SLOVENSKÁ TECHNICKÁ UNIVERZITA
Fakulta elektrotechniky a informatiky
Katedra Telekomunikácií

802.11b –security WEP, WEP2, WPA

Školský rok: 2007/2008
Dňa: 20.11.2007

Filip Horváth
Jozef Grenčík
3.roč.

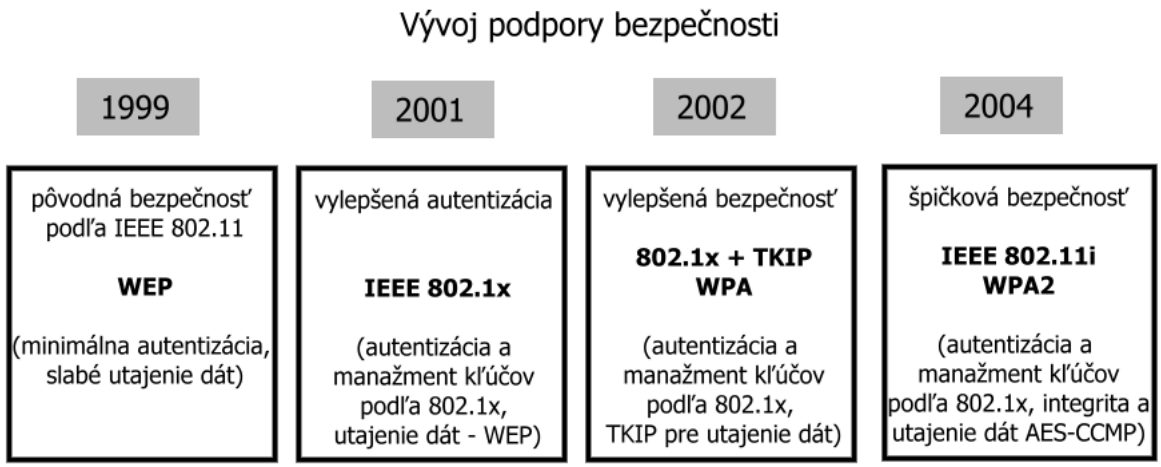
ÚVOD

V dnešnej dobe zažívajú bezdrôtové technológie veľký rozmach. Hlavné výhody sú už z názvu hneď jasné: mobilita a úspora na metalických vedeniach.
K najzvučnejším patria technológie Wi-Fi, BlueTooth, WiMAX, UWB či IrDA. Ale najviac z nich sa rozšírila Wi-Fi, ktorej sa budeme ďalej venovať.

Wi-Fi používa pri prenose dát mikrovlny a vysiela v určenom pásme, ktoré je vyčlenené regulačným orgánom. Americký regulátor FCC, ako aj európsky ETSI vyhradil pre tieto účely pásmo 2,4 GHz.

Zo začiatku každý z výrobcov vyrábal vlastnú technológiu. Aby sa docielila spolupráca medzi zariadeniami vydal štandardizačný inštitút IEEE roku 1997 štandard pre bezdrôtové siete pracujúce v pásme ISM pod číslom 802.11. Táto bezdrôtová sieť ponúkala rýchlosť až 2 Mb/s o dva roky neskôr túto špecifikáciu rozšírili o dve vyššie špecifikácie známe ako 802.11b štandard schopný ponúknuť rýchlosť až 11 Mb/s a štandard 802.11a, ktorý ponúka rýchlosť až 54 Mb/s.

Ďalším problémom, ktorý čakal Wi-Fi bola bezpečnosť odosielaných dát. Problém bezpečnosti je daný podstatou šírenia signálu. Na rozdiel od ethernetových (káblových) sietí, kde sú dáta aspoň z časti chránené, pri bezdrôtovej komunikácii lietajú dáta voľne vzduchom a fyzicky nie je možné obmedziť, kto ich pri prenose zachytí. Takto sa môže každý ľahko dostať k údajom, ktoré mu nie sú určené.



V súčasnosti sa bezpečnosť rieši pomocou šifrovania a autentifikácie. K základným šifrovacím mechanizmom patrí WEP, WEP2 , WPA a WPA2.

