FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
UNIVERZITY KOMENSKÉHO
V BRATISLAVE

DIPLOMOVÁ PRÁCA

BRATISLAVA 2007 EVA SZARKOVÁ

Bezpečnosť bezdrôtových sietí štandardu IEEE 802.11

DIPLOMOVÁ PRÁCA

Eva Szarková

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY
KATEDRA INFORMATIKY

Študijný odbor Informatika

Vedúci diplomovej práce
RNDr. Jaroslav Janáček

BRATISLAVA 2007

Čestné prehlásenie

Čestne prehlasujem, že som diplomovú prácu vypracovala samostatne pod dohľadom vedúceho diplomovej práce a len s použitím uvedenej literatúry.

_____

Poďakovanie

Ďakujem svojmu vedúcemu diplomovej práce RNDr. Jaroslavovi Janáčkovi za odborné vedenie práce, podnetné diskusie a cenné rady.

Ďakujem aj mojej rodine a priateľom za ich podporu v období písania tejto diplomovej práce.

Abstrakt

Diplomová práca sa zaoberá analýzou bezpečnosti bezdrôtových sietí na báze štandardu IEEE 802.11. Práca vychádza zo štúdia odbornej literatúry, štúdia štandardov, z analýzy a odskúšania množstva dostupných produktov a zariadení súvisiacich s danou problematikou.

Práca identifikuje a analyzuje bezpečnostné trhliny štandardu IEEE 802.11 a popisuje možnosti využitia dostupných nástrojov na ochranu alebo aj oslabenie zabezpečenia spomínaného štandardu. Niektoré uvedené techniky a nástroje sa podarilo úspešne experimentálne vyskúšať a overiť ich schopnosti.

Kľúčové slová

IEEE 802.11, WEP, bezpečnosť, bezdrôtové siete, bezpečnosť bezdrôtových sietí

Predhovor

Hlavným cieľom mojej diplomovej práce je analýza techník zabezpečenia alebo oslabenia bezpečnosti štandardu IEEE 802.11 za pomoci množstva odbornej literatúry a dostupných nástrojov z internetu. Zároveň je mojim cieľom poskytnúť široký prehľad a kategorizáciu nástrojov týkajúcich sa vybranej problematiky.

Vzhľadom na to, že podľa mojich informácií v súčasnosti takýto obsiahly a zjednocujúci prehľad možností štandardu IEEE 802.11 v oblasti bezpečnosti s experimentálnymi poznatkami neexistuje, rozhodla som sa formou predloženej práce prispieť a poskytnúť širokej verejnosti komplexný pohľad do uvedenej problematiky.

Zoznam obrázkov

Zoznam tabuliek

Zoznam skratiek

ACK (Acknowledge) - potvrdenie

AP (Access Point) – prístupový bod

ARC4 (Assumed RC4) – šifrovací algoritmus funkčne ekvivalentný s RC4 algoritmom

ARP (Address Resolution Protocol) – sieťový protokol

ASCII (American Standard Code for Information Interchange) – kódová tabuľka

ATIM (Announcement Traffic Indication Message) – druh rámca štandardu 802.11

BSS (Basic Service Set) – množina navzájom prepojených bezdrôtových staníc

CF-ACK (Contention-Free Acknowledgement) – potvrdenie o začatí bezkolízneho vysielania

CF-End (Contention-Free End) – ukončenie bezkolízneho vysielania

CF-Poll (Contention-Free Poll) – odovzdanie tokenu bezkolízneho vysielania

CRC-32 (Cyclic Redundancy Check 32-bit) – 32-bitový kontrolný súčet

CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance) – schéma prístupu k zdieľanému médiu

CTS (Clear to send) – potvrdenie o možnosti odoslať dáta

DA (Destination Address) – cieľová adresa MSDU

DHCP (Dynamic Host Configuration Protocol) - sieťový protokol

DoS (Denial-of-Service) – narušenie dostupnosti služby

DS (Distribution System) – distribučný systém

ESS (Extended Service Set) – rozšírená množina navzájom prepojených bezdrôtových staníc

ETSI (European Telecommunications Standards Institute) – organizácia vyvíjajúca štandardy

FCS (Frame Check Sequence) – kontrolný súčet rámca

FMS (Fluher-Martin-Shamir) – typ útoku na WEP

IBSS (Independent Basic Service Set) – Ad-hoc topológia bezdrôtovej siete

ICMP (Internet Control Message Protocol) - sieťový protokol

ICV (Integrity Check Value) – kontrolný súčet pre zachovanie integrity dát

ID (Identification) - označenie

IEEE (The Institute of Electrical and Electronic Engineers) – organizácia vyvíjajúca štandardy

IETF (Internet Engineering Task Force) - organizácia vyvíjajúca štandardy

IP (Internet Protokol) - sieťový protokol

ISO/OSI (International Standards Organization/Open Systems Interface) –druh modelu sieťovej architektúry

IV (Initialization Vector) – inicializačný vektor

KSA (key scheduling algorithm) – algoritmus generovania kľúčov

LLC (Logical Link Control) – podvrstva logických spojov v ISO/OSI modeli

MAC (Media Access Control) – podvrstva prístupu k médiu v ISO/OSI modeli

MPDU (MAC Protocol Data Unit) – balíček dát MAC protokolu

MSDU (MAC Service Data Unit) – balíček dát MAC vrstvy

NATO (North Atlantic Treaty Organization) – Organizácia Severoatlantickej zmluvy

OFDM (orthogonal frequency-division multiplexing) – modulačná schéma s viacerými nosnými kanálmi

PCMCIA (Personal Computer Memory Card Interface Adapter) – Typ adaptéru do počítača

PDA (Personal Digital Assistant) – vreckový počítač

PRGA (Pseudo Rangom Generator Algorithm) – algoritmus generovania pseudo-náhodných hodnôt

Pwr Mgt (Power Management) – riadenie spotreby energie

QoS (Quality of Service) – kvalita služieb

RA (Receiver Address) – adresa nasledujúcej stanice v DS

RC4 (Rivest Cipher4) – šifrovací algoritmus

RFC (Request for Comments) – dokument k pripomienkovaniu

RTS (Request To Send) – požiadavka na odoslanie dát

SA (Source Address) – adresa odosielateľa MSDU

SQL (Structured Query Language) –programovací jazyk

SSID (Service Set Identifier) – unikátny názov AP

SSL (Secure Sockets Layer) – šifrovací protokol

TA (Transmitter address) – adresa vysielajúcej stanice v DS

TCP SYN (TCP Synchronization) – synchronizačný paket TCP protokolu

TCP (Transmission Control Protocol) - sieťový protokol

UDP (User Datagram Protocol) - sieťový protokol

USA (United States of America) – Spojené štáty americké

WEP (Wired Equivalent Privacy) - bezpečnosť ekvivalentná káblom

WPA (Wi-Fi Protected Access) – bezpečný prístup k bezdrôtovej sieti

XOR (eXclusive OR) – adícia modulo 2

Obsah

Úvod

Aj napriek tomu, že štandard IEEE 802.11 je pomerne starý [20], rozhodla som sa mu venovať z toho dôvodu, že práve v týchto rokoch zaznamenáva najväčší nárast použitia nielen v pracovnom, ale aj v bežnom živote. V posledných rokoch bol zaznamenaný aj vďaka obľúbenosti vysoký nárast produktivity nástrojov na uľahčenie administrácie, sledovania alebo aj oslabenia bezdrôtových sietí.

V silne zahustenom prostredí bezdrôtových sietí sa problematika bezpečnosti stáva čoraz viac aktuálnejšou. Tento problém zvyčajne je spôsobený aj neinformovanosťou používateľov technológií, ponechaním zariadení v základnom nastavení ako aj ľahostajný postoj k bezpečnosti.

Výskum v oblasti bezpečnosti nasledujúcich štandardov rodiny IEEE 802.11 poukazuje na fakt, že existuje snaha o vyriešenie problematických úsekov a stáva sa žiadanou zo strany používateľov. Nasledovníkom WEP je WPA (Wi-Fi Protected Access) a WPA2, ktorému sa v predloženej práci nevenujem, nakoľko sa jedná už o variantu štandardu IEEE 802.11i.

Táto práca sa venuje práve bezpečnosti pôvodného štandardu IEEE 802.11 z hľadiska jeho sily, slabých miest, efektivity, možností a vhodnosti použitia. Pozornosť zameriavam najmä na WEP protokol, ktorý je jeho súčasťou.

Práca čitateľovi umožňuje nahliadnuť do spomínanej problematiky bez nutnosti poznať detaily štandardu a pochopiť slabé miesta jeho zabezpečenia. Čitateľovi pomôže zorientovať sa v množstve nástrojov, ktoré sú dnes dostupné pre rôzne operačné systémy.

V kapitole 1 popisujem základné pojmy potrebné pre pochopenie opisovanej problematiky v ďalších častiach práce. V kapitole 2 sa venujem rozoberaniu pôvodného štandardu IEEE 802.11 od modelu sieťovej architektúry, cez popis služieb až po rozoberanie rámcov hlavičiek paketov prenášaných cez bezdrôtové médium. V 3. kapitole sa venujem WEP protokolu s popisom šifrovacieho RC4 algoritmu a rozoberám proces enkapsulácie dát pred ich odoslaním v zašifrovanej forme a proces dekapsulácie dát pri dešifrovaní. 4. kapitola sa venuje v krátkosti problematike samotného použitia šifrovania v bezdrôtových sieťach spomínaného štandardu.

Najdôležitejšou kapitolou celej práce je kapitola 5, v ktorej opisujem rôzne typy útokov na bezpečnosť štandardu. Upozorňujem, že najmä v tejto kapitole sa od čitateľa vyžadujú základné znalosti sieťovej architektúry a protokolov IP, TCP, UDP, ARP, ICMP a DHCP, ktoré v práci nie sú vysvetlené.

Po 5. kapitole nasleduje experimentálna časť, v ktorej ukazujem možnosti niektorých vybraných nástrojov, ako aj funkcionalitu štandardu a niektoré spôsoby oslabenia bezpečnosti. Pomerne veľký zoznam užitočných nástrojov týkajúcich sa tejto témy s krátkymi informáciami o druhu nástroja a jeho použiteľnosti som umiestnila do prílohy tejto práce.

1 Základné pojmy

1.1 IEEE

IEEE (The Institute of Electrical and Electronic Engineers) je inštitúcia, ktorá sa zaoberá vyvíjaním štandardov pre veľa druhov systémov. Organizácia je známa najmä vďaka štandardom na výmenu informácií medzi počítačmi (triedou 802). Na vývoji štandardov sa podieľajú dobrovoľníci – experti v danej oblasti. Komisie na schvaľovanie štandardov používajú klasické postupy hlasovaním a pripomienkovaním. Po odsúhlasení zverejnia štandard, ktorý je majetkom IEEE a je po 6 mesiacoch zadarmo stiahnuteľný z internetu pre akékoľvek použitie. Všetky štandardy sú k dispozícii na [20] a [30].

IEEE nie je jedinou organizáciou vyvíjajúcou štandardy. K bezdrôtovým sieťam existujú aj štandardy od IETF (Internet Engineering Task Force), ETSI (European Telecommunications Standard Institute) a mnoho ďalších. Okrem iného existuje aj Wi-Fi aliancia, ktorá testuje, či rôzne zariadenia predávané na trhu dokážu navzájom spolupracovať a či spĺňajú štandardy uvádzané v ich špecifikáciách. V prípade, že zariadenie prejde takýmto testom, dostane Wi-Fi certifikát (logo aliancie).

1.2 MSDU

MSDU (MAC Service Data Unit) je základný balíček dát určený na prenos cez fyzickú vrstvu ISO/OSI (International Standards Organization/Open Systems Interface) modelu, ktorý sa ešte v spodných vrstvách modelu môže fragmentovať na menšie kusy, tzv. MPDU (MAC Protocol Data Unit).

1.3 Algoritmus

Algoritmus je explicitná množina inštrukcií, ktoré majú určený štartovný a cieľový bod.

1.4 Bezpečnostné mechanizmy

Základnými bezpečnostnými mechanizmami sú dôvernosť, integrita a dostupnosť, autentifikácia a autorizácia (kontrola prístupu). Nasledujú formálne definície mechanizmov.

