NIEKTORÉ PROBLÉMY BEZPEČNOSTI POČÍTAČOVÝCH SIETÍ ZALOŽENÝCH NA TECHNOLÓGII WiFi

SOME PROBLEMS OF COMPUTER NETWORKS SECURITY BASED ON WiFi TECHNOLOGY

Jaroslav ZEMAN, Pavol TANUŠKA

Autori: ***Ing. Jaroslav Zeman, Doc. Ing. Pavol Tanuška, PhD.***
Pracovisko: ***Katedra aplikovanej informatiky a automatizácie, Materiálovotechnologická fakulta STU***
Adresa: ***Hajdóczyho 1, 917 01 Trnava***
Email: ***tanuska@mtf.stuba.sk***

Abstract

Cieľom tohto článku je analyzovať bezpečnosť sietí založených na technológii WiFi. V prvej časti článku sú popísané základy WiFi technológie – štandardy, komponenty siete, ISO/OSI model. Hlavná časť sa zaoberá bezpečnosťou WiFi sietí. V článku sú tiež spomenuté typy útokov, ale aj spôsob ochrany proti nim.

The aim of this article is the analysis and security layout of wireless networks. In the first part, we have described the fundamentals of WiFi technology - standard specifications, network components and ISO/OSI model. The main part is focused on security of the WiFi networks. Attack techniques and protection of Wifi networks are included, too.

Key words

bezpečnosť, WiFi, počítačové siete, WEP, IEEE, 802.11

security, WiFi, computer networks, WEP, IEEE, 802.11

Úvod

V súčasnosti prežívajú bezdrôtové technológie veľký rozmach. Výhody týchto riešení sú zrejmé – mobilita, flexibilita, úspora nákladov, prispôsobiteľnosť a ďalšie. Súčasne s výhodami sa objavujú aj mnohé nevýhody. Okrem problémov šírenia sa rádiového signálu je to hlavne otázka bezpečnosti a ochrany údajov.

Problém bezpečnosti je daný podstatou šírenia signálu. Na rozdiel od ethernetových sietí, kde sú dáta aspoň sčasti chránené, pri bezdrôtovej komunikácii dáta lietajú voľne vzduchom a fyzicky nie je možné obmedziť ich prenosovú trasu. Tak sa každý môže dostať k údajom, ktoré mu nie sú určené. V tomto článku sa budeme venovať hlavne bezpečnosti WiFi. Na nových technikách zabezpečenia WiFi stále pracujú rôzne skupiny organizácie IEEE a stále prijímajú nové štandardy z oblasti bezpečnosti. Predtým ako sa dostaneme blizšie k samotnej

bezpečnosti WiFi, je potrebné spomenúť aspoň základné pojmy z oblasti bezdrôtových technológií.

Siete 802.11 – WiFi

Inštitút inžinierov elektrotechniky a elektroniky (IEEE) vyvíja a schvaľuje normy pre širokú radu počítačových technológií. Prvá bezdrôtová norma bola prijatá v roku 1997 a bola nazvaná IEEE 802.11.

Názov normy	Frekvencia	Rýchlosť	Frekvenčné spektrum
802.11b	2,4 GHz	11 Mbit/s	DSSS (Direct Sequence Spread Spectrum)
802.11a	5 GHz	54 Mbit/s	OFDM (Orthogonal Frequency Spread Spectrum)
802.11g	2,4 GHz	54 Mbit/s	OFDM (Orthogonal Frequency Spread Spectrum)

Obr. 1. *Normy 802.11*

Medzi doplnkové normy patria:

- 802.11e - Quality of Service
- 802.11h – Spectrum Manager 802.11a
- 802.11i – Enhanced Security
- 802.11d – rieši všeobecné problémy medzinárodnej použiteľnosti
- 802.11f – rieši roaming medzi prístupovými bodmi.

Referenčný model ISO/OSI

Model ISO/OSI (Open System Interconnection) popisuje štruktúru siete a spôsob komunikácie medzi zariadeniami. Má 7 vrstiev: fyzická, linková, sieťová, transportná, relačná, prezentačná, aplikačná. Štandard 802.11 definuje ako vlastné iba dve najnižšie vrstvy OSI, teda fyzickú a linkovú (spojovú). Všetky ostatné vrstvy necháva štandard 802.11 nedotknuté. Linková vrstva, respektíve jej podvrstva označovaná ako MAC (Media Access Control) predstavuje súbor pravidiel určujúcich ako pristupovať k prostriedkom pre prenos dát. Samotné detaily o prenose dát sú však ponechané na fyzickej vrstve PHY.