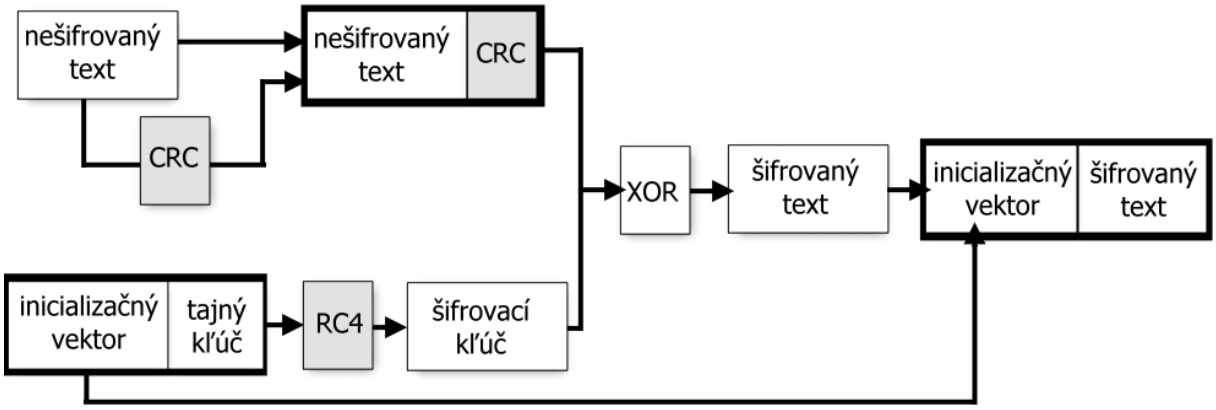
WEP (Wired Equivalent Privacy)

Základy

WEP - Wired Equivalent Privacy je protokol, ktorý zaisťuje bezpečný prenos dát vo Wi-Fi sieťach štandardu IEEE 802.11. Je to bezpečnostná technológia, ktorá pracuje na 2 úrovni OSI - linkovej vrstve (Data Link Layer), ktorá bola navrhnutá tak, aby poskytovala bezdrôtovým sieťam ekvivalentnú úroveň ochrany súkromia porovnateľnú s drôtovými sieťami. WEP definuje šifrovací algoritmus, ktorým sú šifrované prenášané dáta, čím sa zabraňuje ich jednoduchému odchyteniu. To už dnes nie je skoro pravda. Na internete sa nachádza veľké množstvo návodov a softwaru na pomerne rýchle prekonanie ochrany.

Princíp WEP spočíva v zašifrovaní prenášaného textu pomocou tajného kľúča (secret key), ktorý majú všetky stanice a access pointy(AP) v rámci jednej siete rovnaký. WEP používa symetrické šifrovanie. To znamená, že ten istý secret key je použitý na šifrovanie a aj na dešifrovanie. Tento secret key musí byť manuálne nastavený na každom zariadení využívajúce WEP. Mechanizmus bezpečnej distribúcie secret key medzi zariadeniami v jednej sieti, nie je súčasťou špecifikácie štandardu WEP.

Šifrovanie



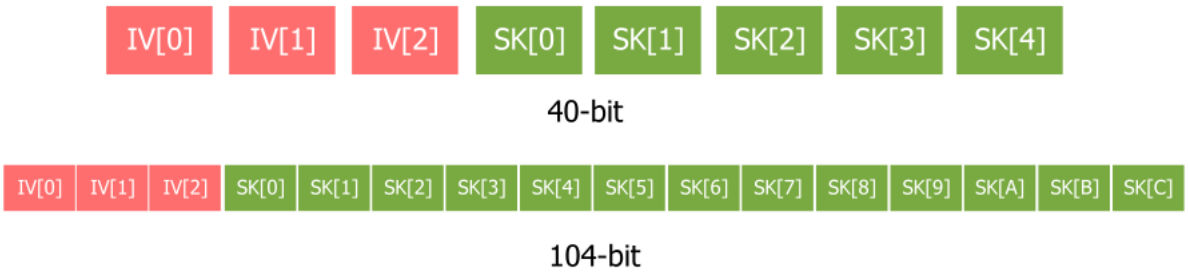
Šifrovanie začína tajným kľúčom, ktorý bol rozdistribuovaný zariadeniam v rámci jednej siete. WEP ako symetrický algoritmus tento kľúč používa na šifrovanie aj dešifrovanie. Tajný kľúč (40b) je zreťazený s inicializačným vektorom (IV, 24b) a vytvorí takzvaný „seed" (jadro, 64b), ktorý je vstupom do generátora pseudonáhodných čísel(PRNG). PRNG používa šifrovací algoritmus RC4 od RSA Data Security. Výstupom PRNG je šifrovací kľúč, ktorý sa rovná dĺžke prenášanej správy.

