BEZPIECZEŃSTWO BEZPRZEWODOWEJ SIECI LAN

WPROWADZENIE

Bezprzewodowe sieci lokalne (LAN) zgodne ze standardem IEEE 802.11 są obecnie wszechobecne i przynoszą znaczne korzyści, takie jak mobilność, elastyczność, szybkie wdrażanie i redukcja kosztów w porównaniu z tradycyjnymi sieciami przewodowymi. Jednak, podobnie jak w przypadku każdej technologii sieciowej, bezprzewodowe sieci LAN stwarzają osobom nieupoważnionym możliwość uzyskania dostępu do sieci przedsiębiorstwa i przesyłanych przez nią informacji. Ta część zawiera przegląd technologii bezprzewodowych sieci LAN i zagrożeń bezpieczeństwa i ataki oraz jak sobie z nimi radzić. Ma następującą strukturę:

* Historia 802.11 i przegląd technologii

* Podstawy bezpieczeństwa 802.11

* Szczegółowy zakres zabezpieczeń 802.11 obejmujący zarówno oryginalną starszą funkcjonalność, jak i ulepszony system zdefiniowany po raz pierwszy w 802.11i-2004

* Podstawowe zagrożenia bezpieczeństwa sieci bezprzewodowej o średnim zasięgu-

* Specyficzne techniczne ataki na bezpieczeństwo sieci bezprzewodowej LAN

* Techniczne kontrole łagodzące dla określonych ataków na bezpieczeństwo

* Nadrzędne zasady bezpiecznego projektowania korporacyjnego

Zakres.

Zakres tej części dotyczy bezpieczeństwa bezprzewodowych sieci LAN zgodnych ze standardem ANSI/IEEE 802.11. Nie uwzględniono żadnych innych systemów bezprzewodowych, takich jak sieci telefonii komórkowej, ani innych standardów bezprzewodowych, takich jak HomeRF, Bluetooth, WiMax lub HiperLAN. Zawieramy ogólny przegląd podstaw z technicznymi głębokimi nurkowaniami w określonych obszarach niezbędnych do zrozumienia zagrożeń.

Korporacyjne użytkowanie bezprzewodowych sieci LAN.

Korporacje korzystają z bezprzewodowych sieci LAN od lat 90. XX wieku. Jednak na początku rynek był dość mały, a technologie zastrzeżone. Pod koniec lat 90. i na początku 2000 r. położono podwaliny pod masową adopcję bezprzewodowych sieci LAN. Punktem wyjścia była publikacja standardu ANSI/IEEE 802.11, który zapewnił podstawowy projekt umożliwiający producentom opracowywanie interoperacyjnych produktów przy niższych kosztach

Funkcjonalne zalety łączności bezprzewodowej.

Główne zalety wdrażania sieci bezprzewodowych to mobilność, elastyczność i redukcja kosztów.

* Mobilność: Technologie bezprzewodowe umożliwiają pracownikom dostęp do informacji sieciowych za pośrednictwem terminali mobilnych podczas poruszania się po kampusie biurowym; przykłady obejmują magazyny, hale produkcyjne i szpitale. W środowisku biurowym technologie bezprzewodowe stanowią elastyczną alternatywę lub dodatek do sieci przewodowej. Często biurka i sale konferencyjne mają ograniczoną liczbę połączeń Ethernet; technologie bezprzewodowe mogą w sposób ekonomiczny zapewnić dodatkowe połączenia sieciowe zgodnie z wymaganiami.

* Elastyczność: Publiczne sieci bezprzewodowe (hotspoty) pozwalają pracownikom na wykorzystanie czasu bezczynności między spotkaniami, na lotniskach, w kawiarniach, a nawet w samolocie. Typowe

zastosowania obejmują dostęp do firmowej sieci LAN wraz z informacjami w Internecie. Publiczne hotspoty mogą być również trankingowe przez bezprzewodową sieć LAN przedsiębiorstwa, aby zapewnić dostęp do Internetu konsultantom i gościom.

* Redukcje kosztów: Koszty można obniżyć, nie instalując fizycznych połączeń sieciowych między budynkami oddzielonymi drogą, rzeką, torami kolejowymi, a nawet blokiem miejskim. Połączenie bezprzewodowe można ustanowić między dwoma budynkami pod warunkiem, że istnieje między nimi nieprzerwana linia wzroku. Ponadto dzięki bezprzewodowemu medium można osiągnąć ekonomię skali. Pojedynczy punkt dostępowy (AP) (gruby lub cienki) może obsłużyć jednego lub wielu użytkowników końcowych i odpowiednio skalować poprzez zderzenie nadmiernej liczby użytkowników z sąsiednimi punktami dostępowymi. Ta funkcja dotyczy wyłącznie sieci bezprzewodowych. Sieć przewodowa ma stałą pojemność dla dostępu do portu i przypisania wirtualnej sieci LAN (VLAN). Korzystanie z sieci bezprzewodowej z obsługą sieci VLAN z identyfikatorem SSID (Service Set Identifier) może zmniejszyć ilość sprzętu sieciowego. W przypadku dynamicznego przydzielania sieci VLAN w przewodowej sieci LAN, ruchy punktu końcowego lub serwera wymagają odpowiedniego przycinania sieci VLAN w warstwie przełącznika, aby zachować bezpieczeństwo, a jednocześnie zapewnić wymagane sieci VLAN. Oszczędności kosztów można osiągnąć w bezprzewodowej sieci LAN, zmniejszając zadania związane z zarządzaniem siecią i ogólną złożoność, aby zmaksymalizować wykorzystanie zasobów i sprzętu.

Korzyści z łączności bezprzewodowej w zakresie bezpieczeństwa

* Bezpieczeństwo fizyczne: punkt dostępowy i sprzęt pomocniczy można ukryć przed użytkownikami końcowymi, aby chronić go przed fizycznym atakiem. Bezprzewodowy punkt dostępowy może być ukryty nad sufitem, w przeciwieństwie do fizycznych gniazd sieciowych punktów końcowych, które muszą być dostępne dla wszystkich użytkowników, którzy potrzebują dostępu do sieci wewnętrznej. Pozostawia to otwarte drzwi dla nieautoryzowanego dostępu do portu sieciowego w przypadku braku zabezpieczeń portu 802.1X w całym przedsiębiorstwie.

* Widoczność segmentacji: Sieci przewodowe często przypisują sieci VLAN na podstawie portu lub w zaawansowanych konfiguracjach, używając jednego na adres Media Access Control (MAC). W przypadku przypisywania sieci VLAN na podstawie portów zarządzanie w dużej mierze opiera się na prawidłowej konfiguracji przełącznika warstwy dostępu i usuwaniu wrażliwych sieci VLAN, które nie są konieczne w przypadku określonej jednostki biznesowej lub lokalizacji. Przypisywanie sieci VLAN na podstawie adresu MAC wymaga użycia przełącznika obsługującego uwierzytelnianie MAC oraz uwierzytelniania zaplecza i serwera RADIUS do mapowania MAC→VLAN. - podszywanie się pod adres. W środowisku bezprzewodowym sieci VLAN można przypisywać na podstawie identyfikatora SSID, co pozwala znacznie ograniczyć nakłady administracyjne. Użytkownik nie jest już ograniczony do określonej fizycznej lokalizacji w celu uzyskania dostępu do niezbędnej sieci VLAN, o ile identyfikator SSID jest dostępny w dostępnych punktach dostępu. W przypadku rozszerzenia, wdrożenie nowego AP w bliskiej odległości zapewni niezbędne sieci VLAN z odpowiednim identyfikatorem SSID, który profil suplikanta klienta jest skonfigurowany do wyszukiwania. Ponieważ przypisanie sieci VLAN może być kontrolowane przez pomniejsze konfiguracje suplikantów klienta i uprawnienia RADIUS zaplecza, segmentacja może być określona podczas procesu udostępniania zasobów i później wymaga stosunkowo niewielkiego zarządzania. W środowisku, które w dużej mierze opiera się na przełącznikach warstwy dostępu do połączeń z punktami końcowymi, nierzadko zdarza się, że protokoły przełączników lub routerów upstream docierają do portów przełączników warstwy dostępu. Należą do nich takie protokoły, jak Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), Hot Standby Router Protocol (HSRP), Cisco Discovery Protocol (CDP), routing Open Shortest Path First

(OSPF) i tak dalej. Użytkownik z dostępem do portu może wykorzystać wiele znanych luk w tych protokołach.

Zarządzanie scentralizowane.

Środowiska punktów dostępowych dla klientów uproszczonych wykorzystują kontrolery bezprzewodowe w celu zapewnienia centralnej konfiguracji dla wszystkich powiązanych punktów dostępowych. Na kontrolerze są konfigurowane punkty dostępowe Thinclient, a inteligencję zapewnia katalog użytkowników zaplecza (Extensible Authentication Protocol - Remote Authentication Dial In User Service lub EAP-RADIUS) oraz sam kontroler. Rozpowszechnione, ale centralne połączenie siatki punktów dostępowych może być dodatkowo wykorzystane do monitorowania bezpieczeństwa bezprzewodowych fal radiowych w sposób Wireless IDS.

Przegląd i historia standardów IEEE 802.11.

Pierwszy standard IEEE 802.11 został opublikowany w 1999 roku. Po publikacji kontynuowano prace nad rozwojem standardu 802.11 z publikowanymi na bieżąco poprawkami. Publikacja standardu 802.11b zwiększyła przepustowość WLAN z 2Mb/s do 11Mb/s, czyniąc go możliwym technicznym zamiennikiem przewodowej sieci LAN. Następnie pojawiły się standardy 802.11a i 802.11g, które zwiększyły przepustowość do 54Mb/s. Te i inne poprawki zostały następnie zebrane w poprawionym standardzie 802.11-2007. Rozwój był kontynuowany poprzez kolejne poprawki, które po raz kolejny zostały połączone z wydaniem 802.11-2012.3 Pierwsza wersja standardu zawierała usługi uwierzytelniania i poufności, aby zapewnić podobny poziom bezpieczeństwa jak przewodowe sieci LAN. Usługa uwierzytelniania składała się z dwóch systemów o nazwie Open Authentication i Shared Key Authentication, a usługa poufności danych została nazwana Wired Equivalent Privacy (WEP). Usługi te są często nazywane starszymi usługami bezpieczeństwa. W 2004 roku opublikowano standard 802.11i, który zdefiniował system Robust Security Network (RSN), który zapewniał ulepszone usługi uwierzytelniania i poufności. Usługa uwierzytelniania ma dwie opcje: pierwsza to użycie wstępnie udostępnionych kluczy przeznaczonych dla użytkowników domowych i małych biur domowych (SOHO), a druga korzysta ze struktury 802.1X/EAP do użytku korporacyjnego. W związku z wydaniem 802.11-2007 wprowadzono poprawki mające na celu zapewnienie mechanizmów bezpieczeństwa dla sieci bezprzewodowych typu mesh oraz wykorzystanie standardu 802.11 do transportu aplikacji. Wprowadzono również ulepszenia do podstawowych algorytmów 802.11i, aby zabezpieczyć niektóre ramki zarządzania i umożliwić szybkie przejście do innych punktów dostępowych dla usług krytycznych czasowo, takich jak Voice over IP (VoIP). Przepustowość została dodatkowo zwiększona do maksymalnie 600 Mb/s w wersji 802.11n-2009.

PODSTAWY BEZPIECZEŃSTWA 802.11.

W tej sekcji opisano podstawy zabezpieczeń 802.11 w ramach przygotowań do szczegółów omówionych w kolejnych sekcjach.

Terminologia.

Aby lepiej zrozumieć tą część, czytelnicy znajdą wyjaśnienie kilku powszechnie błędnie rozumianych terminów 802.11. Sekcja 0 zawiera obszerniejszy słowniczek.

Uwierzytelnianie: Uwierzytelnianie to pierwszy krok w dwuetapowym procesie łączenia klienta z punktem dostępowym. Ten krok weryfikuje uprawnienia klienta do rozpoczęcia kojarzenia z punktem dostępowym. Uwierzytelnianie oparte na sieci, takie jak nazwa użytkownika i hasło, odbywa się po uwierzytelnieniu i powiązaniu warstwy 2.

Powiązanie: Powiązanie to proces akceptowania przez punkt dostępu połączenia klienta i przydzielania mu zasobów. Obejmuje to takie rzeczy, jak dodawanie informacji specyficznych dla klienta, takich jak obsługiwana szybkość transmisji danych, protokół danych 802.11 b/g/n i informacje o adresie MAC.

802.1X: 802.1X zapewnia enkapsulację implementacji Extensible Authentication Protocol (EAP) w 802 mediach komunikacyjnych. 802.1X nie definiuje konkretnej metody uwierzytelniania, ale zapewnia narzędzie dla implementacji EAP i ich podstawowych metod. 802.1X i ostatecznie 802.11i są głównymi składnikami nowoczesnego systemu 802.11 RSN. 802.1X zezwala lub odmawia klientowi dostępu do żądanych zasobów, dopóki klient nie zostanie pomyślnie uwierzytelniony.

RADIUS: Usługa zdalnego uwierzytelniania Dial In User (RADIUS) to protokół sieciowy używany do uwierzytelniania, autoryzacji i rozliczania (AAA). W przeszłości serwery RADIUS wykorzystywały katalog w postaci pliku płaskiego do podejmowania decyzji dotyczących dostępu na podstawie użytkownika, ale nowoczesne implementacje wykorzystują dedykowany katalog, taki jak Windows Active Directory, Lightweight Directory Access Protocol (LDAP), lub racjonalna baza danych, taka jak Microsoft SQL Server lub Oracle. W sieci Robust Security Network (RSN) serwer RADIUS jest odpowiedzialny tylko za pośrednictwo w uwierzytelnianiu/autoryzacji użytkownika żądającego dostępu do punktu dostępowego. Dane uwierzytelniające są w sposób przezroczysty przesyłane z klienta do serwera RADIUS przez punkt dostępowy, a serwer RADIUS wykorzystuje katalog zewnętrzny do określenia odpowiedzi.

SSID kontra BSSID: SSID to unikalny identyfikator używany przez klienta do nawiązywania łączności z określoną siecią bezprzewodową. Punkt dostępowy może zapewnić wiele identyfikatorów SSID na tym samym kanale poprzez użycie tego samego lub wielu interfejsów. BSSID to unikalny identyfikator podstawowego zestawu usług (BSS). BSS składa się z punktu dostępowego i powiązanych klientów lub klientów.

Rozszerzony zestaw usług (ESS) to seria identyfikatorów BSSID (interfejsów AP) współdzielących ten sam identyfikator SSID. Pomaga to klientowi bezprzewodowemu płynnie przemieszczać się między punktami dostępowymi przy użyciu tego samego identyfikatora SSID. BSSID to oddzielny interfejs z własnym adresem MAC; wiele identyfikatorów SSID może współdzielić ten sam interfejs i adres MAC. W komercyjnym AP pierwsza para SSID/VLAN użyje interfejsu BSSID/adresu MAC, a każdy następny SSID będzie używał wirtualnego adresu MAC, który zwiększa BSSID o małą wartość dla każdego SSID. BSSID może być używany do odwoływania się do unikalnego interfejsu lub AP (zakładając, że AP ma tylko jeden interfejs). W zależności od dostawcy konkretnego AP, pojedynczy identyfikator BSSID wyśle sygnały nawigacyjne ze wszystkimi identyfikatorami SSID w jednym cyklu. Jeśli identyfikator SSID zostanie umieszczony we własnym BSSID, będzie miał dedykowany sygnał nawigacyjny, co może poprawić kompatybilność.

Uwierzytelnianie i kontrola dostępu.

W przypadku braku zabezpieczeń portów 802.1X kontrola dostępu w przewodowej sieci LAN jest uzależniona przede wszystkim od zabezpieczeń fizycznych. Aby uzyskać dostęp do sieci LAN, osoba atakująca musi najpierw mieć fizyczny dostęp do punktu połączenia. W przeciwieństwie do tego, charakter bezprzewodowych sieci LAN oznacza, że każdy klient bezprzewodowy znajdujący się w zasięgu radiowym może potencjalnie połączyć się z wewnętrzną siecią LAN, omijając kontrole fizyczne. Aby rozwiązać ten problem, 802.11 udostępnia opcjonalną usługę uwierzytelniania natywnego. Starszy standard 802.11 obejmuje dwa protokoły, uwierzytelnianie otwarte i uwierzytelnianie z kluczem współdzielonym. Żaden z tych protokołów nie był odpowiedni do bezpiecznego dostępu. Uwierzytelnianie otwarte to usługa uwierzytelniania zerowego, która umożliwia wszystkim klientom łączenie się i kojarzenie. Uwierzytelnianie za pomocą klucza współdzielonego (SKA) wymaga od klienta

użycia klucza kryptograficznego w celu pomyślnego uwierzytelnienia. Ta metoda wprowadziła pewnego rodzaju blokadę w sieci, ale wkrótce została wykorzystana przez atakujących, którzy pozyskali materiał klucza, aby pomóc w złamaniu systemu.5 SKA nie posiadała unikalnego, uwierzytelnionego śledzenia użytkowników i wymusiła pozapasmowy proces zarządzania kluczami. SKA od tego czasu jest przestarzały i nie powinien być używany, z wyjątkiem niezbędnej kompatybilności wstecznej ze starszymi urządzeniami. Starszy system zabezpieczeń 802.11 nie zapewniał żadnej funkcji kontroli dostępu. Chociaż większość urządzeń zawierała filtrowanie dostępu w oparciu o adres MAC, ta kontrola nie była częścią standardu i dlatego starsza usługa jest łatwa do pokonania. RSN zdefiniowany przez 802.11i jest znacznie silniejszym systemem i zapewnia wiele mechanizmów uwierzytelniania urządzenia i użytkownika. System definiuje profil osobisty do użytku domowego/SOHO w oparciu o PSK, a także profil korporacyjny oparty na strukturze 802.1X/EAP, który umożliwia korzystanie z serwera uwierzytelniania zaplecza. System uwierzytelniania 802.1X umożliwia również podejmowanie przez sieć decyzji dotyczących kontroli dostępu w celu ograniczenia zasobów sieciowych dostępnych dla uwierzytelnionego użytkownika za pomocą technologii takich jak segmentacja sieci VLAN.

Poufność danych.

Poufność danych w sieci przewodowej zapewnia bezpieczeństwo fizyczne i granice warstwy 2, które ograniczają dostępność danych. O ile atakujący nie jest fizycznie podłączony do przewodowej sieci LAN i logicznie znajduje się między nadawcą a odbiorcą w sieci, poprzez zatrucie ARP lub fizyczną pozycję, dane przesyłane przez sieć nie mogą zostać przechwycone. Bezprzewodowa sieć LAN wykorzystuje fizycznie publiczne medium do przesyłania danych; dlatego każdy pakiet podróżujący między klientem bezprzewodowym a punktem dostępowym jest przesyłany za pomocą sygnałów radiowych i może zostać przechwycony przez dowolnego klienta w zasięgu radiowym. Chociaż przechwycone dane mogą być zaszyfrowane i niełatwo widoczne, należy zauważyć, że każdy klient może w jakiś sposób uzyskać zaszyfrowany tekst pomimo granic warstwy 2 lub logicznych. Aby rozwiązać ten problem, standard 802.11 zapewnia usługę poufności danych. Starszy system zapewniał protokół Wired Equivalent Privacy (WEP), który szyfrował każdą wiadomość kluczem symetrycznym przed transmisją. Jednak protokół ten został skutecznie zaatakowany i zbudowano zautomatyzowane narzędzia umożliwiające złamanie kluczy WEP przez każdego, kto ma podstawowe umiejętności informatyczne i ma dostęp do bezpłatnego zestawu narzędzi. Z biegiem czasu wprowadzono ulepszenia do protokołu WEP, przesuwając go w kierunku bardziej szanowanego rozwiązania korporacyjnego, ale te okazały się niewystarczające i wkrótce zostały zastąpione nowszymi, oddolnymi protokołami. Jeśli konieczne jest użycie WEP, potrzebne są dodatkowe elementy sterujące, aby chronić sieć, na przykład w przypadku starszego istniejącego sprzętu. System RSN udostępnia dwa nowe protokoły poufne danych, zwane Temporal Key Integrity Protocol (TKIP)8 oraz tryb licznika z protokołem CCMP (Cipher-Block Chaining Message Authentication Code Protocol). Oprócz poufności oba protokoły zapewniają również integralność wiadomości.

