SYSTEMY WYKRYWANIA WŁAMAŃ DLA SIECI BEZPRZEWODOWYCH WI-FI

Krzysztof Cabaj*, Krzysztof Szczypiorski**
Politechnika Warszawska

**** Instytut Informatyki PW - e-mail: K.Cabaj@elka.pw.edu.pl***
***** Instytut Telekomunikacji PW - e-mail: K.Szczypiorski@tele.pw.edu.pl***

Wstęp

Bezprzewodowe sieci lokalne (Wireless LANs, zwane dalej sieciami Wi-Fi) stały się jednym z ulubionych celów ataku ze strony hakerów. Wpływ na to ma upowszechnienie się tego typu sieci, a także to, że są one najczęściej uruchamiane bez odpowiednich zabezpieczeń. Prostota, z jaką można się za ich pomocą dostać do dobrze chronionej od strony Internetu przewodowej sieci instytucji, jest także atrakcyjną zachętą. Innym ważnym powodem jest możliwość przeprowadzania tak zwanego ataku parkingowego (znalezienie się w zasięgu sieci Wi-Fi i próba zaatakowania sieci), który praktycznie uniemożliwia identyfikację atakującego.

Jak zabezpieczyć się przed tego typu zagrożeniami? Oczywiście pierwszym krokiem jest poprawna konfiguracja urządzeń sieciowych, oraz stacji klienckich z wykorzystaniem protokołów zabezpieczających na poziomie warstwy MAC (WEP, TKIP, CCMP, IEEE 802.1X/EAP), a także protokołów warstw wyższych, w tym rozwiązań typu bezpieczny VPN. Jednak natura sieci Wi-Fi, polegająca na wykorzystaniu fal radiowych, umożliwia każdemu próby podsłuchu, czy komunikacji z infrastrukturą udostępnianą przez eter. Zabezpieczenia kryptograficzne także w sieciach bezprzewodowych nie gwarantują pełnego bezpieczeństwa. Jest to czasem ironicznie określane mianem umieszczania ogólnodostępnego gniazda sieciowego typu RJ-45 na parkingu. Z tego też powodu sieci Wi-Fi powinny być stale monitorowane. Oczywiście można skorzystać z systemów IDS przewidzianych dla sieci przewodowych, jednak w ten sposób traci się część istotnych informacji, które są wymieniane przy pomocy protokołów warstwy 2. modelu OSI, w szczególności MAC. Dotyczy to głównie ramek sterujących, służących do zarządzania sesjami komunikacyjnymi.

Oprogramowanie specjalizowane do sieci Wi-Fi najczęściej korzysta z trybu *rfmon* (tzw. monitor mode) karty sieciowej. Pozwala to na podsłuch wszelkich ramek na danym kanale radiowym. Dzięki temu można wykryć specyficzne dla tego typu ataki – przykładowo próby ataków typu DoS na klientów, czy punkty dostępowe wykorzystujące ramki zarządzające.

Jakie są możliwe zagrożenia?

Dwoma najczęściej występującymi problemami są:

- **próby włamań przez hakerów** do tego typu sieci

- oraz **uruchamianie przez użytkowników nieautoryzowanych punktów dostępowych**, stających się tylnymi drzwiami do sieci.

Aktualnie wydaje się, że ten drugi problem jest poważniejszy. Nagminnie pracownicy firmy, bez zgody i wiedzy osób odpowiedzialnych za bezpieczeństwo uruchamiają sieci dostępowe. Wpływ na to ma niska cena tego typu urządzeń na rynku, oraz prostota, z jaką można uruchomić tego typu instalację. Standardowa konfiguracja urządzeń pozwala na rozpoczęcie pracy zaraz po wyjęciu urządzenia z pudełka. Uruchomienie sprowadza się do podłączenia urządzenia do sieci elektrycznej oraz wpięcia w istniejącą przewodową sieć lokalną. Niewielu tego typu użytkowników, zmienia standardowe ustawienia, czy włącza szyfrowanie transmisji (chociażby skompromitowany WEP ze statycznymi kluczami). W ten sposób, mimo wielu zabezpieczeń od strony Internetu, sieć staje się praktycznie dostępna dla każdego posiadacza komputera przenośnego z kartą Wi-Fi. Przez komputer przenośny możemy rozumieć także urządzenia typu palmtop, które wyglądając na kolorowe niewinne zabawki, są znakomitymi narzędziami, aby penetrować sieć z ogólnodostępnych miejsc budynku (korytarze, poczekalnie, toalety, barki).