Nad nešifrovaným textom je vykonaný algoritmus, ktorý zaisťuje integritu. V podstate CRC-32, a jeho výstup (32b) je zreťazený s pôvodným textom.

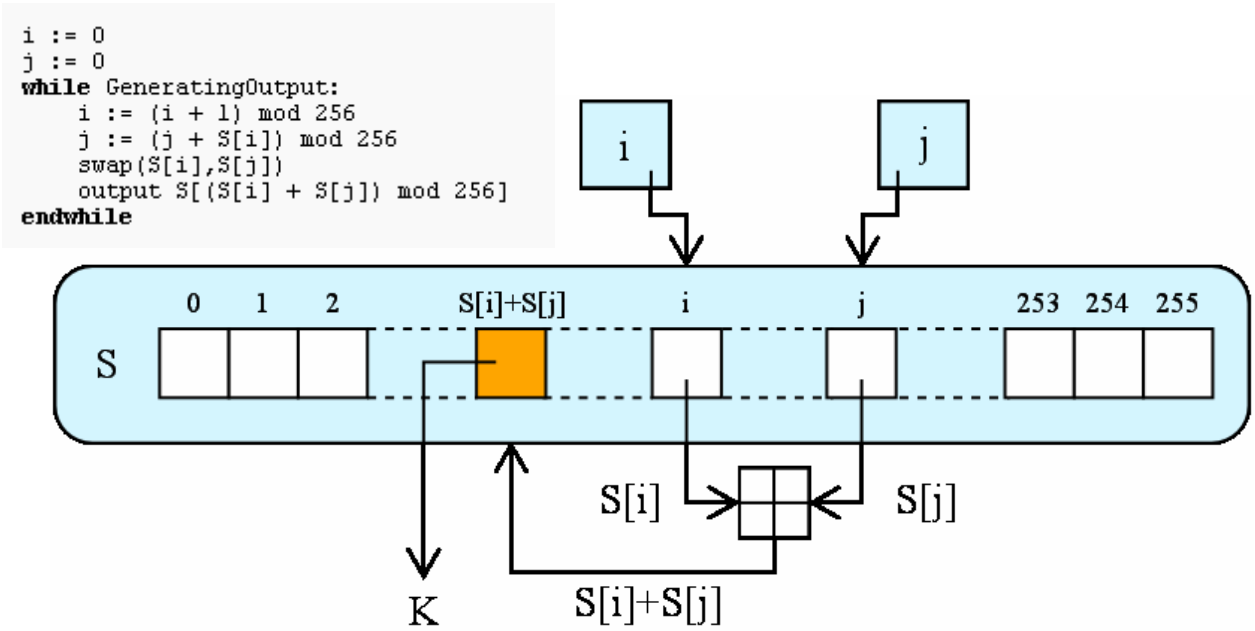
Teraz je šifrovanie dokončené logickou operáciou XOR medzi šifrovacím kľúčom a zreťazeným nešifrovaným textom s CRC32. Výsledkom celého procesu je správa obsahujúca zašifrovaný text a inicializačný vektor.

RC4

Šifrovací mechanizmus RC4 (Rivest Cipher 4), ktorého autorom je Ronald L. Rivest bol zverejnený v roku 1994. Aby bola zvýšená bezpečnosť zadaného kľúča používaného na šifrovanie obsahu paketov, pridáva sa k nemu náhodne generovaný 24-bitový reťazec nazývaný Initialization Vector (IV). Generovanie IV je pseudonáhodné a po určitom množstve paketov sa jeho hodnota musí zopakovať.



Na obrázku je zobrazená štruktúra kľúča použitého pre zašifrovanie rámca. IV sú oktety náhodne generovaného Inicializačného Vektoru, SK sú oktety kľúča zadaného užívateľom (Secret Key).