1.4.1 Dôvernosť

Dôvernosť je možnosť odoslať a prijať dáta bez prezradenia nejakej časti dát neautorizovanej entite počas prenosu dát.

1.4.2 Integrita

Integritou sa rozumie mať možnosť odoslať a prijať dáta tak, aby neautorizovaná entita nemohla zmeniť akúkoľvek časť prenášaných dát bez toho, aby odosielateľ alebo prijímateľ dát vedel zistiť zmenu dát. Ak sú dostupné len mechanizmy na uchovanie integrity dát, dáta môžu byť zmenené, ale prijímateľ, resp. odosielateľ zistia, že boli zmenené počas prenosu.

1.4.3 Dostupnosť

Dostupnosť je možnosť prijať a odoslať dáta.

1.4.4 Autentifikácia

Autentifikácia zisťuje identitu prijímateľa alebo odosielateľa informácií.

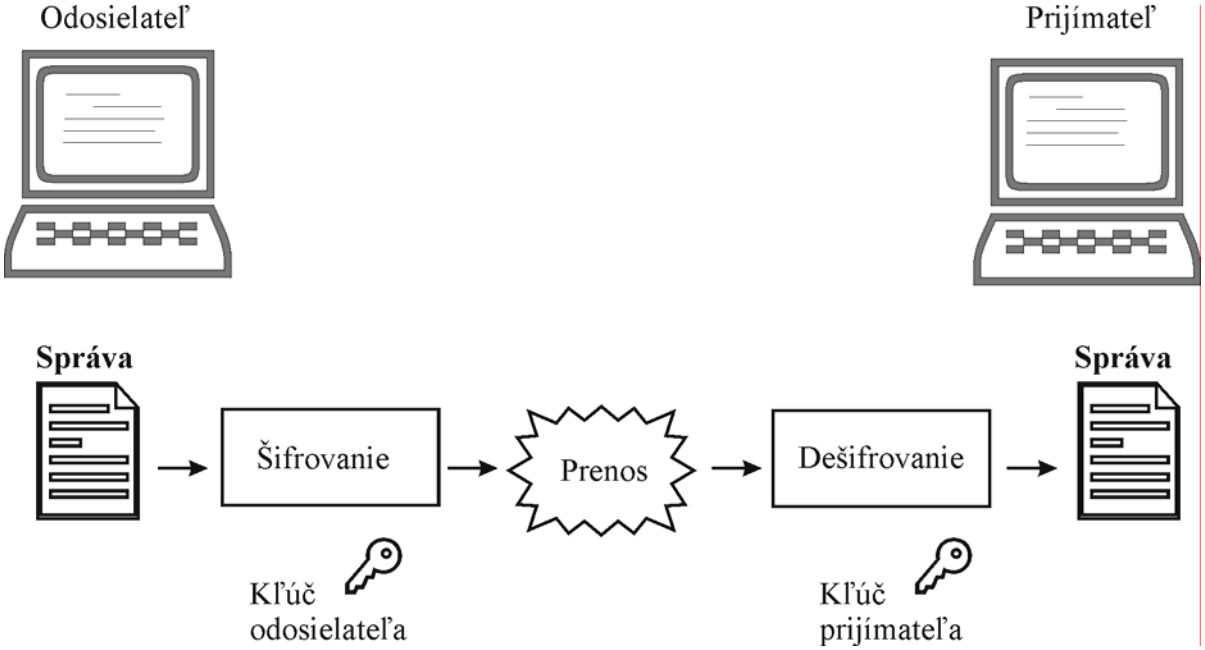
1.4.5 Autorizácia

Autorizácia zisťuje, čo má používateľ dovolené v sieti robiť. Taktiež je nazývaná ako kontrola prístupu k zdrojom siete. Nie vždy je nutná autentifikácia pred autorizáciou, avšak vo väčšine prípadov (najmä v bezdrôtových sieťach) je s ňou pevne spojená.

1.5 Šifrovanie

Šifrovanie (Obr. 1) si kladie za cieľ transformovať vstupné dáta do podoby, v ktorej sú pre potenciálneho útočníka nezrozumiteľné a nie je schopný rekonštruovať ich pôvodný tvar. Zároveň požadujeme, aby oprávnené subjekty mohli pôvodné dáta rekonštruovať. Vstupné dáta v ich pôvodnej podobe budeme nazývať pôvodný text (príp. správa, dáta). Proces ich transformácie sa nazýva šifrovanie a je realizované šifrovacím algoritmom. Výsledok šifrovania je zašifrovaný text. Šifrovací algoritmus je parametrizovaný ďalším vstupom - kľúčom, ktorý nezávisí na pôvodnom texte.

Proces inverznej transformácie, keď zo zašifrovaného textu dostaneme opäť pôvodný text, sa nazýva dešifrovanie a je realizovaný dešifrovacím algoritmom. Dešifrovací algoritmus je taktiež parametrizovaný kľúčom.



Obr. 1 - Šifrovanie

1.5.1 Symetrická šifra

Symetrická šifra zahŕňa všetky spôsoby šifrovania, pri ktorých jediným, teda tým istým kľúčom požadovaný text zašifrujeme aj dešifrujeme. Šifrovanie aj dešifrovanie sú navzájom opačné, ale rovnaké procesy.

Moderné symetrické šifrovacie systémy používajú kľúče pevnej dĺžky (napr. 128 bitov), ktoré môžeme použiť aj na šifrovanie podstatne dlhších textov. Teda na umožnenie dôverného prenosu dát (v podstate) ľubovoľnej dĺžky stačí dôverne preniesť adresátovi relatívne krátky tajný kľúč.

Symetrické šifrovacie systémy môžeme rozdeliť na blokové a prúdové šifry.

1.5.2 Bloková šifra

Blokové šifry spracúvajú vstupný text po blokoch pevnej dĺžky (napr. 64 bitov), pričom šifrovacia funkcia je definovaná ako nemenná transformácia jedného bloku dát. Dešifrovanie je tiež definované nad jednotlivými blokmi. Typicky existuje veľkostná premenná, ktorá určuje aký maximálne veľký kus dát sa šifruje naraz. Bez ohľadu na veľkosť sa na zašifrovanie použije celý kľúč.

Pri šifrovaní sa používa jeden kľúč na celý objem dát. Nasledujúca rovnosť ilustruje jednoduchosť tohto typu šifrovania, ako aj jeho zraniteľnosť:

Šifrovacia funkcia (dáta, heslo) = Výsledok

Poznamenajme, že celý kľúč je použitý pri každom šifrovaní dát v pôvodnej forme. S kontinuálnym používaním toho istého kľúča je blokové šifrovanie slabé.

Šifrovacia funkcia nie je v tradičnej blokovej šifre závislá od predchádzajúcich blokov.

1.5.3 Prúdová šifra

Prúdová šifra je schopná zašifrovať dáta na detailnej úrovni. Bloková šifra môže zakódovať celú stránku textu v jednom kroku, prúdová šifra naopak môže kódovať bity jedného písmenka textu. Toto odstraňuje potrebu zhromažďovania údajov do bloku pred šifrovaním, ako je to nutné v tradičnej blokovej šifre.

Pri prechode prúdovou šifrou sa generujú dva prúdy, z ktorých jeden výstup je vstupom pre druhý. Matematicky vyjadrené, výstup je vytvorený použitím dvoch funkcií na rozdiel od blokovej šifry.

Prúdová šifra používa stavovú premennú k heslu. To znamená, že šifrovací algoritmus potrebuje pamäť pre stavovú premennú. Prvá funkcia využíva hodnotu stavu spolu s heslom a prípadne aj obsahom kódovaných dát na vygenerovanie pseudo-náhodného prúdového kľúča, ktorý sa vďaka stavovej premennej neustále mení. Dobrá prúdová šifra nikdy nepoužije rovnaký prúdový kľúč dvakrát. Prúdový kľúč by mal byť rovnakej veľkosti ako blok šifrovaných dát.

V tradičnej prúdovej šifre je každý prvok (napr. každý bajt) správy šifrovaný nezávisle a nemá vplyv na žiadny ďalší prvok. V niektorých rozšíreniach prúdových šifier môže hodnota jednej správy ovplyvniť zašifrovanie nasledujúcich znakov správy, ale nemôže zmeniť zašifrovanie predchádzajúcich znakov správy. Naproti tomu v blokovej šifre aj zmena posledného bitu bloku bude vo všeobecnosti meniť okolo polovicu predchádzajúcich bitov v tom istom bloku.

Rozdiel medzi prúdovými a blokovými šiframi nie je jednoznačne určený, nakoľko bloková šifra rozšírená o malý kus pamäte s malou veľkostnou premennou vyústi v prúdovú šifru. Vo všeobecnosti sú prúdové šifry rýchlejšie a vhodnejšie do niektorých aplikácií, napr. pri obmedzenej veľkosti pamäti, pri nutnosti okamžitého kódovania prúdu znakov, alebo v prípade chybového prenosového kanála.

Prúdové šifry delíme na synchrónne a asynchrónne.

Synchrónna prúdová šifra

Nasledujú funkcie, ktoré charakterizujú synchrónnu prúdovú šifru:

$$Stav_{čas+1} = \text{Stavová funkcia} (Stav_{čas}, \text{Heslo})$$

$$\text{Prúdový kľúč}_{čas} = \text{Kľúčová funkcia} (Stav_{čas}, \text{Heslo})$$

$$\text{Výsledok} = \text{Šifrovacia funkcia} (\text{Prúdový kľúč}_{čas}, Dáta_{čas})$$

Šifrovacia funkcia môže pozostávať z ľubovoľnej matematickej funkcie počínajúc od jednoduchého sčítania dvoch hodnôt. Počiatočný stav je vypočítaný z kľúča.

Výsledok je závislý od troch premenných (heslo, stav a prúdový kľúč) a , z ktorých sa dve neustále menia (heslo je konštantné). To robí z prúdovej šifry silný nástroj na kódovanie informácií. Aj v prípade, že existuje predpokladaná hodnota dát, stav bude neustále iný a tým značne zníži útočníkovi šancu na extrahovanie relevantných dát zo zašifrovanej správy.

V prípade synchrónnej prúdovej šifry musia byť odosielateľ aj prijímateľ zosynchronizovaní – musia používať rovnaké heslo a byť v tom istom stave. Ak je synchronizácia narušená vložením alebo vymazaním znakov zašifrovaného textu, dešifrovanie zlyhá a musí nastať resynchronizácia. Resynchronizácii môže pomôcť napríklad znovu-inicializácia alebo aj umiestnenie špeciálnych kontrolných značiek v pravidelných intervaloch do šifrovaného textu.

Modifikácia zašifrovaného znaku neovplyvňuje dešifrovací proces ostatných znakov. Avšak je nutné zaviesť ďalšie opatrenia na zabezpečenie integrity dát.

Asynchrónna prúdová šifra

Asynchrónnu alebo samostatne sa synchronizujúcu prúdovú šifru charakterizujú nasledujúce funkcie:

$$\text{Stav}_{\text{čas}} = \text{Stavová funkcia} (\text{Dáta}_{\text{čas}})$$

$$\text{Prúdový kľúč}_{\text{čas}} = \text{Kľúčová funkcia} (\text{Stav}_{\text{čas}}, \text{Heslo})$$

$$\text{Výsledok} = \text{Šifrovacia funkcia} (\text{Prúdový kľúč}_{\text{čas}}, \text{Dáta}_{\text{čas}})$$

Šifrovacia funkcia môže pozostávať z ľubovoľnej matematickej funkcie počínajúc od jednoduchého sčítania dvoch hodnôt. Počiatočný stav nie je tajný.

Vložením alebo vymazaním znakov zašifrovaného textu môže nastať samostatná synchronizácia, pretože stav ovplyvňuje len fixný počet *t* predchádzajúcich znakov šifrovaného textu. V prípade poškodenia niektorého z *t* predchádzajúcich znakov dešifrovací proces všetkých nasledujúcich znakov zlyhá. Preto je nutné zaviesť dodatočnú kontrolu vkladania, mazania a modifikácie znakov šifrovaného textu. Asynchónne prúdové šifry nie sú z tohto dôvodu príliš vhodné do chybového prostredia v porovnaní so synchrónnymi prúdovými šiframi.

