nadkom. Artur Lepalczyk

Zakład Kryminalny
Szkoły Policji w Pile

Bezpieczeństwo sieci Wi-Fi

Dziś niemal każdy użytkownik Internetu ma do niego dostęp praktycznie wszędzie dzięki globalnej sieci i szybkiemu światłowodowi. Często dostęp ten zapewniają operatorzy telefonii komórkowej w ramach pakietów abonamentowych, co pozwala korzystać z Internetu na telefonie z zadowalającą prędkością. Jednak w wielu przypadkach ludzie korzystają z Internetu od lokalnych dostawców usług. Dzięki temu w swoim domu każdy może wybierać spośród wielu ofert różnych firm, aby dopasować usługę do swoich potrzeb i wymagań.

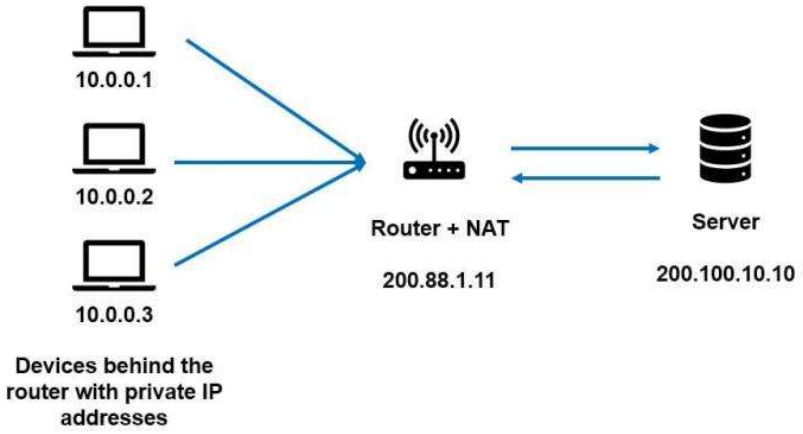
Obecnie wielu dostawców usług umożliwia korzystanie z usługi z prędkością 300 Mb/s, 600Mb/s jak również 1Gb/s danych i cały czas te prędkości są zwiększane, dając możliwość uzyskania nawet 2,5Gb/s danych. Każda z tych prędkości w bardzo komfortowy sposób umożliwia korzystanie z usługi Internet, także na wielu urządzeniach - korzystając z jednego łącza internetowego. Aby umożliwić korzystanie z jednego łącza internetowego na wielu urządzeniach należy zbudować sieć typu LAN dającą możliwość dzierżawy łącza internetowego. Dzięki temu przy zastosowaniu technologii NAT możliwe jest korzystanie z jednej usługi na kilku, a nawet kilkuset urządzeniach, w zależności od konfiguracji urządzeniach jakim jest ROUTER.

Router (ruter, w dosłownym tłumaczeniu – trasownik, pol. wym. ['rutɛr]) – jest urządzeniem sieciowym działającym w trzeciej warstwie modelu OSI. Służy przede wszystkim do łączenia różnych sieci komputerowych (różnych w sensie informatycznym, czyli np. o różnych klasach, maskach), pełni więc rolę węzła komunikacyjnego. Na podstawie informacji zawartych w pakietach TCP/IP jest w stanie przekazać pakiety z dołączonej do siebie sieci źródłowej do docelowej, wybierając ją spośród połączonych ze sobą sieci. Proces kierowania ruchem nosi nazwę trasowania, routingu lub routowania.[1]

Dzięki zastosowaniu technologii routingu w routerach możliwe jest ukierunkowanie odpowiedniego pakietu danych do właściwego urządzenia sieciowego. Procesem routingu sterują protokoły routingu, które określają sposób kierowania pakietami routowalnego protokołu sieciowego, czyli protokołu dopuszczającego kierowanie przepływem pakietów. Przykładem jest tu protokół IP (Internet Protocol).

