesłane, zanim oryginalne urządzenie zacznie udzielać odpowiedzi. Jeśli oba strumienie danych nakładają się, dane zostaną uszkodzone.

3.5 Atak człowieka pośrodku

W klasycznym ataku typu Man-in-the-Middle Attack dwie strony, które chcą ze sobą porozmawiać, zwane Alicją i Bobem, zostają oszukane przez atakującą Eve i wciągnięte w trójstronną rozmowę. Pokazano to na rysunku 1.



Rysunek 1 Konfiguracja typu „człowiek pośrodku”.

Alicja i Bob nie mogą zdawać sobie sprawy z tego, że ze sobą nie rozmawiają, ale że zarówno wysyłają, jak i odbierają dane od Ewy. Taka konfiguracja stanowi klasyczne zagrożenie w nieuwierzytelnionych protokołach uzgadniania kluczy, takich jak protokół Diffiego-Hellmanna. Alicja i Bob chcą uzgodnić tajny klucz, którego następnie użyją do bezpiecznego kanału. Jednakże, ponieważ Ewa jest pośrodku, możliwe jest, że Ewa ustali klucz z Alicją i inny klucz z Bobem. Kiedy Alicja i Bob później używają klucza do zabezpieczenia danych, Eve jest w stanie podsłuchiwać komunikację, a także manipulować przesyłanymi danymi.

Jak by to działało, gdyby połączenie między Alicją i Bobem było łączem NFC?

Zakładając, że Alicja korzysta z trybu aktywnego, a Bob byłby w trybie pasywnym, mamy następującą sytuację. Alicja generuje pole RF i wysyła dane do Boba. Jeśli Ewa będzie wystarczająco blisko, może podsłuchać dane przesyłane przez Alicję. Dodatkowo musi aktywnie zakłócać transmisję Alicji, aby mieć pewność, że Bob nie otrzyma danych. Jest to możliwe w przypadku Ewy, ale Alicja może to również wykryć. W przypadku wykrycia zakłócenia Alicja może zatrzymać protokół uzgodnienia klucza. Załóżmy, że Alicja nie sprawdza

dla aktywnych zakłóceń, dzięki czemu protokół może być kontynuowany. W następnym kroku Ewa musi wysłać dane Bobowi. To już jest problem, ponieważ pole RF generowane przez Alicję wciąż tam jest, więc Eve musi wygenerować drugie pole RF. Powoduje to jednak, że dwa pola RF będą aktywne w tym samym czasie. Praktycznie niemożliwe jest idealne dopasowanie tych dwóch pól RF. Dlatego Bob praktycznie nie ma możliwości zrozumienia danych przesłanych przez Ewę. Z tego powodu oraz możliwości wykrycia ataku przez Alicję znacznie wcześniej, dochodzimy do wniosku, że w tej konfiguracji atak typu Man-in-the-Middle jest praktycznie niemożliwy.

Jedyną inną możliwą konfiguracją jest to, że Alicja używa trybu aktywnego, a Bob również używa trybu aktywnego. W tym przypadku Alicja wysyła Bobowi pewne dane. Ewa może wylistować, a Ewa ponownie musi zakłócić transmisję Alicji, aby mieć pewność, że Bob nie otrzyma danych. W tym momencie Alicja mogła już wykryć zakłócenie dokonane przez Eve i zatrzymać protokół. Załóżmy ponownie, że Alicja nie sprawdza tego i protokół jest kontynuowany. W następnym kroku Ewa będzie musiała wysłać dane Bobowi. Na pierwszy rzut oka wygląda to teraz lepiej, ponieważ Alicja wyłączyła pole RF w ramach komunikacji typu aktywny-aktywny. Teraz Eve włącza pole RF i może wysyłać dane. Problem polega na tym, że także Alice słucha, oczekując odpowiedzi od Boba. Zamiast tego otrzyma dane przesłane przez Eve i będzie mogła ponownie wykryć problem w protokole i zatrzymać protokół. W tej konfiguracji Ewa nie może wysłać danych ani do Alicji, ani do Boba i upewnić się, że dane te nie zostaną odebrane odpowiednio przez Boba lub Alicję.

Twierdzimy, że z powyższych powodów przeprowadzenie ataku typu Man-in-the-Middle w rzeczywistym scenariuszu jest praktycznie niemożliwe.