Zarządzanie kluczami.

Samo szyfrowanie kluczem tajnym jest stosunkowo prostym procesem zaprojektowanym w celu ochrony danych wystarczająco długo, aby klucze szyfrowania były zmieniane w określonych odstępach czasu. Projektanci zaczynają od wyboru odpowiedniego sprawdzonego algorytmu, protokołu i długości klucza, co do których mają pewność, że będą chronić dane użytkownika przez określony czas. Użytkownik (lub program użytkownika) następnie dostarcza ten algorytm z danymi w postaci zwykłego tekstu oraz klucz szyfrujący, a następnie dane są szyfrowane i gotowe do transmisji. Ze względu na szybko rosnącą prędkość przetwarzania (pojedynczych procesorów i procesorów działających równolegle), żaden poziom szyfrowania nie może zapewnić ostatecznej ochrony przez nieograniczony czas - czas wymagany do testowania wszystkich możliwych kluczy w przestrzeni kluczy metodą brute-

force - wymagający potrzeby stworzenia systemu planowania i zarządzania kluczami. . Bezpieczne i powtarzalne ustanawianie wzajemnych kluczy szyfrowania to pojedynczy, najbardziej złożony problem nękający komunikację kryptograficzną między dwiema stronami w fizycznie odseparowanych lokalizacjach. Powtarzalny proces tworzenia kluczy, wzajemnej (i bezpiecznej) wymiany różnych kluczy lub niezależnego wyprowadzania tego samego klucza, a w końcu ich niszczenia, to zarządzanie kluczami. Starsze algorytmy 802.11 nie zapewniały żadnej konkretnej funkcji zarządzania kluczami i producenci musieli sami zaprojektować. Najpopularniejszym systemem we wczesnych samodzielnych punktach dostępowych było ręczne wprowadzanie statycznego klucza WEP o określonej długości do każdego klienta i punktu dostępowego. W przypadku użytkowników domowych system RSN definiuje ręczne wprowadzenie wspólnej zmiennej długości PSK lub hasła w kliencie i punkcie dostępowym. Z tego PSK proces zarządzania kluczami wyprowadza działające klucze kryptograficzne, które są zmieniane dla każdej wiadomości. W przypadku przedsiębiorstw RSN wykorzystuje strukturę 802.1/EAP do ustanowienia bezpiecznego kanału podczas fazy uwierzytelniania użytkownika i urządzenia, umożliwiając skonfigurowanie klucza głównego (PMK) w parach między klientem a punktem dostępowym. Z tego PMK system zarządzania kluczami ustala działające klucze kryptograficzne, które są zmieniane dla każdej wiadomości.

SIEĆ BEZPIECZEŃSTWA IEEE 802.11.

W czerwcu 2004 r. IEEE wydało standard 802.11i w celu poprawy bezpieczeństwa sieci 802.11. Ten nowy system nazywa się Robust Security Network (RSN) i jest przeznaczony zarówno dla użytkowników indywidualnych, jak i korporacyjnych. Użycie korporacyjne opiera się na protokole 802.1X, który zapewnia uwierzytelnianie i ustanawia kontekst bezpieczeństwa. Profil „osobisty" wykorzystuje wstępnie udostępniony klucz (PSK) oparty na haśle dostarczonym dla konsumentów i użytkowników SOHO, którzy nie wymagają niezbędnej infrastruktury uwierzytelniania zaplecza 802.1X. 33.3.1 Funkcje. Podstawowym protokołem RSN jest IEEE 802.1X, który tworzy powiązania RSN (RSNA) z siecią bezprzewodową. RSN zapewnia następujące funkcje:

* Mechanizmy wzajemnego uwierzytelniania. Mechanizmy te mogą uwierzytelniać użytkowników, a także klienta sieciowego lub komputer. AP i serwer uwierzytelniania zaplecza mogą być również uwierzytelniane wobec klienta, pokonując nieuczciwe ataki AP i man-in-the-middle.

* Algorytmy zarządzania kluczami

* Ustanowienie klucza kryptograficznego (poprzez ustanowienie PMK i Pairwise Transient Key [PTK])

* Kody integralności wiadomości kryptograficznych w celu pokonania ataków z przerzucaniem bitów możliwych w oryginalnym standardzie (WEP)

* Dwa protokoły prywatności danych, które również implementują integralność wiadomości:

1. Temporal Key Integrity Protocol (TKIP), który jest opcjonalnym protokołem specjalnie zaprojektowanym, aby można było zaktualizować istniejący sprzęt oparty na WEP, aby go używać.

2. Tryb licznika z protokołem CBC-MAC (CCMP), który jest obowiązkowy dla zgodności z RSNA. Wykorzystuje Advanced Encryption Standard (AES) w trybie licznika dla poufności oraz CBC-MAC dla uwierzytelniania i integralności. CCMP to silny protokół, który został zaprojektowany dla następnej generacji urządzeń bezprzewodowych.

TKIP został zaprojektowany jako tymczasowe rozwiązanie tymczasowe, które będzie działać na istniejącym sprzęcie opartym na WEP, dopóki nowy sprzęt zawierający protokół CCMP nie stanie się powszechny. Podczas gdy TKIP nadal korzystał z istniejącego algorytmu szyfrowania RC4, który był

sercem WEP, CCMP używa algorytmu AES i wymaga mocniejszego sprzętu – obecnie nie stanowi już problemu.

Omówienie 802.1X.

802.1X został pierwotnie zaprojektowany do kontroli dostępu do sieci w oparciu o porty w infrastrukturach IEEE 802LAN. Infrastruktury te obejmują Ethernet, sieć Token Ring i sieci bezprzewodowe. 802.1X uwierzytelnia i autoryzuje urządzenia podłączone do portu LAN i nie pozwoli urządzeniu na dostęp do sieci, jeśli uwierzytelnienie się nie powiedzie.

802.1X definiuje trzy role:

1. Uwierzytelniający. Urządzenie, które uwierzytelnia urządzenie sieciowe przed umożliwieniem mu dostępu do zasobów sieciowych. W sieci 802.11 BSS punkt dostępu jest uwierzytelniaczem.

2. Wnioskodawca. Urządzenie, które chce uzyskać dostęp do zasobów sieciowych i musi zostać uwierzytelnione.

3. Serwer uwierzytelniania (AS). AS przeprowadza faktyczne uwierzytelnienie suplikanta w imieniu uwierzytelniającego. AS można zlokalizować za pomocą wystawcy uwierzytelnienia, ale zwykle jest to system zewnętrzny, taki jak serwer RADIUS.

Standard 802.1X definiuje obiekt Port Access Entity (PAE), który obsługuje algorytmy i protokoły uwierzytelniania w suplikatorze i uwierzytelniaczu. Przegląd architektury 802.1X przedstawiono na Dowodzie 33.2 poniżej. Authenticator ma dwa porty logiczne; pierwszy to niekontrolowany port, który umożliwia dostęp do wymaganych funkcji, takich jak uwierzytelniający PAE. Drugi port to port kontrolowany, który umożliwia dostęp do reszty sieci. Status kontrolowanego portu jest ustalany przez uwierzytelniający PAE i jest zależny od wyniku uwierzytelnienia między suplikantem a serwerem uwierzytelniającym. Komunikaty między suplikantem a wystawcą uwierzytelnienia korzystają ze struktury Extensible Authentication Protocol (EAP) przez LAN (EAPoL) zdefiniowanej w standardzie 802.1X. Komunikacja między uwierzytelniającym a AS wykorzystuje strukturę EAP przenoszoną w protokole wyższej warstwy, takim jak RADIUS.

EAP, EAPoL i PEAP.

802.1X opiera się na protokole EAP11 do przeprowadzania uwierzytelniania suplikanta i wystawcy uwierzytelnienia. Protokół EAP to szereg interfejsów metod, które tworzą strukturę znaną jako EAP. EAP został pierwotnie zaprojektowany do użytku w sieciach modemowych; dlatego specyfikacja 802.1X szczegółowo opisuje rozszerzenie EAP w sieciach Ethernet/Token Ring poprzez rozszerzenie EAPoL (EAP Over LAN)12. Oprócz umieszczania metod EAP w ładunku Ethernet, EAPoL określa szereg dodatkowych funkcji, które pomagają w procesie uwierzytelniania podczas wykrywania i wymiany kluczy. Obecnie istnieje ponad 40 różnych implementacji ram EAP. Podstawowa różnica w implementacjach EAP koncentruje się na sposobie uwierzytelniania suplikanta i osoby uwierzytelniającej. Standardowy protokół EAP nie jest protokołem wzajemnego uwierzytelniania; tylko petent jest uwierzytelniony. To sprawia, że suplikanci są podatni na nieuczciwe ataki AP. Dodatkowo, ze względu na swoją oryginalną konstrukcję dla fizycznych połączeń telefonicznych, EAP nie chroni swoich wiadomości uwierzytelniających przed podsłuchem. Dlatego obecne implementacje EAP/EAPoL ustanawiają bezpieczne tunele, aby zapewnić bezpieczeństwo przed wymianą materiałów uwierzytelniających. Poniżej przedstawiono najczęstsze wdrożenia EAP/EAPoL 802.1X dla przedsiębiorstw uszeregowane według poziomu zapewnianego bezpieczeństwa:

1. EAP-TLS13: Ta implementacja EAP umożliwia tylko wzajemne uwierzytelnianie oparte na certyfikatach za pośrednictwem certyfikatów Transport Layer Security (TLS) X509. Uwierzytelnianie zarówno serwera uwierzytelniającego zaplecza, jak i klienta bezprzewodowego zapewnia wysoki poziom bezpieczeństwa sieci bezprzewodowej, ale wymaga pełnej implementacji infrastruktury klucza publicznego (PKI) w przedsiębiorstwie, aby bezpiecznie dystrybuować i regularnie aktualizować klucze klienta. Problem z EAP-TLS polega na tym, że większość organizacji nie ma niezbędnej infrastruktury PKI do wystawiania certyfikatów TLS klienta suplikantów.

* EAP-TTLS (Tunneled TLS)14: EAP-TTLS jest podobny do EAP-TLS i obsługuje uwierzytelnianie za pomocą certyfikatu wzajemnego, ale nie wymaga certyfikatów po stronie klienta. EAP-TTLS tworzy tunel TLS przed rozpoczęciem jakiegokolwiek procesu uwierzytelniania sieciowego i dlatego może tunelować dowolny mechanizm uwierzytelniania hasła, nawet niezabezpieczone starsze mechanizmy, takie jak PAP.

2. EAP-PEAP (Protected EAP)15: W swojej natywnej formie EAP-PEAP nie obsługuje uwierzytelniania wzajemnego opartego na certyfikatach. Natywny protokół EAP-PEAP używa protokołu TLS tylko do uwierzytelniania serwera katalogowego zaplecza i wykorzystuje oparty na hasłach proces wyzwanie-odpowiedź do uwierzytelniania klienta. Późniejsze rozszerzenia PEAP pomagają złagodzić tę słabość. EAP-PEAP jest natywny dla większości wersji systemu Microsoft Windows i dlatego jest bardzo rozpowszechniony w branży bezprzewodowej. Obecnie istnieją trzy podstawowe typy EAP-PEAP, które zapewniają różne poziomy ochrony:

* EAP-PEAP-MS-CHAP-v2 (Microsoft Challenge Handshake Authentication Protocol: Najpopularniejsza metoda wewnętrznego uwierzytelniania EAP-PEAP wykorzystuje protokół Microsoft CHAP-v2 w celu zapewnienia uwierzytelniania opartego na identyfikatorze użytkownika (identyfikator użytkownika) i hasłach. Proces uwierzytelniania MS-CHAP w przeszłości umożliwiał atakującemu z fizycznym dostępem do punktu dostępowego przechwycenie dostarczonego wyzwania i skrótu odpowiedzi na wyzwanie w postaci zwykłego tekstu. Ze względu na ostatnie postępy w łamaniu nadszedł czas na złamanie skrótu odpowiedzi na wyzwanie MS-CHAP-v2 został skrócony do dni lub mniej i należy go unikać za wszelką cenę, chyba że można ustalić odpowiednie konfiguracje suplikantów klienta.

* EAP-PEAP-TLS18: PEAP-TLS to drugi wewnętrzny protokół PEAP zdefiniowany przez firmę Microsoft. PEAP-TLS tuneluje protokół EAP-TLS w ramach PEAP, aby zapewnić wzajemne uwierzytelnianie oparte na certyfikacie X509.

* EAP-PEAPv1 (EAP-GTC): Trzecia implementacja została zdefiniowana przez firmę Cisco i umożliwia uwierzytelnianie za pomocą ogólnych kart tokenów, takich jak token SecurID firmy RSA, a także identyfikatora użytkownika i hasła.

3. EAP-LEAP19: zastrzeżony protokół opracowany przez firmę Cisco, który przeprowadza uwierzytelnianie na podstawie nazwy użytkownika/hasła w trybie wyzwania-odpowiedź MS-CHAP-v2 w postaci zwykłego tekstu. Atakujący atakujący sieć wykorzystującą EAP-LEAP musi jedynie monitorować ruch, aby przechwycić skróty odpowiedzi na wyzwanie w celu ataku słownikowego offline. Jest to w przeciwieństwie do EAP-PEAP-MS-CHAP-v2, który wymaga nieuczciwego maskarady AP, aby atakujący mógł przechwycić skróty odpowiedzi na wyzwanie MS-CHAP-v2.

4. EAP-FAST20: (Flexible Authentication via Secure Tunneling) został opracowany przez Cisco jako zamiennik podatnego protokołu LEAP. EAP-FAST wprowadził bezpieczne tunele uwierzytelniania wstępnego bez używania certyfikatów. EAP-FAST ma bezpieczne możliwości wzajemnego uwierzytelniania, ale ma również opcję automatycznego przydzielania PAC, która jest podatna na ataki typu man-in-the-middle.

Niezabezpieczone starsze protokoły EAP.

Kiedy EAP został po raz pierwszy zintegrowany z 802.11, powszechnie używane były protokoły EAP-MD5 i Cisco EAP-LEAP. Niestety okazały się one podatne na ataki, co przyspieszyło rozwój bezpiecznych protokołów opisanych powyżej. EAP-MD5 i EAP-LEAP nie powinny być używane do wdrażania sieci bezprzewodowej w przedsiębiorstwie.

Szczegółowa procedura EAP/EAPoL.

Przepływ zarządzania skojarzeniami zabezpieczeń wysokiego poziomu RSN. Składa się z pięciu etapów, które:

1. Ustanawiają bezpieczny kanał między serwerem uwierzytelniającym a serwerem uwierzytelniającym

2. Lokalizują sieć, negocjują algorytmy kryptograficzne i powiąż z nią

3. Zapewniają uwierzytelnianie 802.1X na serwerze uwierzytelniającym

4. Zapewniają wzajemne uwierzytelnianie i utwórz para kluczy kryptograficznych

5. Ustanawiają klucze kryptograficzne grupy/multiemisji

Poniższe sekcje opisują te etapy. Istnieją dwa aspekty, które różnią przepływ skojarzeń zabezpieczeń. Pierwszym z nich jest to, czy sieć bezprzewodowa zawiera punkt dostępowy (podstawowy zestaw usług lub BSS) lub czy jest to niezależny BSS (IBSS), znany również jako sieć ad-hoc, która jest topologią sieci peer-to-peer. Druga dotyczy tego, czy główny klucz kryptograficzny jest globalnym kluczem PSK, czy też został ustanowiony podczas protokołu uwierzytelniania 802.1X.

Etap 1: Ustanowienie bezpiecznego kanału między programem uwierzytelniającym a serwerem uwierzytelniającym

Na tym etapie strona uwierzytelniająca i AS wzajemnie się uwierzytelniają i ustanawiają między sobą bezpieczny kanał przy użyciu protokołu takiego jak RADIUS, IP Security (IPSec) lub TLS. Ten kanał jest używany do bezpiecznego przeprowadzania wymiany uwierzytelniania między suplikantem a AS. Ten etap nie jest wymagany, jeśli sieć korzysta z PSK.

Etap 2: Lokalizowanie sieci i kojarzenie z nią

Ten etap to głównie oryginalna funkcjonalność 802.11 do lokalizowania, uwierzytelniania i kojarzenia z siecią bezprzewodową. Kluczową różnicą w RSN jest to, że ramki nawigacyjne, odpowiedzi sondy i żądania asocjacji zawierają elementy informacyjne, które wskazują:

obsługiwane i dostępne protokoły uwierzytelniania i prywatności. Ponadto szybki protokół przejścia BSS zdefiniowany w 802.11r22 ponownie ulepszył te ramki, aby przyspieszyć roaming AP.

Etap 3-802.1X Uwierzytelnianie na serwerze uwierzytelniania

Celem tego etapu jest wzajemne uwierzytelnienie suplikanta i AS względem siebie oraz niezależne wygenerowanie PMK do wykorzystania w etapie 4. Do tego celu służy opisany powyżej EAP. Komunikaty wymieniane między suplikantem a AS są definiowane metodą EAP. Przegląd tego etapu znajduje się w Dowodzie 33.4. W przypadku sieci BSS klientem bezprzewodowym jest suplikant 802.1X, a punktem uwierzytelniającym jest punkt dostępowy. Punkt dostępowy przekazuje komunikaty uwierzytelniające między suplikantem a serwerem uwierzytelniającym, który może być oddzielną usługą lub wbudowaną. W przypadku IBSS klient chcący powiązać się z innym klientem jest suplikantem, a klient docelowy jest uwierzytelniającym. Oznacza to, że klienci w IBSS mogą

jednocześnie być suplikantami i uwierzytelniającymi, w zależności od tego, kto zainicjował powiązanie. Dodatkowo każdy klient IBSS będzie potrzebował serwera uwierzytelniania, chyba że sieć korzysta z PSK. Jak opisano w etapie 1, przed tą wymianą należy ustanowić bezpieczny kanał między serwerem uwierzytelniającym a serwerem uwierzytelniającym; służy to dwóm celom. Pierwszym jest ochrona integralności i autentyczności wymiany uwierzytelniania, drugim jest umożliwienie AS bezpiecznego wysyłania PMK do uwierzytelniania po zakończeniu uwierzytelniania.

Etap 4 - wzajemne uwierzytelnianie i ustanowienie parami kluczy roboczych

Etap 3 ustanowił PMK zarówno po stronie wnioskującego, jak i uwierzytelniającego. Jeśli sieć używa klucza wstępnego (PSK), to PSK jest PMK. Ten etap nosi nazwę 4-way handshake i ma następujące cele:

1. Wzajemne uwierzytelnienie petenta i osoby uwierzytelniającej względem siebie poprzez potwierdzenie, że obaj mają ten sam ważny PMK.