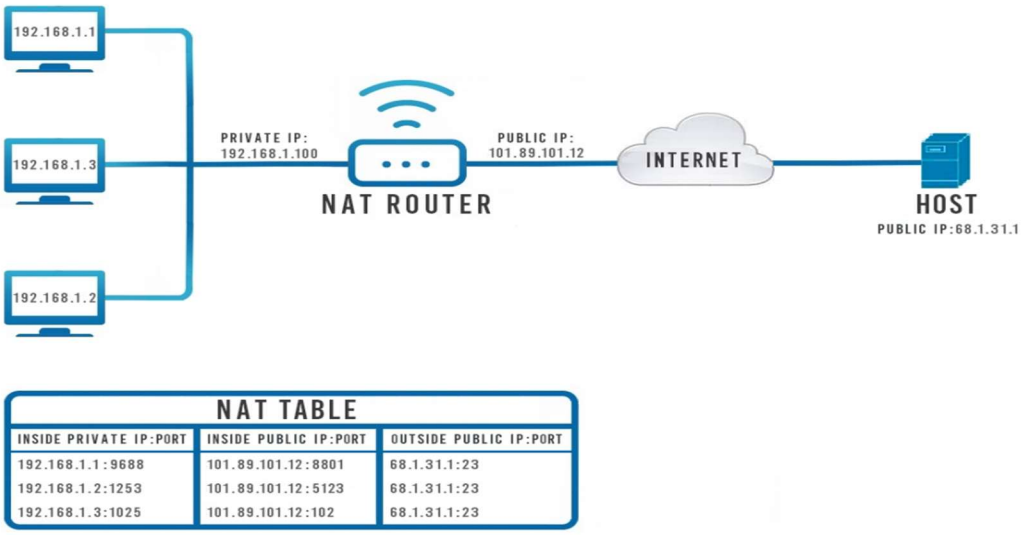
Routery mogą obsługiwać wiele protokołów routingu oraz wiele protokołów routowalnych. Mamy wówczas do czynienia z routingiem wieloprotokołowym. [2]

[1] https://pl.wikipedia.org/wiki/Router
[2] https://sieci.infopl.info/index.php/urzadzenia/routing



Rys. 1. Przykład budowy sieci LAN + Wi-Fi z wykorzystaniem NAT
Źródło: https://ottverse.com/what-is-nat-network-address-translation-webrtc/

Aby móc korzystać z Internetu - na bazie łącza dzierżawionego - wykorzystuje się technologię NAT zastosowaną w routerach. Dzięki zastosowaniu technologii NAT w routerach możliwe jest uzyskanie dostępu do Internetu na każdym urządzeniu będącym w danej strukturze sieci lokalnej LAN skonfigurowanego i działającego w obszarze tego urządzenia. NAT działa poprzez zastosowanie mass-radradingu IP, który jest techniką polegującą na ukryciu całej przestrzeni adresów IP, składających się zwykle z prywatnych adresów IP, za jednym adresem IP w innym, zwykle publicznym miejscu. Adres, który musi być ukryty podmieniany jest na jeden (publiczny) adres IP jako "nowy" adres źródłowy wychodzącego pakietu IP, tak aby wyglądał jako pochodzący nie z ukrytego hosta, ale z samego urządzenia routingowego. [3]



Rys. 2. Przykład sieci LAN - NAT ROUTER i tabela Routingu.
Źródło: https://wiki.teltonika-networks.com/view/Network_Address_Translation

[3] https://wiki.teltonika-networks.com/view/Network_Address_Translation

Obecne na rynku routery umożliwiają budowanie wewnętrznych sieci zarówno z wykorzystaniem okablowania sieciowego LAN, jak również technologii bezprzewodowych Wi-Fi.

Czym jest zatem WiFi? Wi-Fi, wi-fi[a] (wym. [ˈvʲifʲi]; ang. Wi-Fi, wym. [ˈwaɪfaɪ]) – stanowi zestaw standardów stworzonych do budowy bezprzewodowych sieci komputerowych. Szczególnym zastosowaniem standardu wi-fi jest budowanie sieci lokalnych (LAN) opartych na komunikacji radiowej, czyli WLAN (wireless local area network), pozwalając tym samym na budowanie sieci LAN bez wykorzystania okablowania sieciowego Ethernet.

Wi-fi bazuje na takich protokołach warstwy fizycznej, jak:

- DSSS (*ang. Direct Sequence Spread Spectrum*), umożliwiającym bezpośrednie modulowanie nośnej sekwencją kodową, dając możliwość rozpraszania widma (pasma) w systemach szerokopasmowych z wykorzystaniem ciągów kodowych;
- FHSS (*ang. Frequency Hopping Spread Spectrum*), stanowi metodę rozpraszania widma (pasma) w systemach szerokopasmowych;
- OFDM (*ang. Orthogonal Frequency-Division Multiplexing*) stanowi metodę zwielokrotnienia w dziedzinie częstotliwości polegającej na jednoczesnej transmisji wielu strumieni danych na ortogonalnych częstotliwościach nośnych.

Zaletą budowy sieci wewnętrznych w oparciu o technologie Wi-Fi jest przede wszystkim prosta i szybka możliwość budowania dużych sieci bez wykorzystania okablowania strukturalnego. W przypadku budowy sieci wewnętrznych opartych na technologii bezprzewodowej Wi-Fi wykorzystywane są standardy IEEE 802.11.