Na obrázku je graficky znázornené jadro algoritmu RC4

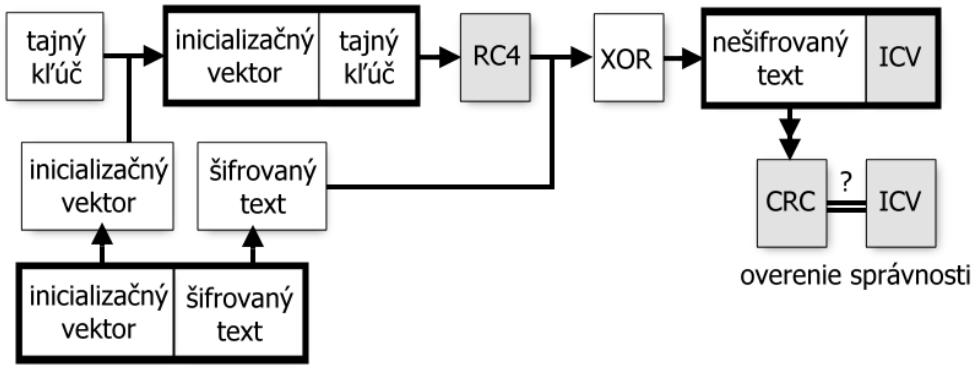
Dešifrovanie

Dešifrovanie začína prijatím zašifrovanej správy. Už pred začatím procesu dešifrovania máme k dispozícii tajný kľúč (secret key), ktorý bol nastavený administrátorom alebo pomocou niektorého externého manažmentu kľúčov.

Zreťazením inicializačného vektora (IV) prichádzajúcej správy a tajného kľúča je vytvorený „seed", ktorý je použitý na vygenerovanie dešifrovacieho kľúča potrebného na dešifrovanie prichádzajúcej správy. Generovanie prebieha pomocou RC4 algoritmu.

XOR-ovaním šifrovaného textu s príslušným dešifrovacím kľúčom dostaneme pôvodný nezašifrovaný text a kód (ICV), ktorý bol vygenerovaný procesom CRC32 pri šifrovaní.

Korektné dešifrovanie je overené algoritmom na kontrolovanie integrity, ktorého výstup je CRC (ICV') a následným porovnaním s ICV preneseným v správe. Ak sa nerovnajú, prijatá správa je chybná a indikácia chyby je poslaná MAC managementu.



Nedostatky protokolu WEP

WEP bol časťou štandardu 802.11 od počiatočnej ratifikácie v Septembri 1999. Neskôr začali byť zrejmé niektoré limitácie protokolu WEP. Aj napriek tomu že v minulosti bolo WEP zabezpečenie významne využívané, za posledných pár rokov boli odhalené mnohé nedostatky.

WEP je napadnuteľný pretože obsahuje relatívne krátky inicializačný vektor a kľúče ostávajú statické. Toto nemá príliš veľa spoločného s kryptovacím algoritmom RC4. S len 24 bitovými inicializačnými vektormi, WEP používa rovnaké IV pre rozdielne dátové pakety.

WEP má tri zásadné bezpečnostné chyby:

1. Krátky, len 24 bitový inicializačný vektor. Môže dôjsť v rušnej sieti k tomu že je za hodinu bude použitý rovnaký IV 2 krát. To spôsobí, že sa v prenose siete objavia také rámce, čo sú dostatočne podobné, na umožnenie odkryptovania rámca.

2. Dlhý čas je používaný rovnaký šifrovací kľúč pre všetky zariadenia v sieti. Keďže žiadny kľúč by nemal byť použitý dvakrát, bázová stanica má za povinnosť zmeniť tajný kľúč akonáhle jeho členovia vyčerpajú všetkých 2^{24} možností odvodených od tajného kľúča. WEP však nedefinuje žiadnu praktickú cestu, ako to splniť, takže v praxi nie sú WEP kľúče vymieňané dosť často na udržanie zamýšľanej úrovne bezpečnosti.

3. ICV(kontrola integrity) je relatívne krátka (4 byty).

WEP je náchylný na nasledovné typy útokov:

- Útok opakovaním – možnosť opakovaného použitia hodnoty IV.
- Podvrhnutie – IV používa 32 bitovú lineárnu hodnotu CRC, s ktorou sa dá manipulovať.
- Útoky založené na kolízii – kolízie IV.
- Útoky na slabé kľúče – šifra RC4 je napadnuteľná útokom FMS.