2. Aby wygenerować klucz przejściowy parami (PTK) z PMK i świeżych kluczy tymczasowych powiązanych z ich adresami MAC.

3. Aby zsynchronizować instalację kluczy w obu urządzeniach.

Czterostronne uzgadnianie jest realizowane za pomocą komunikatów klucza EAPoL wymienianych między suplikantem a uwierzytelniającym i składa się z następujących elementów.

1. Uwierzytelniający i suplikant generują jednorazową wartość jednorazową do wykorzystania w protokole uwierzytelniania. Nonce uwierzytelniającego nazywa się ANOnce, a nonce wnioskującego nazywa się SNonce.

2. Uwierzytelniający wysyła wiadomość EAPoL-Key zawierającą Anonce (Wiadomość 1).

3. Wnioskodawca wyprowadza PTK za pomocą ANOnce i SNonce i oblicza klucz szyfrujący EAPoL-Key (KEK) i EAPoL-Key Message Integrity Code (MIC).

4. Wnioskodawca wysyła wiadomość EAPoL-Key zawierającą SNonce i MIC obliczony przy użyciu klucza EAPoL MIC (Wiadomość 2).

5. Uwierzytelniający może teraz uzyskać PTK, ponieważ ma zarówno ANOnce, jak i SNonce. Następnie oblicza klucz EAPoL-Key KEK i EAPoL-Key MIC Key i weryfikuje MIC w komunikacie 2.

6. Uwierzytelniający wysyła wiadomość zawierającą ANonce oraz flagę nakazującą suplikantowi instalację klucza. Wiadomość jest również uwierzytelniana przez MIC (komunikat 3).

7. Suplikant weryfikuje MIC i wysyła wiadomość do autoryzacji potwierdzającą instalację klucza. Ta wiadomość jest uwierzytelniana przez MIC i szyfrowana przy użyciu klucza EAPoL-KEK (komunikat 4).

8. Autoryzator instaluje nowe klucze i rozpoczyna ostatni etap ustanawiania kluczy grupowych.

Etap 5 - tworzenie grupowych/multiemisji kluczy kryptograficznych

W etapie 4 ustalono klucze PTK i czasowe. Klucze te służą do zabezpieczenia dodatkowej pary komunikatów, w której strona uwierzytelniająca wysyła do klienta zaszyfrowany klucz czasowy grupy (GTK). Klucze grupowe służą do zabezpieczania komunikatów rozgłoszeniowych, takich jak żądania ARP i ruch multiemisji. W sieci BSS wszyscy klienci mają ten sam klucz grupy/multiemisji, który jest wysyłany do każdego klienta przez punkt dostępowy. Jednak w przypadku sieci IBSS nie ma punktu dostępowego, który mógłby ustawić wspólny klucz, więc każdy klient ma swój własny klucz transmisji

grupowej, który wysyła do wszystkich klientów w IBSS. Osiąga się to poprzez wykonanie 4-way handshake i group key handshake w obu kierunkach.

Hierarchia i zarządzanie kluczami RSN.

System zarządzania kluczami wyprowadza klucze robocze (czasowe) z głównego klucza głównego. Dokładna hierarchia kluczy różni się nieco między TKIP i CCMP, ale zasadniczo jest zgodna z tym samym systemem. W tej sekcji opisano system zarządzania kluczami i zwrócono uwagę na różnice między protokołami TKIP i CCMP. Istnieją dwie hierarchie kluczy: pierwsza zawiera klucze parami, które są współdzielone między dwoma urządzeniami bezprzewodowymi (np. między dwoma klientami w IBSS lub między klientem a punktem dostępowym w BSS). Druga hierarchia to klucze grup/multiemisji, które są używane do transmisji sieciowych, takich jak żądania ARP lub ruch multiemisji.

Hierarchia kluczy parami.

W hierarchii kluczy parami istnieją maksymalnie cztery poziomy kluczy kryptograficznych.

1. Klucze uwierzytelniania 802.1X. Te klucze istnieją tylko wtedy, gdy suplikant i serwer uwierzytelniania wzajemnie uwierzytelniają się przy użyciu preinstalowanych kluczy. Przykładem jest EAP-TLS, który wymaga, aby zarówno suplikant, jak i serwer uwierzytelniania miały poświadczenia PKI. Klucze 802.1X służą do ustanowienia klucza głównego parami (PMK).

2. Klucz główny w parach. PMK ma 256 bitów i jest kluczem ustanowionym na poziomie 1 lub PSK zainstalowanym w urządzeniach. PMK, adresy MAC urządzeń i identyfikatory jednorazowe są wprowadzane do funkcji pseudolosowej o zmiennej długości (PRF) w celu wygenerowania klucza przejściowego parami (PTK). Wartość jednorazowa pochodzi z 256-bitowego licznika kluczy, który jest inicjowany podczas uruchamiania systemu na podstawie losowej liczby, czasu i adresu MAC. Wartość jednorazowa jest następnie zwiększana za każdym razem, gdy zmieniany jest klucz.

3. Klucz przejściowy w parach. PTK różni się długością od 128 bitów do 512 bitów i jest dzielony na wymagane klucze czasowe. Długości i liczba kluczy zależą od algorytmu. W przypadku TKIP PTK ma 512 bitów i jest podzielony na 5 kluczy czasowych. W przypadku CCMP PTK ma 384 bity i jest podzielony na 3 klucze czasowe.

4. Klucze czasowe i pakietowe. Klucze czasowe są mieszane ze zmiennymi danymi, takimi jak liczniki pakietów, co skutkuje utworzeniem nowego klucza dla każdego pakietu. Zobacz Załączniki 33.6 i 33.7, aby zapoznać się z opisem kluczy czasowych TKIP i CCMP.

Hierarchia grupy kluczy.

Hierarchia kluczy grupowych ma podobną strukturę do hierarchii kluczy parami. Uwierzytelniający tworzy klucz główny grupy. Ten klucz główny, adres MAC strony uwierzytelniającej i identyfikator jednorazowy grupy (GNonce) są przetwarzane przez PRF w celu utworzenia klucza przejściowego grupy (GTK), który jest następnie dzielony na klucze czasowe.

Protokół integralności klucza tymczasowego (TKIP).

Protokół Temporal Key Integrity Protocol (TKIP) to zestaw algorytmów do rozwiązywania znanych problemów z zarządzaniem kluczami w WEP dla istniejącego już sprzętu 802.11. Mechanizm zarządzania kluczami nigdy nie został konkretnie zidentyfikowany w protokole WEP, do którego adresowania zaprojektowano TKIP. Aby zapewnić kompatybilność z istniejącą bazą produktów bezprzewodowych, firma TKIP musiała uwzględnić architekturę sprzętową istniejących produktów bezprzewodowych. Produkty bezprzewodowe mają dwa procesory; pierwszy znajduje się w chipie

MAC, który implementuje protokół bezprzewodowy, drugi to procesor hosta. W przypadku punktów dostępowych procesor hosta jest dedykowanym procesorem, który obsługuje punkt dostępowy. W przypadku bezprzewodowych kart PC w sieci LAN procesorem hosta jest procesor komputera hosta. Ze względu na wydajność większość chipów MAC ma sprzętowy silnik szyfrowania RC4 do wykonywania szyfrowania. Aby uniknąć niedopuszczalnego wpływu na wydajność poprzez przeniesienie szyfrowania do procesora hosta, TKIP musiał użyć istniejącego mechanizmu szyfrowania MAC. Wymagało to od TKIP dalszego korzystania z RC4 i WEP, ale w sposób umożliwiający przezwyciężenie zidentyfikowanych problemów. Projektanci wymyślili rozwiązanie problemów, w wyniku czego powstał TKIP o następującej funkcjonalności:

* Każda jednostka danych usługi MAC (MSDU) jest uwierzytelniana i chroniona integralność za pomocą kryptograficznego MIC z kluczem. MSDU to komunikat do wysłania do innego klienta. Jednostka MSDU może być podzielona na więcej niż jedną jednostkę danych protokołu MAC (MPDU), które są pakietami/ramkami wysyłanymi przez warstwę fizyczną. Kiedy wszystkie jednostki MPDU zostaną odebrane, odbiorca rekonstruuje jednostkę MSDU i przekazuje ją do stosu protokołów. W obliczeniach MIC uwzględniane są adresy źródłowe i docelowe, a także tekst jawny MSDU. Zapobiega to fałszerstwom i atakom polegającym na maskaradzie.

* Jednak siła MIC jest ograniczona i może być zagrożona metodą prób i błędów. Aby rozwiązać ten problem, TKIP zapewnia opcjonalne środki zaradcze, które przerywają komunikację na pewien czas (60 sekund) po odebraniu nieprawidłowego MIC, a następnie natychmiast wymuszają ponowne nadanie klucza wszystkim klientom. Projektanci oszacowali, że MIC ze środkami zaradczymi będzie odporny na atak przez około rok, zanim atakujący poprawnie odgadnie MIC.

* Każdy TKIP MPDU (pakiet) ma numer sekwencji zakodowany w wektorze inicjującym WEP. Wszelkie jednostki MPDU, które dotrą w złej kolejności, są usuwane.

* TKIP łączy klucz czasowy, adres nadajnika i licznik sekwencji w protokole dwufazowym, tworząc zarodek RC4WEP. Mieszanie odbywa się w taki sposób, aby pokonać słabe ataki.

* RSNA używa komunikatu klucza 802.1X EAPoL do regularnej zmiany kluczy tymczasowych, aby strumienie kluczy RC4 nie były ponownie używane. Zmiana klucza jest wyzwalana automatycznie, gdy licznik sekwencji jest bliski wyczerpania.

Te mechanizmy kontrolne w dużej mierze rozwiązują problemy zidentyfikowane w starszym systemie, wprowadzając uwierzytelnianie kryptograficzne wiadomości, zapobiegając ponownemu wykorzystaniu strumienia klucza i nigdy nie używając słabego IV. Jednak TKIP nadal nie jest uważany za silne rozwiązanie ze względu na siłę MIC. Protokół TKIP powinien być stosowany wyłącznie jako środek tymczasowy do czasu, gdy istniejący sprzęt będzie można zastąpić sprzętem zgodnym z CCMP. Dowody 33.9 i 33.10 przedstawiają proces TKIP w klientach nadawczych i odbiorczych.

Protokół trybu licznika/CBC-MAC (CCMP).

CCMP to obowiązkowy protokół zdefiniowany w RSN w celu zapewnienia poufności, uwierzytelniania, integralności i ochrony odtwarzania dla następnej generacji urządzeń bezprzewodowych. Nie jest możliwe uaktualnienie istniejącego sprzętu do korzystania z tego protokołu ze względu na wymagania dotyczące zasobów sprzętu, który implementuje AES. CCMP używa szyfrowania AES w trybie licznika, aby zapewnić poufność i CBCMAC (AES-CCM) do uwierzytelniania i integralności wiadomości. Dane wejściowe do algorytmu obejmują:

* 128-bitowy klucz szyfrowania blokowego (klucz tymczasowy).

* Wartość jednorazowa oparta na rosnącej liczbie pakietów, która jest używana tylko raz z kluczem szyfrowania do zaszyfrowania wiadomości. Ponowne użycie jednokrotności do zaszyfrowania więcej niż jednej wiadomości niszczy jej właściwości bezpieczeństwa.

* Wiadomość do zaszyfrowania.

* Dodatkowe dane do uwierzytelnienia, ale nie zaszyfrowane, takie jak nagłówek pakietu zawierający źródłowy i docelowy adres MAC.

Szybki bezpieczny roaming.

Po zapoznaniu się z systemem uwierzytelniania RSN, czytelnik może być zaskoczony złożonością systemu i liczbą wiadomości wymaganych do ustanowienia połączenia z siecią. W scenariuszu korporacyjnym wykorzystującym strukturę 802.1X/EAP, roaming między punktami dostępowymi może potrwać do jednej sekundy. Stwarza to problemy z użytecznością aplikacji, w których liczy się czas, takich jak telefon komórkowy. RSN zawiera protokoły buforowania i wstępnego uwierzytelniania PMK, aby spróbować rozwiązać ten problem; jednak oba protokoły mają ograniczenia. Buforowanie PMK polega na tym, że klient i punkty dostępowe pamiętają klucze, których używali ze sobą, gdy klient oddala się. Jest to jednak przydatne tylko w przypadku roamingu z powrotem do punktów dostępowych, z których wędrowałeś. Wstępne uwierzytelnianie rozwiązuje ten problem, przeprowadzając uwierzytelnianie 802.1X i ustanawiając klucze z punktami dostępowymi, gdy się na nie natkną, nawet jeśli klient nigdy nie korzysta z roamingu do tego punktu dostępowego. Powoduje to znaczny niepotrzebny ruch związany z uwierzytelnianiem, który może przeciążyć serwer uwierzytelniający. Komitet 802.11 postanowił ponownie przyjrzeć się problemowi i opracował Standard 802.11r, który rozszerzył buforowanie RSN PMK w celu ustanowienia buforowanego PMK z centralnym kontrolerem, który następnie w razie potrzeby dystrybuuje wariant PMK do punktów dostępowych. Protokół ten nosi nazwę Opportunistic Key Caching (OKC) i oznacza, że długie uwierzytelnianie 802.1X nie jest już wymagane, co skraca czas roamingu do około 100 milisekund. 802.11r rozszerzył również komunikaty uwierzytelniania i asocjacji o parametry OKC, oszczędzając potrzebę dodatkowych par komunikatów.

PODSTAWOWE ZAGROŻENIA BEZPRZEWODOWE.

Ważne jest, aby przedsiębiorstwo było przygotowane do zarządzania wieloma podstawowymi zagrożeniami, które są możliwe dzięki istnieniu bezprzewodowego medium. Ponieważ przedsiębiorstwo analizuje swoją infrastrukturę i potrzeby jako całość, nieodłącznym elementem jest nieuwzględnianie zwiększonego narażenia na zagrożenia spowodowanego eliminacją kontroli warstwy fizycznej. Tego typu kontrole są zwykle przyjmowane za pewnik i nie są brane pod uwagę pomimo zmiany na całkowicie nowy nośnik fizyczny. Ważne jest, aby zrozumieć fundamentalne różnice między medium przewodowym i bezprzewodowym oraz być przygotowanym do podjęcia działań poprzez wdrożenie niezbędnych kontroli w celu zabezpieczenia sieci bezprzewodowej do poziomu odpowiadającego przewodowej sieci LAN. Wdrożenie sieci bezprzewodowej zwiększa dostępność sieci poza ściany obiektu, a nawet parkingi. Często zdarza się, że przeciwnicy siedzą na parkingu firmowym i używają specjalnych anten (zwanych kantenami) do podsłuchiwania komunikacji bezprzewodowej z bezpiecznej odległości. Sieci bezprzewodowe opierają się przede wszystkim na logicznych elementach sterujących, które występują w warstwie łącza danych i powyżej w formie uwierzytelniania i szyfrowania, aby zrekompensować zasadniczo publiczną dostępność medium. Kierując się łatwością dostępu do komunikacji bezprzewodowej, model zagrożeń, przed którymi stoi organizacja z powodu istnienia i korzystania z sieci bezprzewodowej, może ulec zmianie w miarę eliminacji wcześniejszych zagrożeń (takich jak nieautoryzowane użycie gniazd sieciowych) i tworzenia innych. Coraz bardziej złożony krajobraz zagrożeń i obowiązki związane z monitorowaniem bezpieczeństwa mogą wpłynąć na

decyzję przedsiębiorstwa o wdrożeniu rozwiązania bezprzewodowego do określonego zastosowania lub o ograniczeniu jego zakresu do wyznaczonych zastosowań funkcjonalnych. . W tej sekcji omówimy podstawowe zagrożenia związane z korzystaniem z sieci bezprzewodowej i przyjrzymy się bliżej podzbiorowi konkretnych zagrożeń technicznych, które powinny być priorytetem dla przedsiębiorstwa. Nie jest konieczne, aby przedsiębiorstwo rozumiało każde zagrożenie, z jakim może się spotkać, ale konieczne jest uznanie ich obecności i podjęcie praktycznych kroków w celu przeciwdziałania tym zagrożeniom.

Nieautoryzowane rozszerzenia sieci.

Podczas przechodzenia do środowiska bezprzewodowego z sieci przewodowej lub połączenia tych dwóch zagrożeń, które w przeszłości wydawało się łatwe do zidentyfikowania, coraz trudniej jest teraz zarządzać. Ze względu na nieodłączny brak przejrzystości w regulowanych i nieuregulowanych falach radiowych, możliwe jest, że nieautoryzowany punkt dostępu (AP) ukryje się wśród autoryzowanych punktów dostępu poprzez fałszowanie SSID. W środowisku przewodowym trudniej jest ukryć nieautoryzowane urządzenie ze względu na wygląd fizyczny. Zdolność przedsiębiorstwa do zidentyfikowania nieautoryzowanego punktu dostępu będzie wymagać dodatkowych środków kontroli w celu wykonania tej operacji po wdrożeniu autoryzowanego dostępu bezprzewodowego.

Nieuczciwe punkty dostępu.

Arogue AP jest podłączony do sieci bez autoryzacji lub podszywa się pod podłączone urządzenie. Nieuczciwe AP występują w wielu formach:

* Nonmalicious Internal Rogue AP: Ten rodzaj nieuczciwego AP jest często wdrażany przez pracownika lub personel bez złośliwych intencji, ale może być wykorzystany przez atakującego z zewnątrz. Podłączając punkt dostępowy klasy Small Office Home Office (SOHO) do sieci wewnętrznej, można ominąć mechanizmy ochrony klasy korporacyjnej mające na celu powstrzymanie atakujących, takie jak zapory obwodowe, dzięki bezpośredniemu dostępowi do wewnętrznej sieci LAN. Mechanizmy bezpieczeństwa punktów końcowych, takie jak program antywirusowy oparty na hoście i zapory sieciowe, są również unieważniane ze względu na funkcję translacji adresów sieciowych (NAT) routera SOHO. Kontrole bezpieczeństwa klasy konsumenckiej obecne w SOHO AP, w połączeniu z brakiem odpowiedniej konfiguracji zabezpieczeń przez instalatora, mogą prowadzić do udanego kompromisu, co skutkowałoby bezpośrednim dostępem do przewodowej sieci wewnętrznej. Niezłośliwe, nieuczciwe punkty dostępowe można zazwyczaj zidentyfikować za pomocą standardowego identyfikatora SSID, takiego jak „Linksys” lub „netgear”.

* Atakujący Złośliwy wewnętrzny nieuczciwy punkt dostępu: Atakujący może zamaskować punkt dostępu jako legalny korporacyjny punkt dostępu, używając tego samego identyfikatora SSID, co autoryzowane punkty dostępu przedsiębiorstwa. W tej sytuacji niczego niepodejrzewający klient punktu końcowego automatycznie połączy się z dowolnym punktem dostępowym, który rozgłasza żądany identyfikator SSID (np. „employeeWireless”) i wybierze punkt dostępowy z najsilniejszym sygnałem. Atakujący może następnie przeprowadzić ataki typu „odmowa usługi”, aby zmusić klientów do korzystania ze złośliwego punktu dostępu. Złośliwy, nieuczciwy punkt dostępowy z dostępem wewnętrznym może zostać wykorzystany przez atakującego z fizycznym dostępem do obiektu do przechwycenia poświadczeń lub innych danych od niczego niepodejrzewających klientów punktów końcowych, którzy wykorzystują punkt dostępowy do uzyskania dostępu do zasobów wewnętrznych, takich jak panele administracyjne lub portale pracowników. Atakujący z wewnętrznie podłączonym punktem dostępowym ma wiele zalet, ponieważ jest w stanie bezproblemowo umożliwić użytkownikowi dostęp do wszystkich regularnie dostępnych zasobów. Ten rodzaj ataku wymagałby fizycznego dostępu do obiektu i odpowiednich gniazd sieciowych.

