Mechanizmy zabezpieczeń sieci bezprzewodowych

Referat

AGH

AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Piotr Jakubas
Wojciech Kucharski

Informatyka Stosowana V rok

1 Wprowadzenie

Współczesne wymagania mobilności, dostępności pracownika przez 24 godziny, 7 dni w tygodniu powodują, że sieci bezprzewodowe stają się nieodłącznym elementem naszej rzeczywistości. Mówimy tu nie tylko o sieciach lokalnych opartych o technologię 802.11, ale również sieciach personalnych opartych o Bluetooth, czy sieciach miejskich i rozległych. Karty radiowe wbudowywane są w telefony i notebooki. Głównym obiektem naszego zainteresowania będą sieci standardu 802.11.

Tradycyjnie telefony GSM i PDA oferowały szeroką gamę rozwiązań ułatwiających planowanie czasu, pracę grupową czy też dostęp do poczty elektronicznej i stron WWW. Dziś coraz częściej na urządzeniach mobilnych pojawiają się aplikacje biznesowe. W tym przypadku ochrona sieci bezprzewodowej jest tak samo ważna jak budowa systemu bezpieczeństwa wewnątrz firmy.

Tradycyjnie myśląc o polityce bezpieczeństwa myślimy o fizycznym zabezpieczeniu infrastruktury sieciowej. Słyszeliśmy o instalacji, gdzie segmenty sieci były prowadzone w rurach o podniesionym ciśnieniu – próba nawiercenia wywoływała automatyczny spadek ciśnienia i odcięcie całego segmentu sieci. Instytucje rządowe wymagające specjalnego bezpieczeństwa stosują specjalne metody w celu ograniczenia emisji elektromagnetycznej mogącej ujawnić dane obrabiane na komputerach. Już w latach siedemdziesiątych powstał w USA tajny program „Tempest", którego celem było opracowanie technologii oraz norm dotyczących ograniczenia emisji ujawniającej.

W tym kontekście sieci radiowe stanowią całkowite zaprzeczenie uznanych podstaw budowy systemu bezpieczeństwa. Technologia sieci radiowych rozwijała się bardzo dynamicznie. Początkowo sieci 802.11 dostarczały przepustowości na poziomie 1 do 2 Mbps. Szybko jednak podniesione zostały praktycznie do poziomu 100 Mbps. Sieci bezprzewodowe nie miały jednak szczęścia do systemów zabezpieczeń. Zabezpieczenia oferowane przez producentów sieci bezprzewodowych okazały się mało skuteczne. Dopiero standard WPA oraz wprowadzona ostatnio norma 802.11i spowodowały zmianę tego stanu rzeczy.

2 Standardy 802.11 oraz WiFi

Wprowadzony w czerwcu 1997 roku oryginalny standard 802.11 przewidywał wykorzystanie nielicencjonowanej częstotliwości 2,4 GHz oferując transfer danych z prędkością 1 lub 2 Mbps. Szybko jednak, bo pod koniec 1999 roku, wprowadzono standard 802.11b pozwalający na transfer danych z prędkością do 11Mbps. Szansa na wyższe prędkości przesyłania danych pojawiła się z uwolnieniem pasma 5 GHz. Wprowadzony w 1999 roku standard 802.11a oferuje transfer do 54 Mbps. Popularność standardu 802.11b oraz ograniczenia w lokalnej dostępności pasma 5GHz spowodowały, że opracowano wykorzystując technologię analogiczną do 802.11a, standard wykorzystujący również pasmo 2,4 GHz – 802.11g. Został on wprowadzony stosunkowo niedawno, bo prace nad nim zakończono w 2003 roku. Oferuje on również przepustowość do 54 Mbps będąc kompatybilnym z 802.11b.

Standard 802.11 oferuje dwa mody pracy:

- Tryb „ad hoc" umożliwiający bezpośrednie połączenie urządzeń klienckich (STA). Stacje muszą stosować takie same metody uwierzytelniania. Połączone

ze sobą stacje tworzą tzw. niezależną komórkę (ang. „Independent Basic Service Set"), zwaną w skrócie IBSS.200

- Tryb strukturalny zakłada istnienie wydzielonej stacji bazowej zwanej punktem dostępowym (ang. „Access Point"). W tym trybie stacje klienckie (STA) muszą przyłączyć się do punktu dostępowego. Punkt dostępowy pełni często rolę uwierzytelniania połączeń, filtracji ruchu, analizatora ruchu sieciowego etc. Z reguły, z punktu widzenia sieciowego, implementowany jest jako bridge. Wiele urządzeń oferuję funkcjonalność routera. Komórkę utworzoną przez AP oraz stacje klienckie nazywa się komórką bazową (ang. „Basic Service Set"), w skrócie BSS.