Rozlúštenie WEP kľúča V skratke sa dá povedať, že na WEP boli z hľadiska narušenia zabezpečenia u systémov úspešné nasledujúce typy útokov:

- Pasívne útoky zamerané na dešifrovanie prenosov na základe štatistickej analýzy.
- Aktívne útoky zamerané na vkladanie nových prenosov z neautorizovaných klientov na základe znalostí jednoduchého textu, ktoré mohli byť získané za použitia techniky pasívneho útoku.
- Aktívne útoky zamerané na dešifrovanie správ na základe oklamania prístupového bodu.
- Útoky založené na analýze zhruba jednodennej prevádzky. Zhromaždené dáta boli potom použité k automatizovanému dešifrovaniu prevádzky v reálnom čase. Tento typ útoku sa niekedy nazýva *zostavenie slovníka.*

Slovníkový útok Jedná sa o typický slovníkový útok, keď sa útočník snaží nájsť prístupové meno a heslo pomocou prihlasovacích mien uložených v databáze.
Ochrana: Predísť ukradnutiu hesla sa dá vhodným výberom hesla. Odporúča sa náhodná postupnosť znakov a čísel, kombinácia malých a veľkých písmen. Je vhodné aj použiť nealfanumerické znaky. Je ľahšie prelomiť kratšie heslo ako dlhšie.

Ďalšie slabiny protokolu WEP:

- Chýbajúca správa kľúčov.
- Chýbajúca podpora „pokročilých" autentizačných metód (tokeny, čipové karty, biometrika, jednorazové heslá a podobne).
- Chýbajúca identifikácia a autentizácia užívateľov.
- Chýbajúca centralizovaná autentizácia a autorizácia.

WEP je teda určitým stupňom ochrany proti širokej verejnosti, ale z hľadiska nabúrania sa zo strany profesionálnych hackerov nie je úplne bezpečným systémom. Preto by protokol WEP nemal byt jediným bezpečnostným systémom nachádzajúcim sa vo Wi-Fi sieťach.

WEP2

Ide o novšiu verziu bezpečnostného protokolu WEP, ktorá je rozšírená o nasledovné dve bezpečnostné vylepšenia:

1. zväčšený inicializačný vektor
2. zosilnené 128 – bitové kryptovanie

WPA (Wi-Fi Protected Access)

WPA je ďalší systém, ktorý je používaný na zabezpečenie bezdrôtovej siete. Vznikol ako odpoveď na niekoľko závažných slabých stránok predchádzajúceho bezpečnostného systému WEP. Protokol WPA bol ohlásený v roku 2002 alianciou Wi-Fi. Je to vlastne kompromisné riešenie, pretože niektoré časti špecifikácie 802.11i už boli hotové (napríklad 802.1x a TKIP), zatiaľ čo iné ešte nie (napríklad AES a zabezpečená deautentizácia a disasociácia). Wi-Fi aliancia nechcela čakať kým bude ratifikovaný 802.11i, ale vydala to čo už bolo hotové. WPA je teda podmnožinou 802.11i, ktorá sa dá implementovať prostredníctvom aktualizácie softvéru a firmvéru. Rieši ako šifrovanie (TKIP), tak aj riadenie prístupu (802.1x). WPA teda predstavuje medzistupeň v riešení bezpečnosti Wi-Fi sietí, je spätne zlučiteľné s WEP a pritom je dopredne zlučiteľné s 802.11i.

WPA obsahuje oproti protokolu WEP dva bezpečnostné inovatívne prvky:

1. TKIP (Temporal Key Integrity Protocol)
2. 802.1x

Ako šifrovací algoritmus bol z dôvodu spätnej kompatibility použitý RC4. Na rozdiel od WEP je ale použitý šifrovací kľúč o dĺžke 128 bitov, ktorý je zložený s inicializačného vektoru o dĺžke 48 bitov a tajného kľúča o dĺžke 80 bitov.

