Studia i Materiały Informatyki Stosowanej, Tom 7, Nr 18, 2015
str. 15-19

SIECI WI-FI – ZABEZPIECZENIA I METODY ATAKÓW

Ewelina Nitka, Klaudia Kawalec, Andrzej Karpowicz

Ewelina Nitka
Studentki III roku IB
Instytut Techniki
ul.Chodkiewicza 30,
85-064 Bydgoszcz
e-mail: ewelina.nitka@wp.pl
e-mail: kawalec.klaudia@wp.pl
e-mail: andrzejkarpowicz94@gmail.com

Streszczenie: *Sieci Wi-Fi są systemem komunikacji zaprojektowanym jako alternatywa lub uzupełnienie sieci tradycyjnej kablowej. Sieci bezprzewodowe mają bardzo szerokie zastosowanie. Wykorzystuje się je m.in. do projektowania sieci domowych oraz firmowych. Najprostszą i najczęściej stosowaną metodą zabezpieczenia sieci jest protokół WPA 2 Personal. Od początku istnienia sieci bezprzewodowych trwa prawdziwy wyścig zbrojeń. Nowe opracowania protokołów szybko stają się nieaktualne. Hakerzy odkrywają kolejne metody ataków i wskazują wady istniejących rozwiązań. Przeprowadzenie ataku na sieć na ogół poprzedzone jest zbadaniem środowiska obranego celu. Nie wszystkie ataki jednak związane są z wykorzystaniem sprzętu komputerowego, w niektórych przypadkach łatwiejszym celem są użytkownicy sieci.*
Keywords: *Wi-Fi, WEP, WPA/WPA 2, SSID, metody ataku, ataki pasywne, ataki aktywne*

WI-FI NETWORK - SECURITY AND METHODS OF ATTACKS

Abstarct: *Wi-Fi is a system of communication designed with an alternative or a complement for traditional cable network. Wireless networks are very common in use. They are used for example to project a home network or a business network. The easiest and the most popular method of network security is a WPA 2 Personal protocol. From the very beginning, there have been a real arms race. New coverages of the protocols are getting very quickly not actual. Hackers discover new methods of an attack and they show disadvantages of existing solutions. Performing an attack against some network is in general preceded by studying an environment of the aim. Not all attacks are connected with using a hardware. In some cases, users of a network are the easier aim.*

Literatura *Wi-Fi, WEP, WPA/WPA 2, SSID, methods of attack, passive attacks, active attacks*

1. WSTĘP

Wi-Fi jest określane jako zestaw standardów stworzonych do budowy bezprzewodowych sieci komputerowych. Szczególnym zastosowaniem Wi-Fi jest budowanie sieci lokalnych (LAN) opartych na komunikacji radiowej, czyli WLAN. Zasięg od kilku metrów do kilku kilometrów i przepustowości sięgającej 300 Mb/s, transmisja na dwóch kanałach jednocześnie. Wi-Fi bazuje na takich protokołach warstwy fizycznej, jak: DSSS, FHSS i OFDM. Sieć Wi-Fi działa w paśmie częstotliwości od 2400 do 2485 MHz (2,4 GHz) lub 4915 do 5825 MHz (5 GHz).

2. ZABEZPIECZENIA SIECI WI-FI

Stosowane metody zabezpieczeń zgodne ze standardem 802.11[1, 4, 5]:

A. **Uwierzytelniania** – identyfikacja i weryfikacja autentyczności informacji przesyłanych przez użytkownika, który łączy się z siecią (IEEE 802.1X).

B. **Protokół WEP** (ang. Wired Equivalent Privacy) – działa na zasadzie współdzielonego klucza szyfrującego o długości 40 do 104 bitów i 24-bitowym wektorze inicjującym. WEP jest aktualnie bardzo złym zabezpieczeniem, które nie chroni nas przed włamaniami z zewnątrz. W średnio obciążonej sieci klucze WEP można złamać w 90% przypadków, poniżej 1h pasywnego nasłuchiwania pakietów.

