DOI: 10.5604/01.3001.0009.5190

BEZPIECZEŃSTWO HOTSPOTÓW W AUTOBUSACH

Grzegorz Kozieł[1], Jakub Maluga[2]
[1]Politechnika Lubelska, Wydział Elektrotechniki i Informatyki, Instytut Informatyki, [2]Politechnika Lubelska, Wydział Elektrotechniki i Informatyki

Streszczenie. *W artykule omówiony został aspekt bezpieczeństwa mobilnych punktów dostępowych. Takie punkty często są montowane w autobusach na potrzeby pasażerów. Jednak kluczowym problemem jest właściwe zabezpieczenie transmisji pomiędzy klientami a punktem dostępowym. W artykule przeanalizowane zostały możliwości zabezpieczenia i podatności na ataki popularnych standardów zabezpieczeń.*

Słowa kluczowe: sieci bezprzewodowe, bezpieczeństwo

SECURITY OF HOTSPOTS IN BUSES

Abstract. *Paper discusses the security of the mobile hotspots mounted in buses. The analysis of vulnerabilities is done. Chosen aspects of security are examined. Finally the proposal of proper mobile hotspot protection is described.*

Keywords: wireless networks, security

Wstęp

Potrzeba dostępu do Internetu staje się coraz bardziej zauważalna. Niemożliwe jest wykonywanie wielu zawodów bez połączenia z Internetem. Również komunikacja oraz rozrywka przenoszą się w coraz większym stopniu do sieci. Użytkownicy żądają ciągłego dostępu do Internetu, również w podróży. Udostępnienie łącza osobom podróżującym często stanowi o przewadze konkurencyjnej przewoźnika. Dlatego coraz powszechniejsze staje się udostępnianie łącza przewożonym pasażerom. Jednak niesie to ze sobą różnorodne zagrożenia. Przede wszystkim konieczne jest zapewnienie bezpieczeństwa transmisji pomiędzy klientami a punktem dostępowym. Ponadto pożądanym będzie zabezpieczenie przed dostępem osób niepowołanych, czyli podróżujących w sąsiednich pojazdach.

W celu zapewnienia bezpieczeństwa transmisji należy zapewnić mechanizmy uwierzytelniania klientów, szyfrowania transmisji, ochrony przed wzajemnym podsłuchiwaniem się klientów sieci. Nie można też pomijać zagrożeń jakie niosą za sobą fałszywe punkty dostępowe. Możliwe jest bowiem utworzenie fałszywego punktu dostępowego przez osobę, która chce podsłuchiwać transmisję. Każdy klient, który podłączy się do takiego punktu będzie przesyłał przez niego wszystkie swoje dane, w rezultacie czego staną się one dostępne dla atakującego.

Mobilne punkty dostępowe ze względu na swój charakter są szczególnie narażone na różnego typu ataki. Ponadto ich skuteczne zabezpieczenie jest szczególnie trudne. Jednak jest to konieczne ze względu na wymagania użytkowników oraz ryzyko utraty wizerunku w przypadku wystąpienia poważnego incydentu naruszenia bezpieczeństwa.

W artykule przedstawiony zostanie problem zabezpieczania sieci bezprzewodowych i zaproponowany zostanie dobór właściwych zabezpieczeń i rozwiązań pozwalających na zachowanie wysokiego poziomu bezpieczeństwa mobilnych punktów dostępowych.

1. Standardy sieci bezprzewodowych

Budowa sieci bezprzewodowych i ich działanie zostało ustandaryzowane w celu zapewnienia kompatybilności urządzeń. Standardy sieci bezprzewodowych zostały zawarte w grupie 802.11. Obejmuje ona szereg standardów spośród których najważniejszymi są: 802.11a, 802.11b, 802.11g oraz 802.11n określające sposób kodowania, oraz 802.11i istotny z punktu widzenia bezpieczeństwa i uwierzytelniania w sieciach bezprzewodowych [13].

1.1. Standardy 802.11 a-n

Standard 802.11a został wprowadzony jako pierwszy, w 1990 roku. Przeznaczony jest dla sieci pracujących na częstotliwości 5GHz oraz na kanale o szerokości 20 MHz. Maksymalną możliwą do osiągnięcia prędkością transmisji jest 54 Mb/s. Wprowadzenie standardu napotkało liczne problemy takie jak: wysoki koszt produkcji oraz budową podzespołów. Dlatego też został upowszechniony standard 802.11b, który został wprowadzony w roku 1990. Jednakże jako pierwszy miał zastosowanie w domach i małych firmach ze względu ma dużo tańszy koszt od poprzednika. Pracuje na częstotliwości 2,4 GHz i kanale o szerokości 20 MHz. Maksymalna prędkość transmisji wynosi 11 Mb/s, natomiast realna przepustowość 6 Mb/s [1,5].