* Atakujący Złośliwy zewnętrzny nieuczciwy punkt dostępowy: Zewnętrzny nieuczciwy punkt dostępowy używa podobnej taktyki do wewnętrznego nieuczciwego punktu dostępowego, aby zmusić niczego niepodejrzewających klientów punktów końcowych do połączenia się z nim. Podstawową różnicą jest fizyczna bliskość punktu dostępowego i sieci, do której zapewnia dostęp. Atakującemu znacznie łatwiej jest wdrożyć zewnętrzny, nieuczciwy punkt dostępowy na pobliskim parkingu firmowym, niż uzyskać dostęp do obiektu i zainstalować wewnętrznie podłączony punkt dostępowy. Wadą zewnętrznego nieuczciwego punktu dostępowego jest brak możliwości dostarczenia żądanych zasobów wewnętrznych do podłączonego klienta. Jeśli pożądanym zasobem jest Internet, można to zapewnić poprzez proces przekazywania, który umożliwia atakującemu przeglądanie całego ruchu.

Oba typy złośliwych punktów dostępu umożliwiają atakującemu przechwytywanie wrażliwego ruchu sieciowego i atakowanie samego punktu końcowego, próbując wykorzystać luki w systemie operacyjnym punktu końcowego lub usługach sieciowych. Konfiguracje klientów zazwyczaj wymagają, aby bezprzewodowe radio klienta łączyło się z najsilniejszym sygnałem, który odpowiada wymaganiom SSID i uwierzytelniania; np. WPA/WPA2-PSK, WPA/WPA2-Korporacyjne (EAP-PEAP, EAP-TLS).

Zagrożenia powodowane przez nieuczciwe punkty dostępowe obejmują:

* Uzyskiwanie przez atakującego dostępu do sieci przewodowej poprzez złamanie słabych lub brak kontroli bezpieczeństwa w nieuczciwym, zainstalowanym przez pracowników, nieuczciwym punkcie dostępowym

* Pozyskiwanie przez atakującego poufnych danych poprzez przechwytywanie sieciowe klientów podłączonych do nieuczciwego punktu dostępowego dostarczonego przez atakującego (takich jak dane uwierzytelniające domeny). Zagrożenie to jest zwykle bardziej skuteczne, jeśli jest używane w połączeniu z taktykami socjotechniki, takimi jak wstrzykiwanie ramek IFRAMES w ruchu HTTP, który kieruje ich do złośliwej witryny, która zawiera exploity przeglądarki dla różnych wtyczek, takich jak ActiveX lub Adobe.

*Uzyskiwanie dostępu przez atakującego i testowanie penetracji korporacyjnych punktów końcowych połączonych z nieuczciwym punktem dostępowym dostarczonym przez atakującego w innej fizycznej lokalizacji.

* Użytkownicy wewnętrzni omijają konfiguracje przewodowych zabezpieczeń portu 802.1X za pomocą NAT, co pozwala wielu użytkownikom komunikować się przez port WAN zainstalowanego SOHO AP

Ataki warstwy 1.

Pracownicy lub aplikacje biznesowe mogą w dużym stopniu polegać na mediach bezprzewodowych w celu zapewnienia łączności z zasobami sieci przewodowej w lokalizacjach, w których trudno jest wdrożyć łączność fizyczną. Brak zamkniętego prywatnego nośnika fizycznego pozwala na manipulowanie bezprzewodowym sygnałem nośnym warstwy 1 niezależnie od kontroli ochronnych górnej warstwy. Jest to fundamentalne zagrożenie dla jakiejkolwiek formy komunikacji bezprzewodowej, niekoniecznie specyficzne dla 802.11, chociaż każdy protokół bezprzewodowy, taki jak CDMA, 3G lub 802.11, może zawierać mechanizm wykrywania manipulacji, ale nie mogą one zapobiec jego wystąpieniu.

* Protokół 802.11 działa w paśmie 2,4 GHz. Pasmo konsumenckie 2,4 GHz może zostać zakłócone przez użycie czegoś tak prostego jak kuchenka mikrofalowa

- Widmo 2,4 GHz zapewnia tylko trzy nienakładające się kanały. Widmo 802.11 działa w zakresie od 2,412 GHz do 2,462 GHz. Kanały nakładające się są kanałami obok siebie, które poprzez propagację i

inne tendencje bezprzewodowe mogą przenikać do sąsiedniego przydziału pasma 20 MHz. Pobliski punkt dostępu może spowodować drobną odmowę usługi, używając nakładający się kanał.

* Podszywanie się pod ramkę zarządzania

- Ramki zarządzania 802.11 są częścią warstwy MAC protokołu 802.11. Ramki zarządzania służą do uruchamiania uwierzytelniania i kojarzenia klientów z punktem dostępowym. Ramki zarządzania „zarządzają" połączeniem między punktem dostępowym a wszystkimi podłączonymi klientami. Istnieją różne typy ramek zarządzania, z których niektóre są odbierane przez dowolnego klienta w zasięgu AP, a inne są skierowane do podłączonych/połączonych klientów.

Najważniejsze typy ram zarządzania:

* Prośba/odpowiedź sondy

* Uwierzytelnianie

* Prośba o powiązanie

* Odpowiedź stowarzyszenia

* Dysocjacja

Podobnie jak w przypadku przewodowej sieci LAN, nieuwierzytelniony charakter początkowych protokołów warstwy łącza danych, takich jak ramki zarządzania 802.11, może umożliwić atakującemu fałszowanie i ingerowanie w istniejącą sesję lub proces inicjacji sesji. Ta fundamentalna kwestia jest porównywalna z nieuwierzytelnionym protokołem Ethernet → IP ARP, wciąż podatnym na ataki w standardzie 802.11, ale łatwo nadużywanym przez połączenie przewodowe. Bezpieczeństwo zapewniane przewodowym protokołom ładowania początkowego opiera się na ich fizycznych kontrolach, z których żadna nie jest dostępna w trybie bezprzewodowym. Ta pustka skłoniła rodzinę standardów IEEE 802.11 do przyjęcia specyfikacji 802.11w. Ta specyfikacja szczegółowo opisuje użycie kodów MIC do uwierzytelniania ramek zarządzania w ich źródle. To skutecznie wyeliminowałoby możliwość nieuwierzytelnionego atakującego zmuszenia klientów do odejścia z legalnego punktu dostępowego na rzecz nieuczciwego punktu dostępowego dostarczonego przez atakującego. 802.11w brzmi świetnie na papierze, ale w rzeczywistości wdrożenie zajmie lata. Proces uwierzytelniania materiału dla każdej ramki zarządzania zwiększa obciążenie już zajętych procesorów punktu dostępu, co oznacza, że aktualizacja oprogramowania może nie być możliwa dla wszystkich urządzeń. Ponadto wszystkie urządzenia klienckie muszą obsługiwać standard 802.11w, aby tworzyć wychodzące i przetwarzać przychodzące dane MIC. Obsługa klienta wymagałaby nowego oprogramowania układowego sterownika dla radiotelefonów bezprzewodowych i potencjalnie większej akceleracji sprzętowej dla potencjalnie wszystkich podłączonych klientów, w zależności od implementacji 802.11w w punkcie dostępowym.

Ataki na punkty końcowe.

Nową klasę ataków na punkty końcowe umożliwiają bezprzewodowe punkty końcowe. Punkty końcowe mogą obejmować wszystko, od laptopa, drukarki bezprzewodowej lub skanery ręczne. W czystym środowisku przewodowym ryzyko naruszenia bezpieczeństwa bezprzewodowego punktu końcowego jest nieznacznie zmniejszone ze względu na brak korporacyjnych materiałów uwierzytelniających do sieci bezprzewodowej przechowywanych w bezprzewodowym suplikatorze punktu końcowego. Materiały uwierzytelniające obejmują takie elementy, jak pary nazwa użytkownika/hasło domeny, certyfikaty, a nawet klucze współdzielone. Przechowywanie materiałów uwierzytelniających na punkcie końcowym oznacza, że „klucze do królestwa" można uzyskać i

wykorzystać do uzyskania dostępu do sieci bez wchodzenia do obiektu. Chociaż możliwość naruszenia przez atakującego punktu końcowego za pomocą ataku typu hotspot, nadal stanowi realne zagrożenie dla integralności punktu końcowego, środki bezpieczeństwa punktu końcowego, takie jak zapory ogniowe oparte na hoście, IDS i regularne łatanie, mogą złagodzić to zagrożenie dla akceptowalnego poziomu. Konieczne jest zrozumienie, że punkt końcowy jest nadal podatny na te same ataki w środowisku bezprzewodowym przedsiębiorstwa, ale wynik tych ataków może skutkować przechwyceniem materiałów uwierzytelniających używanych do uzyskania dostępu do firmy , bezprzewodowy. Przechwytywanie materiałów uwierzytelniających pozwala uniknąć konieczności naruszenia punktu końcowego w celu uzyskania wewnętrznego dostępu do sieci firmowej. Jeśli pracownicy nie korzystają z bezprzewodowego dostępu korporacyjnego, są mniej narażeni na połączone ataki socjotechniczne z atakiem na hotspot. Przykładem takiej sytuacji jest użycie przez atakującego ataku hotspot w celu uzyskania łączności z punktem końcowym, przechwycenie przeglądania Internetu i monitowanie użytkownika o sfałszowaną witrynę firmowego intranetu, która żąda zdalnych poświadczeń VPN za pośrednictwem prostego formularza sieci Web. Ataki na punkty końcowe możliwe dzięki dostępowi bezprzewodowemu w przedsiębiorstwie:

* Identyfikacja pracodawcy poprzez opisowe żądania sondy SSID.

* Zwiększona skuteczność ataków Hotspot + Socjotechnika w oparciu o fakt, że użytkownik regularnie uzyskuje dostęp do sieci bezprzewodowej przedsiębiorstwa, w przeciwieństwie do użytkownika, który nigdy nie miał dostępu bezprzewodowego.

* Personifikacja RADIUS w celu przechwytywania poświadczeń WPA/WPA2-Enterprise EAP.

SPECYFICZNE BEZPRZEWODOWE ATAKI NA BEZPIECZEŃSTWO

Adres MAC i fałszowanie adresów IP.

Mechanizmy kontroli dostępu oparte na adresach MAC są najsłabiej rozwiniętym owocem zagrożeń bezpieczeństwa sieci bezprzewodowej. Ta forma kontroli dostępu nie jest klasy korporacyjnej i pochodzi głównie z punktów dostępowych i hotspotów klasy SOHO do śledzenia autoryzowanych połączeń bez wydawania unikalnego materiału klucza. Uwierzytelnianie czystego adresu MAC opiera się wyłącznie na adresie MAC urządzenia łączącego; jeśli zidentyfikowany adres MAC znajduje się na wstępnie zdefiniowanej liście dozwolonych adresów MAC, urządzenie może się skojarzyć. Oczywiście nie jest to skalowalny sposób uwierzytelniania ze względu na ciągłe aktualizacje w przypadku mapowań statycznych i jest powszechnie używany do śledzenia prawidłowych połączeń klientów po wstępnym uwierzytelnieniu opartym na sieci Web. Ten typ sytuacji jest powszechnie określany jako portal przechwytujący lub uwierzytelnianie oparte na hotspotach. Punkt dostępowy działa w trybie otwartego uwierzytelniania, pozwalając każdemu się z nim połączyć, ale użytkownicy, którzy jeszcze się nie uwierzytelnili, nie mogą uzyskać dostępu do Internetu i są wrzucani do ograniczonej kary. Użytkownicy są proszeni za pomocą interfejsu internetowego o wprowadzenie poświadczeń, a po pomyślnym uwierzytelnieniu sieciowym uzyskują dostęp do Internetu lub innych chronionych zasobów. Uwierzytelnianie Captive Portal odbywa się w warstwie 4 (aplikacja) i opiera się na warstwie 3 (adres IP) i warstwie 2 (adres MAC) jako niezawodnych mechanizmach śledzenia użytkowników, którzy pomyślnie zostali uwierzytelnieni. Atak ten umożliwia fakt, że cały ruch w systemie Captive Portal jest przesyłany w postaci niezaszyfrowanej. Nie jest konieczne szyfrowanie, aby umożliwić klientom dostęp do strony uwierzytelniania opartego na sieci Web bez wcześniej ustalonych kluczy szyfrowania lub wcześniejszej znajomości punktu dostępowego. Atakujący ma teraz możliwość przechwytywania ruchu w postaci zwykłego tekstu występującego w punkcie dostępu do i od każdego klienta. Odbywa się to poprzez ustawienie kompatybilnej karty bezprzewodowej w tryb monitora. Tryb monitorowania pozwala atakującemu zobaczyć cały ruch na określonym kanale 802.11 bez

konieczności łączenia się z punktem dostępowym. W sieciach bezprzewodowych, które wykorzystują mechanizm szyfrowania, taki jak WPA/WPA2-Enterprise, osoba atakująca nie zobaczy żadnych ładunków w postaci zwykłego tekstu dla ramek 802.11. Atakujący może wykorzystać to do monitorowania ruchu i identyfikowania adresów MAC i adresów IP podłączonych/uwierzytelnionych klientów. Te informacje mogą następnie zostać sfałszowane przez osobę atakującą w celu uzyskania dostępu do zastrzeżonej zawartości portalu (Internetu lub innych zasobów) bez przekierowania przez portal na stronę uwierzytelniania. Uwierzytelnieni klienci są obsługiwani przez punkt dostępowy za pomocą adresu MAC, adresu IP lub kombinacji obu.

(WEP/WPA/WPA-Enterprise) Atak personifikacji RADIUS.

Implementacje bezprzewodowe, które wykorzystują RSN z klientami, które nie zostały skonfigurowane do ufania określonemu typowi punktu dostępowego i nie wykorzystują wzajemnego uwierzytelniania klienta opartego na certyfikatach, są z natury podatne na śmiertelną kombinację fałszywego punktu dostępowego i serwera uwierzytelniania (np. RADIUS). Atak ten opiera się na zdolności osoby atakującej do wymuszenia na klientach połączenia się ze złośliwym punktem dostępu i rozpoczęcia oczekiwanej metody uwierzytelniania EAP. W typowym wdrożeniu protokołu EAP RSN w odpowiedzi na żądanie uwierzytelnienia serwer RADIUS odeśle wezwanie dostępu RADIUS, które jest przekazywane przez punkt dostępowy do klienta. W tym ataku złośliwy punkt dostępowy jest skonfigurowany do korzystania z dostarczonego przez atakującego serwera RADIUS. Ten serwer RADIUS przeprowadza proces uwierzytelniania EAP i zmusza klienta do podania skrótu hasła w odpowiedzi na ustalone, znane wyzwanie. W zależności od używanej implementacji EAP nazwa użytkownika powiązana z klientem może być podana w postaci zwykłego tekstu w odpowiedzi EAP-Identity-Response wysyłanej przed uwierzytelnianiem wymiany materiałów. Ponieważ atakujący nieuczciwy AP używa stałego wyzwania, mamy teraz możliwość brutalnego wymuszenia hasła przy użyciu standardowych ataków słownikowych. Ten atak dotyczy tylko implementacji EAP, które nie używają certyfikatów klienta do uwierzytelniania, ale wykorzystują kombinacje nazwy użytkownika i hasła, takie jak EAP-PEAP z MSCHAP-v2. Jeśli klient łączy się z fałszywym punktem dostępowym, sfałszowany certyfikat serwera uwierzytelniania prawdopodobnie nie zostanie poprawnie zweryfikowany, a użytkownik albo nic nie zobaczy, albo zostanie poproszony o małą wiadomość. Hash wyzwań/odpowiedzi EAP można przechwycić i złamać za pomocą następujących narzędzi:

* FreeRADIUS WPE (Wireless Pwn Edition): Służy do łatwego wdrażania serwera RADIUS w celu akceptowania połączeń z nieuczciwego AP przy użyciu sfałszowanej wersji oczekiwanego typu EAP.

* AsLEAP: Używany do łamania skrótów EAP (PEAP, LEAP, itp.) wyzwań/odpowiedzi przy użyciu skrótu hasła, znanego wyzwania i słownika słów jako danych wejściowych.

Ramy zarządzania.

Ramki 802.11 przenoszą protokół i dane dla protokołów wyższych warstw. Przede wszystkim powszechnie stosowane są dwa typy ramek 802.11, ramki danych i zarządzania. Ramki danych są używane jako nośniki dla protokołów wyższych warstw, podczas gdy ramki zarządzania przenoszą określone informacje dotyczące operacji łącza. Historycznie, ramki zarządzania są podstawową słabością bezpieczeństwa 802.11. W większości wdrożeń bezprzewodowych ramki zarządzania nigdy nie są zabezpieczone i dlatego są zawsze dostępne pomimo mechanizmów uwierzytelniania lub szyfrowania, które mogą zabezpieczać ładunek zawartości ramki danych. Jak opisano wcześniej w sekcji 4.1, 802.11w próbuje rozwiązać ten problem za pomocą MIC, ale podobnie jak większość ulepszeń bezprzewodowych. branża pozostaje w tyle za pełną adaptacją tych kontroli ze względu na kosztowne aktualizacje klientów i nowe urządzenia AP i/lub aktualizacje oprogramowania układowego. Brak przyjęcia jest prawdopodobnie spowodowany faktem, że fałszowanie ramek zarządzania nie jest łatwo

postrzegane jako bezpośrednie zagrożenie, pomimo jego śmiertelnego wpływu w połączeniu z innymi atakami. Podszywanie się pod ramy zarządzania i manipulowanie nimi umożliwia następujące typy zagrożeń:

* Spoofing ramki Beacon: Pozwala atakującemu na maskowanie się jako dowolny AP. Stworzenie ramki beacon sprawi, że pojawisz się w sieciowym „skanowaniu" dostępnych sieci. Ta luka umożliwia przeprowadzanie ataków podszywania się pod hotspot i RADIUS i jest w dużej mierze nie do powstrzymania ze względu na konieczność akceptacji nieuwierzytelnionych ramek sygnału nawigacyjnego przez dowolnego nieskojarzonego klienta w obrębie zasięgu.

* Uwierzytelnianie/Deauthentication: Te ramki są intensywnie używane przez 802.11 podczas procesu bezpiecznego uwierzytelniania. Używany do przekazywania intencji klienta, aby połączyć się z AP. Nawet w sytuacjach, gdy AP używa „otwartego" uwierzytelniania i nie wymaga materiału klucza, wykonywana jest procedura ramki uwierzytelniania. W przypadku uwierzytelniania z kluczem wstępnym WEP, ramki te są wykorzystywane do przenoszenia ruchu związanego z uwierzytelnianiem sieciowym.

* Skojarzenie/Ponowne skojarzenie/Rozłączenie: Ramki odpowiedzi skojarzeń są używane do synchronizacji radiotelefonów między punktem dostępowym a radiem klienta. Obejmuje to szczegóły, takie jak obsługiwane szybkości transmisji danych. Ten proces umożliwia punktowi dostępowemu przydzielenie pamięci dla klienta i rozpoczęcie przetwarzania komunikacji. Ramki ponownego skojarzenia są używane, gdy klient przemieszcza się do innego punktu dostępowego w obrębie tego samego BSSID, co wskazuje oryginalnemu punktowi dostępowemu, że powinien on przekazać wszystkie pozostałe buforowane ramki. Ramka dysocjacji jest wysyłana przez klienta w celu wdzięcznego usunięcia się z punktu dostępowego i umożliwienia punktowi dostępu bezużyteczne zebranie niezbędnej pamięci.