Standardy sieci Wi-Fi IEEE 802.11 to wprowadzane na przestrzeni lat przez firmę Wi-Fi Alliance technologie sieci bezprzewodowej. Do najbardziej znanych standardów należą:

- 802.11, jest to standard sieci pracujący na paśmie 2.4 GHz umożliwiający transmisję danych na poziomie 1-2Mb/s wykorzystujący modulację typu FHSS oraz DSSS;
- 802.11 b, jest to standard sieci pracujący na paśmie 2.4 GHz umożliwiający transmisję danych na poziomie 1-11Mb/s wykorzystujący modulację typu DSSS;
- 802.11 a, jest to standard sieci pracujący na paśmie 5 GHz umożliwiający transmisję danych na poziomie 6-54Mb/s wykorzystujący modulację typu OFDM;
- 802.11 g, jest to standard sieci pracujący na paśmie 2.4 GHz umożliwiający transmisję danych na poziomie 6-54Mb/s wykorzystujący modulację typu DSSS oraz OFDM;
- 802.11 n (Wi-Fi 4), jest to standard sieci pracujący na paśmie 2.4 oraz 5 GHz umożliwiający transmisję danych na poziomie 72-600Mb/s wykorzystujący modulację typu OFDM;
- 802.11 ac (Wi-Fi 5), jest to standard sieci pracujący na paśmie 5 GHz umożliwiający transmisję danych na poziomie 433-6928Mb/s wykorzystujący modulację typu OFDM;
- 802.11 ax (Wi-Fi 6, 6E) jest to standard sieci pracujący na paśmie 2.4, 5 oraz 6 GHz umożliwiający transmisję danych na poziomie 574-9608Mb/s wykorzystujący modulację typu BPSK (*Binary Phase Shift Keying*), QPSK (*Quadrature Phase Shift Keying*), QAM (*Quadrature Amplitude Modulation*);
- 802.11 be (Wi-Fi 7) jest to standard sieci pracujący na paśmie 2.4, 5 oraz 6 GHz umożliwiający transmisję danych na poziomie ponad 40Gb/s wykorzystujący modulację typu OFDMA (Orthogonal frequency-division multiple access, czyli wielodostęp z ortogonalnym

podziałem częstotliwości). OFDMA umożliwia podział przesyłanych danych na mniejsze pakiety, jak również pozwala na podział kanałów na mniejsze częstotliwości nazywane podnośnymi. Poprawia tym samym łączność radiową i efektywność sieci bezprzewodowych.

Standardy te różnią się pomiędzy sobą pod względem parametrów, jakie pozwalają uzyskać, m.in.:

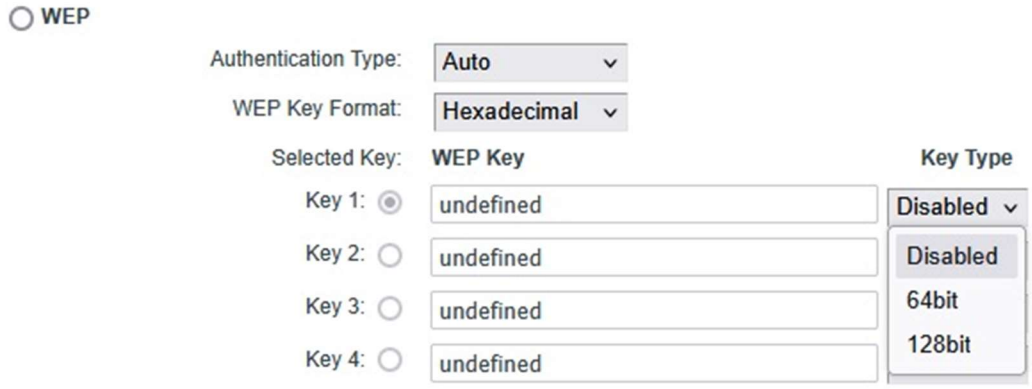
- przepustowości sieci,
- stabilności,
- zasięgu,
- wydajności,
- maksymalnej prędkości połączenia,
- opóźnień w transmisji,
- stosowanych technologii zabezpieczeń dostępu.

Przy budowaniu sieci opartych na technologii Wi-Fi kluczowe znaczenie ma bezpieczeństwo. Dotyczy to bezpośredniego połączenia między urządzeniami sieci oraz przesyłania danych między urządzeniami sieciowymi. Znajomość zasad bezpieczeństwa sieci bezprzewodowych może uchronić użytkownika przed nieuprawnionym dostępem do sieci, pozyskaniem posiadanych przez nas jako użytkowników prywatnych danych, jak również może uchronić przed cyberatakami, czyli aktywnością niepożądanych osób i cyberprzestępstwami, których to użytkownik sieci może stać się potencjalną ofiarą. Należy zwrócić uwagę na to, że budując sieć wewnętrzną opartą głównie na technologii Wi-Fi - istnieje możliwość połączenia się taką siecią za pośrednictwem każdego urządzenia posiadającego wbudowaną kartę sieciową lub urządzenia rozbudowanego o kartę sieciową Wi-Fi - mogą być to komputery stacjonarne, laptopy, tablety, telefony komórkowe, konsole, telewizory itp. Budowanie sieci wewnętrznych opartych na technologii bezprzewodowej transmisji powinno się w szczególności opierać na kwestii zapewnienia właściwego bezpieczeństwa.

