Ataki na sieci bezprzewodowe

Karol Bonenberg

Karol Maciaszek

Plan prezentacji

1. Wstęp
2. WLAN
3. Otwarte sieci (scenariusz 1)
4. Filtrowanie po MAC (scenariusz 2)
5. WEP 128 (scenariusz 3)
6. WPA PSK (scenariusz 4)
7. Podsumowanie
8. Perspektywy

Wstęp

- Zakładamy podstawową wiedze z zakresu sieci bezprzewodowych zdobytą w czasie kursu na przedmiotach SK, BSK i BWSK
- Przypominamy o możliwych konsekwencjach prawnych związanych z łamaniem zabezpieczeń (filtrowanie MAC, WEP, WPA)

Sieci WLAN

- Sieci IEEE 802.11x wykorzystują do transmisji fale radiowe RF o częstotliwości 2,4 GHz lub 5 GHz
- Sieci WLAN zastępują tradycyjne okablowanie strukturalne
- Mają szerokie spektrum zastosowań :
  - Firmy, które chcą zapewnić mobilność i elastyczność
  - Produkcja i magazynowanie
  - Kampusy
  - Hale wystawowe
  - Zabytkowe budynki (!)

Sieci WLAN

- Coraz częściej wykorzystywane przez dostawców usług internetowych
- Publiczne punkty dostępowe – hotspoty (!)
- Wykorzystywane w atakach social engineering do ominięcia zabezpieczeń

- Używając sieci bezprzewodowych, dajemy dostęp do fizycznego medium transmisji **nieograniczonej liczbie osób**.

Otwarte sieci

Filtrowanie po MAC

- Adresy MAC są teoretycznie unikalne
- Gdyby tak było w rzeczywistości, filtrowanie MAC zapewniałoby skuteczną kontrolę dostępu
- Mimo wszystko możliwe byłoby bierne podsłuchiwanie komunikacji
- Obecnie zmiana adresu MAC obsługiwana jest przez większość kart bezprzewodowych

Filtrowanie po MAC

- Do ataku wykorzystujemy kolejno :
  - kismet
  - ifconfig
  - aireplay-ng -0 (opcjonalnie)
- Scenariusz 2 - pokaz

WEP

WPA

- Ze względu na wady mechanizmu WEP stworzono nowy standard 802.11i czyli WPA2
- WPA to standard przejściowy między WEP a WPA2
- Na WPA składają się :
  - 802.1x standard IEEE dla kontroli dostępu
  - EAP uwierzytelnia za pomocą arch. klient/serwer
  - Mechanizm Michael zapewnia integralność
  - Protokół TKIP zabezpiecza warstwę łącza danych

WPA

- WPA = 802.1x+EAP+TKIP+MIC
- WPA dzieli się na :
  - Enterprise – korzysta z serwera RADIUS
  - Personal – wykorzystuje klucz PSK
- WPA różni się od WPA2 (802.11i) metodami szyfrowania

WPA a WPA 2

- WPA wykorzystuje do szyfrowania protokół TKIP
- WPA2 wykorzystuje protokół CCMP (oparty na symetrycznym algorytmie Rijndael)
- WPA wykorzystuje również Michael (MIC)
- To co nas interesuje najbardziej, to fakt, że **nie ma różnicy w łamaniu sieci zabezpieczonych WPA oraz WPA2 wykorzystujących PSK.**

Łamanie WPA

- Klucz PSK to alternatywa dla uwierzytelniania za pomocą serwera
- PSK składa się z ciągu 256 bitów lub hasła o długości od 8 do 63 znaków z którego generowany jest wspomniany ciąg
- PSK = PBKDF2(hasło, SSID, długość, SSID, 4096, 256)
- Klucz jest zależny od nazwy sieci, 4096 operacji mieszania na każde sprawdzane hasło spowalnia atak siłowy **ale jest możliwy!**

Łamanie WPA

- Wykorzystujemy słabość negocjacji czteroetapowej przy generowaniu kluczy (4-way handshake)
- Atak sprowadza się do przechwycenia negocjacji i poddania słownikowemu lub siłowemu atakowi w trybie **offline**
- Ostatnia cecha czyni łamanie WPA trochę bardziej przyjemne

Atak na WPA

- W przykładzie łamiemy WPA-PSK
- Aby zdobyć komunikaty negocjacji czteroetapowej przeprowadzamy deautentykacje
- Wykorzystujemy kolejno:
  - kismet
  - airodump-ng
  - aireplay-ng -0 (deautentykacja)
  - aircrack-ng

Atak na WPA

- Atak jest dosyć wolny, możliwe jest przyspieszenie dzięki rozproszeniu obliczeń
  - aircrack na laptopie – około 60 h/s
  - egik Marcina Szymankiewicza – około 6 000 h/s
- Scenariusz 4

Atak na WPA

- Po wejściu do sieci wedle uznania :
  - thcrut
  - p0f
  - nmap
  - metasploit framework
  - hydra-ng
  - dsniff / tcpdump
  - arpspoof
  - jedyne ograniczenie to wyobraźnia

Podsumowanie

- Teoretycznie standard WPA2 zapewnia całkowite bezpieczeństwo, jednak z nieznanych nam przyczyn sieci bezprzewodowych nie stosuje się w najważniejszych instytucjach (banki, ambasady)

Zabezpieczenia w praktyce

- Tutaj mapa

Zabezpieczanie

- AP nie powinien być połączony bezpośrednio z siecią przewodową
- Użytkownicy sieci WLAN powinni być uwierzytelniani (VPN, SSH, 802.1X itp.)

Zabezpieczanie

- Włączyć ukrywanie SSID
- Zmieniać domyślne ustawienia AP
- Aktualizować firmware AP
- Włączyć kontrolę dostępu MAC i IP
- Unikać krótkich i łatwych do odgadnięcia haseł
- Obserwować czy nie powstają inne AP
- Kontrolować moc nadajników
- Pozostałe mechanizmy jak w sieciach przewodowych