TKIP vylepšuje protokol WEP o nasledovné zosilnenia:

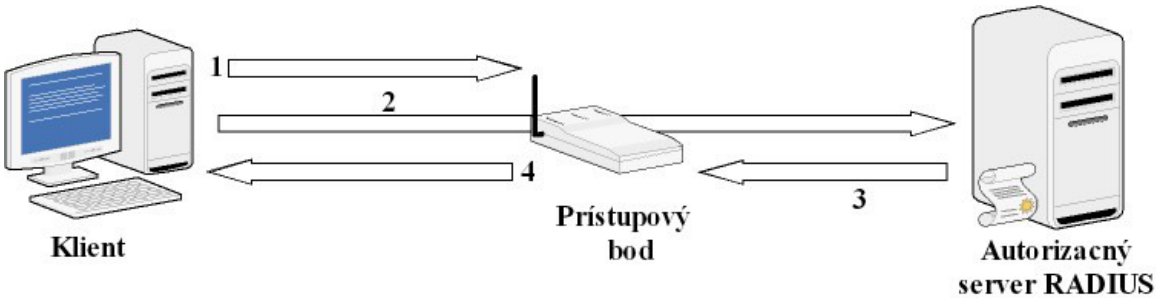
1. **48-bitový inicializačný vektor**
   Pre silnejšie zabezpečenie je využívaný dynamicky sa meniaci kľúč pre každý paket a predĺženú dĺžku inicializačného vektora na 48 bitov.
   Vo WEP bol používaný 24 bitový inicializačný vektor, pričom WEP používa rovnaký IV na rozdielne dátové pakety. V zásade, k znovuobjaveniu IV vo WEP môže dôjsť v rušných sieťach približne do hodiny. Výsledkom prenosu takýchto rámcov s rovnakým inicializačným vektorom, môže viesť k odkryptovaniu 802.11 rámcov. WPA s protokolom TKIP, keďže používa 48 bitový inicializačný vektor, ktorý výrazne redukuje znovupoužitie IV a tým aj možnosť, že hacker zozbiera dostatočné množstvo 802.11 rámcov na cracknutie kryptovania.

2. **Per-packet konštrukcia a distribúcia kľúčov**
   WPA automaticky generuje nový unikátny kryptovací kód pravidelne pre každého klienta. V zásade WPA požíva unikátny kľúč pre každý 802.11 rámec. Týmto sa WPA vyhýba tomu, aby bol po dlhú dobu využívaný jeden kryptovací kľúč ako tomu bolo vo WEP. Je to veľmi podobné výmene zámkov na dome po každom odchode, tým robí nemožné dostať sa do domu niekomu kto mal predošlú kópiu kľúča.

3. **Message integrity code (MIC)**
   WPA implementuje bezpečnostný prvok MIC, často nazývaný "Miachael".
   Je to vlastne bezpečnostný nástroj na kontrolu integrity správ. WPA pridáva pred ICV (integrity check value) 8-bitový MIC, čím zabezpečuje možnosť zmeny bitov v rámci.

802.1x je protokol umožňujúci autentizáciu na portoch (v tomto kontexte porty chápeme ako súčasť prvej sieťovej vrstvy, teda fyzické porty na prepínači). 802.1x blokuje všetku komunikáciu na danom porte až do doby, kým sa klient autentizuje prostredníctvom údajov, ktoré sú uložené na back-end serveri, ktorým je typicky RADIUS. Protokol 802.1x vychádza z protokolu PPP (Point-to-Point Protocol). Protokol PPP je obmedzený tým, že umožňuje autentizáciu založenú len na kombinácii užívateľského mena a hesla. Ako rozšírenie protokolu PPP bol vytvorený protokol EAP (Extensible Authentication Protocol). Základným cieľom bolo vytvoriť všeobecnú platformu pre rôzne autentizačné metódy. Dajú sa používať heslá, certifikáty, tokeny, PKI, čipové karty, Kerberos, biometrika atď. Otvorený štandard zaisťuje, že kedykoľvek v budúcnosti sa budú môcť použiť mechanizmy, ktoré v súčasnosti ešte nie sú známe.
802.1x je protokol, ktorý umožňuje používať EAP na metalických alebo bezdrôtových sieťach. Základnými komponentmi sú ***žiadateľ***, ***autentizátor*** *a* ***autentizačný server.***

Overovanie v bezdrôtovej sieti zabezpečuje prístupový bod pre klientov na základe ich výzvy, pomocou zoznamu alebo externého autentizačného systému založeného na serveri Kerberos alebo RADIUS *(Remote Authentication Dial In User Service).* Len overený používateľ má možnosť prístupu k bezdrôtovej sieti. Autentizácia podľa 802.1x je znázornená na nasledujúcom obrázku:



802.1x používa k šifrovaniu dátovej komunikácie pre každé autentizované zariadenie dynamické kľúče. Tieto kľúče sú známe len danému zariadeniu, majú obmedzenú životnosť a využívajú sa k šifrovaniu rámcov na danom porte, dokiaľ sa zariadenie neodhlási alebo neodpojí.