Analýza bezpečnosti 802.11

Do bezpečnosti sa dá zaradiť aj riadenie prístupu do siete, resp. do Internetu. Tým sa obmedzí pripojenie k sieti neoprávneným osobám. Bezpečnosť bezdrôtových sietí môžeme rozdeliť do dvoch hlavných skupín:

- Šifrovanie – zabezpečenie prenášaných dát pred odpočúvaním
- Autentizácia – riadenie prístupu oprávnených používateľov

802.11 špecifikuje 2 metódy autentizácie:

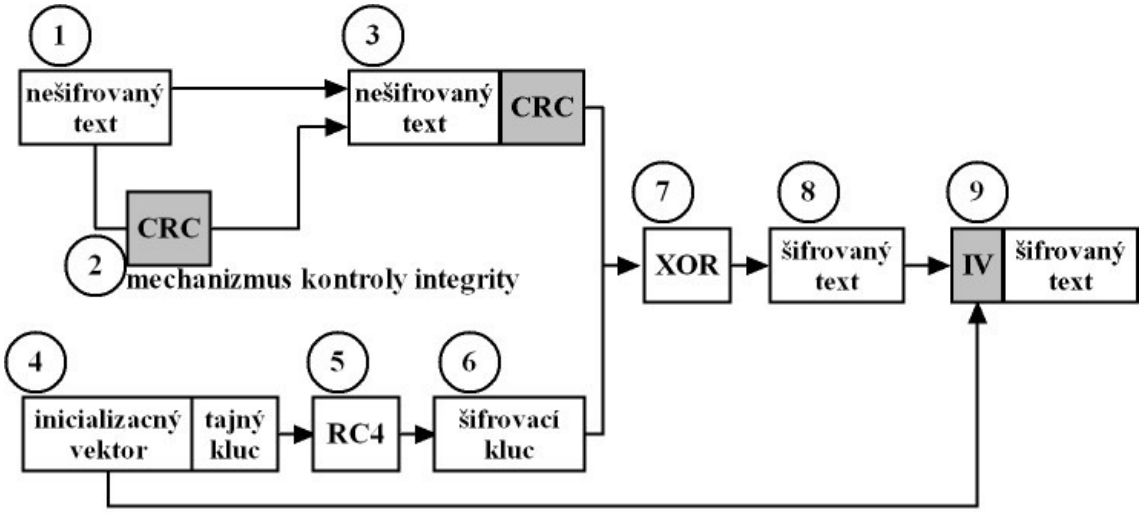
- Open-system autentizácia
- Shared-key autentizácia

Autentizácia v 802.11 je jednosmerný proces. Stanica si musí o autentizáciu do siete zažiadať, zatiaľ čo sieť sa voči staniciam autentizovať nemusí.

1. WEP

Skratka WEP *(Wireless Equivalent Policy)* je štandardom odvodeným organizáciou IEEE, ktorý definuje schému ochrany bezdrôtových sietí 802.11 na úrovni druhej vrstvy podľa OSI. Jeho účelom nie je celkové zabezpečenie siete, ale skôr ochrana dát pred pasívnym a nechceným odpočúvaním sieťovej komunikácie. Algoritmus WEP nešifruje hlavičku 802.11, identifikátor siete, ani inicializačný vektor (IV). [3]

WEP zabezpečuje komunikáciu medzi WiFi zariadeniami až na úroveň prístupového bodu. Za ním už bezpečnosť nezaistí. Štandard WEP používa symetrickú streamovú šifru RC4, teda šifru s tajným kľúčom. Podstatou tejto šifry je, že sa odosielaná správa šifruje podľa nejakého kľúča (obvykle slova alebo sekvencie znakov) a na cieľovom bode sa zasa podľa tohto kľúča dešifruje. Konkrétne to prebieha tak, že sa kľúč expanduje v pseudonáhodný kľúčovací tok (keystream) o rovnakej dĺžke akú má šifrovaná správa. O „pseudonáhodnosť" sa stará generátor pseudonáhodných čísel PRNG – teda zostava pravidiel, podľa ktorých sa kľúč rozšíri na dĺžku správy do kľúčovacieho streamu. Šifrovanie prebieha tak, že na šifrovanej hodnote sa prevedie logická operácia XOR s kľúčovacím tokom, dešifrovanie prebieha rovnako. Obe zariadenia, medzi ktorými má byť komunikácia šifrovaná, musia obsahovať rovnaké pravidlá PRNG a musia poznať tajný kľúč. Problémom tajného kľúča je fakt, že štandard nijako nerieši jeho automatickú distribúciu. [2]