* Request to Send (RST) i Clear To Send (CST): Ramki RST są opcjonalne i zapewniają sposób na przetrwanie w sytuacji, w której jeden klient nie widzi ruchu innego klienta z powodu fizycznej bliskości punktu dostępowego. Ta ramka jest wysyłana do AP i AP odpowie ramką CTS. Ramka CTS zawiera wąski przedział czasowy, w którym klient może wysłać dane, podczas gdy wszyscy inni połączeni klienci muszą czekać. Ta procedura zmniejsza kolizje z ukrytymi klientami AP.

Manipulowanie ramkami zarządzania odbywa się poprzez wstrzykiwanie ich do fal radiowych i fałszowanie źródła tak, jakby pochodziły z AP BSSID. Ramki te nie są widoczne ze standardowego przechwytywania pakietów w systemie hosta, ponieważ sterownik karty bezprzewodowej nie przekaże tego ruchu do bazowego systemu operacyjnego. Sfałszowanie ramek zarządzania nie wpływa na punkt dostępowy, ponieważ jest on nieświadomy ich obecności.

Następujące narzędzia Aircrack25 mogą być używane z kompatybilną kartą bezprzewodową ustawioną w trybie monitorowania w celu manipulowania ramkami zarządzania26:

* Aireplay-ng -0: fałszowanie deauthentication w celu usunięcia klienta z punktu dostępowego poprzez wysyłanie skojarzonych pakietów do jednego lub większej liczby klientów, którzy są obecnie skojarzeni przez sfałszowanie skojarzonego pakietu ze źródłowym adresem MAC celu.

* Aireplay-ng -1: Fałszywe uwierzytelnianie z AP przy użyciu określonego źródłowego i docelowego adresu MAC poprzez wysyłanie ramek zarządzania asocjacjami.

Ataki Hotspot i Cafe Latte.

W zależności od chipsetu bezprzewodowego i sterownika, klienci bezprzewodowi zazwyczaj aktywnie wyszukują wszystkie sieci, z którymi byli powiązani w przeszłości, a gdy punkt dostępowy odpowiada, automatycznie się z nim kojarzą. Źródło tej luki wynika z zachowania klientów bezprzewodowych i braku uwierzytelniania AP na wczesnych etapach uwierzytelniania. Tylko SSID i typ uwierzytelniania/szyfrowania muszą być zgodne ze stanem „znany", aby klient mógł rozpocząć proces kojarzenia. Z powodu wdrożeń bezprzewodowych cienkich punktów dostępowych klient bezprzewodowy nie może określić ani zapamiętać adresu MAC punktu dostępowego, z którym żąda połączenia, nawet jeśli znacznie ograniczyłoby to ten atak. Klient bezprzewodowy sondujący ostatnio używany identyfikator SSID z publicznego hotspotu Wi-Fi może zostać zidentyfikowany przez atakującego i zamaskowany tak, jakby był publicznym hotspotem Wi-Fi, nawet jeśli ofiara nie znajduje się nigdzie w lokalizacji wcześniej zapamiętanego publicznego hotspotu . Ponieważ większość publicznych hotspotów nie wymaga uwierzytelniania, atakujący może bezpiecznie założyć, że wystarczy dopasować żądany identyfikator SSID i nie ma żadnych innych cech, aby ułatwić udane połączenie docelowej ofiary. Jeśli AP, którego szuka klient, wymaga WEP lub WPA, nie połączy się automatycznie z żadnym AP o tej samej nazwie. Szybkości przesyłania danych i poziomy szyfrowania muszą być zgodne, zgodnie z opisem w procesie kojarzenia. Atakujący węszący w sieci bezprzewodowej w poszukiwaniu żądań sondy SSID niekoniecznie będzie wiedział, które sieci wymagają szyfrowania, a które nie, ale próba i błędy w końcu dostarczą poprawnej odpowiedzi. Poniżej przedstawiono proces związany z podszywaniem się pod hotspot, w którym osoba atakująca rozpoznaje określonego klienta bezprzewodowego, który chciałby połączyć się z punktem dostępowym, który może być obecny lub nie (jest to natura automatycznego łączenia Wi-Fi) i aktywnie podszywa się pod żądanego AP w celu zaspokojenia klienta i uzyskania chwilowej łączności (w przypadku, gdy klient rozłączy się z powodu nieprawidłowego procesu zarządzania kluczami).

Procedura ataku na hotspot

1. Maszyna ofiary wysyła żądania sondy SSID dla punktów dostępowych, z którymi komunikowała się w przeszłości (supplikanci przechowują tę historię, aby umożliwić szybkie połączenia).

2. Atakująca maszyna monitoruje fale radiowe pod kątem sond SSID i odnotowuje żądane nazwy punktów dostępu (np. „coffeeshop", „airportWifi" itp.).

3. Atakująca maszyna tworzy AP o nazwie SSID żądanej przez klienta (np. „kawiarnia", „airportWifi" itp.).

4. Maszyna ofiary automatycznie kojarzy się z nowym punktem dostępowym, a poziomy szyfrowania/uwierzytelniania są dokładne.

W tym momencie atakujący może poprawnie odgadnąć szyfrowanie, którego oczekuje klient (WPA/WPA2/WEP) lub otwarte (brak). Bardzo często system Microsoft Windows i suplikanci innych firm automatycznie łączą się ze znanym punktem dostępowym w tle i nie wyświetlają żadnego ostrzeżenia o połączeniu, z wyjątkiem symbolu „podłączony" na pasku zadań.

5. Ofiara ma teraz funkcjonalne połączenie z punktem dostępowym atakującego, a atakujący może ustanowić ruch typu „man-in-the-middle" (MITM), przekazując go do legalnego punktu dostępowego na sąsiednim interfejsie lub w Internecie, lub zaatakować ofiarę, wykorzystując luki w podłączonym systemie.

Starsze, ale cenne rozszerzenie tego ataku dotyczy identyfikatora SSID, który jest nadawany przez „zaparkowaną" kartę bezprzewodową i jest powszechny w starszych sterownikach bezprzewodowych systemu Windows. Podczas konfiguracji zerowej sieci bezprzewodowej w systemie Windows karta

bezprzewodowa będzie próbowała połączyć się ze wszystkimi wcześniej znanymi sieciami, zanim przejdzie w stan „zaparkowania". Warunek „zaparkowany" polega na tym, że adapter zaprzestaje próbowania połączeń i używa dynamicznie generowanego identyfikatora SSID jako wartości domyślnej. Po przypisaniu tej wartości domyślnej karta bezprzewodowa nie będzie już aktywnie wyszukiwać sieci, ale będzie kontynuować normalne zachowanie sygnału nawigacyjnego, tym razem z zaparkowanym identyfikatorem SSID. To zachowanie wprowadziło nową lukę, dzięki której osoba atakująca może zawsze mieć identyfikator SSID, na którym może polegać, nawet jeśli klient nie ma żadnych poprzednich sieci, których mógłby szukać. Ta luka została od tego czasu rozwiązana poprzez ustawienie poziomu szyfrowania (WPA/WPA2) i losowego klucza do użycia przez kartę bezprzewodową w trybie parkowania

Współczynnik WEP Cafe-Latte.

Dodatkowy zwrot w fałszowaniu hotspotów idzie o krok dalej, aktywnie atakując klienta, który emituje określony identyfikator SSID z sieci, która wdraża szyfrowanie WEP. Ten atak wykorzystuje wiele Luk WEP umożliwiające złamanie klucza WEP przekazanego przez klienta. Wszyscy klienci będą przechowywać klucz WEP w ramach suplikanta lub jakiegoś rodzaju rejestru do późniejszego wykorzystania. Atakujący może zmusić klienta do zaszyfrowania niektórych pakietów przy użyciu tego klucza podczas wykonywania wspomnianych wyżej ataków typu hotspot spoofing w celu przyciągnięcia klienta do punktu dostępowego, który podszywa się pod żądany, przy użyciu szyfrowania WEP (choć z niepoprawnym pasującym kluczem). Określone pakiety są zawsze wysyłane przez klienta po nawiązaniu i podczas początkowego uwierzytelniania w ramach „szybkiego ponownego połączenia", które są szyfrowane przy użyciu zapisanego klucza WEP klienta. Należą do nich ARP, DHCP i określone ramki zarządzania 802.11. Szczególnie interesujące są bezpłatne pakiety ARP wysyłane przez klienta po skojarzeniu z punktem dostępowym, który jego zdaniem jest uzasadniony. Dzięki technikom przerzucania bitów atakujący może sfałszować zaszyfrowane ARPrequests do łączącego się klienta, ponownie wykorzystując wcześniej przechwycone nieuzasadnione pakiety ARP i zamieniając je w żądanie. Ta technika wykorzystuje brak kontroli integralności WEP i poleganie na mechanizmie kontroli błędów CRC jako jedynej kontroli integralności. Algorytmy CRC nie mają na celu zapewnienia niczego poza integralnością opartą na błędach i są podatne na nadużycia w atakach WEP. Kompilacja luk w zabezpieczeniach hotspotów i WEP może dostarczyć klucz WEP do sieci firmowej w ciągu sześciu minut, nawet bez konieczności dostępu do rzeczywistej sieci. Atakujący może teraz zabrać swoje latte, Twój firmowy klucz WEP, zlokalizować sieć firmową i połączyć się z parkingu.

Procedura ataku Caffe-Latte

1. Maszyna ofiary wysyła żądania sondy SSID dla punktów dostępowych, z którymi komunikowała się w przeszłości (prawie wszyscy suplikanci przechowują tę historię, aby umożliwić szybkie ponowne połączenia).

2. Atakująca maszyna monitoruje fale radiowe pod kątem sond SSID i odnotowuje żądane nazwy punktów dostępu (np. „coffeeshop", „airportWifi" itp.).

3. Atakująca maszyna tworzy AP z nazwą SSID żądaną przez klienta (np. „coffeeshop", „airportWifi" itp.).

4. Maszyna ofiary próbuje się połączyć, ale kończy się niepowodzeniem, prawdopodobnie z powodu niezgodności szyfrowania.

5. Atakująca maszyna modyfikuje AP, aby posiadała szyfrowanie WEP z fałszywym kluczem.

6. Urządzenie ofiary próbuje ponownie połączyć się z punktem dostępowym i pomyślnie uwierzytelnia się z powodu prawidłowo dopasowanej nazwy SSID i stopnia szyfrowania.

7. Maszyna ofiary zatrzymuje się podczas dalszego uwierzytelniania opartego na sieci z powodu niezgodności klucza i nigdy nie jest w pełni skojarzona.

8. Atakujący przechwytuje nieuzasadnione pakiety ARP, DHCP i inne wysyłane przez ofiarę po skojarzeniu, które są szyfrowane za pomocą przechowywanego klucza WEP ofiary.

9. Atakujący dostarcza zaszyfrowany przez ofiarę bezpłatny pakiet ARP do./cafe-latte, co skutkuje przerzucaniem bitów w celu wygenerowania zaszyfrowanego żądania ARP z poprawnym CRC.

10. Atakujący odtwarza zaszyfrowane żądanie ARP, aby uzyskać odpowiedzi od ofiary za pomocą nowych IV, dopóki nie zostanie przechwycona wystarczająca ilość IV, aby wyczerpać 40-bitową przestrzeń klucza.

11. Atakujący uruchamia Aireplay-ng (lub porównywalne narzędzie do łamania WEP), dostarczając IV przechwycone podczas powtórek żądań ARP.

12. Atak otrzymuje heksadecymalny klucz WEP w postaci zwykłego tekstu i wykorzystuje go do uzyskania dostępu do sieci docelowej.

Następujące narzędzia mogą być użyte do przeprowadzenia ataku typu hotspot i cafe latte:

* Airbase-ng: Utwórz AP z określonym SSID

* Cafe-latte: Skrypt łamania WEP, który pobiera przechwycony bezpłatny pakiet ARP i przekształca go w żądanie, które może być powtarzane klientowi tysiące razy.

A co z WPA/WPA2?

WPA i WPA2 wdrażają kontrole integralności kryptograficznej, które usuwają jakąkolwiek możliwość wydedukowania klucza w postaci zwykłego tekstu, ale nadal cierpią z powodu ataku typu hotspot. Atak dostosowany do AWPA/WPA2 polega na maskowaniu się jako znany AP, w którym klient oczekuje szyfrowania WPA lub WPA2. Po podaniu poprawnego poziomu szyfrowania klient będzie próbował się połączyć i nie powiedzie się z powodu braku odpowiedniego klucza przez punkt dostępowy. Oczekuje się niepowodzenia, ponieważ wstępnie udostępnione skróty klucza z solą identyfikatora SSID zostały już wysłane od klienta i przechwycone przez atakującego. Ten skrót może być następnie brutalnie wymuszony.

WEP.

Pomimo publicznego i długiego ujawniania luk w zabezpieczeniach WEP i niewielkiego poziomu bezpieczeństwa, jaki faktycznie zapewnia, jego szerokie zastosowanie na poziomie przedsiębiorstwa jest szokujące, ale zwykle nieznane ze względu na jego wykorzystanie w wielu małych szczelinach firmy, które mogły się zaklinować wiele lat temu. WEP powstał w czasach, gdy moc obliczeniowa, aw szczególności moc obliczeniowa wbudowana, była trudna do zdobycia. Moc obliczeniowa wymagana do przeprowadzenia szyfrowania WEP RC4 i zarządzania kluczami jest bardzo minimalna, co doskonale pokrywa się z mocą obliczeniową wielu urządzeń przenośnych i innych urządzeń wbudowanych. To właśnie jest głównym powodem, dla którego WEP pozostaje w wielu środowiskach i będzie w przewidywalnej przyszłości. Koszty utopione w urządzeniach infrastrukturalnych niezdolnych do wykonywania funkcji obciążających zasoby, takich jak AES i CCMP w WPA2.

Wdrożenie WPA

TKIP został precyzyjnie wykonany, aby umożliwić wsteczną kompatybilność ze sprzętem WEP. W dzisiejszym środowisku korporacyjnym powszechne jest, że WEP został całkowicie usunięty z pracowniczych sieci WLAN, ale jest powszechny w centrach handlowych lub dystrybucyjnych na urządzeniach przenośnych i innych urządzeniach przenośnych. Kolejnym czynnikiem pogarszającym słabą implementację szyfrowania strumieniowego RC4 przez WEP jest niejednoznaczna definicja w ramach standardu dla określonych procesów funkcji szyfrowania, w dużej mierze pozostawiająca decyzję dostawcy. Jest to szczególnie widoczne w sposobie generowania wektorów inicjujących; niektórzy dostawcy używają pseudogeneratora liczb losowych (PRNG), a inni zaczynają od 000000 i kierują się do FFFFFF. Pokrótce zagłębimy się w następujące wypróbowane i prawdziwe podstawowe luki w zabezpieczeniach wpływające na WEP oraz brak odpowiedniego zarządzania kluczami, integralności lub szyfrowania, a zakończymy krótkim opisem postępów WPA/WPA2 w tym obszarze.

(WEP) Powtarzające się wektory inicjujące (IV).

WEP zawiera wiele luk w zabezpieczeniach, w tym FMS, KoreK, PTW i ChopChop. Zamierzamy omówić tylko najbardziej znany i oryginalny atak, zwany FMS. WEP odeszło wieki temu na rzecz alternatywnych technologii; w związku z tym zagłębimy się w szczegóły tej luki tylko po to, aby rzucić światło na postępy, które poczyniono od czasu jej odkrycia. Podstawowe szyfrowanie WEP obraca się wokół szyfru strumieniowego RC4. Inicjalizacja wektora (IV) służy do zapewnienia, że dwa identyczne dane wejściowe nie dadzą w wyniku tego samego wyniku zaszyfrowanego tekstu. IV służy do wydłużenia żywotności klucza poprzez unikatowe generowanie IV dla każdej klatki. Klucze WEP występują w dwóch formach, w zależności od wersji, 40-bitowe efektywne (64, w tym IV), a niektóre implementacje sięgają tak samo jak efektywne 104 bity (128 w tym IV) WEP używa 24-bitowego IV, który w obciążonej sieci jest 50-procentowym prawdopodobieństwem, że IV powtórzy się po 5000 pakietów. Podstawowym rozwiązaniem problemu podatności na szeregowanie kluczy WEP IV jest użycie kluczy sesji ustanowionych na początku uwierzytelniania i szyfrowania, które są używane przez określony czas podczas sesji szyfrowania. Proces używany do wyprowadzania klucza tymczasowego lub sesyjnego ma kluczowe znaczenie dla powodzenia procesu planowania kluczy. WEP cierpiał z powodu połączenia wyjścia RC4 z IV i został ulepszony dzięki „mieszaniu" tych wartości przez TKIP przed RC4. Jeśli można ustanowić funkcję planowania i zarządzania kluczem stałym, sama procedura szyfrowania będzie działać zgodnie z oczekiwaniami. Ataki, których celem są luki w kluczowym procesie planowania WEP, obejmują słynny atak FMS, nazwany na cześć wynalazców Fluhrera, Mantina i Shamira.

Zarządzanie kluczami.

WEP nie zapewnia żadnej formy zarządzania kluczami, takiej jak możliwość rotacji kluczy z klientami. Rezultatem braku struktury zarządzania kluczami jest ponowne wykorzystanie przestarzałych kluczy jako danych wejściowych do planowania kluczy i podstawowego procesu szyfrowania przez dłuższy czas, co dodatkowo potęguje wspomnianą wcześniej powtarzającą się lukę IV. WPA i WPA2 zapewniają oparte na sesji zarządzanie kluczami poprzez implementację TKIP (WPA), a później CCMP/AES (WPA2). Należy podkreślić, że klucz tajny w implementacji klucza wstępnego (WPA/WPA2-PSK) jest tak naprawdę wykorzystywany tylko do uwierzytelniania; szyfrowanie pochodzi od klienta i punktu dostępowego posiadających ten sam klucz, ale klucz wstępny nie jest bezpośrednio zaangażowany. Jest to przeciwieństwo używania klucza wstępnego przez WEP bezpośrednio w procesie szyfrowania poprzez wykorzystanie go do uwierzytelniania i włączenie go do szyfru strumieniowego RC4. Dzięki wykorzystaniu EAP i RADIUS edycje WPA i WPA2 Enterprise w pełni obsługują zarządzanie kluczami poprzez struktury oparte na katalogach. Te katalogi zarządzają kluczami uwierzytelniania poza implementacją WPA/WPA2 i zwiększają bezpieczeństwo dzięki połączeniu zarządzania kluczami uwierzytelniania opartego na katalogach (LDAP/Active Directory) i zarządzanie kluczami szyfrowania TKIP/CCMP. Narzędzia wykorzystywane do wykorzystywania luk WEP:

* Airmon-ng30: Służy do przełączania adaptera bezprzewodowego w tryb monitora.

* Airodump-ng: Służy do przechwytywania WEP IV w trybie monitora.

* Aireplay-ng-1: Fałszywe uwierzytelnianie do AP; pozwoli to na powiązanie z punktem dostępowym, ale nie będzie kontynuowania procesu uwierzytelniania. Jest to konieczne, aby punkt dostępu odbierał dane z karty sieci bezprzewodowej.

* Aireplay-ng-3: tryb ataku z odtworzeniem żądania ARP, będzie nasłuchiwał zaszyfrowanych bezpłatnych pakietów ARP wysyłanych przez legalnego podłączonego klienta. Ten tryb identyfikuje pakiety ARP według rozmiaru i innych czynników, mimo że są zaszyfrowane. Po znalezieniu pakietu ARP, Aireplay przewróci bity i zamieni go w żądanie, na które odpowiedź zostanie udzielona tysiące razy. Celem tego jest wygenerowanie wielu zaszyfrowanych pakietów od ofiary i rozpoczęcie wyczerpywania przestrzeni IV.