C. **Protokoły WPA/WPA2** – nowe, dużo bardziej bezpieczne mechanizmy szyfrowania przesyłanych danych [7]:

- **Wi-Fi Protected Access (WPA)** – Najpopularniejszą konfiguracją WPA jest WPA-PSK (Pre-Shared Key). Klucze używane przez WPA są 256-bitowe, co jest dużą różnicą w porównaniu do tych WEP-owskich. Kilka znaczących zmian, które zostały wprowadzone wraz z WPA to m.in. sprawdzenie wiadomości uwierzytelniającej (aby ustalić, czy atakujący zdobył lub zmieniał pakiety przechodzące pomiędzy routerem/access pointem a klientem) czy też TKIP (Temporal Key Integrity Protocol). TKIP wykorzystuje klucze związane z pakietami, a nie już ustalony wcześniej klucz do całości, jak to było w WEP. TKIP zostało później wyparte przez AES (Advanced Encryption Standard).
- **Wi-Fi Protected Access II (WPA2**) – Jedną ze znaczących zmian w WPA2 było obowiązkowe użycie AES i CCMP jako zamiennika dla TKIP (nadal zachowany w WPA2 jako rezerwowy system dla kompatybilności z WPA).

Można wyróżnić dwa rodzaje kodowań WPA/WPA2 – Personal i WPA/WPA2-Enterprise. Jest to forma zabezpieczenia sieci bezprzewodowej przed nie autoryzowanym korzystaniem z naszego Internetu czy zasobów naszej sieci wewnętrznej [6]:

- **WPA/WPA2 – Personal** jest najprostszą metodą zabezpieczenia, gdyż wszystko możemy skonfigurować na swoim urządzeniu/routerze bez żadnych innych komputerów czy też urządzeń zewnętrznych,

Rys 1. WPA/WPA2 – Personal [4].

- **WPA/WPA2 – Enterprise (WPA-802.1x, RADIUS)** dla tej wersji zabezpieczenia naszej sieci musimy posiadać w sieci komputer z zainstalowanym serwerem Radius-a, czyli aplikacji którą możemy generować hasła dostępowe i autoryzować połączenia które będą wykonywane w sieci.

Rys 2. WPA/WPA2 – Enterprise (WPA-802.1x, RADIUS) [4].

D. **Autoryzacja** – zgoda lub brak zgody na żądaną usługę przez uwierzytelnionego użytkownika.

Zabezpieczenie to jest wykonane przez punkt dostępu lub serwer dostępu.

E. **Rejestracja raportów** – rejestr akcji użytkownika związanych z dostępem do sieci. Kontrola raportów pozwala na szybką reakcję administratorów na niepokojące zdarzenia w sieci.

Aby zabezpieczyć sieć Wi-Fi przed intruzami należy przestrzegać kilka złotych zasad [5]:

- **Nazwa sieci, czyli SSID**

Większość urządzeń kupowanych przeciętnie w sklepie ma domyślnie włączoną opcję aby rozsyłać nazwę sieci „w świat", a jeszcze częściej – jeżeli jej nie zmienimy, routery same „przedstawiają się", bo jako nazwę sieci ustawione mają markę a nawet i model. By utrudnić odnalezienie i włamanie się potencjalnemu hakerowi zwanemu War Driver, należy jedynie odznaczyć w ustawieniach naszego urządzenia rozsyłania nazwy sieci.

- **Zabezpieczmy się, używając MAC**

Wszystkie karty sieciowe mają przypisany swój nr „identyfikacyjny" czyli MAC. W opcjach urządzenia wystarczy dodać taki numer, aby sprawić by nasz punkt udostępniania sieci współpracował tylko ze znanymi adresami MAC, a resztę – ignorował. Jednak nie jest to zbyt skuteczna ochrona, niestety hakerzy stworzyli program, który zmienia domyślny numer MAC. Jednak by wejść do sieci, trzeba znać numery dodane do zaufanych.

- **Zabezpieczmy się, ograniczając zasięg**

Nic tak nie denerwuje jak brak zasięgu w telefonie gdzieś w lesie lub w szczerym polu. Taki sam „las" możemy stworzyć wokół naszego domu, gdzie nie chcemy by zasięg naszej sieci docierał. Wtedy żadne programy, czy kody nie pomogą – po prostu potencjalny włamywacz nie będzie w zasięgu sieci i nic nie zdziała. Wystarczy zastosować tłumik decybeli, który w niektórych urządzeniach jest domyślnie.

W sieciach bezprzewodowych Wi-Fi zabezpieczenia można podzielić na dwa typy: autoryzacji i transmisji. Autoryzacja ma na celu potwierdzić tożsamość użytkownika, natomiast typ transmisji ma nas zabezpieczyć przed podsłuchiwaniem. Obecnie są już nowe systemy zabezpieczeń, które posiadają same w sobie zabezpieczenie autoryzacji i transmisji.

