Jan Luch 218150

K6 - Bezpieczeństwo komunikacji bezprzewodowej i transakcji sieciowych

Niebezpieczeństwa transakcji sieciowych

Phishing to metoda, aby nakłonić do ujawnienia informacji osobistych, takich jak hasła lub numery kart kredytowych, ubezpieczeń i kont bankowych. Robią to poprzez wysyłanie fałszywych e-maili lub przekierowywanie na fałszywe strony internetowe.

Sniffing jest powszechnie stosowany do monitorowania i analizowania ruchu w sieci w celu wykrywania problemów oraz dbania o przepustowość i płynność przepływu danych. Ale sniffer może także zostać wykorzystany ze szkodą dla innych. Sniffery śledzą wszystkie dane, które przez nie przechodzą, w tym szyfrowane hasła i nazwy użytkowników, dzięki czemu hakerzy z dostępem do sniffera mają też dostęp do konta użytkownika, którego dane są monitorowane.

Spoofing polega podszywaniu się pod kogoś lub coś, aby wykraść ważne informacje lub zyskać dostęp do kont bankowych ofiary. Jest to zbiorczy termin obejmujący spoofing adresu IP (wysyłanie komunikatów do komputera z adresu IP, który sugeruje, że wiadomość pochodzi z zaufanego źródła), spoofing e-maila (podrabianie nagłówka e-maila, aby wyglądał jakby pochodził od innej osoby lub z innego miejsca niż rzeczywiście) i spoofing DNS (modyfikacja serwera DNS w celu przekierowania ruchu z konkretnej domeny na inny adres IP).

Pharming to rodzaj oszustwa przypominający phishing, ale w tym przypadku odwiedzający prawdziwą stronę są przekierowani na podszywające się pod nią strony, które instalują na ich urządzeniach złośliwe oprogramowanie lub zbierają dane osobowe, np. hasła lub dane kont bankowych.

Zagrożenia komunikacji bezprzewodowej

Rouge Access Point to dodatkowy punkt dostępowy. Rouge Access Point jest podłączany do sieci lokalnej, z którą współpracuje również sieć bezprzewodowa mająca być przedmiotem ataku.
Tego rodzaju punkty dostępowe są trudne do wykrycia, przede wszystkim wówczas, gdy napastnik sam stosuje środki bezpieczeństwa w rodzaju biernego rozsyłania SSID.

Man in the middle polega na umieszczeniu jako serwer/klient dodatkowego punktu pomiędzy regularnym klientem a punktem dostępowym. Jego zadaniem jest przechwycenie i przejęcie komunikacji między uczestnikiem a punktem dostępowym.

Network Injection - wstrzykiwanie pakietów (packet injection) polega na tym, że przez naszą kartę sieciową możemy wysłać co tylko chcemy i do kogo tylko chcemy. Wstrzykiwanie pakietów ARP ma na celu sztuczne generowanie ruchu w sieci bezprzewodowej, co znacznie przyspiesza łamanie klucza WEP.

Ataki DOS - blokada usług (ang. Denial of Service, DoS), atak mający na celu uniemożliwienia działania. Atak polega zwykle na przeciążeniu aplikacji serwującej określone dane czy obsługującej danych klientów. W sieciach komputerowych atak DoS oznacza zwykle zalewanie sieci (ang. flooding) nadmiarową ilością danych mających na celu wysycenie dostępnego pasma, którym dysponuje atakowany host.

Standardy bezpieczeństwa

WEP - był domyślnym protokołem wprowadzonym w pierwszym standardzie IEEE 802.11 jeszcze w 1999 roku. Bazuje na algorytmie szyfrującym RC4, w którym tajny klucz o długości 40 lub 104 bitów jest łączony z 24-bitowym wektorem inicjalizacyjnym (WI), tworząc ciąg używany do zaszyfrowania tekstu jawnego *M* oraz jego sumy kontrolnej ICV (*Integrity Check Value*).

Bezpieczeństwo transmisji WEP zależy od wektora inicjalizacyjnego, który dla utrzymania przyzwoitego go poziomu zabezpieczeń i minimalizacji ujawnień powinien być zwiększany dla każdego pakietu tak, by każdy kolejny pakiet był szyfrowany innym kluczem. Niestety, WI jest przesyłany otwartym tekstem a standard 802.11 nie przewiduje obowiązkowej jego inkrementacji. W efekcie dostępność tego zabezpieczenia zależy wyłącznie od implementacji standardu, która będzie działać na konkretnej stacji bezprzewodowej (punkcie dostępowym lub karcie bezprzewodowej).

WPA (ang. Wi-Fi Protected Access) – standard szyfrowania stosowany w sieciach bezprzewodowych standardu IEEE 802.11. WPA został wprowadzony jako standard przejściowy pomiędzy WEP, a zabezpieczeniem 802.11i czyli WPA2 w celu zwiększenia bezpieczeństwa użytkowników sprzętu mającego na stałe zaimplementowany WEP bez konieczności ich wymiany. Osiągnięto to przez cykliczną zmianę klucza szyfrującego WEP, co przy odpowiedniej częstotliwości zmian uniemożliwia jego złamanie pomimo istniejących podatności.

WPA2 jest ostateczną wersją "WiFi Protected Acces". Jest to najbardziej bezpieczna opcja z dostępnych i powinno się właśnie jej używać. Nowe urządzenia używają WPA2 od razu bez zbędnych konfiguracji. Są dwie wersje WPA2 z których można wybrać, jedna to WPA2 – Personal, a druga to WPA2-Enterprise. W porównaniu z WEP wykorzystuje 128-bitowe klucze kryptograficzne, ma poprawione wszystkie znalezione luki w zabezpieczeniach WEP, wykorzystuje dynamiczne klucze (na poziomie użytkownika, sesji, pakietów), automatycznie dystrybuuje klucze orazposiada podniesiony poziom bezpieczeństwa autoryzacji użytkownika.

- WPA2 – Personal, czyli WPA2-PSK(Pre-Shared Key). PSK został zaprojektowany do pracy w małym biurze lub w domu, gdy wszyscy użytkownicy będą posługiwać się tym samym kluczem. WPA-PSK jest też z tego powody nazywany WPA-Personal. Router szyfruje ruch sieciowy za pomocą klucza. Z WPA-Personal, ten klucz jest obliczany z hasłem Wi-Fi skonfigurowanym routerze. Zanim urządzenie będzie mogło połączyć się z siecią i zrozumieć szyfrowanie, musimy wpisać nasze hasło.

- WPA2-Enterptise jest również określane jako WPA2-802.1X, ze względu na standard, który wprowadza. Enterprise jest rozwiązaniem kierowanym dla sieci firmowych, ponieważ wymaga więcej sprzętu i jest trudniejsze w konfiguracji i utrzymaniu.

  Aby używać WPA2-Enterprise, potrzebny jest serwer uwierzytelniania RADIUS. Po połączeniu z siecią WiFi, każdy użytkownik będzie musiał zalogować się loginem i hasłem. Połączenie z każdym klientem będzie szyfrowane unikalny kluczem szyfrowania.