Ze względu na duże zapotrzebowanie na większą przepustowość wprowadzono standard 802.11g. Pracuje on na częstotliwości 2,4GHz oraz szerokości kanału 20 MHz. Maksymalna przepustowość wynosi 54 Mb/s, natomiast realna prędkość transmisji nie przekracza 25 Mb/s [1, 5].

Najnowszym standardem wprowadzonym w 2009 roku jest 802.11n. Oparty jest na technologii łączącej częstotliwości 2,4GHz oraz 5GHz i szerokości kanału 20MHz oraz 40 MHz. Została w nim użyta technika MIMO (multiple-input multiple-output) oraz agregacja ramek. Ma to na celu zwiększenie maksymalnej prędkości transmisji do 600 Mb/s. Realna przepustowość wynosi 100 Mb/s [1,5].

1.2. Standard 802.11i

Jest standardem sieci bezprzewodowych, który zapewnia szyfrowanie danych w sieciach wykorzystujących popularne standardy 802.11a, 802.11b, 802.11g oraz 802.11n. Standard 802.11i wykorzystuje protokoły szyfrujące, takie jak TKIP oraz AES. W roku 2004 został oficjalnie zatwierdzony przez IEEE jako część rodziny 802.11. Zapewnia wysoki poziom bezpieczeństwa. W jego skład wchodzą takie standardy jak WPA i WPA2 [10, 12].

2. Metody zabezpieczeń

Istnieją różne metody zabezpieczeń sieci bezprzewodowych. Podstawowymi zabezpieczeniami są [2, 4, 6, 8]:

- Wyłączenie rozgłaszania identyfikatora sieci – komputery znajdujące się w zasięgu sieci nie otrzymują informacji o jej nazwie. Jednak przełączenie karty sieciowej w tryb monitora (nasłuchu wszystkich pakietów) pozwala na podsłuchanie trwającej transmisji i przechwycenie identyfikatora sieci.
- Filtrowanie adresów sprzętowych (MAC) – jest to rozwiązanie pozwalające kontrolować adresy MAC urządzeń, które próbują nawiązać połączenie z punktem dostępowym (ang. access point – AP). AP zezwala na nawiązanie połączenia jedynie urządzeniom posiadającym adresy MAC z puli zdefiniowanej w jego konfiguracji. Jednakże ze względu na możliwość podsłuchania adresów MAC urządzeń autoryzowanych w sieci oraz łatwej zmiany adresu sprzętowego komputera zabezpieczenie to nie jest skuteczne.
- Szyfrowanie – jest to rozwiązanie które szyfruje całą transmisję pomiędzy urządzeniem klienckim a punktem

dostępowym oraz zezwala na nawiązanie połączenia jedynie urządzeniom posiadającym klucz kryptograficzny. Podstawowymi zabezpieczeniami są:

- WEP,
- WPA,
- WPA2,
- WPA/WPA2 Enterprise.

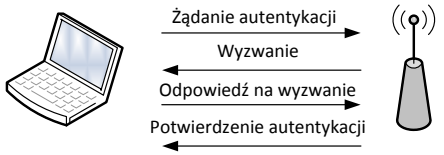
2.1. WEP

WEP (Standard Wired Equivalent Privacy) opracowany został w 1999 roku. Celem protokołu miało być zapewnienie poufności i bezpieczeństwa danych na poziomie zbliżonym do sieci kablowych [9]. Protokół do zapewnienia poufności używa szyfru strumieniowego RC, natomiast do zapewnienia integralności używana jest suma kontrolna CRC-32.

Już w 2000 roku odkryte zostały luki w zabezpieczeniach protokołu WEP, jednak do dziś ten standard jest stosowanych w celu zabezpieczenia sieci. Punkty dostępowe nadal mają wbudowany mechanizm szyfrowania protokołem WEP [9].

Niestety protokół WEP jest bardzo podatny na ataki kryptograficzne. Słabością tego protokołu jest to, że podstawowym algorytmem szyfrowania jest RC4. Ponadto protokół ten obsługuje zbyt mały rozmiar wektora inicjalizującego (IV), który jest powtarzany jest co 224 pakiety. Dzięki temu istnieje 50% szansa na to, że w zbiorze 5000 pakietów zostanie powtórzony klucz szyfrowania co najmniej 4 razy.

Dodatkową podatnością WEP jest brak autentykacji urządzenia klienckiego w trakcie transmisji. Autentykacja następuje podczas nawiązywania połączenia z punktem dostępowym poprzez wymianę informacji uwierzytelniających (ang. 4-way handshake), tak jak to zaprezentowano na rysunku 1.