Warto podkreślić, że problem ten dotyka nie tylko instytucji, które posiadają wdrożone instalacje Wi-Fi. Co gorsze: dla tych, które nie posiadają tego typu instalacji, problem jest jeszcze groźniejszy. Nie ma tam najczęściej sprzętu oraz oprogramowania, które chroniłyby sieć instytucji od bezprzewodowego świata. Nikt też nie bierze pod uwagę nasłuchu sieci radiowych, ponieważ oficjalnie ich po prostu nie ma.

Co można zrobić, aby się przed tym zagrożeniem bronić?

Wydaje się, że najpilniejszym problemem jest permanentne monitorowanie, czy na naszym terenie nie zostały uruchomione żadne nowe punkty dostępowe. Pojawiający się punkt dostępowy może oznaczać próbę ataku typu „man in the middle” lub uruchomienie tego urządzania przez pracownika na własną rękę.

Rozwiązania programowe, które mogą pomóc w wykryciu tego typu urządzeń nie są skomplikowane. Przykładem programu, który warto wskazać jest **WIDZ** – Wireless IDS [4]. Jest to pakiet oprogramowania, specjalnie przystosowany do wykrywania zagrożeń w sieciach Wi-Fi. Mimo tego, że jest to oprogramowanie napisane jako „proof of concept” można wykorzystać je do ochrony sieci. Do tego celu posłużyć może program ***widz_apmon***. Działanie tego programu jest równie proste, co skuteczne. Program działa w dwóch trybach. W pierwszym, nauki, zapisuje do pliku wszelkie działające sieci. Informacja ta po sprawdzeniu przez osobę odpowiedzialną za bezpieczeństwo staje się listą legalnych punktów dostępowych. W drugim trybie – monitoringu - program próbuje podłączyć się do wszystkich dostępnych aktualnie punktów dostępowych. Podczas tego procesu zbiera SSID sieci oraz adres MAC karty AP. Informacje te porównuje z zapisanymi w pliku danymi o legalnych punktach dostępowych. Jeśli wykryje nową sieć, wcześniej nie obserwowany SSID, bądź

zmianę adresu MAC generuje alarm. W ten sposób można wykryć pojawiające się AP jak i próby ataków typu „man in the middle”.

Wykrycie, że na danym terenie jest uruchomiony nielegalny punkty dostępowy jest tylko początkiem działań zmierzających do usunięcia go. Trzeba teraz możliwie szybko zlokalizować jego miejsce. Oczywiście jednym z możliwych rozwiązań jest zaopatrzenie się w komputer przenośny z kartą Wi-Fi (pamiętajmy o palmtopach!) i wyszukiwanie miejsca za pomocą pomiaru mocy sygnału. Jednak dla instytucji obejmujących wiele budynków, bądź też nawet jeden, ale z różnymi strefami dostępu, tego typu podejście może być bardzo kłopotliwe do zastosowania.

Pomocnym może się stać pakiet ***Kismet*** [2]. Jest to program umożliwiający podsłuch sieci radiowych i wykrywanie wszelkiego ruchu w eterze. Przydatnymi w tym celu funkcjami są: możliwość nasłuchu na wielu kanałach czy wykrywanie adresów IP na podstawie podsłuchanego ruchu sieciowego. Program także umożliwia wykrywanie sieci, które się nie ogłaszają na podstawie bezpośredniej transmisji pomiędzy urządzeniami.

Do wyśledzenia miejsca gdzie może być umieszczony nieautoryzowany punkt dostępowy może pomóc nam także idea działania większości AP. Tego typu urządzenia działają jako most, pomiędzy sieciami standardów IEEE 802.11 i (najczęściej) IEEE 802.3 (rodzina Ethernet). Umieszczenie w sieci przewodowej AP spowoduje, że wszystkie informacje przesyłane przy pomocy broadcastów i multicastów zostaną wysłane w eter. Dotyczy to między innymi zapytań o MAC adresy wysyłane przez protokół ARP. W przypadku, najczęściej dzisiaj wykorzystywanych, maszyn działających pod kontrolą systemu Microsoft Windows, do tego celu mogą posłużyć także cyklicznie rozsyłane przez maszyny informacje o ich działaniu (ruch UDP na porcie 137). Zadanie to mogą ułatwić także wszelkiego typu specyficzne urządzenia, które rozsyłają pewne informacje przy pomocy broadcastów.