Oryginalny standard 802.11 pozostawiał spore możliwości interpretacyjne. Okazało się, że urządzenia różnych producentów nie chcą ze sobą współpracować. Producenci sprzętu radiowego stworzyli porozumienie WiFi Alliance, które miało na celu zapewnienie kompatybilności bazowych funkcji systemów. Certyfikacja WiFi obejmuje:

- 802.11a
- 802.11b
- 802.11g
- Bezpieczeństwo:
  - WEP
  - 802.1x
  - WPA
  - WPA2
- WMM QoS i WMM-SA QoS (prace w toku)

Wybór sieci radiowej jest dokonywany na podstawie jej nazwy (ang. „Service Set Identifier"), zwanej w skrócie SSID. Nazwa sieci jest rozgłaszana w specjalnych ramkach zwanych po angielsku „beacon". Ramki te przenoszą również inne użyteczne informacje takie jak: numer kanału, wspierane szybkości transmisji, informacje o synchronizacji czasowej czy regulacji prawnej. Rozgłaszanie informacji o regulacji prawnej reguluje standard 802.11d. Umożliwia to automatyczne dopasowanie parametrów karty klienckiej do regulacji prawnej punktu dostępowego, w którego zasięgu znalazła się karta.

Często zapomina się o tym, że sieci standardu 802.11 mogą stosować dwie metody uwierzytelniania:

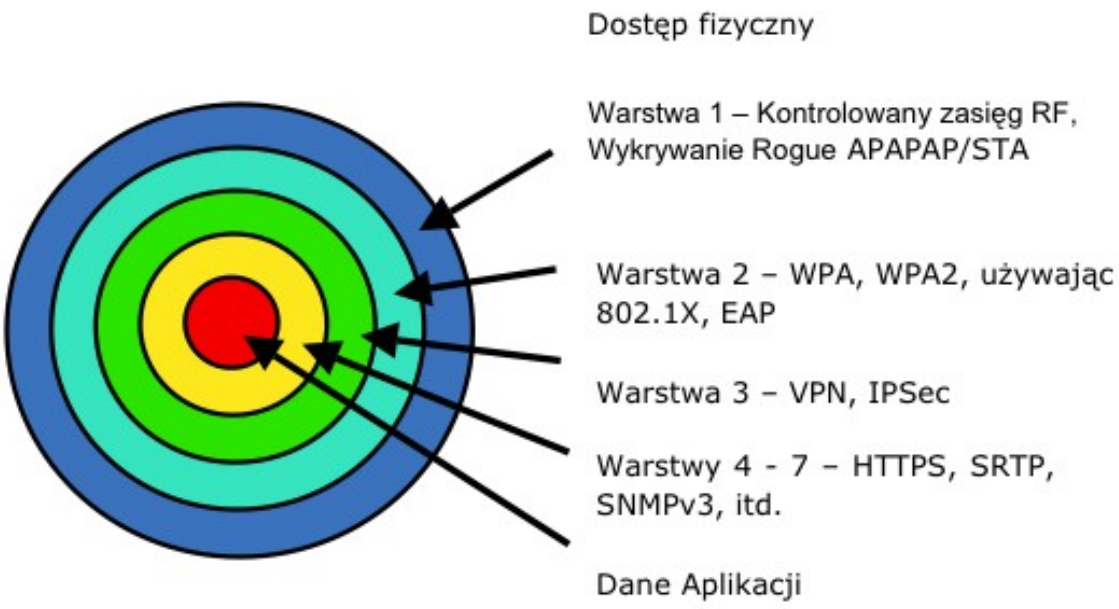
- Metoda otwarta, w której punkt dostępowy zawsze akceptuje próby uwierzytelnienia
- Metoda uwierzytelniania kluczem współdzielonym WEP, o którym dokładniej wspomnimy poniżej. W tej metodzie klient wysyłający żądanie uwierzytelnienia otrzymuje losowy „challenge". Klient szyfruje „challenge" współdzielonym kluczem za pomocą WEP i odsyła z powrotem do AP. AP deszyfruje „challenge" i porównuje go z wcześniej wysłanym do żądającego uwierzytelnienia klienta. Dopiero w przypadku gdy oba „challenge" są zgodne podejmowana zostaje próba uwierzytelnienia klienta.