Rys. 1. Proces autentykacji urządzenia w sieci bezprzewodowej (4-way handshake)

Proces uwierzytelnienia składa się z czterech kroków i opiera się o współdzielony klucz kryptograficzny. Inicjowany jest przez urządzenie klienta, które przesyła do punktu dostępowego żądanie uwierzytelnienia w sieci. Punkt dostępowy w odpowiedzi na żądanie przesyła do urządzenia klienta 128 bitową liczbę losową. Klient szyfruje tę liczbę współdzielonym kluczem kryptograficznym po czym przesyła ją w postaci zaszyfrowanej do punktu dostępowego, gdzie zostaje ona odszyfrowana. Jeśli urządzenie punktu dostępowego stwierdzi, że odszyfrowana liczba jest taka sama jak wysłana wcześniej do klienta to autoryzuje urządzenie klienckie i wysyła mu potwierdzenie autentykacji. W ten sposób urządzenie klienckie potwierdza znajomość klucza szyfrującego pozwalającego na dostęp do sieci. Niestety proces ten nie pozwala na stwierdzenie czy punkt dostępowy zna hasło, czyli nie zabezpiecza przed fałszywymi punktami dostępowymi. Dodatkowym poważnym problemem jest możliwość podszycia się innego urządzenia pod autoryzowane w sieci urządzenie klienckie gdyż autentykacja nie jest kontrolowana w trakcie dalszej wymiany danych. Ponadto hasło dostępowe do sieci używane jest jako klucz szyfrujący wspólny dal wszystkich klientów sieci, co stwarza możliwość podsłuchiwania transmisji przez innych użytkowników sieci[9].

2.2. WPA

Ze względu na zbyt niski poziom bezpieczeństwa WEP i jego podatność na ataki rozpoczęto prace nad nowym standardem 802.11i. Jednak brak możliwości szybkiego wdrożenia pełnego standardu (głównie ze względu na ograniczenia sprzętowe istniejących urządzeń) spowodował wprowadzenie standardu WPA jako tymczasowego rozwiązania [10].

Metoda szyfrowania WPA wykorzystuje algorytm szyfrowania TKIP, który usuwa słabości WEP. WPA wprowadziło kontrolę integralności informacji, rozszerzyło wektor inicjujący oraz mechanizm wprowadzania ponownie klucza WPA. Miało to na celu zapewnienie wyższego poziomu zabezpieczenia i uwierzytelnienie użytkownika w oparciu o 802.11 oraz Extensible Authentication Protocol (EAP). Wi-Fi Protected Access (WPA) jest kompatybilny z IEEE 802.11i [7, 10].

Aby zapewnić większe bezpieczeństwo sieci Wi-Fi w porównaniu do WEP, Standard 802.11i wprowadził RSN (Robust Security Network). Wprowadzenie RSN ma na celu rozwiązanie problemów bezpieczeństwa, które występowały w WEP. Podstawowymi problemami, które postanowiono rozwiązać to: ochrona współdzielonego klucza, bezpieczeństwo szyfrowania, uwierzytelnianie, zmienność klucza oraz integralność [1, 10].

RSN obejmuje następujące elementy bezpieczeństwa architektury sieci [1, 10]:

- klucz szyfrujący nie jest bezpośrednio używany do szyfrowania tylko wykorzystywany jest do generowania tymczasowego klucza szyfrującego,
- wykorzystanie protokołu 802.11X do uwierzytelniania podłączonego urządzenia,
- określenie metod szyfrowania oraz 4-way handshake,
- zagwarantowanie poufności i integralności poprzez użycie TKIP i CCMP,
- ustalenie polityki bezpieczeństwa.

Uwierzytelnienie przy pomocy współdzielonego klucza działa analogicznie jak w przypadku sieci WEP. Polega to na wprowadzeniu przez użytkownika klucza. Ten rodzaj szyfrowania stosowany jest głównie w domach i małych firmach, ze względu na swą prostotę. Rozwiązanie to nazywane jest WPA-Personal lub WPA-PSK [10].

2.3. WPA2

W 2004 WPA2 zostało określone jako pełna implementacja standardu 802.11i. Podstawową zmianą jaka została wprowadzona przez standard IEEE 802.11i było oddzielenie uwierzytelnienia użytkowników od zapewnienia poufności oraz integralności danych. Dzięki temu utworzona została skalowalna oraz niezawodna architektura bezpieczeństwa (RSN) mająca zastosowanie w dużych sieciach korporacyjnych jak i w sieciach domowych. RSN wykorzystuje nowe mechanizmy poufności oraz integralności. Kolejną wprowadzoną zmianą jest wykorzystanie protokołu 802.1x do uwierzytelniania. Bezpieczna komunikacja składa się z czterech faz [1, 10]:

- uzgodnienia polityki bezpieczeństwa,
- uwierzytelnienia 802.1x,
- generowania i dystrybucji klucza,
- w ramach architektury RSN – zapewnienia integralności i poufności danych.

Protokół wykorzystuje do autentykacji tzw. 4-way handshake.