Zatem jak wykryć przybliżone miejsce uruchomienia punktu dostępowego? Jeśli w sieć instytucji zostanie umieszczony AP działający jako most informacje dotyczące ruchu w danej domenie rozgłoszeniowej zostaną wyłapane przez program ***Kismet***. Zaobserwowane adresy IP pozwolą zlokalizować podsieć, do której podłączony jest AP, a zatem jego przybliżone miejsce. Oczywiście informacje o lokalizacji będą podawane z różną dokładnością, w zależności od topologii sieci i sposobu przydziału adresów IP. Odpowiedni podział sieci na podsieci czy zastosowanie **VLAN** może ułatwić dokładniejsze zlokalizowanie miejsce AP.

Przykładowo włączenie w ramach eksperymentu AP zamiast komputera, w jedną z uczelnianych sieci laboratoryjnych na Wydziale Elektroniki i Technik Informacyjnych PW, pozwoliło w kilkanaście minut wykryć większość serwerów z danego laboratorium, a także maszyny pracownicze oraz adresy bramy do reszty sieci. Informacje te pozwalają łatwo zidentyfikować podsieć, w której został umieszczony punkt dostępowy.

Oczywiście wykrycie punktu dostępowego można przeprowadzić także od strony sieci przewodowej. W tym wypadku wykrycie polega na nasłuchu pojawiających się adresów MAC, które nie należą do kart sieciowych zainstalowanych w komputerach instytucji. W tym wypadku można wykorzystać programy, czy systemy IDS dedykowane sieciom przewodowym. Przykładowo program ***arpwatch***.

Inną przydatną funkcją programu ***Kismet*** jest możliwość nasłuchu na wszystkich kanałach. Jest to wykorzystanie funkcjonalności trybu „monitor mode" karty Wi-Fi. Oczywiście nasłuch nie jest realizowany równolegle. Program nasłuchuje na jednym kanale radiowym przez pewien czas, a następnie przechodzi do kolejnego. Praca w tym trybie może spowodować utratę pewnych informacji, jednak umożliwia przy pomocy jednej karty Wi-Fi sprawdzanie wszystkich dostępnych kanałów. Przy odpowiednio długiej transmisji, lub czasie działania wszystkie sieci zostaną wykryte.

Program ***Kismet*** można także wykorzystać jako system IDS specjalizowany w wykrywaniu ataków skierowanych na sieci Wi-Fi. W tym momencie zostają wykorzystywane dane z warstwy 2. Rozwiązanie to jest lepsze niż wykorzystanie systemów IDS dla sieci przewodowych, które nie mają dostępu do tego typu danych. W czasie tego trybu pracy, karta Wi-Fi zostaje przełączona również w tryb „monitor mode". Dzięki temu możliwy jest nasłuch wszelkich danych dochodzących do karty, a nie tylko ramek niosących dane. Aktualnie ***Kismet*** jest w stanie wykryć najpopularniejsze ataki. Częściowo robi to na podstawie pewnych charakterystycznych ustawień pakietów np.: program ***AirJack*** [6] ustawia SSID na *airjack* itp. Oprócz tego analizuje pewne niepokojące zdarzenia jak np. próba rozłączenie użytkownika czy przełączenie go na nowy kanał z tym samym numerem SSID. Niestety aktualnie wadą tego programu jest brak możliwości dopisywania własnych sygnatur. Przykładowo - najnowsza dostępna wersja programu ***Kismet*** (z kwietnia 2004) nie wykrywa już najnowszej wersji ***NetStumblera*** [7] (0.4.0), chociaż dzielnie radzi sobie z wersjami 0.3.x.

Na uwagę zasługuje także architektura całego systemu. Kismet może analizować dane z różnych źródeł. Najczęściej źródłem jest sterownik lokalnej karty Wi-Fi. Jednak możliwe jest uruchomienie sensora na wybranej maszynie a analizowanie danych z niej pochodzących w innym miejscu. W ten sposób można centralnie analizować dane spływające z wielu sensorów. Informacja o tym, z którego sensora pochodzą dane, umożliwia także łatwiejsze zlokalizowanie miejsca transmisji. Osobna konfiguracja każdego sensora pozwala także na elastyczne tworzenie instalacji, które są najbardziej dopasowane do potrzeb. Przykładowo, na kanałach, które są wykorzystywane przez sprzęt w danej firmie można prowadzić ciągły nasłuch, a wykrywanie prób skanowań aktywnych, innych ataków czy pojawiających się nielegalnych punktów dostępowych, można prowadzić przy pomocy jednej karty. W ten sposób na chronionych kanałach jest zminimalizowana szansa utraty zdarzeń, a oprócz tego pozostałe kanały są monitorowane przy zachowaniu stosunkowo niskich kosztów.

