Kryptografia i bezpieczeństwo systemów informatycznych

Projekt zaliczeniowy

Bezpieczeństwo sieci Wi-Fi - standardy WEP, WPA, WPA 2, WPA 3

Karol Perec
Dominik Wróbel

Spis Treści

1. Wstęp

Technologie bezprzewodowe od momentu ich wprowadzenia na przełomie XX i XXI wieku cieszą się stale rosnącą popularnością. Korzystanie z sieci bezprzewodowych stało się dziś na tyle powszechne, że trudno wyobrazić jest sobie dzisiejszą rzeczywistość bez tego rodzaju transmisji.

Spektrum urządzeń korzystających z transmisji bezprzewodowej jest bardzo szerokie i stale rośnie - do urządzeń tych zaliczamy laptopy, smartfony, tablety, telewizory, drukarki, samochody, drony i wiele więcej.

Technologie te są niezastąpione w zastosowaniach gdzie konieczna jest mobilność urządzeń. Kolejnym czynnikiem warunkującym sukces tej technologii jest wygoda użytkownika, która wzrasta wraz z usunięciem mediów fizycznych.

Łatwość użycia technologii bezprzewodowych przychodzi jednak z nowymi wyzwaniami względem ich bezpieczeństwa.

W projekcie tym, wykonany zostanie przegląd i omówienie rozwiązań stosowanych w zapewnianiu bezpieczeństwa dla sieci bezprzewodowych.

1. Standardy 802.11 i 802.11i

1.1 IEEE 802

Institute of Electrical and Electronic Engineers (IEEE) to organizacja zajmująca się standaryzacją w dyscyplinach związanych z elektroniką i elektryką. Jednym z projektów tej organizacji jest grupa standardów nazwana IEEE 802. Standardy te obejmują swoim zakresem lokalne (LAN) i miejskie sieci komputerowe (MAN) przesyłające dane w systemie pakietowym. Jedną z podgrup tego standardu jest standard IEEE 802.11, który opisuje działanie bezprzewodowych sieci lokalnych Wireless Local Area Network (WLAN).

1.2 IEEE 802.11

Standard ten opisuje warstwę fizyczną i podwarstwę MAC bezprzewodowych sieci lokalnych (WLAN). W standardzie tym zawarte są podstawowe usługi i parametry działania sieci bezprzewodowych. Istnieje wiele wersji tego standardu, przykładowo 802.11a/b/g/n, które różnią się głównie szybkością, techniką modulacji czy kompatybilnością wstecz. Sieci bezprzewodowe od początku swojej standaryzacji miały zapewniać bezpieczeństwo i ochronę prywatności. Pierwszym

mechanizmem mającym zapewniać bezpieczeństwo był **Wired Equivalent Privacy** (**WEP**). Algorytm ten zdefiniowany został w pierwszej oryginalnej specyfikacji 802.11. Mechanizm ten okazał się być jednak dotkniętymi poważnymi brakami, co wymusiło wprowadzenie nowych rozwiązań względem bezpieczeństwa.

1.3 IEEE 802.11i

W związku z brakami jakie zawierał mechanizm WEP w kolejnym ze standardów 802.11i wprowadzono solidniejsze mechanizmy bezpieczeństwa, m.in. **Wi-Fi Protected Access** (**WPA**). Standard WPA został stworzony przez stowarzyszenie Wi-Fi Alliance, które zrzesza w swojej działalności firmy przemysłowe zajmujące się sprzętem działającym w standardzie 802.11. Rozwinięciem standardu bezpieczeństwa WPA były jego kolejne wersje WPA 2 oraz WPA 3.

2. Problemy bezpieczeństwa w sieciach bezprzewodowych

W tym rozdziale omówione zostaną podstawowe problemy bezpieczeństwa w sieciach bezprzewodowych, w kolejnych rozdziałach przedstawione zostaną mechanizmy i rozwiązania ukierunkowane na rozwiązanie tych problemów.