Podczas czteroetapowej negocjacji (4-way handshake) klucz PTK wyliczany jest na podstawie kliku różnych parametrów, takich jak: klucz PMK, wartość losowa generowana przez klienta-suplikanta (SNonce), wartość losowa generowana przez podmiot uwierzytelniający (ANonce), stały ciąg znaków, adresu MAC punktu dostępowego i suplikanta [1,10].

WPA2 wymaga wsparcia CCMP – trybu pracy algorytmu szyfrującego opartego na algorytmie AES. Używa 128 bitowego klucza oraz bloku o tym samym rozmiarze.

2.4. WPA/WPA2 Enterprise

W przypadku WPA/WPA2 Enterprise wymagany jest serwer Radius. W tym przypadku serwer wykonuje operacje autoryzacji, księgowania oraz uwierzytelniania. Rozwiązanie to wzbogaca funkcjonalność WPA2. Głównymi zaletami stosowania WPA/WPA2 Enterprise są [11]:

- zastosowanie indywidualnych danych dostępu do sieci dla każdego użytkownika jak i urządzenia,
- podłączenie użytkownika do sieci poprzedzone jest uwierzytelnieniem,
- zarządzanie użytkownikami,
- opcja uwierzytelnienia infrastruktury, do której użytkownik się podłącza, w celu uzyskania odporności na atak na AP,
- w przypadku zastosowania limitów np. czasu połączenia, przesyłu danych możliwe jest zliczanie wartości tych parametrów (realizacja księgowania),
- odłączenie pojedynczego użytkownika nie wymaga zmiany hasła dla wszystkich użytkowników sieci.

Dużym minusem oraz problemem jest zbudowanie infrastruktury opartej na tym standardzie. Zbudowanie sieci opartej na 802.1X i serwerze Radius wymaga specjalistycznej wiedzy oraz sprzętu obsługującego wybraną metodę EAP.

W 2004 roku, gdy został wydany standard 802.11i pro-gram certyfikacji urządzeń zawierał tylko jedną metodę uwierzytelnienia tzw. EAP-TLS. Była ona stosunkowo trudna w implementacji. Wraz z rozwojem zostały opracowane nowe metody ułatwiające wdrażanie WPA-Enterprise[1,11].

3. Zagrożenia sieci bezprzewodowych

W sieciach bezprzewodowych brak okablowania, łatwość dostępu oraz mobilność jest ich największą zaletą. Jednak stanowi to również ich największą wadę, ponieważ brak jest fizycznego ograniczenia dostępu do sieci [3, 4, 6].

Podstawowymi zagrożeniami sieci bezprzewodowych są:

- nasłuchiwanie i podsłuchiwane,
- wstrzykiwanie pakietów,
- łamanie haseł,
- podszywanie się.

Ze względu na fakt, iż sieć jest dostępna dla każdego kto znajduje się w jej zasięgu, możliwe jest podsłuchiwane ruchu sieciowego. Polega ono na analizowaniu ruchu sieciowego poprzez odbieranie pakietów, które są adresowane do innych użytkowników. Przykładowym programem do analizowania ruchu w sieci jest Wireshark [4].

Kolejnym zagrożeniem występującym w sieciach bezprzewodowych jest wstrzykiwanie pakietów. Polega ono na tym, iż nieproszony użytkownik sieci jest w stanie np. anulować uwierzytelnienie poprzez wstrzykniecie do sieci ramki zarządzającej De-authentication, powodującej rozłączenie użytkowników sieci [8].

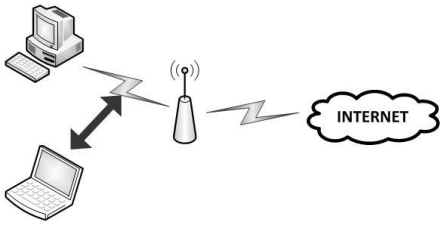
Następnym niebezpieczeństwem, które dotyczy sieci bezprzewodowych jest łamanie haseł. Nie mniej istotnym zagrożeniem jest podszywanie się. Jest to atak typu „Man In the Middle". Atakujący podszywa się pod punkt dostępowy w celu zmylenia użytkowników sieci aby połączyli się z tym spreparowanym punktem dostępowym, który daje atakującemu możliwość podsłuchiwania ruchu sieciowego [8].

4. Stanowisko badawcze

W celu weryfikacji kluczowych podatności sieci bezprzewodowych zbudowane zostało stanowisko badawcze pozwalające na badanie rzeczywistego działania małej sieci bezprzewodowej. W skład stanowiska wchodził punkt dostępowy (AP) podłączony do Internetu oraz dwa komputery – jeden w roli klienta sieci, drugi jako maszyna do przeprowadzenia ataków. Schemat stanowiska badawczego przedstawiono na rysunku 2. W badaniach pominięto kwestię podłączenia do Internetu, gdyż kwestię tą reguluje dostawca łącza internetowego i nie mamy wpływu na oferowane zabezpieczenia.