2 Špecifikácia štandardu IEEE 802.11

Štandard IEEE 802.11 [20] vznikol v roku 1999. Štandard sa týka bezdrôtových sietí používajúcich rádiový signál vo voľnej frekvencii 2.4 GHz alebo v infračervenej frekvencii. Maximálna prenosová rýchlosť pôvodného štandardu je 2 Mbps. Neskôr bol štandard rozšírený o ďalšie frekvencie, rýchlosti prenosu, ďalšie druhy zabezpečení a QoS (Quality of Service) služieb.

Všetky ďalšie verzie štandardu 802.11 sú označené písmenom. Medzi najznámejšie patrí 802.11b, ktorý dosahuje rýchlosti 5 a 11 Mbps vo frekvencii 2,4 GHz a má možnosť rozšírenia WEP (Wired Equivalent Privacy) hesla na 104 bitov. Ďalším obľúbeným štandardom je 802.11a operujúci na frekvencii 5 GHz s prenosovými rýchlosťami do 54 Mbps a nesmiem vynechať ani pomerne nový štandard 802.11g, ktorý má lepšie zabezpečenie dôvernosti dát a vďaka tomu, že používa rovnaký spôsob multiplexovania OFDM (orthogonal frequency-division multiplexing) ako 802.11a, dosahuje prenosovú rýchlosť do 54 Mbps už aj na frekvencii 2,4 GHz .

2.1 Model sieťovej architektúry

Pôvodný štandard IEEE 802.11 (ďalej len štandard 802.11 alebo štandard) špecifikuje prvé dve vrstvy štandardného modelu sieťovej architektúry ISO/OSI (Obr. 2) – fyzickú vrstvu a časť linkovej vrstvy, tzv. podvrstvu riadenia prístupu k médiu (Media Access Control – MAC vrstva).

Úlohou fyzickej vrstvy siete je prenos signálu po prenosovom médiu. Fyzická vrstva popisuje samotné prenosové médium a povahu prenášaného signálu. Samotným prenášaným dátam nerozumie, chápe ich len ako prúd bitov. Fyzickej vrstve sa v tejto práci venovať nebudem.

Linková vrstva zabezpečuje prenos údajov (dátových rámcov) po fyzickom médiu z jedného koncového zariadenia do druhého. Je rozdelená do podvrstvy logických spojov (Logical Link Control - LLC) a podvrstvy riadenia prístupu k médiu (MAC), ktorá už pracuje s fyzickými adresami. MAC podvrstva poskytuje služby LLC podvrstve a využíva služby fyzickej vrstvy. LLC podvrstva používaná v bezdrôtových sieťach je definovaná štandardom IEEE 802.2.

Podvrstva MAC v štandarde 802.11 má tri funkcie:

- Poskytuje funkcionalitu na zabezpečenie spoľahlivého prenosu dát pre vyššie vrstvy. Samotný prenos dát je asynchrónny, connectionless (nevytvára sa spojenie pred odosielaním rámcov) a bez garancie doručenia rámcov.
- Poskytuje kontrolu prístupu k zdieľanému bezdrôtovému médiu pomocou CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance) metódy. Táto metóda sa využíva hlavne v bezdrôtových sieťach, kde nie je možné spoľahlivo zistiť kolíziu.

- Poskytuje možnosť zabezpečiť prenášané dáta pomocou WEP protokolu.

	Druh dát	Vrstvy modelu	
Vrstvy stroja	Dáta	**Aplikačná** Sieťový proces aplikácií	
	Dáta	**Prezentačná** Jednotná reprezentácia dátových štruktúr	
	Dáta	**Relačná** Komunikácia medzi strojmi	
	Segmenty	**Transportná** Vytvára zdanie bezchybného kanála medzi dvomi procesmi bežiacimi v ľubovoľných uzloch siete	
Vrstvy média	Pakety	**Sieťová** Rieši doručenie správy na ľubovoľné miesto v sieti (logické adresovanie)	
	Rámce	**Linková** Vytvára zdanie bezchybného kanála medzi susednými uzlami (fyzické adresovanie)	LLC MAC
	Bity	**Fyzická** Prenos bitov cez fyzické médium	

Obr. 2 – ISO/OSI model sieťovej architektúry

2.1.1 CSMA/CA

CSMA/CA metóda funguje na princípe „počúvaj predtým, než začneš hovoriť“. To znamená, že odosielateľ dát, ktorý chce vysielať sleduje prenos na vysielacom kanále a až keď je médium voľné začne vysielať. Značné percento dostupnej kapacity prenosového kanála je obetované (mechanizmom CSMA/CA) za účelom zvýšenia spoľahlivosti pri prenose údajov cez rôzne heterogénne a znečistené prostredia.

CSMA/CA sa vyhýba kolíziám na médiu stanovením náhodného času čakania pri neúspešnom vysielaní. V prípade, že médium je opakovane obsadené, bude odosielateľ naďalej čakať stále s náhodným, ale s exponenciálne menším časovým odstupom.

Kým metódy na detekciu kolízií sú dobrým nástrojom v káblových sieťach, v bezdrôtových sú nepoužiteľné z dvoch dôvodov:

- Implementácia mechanizmu na detekciu kolízií by vyžadovala implementáciu obojsmernej komunikácie v jednom čase.
- Nedá sa zabezpečiť, aby sa všetky stanice navzájom počuli a preto môže nastať situácia, že kolízia nastane u prijímateľa dát, ktorý môže byť medzi dvomi naraz vysielajúcimi odosielateľmi. Tento problém sa nazýva kolízia navzájom sa nepočujúcich staníc.

2.2 Architektúra

Architektúra štandardu 802.11 pozostáva z niekoľkých komponentov a služieb, ktoré vzájomne poskytujú mobilitu transparentnú pre vyššie sieťové vrstvy ISO/OSI modelu.

2.2.1 Stanica

Stanica je najzákladnejší komponent bezdrôtovej siete. Stanica je ľubovoľné zariadenie, ktoré obsahuje funkcionalitu 802.11 protokolu. Stanicou môže byť prístupový bod (Access Point alebo AP), notebook, PDA (Personal Digital Assistant – vreckový počítač) alebo iné zariadenie podporujúce štandard 802.11. Stanice môžu byť pohyblivé alebo aj stacionárne.

2.2.2 Basic Service Set (BSS)

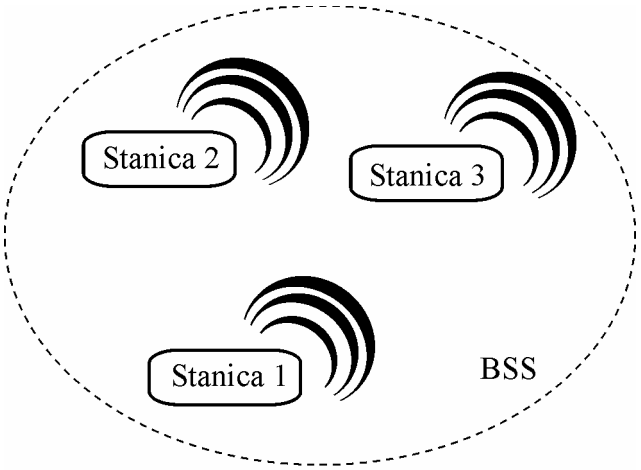
BSS je základným stavebným kameňom bezdrôtovej siete 802.11. Pozostáva z akéhokoľvek počtu prepojených staníc.

2.3 Topológie

2.3.1 Ad-hoc

Najzákladnejšou topológiou BSS je množina staníc, ktoré sa navzájom poznajú a sú prepojené cez bezdrôtové médium v podobe peer-to-peer. Táto forma topológie (Obr. 3) sa nazýva taktiež IBSS (Independent Basic Service Set).

V tejto topológii komunikujú stanice priamo medzi sebou. Každá stanica komunikuje len so stanicou v jej dosahu, keďže neexistujú funkcie preposielania (relay).

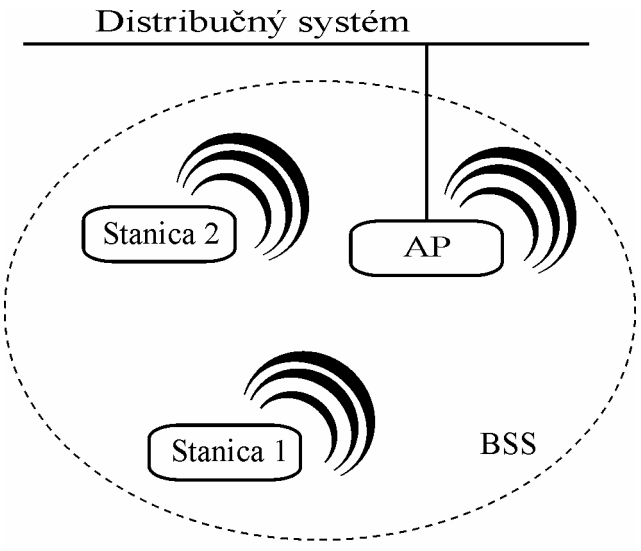


Obr. 3 - Ad-hoc (resp. IBSS) topológia

2.3.2 Infrastructure

Topológia Infrastructure (Obr. 4) má v BSS prvok nazývaný prístupový bod (Access Point alebo AP). AP poskytuje lokálnu funkciu preposielania pre BSS. Všetky ostatné stanice (klienti) v BSS komunikujú medzi sebou už jedine cez AP. Takáto lokálna funkcia preposielania efektívne zdvojnásobí dosah BSS.

AP môže poskytovať aj pripojenie do distribučného systému (DS).



Obr. 4 – Infrastructure topológia

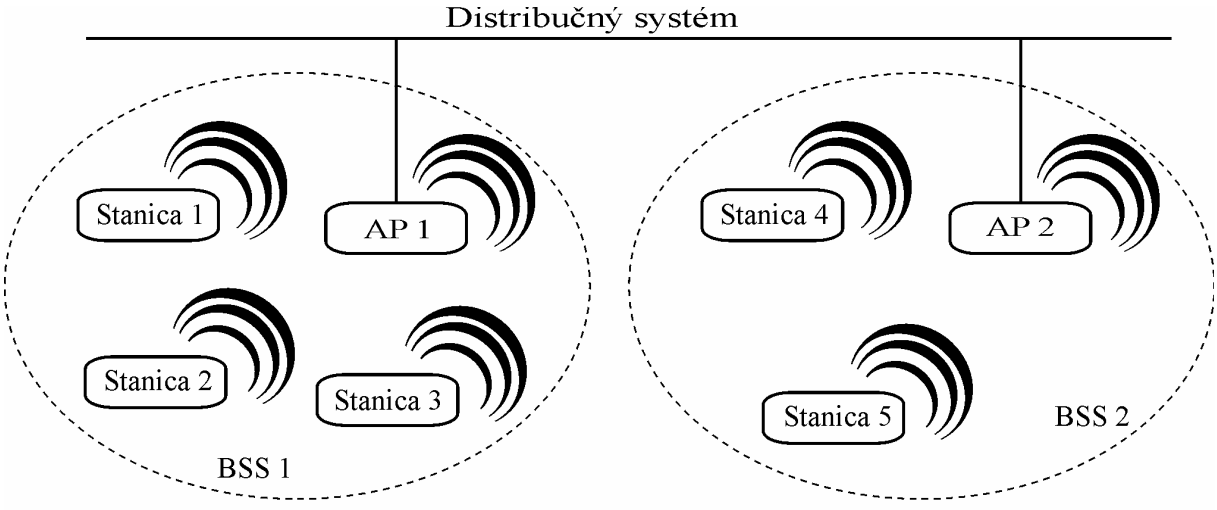
Distribučný systém (DS)

Distribučný systém slúži okrem prepojenia s káblovou sieťou aj na prepojenie viacerých AP, resp. BSS a na poskytnutie roamingu stanici, t.j. plynulého prechodu z jedného BSS do druhého bez prerušenia spojenia. Štandard 802.11 popisuje distribučný systém nie nutne ako sieť a nevymedzuje, ako má byť implementovaný. Typicky je to tenká vrstva implementácie

každého AP, ktorá určuje cieľ každého paketu. Distribučný systém zistí, či paket prijatý z BSS má byť odoslaný naspäť do BSS alebo preposlaný inému AP alebo do káblovej siete mimo Extended Service Set (ESS). Paket prijatý z distribučného systému je preposlaný k cieľovej stanici v rámci BSS.