* Aircrack-ng-b: Wykonuje analizę statystyczną i brutalną siłę przechwyconego ruchu WEP w celu odzyskania klucza. Proces polega na użyciu analizy statystycznej, aby określić potencjalne wartości bajtów w każdej lokalizacji klucza, a następnie użyć brutalnej siły, aby zakończyć proces.

Wstępnie udostępniony klucz WPA/WPA2.

WPA, a później WPA2 miały na celu usunięcie wielu niedociągnięć w postępach WEP i WEP. Oto wektory ataków i mechanizmy kontroli mitygacji zaimplementowane w standardzie WPA:

* 48-bitowe wektory inicjujące: rozwiązuje 24-bitową lukę WEP i słabą implementację RC4 poprzez użycie TKIP/CCMP w celu znacznego zmniejszenia ponownego użycia IV i poprawy możliwości „zaszczepiania" funkcji szyfrowania.

* Zarządzanie kluczami: TKIP i CCMP/AES zapewniają unikatowe klucze szyfrowania na klatkę, w przeciwieństwie do przechowywania starych kluczy WEP wśród suplikantów klienta i polegania na IV jako głównym czynniku różnicującym. WPA/WPA2 obsługuje również natywnie zarówno PSK, jak i mechanizmy uwierzytelniania oparte na przedsiębiorstwach do zarządzania kluczami uwierzytelniania innych firm (np. Katalog LDAP).

* Długość klucza: WPA/WPA2 zapewniają minimalną długość 256-bitowego klucza współdzielonego.

* Message Integrity Code: WPA prawidłowo zapewnia integralność wiadomości poprzez mechanizm mieszający znany jako MIC lub Message Integrity Code. Jest to przeciwieństwo wartości kontroli integralności (ICV) WEP, która składa się z zaszyfrowanej kontroli błędów CRC-32. ICV WEP jest nękany przez ataki z przerzucaniem bitów z powodu jego nieprawidłowego użycia jako mechanizmu integralności pomimo zamierzonego użycia CRC-32 jako mechanizmu wykrywania błędów transmisji

* Wzajemne uwierzytelnianie: WPA/WPA2 umożliwia uwierzytelnianie punktu dostępowego przez klienta za pomocą certyfikatów i RSN.

Podstawowa luka, która nęka WPA/WPA2 niekoniecznie jest luką w implementacji, ale atrybutem niezbędnego 4-way handshake process (EAPoL) do podstawowego uwierzytelniania klucza wstępnego. PSK nie jest przeznaczony do użytku korporacyjnego (ale mimo to znajduje się w przedsiębiorstwie), dlatego w ramach WPA/WPA2 istnieją rozwiązania eliminujące tę lukę na poziomie przedsiębiorstwa, ale nie na poziomie SOHO. Uwierzytelnianie za pomocą klucza wstępnego jest powszechnie używane w przypadku braku katalogu zaplecza normalnie dostępny przez protokoły RADIUS i LDAP. Ten rodzaj implementacji jest powszechny dla rozwiązań, które nie są przeznaczone dla szerokiej gamy klientów i dlatego koszt wdrożenia takiego rozwiązania jest nieopłacalny. Uwierzytelnianie z kluczem

współdzielonym opiera się na pozapasmowym systemie zarządzania kluczami. WPA-PSK i WPA2-PSK nie zapewniają zarządzania kluczami ani tunelowego szyfrowania procesu uzgadniania uwierzytelniania z kluczem wstępnym. Procedura skrótu hasła używana przez WPA/WPA2 łączy zapisane hasło z solą identyfikatora SSID docelowego punktu dostępowego i przesyła je w postaci zwykłego tekstu. Poleganie na jednym atrybucie kontroli dostępu oznacza, że każdy klient jest nieodróżnialny od następnego i nie można przyznać żadnej odpowiedzialności każdemu użytkownikowi poza dziennikiem adresów MAC DHCP.

Klucz WPA/WPA2

Hash Capture i pękanie. Proces uwierzytelniania z kluczem wstępnym WPA/WPA2 to seria uścisków dłoni używanych do ostatecznego przesłania skrou hasła do punktu dostępowego. Ten proces można przechwycić w trybie monitorowania i wykorzystać do wyodrębnienia zaszyfrowanego hasła. Ponieważ proces ten występuje tylko wtedy, gdy klienci są początkowo uwierzytelniani w punkcie dostępowym, osoba atakująca może albo poczekać na nowego klienta, albo przeprowadzić deautentyfikację istniejącego klienta przez fałszowanie ramek zarządzania, jak opisano wcześniej w tym rozdziale. Po uzyskaniu skrótu WPA atakujący może spróbować go złamać przy użyciu brutalnej siły. Ze względu na solenie haszyszu identyfikatorem SSID AP, tablice tęczowe nie mogą być używane do wspomagania procesu pękania. Użycie solonego skrótu w połączeniu z długim procesem mieszania powoduje powolne łamanie skrótów WPA w systemach opartych na procesorach. Wyczerpujący atak słownikowy na system oparty na procesorze może zazwyczaj przetworzyć od 5 000 do 15 000 par głównych kluczy na sekundę. Systemy łamania oparte na GPU stają się coraz bardziej popularne, ponieważ interfejsy programistyczne, takie jak CUDA firmy Nvidia, otworzyły deweloperom drzwi do dostępu do wielu komponentów GPU, które normalnie wymagałyby zaawansowanego doświadczenia programistycznego. GPU można wykorzystać do znacznego zwiększenia prawdopodobieństwa pomyślnego złamania przechwyconego uzgadniania WPA do ponad 50 000 par kluczy głównych na sekundę dla przeciętnego zestawu kart graficznych GPU obsługujących CUDA. Narzędzia używane do przechwytywania i łamania klucza wstępnego WPA/WPA2:

* Airmon-ng31: Służy do przełączania adaptera bezprzewodowego w tryb monitora.

* Airodump-ng: Służy do przechwytywania ruchu w trybie monitorowania.

* Aireplay-ng-0: dezaktywuje klienta z punktu dostępowego i zmusza go do ponownego uwierzytelnienia i wykonania wstępnego uzgadniania klucza współdzielonego. To narzędzie jest niezbędne, aby umożliwić Airodump-ng przechwycenie klucza wstępnego podczas procesu ponownego uwierzytelniania.

WPA/WPA2: Wi-Fi Protected Setup (WPS).

Wi-Fi Protected Setup pozwala użytkownikom, którzy nie rozumieją konfiguracji zabezpieczeń bezprzewodowych, na łatwe skonfigurowanie wstępnie udostępnionej konfiguracji klucza bez konieczności logowania się do routera. WPS opisuje protokół i sekwencję osobistego numeru identyfikacyjnego (PIN) używaną do negocjowania klucza wstępnego WPA/WPA2 bez konieczności ręcznego konfigurowania go na kliencie i punkcie dostępowym. WPS jest dostępny tylko w punktach dostępowych klasy SOHO, a nie na sprzęcie klasy korporacyjnej. Ta luka może dotyczyć środowiska przedsiębiorstwa, ponieważ istnieje jako niezłośliwy, nieuczciwy punkt dostępu, który użytkownik wewnętrzny bezpiecznie skonfigurował, ale jest podatny na WPS. Istnieją dwa rodzaje WPS:

* Połączenie za pomocą przycisku (PBC)

* 8-cyfrowy kod PIN

Numer PIN może być dostarczony przez punkt dostępowy do wprowadzenia do agenta WPS klienta lub agent WPS klienta może dostarczyć numer PIN do wprowadzenia do monitu WPS punktu dostępowego. Uwierzytelnianie WPS opiera się na 802.1X EAP i implementacji EAP specyficznej dla dostawcy, która wykorzystuje wymianę kluczy Diffie-Hellman do udowodnienia posiadania pierwszej połowy kodu PIN między punktem dostępowym a klientem, a ostatecznie drugiej połowy. Ponieważ WPS dzieli kod PIN na dwa oddzielne etapy uwierzytelniania, proces ten poważnie ogranicza liczbę kombinacji dla każdej połowy kodu PIN. Atakujący może uzyskać pierwszą i drugą część kodu PIN poprzez nadużycie komunikatu EAP „EAP-NACK". Ten komunikat jest wysyłany przez punkt dostępowy w przypadku niedostarczenia prawidłowej pierwszej lub drugiej części kodu PIN. Brutalne wymuszanie każdej oddzielnej części kodu PIN wymaga najwyżej 104 prób, więc istnieją tylko 104 + 104 = 20 000 możliwych kombinacji zamiast oryginalnej przestrzeni kluczy wynoszącej 108 lub 1 000 000 000.32 Średnio narzędzia do łamania WPS mogą odzyskać tekst jawny WPA/WPA2 hasło za 4–10 godzin. Narzędzia używane do wykonania ataku WPS:

* Airmon-ng: Aby wykryć docelowy AP i umieścić adapter w trybie monitora.

* Reaver33: Brute zmusza proces WPS EAP do odzyskania klucza WPA/WPA2.

* Wpscrack.py34: alternatywne narzędzie do brutalnego wymuszenia procesu WPS EAP w celu odzyskania klucza WPA/WPA2.

MS-CHAP-v2 - Dziel i zwyciężaj.

Implementacje EAP wykorzystujące protokół MS-CHAP-v2 zostały już omówione jako podatne na ataki słownikowe przy użyciu protokołu EAP-LEAP lub EAP-PEAP-MSCHAP ze słabymi konfiguracjami suplikantów. Tradycyjnie jedynym możliwym podejściem do wykorzystania tej luki był proces łamania funkcji hash challenge-response, w którym programowi łamanemu dostarcza się hash challenge-response wraz ze słownikiem. Dzięki badaniom Moxie Marlinspike (również autora SSLStrip), proces ten został ostatnio przyspieszony dzięki nowemu zrozumieniu pozornie oczywistej i często pomijanej funkcjonalności protokołu MS-CHAP-v2. Podczas MSCHAP-v2 hash MD4 hasła użytkownika jest dzielony bitowo w celu utworzenia trzech oddzielnych kluczy DES (po siedem bajtów każdy). Typowe narzędzie do testowania penetracji, takie jak Asleep, wprowadzi hash MD4, podzieli go na trzy klucze DES i użyje tych kluczy do zaszyfrowania danej wartości słownika tekstu jawnego w celu porównania z oryginalnym hashem tekstu zaszyfrowanego. Tradycyjne podejście do pękania skutkowałoby całkowitą przestrzenią kluczy wynoszącą 2 (56 + 56 + 56) lub około 1050 – bardzo dużą liczbę, która jest niewykonalna w przypadku stopniowego pękania metodą brute-force. To jest dokładnie powód, dla którego słowniki były tradycyjnie używane jako podejście „najlepsze zgadywanie", ponieważ przyrostowe (znak po znaku) brutalne wymuszanie po prostu nie jest opcją przez jakikolwiek rozsądny czas ze względu na solenie słowników za pomocą wyzwanie. Użycie trzech kluczy DES to podstawa eksploatacji. MD4hash ma tylko 16 bajtów, podczas gdy trzy siedmiobajtowe klucze DES dają nam w sumie 21 bajtów. Jak powstała różnica? Dopełnienie, które zmniejsza efektywną długość trzeciego klucza DES do dwóch bajtów. Jeśli każdy z dwóch siedmiobajtowych i pojedynczych kluczy dwubajtowych zostanie złamany indywidualnie, efektywna przestrzeń kluczy zostanie zmniejszona do 256 +256 +216 lub około 1017-zmniejszenie w przestrzeni kluczy o współczynnik 1032. Ciekawa część dotycząca MS- CHAP-v2routine polega na tym, że każdy klucz DES jest używany do szyfrowania tego samego tekstu jawnego; dlatego podczas procesu łamania możemy użyć tego samego klucza wejściowego dla każdej z dwóch funkcji DES, skutecznie zmniejszając liczbę funkcji DES dla każdej iteracji do jednej, pozostawiając jedyną podwójną operację, jaką jest porównanie wyjścia DES z każdą z dwa wcześniej ustalone szyfrogramy. Jest to ostateczna efektywna przestrzeń kluczy wynosząca 256 (1016), która w 1998 r. mogła zostać złamana średnio w 4,5 dnia, a w przypadku masowo równoległych

architektur dostępnych komercyjnie na początku 2010 r. średnio w około pół dnia. Narzędzia używane do łamania MS -CHAP-v2:

* Airmon-ng: do przechwytywania materiału klucza MS-CHAP-v2 podczas procesu challenge-response.

* Aireplay-ng-0: Służy do dezaktywacji połączonego klienta MS-CHAP-v2.

* Chapcrack.py: Używany do analizowania/wyodrębniania materiału klucza z uzgadniania MS-CHAP-v2.

* Super Computer: Przyspieszona sprzętowo maszyna do łamania zabezpieczeń zaprojektowana do łamania pojedynczej procedury DES (dostępna za pośrednictwem usług w chmurze).

KONTROLE ŁAGODZĄCE.

W tej sekcji przedstawiono techniczne środki kontroli ryzyka klasy korporacyjnej, które należy oceniać w każdym rozwiązaniu bezprzewodowym, niezależnie od implementacji konkretnego dostawcy. . Te kontrolki odpowiadają na omówione wcześniej podstawowe problemy związane z bezpieczeństwem sieci bezprzewodowej i zapewniają warstwową ochronę w ramach bezpiecznego projektowania przedsiębiorstwa.

Ulepszenia.

Kontrola dostępu przewodowego pozostała stosunkowo stabilna wraz z pojawieniem się uwierzytelniania opartego na portach 802.1X, które jest obecnie standardem w większości nowoczesnych przełączników. Uwierzytelnianie oparte na portach 802.1X to zasadniczo ta sama funkcja uwierzytelniania, która jest wypiekana w standardzie zabezpieczeń WPA i połączona z protokołem TemporalKey Integrity Protocol (TKIP). WPA2 opiera się na protokole WPA, dodając jeszcze silniejsze szyfrowanie, które wymaga dedykowanego sprzętu do szyfrowania AES. Standard przewodowy 802.1X jest w pełni zaimplementowany w WPA i WPA2, ale zależy od konfiguracji, czy jest wykorzystywany, np. WPA-Personal, który wykorzystuje klucz wstępny, lub WPA-Enterprise, który korzysta z centralnego repozytorium uwierzytelniania.

Zastosowanie łączności bezprzewodowej do łączności z punktami końcowymi może zapewnić bezpieczeństwo, które może konkurować z tradycyjną architekturą przewodową dzięki łatwości administrowania i zarządzania środowiskiem punktów dostępowych klienta uproszczonego oraz dławikami sieci w celu monitorowania w bliskiej odległości od klientów inicjujących na najbardziej zewnętrznej krawędzi sieć.

RSN.

Pełna obsługa RSN w wersji roboczej WPA2 i 802.11i w standardzie WPA jest niezbędny do zapewnienia poufności i integralności sieci bezprzewodowej. Aby wdrożyć RSN, wystarczy dowolny punkt dostępowy, który może przeprowadzić uwierzytelnianie 802.1X. Obsługa 802.1X w punkcie dostępowym to zwykle tylko kwestia zrozumienia protokołu EAPoL i zaakceptowania serwera RADIUS jako parametru konfiguracyjnego. AP nie musi być konfigurowany dla żadnego konkretnego typu EAP, ponieważ ten aspekt sieci jest całkowicie przezroczysty dla AP. W typowym środowisku bezprzewodowym działają dwie podstawowe funkcje zarządzania: zarządzanie uwierzytelnianiem użytkownika i zarządzanie kluczami do szyfrowania, początkowy materiał klucza i dystrybucja kluczy. W implementacji innej niż korporacyjna można łączyć funkcje zarządzania użytkownikami i kluczami. Fakt, że klient posiada poprawny klucz wstępny, uwierzytelnia go w punkcie dostępowym, a bity, które tworzą klucz wstępny, mogą być użyte w procesie szyfrowania w celu uzyskania parami kluczy przejściowych do szyfrowania ładunku 802.11.

Zagadnienia dotyczące uwierzytelniania i kontroli dostępu do zarządzania kluczami

* Solidne zarządzanie kluczami uwierzytelniania jest niezbędne do zapewnienia bezpiecznej komunikacji kluczy, w przeciwieństwie do środowiska kluczy wstępnych, w którym klucze muszą być dystrybuowane za pośrednictwem mechanizmu pozapasmowego. Klucz może mieć postać kombinacji użytkownika/hasła, certyfikatu lub innego materiału identyfikującego, takiego jak RSA

Numer SecurID i PIN.

* Wykorzystaj istniejącą infrastrukturę opartą na katalogach używaną do uwierzytelniania użytkowników w systemach komputerowych w bezprzewodowej sieci LAN lub wdrażaj infrastrukturę PKI punktów końcowych. Wykorzystanie EAP i repozytorium użytkowników zaplecza do uwierzytelniania za pomocą protokołu RADIUS to srebrny standard metody uwierzytelniania. Infrastruktura PKI, która zapewnia klientowi publiczne/prywatne klucze do każdego bezprzewodowego punktu końcowego, skutecznie eliminuje możliwość przechwycenia przez atakującego odpowiedzi na wyzwanie haszowania hasła.

* Implementacje silnego protokołu EAP obejmują tunel TLS ustanowiony między klientem punktu końcowego a serwerem uwierzytelniania zaplecza (np. RADIUS) przed wymianą jakichkolwiek identyfikowalnych informacji.

Uwagi dotyczące zarządzania kluczami szyfrowania.

Jak opisano, zarządzanie kluczami szyfrowania jest piętą achillesową poufności. Nowoczesne algorytmy szyfrowania dojrzały do punktu perfekcji, podobnie jak AES, i są tak słabe, jak ich najsłabsze ogniwo, czyli dane wejściowe. Najlepsze funkcje zarządzania kluczami są dostępne tylko w najnowszych osiągnięciach technologii bezprzewodowych. AES/CCMP WPA2-Enterprise jest de facto standardem i powinien być minimalnym wymogiem dla każdej nowej implementacji. WEP, WPA i WPA-2 prezentują wiele metod zarządzania kluczami z udoskonaleniem w każdej generacji schematów uwierzytelniania/szyfrowania 802.11.

Certyfikaty serwera i klienta uwierzytelniania.

Uwierzytelnianie oparte na certyfikatach między klientem a serwerem uwierzytelniania zaplecza jest de facto standardem uwierzytelniania bezprzewodowego. Certyfikaty X.509 są używane do uwierzytelniania serwera z klientem (RADIUS jako broker), klienta z serwerem uwierzytelniania lub obu. Wykorzystanie certyfikatów użytkowników końcowych i komputerów do uwierzytelniania zamiast uwierzytelniania opartego na hasłach katalogowych wymaga wdrożenia pełnej infrastruktury klucza publicznego (PKI). PKI jest niezbędne do dostarczania i regularnego aktualizowania/kojarzenia certyfikatów z urządzeniami końcowymi i podpisywania ich za pomocą głównego urzędu certyfikacji przedsiębiorstwa (CA) lub zewnętrznego głównego urzędu certyfikacji, takiego jak VeriSign. Poniżej przedstawiono trzy najczęstsze zastosowania certyfikatów punktów dostępowych lub klientów w nowoczesnych wdrożeniach bezprzewodowych w przedsiębiorstwach:

* Tylko certyfikaty serwera uwierzytelniania:

* Implementacja protokołu RSN EAP w wersji szkieletowej powinna wymagać co najmniej podpisanego certyfikatu serwera uwierzytelniania. Zapewnia to łączącym się klientom, że przeprowadzają uwierzytelnianie z zaufanym punktem dostępu i serwerem uwierzytelniania. W przypadku braku certyfikatu serwera klienci są podatni na ataki MITM, których można użyć do przechwycenia od klienta skrótów typu wyzwanie-odpowiedź EAP. Protokół RSN zapewnia, że klient musi uwierzytelnić serwer

uwierzytelniania przed uwierzytelnieniem się na serwerze. Ta sekwencja chroni przed atakami RADIUSimpersonation i nieuczciwymi punktami dostępowymi, jeśli jest poprawnie skonfigurowana.