W zbudowanym laboratorium wykorzystano następujące urządzenia:

- laptop skonfigurowany do pracy w sieci bezprzewodowej i łączący się z Internetem. Będzie on pełnił rolę „ofiary". Urządzenie to wyposażono w system operacyjny Windows 7.
- komputer stacjonarny przeznaczony do przeprowadzania testów penetracyjnych. Zalecane jest aby posiadał minimum 3GB pamięci RAM, gdyż w doświadczeniach zostaną wykorzystane narzędzia i oprogramowanie które, aby spełniało prawidłowo swoje zadanie, potrzebuje odpowiednio dużej pojemności pamięci operacyjnej. Komputer musi być wyposażony w bezprzewodową kartę sieciową obsługującą mechanizm wstrzykiwania, przechwytywania oraz nasłuchiwania pakietów. W badaniach została użyta bezprzewodowa karta sieciowa Edimax – 7711USn. Komputer ten został dodatkowo wyposażony w system operacyjny Kali Linux. System ten został wybrany ze względu na to, że posiada wbudowaną obsługę użytej karty Edimax wraz ze wszystkimi sterownikami potrzebnymi do wstrzykiwania i nasłuchiwania pakietów.
- punkt dostępowy TP-Link 841N. Istnieje jednak możliwość wykorzystania dowolnego punktu dostępowego obsługującego szyfrowanie WEP/WPA/WPA2.
- łącze internetowe.



Rys. 2. Schemat stanowiska badawczego

Przygotowany sprzęt został wstępnie skonfigurowany i przygotowany do przeprowadzenia badań. Konfiguracja punktu dostępowego została przywrócona do ustawień fabrycznych a następnie skonfigurowano go jako ruter pełniący funkcję punktu dostępowego sieci bezprzewodowej o identyfikatorze (SSID) „t1". W kolejnym kroku skonfigurowano połączenie z Internetem, korzystając z połączenia kablowego. Na tym etapie nie konfigurowano żadnych zabezpieczeń. Całość sieci badawczej podłączona była z Internetem za pośrednictwem zapory sieciowej.

Do wstępnie skonfigurowanej sieci podłączony został laptop, po czym nawiązano na nim połączenie z Internetem. W ten sposób sprawdzono poprawność działania zestawionych połączeń i wykonanej konfiguracji.

5. Ocena skuteczności metod zabezpieczeń

W celu praktycznej weryfikacji poziomu bezpieczeństwa sieci bezprzewodowej przeprowadzono badania ich odporności pod kątem odporności na złamanie hasła. Łamanie hasła jest jednym z najczęstszych sposobów naruszenia bezpieczeństwa sieci.

Przedstawiona zostanie analiza bezpieczeństwa sieci bezprzewodowych poprzez określenie wpływu wybranych parametrów na czas łamania hasła. Badane będą: siła sygnału oraz siła użytego hasła.

5.1. Siła sygnału

W niniejszym rozdziale przedstawiono wyniki eksperymentu mającego zweryfikować czy siła sygnału sieci bezprzewodowej wpływa na czas łamania hasła. Przy pomocy programu Wi-Fi Analytics Tool została przeprowadzona analiza sygnału punktu dostępowego.

Wi-Fi Analytics Tool jest narzędziem analizującym sieci bezprzewodowe. Na podstawie wykresów przedstawia siłę sygnału, kanał oraz zakłócenia na wybranych kanałach. Analiza wypływu siły sygnału na czas łamania zabezpieczenia WEP została opracowana na podstawie czterech statusów pomiaru siły sygnału:

- bardzo dobra,
- dobra,
- dopuszczalna,
- bardzo słaba.

Przeprowadzono badanie mające na calu sprawdzenie czy siła sygnału ma znaczenie na czas łamania podczas szyfrowania WEP. Aby zróżnicować siłę sygnału punkt dostępowy był ustawiany w różnych lokalizacjach.

Każdy pomiar został powtórzony 5 razy. Na podstawie przeprowadzonych pomiarów został wyliczony średni czas łamania zabezpieczenia przy danej sile sygnału. Wyniki przeprowadzonego badania przedstawia tabela 1.

Tabela 1. Wpływ siły sygnału na czas ataku na sieć używającą szyfrowania WEP

Rodzaj szyfrowania	Siła sygnału (dBm)	Średn Czas (hh:mm:ss)	Powodzenie ataku
WEP	-44 dBm	00:00:35	TAK
WEP	-74 dBm	00:00:36	TAK
WEP	-88 dBm	00:00:34	TAK
WEP	-95 dBm	00:00:35	TAK

Wszystkie próby złamania hasła szyfrowania WEP zakończyły się powodzeniem. Za pomocą polecenia `aircrack -ng` możliwe jest przeprowadzenie ataku na sieć zabezpieczoną protokołem WEP.