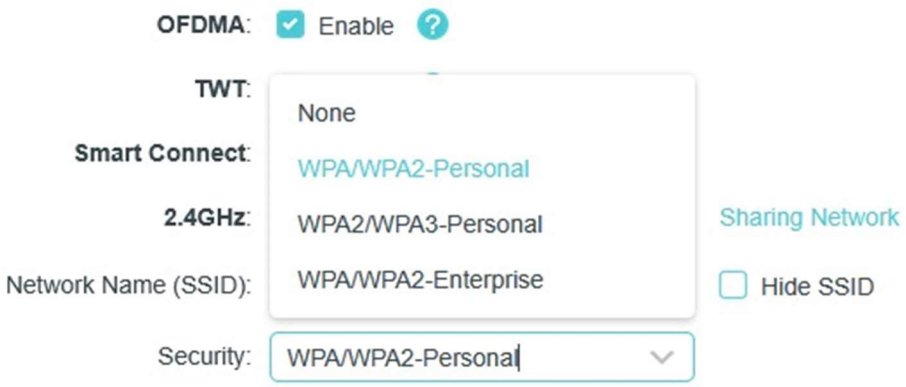
Biorąc pod uwagę bezpieczeństwo sieci bezprzewodowych, w pierwszej kolejności należy wziąć pod uwagę szyfrowanie sieci. Nieszyfrowane sieci bezprzewodowe stanowią „łakomy kąsek" dla cyberprzestępców, a to dlatego, że występuje tutaj pełny dostęp do wewnętrznej sieci bezprzewodowej, jak również dostęp do połączonych do tej sieci urządzeń końcowych. W przypadku podłączenia się pod niezabezpieczoną sieć bezprzewodową istnieje możliwość w dość prosty sposób „podsłuchać" przesyłane w obrębie danej sieci pakiety danych. To także okoliczność, która daje możliwość cyberprzestępcy posłużenia się w obrębie takiej sieci zaimplementowania złośliwego oprogramowania umożliwiającego przejęcie pełnej kontroli nad urządzeniami podłączonymi w takiej niezabezpieczonej sieci, a także pozyskanie danych, do których taka osoba nie jest uprawniona. Niezabezpieczenie posiadanej własnej sieci bezprzewodowej w dobie dzisiejszej przestępczości internetowej może przyczynić się do zaistnienia przestępstw związanych z nielegalnym pozyskaniem danych osobowych, nielegalnego przejęcia kont bankowych oraz kradzieży zgromadzonych środków pieniężnych, jak i innych przestępstw. Bezpieczeństwo sieci bezprzewodowych wiąże się z wykorzystaniem odpowiedniego hasła oraz klucza szyfrującego, uniemożliwiając tym samym dostęp do zbudowanej sieci osobom nieuprawnionym. Bez odpowiedniego uwierzytelnienia użytkownika danej sieci nie jest możliwe pozyskanie adresów IP przydzielanych przez router, który zarządza daną siecią.

Po prostu informacja przesyłana bezprzewodową transmisją danych jest niezrozumiała i zarazem niedostępna dla nieautoryzowanych użytkowników. Na przełomie kilku lat i zmian standardów sieci bezprzewodowej Wi-Fi rozróżnia się wiele algorytmów szyfrujących. Obecnie rozróżnia się cztery algorytmy szyfrujące i są nimi: WEP, WPA, WPA-2 i WPA-3.

Poniżej przedstawiono możliwości wyboru klucza szyfrującego przy konfigurowaniu routera. Jest to uzależnione od rodzaju posiadanego routera oraz standardu zabezpieczeń jaki oferuje użytkownikowi dany model routera.



Rys. 3. Przykład możliwości szyfrowania łącza bezprzewodowego z wykorzystaniem klucza szyfrującego WEP.
Źródło: Opracowanie własne.



Rys. 4. Wybór możliwości szyfrowania łącza bezprzewodowego z wykorzystaniem klucza szyfrującego WPA.
Źródło: Opracowanie własne.