2.3.3 Extended Service Set (ESS)

ESS (Obr. 5) je množina BSS navzájom prepojených jedným distribučným systémom. Sieťové vybavenie mimo ESS vidí ESS a všetky mobilné stanice ako fyzicky pevné prvky jednotnej siete na MAC vrstve. ESS skrýva mobilitu pred všetkým mimo ESS. Architektúra 802.11 pre túto kompatibilitu na vrstve MAC umožňuje existujúcim protokolom komunikovať korektne s bezdrôtovou sieťou akoby bola pevnou sieťou.



Obr. 5 – ESS (Extended Service Set)

V prípade, že Stanica 1 v BSS 1 chce komunikovať so Stanicou 4 v BSS 2, bude komunikácia prebiehať nasledujúco: Stanica 1 odošle správu AP vo svojom BSS (teda konkrétne AP 1) a to ďalej pomocou distribučného systému prepošle správu AP 2. AP 2 po prijatí správy zistí, že cieľovou stanicou je Stanica 4 v jeho BSS, ktorej správu nakoniec doručí.

2.4 Služby

Štandard IEEE 802.11 nepopisuje konkrétnu implementáciu distribučného systému, popisuje len 9 typov služieb, ktoré sú rozdelené do dvoch kategórií – služby stanice a služby DS. 6 služieb slúži na doručenie MSDU medzi stanicami, 3 slúžia na kontrolu prístupu a dôvernosti.

Služby stanice:

- Autentifikácia
- Deautentifikácia
- Dôvernosť
- Doručenie MSDU

Služby DS:

- Asociácia
- Deasociácia
- Distribúcia
- Integrácia
- Reasociácia

2.4.1 Autentifikácia

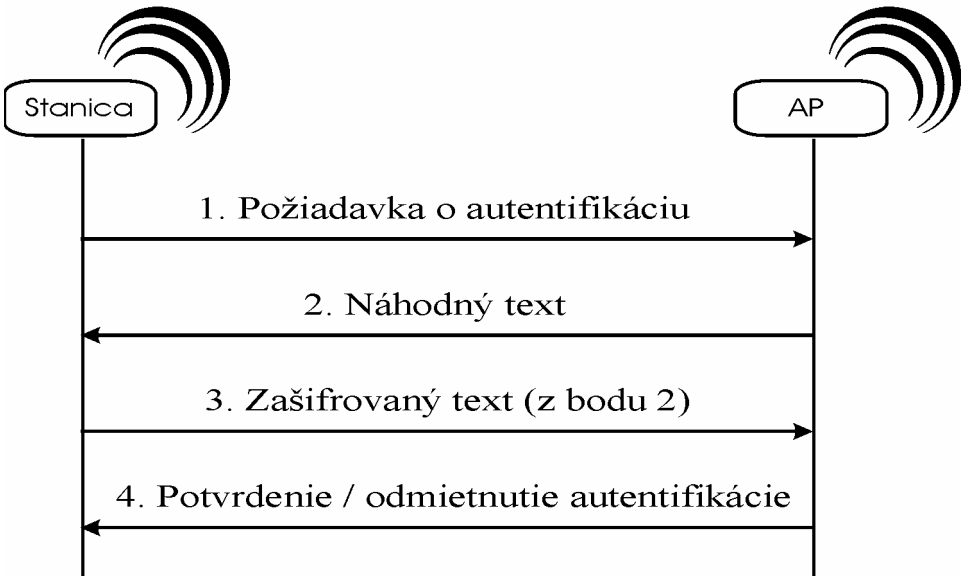
Štandard 802.11 poskytuje možnosť kontroly prístupu k zdrojom siete pomocou služby autentifikácie. Klient môže byť autentifikovaný s viacerými AP naraz. Služba sa nachádza na linkovej vrstve a delí sa na 2 kategórie – Open system a Shared Key.

Open System

Open system autentifikácia je najjednoduchší spôsob autentifikácie. Najskôr stanica pošle požiadavku o open system autentifikáciu s udaním svojej MAC adresy. Následne autentifikačná stanica (obvykle AP) pošle odpoveď s príznakom úspešnosti autentifikácie.

Shared Key

Shared Key autentifikácia vyžaduje aktivované WEP, pretože vyžaduje znalosť zdieľaného WEP hesla a použitie RC4 (Rivest Cipher4) algoritmu. V prípade, že je WEP deaktivované, je povolená len Open System autentifikácia.



Obr. 6 – Shared Key autentifikácia

Autentifikácia prebieha v štyroch krokoch (viď. Obr. 6):

1. Stanica požiada AP o autentifikáciu
2. AP pošle stanici náhodný text (veľkosti 128 oktetov) na zašifrovanie

3. Stanica pošle AP zašifrovaný text (z bodu 2) pomocou WEP hesla a RC4 algoritmu
4. AP po dešifrovaní obdržaného zašifrovaného textu od stanice tento text porovná s pôvodným textom a pošle stanici potvrdenie alebo odmietnutie Shared Key autentifikácie.

Deautentifikácia je vyvolaná v prípade, že existujúca autentifikácia má byť ukončená. Deautentifikácia nie je požiadavka, ale oznámenie a nie je možné ju odmietnuť.

2.4.2 Asociácia

Služba asociácie vytvára vzťah medzi stanicou a AP a umožňuje stanici využívať zdroje DS. Stanica môže byť asociovaná len s jedným AP.

Deasociácia je ukončenie existujúcej asociácie. Realizovaná je formou oznámenia rovnako ako deautentifikácia.

2.4.3 Reasociácia

Reasociácia je prechod asociácie klienta od pôvodného AP k novému AP, ktorý má lepší signál v rámci ESS (tzv. roaming) alebo aj požiadavka stanice o znovu-asociáciu k pôvodnému AP po strate a následnej obnove signálu. Táto služba je takisto používaná na zmenu atribútov aktuálnej asociácie medzi stanicou a AP.

2.4.4 Bezpečnosť

Možnosť zašifrovania obsahu prenášaných dát je tiež súčasťou štandardu 802.11. Algoritmus zabezpečenia sa nazýva WEP (Wired Equivalent Privacy – bezpečnosť ekvivalentná káblom) protokol a je popísaný v ďalších častiach tejto práce.

2.4.5 Distribúcia

Distribúcia je služba, ktorá zabezpečuje doručenie správ. Keď stanica chce poslať správu inej stanici, pošle ju svojmu prístupovému bodu a ten použije distribučnú službu na zistenie, kde sa nachádza cieľová stanica. Pokiaľ sa stanica nachádza v pokrytí prístupového bodu, tak pošle správu cieľovej stanici, alebo v opačnom prípade pošle správu inému prístupovému bodu v ESS, v ktorého pokrytí sa cieľová stanica nachádza.

2.4.6 Integrácia

Integrácia slúži na prenos správ mimo hranice bezdrôtovej siete. Integrácia je spojená v prípade potreby s prekladom adries. Ak služba zistí, že cieľ správy je mimo bezdrôtovej siete, tento rámec je odoslaný bráne, ktorá ďalej určí routovanie správy do cieľa.

2.5 Vzťahy medzi službami

Stanica si udržiava informáciu o autentifikačnom a asociačnom stave v dvoch premenných, ktoré môžu byť autentifikovaný, neautentifikovaný a asociovaný, neasociovaný. Tieto dve premenné určujú, v akom stave sa stanica práve nachádza. Štandard 802.11 popisuje 3 základné stavy:

- Stav 1: iniciačný stav, neautentifikovaný, neasociovaný
- Stav 2: autentifikovaný, neasociovaný
- Stav 3: autentifikovaný, asociovaný

Aktuálny stav stanice určuje, ktoré typy rámcov môže obdržať alebo vysielať. Stavový diagram stanice je zobrazený na Obr.7.

Rámce triedy 1

- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgement (ACK)
- Contention-Free (CF)-End + ACK
- Contention-Free (CF)-End
- Probe request/response
- Beacon
- Authentication
- Deauthentication
- Annoucement traffic indication message (ATIM)
- Data rámce (iba tie, ktoré majú To DS a From DS s hodnotou 0)

Rámce triedy 2

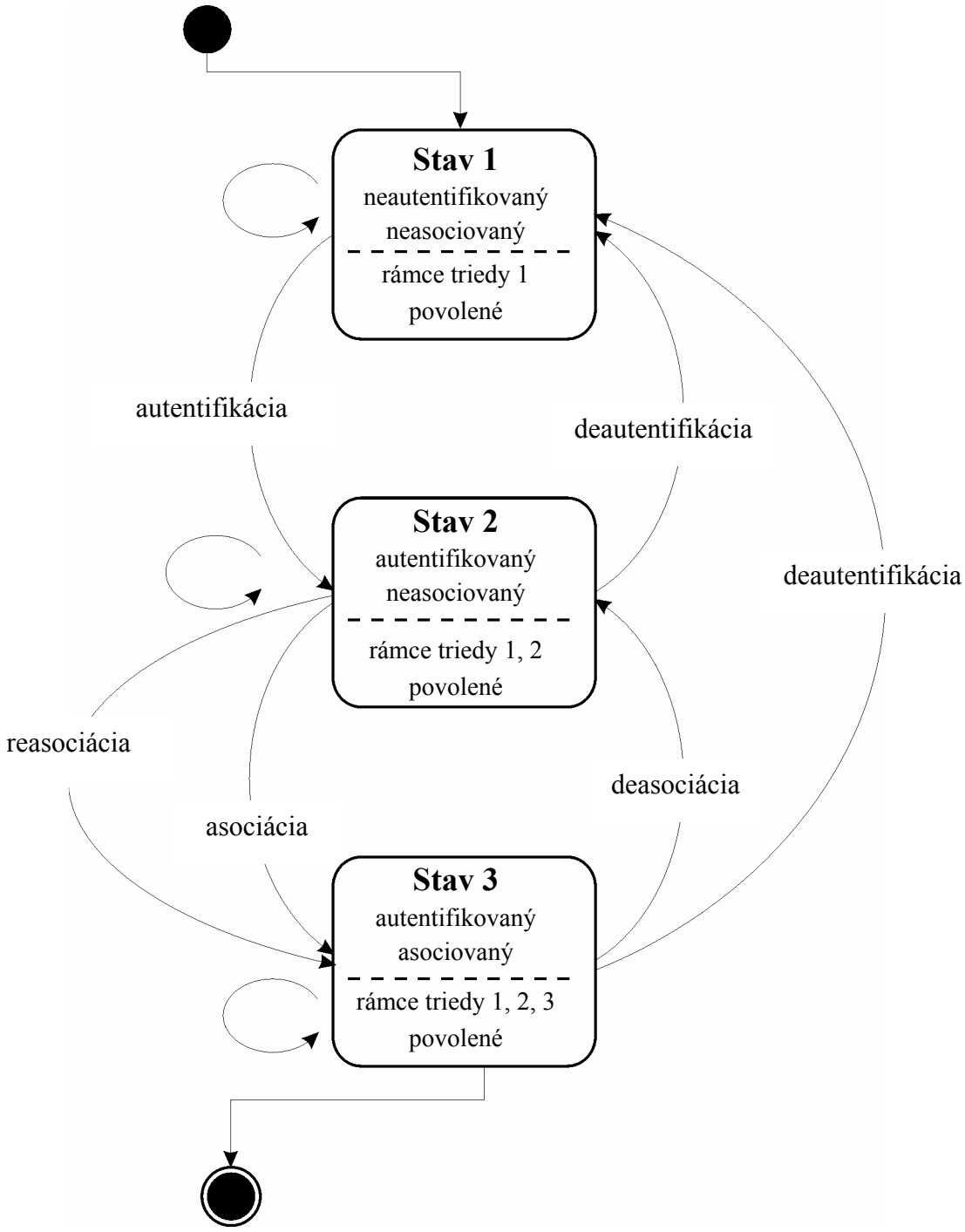
- Association request/response
- Reassociation request/response
- Deassociation

Rámce triedy 3

- Data rámce
- Power Save-Poll

Ak stanica A obdrží rámec triedy 3 od stanice B, ktorá je autentifikovaná, ale nie je asociovaná so stanicou A, stanica A pošle deasociačný rámec stanici B.