Wspomnianą wcześniej wadą programu ***Kismet***, brak tworzenia własnych reguł można rozwiązać stosując program ***Wireless-Snort*** [3]. Jest to zestaw preprocesorów oraz łatka na ***Snort'a*** [1] – aktualnie najlepszy darmowy system IDS. Po instalacji tego pakietu dostajemy możliwość analizowania ruchu w sieciach Wi-Fi. Przy pisaniu własnych reguł dostajemy nowy protokół – **wifi,** oraz dodatkowe opcje z nim związane. Opcje te dotyczą pól występujących tylko w ramkach standardu IEEE 802.11. W ten sposób można generować alarm, jeśli zostanie wykryta ramka z pewnymi ustawieniami SSID. Możliwe jest także tworzenie reguł, które analizują specyficzne ramki zarządzające, czy sterujące. Przykładowa reguła pozwala na wykrycie podszywania się pod AP o określonym SSID i adresie MAC.

```
alert wifi !00:0D:88:91:52:1F -> any (msg:"Atak man-in-the-middle ";stype:STYPE_BEACON;ssid:"My AP1";)
```

Możliwość tworzenia własnych reguł pozwala na wykrywanie znanych ataków i szybką rakcję na zmiany w oprogramowaniu hakerskim. Za pomoca **Snort'a** można próbować wykrywać przykładowo próby skanowań opisane w pracy Joshua Wrighta [5].

W skład pakietu wchodzi także zestaw dodatkowych preprocesorów specjalizowanych do wykrywania ataków na sieci bezprzewodowe. Przykładowe preprocesory to ***rogue_ap*** (wykrywający pojawiające się sieci), ***deauth_flood*** (wykrywający ataki polegające na rozłączeniu zalogowanych do AP użytkowników), czy ***antistambler*** (wykrywający użycie programu ***NetStambler*** do wyszukania aktualnie działających sieci Wi-Fi).

Podsumowanie

Pojawianie się w instytucjach sieci Wi-Fi jest faktem – istotne jest rozważenie tego czynnika podczas projektowania systemu zabezpieczeń. Dotyczy to instytucji, które posiadają już wdrożone instalacje Wi-Fi jak i tych, które tego nie planują. Wykrywanie zagrożeń związanych z atakami na sieci bezprzewodowe można wykonywać za pomocą dobrze znanych i sprawdzonych narzędzi dla sieci przewodowych, jednak w ten sposób pewne zdarzenia mogą pozostać niezauważone lub zostać wykryte za późno. Przedstawione w tym artykule specjalizowane dla sieci Wi-Fi narzędzia pozwalają wykrywać część z tych zagrożeń. Aktualnie narzędzia te nie są jeszcze do końca dopracowane, jednak pozwalają na zwiększenie bezpieczeństwa przy relatywnie małych kosztach. W większości do ich wdrożenia potrzebny jest komputer z zainstalowanym systemem ***Linux***, kartą Wi-Fi i prezentowanym oprogramowaniem.

Literatura

[1] Snort, Martin Roesch
http://www.snort.org
[2] Kismet, Mike Kershaw
http://www.kismetwireless.net/documentation.shtml
[3] Snort-Wireless, Andrew Lockhart
http://www.snort-wireless.org/

[4] WIDZ (Wireless IDS), Mark "Fat Bloke" Osborne
http://www.loud-fat-bloke.co.uk/w80211.html
[5] „Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection”, Joshua Wright
http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf
[6] AirJack
http://sourceforge.net/projects/airjack
[7] NetStumbler, Marius Milner
http://www.netstumbler.com/

Lista skrótów

AP	Access Point
ARP	Address Resolution Protocol
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
DoS	Denial of Service
EAP	Extensible Authentication Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
OSI	Open System Interconnection
RJ	Registered Jack
SSID	Service Set IDentifier
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
VLAN	Virtual LAN
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless-Fidelity