Większość urządzeń standardowo oferuje uwierzytelnianie otwarte.

Zastosowanie metody uwierzytelniania z kluczem współdzielonym WEP podnosi wyżej poprzeczkę dla atakującego naszą sieć.

3 Zabezpieczanie sieci bezprzewodowych

Zabezpieczenia sieci bezprzewodowych obejmują zarówno mechanizmy kontroli dostępu, jak i szyfrowania przesyłanych danych. Wydaje się, że najlepszą obecnie metodą zabezpieczania danych aplikacyjnych przesyłanych sieciami bezprzewodowymi jest metoda wielopoziomowa tak jak pokazano to na rysunku – zaczynamy od bezpieczeństwa fizycznego, a kończymy na warstwie aplikacyjnej.



Rys. 1. Warstwowy model ochrony sieci bezprzewodowych

Metody stosowane do zabezpieczania sieci obejmują:

- Ukrywanie nazwy sieci SSID
- Filtracja i uwierzytelnienie na podstawie adresów MAC
- Blokowanie łączności pomiędzy stacjami
- Forwardowanie portów
- WEP
- 802.1X
- WPA, WPA-PSK
- WPA2 – 802.11i, WPA2-PSK

3.1 Ukrywanie nazwy sieci

Ukrywanie nazwy sieci było jedną z pierwszych metod stosowanych do ochrony sieci radiowych. Niestety nie jest to metoda skuteczna. Nazwa sieci znika co prawda z ramek typu „Beacon", ale pozostaje w innych pakietach. Haker wyposażony w dowolny sniffer bezprzewodowy zdobywa nazwę w momencie pojawienia się ruchu aplikacyjnego pomiędzy AP a stacją kliencką. Dodatkowo metoda ukrywania SSID nie jest zestandaryzowana, co powoduje, że nie wszystkie urządzenia współpracują ze sobą poprawnie w tym trybie.

3.2 Filtracja adresów i uwierzytelnianie na podstawie adresów MAC

Większość punktów dostępowych oferuje funkcje filtracji adresów MAC urządzeń podłączających się do AP. Mogą to być lokalnie konfigurowane „czarne" lub „białe listy", a także często możliwość współpracy z serwerem RADIUS. Filtracja MAC adresów jest w dużych sieciach skomplikowana organizacyjnie. Nie zapewnia również wysokiego poziomu bezpieczeństwa. Sniffując ruch sieciowy haker z łatwością wykryje adresy MAC dopuszczone do danego AP. W chwili obecnej standardowo Linux oferuje komendy pozwalające na zmianę adresu MAC (standardowa komenda ifconfig). Pod system Windows dostępne są programy takie jak Amac, Smac, MACMakeup czy EtherChange pozwalające na zmianę adresu MAC karty sieciowej. Wykorzystując więc dowolną z powyższych metod możemy zdobyć dostęp do AP.

3.3 Blokowanie komunikacji pomiędzy stacjami

W wielu przypadkach nie jest wskazane aby stacje klienckie podłączone do AP mogły komunikować się poprzez AP. Ma to na przykład miejsce w „hot spot'ach" gdzie taka możliwość mogłaby zostać wykorzystania do „hakowania" innych stacji klienckich. Blokowanie następuje na poziomie warstwy drugiej. Oczywiście urządzenia następnych warstw mogą taką komunikację warunkowo dopuścić. Stosując jako koncentrator rozwiązanie VPN Check Point VPN-1 możemy zapewnić przywrócenie komunikacji poprzez zastosowanie mechanizmu VPN routing. Jednak ruch pomiędzy klientami jest wtedy filtrowany poprzez firewall.

Mechanizm blokowania ruchu pomiędzy stacjami klienckimi jest cennym uzupełnieniem dla innych stosowanych mechanizmów.

3.4 Mechanizm „port forwarding"

Ponieważ wiele AP pracuje w trybie bridge popularnie stosowane są mechanizmy warstwy drugiej. Interesującym rozwiązaniem jest mechanizm pozwalający cały ruch wychodzący z AP skierować na wybrany adres MAC. W połączeniu z opisanym wyżej mechanizmem blokowania ruchu pomiędzy stacjami klienckimi w ramach AP daje on całkiem ciekawe możliwości konfiguracyjne. W szczególności poprzez połączenie tych dwóch mechanizmów możemy skierować ruch na wybraną bramkę aplikacyjną lub koncentrator VPN.