3. METODY ATAKU

W sieciach komputerowych przesyłane są dane niekiedy o bardzo dużej wartości dla użytkowników i przedsiębiorstw. Bardzo duże znaczenie ma odpowiednie zabezpieczenie danych przed dostępem osób nieupoważnionych, które chciałyby uzyskać dostęp do danych lub urządzeń. Techniki włamań do sieci są bardzo zróżnicowane: od bardzo prostych do niezwykle trudnych. Można je podzielić na dwie kategorie: ataki pasywne i ataki aktywne [2, 9].

Ataki pasywne (passive attacks) – polegają na śledzeniu i podsłuchiwaniu w celu zyskania informacji lub dokonania analizy ruchu sieciowego. Ataki te są pierwszym krokiem do przeprowadzenia ataku aktywnego.

Przykłady [9]:

- **Social engineering** – jest to sposób na pozyskanie informacji istotnych z punktu widzenia bezpieczeństwa, takich jak: hasła, loginy, procedury bezpieczeństwa. Polega na manipulowaniu ludzką lekkomyślnością w celu osiągnięcia korzyści. Przykładami metod pozyskiwania danych są:

– fałszywe e-maile,
– podglądanie wpisywanych z klawiatury loginów i haseł,
– przeglądanie wyrzuconej dokumentacji, z której można pozyskać prywatne informacje.

- **Ataki na hasło** – każdy użytkownik sieci komputerowej ma swoje konto i hasło, które umożliwia identyfikowanie i przydzielanie uprawnień do zasobów. Użytkownik powinien je od razu zmienić po pierwszym logowaniu. Atak na hasło może być przeprowadzony metodą siłową (brute force) – sprawdzane są wszystkie możliwe kombinacje znaków lub metodą słownikową (dictionary attack) – wykorzystuje się zbiór potencjalnych haseł, które sprawdzane są po kolei.

- **Skanowanie sieci** – sondowanie atakowanego systemu poprzez przegląd jego adresów sieciowych oraz portów sieciowych. Skanowanie adresów sieciowych polega na przeglądaniu kolejnych adresów IP ze złożonego zakresu w celu wytypowania ofiary lub też poznania topologii atakowanej sieci.

Nasłuchiwanie (sniffing) – ten atak pasywny polega na monitorowaniu i rejestrowaniu identyfikatorów i haseł używanych w trakcie logowania się autoryzowanych użytkowników do sieci chronionych w celu uzyskania dostępu do systemów zabezpieczających.
Ataki aktywne (active attacks) – polegają na modyfikacji strumienia danych lub tworzeniu danych o zmienionej strukturze. Przykłady[8, 9, 11]:

- **Spoofing** - polega na podszywaniu się pod inny autoryzowany komputer. Cel pozostaje ten sam, oszukanie systemów zabezpieczających. Tradycyjnie, podszywanie oznaczało działanie atakującego, polegające na przeprowadzeniu procesu autoryzacji z jednego komputera do drugiego poprzez sfałszowanie pakietów z "zaufanego" hosta.

- **Przechwycenie sesji (hijacking)** – polega na przechwyceniu sesji w protokole TCP. Atakujący zrywa połączenie między serwerem i klientem, aby jako autoryzowany użytkownik móc kontynuować komunikację (bez konieczności logowania).

- **Koń trojański (trojan horse)** – to program, który podszywając się pod aplikacje użytkownika, dodatkowo implementuje niepożądane, ukryte przed użytkownikiem funkcje, np. wysyłanie do serwera napastnika informacji o kontach i hasłach.

- **Ataki typu DOS** – mają na celu uniemożliwienie legalnym użytkownikom dostępu do wybranych lub wszystkich usług. Mogą być wykonywane zarówno zdalnie, jak i lokalnie.

Ataki typu DOS najczęściej wykorzystywane są w celu:
- rewanżu na użytkownikach systemu lub administratorach,
- uzyskania korzyści finansowych przez nieuczciwych konkurentów,
- nieuzasadnionej, złośliwej rozrywki.

Przykładami ataków typu DOS są [10, 11]:

- **Ataki typu SYN Flood** – polegają na nawiązywaniu dużej liczby połączeń TCP z komputerem, tak aby wyczerpać jego zasoby.

- **Atak Ping of Death** – polega na wysłaniu bardzo dużej liczby pakietów testowych za pomocą polenenia ping z ustawionym rozmiarem pakietu testowego przekraczającego dopuszczalny zakres.

- **Atak smerfów (smurf attack)** – jego działanie opiera się na generowaniu dużej ilości pingów kierowanych na adresy rozgłoszeniowe z adresami źródłowymi zamienionymi na adres ofiary.