Obr. 2. *Šifrovanie protokolom WEP*

V súčasnosti existujú rôzne dĺžky šifrovacieho kľúča. Výrobcovia udávajú dĺžky 64, 128 a 256 bitov. V skutočnosti je to trochu inak. Šifrovací WEP kľúč má dĺžku 40 bitov. Pred týchto 40 bitov sa predsadí 24 bitov inicializačného vektora IV (ten sa používa práve pre pseudonáhodnoť kľúčovacieho toku). A dokopy je to teda 64 bitov. Takisto je to pri dĺžkach 128 a 256 bitov. 24 bitov je vždy vyhradených pre inicializačný vektor.

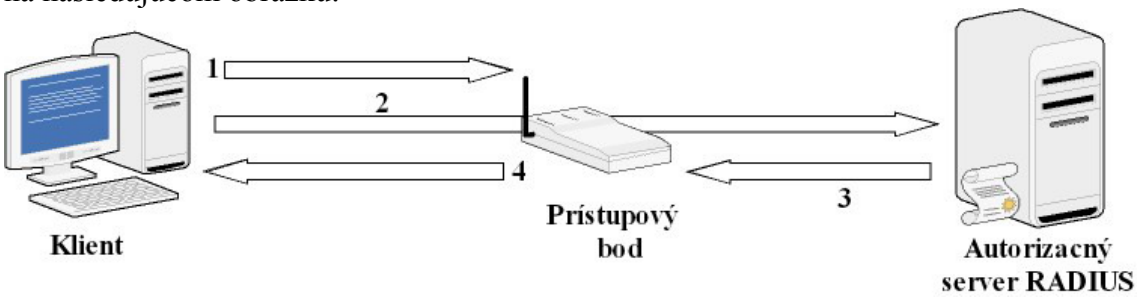
2. 802.1x

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. [1]

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:



Obr. 3. *Autentizácia podľa 802.1x*

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 [2].

3. WPA

Protokol WPA bol ohlásený v roku 2002 alianciou WiFi. 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). WiFi 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) [1].

WPA rieši problémy protokolu WEP prostredníctvom mechanizmov TKIP a 802.1x nasledovne:

TKIP rieši tieto slabiny [1]:

- 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.

Protokol 802.1x rieši tieto slabiny [1]:

- 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.

4. IEEE 802.11i

IEEE 802.11i je ďalším rozšírením bezpečnosti bezdrôtových sietí. Tento štandard bude platný pre všetky bezdrôtové siete a bude založený na šifrovaní pomocou šifry AES v rámci autentizačného rámca EAP. Produkty podporujúce 802.11 by sa mali postupne dostávať na trh. Implementácia AES si vyžiada zvýšenie výkonu hardvéru pre šifrovanie a dešifrovanie. [2]

Podmnožinou 802.11i je WPA, ktoré slúži ako dočasné riešenie pre zvýšenie bezpečnosti. V čase nasadenia WPA ešte nebola hotová primárna časť protokolu 802.11i, ktorou je šifra AES. V špecifikácii 802.11i je AES povinné, pričom TKIP je voliteľné. Šifra AES bola navrhnutá ako náhrada za šifru RC4. AES ponúka rôzne režimy činnosti, v špecifikácii 802.11i sa používa čítačový režim s protokolom CBC-MAC (CCM), obvykle označovaný ako AES-CCMP. Čítačový režim zaisťuje šifrovanie, CBC-MAC potom zaisťuje autentizáciu a integritu dát. 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. CCMP obsahuje nový algoritmus MIC, ktorý zaisťuje aby nedošlo k modifikácii prenášaných dát. Výpočet MIC je založený na inicializačných hodnotách vychádzajúcich z IV a z ďalších hlavičkových informácií. Pracuje sa v 128 bitových blokoch a počíta sa cez jednotlivé bloky až nakoniec originálnej správy, keď sa vypočíta originálna hodnota. [1]

Čítačový režim šifrovania šifrou AES sa výrazne odlišuje od WEP/TKIP a RC4. Výstupom šifry AES je po inicializácii (založenej na IV a ďalších hlavičkových informáciách) len 128 bitový blok. 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. AES vyžaduje nový, výkonnejší hardvér a je preto nekompatibilný so súčasnou generáciou bezdrôtových zariadení [1].