3.5 Wired Equivalent Privacy – WEP

WEP był jednym z pierwszych mechanizmów stosowanych do kontroli dostępu oraz szyfrowania transmitowanych danych. WEP wykorzystuje mechanizm współdzielonych haseł oraz szyfrowanie oparte o algorytm RC4. Standardowo szyfrowanie WEP wykorzystuje klucz 64 lub 128 bitowy. Efektywna długość klucza, ze względu na implementację protokołu, wynosi odpowiednio 40 i 104 bity. Specyfikacja protokołu WEP nie przewidywała mechanizmu wymiany klucza sesyjnego czyniąc go tym samym podatnym na ataki typu statystycznego. Generalnie WEP łamie podstawowe zasady kryptografii poprzez brak mechanizmu wymiany klucza. Istotną wadą WEP jest to, że klucz jest wspólny dla wszystkich uczestników ruchu, a więc jego kompromitacja jest kwestią czasu.

Prace teoretyczne zespołu Martin, Fluhrer i Shamir pokazały, że WEP w pewnych warunkach może wygenerować sekwencję pakietów prowadzącą do kompromitacji klucza. W chwili obecnej poznanych słabości WEP jest znacznie więcej. Istnieją programy takie jak AirCrack pozwalające na złamanie haseł WEP wykorzystując zebraną próbkę od 10000 do 0.5 mln pakietów. Czas łamania klucza 40-bitowego kształtuje się na poziomie kilku sekund.

3.6 Standard 802.1X

Generalną tendencją w budowie systemów bezpieczeństwa jest blokowanie zagrożeń na możliwie najwcześniejszym etapie. W związku z pojawieniem się technik umożliwiających snifowanie ruchu sieciowego na przełącznikach powstał problem ich zabezpieczenia. Wykorzystanie protokołu 802.1X pozwala na rozwiązanie tego typu problemów.

Protokół 802.1X to protokół transportu w warstwie drugiej oraz kontroli dostępu na poziomie portu. Wykorzystuje protokół EAP (ang. „Extensible Authentication Protocol") w celu realizacji operacji uwierzytelniania użytkowników sieci LAN. 802.1x określa w jaki sposób EAP będzie zastosowane do kontroli dostępu na poziomie portu w sieciach WLAN oraz Ethernet. Zadaniem protokołu EAP jest umożliwienie zastosowania różnych algorytmów uwierzytelniania pomiędzy klientem (próbującym uzyskać dostęp do sieci) a serwerem uwierzytelniającym. W tym celu wykorzystywany jest serwer RADIUS z rozszerzeniami EAP. Zastosowanie serwera uwierzytelniającego pozwala na centralizację zarządzania użytkownikami. Konfiguracja urządzeń zostaje również uproszczona do minimum. W ramach protokołu 802.1X port przełącznika czy dostęp do AP jest blokowany do momentu poprawnego uwierzytelnienia użytkownika.

Protokół 802.1X może być stosowany zarówno w sieciach Ethernet, jak i w sieciach bezprzewodowych. Nie jest rozwiązaniem wszystkich problemów. Pozwala on bowiem na uwierzytelnienie użytkowników i negocjację klucza sesyjnego – nie rozwiązuje problemu ochrony transmisji danych. W chwili obecnej wsparcie protokołu 802.1X nie jest jeszcze zbyt powszechne. Windows 2000 SP3 z poprawkami oferuje klienta 802.1X. Lepsze wsparcie dla 802.1X wbudowane jest w Windows XP. Poprawka SP2 dla Windows XP przyniosła duże usprawnienia w konfiguracji i obsłudze sieci bezprzewodowych. Funk Software i Meetinghouse oferują oprogramowanie klienckie 802.1X na inne systemy Windows oferujące szeroką gamę metod uwierzytelniania takich jak: EAP-TLS, EAP-TTLS czy EAP-PEAP.