Biorąc pod uwagę wykonane badanie warto zauważyć, iż czas łamania zabezpieczenia oscyluje w okolicach 35 sekund. Uzyskanie tak krótkiego czasu jest możliwe dzięki wykorzystaniu polecenia `aircrack` do wstrzyknięcia pakietów, ponieważ podstawowym elementem niezbędnym do złamania zabezpieczenia WEP są przechwycone pakiety. Ze względu na to iż, wektor inicjalizujący powtarzany jest co 224 pakiety. Istnieje 50% szansa na to, że w zbiorze 5000 pakietów zostanie powtórzony klucz szyfrowania co najmniej 4 razy. Im program mniej przechwyci pakietów, tym czas łamania zabezpieczenia zostanie wydłużony.

Na podstawie uzyskanych wyników możliwe jest stwierdzenie, że czas łamania nie jest zależny od siły sygnału. W każdym z badanych przypadków średnie czasy łamania były zbliżone.

Analogiczne badanie zostało przeprowadzone w sieci wykorzystującej szyfrowanie WPA/WPA2 PSK. Nadmienić należy, że w tym przypadku `aircrack` korzystał ze słownika haseł. Aby zbadać wpływ siły sygnału na czas łamania wprowadzono do słownika hasło użyte do zabezpieczenia analizowanej sieci. Jako że komputer kliencki wyposażony był w system obsługujący szyfrowanie WPA2, taki właśnie algorytm szyfrujący używany był do zabezpieczenia badanej sieci bezprzewodowej.

Każde doświadczenie zostało wykonane w przygotowanym laboratorium oraz powtórzone 5 razy. Na podstawie pomiarów została wyliczona średnia czasów łamania zabezpieczenia. Tabela 2 przedstawia wynik przeprowadzonego badania.

Tabela 2. Wpływ siły sygnału na czas ataku na sieć używającą szyfrowania WPA/WPA2 PSK

Rodzaj szyfrowania	Siła sygnału (dBm)	Średni Czas (hh:mm:ss)	Powodzenie ataku
WPA/WPA2	-40 dBm	00:00:25	TAK
WPA/WPA2	-70 dBm	00:00:24	TAK
WPA/WPA2	-80 dBm	00:00:25	TAK
WPA/WPA2	-95 dBm	00:00:23	TAK

Na podstawie danych z tabeli 2, można zauważyć, że czasy łamania zabezpieczenia WPA/WPA2 PSK, są bardzo do siebie zbliżone. Efekt doświadczenia udowadnia, że siła sygnału nie ma żadnego znaczenia na czas łamana zabezpieczenia. Zbliżone czasy łamania klucza związane są z tym, że do każdego przeprowadzonego ataku zostało użyte to samo hasło.

5.2. Siła hasła

Każda sieć wykorzystująca szyfrowanie posiada hasło stanowiące klucz dostępu do sieci. Na podstawie tego hasła generowany jest również klucz szyfrujący. Odgadnięcie (złamanie) hasła pozwala więc atakującemu na swobodny dostęp do sieci. Dlatego też istotne jest stosowanie silnych haseł, czyli takich, które będą trudne do odgadnięcia. Siła hasła zależy od liczby znaków oraz kombinacji elementów z poniższych grup:

- cyfry,
- małe litery,
- wielkie litery,
- znaki specjalne.

Silne hasło powinno zawierać co najmniej 8 znaków, przy czym powinno zawierać znaki z każdej z wyszczególnionych powyżej grup. Ponadto hasło nie może być oparte na słowie pochodzącym ze słownika oraz nie może w żaden sposób kojarzyć się z użytkownikiem. Popełnienie błędu przy konstruowaniu hasła skutkuje obniżeniem jego entropii i ułatwia złamanie. Standardem podczas tworzenia zabezpieczeniem jest połączenie cyfr, małych wielkich liter oraz znaków specjalnych.

Pierwszy etap badań dotyczył wpływu siły hasła na czas łamania zabezpieczeń w szyfrowaniu WEP. Do celów eksperymentu zabezpieczano sieć używając czterech haseł o różnej sile. Dla każdego hasła badanie zostało powtórzone 5 razy oraz została wyliczona średnia czasów łamania zabezpieczania. Wynik przeprowadzonego badania przedstawia tabela 3.