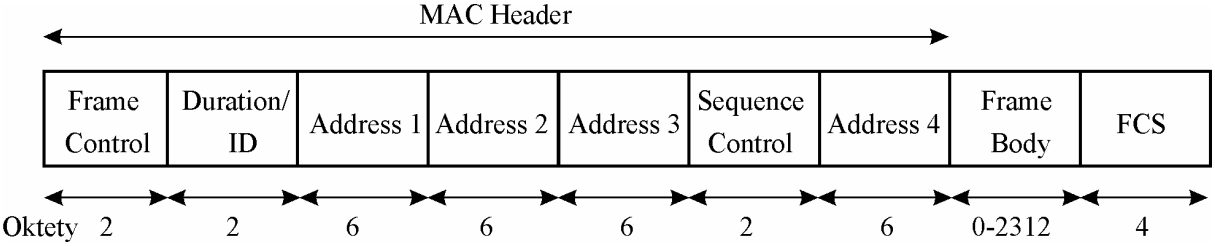
Ak stanica A obdrží rámec triedy 3 od stanice B, ktorá nie je autentifikovaná so stanicou A, stanica A pošle deautentifikačný rámec stanici B.



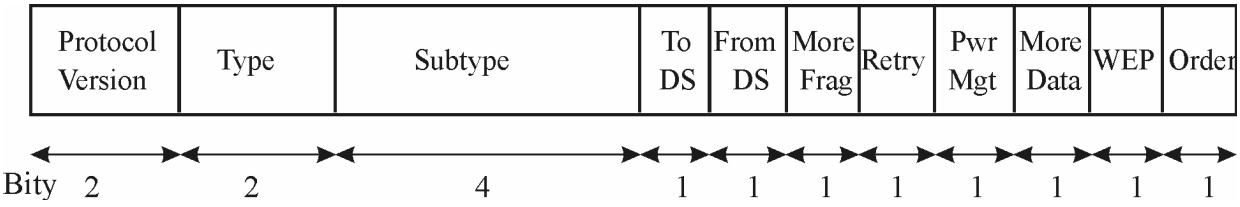
Obr. 7 – Stavový diagram stanice

2.6 Popis hlavičky štandardu 802.11

Každý paket prenášaný bezdrôtovo pomocou štandardu 802.11 má určitý tvar hlavičky v závislosti od jeho účelu. Všeobecný model hlavičky je na Obr. 8. Povinné časti hlavičky sú Frame Control (Obr. 9), Duration, Sequence Control, Frame Body a FCS (Frame Check Sequence).



Obr. 8 – Všeobecný model hlavičky 802.11



Obr. 9 – Frame Control rámec hlavičky 802.11

2.6.1 Frame Control

Protocol version

Protocol version je v prípade štandardu 802.11 vždy 0.

Type a Subtype

Nasledujúca tabuľka je prehľad všetkých možných kombinácií Type a Subtype.

Type	Type popis	Subtype	Popis kombinácie Type a Subtype
00	Management	0000	Association request - požiadavka na asociáciu
00	Management	0001	Association response - odpoveď na požiadavku o asociáciu

00	Management	0010	Reassociation request - požiadavka o reasociáciu
00	Management	0011	Reassociation response - odpoveď na požiadavku o reasociáciu
00	Management	0100	Probe request – požiadavka o poskytnutie informácií
00	Management	0101	Probe response – odpoveď na požiadavku o poskytnutie informácií
00	Management	0110-0111	Rezervované
00	Management	1000	Beacon – oznam o dostupnosti AP s jeho parametrami
00	Management	1001	ATIM (Announcement Traffic Indicator Message) – to isté čo Beacon v IBSS
00	Management	1010	Deassociation - oznam o deasociácii
00	Management	1011	Authentication request/response – autentifikačné rámce
00	Management	1100	Deauthentication - oznam o deautentifikácii (o ukončení bezpečnej komunikácie)
00	Management	1101-1111	Rezervované
01	Control	0000-1001	Rezervované
01	Control	1010	Power Save (PS) poll – stanica v PS móde vyžaduje od AP odoslanie dát, ktoré pre ňu AP uschovalo.
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Ack (Acknowledgement) – potvrdenie o prijatí korektných dát
01	Control	1110	CF-End – odovzdanie tokenu nazad k AP
01	Control	1111	CF-End + CF-ACK

10	Data	0000	Dáta
10	Data	0001	Dáta + CF-ACK
10	Data	0010	Dáta + CF-Poll
10	Data	0011	Dáta + CF-ACK + CF-Poll
10	Data	0100	Žiadna funkcionalita (žiadne dáta)
10	Data	0101	CF-ACK (žiadne dáta) – potvrdenie prijatia tokenu
10	Data	0110	CF-Poll (žiadne dáta) – odovzdanie tokenu stanici, ktorá má vysielať
10	Data	0111	CF-ACK + CF-Poll (žiadne dáta)
10	Data	1000-1111	Rezervované
11	Reserved	0000-1111	Rezervované

Tab. 1 – Kombinácie Type a Subtype

To DS a From DS

Nasledujúca tabuľka je prehľad všetkých možných kombinácií To DS a From DS.

To DS	From DS	Popis
0	0	Dáta v rámci BSS medzi dvomi stanicami
1	0	Dáta určené pre DS
0	1	Dáta opúšťajúce DS
1	1	Dáta z AP na AP

Tab. 2 – Kombinácie To DS a From DS

More Frag

Používa sa v prípade, ak správa pozostáva z viacerých fragmentov.

Retry

Položka Retry má hodnotu 1 v prípade retransmisie skoršieho rámca.

Pwr Mgt (Power Management)

Položka Power Management (riadenie spotreby energie) oznamuje po úspešnej výmene rámcov nasledujúci mód stanice. Ak má hodnotu 1, stanica bude po ďalšiu výmenu rámcov v Power Save móde.

More Data

Položka More Data je použitá pre klienta, ktorý je v power-save móde a oznamuje mu, že môže očakávať ďalšie dáta na prijatie.

WEP

Používa sa v prípade, že sa jedná o šifrované dáta pomocou WEP.

Order

S Používa sa v prípade, že je striktne nutné dodržať poradie správ.

Duration

Duration (trvanie prenosu) sa používa pre zabránenie kolízií vo vysielaní. Duration je časový údaj, ktorý oznámi klientom, že nemajú vysielať po určitú dobu prenosu. Maximálna hodnota je 1/30 sekundy.

V prípade staníc v Power Save móde je Duration nahradené ID (Identification – označenie) stanice nachádzajúcej sa v spomínanom móde.

2.6.2 Adresy

MAC vrstva v štandarde 802.11 používa rovnakú adresnú schému ako Ethernet (štandard IEEE 802.3), kde každá stanica má svoju vlastnú 48-bitovú MAC adresu. Popis jednotlivých kombinácií adries v MAC hlavičke 802.11 je v nasledujúcej tabuľke:

Popis	Adresa 1	Adresa 2	Adresa 3	Adresa 4
Dáta v rámci IBSS medzi dvomi stanicami	DA	SA	BSS ID	-
Dáta z DS	DA	BSS ID	SA	-
Dáta pre DS	BSS ID	SA	DA	-
Dáta z AP na AP	RA	TA	DA	SA

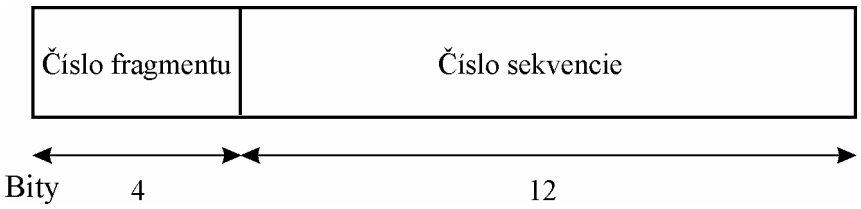
Tab. 3 – Kombinácie adries

DA (Destination Address) – cieľová adresa MSDU
SA (Source Address) – adresa odosielateľa MSDU
BSS ID – adresa AP, ku ktorému je asociovaný klient, alebo v prípade IBSS adresa IBSS

RA (Receiver Address) – adresa nasledujúcej stanice v DS
TA (Transmitter Address) – adresa vysielajúcej stanice v DS (nie vždy zdrojovej)

2.6.3 Sequence Control

Sequence control (Obr. 10) slúži na kontrolu postupnosti paketov. Pozostáva z dvoch častí – čísla fragmentu a čísla sekvencie. Každý MSDU má pridelené iné sekvenčné číslo od 0 do 4096. Číslo sekvencie sa každým novým MSDU zvyšuje o 1. Pri retransmisii fragmentu ostáva číslo fragmentu MSDU konštantné, ale číslo sekvencie už nie.



Obr. 10 – Sequence Control rámec hlavičky 802.11

2.6.4 FCS (Frame Check Sequence)

FCS je CRC-32 (Cyclic Redundancy Check 32-bit – 32-bitový kontrolný súčet) zo štandardu RFC 3309 kalkulované cez všetky polia MAC hlavičky a Frame Body.

2.6.5 Control rámce

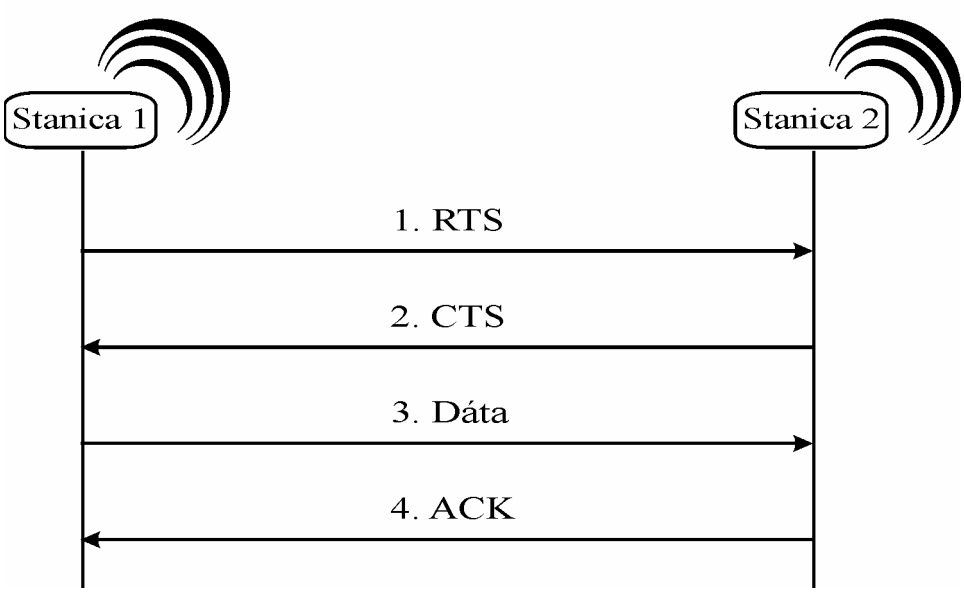
ACK

ACK je potvrdenie prijatia dát, ktoré odosiela stanica len v prípade obdržania korektných dát.

RTS a CTS

CSMA/CA je doplnená o výmenu Request to Send (RTS) a Clear to Send (CTS) paketov (viď. Obr. 11), ktoré oznamujú blížiacu sa výmenu dát a stanovujú čas ticha na médiu. Táto výmena rieši problém kolízie nepočujúcich sa staníc. RTS odosiela odosielateľ dát a CTS odosiela prijímateľ dát po obdržaní RTS. Všetci ostatní, ktorí zachytia RTS a CTS, prestanú odosielať dáta až do uplynutia stanovenej doby. V prípade, že niekto obdrží iba RTS, môže vysielať ostatným okrem odosielateľa RTS.

RTS a CTS sú obvykle vypnuté funkcie až kým veľkosť paketu nepresiahne 2346 oktetov. V takom prípade je automaticky vyžadované použitie RTS a CTS rámcov.



Obr. 11 – Komunikácia RTS/CTS metódou medzi stanicami

CF-Poll, CF-End a CF-ACK

Štandard 802.11 obsahuje okrem RTS a CTS aj druhú (nepovinnú) koordinačnú funkciu na poskytnutie iného spôsobu prístupu k zdieľanému bezdrôtovému médiu (inú od CSMA/CA). Prístup sa podobá schéme odovzdávania tokenu, pričom AP je koordinátor a pomocou CF (Contention Free) rámcov CF-Poll, CF-End a CF-ACK odovzdáva a odoberá staniciam token.