Wraz z rozwojem technologicznym, kiedy to routery otrzymały możliwość budowania sieci w oparciu o technologię sieci bezprzewodowej Wi-Fi zastanawiano się, jak skutecznie zabezpieczać transmisje danych. W 1999 roku wprowadzono mechanizm szyfrujący WEP (*Wired Equivalent Privacy*) jako oryginalną część standardu IEEE 802.11, działający na zasadzie współdzielonego klucza szyfrującego o długości od 40 do 104 bitów i 24-bitowym wektorze inicjującym. Niestety, okazał się bardzo nieskuteczny.[4] Algorytm szyfrujący WEP był obsługiwany w routerach dając możliwość zabezpieczenia swojej sieci bezprzewodowej, jednakże

[4] https://odo24.pl/blog/jak-bezpiecznie-korzystac-z-wi-fi.php.zamow-rozmowe

z uwagi na liczne błędy, a zarazem słaby klucz szyfrujący RC4 oraz sumę kontrolną CRC-32 dającą się w dość łatwy sposób rozszyfrować, nie powinien być obecnie wykorzystywany. Algorytm szyfrujący WEP umożliwiał zastosowanie klucza o długości 64 bit oraz 128 bit, choć także była wersja 256 bit, która niestety się nie przyjęła jako oferowany standard. W RC4 tekst jawny jest szyfrowany przy pomocy operacji XOR ze strumieniem klucza, tworząc szyfrogram.[5]

Klucz symetryczny RC4 jest podatny na ataki polegające na analizie danych zaszyfrowanych tym samym kluczem, dlatego strumień klucza nie może się powtarzać, ponadto klucz RC4 zastosowany WEP jest stosunkowo krótki, co za tym idzie zdecydowano się na wprowadzenie zabezpieczenia kryptograficznego, polegającego na użyciu tzw. wektora inicjującego (IV). W przypadku WEP jest to 24-bitowa liczba, zmieniana dla każdego transmitowanego pakietu. Jest on konkatenowany wraz z kluczem podanym przez użytkownika (który jest stały), tworząc unikatowy dla każdego pakietu klucz algorytmu RC4. Ze względu na rozmiar IV, długość klucza użytkownika może wynosić 40 bitów (dla klucza RC4 o rozmiarze 64) lub 104 bity (dla klucza RC4 o rozmiarze 128). Wobec tego w ramach standardu 802.11 na podstawie długości klucza określono dwie wersje WEP-40 oraz WEP-104 oraz adekwatnie do wersji klucza jego budowa stanowiła 10 lub 26 cyfr heksadecymalnych.[6]

Opcjonalnie wprowadzono możliwość podawania klucza jako ciągu znaków ASCII – w takim jednak wypadku, ze względu na konieczność użycia znaków drukowalnych, rozmiar przestrzeni wszystkich dostępnych kluczy jest znacząco zredukowany.[7]

Z uwagi na słabe strony klucza szyfrującego WEP oraz łatwą możliwość złamania hasła zabezpieczającego zaistniała konieczności szybkiego poprawienia błędów mających wpływ na bezpieczeństwo sieci bezprzewodowych, a tym samym do wprowadzenia nowego standardu zabezpieczenia.

Wady bezpieczeństwa protokołu WEP można podsumować następująco:

- słabości algorytmu RC4 przeniesione na WEP ze względu na metodę generowania klucza,
- zbyt krótki wektor inicjalizacyjny (WI) (24 bity – wystarczy niecałe 5000 pakietów, by osiągnąć 50% prawdopodobieństwo kolizji) i dopuszczenie powtórnego wykorzystania tego samego WI (brak ochrony przed atakami z powtórzeniem wiadomości),
- brak przyzwoitego sprawdzania integralności (algorytm CRC32 nadaje się do wykrywania błędów, ale nie jest kryptograficznie bezpieczny ze względu na swą liniowość),
- brak wbudowanej metody aktualizacji kluczy.[8]

Wynikiem tego w 2003 roku nastąpiło masowe, a zarazem szybkie wdrożenie standardu szyfrowania WPA (*Wi-Fi Protected Access*). Klucz szyfrujący WPA zawiera niektóre zmiany zaprojektowane dla 802.11i mające zlikwidować największe podatności klucza szyfrującego WEP.