3.7 WPA WiFi Protected Access

Przedłużające się prace nad standardem 802.11i przy nierozwiązanym problemie bezpieczeństwa sieci bezprzewodowych spowodowały powstanie nowego standardu WPA. Głównym celem WPA było usunięcie największej słabości WEP czyli braku mechanizmów wymiany klucza szyfrowania. WPA stosuje do szyfrowania danych algorytm TKIP, będący pochodną WEP jednak z dobrze zaprojektowanym mechanizmem wymiany klucza. Zmianie uległ też algorytm uwierzytelniania pakietów – dodatkowo zastosowano algorytm (kontroli integralności) MIC. Algorytm ten uniemożliwia ataki typu retransmisji pakietów („replay attack") prowadzące do kompromitacji klucza. Pozostawienie WEP jako mechanizmu szyfrowania ma swoje głębokie uzasadnienie. Standard 802.11i przewidywał wykorzystanie AES, a tym samym prowadził do zwiększenia zapotrzebowania moc obliczeniową zarówno po stronie klienta, jak i serwera uwierzytelniającego. W przypadku starszych AP i kart oznacza to praktycznie wymianę sprzętu. W przypadku WPA sprowadza się to najczęściej do wymiany oprogramowania.

Konieczność wykorzystania serwera RADIUS do uwierzytelniania użytkowników nie jest atrakcyjną możliwością dla małych firm czy użytkowników domowych. Standard WPA-PSK (ang. „WPA-PreShared Key") wykorzystuje współdzielony klucz do uwierzytelniania użytkowników. Niestety WPA-PSK przesyła hash współdzielonego klucza otwartym tekstem. Atak na WPA-PSK następuje w momencie uwierzytelniania użytkownika. Zdobyty hash hasła poddawany jest już offline'owo atakowi słownikowemu. Słabość tę wykorzystuje w praktyce program „cowpatty". Oczywiście „cowpatty" nie jest programem przystosowanym do szybkiego łamania haseł. Na przeciętnym komputerze „cowpatty" potrafi sprawdzić około 40 haseł na sekundę. Wykorzystanie metod typu „rainbowcrack" może prowadzić do kompromitacji hasła w stosunkowo krótkim czasie. WPA-PSK nie działa również w trybie „ad hoc".

3.8 Standard 802.11i

Długo oczekiwany standard 802.11i zwany też WPA-2 jest kompatybilny z WPA. Dodaje brakującą funkcjonalność:

- Secure IBSS dla trybu „ad hoc"
- Szyfrowanie standardem AES-CCMP

Zastosowanie szyfrowania algorytmu AES do szyfrowania danych wydaje się być logiczną konsekwencją wprowadzenia AES jako standardu szyfrowania danych. W chwili obecnej wszystkie dostępne na rynku AP i kart wspierają standard 802.11i. Jest on jak na razie najbezpieczniejszym sposobem na zabezpieczenie sieci.

3.9 Projektowanie sieci bezprzewodowych

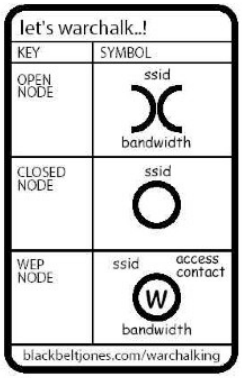
W chwili obecnej w związku ze znacznym rozpowszechnieniem sieci bezprzewodowych pojawiły się narzędzia wspomagające ich projektowanie. Decydującym co prawda pozostają praktyczne testy rozwiązania, ale można zaryzykować twierdzenie, że jeśli coś nie działa podczas symulacji, nie ma szans zadziałać w praktyce. Narzędzia wspierające projektowanie sieci bezprzewodowych pozwalają na ograniczenie ich zasięgu do niezbędnego minimum, a więc redukują możliwości podpięcia się z zewnątrz.

Wykorzystujemy tu zarówno możliwości oferowane przez zastosowanie anten kierunkowych, jak i mechanizmy regulacji mocy emitowanej oraz czułości odbiorników. Przykładem takiego narzędzia jest oprogramowanie Ekahau, które wspiera zarówno projektowanie sieci wewnątrz budynków jak i na zewnątrz. Dodatkowo oferuje dla sieci prowadzonych na zewnątrz budynków współpracę z odbiornikami GPS. Pozwala na import planów budynków i terenu. Wspomniane narzędzie może być również używane do audytu sieci bezprzewodowych.

4 Skala zagrożeń

Ze względów historycznych skala zagrożenia może być znaczna. Stare urządzenia nie zawsze pozwalają na uaktualnienia oprogramowania. W USA szacuje się, że ponad 30% sieci 802.11 stosuje WEP jako element zabezpieczenia sieci. Dodatkowym problemem jest to, że większość urządzeń jest prekonfigurowanych w taki sposób, że od razu działają w trybie dopuszczającym dowolną komunikację. Większość użytkowników nie podejmuje jakichkolwiek prób zmiany konfiguracji. Urządzenia są więc podwójnie podatne – nie tylko na próby dostępu do sieci bezprzewodowej, ale również poprzez możliwość dostępu do konfiguracji urządzeń za pomocą standardowych haseł.