4 Rozwiązania i zalecenia

4.1 Podsłuch

Jak opisano w sekcji 3.1, NFC samo w sobie nie jest w stanie chronić przed podsłuchem. Należy zauważyć, że dane przesyłane w trybie pasywnym są znacznie trudniejsze do podsłuchania, ale samo użycie trybu pasywnego prawdopodobnie nie wystarczy w przypadku większości aplikacji przesyłających wrażliwe dane.

Jedynym realnym rozwiązaniem problemu podsłuchu jest ustanowienie bezpiecznego kanału zgodnie z opisem w sekcji 4.6.

4.2 Uszkodzenie danych

Urządzenia NFC mogą przeciwdziałać temu atakowi, ponieważ mogą sprawdzać pole RF podczas przesyłania danych. Jeśli urządzenie NFC to zrobi, będzie w stanie wykryć atak. Moc potrzebna do uszkodzenia danych jest znacznie większa niż moc, którą może wykryć urządzenie NFC. Zatem każdy taki atak powinien być wykrywalny.

4.3 Modyfikacja danych

Ochronę przed modyfikacją danych można osiągnąć na różne sposoby.

Używając 106 kb/s w trybie aktywnym, atakujący nie może zmodyfikować wszystkich danych przesyłanych łączem RF, jak opisano w sekcji 3.3. Oznacza to, że dla obu kierunków potrzebny byłby tryb aktywny chroniący przed modyfikacją danych. Chociaż jest to możliwe, ma to jednak poważną wadę: ten tryb jest najbardziej podatny na podsłuchiwanie.

świst. Również ochrona przed modyfikacjami nie jest doskonała, ponieważ nawet przy 106 kbodach niektóre bity można modyfikować. Preferowane mogą być zatem dwie pozostałe opcje.

Urządzenia NFC mogą sprawdzać pole RF podczas wysyłania. Oznacza to, że urządzenie wysyłające może stale sprawdzać, czy nie doszło do takiego ataku, a w przypadku wykrycia ataku może zatrzymać transmisję danych.

Trzecim i prawdopodobnie najlepszym rozwiązaniem byłby bezpieczny kanał opisany w sekcji 4.6.

4.4 Wprowadzanie danych

Istnieją trzy możliwe środki zaradcze. Po pierwsze, automatyczna sekretarka odpowiada bez opóźnienia. W tym przypadku atakujący nie może być szybszy niż właściwe urządzenie. Osoba atakująca może być tak szybka, jak właściwe urządzenie, ale jeśli dwa urządzenia odpowiedzą w tym samym czasie, prawidłowe dane nie zostaną odebrane.

Drugim możliwym środkiem zaradczym jest nasłuchiwanie przez automatyczną sekretarkę kanału w czasie, gdy jest on otwarty i w momencie rozpoczęcia transmisji. Urządzenie może wtedy wykryć atakującego, który chce wprowadzić dane.

Trzecią opcją jest ponownie bezpieczny kanał między dwoma urządzeniami.

4.5 Atak człowieka pośrodku

Jak już wspomniano w sekcji 3.5, praktycznie niemożliwe jest wykonanie ataku typu Man-in-the-Middle na łączu NFC. Zaleca się używanie trybu komunikacji aktywno-pasywnej, tak aby pole RF było stale generowane przez jedną z ważnych stron.
Dodatkowo strona aktywna powinna nasłuchiwać sygnału RF podczas wysyłania danych, aby móc wykryć wszelkie zakłócenia spowodowane przez potencjalnego atakującego.

4.6 Bezpieczny kanał dla NFC

Utworzenie bezpiecznego kanału między dwoma urządzeniami NFC jest zdecydowanie najlepszym podejściem do ochrony przed podsłuchiwaniem i wszelkiego rodzaju atakami polegającymi na modyfikacji danych.

Ze względu na nieodłączną ochronę NFC przed atakami typu Man-in-the-Middle-
Konfiguracja bezpiecznego kanału jest łatwa i prosta.

Do ustalenia wspólnego sekretu między dwoma urządzeniami można zastosować standardowy protokół uzgadniania kluczy, taki jak Diffie-Hellmann oparty na RSA [4] lub krzywych eliptycznych. Ponieważ Man-in-the-Middle nie stanowi zagrożenia, standardowa, nieuwierzytelniona wersja Diffie-Hellman działa doskonale.

Wspólny sekret można następnie wykorzystać do uzyskania klucza symetrycznego, takiego jak 3DES lub AES, który jest następnie używany w bezpiecznym kanale zapewniającym poufność, integralność i autentyczność przesyłanych danych. Dla takiego bezpiecznego kanału można zastosować różne tryby pracy dla 3DES i AES, co można znaleźć w literaturze [3].