* Implementacje bezprzewodowe, które wykorzystują certyfikaty serwera uwierzytelniania, ale nie wymuszają ich na poziomie suplikanta, rezygnują z wszelkich zabezpieczeń zapewnianych przez tę kontrolę. Atakujący może podszywać się pod prawdziwy serwer uwierzytelniania zaplecza za pomocą tego samego identyfikatora SSID i przejąć kontrolę nad procesem uwierzytelniania.

* Wzajemne uwierzytelnianie klienta i serwera oparte na certyfikatach: Każdy klient punktu końcowego otrzymuje certyfikat podpisany przez główny urząd przedsiębiorstwa i zainstalowany w magazynie certyfikatów systemu operacyjnego. Protokół EAP-TLS jest powszechnie używany w tego typu infrastrukturze PKI do uwierzytelniania certyfikatu serwera (jak w przypadku uwierzytelniania opartego na katalogach) oraz certyfikatu klienta poprzez weryfikację podpisu certyfikatu. Ten certyfikat klienta zawiera również informacje z pól służące do identyfikacji użytkownika oraz wszelkie inne odpowiednie informacje do wykorzystania przez serwer uwierzytelniania.

* Uwierzytelnianie oparte na kliencie i serwerze za pomocą zewnętrznych certyfikatów klienta: infrastruktura PKI może zapewnić jeszcze większe bezpieczeństwo w postaci „czegoś, co mam, czego nie mają inni". Certyfikat klienta (klucz prywatny) może być przechowywany na karcie inteligentnej, co wymaga od użytkownika posiadania certyfikatu niezależnie od systemu operacyjnego w przypadku zgubienia lub kradzieży laptopa. Karta inteligentna musi być włożona do komputera przed próbą uwierzytelnienia.

Konfiguracje dostawcy punktów końcowych.

Konfiguracja klient-punkt końcowy jest kluczowym i często pomijanym elementem bezpiecznego wdrożenia sieci bezprzewodowej. Wdrożenie bezpiecznej sieci bezprzewodowej w przedsiębiorstwie chroni sieć wewnętrzną, ale większość wdrożeń zaniedbuje ocenę bezpieczeństwa punktów końcowych, które łączą się z nową siecią bezprzewodową.

Włączenie łączności bezprzewodowej na poziomie przedsiębiorstwa oznacza, że laptopy, które są zabierane poza biuro, prawie zawsze będą miały włączone bezprzewodowe radio. Bezprzewodowa łączność radiowa nie jest nieodłącznym ryzykiem, ale w połączeniu z domyślnymi konfiguracjami systemu operacyjnego i sterowników takie niechronione urządzenia mogą z łatwością dostarczać stronom nasłuchującym wszelkiego rodzaju informacje o łączności. Większość domyślnych suplikantów klientów bezprzewodowych poddaje się pewnego rodzaju atakom, które mogą potencjalnie zagrozić punktowi końcowemu w zdalnej lokalizacji, takiej jak kawiarnia, i ponownie nawiązać łączność, gdy klient idzie do pracy i łączy zainfekowaną maszynę z przedsiębiorstwem Sieć bezprzewodowa. Pracownicy mogą latać, siedzieć w autobusie lub po prostu łapać coś do jedzenia – a jeśli odpowiednio długo siedzą w fizycznej lokalizacji, atakujący może zebrać mnóstwo informacji z niezabezpieczonej konfiguracji petentów. Informacje te mogą obejmować wstępnie udostępniony skrót klucza dla sieci domowej, zapamiętane identyfikatory SSID (np. bezprzewodowy identyfikator SSID przedsiębiorstwa), a nawet skróty haseł do uwierzytelniania opartego na katalogu przedsiębiorstwa. Poniżej przedstawiono zalecenia dotyczące zabezpieczania konfiguracji suplikanta punktu końcowego:

* Wyłącz żądania sondowania SSID: Wiele systemów operacyjnych i zewnętrznych suplikantów będzie stale sondować ostatnie znane identyfikatory SSID. Ten proces jest wykonywany w celu upewnienia się, że klient może połączyć się z punktem dostępowym, który może nie wysyłać ramek nawigacyjnych w celu identyfikacji lub jeśli klient przeoczył interwał sygnału nawigacyjnego punktu dostępowego. Interwał sygnału nawigacyjnego jest zdefiniowany w punkcie AP jako okres czasu między wysyłaniem

ramek sygnału nawigacyjnego w celu identyfikacji siebie przez wszystkich nieskojarzonych klientów w zasięgu. Wyłączenie tej funkcji uniemożliwia atakującemu pasywne monitorowanie ruchu 802.11 i uzyskanie listy identyfikatorów SSID, z którymi dany klient próbuje się połączyć. Informacje te można następnie wykorzystać do zmuszenia klienta do połączenia się z nieuczciwym punktem dostępowym podszywającym się pod jeden ze zidentyfikowanych punktów dostępowych.36

* Profile sieci bezprzewodowej: Profile sieci bezprzewodowej należy skonfigurować tak, aby oddzielić profile firmowych punktów dostępu od profili punktów dostępu lub domowych punktów dostępu. Zewnętrzni suplikanci często zapewniają tę możliwość, aby zapobiec sytuacji, w której pracownik firmy korzysta z komputera w kawiarni, a jego sterownik sieci bezprzewodowej nieświadomie nadaje identyfikator SSID firmy, zachęcając w ten sposób atakującego do maskarady i potencjalnego przechwycenia klucza wstępnego WPA/WPA2 skrót lub skrót hasła oparty na katalogu odpowiedzi na wyzwanie. Korzystanie z różnych profili ogranicza możliwość, aby klient wiedział, jak połączyć się z punktami dostępowymi w sieci firmowej, gdy nie znajduje się w biurze.

* Konfiguracja bezpiecznego serwera uwierzytelniania

* Urząd certyfikacji: suplikant powinien akceptować tylko certyfikaty serwera uwierzytelniania, które zostały podpisane przez wyznaczony/pojedynczy główny urząd certyfikacji. Ta sytuacja uniemożliwia nawiązanie połączenia z punktem dostępu i bazowym serwerem uwierzytelniania, który wyświetla prawidłową/pasującą nazwę pospolitą podpisaną przez legalny, ale inny główny urząd certyfikacji.

* CertificateValidation: Użytkownicy nie powinni mieć możliwości nadpisywania i włączania korzystania z niezaufanego certyfikatu serwera podczas procesu uwierzytelniania. Domyślnie wielu suplikantów pyta użytkownika w przypadku wykrycia nieprawidłowego certyfikatu i udostępnia opcję zignorowania. Suplikant powinien być skonfigurowany tak, aby nie monitował użytkownika i usuwał wszelkie możliwości udanych prób uwierzytelnienia do punktu dostępowego z nieważnym lub niezaufanym certyfikatem.

* Nazwa pospolita (CN): Upewnij się, że w kliencie określono nazwę pospolitą lub CN serwera uwierzytelniania zaplecza. Zapobiegnie to połączeniu z punktem dostępowym i serwerem uwierzytelniania, które posiadają zaufany certyfikat (zakładając, że główny urząd certyfikacji nie jest specyficzny dla przedsiębiorstwa), ale używają nieprawidłowej nazwy hosta/FQDN.

Bezprzewodowe systemy wykrywania włamań.

Bezprzewodowy system wykrywania włamań (WIDS) przeszedł długą drogę, aby stać się standardowym urządzeniem do monitorowania bezpieczeństwa sieci, stając się codziennym narzędziem do monitorowania bezpieczeństwa, podobnie jak tradycyjny przewodowy system IDS. WIDS jest w stanie monitorować fale radiowe 802.11 na łączu danych i warstwie MAC niezależnie od szyfrowania lub uwierzytelniania. Chociaż WIDS nie może być używany zamiast przewodowego IDS, może zapewnić wgląd w pochmurny segment krawędzi sieci. WIDS nie ogranicza się również do przedsiębiorstw, które wdrażają sieć bezprzewodową. WIDS może również stanowić wartość dla przedsiębiorstw, które nie wdrażają sieci bezprzewodowych, zabezpieczając przed nieautoryzowanym użyciem połączeń bezprzewodowych poprzez ciągłe monitorowanie fal radiowych i odpowiednie ostrzeganie o wewnętrznych nieuczciwych punktów dostępu. Wiele dużych naruszeń wynikało ze słabego zarządzania siecią bezprzewodową i widoczności. Jest to duży problem dla organizacji posiadających wiele fizycznych punktów sprzedaży detalicznej lub korporacyjnych. Ze względu na szerokie zastosowanie i łatwość instalacji SOHO AP uzyskanego z konsumenckiego punktu sprzedaży detalicznej, coraz ważniejsze staje się wykrywanie nieautoryzowanych rozszerzeń sieci korporacyjnej. Ponadto zwiększone uzależnienie od komunikacji bezprzewodowej w różnych przypadkach

biznesowych (takich jak dostęp korporacyjny, urządzenia dostawców wymagające własnego punktu dostępowego lub urządzenia detaliczne wymagające dedykowanych punktów dostępowych z szyfrowaniem niskiej jakości ze względu na niski poziom mocy procesu) spowodowało większe trudności w inwentaryzacji autoryzowanych punktów dostępowych sieci i potwierdzanie prawidłowej segmentacji lub braku łączności wewnętrznej dla niekorporacyjnych punktów dostępowych. W przypadku, gdy przedsiębiorstwo może zarządzać wszystkimi znanymi punktami dostępowymi i inwentaryzować je, nie ma natywnego rozwiązania do szybkiego i dokładnego audytu wdrożenia standardowych poziomów uwierzytelniania i szyfrowania korporacyjnego ze zdalnej lokalizacji.

Rodzaje WIDS.

Większość nowoczesnych infrastruktur WIDS można skonfigurować tak, aby wykorzystywać istniejące punkty dostępowe lub używać dedykowanych czujników do monitorowania ruchu 802.11. Dedykowane czujniki zapewniają znacznie większą funkcjonalność kosztem dodatkowych kosztów. Dedykowany czujnik ma czas i procesor na pozyskiwanie przydatnych danych od sąsiednich punktów dostępowych i klientów, podczas gdy istniejący punkt dostępowy typu korporacyjnego typu „thin" może przeznaczyć tylko część przetwarzania na te funkcje.

Przypadki użycia.

Ze względu na szyfrowanie, które ma miejsce w warstwie łącza danych i powyżej, system WIDS nie może kontrolować ruchu w warstwie danych. Większość zagrożeń bezprzewodowych wiąże się z wykorzystaniem luki w zabezpieczeniach, która istnieje w warstwie łącza danych, takiej jak sam protokół 802.11 lub następujących procesach uwierzytelniania i szyfrowania. . Podstawowa wartość WIDS polega na możliwości zapewnienia bezpieczeństwa kontroli bezprzewodowych poprzez weryfikację ich istnienia i ciągłe monitorowanie pod kątem nieautoryzowanych zmian. Dedykowany WIDS może świadczyć następujące usługi:

* Identyfikuj nieautoryzowane punkty dostępowe we wszystkich fizycznych lokalizacjach (nieuczciwe punkty dostępowe).

* Wykrywaj i blokuj korzystanie z różnych bezprzewodowych narzędzi hakerskich z możliwymi do zidentyfikowania sygnaturami warstwy 1/2.

* Identyfikuj i stale monitoruj mechanizmy szyfrowania lub uwierzytelniania poniżej klasy korporacyjnej w autoryzowanych punktach dostępu.

* Wykrywaj i blokuj nieautoryzowane połączenia z wewnętrznymi punktami dostępowymi od klientów z nieautoryzowanymi kartami bezprzewodowymi.

* Określ parametry konfiguracyjne suplikanta klienta, ponieważ odnoszą się one do przesyłania znanych sygnałów nawigacyjnych SSID.

Szczegółowe korzyści WIDS

Zgodność z przepisami. Regularne testy penetracji sieci bezprzewodowych i nieuczciwe audyty AP są niezbędną funkcją wielu certyfikatów regulacyjnych (takich jak Payment Card Industry [PCI]). Wykorzystanie zdalnego dedykowanego czujnika WIDS może być opłacalną alternatywą dla rozmieszczenia wykonawców lub pracowników wewnętrznych w każdej fizycznej lokalizacji w celu zbadania i oceny kontroli.

Wykrywanie nieuczciwych punktów dostępu. Nieuczciwe punkty dostępowe to problem numer jeden zagrażający bezpieczeństwu sieci bezprzewodowej.37 Nawet w obliczu kontroli dostępu do portów

przełączników 802.1X, funkcja PAT (Port Address Translation) może zapewnić dostęp do sieci przewodowej wielu klientom bezprzewodowym poprzez współdzielenie jednego autoryzowanego adresu MAC. Pojedynczy niezarządzany punkt dostępowy może zapewnić nieograniczony dostęp do sieci wewnętrznej przez dłuższy czas. Metody wykrywania nieuczciwych punktów dostępu:

* Umieszczenie na białej liście firmowych punktów dostępu przez:

* Dostawca: Nieuczciwe punkty dostępowe można wykryć na podstawie niestandardowej marki/modelu, przeszukując część adresu MAC klienta bazowego OUI.

* SSID: Nieuczciwe punkty dostępowe można wykryć poprzez identyfikację przesyłanych sygnałów nawigacyjnych SSID zawierających niestandardowy identyfikator SSID przedsiębiorstwa (np. „Linksys" lub „Netgear").

* Adres MAC: Statyczną listę adresów MAC autoryzowanych punktów dostępu można uzyskać za pośrednictwem protokołu SNMP lub innych środków i dostarczyć do systemu WIDS jako „znane dobre" punkty dostępowe.

* Stopień szyfrowania/uwierzytelniania: TheWIDScan próbuje połączyć się z potencjalnymi nieuczciwymi punktami dostępowymi i wyliczyć dostępne/żądane poziomy szyfrowania/uwierzytelniania. Niestandardowy poziom lub metoda wskazywałaby na nieuczciwy AP.

* Powiązani klienci

* WIDS może przeprowadzić analizę podłączonych klientów potencjalnego nieuczciwego punktu dostępowego, aby określić, czy klienci są dostarczani przez przedsiębiorstwa na podstawie OUI adresów MAC.

* Siła sygnału

* WIDS stale monitoruje fale radiowe i może ostrzegać o wykryciu anomalii nowego AP w bliskiej odległości od fizycznego czujnika/lokalizacji, określając siłę sygnału potencjalnego fałszywego AP mierzoną w dBm. Jeśli siła dBm spadnie w zakresie progu skonfigurowanego przez użytkownika, może zostać wyzwolony alert.

Potwierdzenie wewnętrznej łączności LAN:

* Łączność z urządzeniami wewnętrznymi: Zdalny czujnik WIDS może próbować połączyć się z nieuczciwą siecią bezprzewodową i pingować znane urządzenie wewnętrzne, aby potwierdzić łączność z siecią przedsiębiorstwa (przy założeniu braku uwierzytelniania).

* Wyliczanie tabel CAM (Simple Network Management Protocol) w pamięci adresowalnej zawartością: Tabele CAM wewnętrznego przełącznika sieciowego zawierają wszystkie adresy MAC, o których wie urządzenie i na którym porcie się znajdują. Ta technika wykrywania opiera się na fakcie, że bezprzewodowe punkty dostępowe posiadają dwie karty sieciowe. Jedna karta sieciowa znajduje się po przewodowej stronie punktu dostępowego, a druga po stronie bezprzewodowej/radiu. Obie te karty posiadają adresy MAC, które różnią się jedną lub dwiema wartościami. Czujnik WIDS może identyfikować adres MAC używany przez radio bezprzewodowe poprzez pasywne monitorowanie warstwy łącza danych i przeszukiwać wszystkie znane tabele przełączników CAM za pośrednictwem SNMP w celu znalezienia podobnego adresu MAC. Kontroler WIDS może być wyposażony w ciąg odczytu SNMP do środowiska przełączników w całym przedsiębiorstwie używanego przez zespół zarządzający siecią do różnych procesów monitorowania/odpytywania.

Przeciwdziałanie. W przypadku wykrycia nieuczciwego punktu dostępowego, system WIDS można skonfigurować tak, aby wyłączyć port przełącznika, na którym się on znajduje, za pomocą ciągów zapisu SNMP lub przechwycić alert na konsoli centralnej. Czujnik WIDS można również ustawić w trybie blokowania, który będzie wykorzystywał

sfałszowane pakiety deauthentication 802.11, aby uniemożliwić klientom pomyślne nawiązanie połączenia z fałszywym punktem dostępowym. Sfałszowane pakiety deauthentication zostały omówione wcześniej w Sekcji 33.5.3, Ramki zarządzania iw odpowiednich okolicznościach mogą być użyte do zwiększenia bezpieczeństwa. Działania te należy dokładnie przeanalizować przed ich wykonaniem, aby zminimalizować prawdopodobieństwo nieświadomego zaatakowania legalnej sąsiedniej firmy lub gospodarstwa domowego.

Obrona w głąb — podstawowe sterowanie. Opisane wcześniej formanty są najlepszymi praktykami, które mogą stworzyć lub złamać zabezpieczenia sieci bezprzewodowej w przedsiębiorstwie. Oprócz tych kontroli, istnieją pewne kontrole, które same w sobie nie zapewniają dużej ochrony, ale razem mogą zmniejszyć wskaźnik sukcesu atakującego. Bezpieczeństwo poprzez ukrywanie może być złym pomysłem, jeśli jest to jedyny środek bezpieczeństwa, ale w połączeniu z solidnymi kontrolami bezpieczeństwa, można potencjalnie ograniczyć uzasadnione ataki na podstawową kontrolę bezpieczeństwa (taką jak EAP-MS-CHAP-v2). Te kontrolki nazywamy kontrolkami script-kiddie; stawiają niewielki opór doświadczonemu napastnikowi, ale powodują, że przeciwnik podejmuje wiele kroków, zanim nawet ujawni swój cel.

*Ograniczenia oparte na adresie MAC: W zależności od możliwości każdego punktu dostępowego określonego producenta, może być możliwe ograniczenie powiązania do punktu dostępowego na podstawie adresu MAC, nawet w środowisku korporacyjnym. Istnieją metody dynamicznej aktualizacji mapowań adresów MAC w repozytorium zaplecza, podobne do przypisywania VLAN opartego na przewodowym MAC.

* Maskowanie SSID: Maskowanie SSID jest doskonałym przykładem zabezpieczenia poprzez ukrywanie. Obecność punktu dostępowego i identyfikatora BSSID można zidentyfikować za pomocą różnych narzędzi do testowania penetracji, które mogą analizować surowy ruch 802.11, ale zwykły domyślny system operacyjny lub suplikant klienta innej firmy nie wyświetlają obecności punktu dostępowego z nierozgłaszającym identyfikatorem SSID.