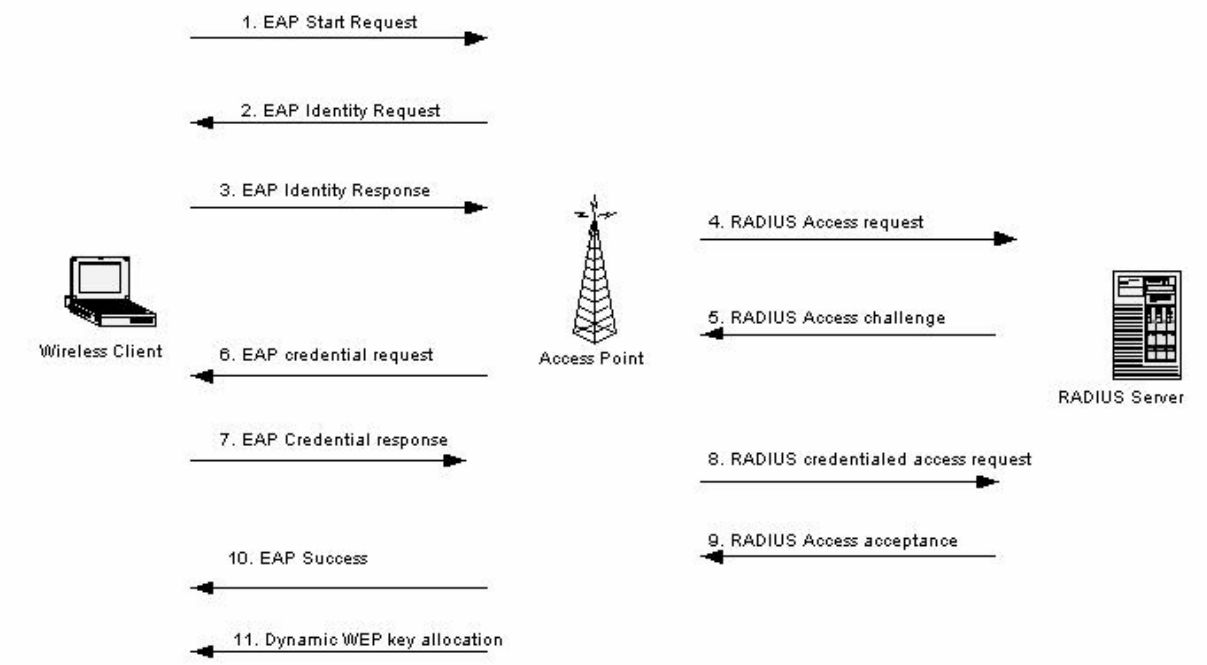
Najvýznamnejšia časť, ktorá pribudla od éry WEP je možnosť autentizovať užívateľov. Na základe takejto autentizácie sú potom jednotlivým zariadeniam dynamicky generované a priraďované šifrovacie kľúče. To prináša okrem lepšej kontroly a prehľadu prihlásených užívateľov aj zbavenie sa povinnosti manuálne prideľovať" všetkým rovnaký šifrovací kľuč.

WPA poskytuje dve autentizačné schémy:
1. PSK mode
2. Enterprise mode

PSK mode: PSK znamená "PreShared Key". Tento mód sa odporúča jedine v prípade malých, napr. domácich sietí, v prípade kde nie je dostupný autentizačný server. V takomto prípade je nutné priradiť zdieľané tajomstvo každej stanici aj prístupovému bodu. Toto heslo môže pozostávať z 8 až 63 ASCII znakov, alebo 64 hexadecimálnych číslic. Tento mód nás ale oberá a vyššie vymenované výhody autentizácie. Napriek tomu ale stále poskytuje vyššiu bezpečnosť z hľadiska utajenia a integrity. V tomto móde je ale potrebné dbať na to aby heslo bolo dostatočne komplexné, preto že na jeho základe sa šifruje komunikácia. Heslo by malo obsahovať minimálne 14 úplne náhodných znakov, pre zaručenie najvyššej bezpečnosti 22 úplne náhodných znakov.