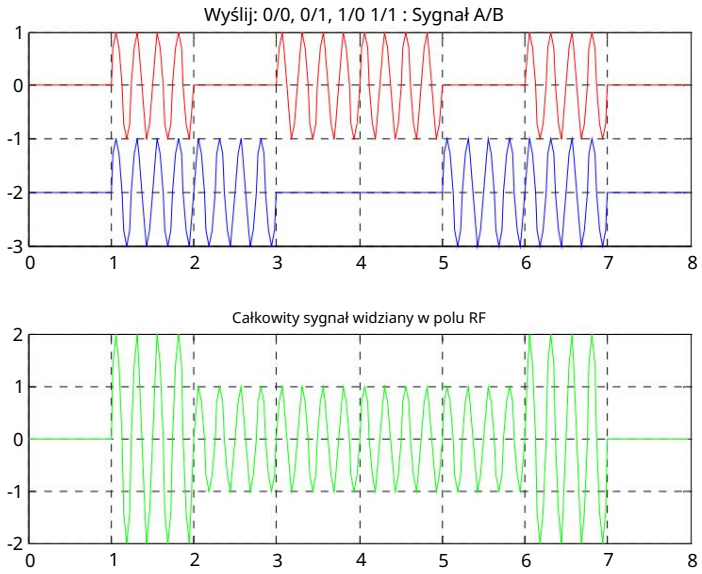
4.6.1 Specyficzna umowa kluczowa NFC

Oprócz standardowego mechanizmu uzgadniania kluczy możliwe jest również wdrożenie uzgadniania kluczy specyficznego dla NFC. Ten nie wymaga żadnej kryptografii asymetrycznej i dlatego znacznie zmniejsza wymagania obliczeniowe. Teoretycznie zapewnia także doskonałe bezpieczeństwo.

Schemat działa tylko ze 100% ASK i nie jest częścią standardu ISO dotyczącego NFC. Pomysł jest taki, że oba urządzenia, powiedzmy urządzenie A i urządzenie B, wysyłają losowe dane w tym samym czasie. W fazie konfiguracji oba urządzenia synchronizują się pod względem dokładnego taktowania bitów, a także amplitud i faz sygnału RF. Jest to możliwe, ponieważ urządzenia mogą jednocześnie wysyłać i odbierać. Po tej synchronizacji A i B mogą nadawać dokładnie w tym samym czasie, z dokładnie tymi samymi amplitudami i fazami.

Wysyłając losowe bity 0 lub 1, każde urządzenie nasłuchuje również pola RF. Gdy oba urządzenia wysyłają zero, suma sygnału wynosi zero, a atakujący, który nasłuchuje, będzie wiedział, że oba urządzenia wysłały zero. To nie pomaga. To samo dzieje się, gdy zarówno A, jak i B wysyłają jedynkę. Suma stanowi podwójny sygnał RF i atakujący wie, że oba urządzenia wysłały jeden. Robi się interesująco, gdy A wysyła zero, a B wysyła jedynkę i odwrotnie.

W tym przypadku oba urządzenia wiedzą, co wysłało drugie urządzenie, ponieważ urządzenia wiedzą, co same wysłały. Jednak osoba atakująca widzi tylko sumę sygnału RF i nie jest w stanie ustalić, które urządzenie wysłało zero, a które jedynkę. Pomysł ten ilustruje rysunek 2. Górny wykres przedstawia sygnały wytwarzane przez A na czerwono i przez B na niebiesko. A wysyła cztery bity: 0, 0, 1 i 1. B wysyła cztery bity: 0, 1, 0 i 1. Dolny wykres przedstawia sumę sygnału widzianą przez atakującego. Pokazuje, że dla kombinacji bitów (A wysyła 0, B wysyła 1) i (A wysyła 1, B wysyła 0) wynik dla atakującego jest absolutnie taki sam i atakujący nie jest w stanie rozróżnić tych dwóch przypadków.