Power Save (PS)

Štandard 802.11 zahŕňa aj prechod staníc do PS módu v prípade dlhšieho časového obdobia bez prenosu dát. AP uchováva informáciu o staniciach, ktoré sú v PS móde a pre tieto stanice uschováva pakety pokiaľ si ich stanica nevypýta pomocou PS-Poll rámca alebo pokým stanica nezruší PS mód. AP v Beacon rámcoch pravidelne informuje stanice v PS móde o existencii rámcov uschovaných pre konkrétnu stanicu.

2.6.6 Management rámce

Management rámce umožňujú staniciam vytvoriť a spravovať komunikáciu. Nasleduje niekoľko vybraných druhov rámcov s podrobnejším popisom.

Beacon

Beacon je vysielané automaticky v pravidelných intervaloch od AP (alebo jeho ekvivalentu v IBSS) k staniciam. Automatické vysielanie beacon rámcov sa môže deaktivovať. Obsahuje informácie pre stanice, akými sú SSID (Service Set Identifier) – unikátny názov AP v alfa-numerickom tvare na separáciu bezdrôtových sietí, BSS ID, adresu AP, podporované prenosové rýchlosti, vysielací kanál, spôsob modulácie frekvencie, interval vysielania beacon rámcov a ďalšie parametre.

Probe request/response

Požiadavka od stanice na poskytnutie konkrétnej množiny informácií o AP alebo IBSS. Odpoveď na túto požiadavku dokáže obsahovať tie isté informácie ako beacon. Informácie môže žiadať stanica priamo od AP alebo aj od inej asociovanej stanice k AP.

Association request/response

Požiadavka o asociáciu obsahuje aj SSID AP, ku ktorému sa chce asociovať.

Deassociation a deautentification

Obidva druhy rámcov sú len oznamom pre stanice. Môžu byť smerované konkrétnej stanici, alebo aj vo forme broadcastu. Obidve obsahujú adresu stanice (alebo staníc), adresu AP a kódy na určenie dôvodu zrušenia asociácie, resp. autentifikácie.

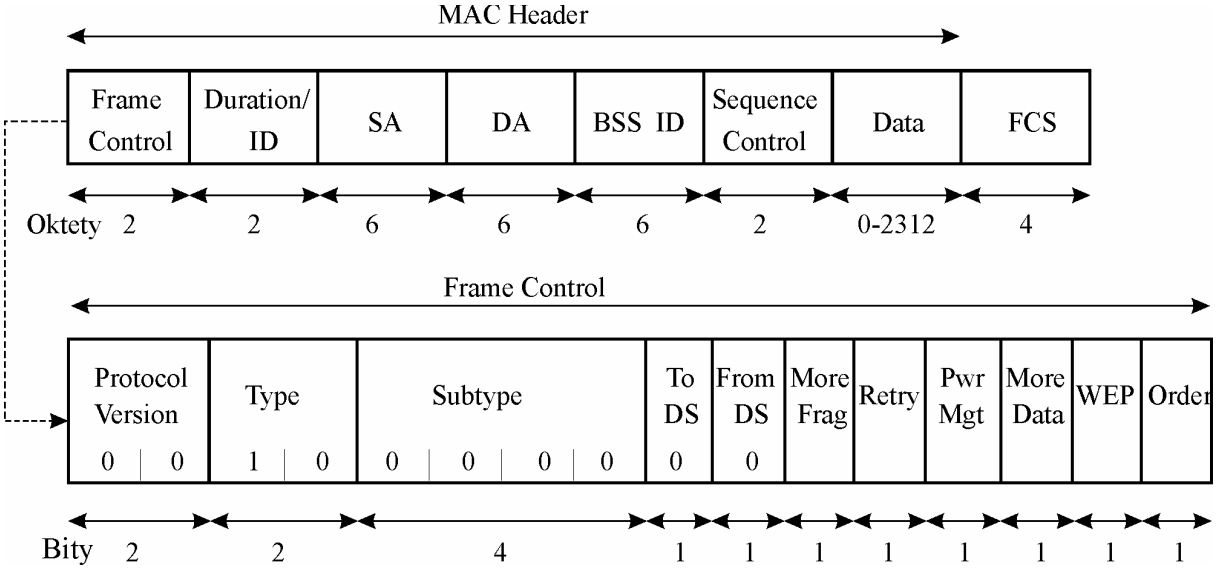
Reassociation request/response

Požiadavka aj odpoveď na reasociáciu obsahujú vždy adresu stanice, pôvodného AP ku ktorému bola stanica asociovaná, adresu nového AP a ESS ID. Odpoveď navyše obsahuje úspešnosť reasociácie.

V prípade roamingu môže nový AP ešte vyžiadať a doručiť stanici čakajúce rámce od pôvodného AP, nakoľko pozná adresu pôvodného AP.

2.6.7 Data rámce

Hlavným účelom bezdrôtovej siete je prenášať dáta. 802.11 definuje aj rámce pre dáta, v ktorých sa prenášajú pakety z vyšších vrstiev ISO/OSI modelu. Všeobecný model dátových rámcov je nasledujúci:



Obr. 12 – Všeobecný model Data rámcov hlavičky 802.11

3 WEP

3.1 Úvod

Hlavným rozdielom medzi prenosom po kábli a bezdrôtovým prenosom (okrem neprítomnosti kabeláže) sú signály prenášané vzduchom. Všetky predpoklady prijaté v káblovom svete (pružnosť voči náhodnému odpočúvaniu, signál „pripútaný“ ku kabeláži, možnosť zakončiť pripojenie konektorom) sú v bezdrôtovom svete nesprávne. V káblovom svete je pripojenie zaznamenateľné, avšak v bezdrôtovom svete nie, hocikto môže načúvať a odchytávať dáta bez stopovania – iným slovom nedetekovateľné pasívne odpočúvanie. Takýto typ monitoringu je očakávaný a je dôvodom zavedenia zabezpečenia do štandardu IEEE 802.11.

Zabezpečenie štandardu, nazývané WEP (Wired Equivalent Privacy – bezpečnosť ekvivalentná kabeláži) protokol, definuje množinu inštrukcií a pravidiel na zabezpečenie dát prenášaných vzduchom. V prvej verzii štandardu mal WEP slúžiť ako doplnok mobility ku káblovým sieťam.

S pomocou WEP sú dáta zašifrované tak, že pri odpočúvaní nedávajú zmysel. Toto docieli dôvernosť dát ekvivalentnú kabeláži. Naviac, používateľ je autentifikovaný predtým, než sa môže pripojiť do siete a obdrží kľúče na dešifrovanie informácie. V tomto smere WEP dáva ekvivalenciu konektoru v stene.

K zabezpečeniu dát používa WEP algoritmus RC4 na zašifrovanie paketov v poradí v akom sú vysielané do vzdušného priestoru. RC4 algoritmus je pomerne populárnou metódou zabezpečenia, ktorý používa prúdovú šifru na generovanie unikátneho kľúča pre každý paket. Tento algoritmus je rovnaký, aký sa používa v mnohých zabezpečených internetových aplikáciách, ako aj SSL (Secure Sockets Layer), Oracle Secure SQL (Structured Query Language) alebo Lotus. SSL je najčastejšie používaným protokolom v online obchodoch, slúžiacim na zabezpečenie informácií o zákazníkovi prenášaných cez internet. Takéto zabezpečenie znižuje riziko odhalenia informácií o platobnej karte zákazníka a procesu transakcie.

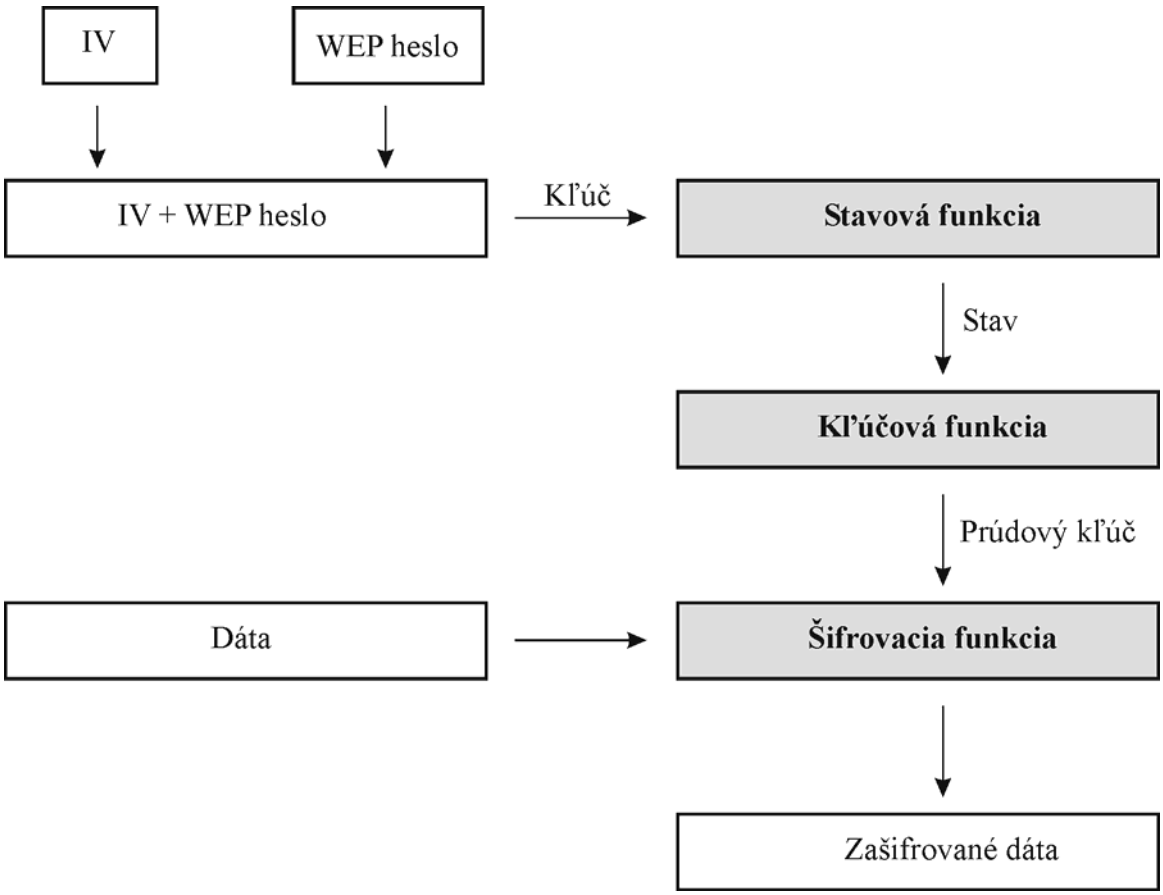
WEP ma 3 ciele:

- prevencia pred odhalením obsahu dát
- prevencia modifikácie dát pri prenose
- poskytnúť kontrolu prístupu do siete

Aj keď WEP nezastaví odchytenie dát, môže zastaviť príležitostné rozoberanie zachytených dát.

3.2 RC4 algoritmus

Algoritmus RC4 (viď. Obr. 13) slúži na zašifrovanie dát tak, že by pri korektnej implementácii algoritmu trvalo roky ich dešifrovať bez použitia správneho kľúča s použitím dnešnej výpočtovej sily.



Obr. 13 – RC4 algoritmus

RC4 bolo vyvinuté v roku 1987 Ronom Rivestom z RSA Data Security Inc. a nebol nikdy oficiálne publikovaný. Bol obchodným tajomstvom až do roku 1994, kedy šifrovací program používajúci RC4 bol anonymne publikovaný. Publikovaný algoritmus bol nazvaný ako Arcfour (taktiež nazývaný ARC4 alebo Assumed RC4). RSA nikdy nepotvrdilo, že tento algoritmus je zhodný s RC4 algoritmom, ale bolo dokázané, že funkčne sú obidva algoritmy rovnaké.

RSA má stále obchodnú značku na názov RC4, avšak nie na samotný algoritmus. Niektorí sa snažia obísť licenciu RSA algoritmom Arcfour, avšak legalita tohto kroku je otázna. Táto práca popisuje algoritmus Arcfour, ale nazýva ho RC4 algoritmom pre jeho funkčnú ekvivalenciu.

Aj keď algoritmus je obchodným tajomstvom RSA, našiel si cestu do množstva technológií.