[5] https://sekurak.pl/bezpieczenstwo-sieci-wi-fi-czesc-3-wep/
[6] Ibidem
[7] Ibidem
[8] Guillaume Lehembre - Bezpieczeństwo WIFI-WEP,WPA i WPA2 - hakin9 Nr 1/2006 s. 14

Najważniejsze problemy WEP, które postanowiono rozwiązać w 802.11i to:

1) ochrona współdzielonego klucza ukierunkowana na bezpieczeństwo jego ochrony,
2) bezpieczeństwo szyfrowania – hasło stanowiące dostęp do sieci stanowi wspólny klucz szyfrujący, co osłabia bezpieczeństwo,
3) uwierzytelnianie – brak wsparcia dla zaawansowanych technologii uwierzytelniania pozwalających na identyfikację poszczególnych użytkowników, a nie z wykorzystaniem współdzielonego sekretu (przykładami mogą być indywidualny login/hasło lub certyfikaty),
4) zmienność klucza – brak mechanizmu zapewniającego odpowiednią częstotliwość zmiany klucza,
5) integralność – słabe mechanizmy zapewniające integralność danych.[9]

Standard szyfrujący WPA wykorzystuje funkcjonalnie dwa rodzaje protokołów: TKIP (Temporal Key Integrity Protocol) i EAP (Extensible Authentication Protocol). Protokół TKIP wykorzystywany jest do zabezpieczenia warstwy łącza danych modelu OSI w sieciach bezprzewodowych i miał rozwiązać najważniejsze problemy swojego poprzednika. Protokół TKIP wykorzystuje tak jak protokół WEP algorytm szyfrujący RC4 oparty na nowych mechanizmach, mających znaczny wpływ na bezpieczeństwo ochrony przed potencjalnymi atakami, stając się protokołem bardziej odpornym na potencjalne ataki niż protokół WEP. Protokół TKIP zbudowany jest z trzech protokołów:

1) kryptograficznego algorytmu integralności komunikatów,
2) algorytmu mieszania kluczy (Per Packet Key),
3) rozszerzenia wektora początkowego.

Jednym z zastosowanych nowych mechanizmów bezpieczeństwa klucza WPA w oparciu o rozbudowany klucz RC4 jest generowanie innego klucza dla każdego przesyłanego pakietu. CRC-32, czyli cykliczny kod nadmiarowy, został tu zastąpiony przez nowy kod integralności MIC (Message Integrity Check – gwarantujący integralność przesyłanych danych) o nazwie Michael. Został on utworzony specjalnie na potrzeby klucza TKIP. Algorytm klucza TKIP wykorzystuje unikatowy klucz, który jest mieszany ze źródłowym i docelowym adresem MAC, całym fragmentem pakietu zawierającym niezaszyfrowane dane.

Zastosowanie algorytmu szyfrującego WEP stanowiło podstawę do tworzenia algorytmu szyfrującego protokołu TKIP, a zaimplementowane funkcje znacznie zmniejszyły wrażliwość algorytmu na ataki. Klucz szyfrujący WPA stanowiący lepszy poziom bezpieczeństwa, umożliwia zastosowanie zamiast protokołu TKIP z Advanced Encryption Standard, czyli AES. Wykonuje on 10 (klucz 128 bitów), 12 (klucz 192 bity) lub 14 (klucz 256 bitów) cykli szyfrujących. Składają się one z substytucji wstępnej, permutacji macierzowej, polegającej na mieszaniu wierszy i kolumn oraz modyfikacji za pomocą klucza.[10] Zastosowanie protokołu TKIP pozwoliło na zablokowanie możliwości oddziaływania na ataki z powtórzeniami. Rzecz w tym, że tego typu ataki przy szyfrowaniu WEP były nieuchronne. Zastosowanie wówczas protokołu TKIP pozwoliło na zapobieganie tym atakom, które polegają na wielokrotnym przesyłaniu do

[9] https://sekurak.pl/bezpieczenstwo-sieci-wi-fi-czesc-4-standard-802-11i-czyli-wpa-i-wpa2/
[10] https://odo24.pl/blog/jak-bezpiecznie-korzystac-z-wi-fi.php.zamow-rozmowe

danej sieci tego samego pakietu, stąd też mówi się o ataku z powtórzeniami. Zapobieganie tego typu atakom w przypadku protokołu TKIP, polega na wprowadzeniu licznika sekwencyjnego pakietów, który powoduje, że Access Point blokuje i odrzuca pakiety spoza zakresu obsługiwanych w danym momencie wartości.