Popularnym stało się zjawisko znakowania sieci bezprzewodowych „WarChalking". Na podstawie rozpoznania metodami „WarDriving" czy „WarWalking" położenie sieci jest markowane na ścianach budynków. Znaki kreślone są na ścianach budynku przy pomocy kredy. Dlaczego kreda? Ano dlatego, że wymalowanie trwałe oznaczenie ściany budynku może spowodować dla znaczącego takie przykre konsekwencje jak areszt, pokrycie kosztów usunięcia oznakowania i inne. Na Rys. 2 pokazano takie oznaczenia.



Rys. 2. Znaki „WarChalking": system otwarty, system z ukrytym SSID, WEP.

5 Inne sieci bezprzewodowe

Sieci radiowe 802.11 są dziś bardzo popularne. W dużych miastach zaczyna być tłoczno w eterze. W okolicy AGH jest ich stale widocznych kilkanaście. Ale przecież wykorzystujemy na co dzień również sieci Bluetooth, czy GSM.

Niewielu z nas wykorzystując słuchawkę Bluetooth czy zestaw samochodowy

zastanawia nad problemem bezpieczeństwa. Tymczasem poprzez problemy implementacyjne sieci Bluetooth mogą być wykorzystane do kradzieży naszych danych. Niedawna było bardzo głośno o aferach z Bluesnarfingiem. Rozwijane są technologie takie jak Bluejacking czy CarWhispering wykorzystujące słabości sieci Bluetooth. Mało z nas pamięta, aby wyłączyć tryb publiczny interfejsu Bluetooth po uwierzytelnieniu koniecznych urządzeń. Mitem jest również mały zasięg urządzeń Bluetooth. Istnieją udokumentowane próby Bluesnarfingu na odległość prawie 2 km wykorzystując anteny kierunkowe o dużym zysku.

Sieci GSM pozwalają w chwili obecnej nie tylko na przesyłanie głosu i danych, ale również na lokalizację urządzeń. Coraz częściej na naszych telefonach pojawia się nazwa ulicy, na której jesteśmy, a nie tylko nazwa miasta. Wykorzystując zasady triangulacji można w chwili obecnej zlokalizować użytkownika z dokładnością do kilkudziesięciu metrów.

Osobny rozdział stanowią etykiety RFID. Pomyślane jako zabezpieczenie przed kradzieżą z możliwością identyfikacji produktu znajdują coraz szersze zastosowanie. Dla pracodawców atrakcyjna jest wizja hipermarketu, w którym nie będzie kolejek, a liczbę kasjerów można drastycznie zredukować dzięki zastosowaniu etykiet RFID. Przejeżdżając wózkiem koło kasy automatycznie zostaną zsumowana wartość naszych zakupów... Niestety jak w każdej technologii i tu otwiera się możliwość nadużyć. Etykiety ukryte w przedmiotach pozwalają na lokalizację właściciela nawet do 20 km.

Generalnie problemem jest jakość oferowanych zabezpieczeń oraz coraz częściej widoczne próby naruszania prywatności użytkowników.

6 Podsumowanie

Sieci bezprzewodowe nie muszą być niebezpieczne. Ochrona danych aplikacyjnych powinna być konstruowana wielowarstwowo. Wydaje się, że żadna z technik nie gwarantuje absolutnej pewności. Wielowarstwowość ochrony danych zapewnia ochronę nie tylko przed znanymi zagrożeniami, ale również dzięki heterogeniczności systemu zabezpieczeń mamy większą szansę na ochronę przed atakami skierowanymi na przełamanie pojedynczej technologii. Skojarzenie silnego uwierzytelniania, technologii VPN, specyficznych technik ochrony sieci bezprzewodowych oraz ochrony aplikacyjnej to w chwili obecnej najlepsza recepta na zabezpieczenie sieci bezprzewodowych.

Inne sieci bezprzewodowe kryją w sobie również wiele niespodzianek. Musimy nauczyć się analizować zagrożenia zanim zdecydujemy się na zastosowanie nowych technologii do krytycznych zastosowań.

Osobnym problemem są naruszenia prywatności związane ze stosowaniem nowych technologii. Niestety regulacje prawne pozostają w tyle za szybko rozwijającą się technologią.