Typy útokov na bezdrôtové siete a spôsob ochrany

Ak chceme niečo chrániť, je potrebné mať prehľad o možných spôsoboch útokov. V nasledujúcej časti článku v krátkosti popisujeme niektoré typy útokov:

- **Zistenie hodnoty SSID**
  Nepatrí medzi útoky, ale hodnota SSID je prvou a najdôležitejšou informáciou, ktorú je potrebné zistiť ak sa chceme prihlásiť do bezdrôtovej siete. V protokole 802.11 sa SSID používa k rozlíšeniu medzi prístupovými bodmi. Zistenie hodnoty SSID je jednoduché, zobrazí ho každá metóda prieskumu siete pretože hodnoty SSID sa nájdu v mnohých typoch komunikácie: signálny paket (Beacon), sondážny paket (Probe Request), odpovede na sondy (Probe Response), žiadosti o pridruženie (Reassociation Request). [3]
- **Rozlúštenie WEP kľúča**
  V skratke sa dá povedať, že na WEP boli z hľadiska narušenia zabezpečenia u systémov úspešné nasledujúce typy útokov: [1]
  - 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.*
  Ochrana: používať ďalšie šifrovanie a autentizačné mechanizmy, napríklad VPN a 802.1x.

- **Zistenie MAC adresy (MAC attack)**
  Ak nie je aktivované WEP, stačí útočníkovi odchytávať komunikáciu, vyhľadať si hlavičku rámca a nájsť tam MAC adresu. Ak je WEP aktivované, je potrebné najskôr WEP dekódovať, ale na to stačí aj offline analýza zachytených dátových rámcov. Ak má útočník k dispozícii MAC adresu, môže vystupovať ako oprávnený klient.
  Ochrana: tomuto typu útokov sa dá predchádzať použitím autentizačných mechanizmov ako 802.1x a použitím zabezpečenia na báze VPN.
- **Útok typu Man-in-the-Middle**
  Útok typu *„muž uprostred“* funguje tak, že útočník vstúpi medzi prístupový bod a klienta. Klient aj prístupový bod si myslia, že komunikujú medzi sebou a *„muža uprostred“* nevidia.
  Ochrana: samotný útok je náročnejší, ale aj ochrana proti nemu je veľmi zložitá. Ak sa podarí takýto útok, je veľmi ťažké prísť na to, že vôbec prebieha. Čiastočnou ochranou môže byť použitie VPN a autentizačných mechanizmov 802.1x. Je dobré mať rádiovú mapu siete a z času na čas manuálne skontrolovať či náhodou nevysiela nejaký podvrhnutý prístupový bod.
- **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.
- **Session Hijacking**
  Session Hijacking znamená, že útočník nielenže odchytáva prenášané dáta, ale tiež do nich vkladá vlastné informácie.
  Ochrana: autentizácia 802.1x a VPN môžu zosilniť ochranu proti tomuto typu útoku.
- **Denial of Service (DoS)**
  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.
  Ochrana: ak sú útoky vedené zvonka (z Internetu), veľmi účinné je filtrovanie MAC adries. Tiež pomáha dobre nastavený firewall s dobrou analýzou paketov.

Záver

Existujú aliancie a skupiny, ktoré sa zaoberajú bezpečnosťou WiFi. Stále sa pracuje na nových štandardoch a nových formách zabezpečenia sietí. Napriek tomu je znalosť používateľov veľmi nízka a existuje len málo ľudí, ktorí si dokážu zabezpečiť sieť. Zvyčajne sa jedná o veľké firmy. Pre skúsenejšieho človeka nie je problém dostať sa do väčšiny sietí – z praxe nám vychádza, že je to približne 90 %. Z toho vyplýva, že hlavným bodom úrazu, okrem slabých mechanizmov ako WEP, je malá informovanosť ľudí v oblasti bezpečnosti.

Zoznam bibliografických odkazov:

[1] BARKEN, Lee. *Wi-Fi - Jak zabezpečit bezdrátovou síť.* Brno: Computer Press, 2004. 174 s. ISBN 80-251-0346-3

[2] ZANDL, Patrick. *Bezdrátové síte WiFi, praktický prúvodce.* Brno: Computer Press, 2003. 198 s. ISBN 80-7226-632-2

[3] McCLURE, S., SCAMBARY, J., KURTZ, G. *Hacking bez tajemství.* Brno: Computer Press, 2003. 612 s. ISBN 80-7226-948-8