Przy zastosowaniu klucza szyfrującego WPA istnieją dwie możliwości jego uwierzytelnienia: WPA-Personal oraz WPA-Enterprise. Przy zastosowaniu uwierzytelnienia WPA-Enterprise router wykorzystuje Serwer RADIUS, którego zadaniem jest przydzielanie użytkownikom kluczy. Zadaniem serwera RADIUS jest zezwolenie na przydzielenie dostępu dla poszczególnych urządzeń w sieci oraz przesyła on taką informację do AP. AP wykonuje następnie decyzję serwera RADIUS. W przypadku WPA - Enterprise uwierzytelnienie użytkownika następuje jeszcze przed podłączeniem urządzenia do sieci. Po uwierzytelnieniu nadawany jest klucz PMK (Pairwise Master Key), który jest niezmienny i stały podczas całej sesji. Klucz PMK jest ustalany z Serwerem RADIUS w ramach sesji EAP. Są wówczas generowane klucze szyfrujące transmisję pakietów. Natomiast w przypadku WPA-Personal jest przydzielany jeden wspólny klucz dla wszystkich podłączonych stacji (PSK - Pre Schared Key). Dla WPA-PSK PMK tworzony jest przy pomocy funkcji haszującej PBKDF2 z użyciem SSID, PSK oraz 4096 iteracji HMAC (dla WPA PBKDF2-MD5, a dla WPA2 PBKDF2-SHA1).[11]

W roku 2006 algorytm szyfrujący WPA został całkowicie wyparty nowym algorytmem - WPA 2. Najbardziej znaczącą różnicą między tymi dwoma protokołami, było obowiązkowe użycie protokołu AES (Advanced Encryption Standard) oraz CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) w zamian za uprzednio wykorzystywany protokół TKIP. Algorytm szyfrujący WPA 2 jest bezpieczniejszy od swojego poprzednika, choć też jest podatny na przechwycenie pakietów podczas uwierzytelniania oraz słownikowe łamanie kluczy, szczególnie wtedy, gdy mamy uruchomione WPS (WiFi Potected Setup). W przypadku zbudowania własnej domowej sieci bezprzewodowej, jeśli posiadany przez nas router nie obsługuje najnowszego algorytmu WPA 3, wówczas najbezpieczniejszym rozwiązaniem jest wykorzystanie algorytmu szyfrującego WPA 2 - PSK z kluczem szyfrującym AES, przy wyłączeniu możliwości uwierzytelnienia i podłączenia się do sieci z wykorzystaniem WPS.

Pojawienie się nowych technologii sieci bezprzewodowych opartych na standardzie Wi-Fi 6 pozwoliło na wprowadzenie także nowych rozwiązań technologicznych mających znaczenie dla bezpieczeństwa sieci bezprzewodowych. Nowy standard bezpieczeństwa sieci bezprzewodowych WPA 3 ma kluczowe znaczenie dla bezpieczeństwa, wprowadzając nowe możliwości uwierzytelniania. Standard WPA 3 korzysta z protokołu szyfrującego SAE uniemożliwiając realizowanie ataków słownikowych w trybie offline, poprzez wzmocnienie zabezpieczenia rotacji kluczy. Ponadto ochrona oparta jest na oddzielnych kluczach PMK generowanych w trybie ciągłym dla każdej komunikacji Klient-AP. Zmniejsza to znacznie podatność na ataki typu „brute force". Szyfrowanie WPA 3 oparte jest na kluczach 192 bit, wynikiem czego utworzona sieć z punktu widzenia bezpieczeństwa jest bardziej zaawansowana, przy czym następuje minimalizacja podatności na ataki. W standardzie WPA3 zrezygnowano z szyfrowania 128-bitowego, który jest podstawą standardu WPA2-Enterprise, na rzecz szyfrowania opartego na kluczach 192-bitowych. Integracja z zestawem algorytmów CNSA umożliwia korzystanie z 48-

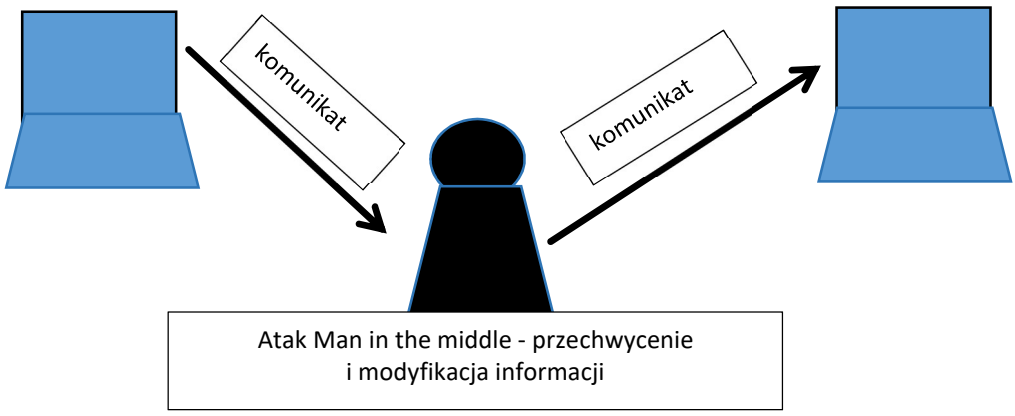
[11] https://sekurak.pl/bezpieczenstwo-sieci-wi-fi-czesc-4-standard-802-11i-czyli-wpa-i-wpa2/

bitowego wektora inicjalizującego — rozwiązania wymaganego w środowiskach rządowych i przemysłowych, ponieważ zapewnia najwyższy poziom bezpieczeństwa.[12]