Enterprise mode: Tento mód sa používa typicky vo firmách kde je požadovaná autentizácia užívateľov. Zároveň je nutné aby bol dostupný autentizačný server. Tento je väčšinou implementovaný ako RADIUS server a je umiestnený na samostatnom sieťovom serveri. Systém WPA definuje ale autentizačný proces prebiehajúci medzi klientskou stanicou a prístupovým bodom. Tento je popísaným autentizačným rámcom EAP.

Proces autentikácie pomocou protokolu EAP:



V prvom kole štandardizácie bola schválená jediná autentizačná metóda a to EAP-TLS. Neskôr boli zavedené aj d'alšie metódy (uvádzame len dve základné):

1. EAP-TLS (EAP-Transport Layer Security) je prvý a zároveň najbezpečnejšíí typ autentizácie klienta. Tento typ autentizácie bol dlho jediným podporovaným pre WPA aj WPA2.

2. EAP-TTLS (EAP-Tunneled Transport Layer Security) je zjednodušená forma autentizácie. V tomto prípade je požadovaný len certifikát pre server, klientské certifikáty nie sú potrebné.

Problém, ktorý WPA zatiaľ nerieši sú potenciálne útoky na odmietnutie služby DoS (Denial Of Service). DoS nie je tradičným typom útoku, nesnaží sa dostať do siete a získať prístup, ale Denial of Service sa snaží o zahltenie siete a jej následné vyradenie z prevádzky. DoS útok zvyčajne predchádza útoku typu man-in-the-middle. Pri zlyhaní siete a odstavení klienta je útočníkovi jednoduchšie sa tváriť ako podvrhnutý prístupový bod.

WPA2

Štandard WPA2 je tiež známy pod menom protokolu 802.11i. Tento protokol bol prijatý v roku 2004. Obsahuje sadu bezpečnostných mechanizmov pre zabezpečenie protokolov 802.11x. Bol navrhnutý s prioritou poskytnutia čo najvyššieho stupňa zabezpečenia. Systém WPA je založený na podmnožine zabezpečovacích mechanizmov definovaných v 802.11i. WPA2 poskytuje nástroje pre utajenie a integritu sieťovej komunikácie a zároveň pre autentizáciu užívateľov. Nevýhodou WPA2 je spätná nekompatibilita so staršími klientskymi kartami a prístupovými bodmi. Príčinou je nepostačujúci HW pre pokročilé šifrovanie. WPA2 ponúka rozšírenie v podobe možnosti šifrovania aj podpisovania pomocou modifikácie algoritmu AES (Advanced Encryption Standart). Ten je v súčasnosti považovaný za jeden z najspoľahlivejších a v praxi nasadzovaných riešení.

Šifra AES bola navrhnutá ako náhrada za šifru RC4. Rovnako ako RC4, aj šifra AES je symetrickým kľúčom, čo znamená, že sa text šifruje aj dešifruje rovnakým zdieľaným tajným kľúčom. Na rozdiel od šifry RC4, ktorá šifruje lineárne každý bajt funkciou XOR s náhodnou postupnosťou, AES pracuje s blokmi o veľkosti 128 bitov a preto sa označuje ako bloková šifra. Celý výstupný text sa rozdelí na 128 bitové bloky a tie sa postupne XORujú so 128 bitovým, vždy nanovo generovaným výstupom AES tak dlho, pokiaľ nedôjde k zašifrovaniu celej pôvodnej správy. Nakoniec sa čítač vynuluje, XORuje sa hodnota MIC, ktorá sa pridáva na koniec rámca. Výsledkom je oveľa silnejšia šifra. Má ale zvýšené nároky na HW prostriedky. Momentálne nie je známa žiadna bezpečnostná chyba v samotnom algoritme ani v jeho implementácii pre WPA2.

Zdroje:

- http://www.fit.vutbr.cz/study/DP/rpfile.php?id=5091
- http://www.mtf.stuba.sk/docs//internetovy_casopis/2006/2/tanuska.pdf
- http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
- http://islab.oregonstate.edu/koc/ece478/05Report/Browning.pdf
- http://www.wi-fiplanet.com/tutorials/article.php/1368661
- http://www.wi-fiplanet.com/tutorials/article.php/1377171
- http://www.wi-fiplanet.com/tutorials/article.php/2148721
- http://www.pripojsa.sk/?page=co-je-wifi/