2.1 Uwierzytelnianie

Uwierzytelnianie w sieciach bezprzewodowych polega na potwierdzeniu przez klienta, że jest on tym za kogo się podaje i, że jest uprawniony do korzystania z sieci do której chce się połączyć. Najczęściej realizowane jest to przy pomocy informacji, które znajdują się tylko po stronie udostępniającego sieć, przykładowo hasło. Najbardziej powszechne mechanizmy uwierzytelniania to:

- WEP key
- WPA pre-shared key
- Central database
- Two-factor authentication

2.2 Szyfrowanie

Szyfrowanie to proces zamiany danych według pewnego algorytmu w taki sposób aby osoba, która przechwyci wiadomość nie była jej w stanie odczytać.

Szyfrowanie byłoby samo w sobie bezużyteczne gdyby zaszyfrowana wiadomość nie mogła zostać odszyfrowana.

Dwie najważniejsze techniki szyfrowania to:

- szyfrowanie z kluczem symetrycznym

Polega na zastosowaniu tego samego klucza do szyfrowania i odszyfrowania wiadomości. Taki rodzaj szyfrowania używany jest przez mechanizm WEP.

- szyfrowanie z kluczem asymetrycznym

Polega na zastosowaniu dwóch różnych kluczy do szyfrowania i odszyfrowania wiadomości.

3. Wired equivalent privacy - WEP

W rozdziale tym przedstawione zostaną rozwiązania stosowane pierwotnie w zabezpieczeniach sieci bezprzewodowych ustanowione przez WEP. Po dyskusji mechanizmów bezpieczeństwa przedstawione zostaną braki jakie posiadały przez co finalnie wyszły z użycia.

3.1 Uwierzytelnianie WEP

WEP pozwala na uwierzytelnianie nowego klienta na dwa sposoby: *shared-key authentication* oraz *open authentication*.

3.1.1 Shared-key authentication

Klucz WEP stosowany jest do sprawdzania czy użytkownik powinien mieć dostęp do sieci bezprzewodowej. Access Point oraz klient przechodzą przez procedurę, która nazywana jest *four-way-handshake:*

1. Klient wysyła żądanie uwierzytelnienia do Access Point

2. Access Point wysyła do klienta wiadomość (challenge) w formacie clear-text
3. Klient szyfruje otrzymaną liczbę skonfigurowanym kluczem WEP i odsyła wiadomość do Access Point z kolejnym żądaniem uwierzytelnienia
4. Access Point odszyfrowuje wiadomość i porównuje z wysłaną wiadomością, jeśli pasują, wysyła pozytywną odpowiedź

Po pozytywnym uwierzytelnieniu klucz WEP używany jest do szyfrowania z użyciem algorytmu RC4.

3.1.2 Open authentication

W tym sposobie w celu uwierzytelnienia wysyłane są tylko dwie wiadomości:

1. Klient wysyła żądanie uwierzytelnienia do Access Point
2. Access Point wysyła wiadomość zwrotną, że klient jest uwierzytelniony

W tym podejściu AccessPoint opiera się na przekonaniu, że jeśli jest w stanie odczytać wiadomość od klienta przy użyciu swojego klucza WEP, to zarówno on jak i klient muszą mieć ten sam klucz WEP.

3.1.3 Porównanie metod

Lepszą metodą uwierzytelniania jest metoda *Open authentication*, choć z początku może wydawać się mniej bezpieczna.

Metoda *Shared-key* jest tak naprawdę poważnym naruszeniem bezpieczeństwa. Dzieje się tak dlatego, że w tym podejściu podsłuchujący transmisję ma dostęp zarówno do danych w postaci *clear-text* oraz tych samych danych w postaci zaszyfrowanej kluczem WEP.