- **E-mail bombing** – polega na wysyłaniu dużej liczby wiadomości z nieistotnymi treściami, adresowanych do skrzynki osoby poszkodowanej.

- **E-mail spamming** – polega na wysyłaniu litów do wszystkich osób korzystających z określonego serwera.

- **Disable accounts** – systemy blokują funkcjonowanie konta po określonej liczbie niewłaściwych logowań bądź narzucają przerwy między kolejnymi próbami.

- **Ataki przepełnienia bufora (buffer overflow)** – wykorzystuję błąd programistyczny polegający na zapisaniu do wyznaczonego obszaru pamięci (bufora większej ilości danych, niż zarezerwował na ten cel programista.

- **Metoda tylnych drzwi (backdoor)** - aplikacja umożliwiająca swojemu autorowi wielokrotny nieautoryzwany dostęp do zdalnego systemu po uprzednim zdobyciu na nim praw administratora. Jednym ze sposobów wprowadzenia tylnego wejścia do systemu jest utworzenie konta lub procesu umożliwiającego uruchomienie innych programów z uprawnieniami super użytkownika.

4. PODSUMOWANIE I WNIOSKI

W niniejszym artykule przedstawiono zabezpieczenia i metody ataku sieci Wi-Fi. Sieć bezprzewodowa stanowi dziś najwygodniejszy sposób podziału łącza internetowego pomiędzy nowe urządzenia. Warto zadbać, aby dostęp do naszej sieci był możliwy tylko dla naszych urządzeń.
Jeżeli planujemy korzystać z sieci bezprzewodowej, musimy ją tak skonfigurować, aby tylko wybrane osoby miały do niej dostęp. W innym wypadku staniemy się ofiarami bardzo powszechnych włamań, ktoś niepożądany może podkraść nasze hasła, czytać nasze e-maile, podkradać pieniądze z naszego internetowego konta w

banku. Jeżeli nie zabezpieczymy dobrze swojej sieci może także dojść do sytuacji, gdy sąsiedzi będą korzystać z naszego łącza internetowego, przez co będzie działać wolniej. Do bezpieczeństwa należy mieć podejście ofensywne, pamiętając, że nasze sieci będą bezpieczne tylko wtedy, gdy będą regularnie testowane pod kątem ich odporności na atak. O konieczności ochrony sieci Wi-Fi raczej nikogo nie trzeba przekonywać. Jednak samo stosowanie trudnych do złamania haseł to za mało. Włamywacze stosują metody i narzędzia, które umożliwiają im łatwe łamanie takich zabezpieczeń [3, 12].

Celem artykułu nie było opisanie wszystkich zagadnień z zakresu Wi-Fi lecz zbudowanie materiału o charakterze edukacyjnym na poziomie podstawowym. Jeśli ktoś będzie zainteresowany tematem, może poszerzyć swoją wiedzę we własnym zakresie. Jest to krótki tekst mający na celu zainteresowanie czytelnika zagadnieniem i wytłumaczenie niektórych kwestii.

Literatura

1. Danowski B. „Wi-Fi. Domowe sieci bezprzewodowe. Ilustrowany przewodnik.” Helion, 2010,
2. Ross J. „The Book of Wireless: A Painless Guide to Wi-Fi and Broadband Wireless, 2nd edition”, 2009,
3. Sosinsky B. „Sieci komputerowe. Biblia” Helion, 2011,
4. http://www.continuum.com.pl/index.php/sieci/sieci-bezprzewodowe.html, (31.05.2016),
5. www.jakubas.net.pl/wp-content/uploads/2010/03/IS5-Mechanizmy-zabezpiecze%C5%84-sieci-bezprzewodowych-Jakubas-Kucharski.pdf, (31.05.2016),
6. www.tplink-forum.pl/faq-konfiguracja-tp-link-a/wpa-personal-a-wpa-enterprise/, (31.05.2016),
7. www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/, (31.05.2016)
8. 4titzubel.blogspot.com/2013/01/metody-atakow-na-sieci-komputerowe.html, (31.05.2016),
9. www.computerworld.pl/news/401611/Ataki.na.Wi.Fi.i.techniki.obrony.html, (31.05.2016)
10. http://magazynt3.pl/Ataki-typu-DoS-Anatomia-zagrozenia-i-metody-obrony/, (31.05.2016)
11. http://www.testinformatyk.cba.pl/klasa2.php?te=Ataki%20sieciowe%202, (31.05.2016),
12. http://www.continuum.com.pl/index.php/bezpieczenstwo/jak-zabezpieczyc-siec-wifi.html, (31.05.2016).