Tabela 3. Wpływ siły hasła na czas łamania zabezpieczeń w sieci używającej szyfrowania WEP

Rodzaj szyfrowania	Hasło	Średni Czas (hh:mm:ss)	Powodzenie ataku
WEP	1234567890	00:00:31	TAK
WEP	klucz123	00:00:33	TAK
WEP	Zn4k$pecj@lny	00:00:32	TAK
WEP	@#$%^&**^%$#	00:00:32	TAK

W przypadku szyfrowania WEP, każde wykonanie próby złamania klucza zakończyło się powodzeniem. Protokół WEP jest kryptologicznie podatny na ataki. Na podstawie uzyskanych danych, można stwierdzić, że niezależnie od tego jak bardzo złożone jest hasło to narzędzie aircrack –ng jest w stanie złamać szyfrowanie. Również zmiana siły hasła nie ma wpływu na czas łamania zabezpieczeń.

Analogiczne badanie przeprowadzono w sieci zabezpieczonej zgodnie ze standardem 802.11i czyli używającej szyfrowania WPA/WPA2 PSK. Na podstawie podstawowych zasad tworzenia kluczy w zależności od siły hasła zostały utworzone cztery ciągi znaków. Każdy kolejny ciąg znaków stanowi hasło o większej sile. Każdy z nich został użyty do zabezpieczenia sieci. Doświadczenie zostało powtórzone pięciokrotnie dla pierwszych trzech haseł oraz wyliczona została średnia czasów złamania zabezpieczenia. Natomiast w przypadku najsilniejszego hasła pomiar był wykonany tylko raz, ponieważ nie udało się złamać zabezpieczenia. Powodem tego był fakt, że słownik nie zawierał używanego w sieci klucza. Tabela 4 przedstawia wyniki przeprowadzonego badania.

Tabela 4. Wpływ siły hasła na czas łamania zabezpieczeń sieci zabezpieczonej zgodnie ze standardem 802.11i

Rodzaj szyfrowania	Hasło	Średni czas (hh:mm:ss)	Liczba kluczy	Powodzenie ataku
WPA/WPA2	1011990	00:00:00	12	TAK
WPA/WPA2	ASIANNA008	00:14:29	1457328	TAK
WPA/WPA2	Dodge9404.0	00:40:20	4057896	TAK
WPA/WPA2	@%##*Fj^!	20:46:09	468202214	NIE

Pole „liczba kluczy” w tabeli 4 określa liczbę sprawdzonych pozycji w słowniku haseł. Na podstawie danych z tabeli 4 można zauważyć, iż słownik zawierał 468202214 kluczy - ponieważ dla ostatniego hasła program sprawdził wszystkie znajdujące się w słowniku pozycje i zakończył działanie. Złamanie hasła o największej sile zakończyło się niepowodzeniem, mimo dużej liczby kluczy w słowniku.

Jako, że łamanie zabezpieczenia sprowadza się do dopasowywania kolejnych haseł pobieranych ze słownika, czas łamania jest proporcjonalny do liczby sprawdzonych pozycji. Jeśli hasło nie figuruje w słowniku to próba łamania zakończy się niepowodzeniem. Dobry słownik powinien zawierać najczęściej stosowane przez użytkowników hasła. Jeśli mimo braku powodzenia chcemy kontynuować atak możemy tego dokonać metodą siłową (ang. brute force). Polegało to będzie na generowaniu wszystkich możliwych kombinacji znaków i próby użycia ich jako hasła. Takie postępowanie jest jednak czasochłonne. Bazując na uzyskanych w trakcie badań czasach, zakładamy, że możliwe jest sprawdzenie średnio 100 000 haseł w ciągu minuty. Tak więc czasy sprawdzenia wszystkich możliwych kombinacji haseł o określonej długości będą się przedstawiały tak jak zaprezentowano w tabeli 5.

Jak pokazują przedstawione w tabeli 5 dane hasła o długości mniejszej niż 7 znaków mogą zostać złamane w rozsądnym czasie. Aby zapewnić bezpieczeństwo sieci należy stosować hasła o długości nie mniejszej niż 8 znaków. Wówczas nie tylko maksymalny czas sprawdzenia wszystkich kombinacji będzie długi ale również prawdopodobieństwo, że użyte hasło wystąpi na początku słownika będzie niewielkie. Poza tym algorytmy siłowe najczęściej sprawdzają wszystkie hasła kolejno poczynając od najkrótszych. Tak więc zanim algorytm przystąpi do sprawdzania haseł ośmioznakowych sprawdzi hasła krótsze, co dodatkowo wydłuży czas łamania.