Mając dostęp do postaci *clear-text* oraz zaszyfrowanej tej samej wiadomości oraz wiedząc, że WEP opiera się o algorytm szyfrowania RC4, możliwe są próby odtworzenia szyfru WEP.

3.2 Szyfrowanie WEP

Szyfrowanie WEP korzysta z algorytmu RC4 oraz używa współdzielonego klucza symetrycznego, szyfrowanie to działa na zasadzie szyfru strumieniowego.

WEP jest szyfrowaniem, które działa w warstwie 2 modelu OSI.

Obecnie WEP jest jednak uznawany za zupełnie nieakceptowalny algorytm szyfrowania ze względu na to, że jest podatny na ataki.

3.2.1 Klucz WEP

Klucze WEP konfigurowane są przez administratora, ich długość to 40 lub 104 bit (plus 24 bity tzw. wektora inicjalizującego, który zmienia się z każdym pakietem). Wektor ten został wprowadzony w celu zwiększenia bezpieczeństwa aby każdy z pakietów był szyfrowany innym kluczem.

Aby klient mógł odczytać wiadomość, potrzebuje znać cały klucz wraz z wektorem inicjalizującym, wektor ten przesyłany jest w każdym pakiecie jako *clear-text*.

Klucz WEP używany w szyfrowaniu to po prostu hasło do Access Point, które konfigurowane jest przez administratora, a które każdy klient podaje gdy chce się podłączyć do sieci. Oczywiście hasło to musi wcześniej zostać dostarczone do wszystkich upoważnionych klientów pewnym bezpiecznym kanałem (*pre-shared key*).

3.2.2 Algorytm RC4

WEP korzysta z algorytmu RC4 do szyfrowania wiadomości, algorytm ten nie jest jednak bezpieczny w tej implementacji. Sam algorytm RC4 jest powszechnie stosowany w innych protokołach, gdzie zapewnia wymagany poziom bezpieczeństwa (przykładowo WPA). Niewystarczające bezpieczeństwo WEP nie jest więc

wynikiem niepoprawności algorytmu RC4, ale raczej jego niewłaściwej implementacji i stosowania.

Algorytm RC4 traktuje klucz WEP jako wejście do algorytmu, szyfrowanie RC4 można w uproszczeniu opisać w następujących krokach:

1. Przy użyciu klucza WEP generowany jest tzw. keystream, algorytm generujący keystream nazywany jest Key-scheduling algorithm (KSA)
2. Wygenerowany keystream poddawany jest pewnym modyfikacjom przy użyciu algorytmu Pseudo-random generation algorithm (PRGA)
3. Następnie właściwa wiadomość poddawana jest operacji XOR z wygenerowanym ciągiem i wysyłana jest do odbiorcy

Podobnie przebiega algorytm deszyfrowania, kolejne czynności wykonywane są w odwrotnej kolejności.

3.3 Złamanie zabezpieczeń WEP

WEP został po raz pierwszy złamany w roku 2001 przez trzech naukowców zajmujących się kryptografią.

Słabością zabezpieczeń WEP jest 24-bitowy losowy wektor dołączany do klucza. Wektor ten jest dołączany

po to aby wszystkie pakiety szyfrowane były różnymi kluczami.

Problem powstaje jednak w przypadku gdy dla dwóch pakietów zostanie wylosowany ten sam wektor losowy, co jest mało prawdopodobne, ale możliwe (24 bity pozwalają na wygenerowanie 16,777,216 unikalnych wektorów).

Atak polega na podsłuchiwaniu wymienianych w sieci pakietów podczas jej normalnego funkcjonowania. Znalezienie odpowiedniej liczby pakietów z takim samym wektorem losowym pozwala na odgadnięcie klucza WEP.

Zapewnienie bezpieczeństwa sieciom bezprzewodowym wiązało się zatem z koniecznością wprowadzenia nowych rozwiązań, w wyniku tego powstał standard WPA.

4. Wi-Fi Protected Access - WPA

Literatura