Rysunek 2 Kluczowa umowa dotycząca NFC

Obydwa urządzenia odrzucają teraz wszystkie bity, w przypadku których oba urządzenia wysłały tę samą wartość, i zbierają wszystkie bity, w przypadku których oba urządzenia wysłały różne wartości. Mogą albo odebrać bity wysłane przez A, albo przez B. Należy to uzgodnić przy uruchomieniu, ale to nie ma znaczenia. W ten sposób A i B mogą uzgodnić dowolny, długi wspólny sekret. Nowy bit jest generowany z prawdopodobieństwem 50%. Zatem wygenerowanie 128-bitowego wspólnego sekretu wymagałoby przybliżenia-

maksymalnie 256 bitów do przesłania. Przy szybkości transmisji 106 kbodów zajmuje to około 2,4 ms i dlatego jest wystarczająco szybki dla wszystkich zastosowań.

Bezpieczeństwo tego protokołu w praktyce zależy od jakości synchronizacji jaka jest osiągnięta pomiędzy obydwoma urządzeniami. Oczywiście, jeśli podsłuchujący potrafi odróżnić dane wysłane przez A od danych przesłanych przez B, protokół jest uszkodzony. Dane muszą być zgodne pod względem amplitudy i fazy. Gdy różnice między A i B są znacznie niższe od poziomu szumu odbieranego przez podsłuchującego, protokół jest bezpieczny. Poziom bezpieczeństwa zależy zatem również od jakości sygnału w odbiorniku. Jakość sygnału zależy jednak ponownie od wielu parametrów (np. odległości) osoby podsłuchującej. W praktyce oba urządzenia A i B muszą mieć na celu idealną synchronizację. Można to osiągnąć tylko wtedy, gdy co najmniej jedno z A lub B jest aktywnym urządzeniem do przeprowadzania tej synchronizacji.

Należy zauważyć, że w niedawno opublikowanej pracy [5] ten sam pomysł na kluczową zgodność pomiędzy czytnikiem RF a znacznikiem RF jest przedstawiony w nieco innej konfiguracji. W papierze zastosowano specjalny tzw. hałaśliwy tag. Ten zaszumiony znacznik to standardowy znacznik RFID, który działa jak strona trzecia wstawiająca losowo wyglądające bity do komunikacji między prawdziwym znacznikiem a prawdziwym czytnikiem. Czytnik może jednak obliczyć bity wysłane przez znacznik zaszumiony, a następnie obliczyć bity wysłane przez znacznik rzeczywisty. Problem, jaki widzimy w tym podejściu, polega na tym, że zaszumiony tag nie będzie w stanie przeprowadzić żadnej synchronizacji z prawdziwym tagiem. Byłoby to zbyt skomplikowane dla prostego tagu. Dlatego uważamy, że takie podejście nie może sprawdzić się w praktyce. Aby bezpiecznie uruchomić ten protokół, potrzebne byłoby bardziej wyrafinowane hałaśliwe urządzenie zamiast hałaśliwego znacznika.

5. Wniosek

Zaprezentowaliśmy typowe przypadki użycia interfejsów NFC. Opracowano i zaadresowano listę zagrożeń. Technologia NFC sama w sobie nie jest w stanie zapewnić ochrony przed podsłuchem lub modyfikacją danych. Jedynym rozwiązaniem pozwalającym to osiągnąć jest utworzenie bezpiecznego kanału poprzez NFC. Można to zrobić bardzo łatwo, gdyż łącze NFC nie jest podatne na atak Man-in-the-Middle. Dlatego też w celu zapewnienia standardowego bezpiecznego kanału można zastosować dobrze znane i łatwe do zastosowania techniki uzgadniania kluczy bez uwierzytelniania.
Ta odporność na ataki Man-in-the-Middle sprawia, że NFC jest idealną metodą bezpiecznego parowania urządzeń. Dodatkowo wprowadziliśmy mechanizm uzgadniania kluczy specyficzny dla NFC, który zapewnia tanie i szybkie bezpieczne uzgadnianie kluczy.

Bibliografia

[1] „Technologia informatyczna – Telekomunikacja i wymiana informacji między systemami – Komunikacja bliskiego zasięgu – Interfejs i protokół (NFCIP-1)”, ISO/IEC 18092, wydanie pierwsze, 2004-04-01.

[2] Klaus Finkenzeller, „Podręcznik RFID”, Hanser Verlag, 2002.

[3] Morris Dworkin, „Zalecenia dotyczące trybów działania szyfru blokowego”, NIST Special Publikacja 800-38A, 2001.

[4] W. Diffie i ME Hellman, „Nowe kierunki kryptografii”, IEEE Transactions on In- Teoria formacji 22 (1976), 644-654.

[5] C. Castelluccia i G. Avoine, „Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags”, Proceedings of CARDIS 2006, LNCS 3928, 289-299, 2006.