Keďže RC4 je symetrická synchrónna prúdová šifra, pozostáva zo stavovej premennej, hesla a 3 základných funkcií – stavovej, kľúčovej a šifrovacej. Naviac obsahuje iniciačný vektor (Initialization Vector - IV), ktorý sa pripája k heslu a neustále mení pomocou algoritmu generátora IV.

3.2.1 Iniciačný vektor – IV

Bolo by príliš nebezpečné ponechať len heslo ako jediný ovplyvniteľný prvok algoritmu. Čo robí z RC4 dobrú prúdovú šifru je práve použitie náhodne generovanej hodnoty počas šifrovacieho procesu. Touto náhodnou hodnotou je spojenie IV, ktoré sa neustále mení s WEP heslom, ktoré býva často statické, aby vytvorilo dlhšie a neustále sa meniace heslo.

Prúdový kľúč je počítaný s použitím stavovej premennej, IV a vlastností WEP hesla, ako je napr. jeho dĺžka a hodnota znakov. V závislosti od implementácie RC4 algoritmu môže byť IV rôzne veľké. V prípade WEP je IV o veľkosti 24 bitov (3 bajty).

IV je obvykle pri implementáciách generované od 0 a zvyšované o 1 pre každý fragment dát. Tým, že sa spája s WEP heslom a vchádza do stavovej funkcie zabezpečí, že sa vytvorí unikátna stavová tabuľka pre každý paket. Následne ovplyvňuje aj ďalší šifrovací proces, takže každý odoslaný paket je zašifrovaný s iným prúdovým kľúčom. Preto náhodnosť IV ako takého nie je nutnosť. V štandarde 802.11 nie je uvedený spôsob obmieňania IV. Niektoré implementácie dokonca nechávajú IV statickými, čím degradujú silu RC4 algoritmu.

Napriek tomu, že IV vytvára bezpečnejšie prostredie na prenos dát, vyžaduje to zdieľanie dvoch informácií. Prijímateľ zašifrovaných dát potrebuje na začatie dešifrovacieho procesu IV aj WEP heslo. Ako som ukázala v kapitole 1, stavová premenná je dôležitým prvkom pri prúdových šifrách a na správne dešifrovanie musí prijímateľ dát dosiahnuť ten istý stav ako odosielateľ. Bez IV by RC4 algoritmus prijímateľa nevytvoril správnu stavovú premennú. Keďže IV sa mení pre každý paket, musí byť prenesené vzduchom spôsobom, aby druhá komunikujúca strana vedela zistiť jeho hodnotu. Preto je IV pripojené k šifrovanému paketu a odoslané príjemcovi. IV je pripájané do hlavičky paketu v nešifrovanom formáte.

3.2.2 Kľúč

Kľúč je spojenie IV s WEP heslom. RC4 v prípade WEP používa buď 40-bitové alebo 104-bitové zdieľané WEP heslo (104-bitové heslo je obsiahnuté až v štandarde 802.11b) s 24-bitovým IV. WEP heslo je premenené na jeho binárny ekvivalent, pričom každé písmenko WEP hesla pozostáva z 8 bitov. Celkovo teda má 5 alebo 13 znakov. V technických špecifikáciách produktov sa píše obvykle 64 alebo 128-bitový WEP. To je udávaná veľkosť kľúča spojením WEP hesla s IV. Takéto technické detaily môžu uviesť používateľa k omylu, že celých 64 alebo 128 bitov je chránených informácií, avšak IV bity nie sú v skutočnosti bezpečné z dôvodu toho, že sú prenášané vzduchom v nešifrovanej forme.

Implementácie sa môžu líšiť aj v tom zmysle, že niektoré zariadenia vyžadujú namiesto ASCII (kódová tabuľka) znakov WEP hesla hexadecimálne hodnoty na plných 40 alebo 104 bitov. Takisto štandard podporuje pre zvýšenie bezpečnosti možnosť zvoliť až zo 4 rôznych WEP hesiel, ktoré sa cyklicky obmieňajú a tým pádom ešte viacej zmenšujú útočníkovi šance na odhalenie hesla. Niektoré zariadenia na vytvorenie viacerých WEP hesiel používajú

hashovaciu funkciu. Hashovacia funkcia vezme dáta ľubovoľnej dĺžky a vyrobí z nich zašifrované dáta pevnej dĺžky, tzv. hash pôvodných dát. Hashovacia funkcia musí byť konzistentná (pre rovnaké pôvodné dáta musí vždy vyrobiť rovnaké zašifrované dáta) a hlavne jednosmerná. Zašifrovaný text sa už nedá dešifrovať, dá sa iba porovnávať s inými zašifrovanými dátami. V takýchto prípadoch je vhodné použiť minimálne rovnaké implementácie ak nie rovnaké typy zariadení na bezdrôtovú komunikáciu.

Spôsob obmieňania viacerých hesiel nie je v štandarde 802.11 spomenutý. Takisto v špecifikácii WEP chýba manažment kľúčov, takže sa stáva, že heslo ostáva dlhodobo nezmenené a tým pádom má útočník viacej času na jeho zlomenie a používanie.

Veľkosť WEP kľúča bola obmedzená na 40 bitov z dôvodu povojnovej regulácie vládou USA (United States of America) a NATO (North Atlantic Treaty Organization – Organizácia Severoatlantickej zmluvy). Chceli zabrániť šíreniu silných šifier potenciálnym nepriateľom. Neskôr, keď zvýšili limity, takmer okamžite vyšiel štandard 802.11b, ktorý už obsahoval 104-bitový kľúč.

3.2.3 Stavová premenná

Stavová premenná je pole o veľkosti 256 8-bitových hodnôt. Pri inicializácii algoritmu sa do poľa uložia čísla od 1 do 256. Počas stavovej aj kľúčovej funkcie sa v poli prehadzujú navzájom hodnoty poľa v závislosti od kľúča (WEP heslo s IV). Hodnoty však stále ostávajú nezmenené, t.j. keď utriedime pole, dostaneme znovu čísla od 1 do 256.

Pri vhodnom použití je stavová premenná relatívne nepredvídateľná.

3.2.4 Stavová funkcia

Prvú časť šifrovacieho procesu, tzv. stavovú funkciu robí algoritmus generovania kľúčov (KSA – key scheduling algorithm). Všeobecne KSA vytvára rôzne veľké pole hodnôt rôznych veľkostí. V prípade WEP je použitý 8-bitový RC4 algoritmus, teda KSA operuje na 8-bitových hodnotách s použitím poľa o veľkosti 256 8-bitových hodnôt.

Ďalším krokom KSA je poprehadzovanie poľa. To sa udeje s použitím kombinácie znakov kľúča, dĺžky kľúča a hodnôt v poli počas cyklu prehadzovania. Po niekoľkých stovkách súčtov a presunov je stavové pole dôkladne zamiešané a môže sa pokračovať v ďalšej časti šifrovacieho procesu.

Kód KSA

K – pole, v ktorom je uložený kľúč (konštantné)
d – dĺžka kľúča (dĺžka poľa K - pri 40-bit. WEP je dĺžka konštantne rovná 5)
S – stavové pole (256 8-bitových hodnôt, premenné)
m – veľkosť stavového poľa (konštantne 256 hodnôt)
swap(g,h) – funkcia pre zámenu prvkov *g* a *h*

naplnenie stavového poľa hodnotami od 0 do 255

```
for i from 0 to m-1
    S[i] := i
endfor
```

poprehadzovanie stavového poľa s použitím vlastností kľúča

```
j := 0
for i from 0 to m-1
    j := (j + S[i] + K[i mod d]) mod m
    swap(S[i],S[j])
endfor
return S
```

3.2.5 Kľúčová funkcia

Kľúčovou funkciou RC4 algoritmu je pseudo-náhodný generátor – PRGA (Pseudo Rangom Generator Algorithm). Táto časť algoritmu RC4 je zodpovedná za vytvorenie prúdového kľúča na zašifrovanie vstupných dát. Prúd je vytvorený pomocou cyklu cez algoritmus nižšie pre každý bajt fragmentu dát určený na zašifrovanie. Prúdový kľúč musí byť rovnako veľký ako veľkosť fragmentu dát.

KÓD PRGA

L – dĺžka požadovaného prúdového kľúča
P – pole o veľkosti L, v ktorom bude uložený prúdový kľúč
S – stavové pole (256 8-bitových hodnôt)
m – veľkosť stavového poľa (konštantne 256)
swap(g,h) – funkcia pre zámenu prvkov *g* a *h*

```
i := 0
j := 0
for k from 0 to L-1
    i := (i + 1) mod m
    j := (j + S[i]) mod m
    swap(S[i],S[j])
    P[k] := S[(S[i] + S[j]) mod m]
endfor
return P
```

Každá hodnota poľa S je zamenená aspoň raz každých 256 iterácií.

3.2.6 Šifrovacia funkcia

Šifrovacou funkciou RC4 je matematická operácia XOR (eXclusive OR - binárna adícia modulo 2).

XOR je veľmi populárna metóda šifrovania z dvoch dôvodov:

1. je rýchla
2. pracuje na úrovni bitov.

Avšak aj napriek svojej rýchlosti a úrovni, na ktorej pracuje prináša XOR jeden závažný problém. Pri kódovaní prázdneho reťazca núl je výsledkom samotný prúdový kľúč. Táto nepríjemnosť je vyriešená stavovou premennou. Stavová premenná by sa mala náhodne meniť a tým pádom aj neustále meniť prúdový kľúč. V takom prípade prenesenie prúdového kľúča by sa vyskytovalo náhodne a bolo by takmer nemožné ho odhaliť.