Standard WPA3 wykorzystuje model Enhanced Open™, aby zapewniać bezpieczeństwo danych podczas korzystania z otwartej sieci Wi-Fi. Każde połączenie pomiędzy użytkownikiem a punktem dostępowym szyfrowane jest unikalnym kluczem, co obniża skuteczność popularnych ataków kryptologicznych Man in the middle.[13]

Ataki „Man in the middle" są bardzo powszechnym rodzajem ataków ukierunkowanych na bezpieczeństwo sieci bezprzewodowych, ponieważ polegają one na podsłuchiwaniu informacji między dwoma celami. Tego typu działanie powstaje z chwilą uzyskania nieautoryzowanego dostępu, który jest całkowicie niewidoczny dla użytkowników sieci oraz na przechwyceniu i odszyfrowaniu komunikacji między dwoma stronami, np. między dwoma komunikującymi się urządzeniami. Wynikiem czego sprawca takiego ataku całkowicie niepostrzeżenie ma możliwość manipulować przesyłanymi informacjami.

Poniżej przedstawiono schemat takiego działania.



Rys. 5. Przykład ataku Man in the middle.
Źródło: Opracowanie własne.

Skutkiem przeprowadzenia tego typu cyberataku może być:

1) pozyskanie przez sprawcę cyberataku dostępu do danych nieuprawnionych, m.in. mogą być to dane do logowania na konto użytkownika, sieci oraz wielu innych zasobów,
2) przechwytywanie oraz podmiana plików, które mogą zawierać np. numery kont bankowych, wynikiem czego ofiara takiego ataku może utracić przelewaną gotówkę,

Użytkownicy posiadający dostęp do Internetu, np. w swoim miejscu zamieszkania, czy w firmie, niejednokrotnie analizują możliwość rozdzielenia łącza internetowego celem podłączenia kilku posiadanych urządzeń. Należy wówczas przeanalizować techniczną możliwość

[12] https://www.tp-link.com/pl/wpa3/
[13] Ibidem

wykonania bezprzewodowej sieci, uwzględniając w szczególności rodzaj i możliwości sprzętowe wykorzystane do budowy takiej sieci. Oczywiste jest, że w miejscu swojego zamieszkania taki użytkownik nie bezie budował profesjonalnej serwerowni gwarantującej wysokie standardy bezpieczeństwa, a jedynie skupi się na prostych urządzeniach umożliwiających w dość łatwy sposób zbudowanie wewnętrznej sieci wykorzystując technologię Wi-Fi. Wobec powyższego, przed przystąpieniem do zakupu urządzeń sieciowych należy przeanalizować obecne na rynku urządzenia typu Router/AP pod kątem zastosowanych technologii, w szczególności pod kątem gwarantowanych standardów bezpieczeństwa. Owszem, każdy router Wi-Fi będzie miał jeden ze wskazanych w artykule standardów bezpieczeństwa, jednakże im wyższy standard bezpieczeństwa, tym bezpieczniejsza jest utworzona sieć. Budując sieć opartą na technologii Wi-Fi ważne jest, aby:

- utworzyć sieć opierając się na możliwie najwyższym oferowanym standardzie bezpieczeństwa,
- tworzone hasła dostępu do sieci powinny składać się z co najmniej 12 znaków i powinny charakteryzować się dużą złożonością, zawierając małe i duże litery, znaki specjalne oraz cyfry. Im dłuższe i bardziej złożone hasło, tym trudniejsze będzie do złamania przez potencjalnego sprawcę.
- należy usunąć ze struktury sieci nieautoryzowane punkty dostępowe (jeżeli takie się znajdują),
- w przypadku zastosowania urządzeń oferujących standard bezpieczeństwa WPA/WPA2, a posiadających możliwość autoryzacji urządzeń z wykorzystaniem WPS - celem poprawy bezpieczeństwa sieci bezprzewodowej zalecane jest wyłączenie funkcji WPS,
- ustawienie ręcznego przydzielania adresów IP uwierzytelnionym użytkownikom sieci, dla zapewnienia lepszej kontroli, aniżeli automatyczne przydzielanie adresów za pośrednictwem DHCP.

Odpowiednie skonfigurowanie posiadanej sieci bezprzewodowej przyczyni się do poprawy bezpieczeństwa zarządzaną siecią, a tym samym uchroni przed różnymi cyberatakami, chroniąc urządzenia sieci przed nieuprawnionym dostępem.