Tabela 5. Czas sprawdzenia wszystkich kombinacji hasła o określonych długościach w sieci zabezpieczonej w standardzie 802.11i

Liczba znaków hasła	Liczba możliwych kombinacji hasła	Czas sprawdzenia wszystkich kombinacji
1	95	0,001 s
2	9025	0,09 s
3	857375	8,5 s
4	81450625	13,5 min
5	7,74E9	21,54 h
6	7,35E11	85 dni
7	6,98E13	22 lata
8	6,63E15	2103 lata
9	6,3E17	200 tys. lat

6. Wnioski

Szyfrowanie WEP okazało się całkowicie podatne na ataki i nie stanowi zabezpieczenia nawet w sytuacji, gdy hasło jest bardzo silne. Ponadto stosuje jeden wspólny klucz szyfrujący dla wszystkich klientów, przez co mogą oni podsłuchiwać ruch sieciowy innych użytkowników sieci. Jak wykazały badania jedyną skuteczną metodą zabezpieczenia małej sieci bezprzewodowej jest stosowanie standardu 802.11i, niezależnie od standardu transmisji danych. Podczas szyfrowania WPA/WPA2 jedyną metodą złamania zabezpieczenia jest metoda słownikowa lub siłowa wymagająca długiego czasu analizy w przypadku zastosowania długich i złożonych haseł.

Większą skuteczność i dodatkowe możliwości w dziedzinie zabezpieczenia sieci oferuje jedynie standard enterprise oparty o serwer radius. Jednak ten rodzaj zabezpieczeń nie był zanalizowany ze względu na trudność zrealizowania tak złożonej struktury jako mobilnego hotspota oraz wysoki koszt implementacji tegoż zabezpieczenia. Dlatego też w celu uzyskania wysokiego poziomu bezpieczeństwa i dostępności łącza internetowego udostępnianego przez mobilne punkty dostępowe należy zabezpieczać transmisję w standardzie 802.11i, udostępniając hasło dostępowe klientom. Należy jednak zadbać o systematyczną zmianę tychże haseł.

Literatura

[1] Gast M. S.: 802.11. Sieci bezprzewodowe. Przewodnik encyklopedyczny, Helion 2003.
[2] Gliwiński M., Dylewski R.: Raport specjalny szkoły hakerów część 1. Ataki na sieci bezprzewodowe. Teoria i praktyk, Kwidzyń 2010.
[3] Hutchens J.: Skanowanie sieci z Kali Linux. Receptury, Gliwice 2015.
[4] Kowalczyk G.: Kali Linux Audyt bezpieczeństwa sieci Wi-Fi dla każdego Wydanie II, Gliwice 2016.
[5] Leary J., Pejman R.: Bezprzewodowe sieci LAN 802.11 podstawy, PWN 2006 Potter B., Fleck B.: 802.11. Bezpieczeństwo, Helion 2004.
[6] Weidman G.: Bezpieczny system w praktyce. Wyższa szkoła Hawkingu i testy penetracyjne, Gliwice 2015.
[7] http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+7.+WPA+RSN+and+IEEE+802.11i/Security+Layers/, [11.06.2016].
[8] http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_PL.pdf, [11.06.2016].
[9] Smutnicki A.: Bezpieczeństwo sieci Wi-Fi – część 3. (WEP), http://sekurak.pl/bezpieczenstwo-sieci-wi-fi-czesc-3-wep/, [11.06.2016].
[10] Smutnicki A.: Bezpieczeństwo sieci Wi-Fi – część 4. (Standard 802.11i czyli WPA i WPA2), http://sekurak.pl/bezpieczenstwo-sieci-wi-fi-czesc-4-standard-802-11i-czyli-wpa-i-wpa2/, [11.06.2016].
[11] Smutnicki A.: Bezpieczeństwo sieci Wi-Fi – część 7. (WPA/WPA2-Enterprise: 802.1X i EAP), http://sekurak.pl/bezpieczenstwo-sieci-wi-fi-czesc-7-wpawpa2-enterprise-802-1x-i-eap/, [11.06.2016].
[12] 802.1X-2004 - Port Based Network Access Control, http://www.ieee802.org/1/pages/802.1x-2004.html, [19.06.2016].

Dr inż. Grzegorz Kozieł
e-mail: g.koziel@pollub.pl

Absolwent Wydziału Elektrycznego Politechniki Lubelskiej, gdzie również uzyskał tytuł doktora w 2011 roku, broniąc pracę „Zmodyfikowane metody cyfrowego przetwarzania sygnałów dźwiękowych w steganografii komputerowej”. Pracownik Instytutu Informatyki na Wydziale Elektrotechniki i Informatyki Politechniki Lubelskiej, początkowo, jako asystent, później, jako adiunkt a obecnie zastępca dyrektora Instytutu ds. ogólnych.
Działalność naukowa obejmuje steganografię oraz analizę danych ruchu.

Inż. Jakub Maluga
e-mail:jakubmaluga@gmail.com

Absolwent Państwowej Szkoły Wyższej im. Jana Pawła II w Białej Podlaskiej, gdzie uzyskał tytuł inżyniera. Obecnie dyplomant Instytutu Informatyki na Wydziale Elektrotechniki i Informatyki Politechniki Lubelskiej oraz pracownik firmy TAU INTERNET na stanowisku: monter sieci i urządzeń telekomunikacyjnych.

otrzymano/received: 20.06.2016 *przyjęto do druku/accepted: 30.10.2016*