* Izolacja klienta: Izolacja klienta to kontrola specyficzna dla punktu dostępu, która monitoruje docelowy adres MAC ruchu przychodzącego. Jeśli ruch jest przeznaczony dla innego klienta w tym samym punkcie dostępowym lub identyfikatorze SSID w środowisku cienkiego klienta, dostęp do niego zostanie odrzucony. Celem tej kontroli jest ograniczenie możliwości komunikowania się złośliwego użytkownika z innymi urządzeniami podłączonymi do AP. Ta funkcja jest powszechna w publicznych punktach dostępowych, w których użytkownik końcowy niekoniecznie jest dobrze sprawdzony lub uwierzytelniony. W zależności od zastosowania w przedsiębiorstwie konkretnego identyfikatora SSID/VLAN, ta funkcja może być włączona, aby uniemożliwić dostęp do innych punktów końcowych w środowisku, w którym usługi są świadczone bezprzewodowo przez innych klientów bezprzewodowych, takich jak drukarka; należy przeprowadzić analizę, aby umożliwić tylko podzbiór komunikacji z tymi urządzeniami.

BEZPIECZNE PROJEKTOWANIE PRZEDSIĘBIORSTWA.

Wcześniej szczegółowo omówiliśmy podstawowe i konkretne luki w zabezpieczeniach, aby wyeksponować nieodłączne ryzyko związane z mediami sieci bezprzewodowej i przedstawić tło niektórych najnowszych i największych zagrożeń, którymi należy się zająć. Zrozumienie ryzyk

organizacji i związanych z nimi zagrożeń, ponieważ odnoszą się one do jej unikalnego środowiska sieciowego, ma kluczowe znaczenie dla zapewnienia prawidłowego zarządzania nimi. Właściwe zarządzanie ryzykiem związanym z bezpieczeństwem technicznym zaczyna się od bezpiecznego projektu, a kończy na wdrożeniu bezpiecznych kontroli technicznych w celu dalszego wspierania bezpiecznego projektu. Wyrażenie „chrupiące na zewnątrz, miękkie i łatwe do pogryzienia w środku" ma bezpośredni wpływ na ten szczególny rodzaj zarządzania. Kontrole łagodzące mogą zapewnić chrupiący obwód, ale bezpieczna konstrukcja zapobiega przeżuwaniu wnętrza w przypadku awarii kontroli obwodu. W tej sekcji omówimy priorytetowe kwestie projektowe, które sprzyjają bezpiecznej sieci bezprzewodowej w przedsiębiorstwie. Tym rozważaniom projektowym powinny towarzyszyć omówione wcześniej techniczne środki kontroli łagodzącej, aby zapewnić zdrowe podejście. Integracja i dopuszczenie różnych rodzajów technicznych środków kontroli łagodzących, takich jak metody EAP, identyfikatory SSID, infrastruktury PKI, certyfikaty AP lub konfiguracje suplikantów podczas początkowej fazy projektowania sieci bezprzewodowej, może zwiększyć ich skuteczność, ponieważ działają one jako całość, w przeciwieństwie do sytuacji po fakcie dodatki.

Zalety architektury kontrolera bezprzewodowego.

Sprzęt sieci bezprzewodowej dla przedsiębiorstw jest dostępny w dwóch podstawowych odmianach: cienkie (lekkie) i grube (autonomiczne) punkty dostępowe. Te dwa typy projektów będą miały duży wpływ na sposób obsługi i zarządzania siecią bezprzewodową oraz zakres dostępnych kontroli w celu jej zabezpieczenia.

* Athick AP posiada dużo inteligencji i funkcji poza podstawowymi funkcjami 802.11 lub RSN. Funkcje te obejmują usługi pomocnicze, takie jak DHCP, SNMP, QOS, zapory itp. Chociaż tego typu usługi zdecydowanie mają swoje miejsce, z punktu widzenia zarządzania synchronizacja konfiguracji między grubymi klientami lub różnymi dostawcami może być trudna.

* Punkty dostępowe Thin Client to punkty dostępowe typu bare-bone, które implementują tylko niezbędne funkcje 802.11/RSN. Przedsiębiorstwa powinny wykorzystywać punkty dostępowe dla klientów uproszczonych, aby obniżyć koszty i zwiększyć bezpieczeństwo zarządzania siecią bezprzewodową. Te punkty dostępowe wykorzystują podłączony sprzęt przełącznika lub dedykowane kontrolery bezprzewodowe w celu uzyskania informacji i ustawień konfiguracyjnych. Po uruchomieniu i inicjalizacji cienki klient wykryje, skontaktuje się i pobierze najnowsze ustawienia konfiguracyjne. Bezpieczeństwo zapewniane przez środowisko cienkiego klienta wykracza poza łatwość zarządzania urządzeniami, zapewniając następujące dodatkowe korzyści:

* Fizyczne zabezpieczenie danych konfiguracyjnych: konfiguracja grubego klienta może zostać naruszona przez fizyczną kradzież i analizę. Cienki klient przechowuje konfigurację typu „bare bone", aby umożliwić łączność 802.11, współdzielone klucze tajne RADIUS i ciągi SNMP; inne przechowywane informacje o konfiguracji są przechowywane na przełączniku zaplecza lub kontrolerze bezprzewodowym

* Mesh Security Functions: Powszechna forma komunikacji między punktami dostępowymi, taka jak Lightweight Access Point Protocol (LWAPP)39, umożliwia powszechną komunikację między punktami dostępowymi i kontrolerami w całym przedsiębiorstwie. Ten mechanizm komunikacji w połączeniu z fizyczną obecnością punktów dostępowych w lokalizacjach głównych i zdalnych umożliwia wykorzystanie ich do funkcji bezpieczeństwa. Wykorzystanie klienckich punktów dostępowych do monitorowania bezpieczeństwa może być korzystne z punktu widzenia oszczędności kosztów na rzecz dedykowanego systemu WIDS, aczkolwiek przy braku funkcjonalności.

- Wykrywaj nieuczciwe punkty dostępowe za pomocą technik wykrywania nieuczciwego dostępu do infrastruktury AP. Istnieją rozwiązania specyficzne dla dostawców, które wykorzystują punkty dostępowe obsługujące klientów do chwilowego skanowania w poszukiwaniu fałszywych sygnałów nawigacyjnych AP, które nie są częścią sieci LWAPP.

- Punkt dostępowy można ustawić w roli wykrywania i podłączyć do portu analizatora portów przełączanych (SPAN), aby wyśledzić potencjalne nieuczciwe sygnały nawigacyjne AP dla wewnętrznej łączności sieciowej

Segmentacja sieci.

Podstawowa sieć bezprzewodowa powinna być podzielona na dwa sposoby. Po pierwsze, sieć bezprzewodowa powinna być podzielona na segmenty z wewnętrznej sieci LAN, a po drugie, sieci bezprzewodowe powinny być podzielone na sieci bezprzewodowe o różnych zastosowaniach biznesowych. Ponadto podczas procesu segmentacji należy rozważyć umieszczenie czujnika WIDS z możliwością fizycznego pokrycia wszystkich obszarów sieci przewodowej.

Segmentacja punktów końcowych sieci przewodowej i bezprzewodowej.

Sieci przewodowe zwykle przypisują sieci VLAN na podstawie portu lub adresu MAC. W przypadku przypisywania sieci VLAN na podstawie portów zarządzanie w dużej mierze opiera się na prawidłowej konfiguracji przełączników warstwy dostępu, konfiguracji portów trunkingowych dla uplinków oraz eliminowaniu propagacji wrażliwych sieci VLAN w różnych lokalizacjach fizycznych. Zmiany operacyjne mogą dyktować aktualizację wielu przełączników w przypadku stosunkowo niewielkich ruchów. W przypadku przypisania sieci VLAN na podstawie przewodowego adresu MAC, należy użyć przełącznika obsługującego uwierzytelnianie MAC i serwerów RADIUS zaplecza dla mapowania MAC->VLAN. Przypisywanie sieci VLAN oparte na adresach MAC może poprawić możliwości zarządzania i nadzoru, ale stwarza poważne zagrożenie bezpieczeństwa, ponieważ są one podatne na fałszowanie adresu MAC, co może umożliwić atakującemu dostęp do wrażliwych sieci VLAN poprzez fałszowanie adresu MAC uwierzytelnionego urządzenia. W środowisku bezprzewodowym sieci VLAN można przypisywać na podstawie identyfikatora SSID lub grupy użytkowników, a działania administracyjne związane z udostępnieniem użytkownikowi sieci VLAN można znacznie ograniczyć lub całkowicie usunąć. Użytkownik nie jest już ograniczony do określonej fizycznej lokalizacji, aby uzyskać dostęp do wymaganej sieci VLAN, ponieważ niezbędny identyfikator SSID może być dostępny w dowolnym miejscu na terenie kampusu. W przypadku rozszerzenia wdrożenie nowego cienkiego punktu dostępowego w bliskiej odległości zapewni niezbędne sieci VLAN, dla których skonfigurowany jest profil suplikanta klienta. Ponieważ przypisanie sieci VLAN może być kontrolowane przez pomniejsze konfiguracje suplikantów klienta i uprawnienia RADIUS zaplecza, segmentację można określić podczas procesu udostępniania zasobów, a następnie wymagać stosunkowo niewielkiego zarządzania.

Segmentacja z przewodowej sieci LAN.

Ze względu na publiczną dostępność bezprzewodowej transmisji radiowej (szyfrowanej lub nie), należy zająć się segmentacją w ramach istniejącej sieci LAN, aby zmniejszyć ryzyko pełnego dostępu wewnętrznego z powodu wygaśnięcie zabezpieczeń bezprzewodowych. Solidna postawa bezpieczeństwa sieci zakłada, że szczególnie ryzykowny segment może zostać naruszony i ma na celu złagodzenie szkód spowodowanych taką katastrofą. Wartość segmentacji bezprzewodowej sieci LAN od przewodowej sieci LAN opiera się na możliwości zabezpieczenia się przed następującymi zdarzeniami, które mogą prowadzić do naruszenia bezpieczeństwa sieci LAN ze zdalnej lokalizacji, takiej jak parking firmowy.

* Złośliwe wykorzystanie zhakowanych danych uwierzytelniających opartych na nazwie użytkownika/hasło pracownika za pośrednictwem wiadomości e-mail typu spear phishing lub innej kradzieży.

* Błędna konfiguracja kontroli bezpieczeństwa sieci bezprzewodowej, taka jak słaba implementacja EAP (EAP-LEAP lub brak weryfikacji certyfikatu AP w EAP-PEAP-MSCHAP-v2), która może być wykorzystywana do ataków podszywania się na słownik lub RADIUS.

* Nieuczciwe „hotspotting" AP laptopów pracowników w celu nawiązania łączności i narażenia punktu końcowego na eksploatację usług lub ruchu HTTP MITM. Gdy punkt końcowy zostanie podłączony do legalnej sieci bezprzewodowej przedsiębiorstwa, osoba atakująca może uzyskać dostęp do sieci LAN.

Potrzeba segmentacji ruchu bezprzewodowego wynika z nieodłącznego braku fizycznej kontroli ruchu 802.11 i zasięgu dostępności. Zewnętrzny atak na strefę DMZ lub inne urządzenie z dostępem do Internetu może prowadzić do naruszenia zasobów strefy DMZ, ale mechanizmy kontrolne zazwyczaj występują w postaci wieloodcinkowych lub warstwowych zapór ogniowych, które ograniczają ekspozycję z sieci DMZ i uniemożliwiają bezpośrednią łączność LAN. Ten rodzaj segmentacji powinien być stosowany w środowisku bezprzewodowym z podobnych powodów, aczkolwiek o różnych wektorach ataku.

VPN przez sieć bezprzewodową.

W zależności od przeznaczenia sieci bezprzewodowej, użytkownicy mogą wymagać takiego samego dostępu w sieci bezprzewodowej, jaki zapewnia przewodowa sieć LAN. Na korzyść udostępnienia sieci bezprzewodowej całej przewodowej sieci LAN można zastosować rozwiązanie VPN. Taka architektura umożliwiłaby dostęp sieci bezprzewodowej do Internetu, tylko bramy VPN lub innych podstawowych zasobów wewnętrznych (takich jak witryna intranetowa), które wymuszają użycie bramy VPN dla wszelkich innych zasobów. Dodatkową siłą zapewnianą przez VPN, oprócz uwierzytelniania bezprzewodowego, jest dogłębna ochrona. Aby uzyskać dostęp do wewnętrznej sieci LAN z sieci bezprzewodowej, osoba atakująca musi złamać zabezpieczenia i uzyskać dostęp do sieci VPN oprócz wszelkich mechanizmów uwierzytelniania bezprzewodowego/kontroli dostępu w warstwie 2. Atakujący, który uzyska dostęp do bezprzewodowego medium, prawdopodobnie nigdy nie podejrzewałby korzystania z VPN i zakładał stan ograniczonego dostępu wewnętrznego lub pomyliłby obecny stan z całą siecią LAN. Należy przeprowadzić ocenę, aby zrozumieć przypadek biznesowy, w którym zasoby bezprzewodowe wymagają pełnego dostępu do firmowej sieci LAN i wyraźnego zezwolenia na dostęp na podstawie adresu IP/portu. Szczegółową segmentację można uzyskać, wykorzystując przypisania sieci VLAN na podstawie SSID, wyjaśnione szczegółowo w kolejnych sekcjach, w celu przypisania ograniczeń dla poszczególnych sieci VLAN z obsługą list ACL w wyższych punktach sieci.

Segmentacja sieci bezprzewodowej.

Segmentacja międzysieciowa umożliwia różnym typom użytkowników łączenie się z różnymi identyfikatorami SSID dostarczanymi przez ten sam fizyczny punkt dostępu i zapewnianie różnych uprawnień dostępu w oparciu o sieć. Proces segmentacji każdego identyfikatora SSID we własnej sieci zwykle obejmuje tagowanie VLAN na poziomie punktu dostępowego w celu rozróżnienia ruchu warstwy 2 poprzez wymuszenie przepływu komunikacji między sieciami VLAN przez zaporę sieciową lub router upstream z listami ACL opartymi na sieci VLAN/IP. Systemy katalogowe zaplecza, takie jak LDAP, mogą być wykorzystywane przez nowoczesne punkty dostępowe do podejmowania decyzji o przypisaniu sieci VLAN, jakie otrzyma dany użytkownik, niezależnie od identyfikatora SSID, pod którym aktualnie się znajduje. Dynamiczne systemy oparte na katalogach zaplecza nie są całkowicie

bezpieczne ze względu na to, że adresy MAC są używane jako unikalny agent identyfikacji. Ten rodzaj segmentacji może być wymuszony w warstwie sieciowej, poprzez wspomniany wcześniej firewall VLAN lub poprzez listy dostępu VPN, jeśli dostęp bezprzewodowy pracowników jest wymuszony przez tunel VPN w celu komunikowania się z zasobami LAN.

Zalety i wady segmentacji opartej na SSID/VLAN.

Zalety segmentacji opartej na SSID/VLAN obejmują:

* Zróżnicowane traktowanie użytkowników bezprzewodowych według grupy lub SSID; na przykład,

* Identyfikator SSID „sprzedaż korporacyjna" i „firma-hr" może zapewniać różne poziomy dostępu. Najlepszą praktyką byłoby ukrycie i zamaskowanie nazw SSID, aby zaciemnić ich cel osobie z zewnątrz.

* Łatwość administrowania siecią poprzez eliminację konieczności przypisywania sieci VLAN na podstawie perportu. Przypisanie sieci VLAN opartej na identyfikatorze SSID wymaga jedynie konfiguracji punktu końcowego, aby zapewnić, że punkt końcowy zapewnia poświadczenia niezbędne do uwierzytelnienia przy określonym identyfikatorze SSID.

Wadą segmentacji opartej na SSID/VLAN jest zwiększone obciążenie sieci bezprzewodowej i zmniejszona wydajność z powodu wielu wymagań dotyczących pamięci SSID.

Podsumowanie kontroli segmentacji sieci bezprzewodowej

* Segmentacja sieci LAN: chroni wewnętrzną sieć LAN w przypadku naruszenia bezpieczeństwa sieci bezprzewodowej poprzez VLAN i bezprzewodowe listy ACL zapory sieciowej oparte na IP.

* Sieci VPN mogą być używane przez medium bezprzewodowe, aby umożliwić użytkownikom dostęp do zasobów sieci LAN.

* Segmentacja sieci wewnątrzprzewodowej:

* Na podstawie SSID: użycie oddzielnych identyfikatorów SSID dla różnych przypadków biznesowych można łatwo mapować do sieci VLAN i zapewniać różne poziomy segmentacji.

* W oparciu o grupy: przypisanie VLAN oparte na RADIUS dla bieżących uprawnień grupowych użytkownika bezprzewodowego

Segmentacja użytkowników.

Serwer RADIUS może podejmować zaawansowane decyzje dotyczące autoryzacji dla prawidłowego dopasowania nazwy użytkownika/hasła. Wykorzystanie wyznaczonych grup użytkowników w procesie autoryzacji może zapewnić precyzyjną kontrolę nad tym, którzy użytkownicy mogą korzystać z sieci bezprzewodowej podzielonej na duże odległości. Jeśli wiadomo, że administratorzy domeny, użytkownicy zaawansowani lub konta usług ogólnych nigdy nie powinni mieć możliwości uwierzytelniania za pośrednictwem połączenia bezprzewodowego, można im niejawnie odmówić członkostwa w grupie użytkowników bezprzewodowych. Każda grupa użytkowników, która wymaga możliwości uwierzytelniania przez sieć bezprzewodową, powinna być członkiem tej grupy. Domyślna implementacja RSN, która może i będzie autoryzować dowolnego użytkownika w podanym katalogu, może stać się ofiarą ataków na konta domyślne, nieaktywne, gościnne lub testowe w wyznaczonym katalogu. Konta testowe mogą być podatne na słabe hasła kanoniczne (np. „testowe" lub „hasło") ze względu na ich utworzenie na wczesnych etapach tworzenia oprogramowania lub katalogów lub za pomocą innych środków, które omijają firmową politykę haseł. Gdy w grę wchodzi mechanizm uwierzytelniania nazwy użytkownika/hasła, atakujący może próbować podstawowych ataków brute-

force, aby uzyskać dostęp do sieci za pomocą standardowych kont testowych lub kont gości. Wiele organizacji nie uważa, że jest to poważny problem, ale gdy katalog zawiera tysiące kont, a organizacje nie przeprowadzają regularnych audytów, łatwo jest prześlizgnąć się przez szczeliny. Korzystanie z wyznaczonej grupy bezprzewodowej:

* Zmniejsza obszar ataku, nawet jeśli przeciwnik jest w stanie uzyskać listę kont użytkowników i wykorzystać je do brutalnego wymuszenia sieci bezprzewodowej przy użyciu podstawowych haseł.

* Zmniejsza liczbę punktów końcowych z zapisanymi lub zapamiętanymi profilami sieciowymi, które mogą zostać zaatakowane i użyte do przechwytywania skrótów wyzwań związanych z nazwą użytkownika/hasłem w hotspotu lub ataku typu personifikacja RADIUS.

NARZĘDZIA KONTROLI BEZPIECZEŃSTWA.

W tej sekcji przyjrzymy się dostępnym narzędziom open source i komercyjnym, które pomagają w audycie środowiska bezprzewodowego i zrozumieniu narzędzi, które sterowniki wojenne mają do atakowania sieci.

UWAGI KOŃCOWE.

Wygoda i zwiększająca się przepustowość sieci bezprzewodowych nieuchronnie spowodują dalszy wzrost zarówno ulepszeń technologicznych, jak i wdrożeń. Menedżerowie sieci i bezpieczeństwa muszą nadal monitorować te zmiany i podejmować odpowiednie działania w celu zabezpieczenia wszystkich swoich systemów przed stale ewoluującymi zagrożeniami dla bezpieczeństwa informacji.