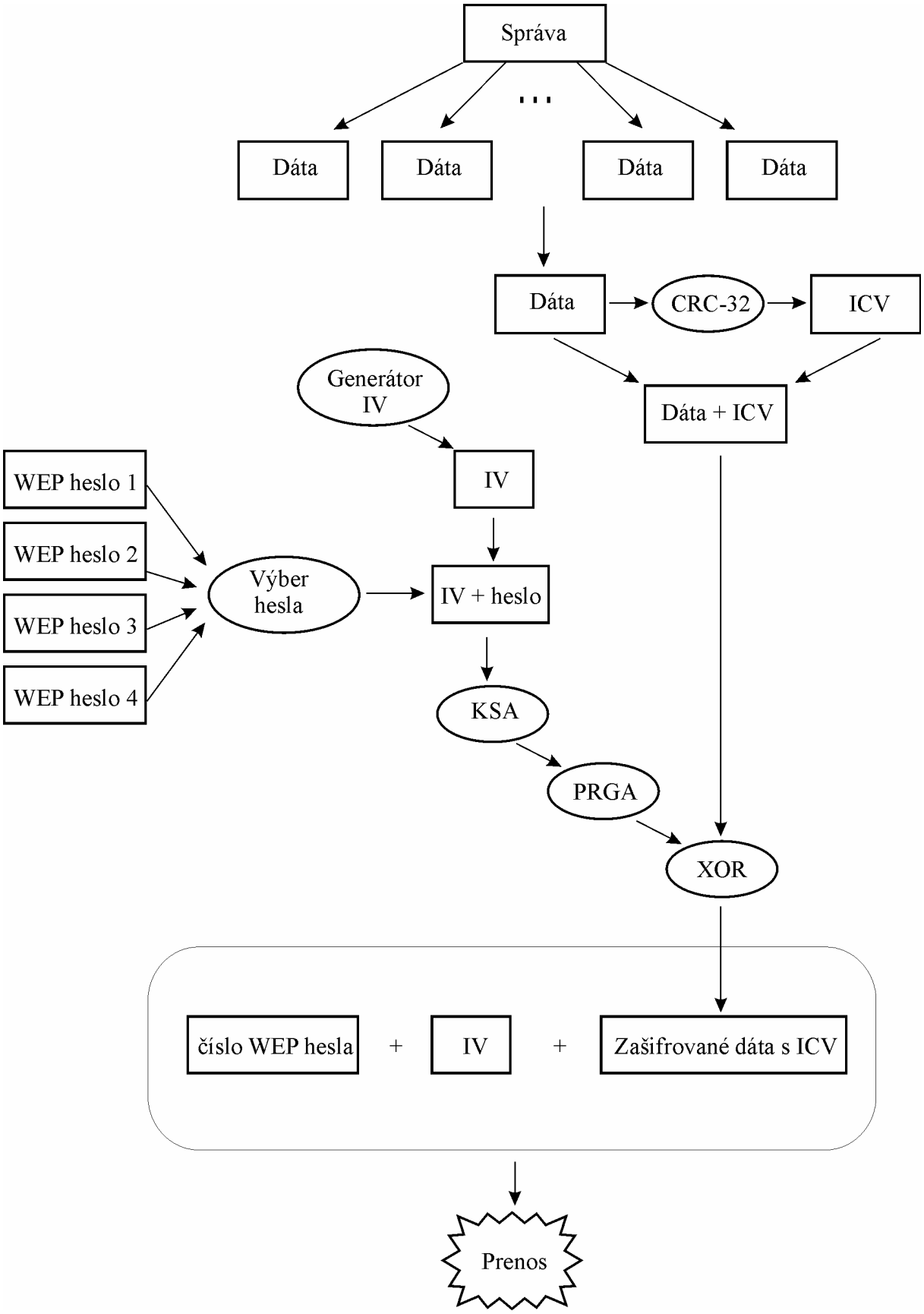
3.3 WEP proces

3.3.1 Proces šifrovania (viď. Obr. 14)

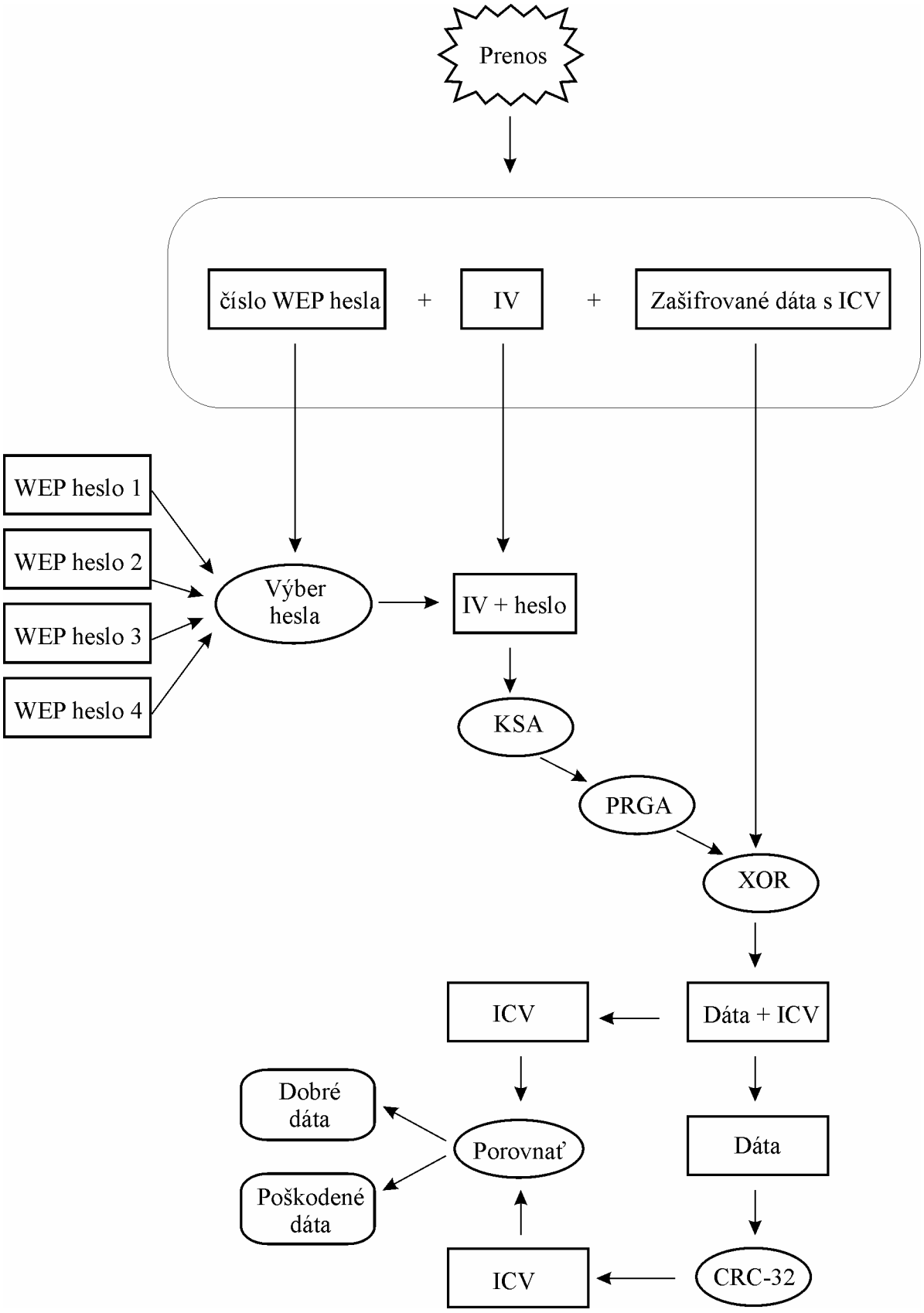
Správa sa rozdelí na viacero menších častí - fragmentov. Ku každému fragmentu sa pripojí ICV (Integrity Check Value), čo je 4-oktetový lineárny kontrolný súčet kalkulovaný cez fragment. Používa CRC-32. ICV by sa nemalo pliesť s frame check sequence (FCS), ktoré je ďalšie CRC-32 na zisťovanie chýb v transmisií paketu. FCS je pripojené na koniec hlavičky pred prenosom. Kľúčovým rozdielom je, že ICV je šifrované spolu s dátami. Algoritmus na generovanie IV vyrobí pri každom fragmente nové IV a pripojí ho k jednému z (možno viacerých) WEP hesiel. IV s WEP heslom tvoria heslo, ktoré vstupuje do stavovej funkcie (KSA) RC4 algoritmu a následne aj do kľúčovej funkcie (PRGA), odkiaľ vypadne prúdový kľúč. Prúdový kľúč ďalej vstupuje s fragmentom a jeho ICV do šifrovacej funkcie (XOR). Z tejto funkcie už dostaneme zašifrovanú informáciu, ku ktorej pripojíme hlavičky a odošleme vo forme paketu bezdrôtovým kanálom k príjemcovi. Do hlavičky ale pripojíme ešte IV a poradie použitého WEP hesla v nešifrovanom formáte, aby príjemca mohol úspešne dešifrovať paket bez synchronizácie generátora IV.

3.3.2 Proces dešifrovania (viď. Obr. 15)

Príjemca po prijatí zašifrovaného paketu použije IV a poradie WEP hesla z hlavičky na správne vytvorenie hesla, ktoré tiež prejde cez rovnakú stavovú aj kľúčovú funkciu a následne aj cez rovnakú šifrovaciu funkciu ako u odosielateľa. Keďže XOR je symetrický operátor, prúdový kľúč so zašifrovaným obsahom paketu dá za výsledok pôvodný obsah paketu s ICV. Následne sa z paketu odpojí z neho ICV a skontroluje integrita dát porovnaním prijatého ICV s CRC-32 kontrolným súčtom cez pôvodný obsah paketu.



Obr. 14 – Šifrovací WEP proces

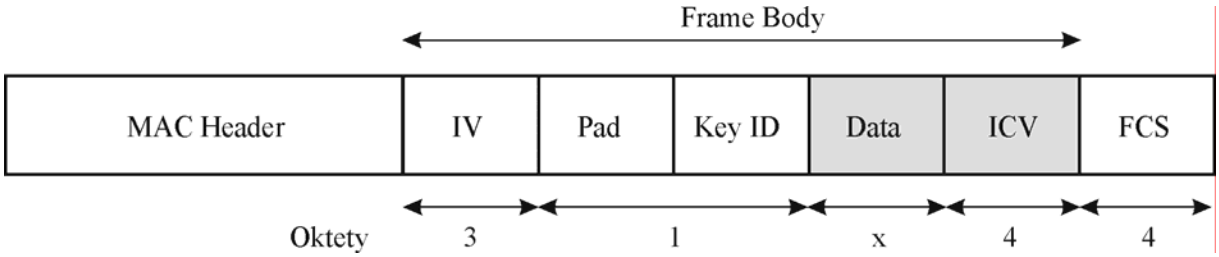


Obr. 15 – Dešifrovací WEP proces

3.4 WEP paket

Vytvorenie WEP paketu je transformácia dát zo sieťovej vrstvy do nižšej. V prípade algoritmov v tejto sekcii toto zahŕňa zašifrovanie, kontrolu integrity, možnú fragmentáciu a pripojenie hlavičiek k paketu. Prijímateľ paketu robí opačný proces transformácie.

Všeobecný model WEP paketu je na Obr. 16.



Obr. 16 – WEP paket

Pad je o veľkosti 6 bitov a stále má hodnotu 0.
Key ID je o veľkosti 2 bity a obsahuje poradie WEP kľúča, ktorý bol použitý na zašifrovanie obsahu dát s ICV.
Dáta a ICV sú jediné zašifrované informácie vo WEP pakete.

4 Nevýhody šifrovania

Je zrejmé, že šifrovanie ponúka mnoho výhod. Môže byť použité na autentifikáciu používateľov, autorizáciu prístupu k utajovaným informáciám, zabezpečenie dôvernosti dát a garanciu integrity dát. Avšak existuje niekoľko potenciálnych problémov spojených so šifrovaním dát. Tieto problémy zahŕňajú okrem iných aj stratu hesla, falošný pocit bezpečia a spomalenie zariadenia použitého pri šifrovaní. V tejto kapitole zbežne prejdeme základné problémy šifrovania týkajúce sa bezdrôtového prenosu.

4.1.1 Heslo

Jeden z problémov šifrovania je v prípade straty hesla. V takomto prípade jediný spôsob okrem nájdenia hesla je jeho zlomenie. Avšak v závislosti od použitej metódy šifrovania sa môže stať, že lámanie hesla bude v priemernom prípade trvať niekoľko rokov.

Zdieľané heslo medzi používateľmi je tiež nebezpečné. Ak sú heslá jednoduché, dajú sa uhádnuť pomocou slovníkového útoku. Ak sú heslá zložité, používatelia ich môžu uložiť na nechránené miesto. V prípade straty zdieľaného hesla medzi viacerými používateľmi je jednoduchšie ho obnoviť.

Nakoľko zmena zdieľaného hesla vyžaduje zmenu u každého klienta, je zrejmé, že k takýmto zmenám nebude dochádzať príliš často. Tým pádom má útočník viacej času na odhalenie hesla alebo dát a v prípade úspešného obdržania hesla má viac času na sledovanie dôverných informácií.

4.1.2 Použitie šifrovania negarantuje bezpečnosť

Tento problém je zrejme najdôležitejší v prípade bezdrôtového prenosu. Veľa ľudí považuje ich sieť alebo pripojenie do siete za bezpečný aj v prípade, že je zabezpečený pomocou WEP. Táto domienka je chybná v prípade, že heslo je ponechané prázdne alebo základné od výrobcu zariadenia. K doplneniu, WEP nechráni pred najčastejšími útokmi hackerov. A napokon WEP ako taký je v základe chybný. Použitie WEP je odporúčané aspoň ako doplnok bezpečnosti, avšak nemal by byť použitý ako jediný prvok zabezpečenia siete.

4.1.3 Šifrovacia réžia

Neposledným problémom, ktorý sa taktiež vyskytuje v bezdrôtovom prenose informácií je príliš vysoká réžia na šifrovanie informácií. Takáto záťaž na zariadenia môže mať vážny dopad na produktivitu sieťových aplikácií a môže mať škodlivý vplyv na časovo-náročné situácie.

Ľubovoľné šifrovanie pridáva réžiu na spracovanie požiadaviek sieťového systému. Šifrovanie spomaľuje proces vysielania a môže nepriaznivo ovplyvniť schopnosť procesoru sieťového zariadenia vysporiadať sa s inými kritickými situáciami.

5 Útoky na bezpečnosť 802.11

5.1 Úvod

Bezdrôtová sieť reprezentuje obvykle najzraniteľnejší vchod do vnútra siete ak ďalšie vnútorné zabezpečenie neexistuje. Z tohto dôvodu sú pomerne obľúbeným cieľom útočníkov.

Útoky na bezdrôtové siete sa dajú rozdeliť na:

- Pasívne útoky
  - Odpočúvanie prenosu
  - Analýza prenosu
- Aktívne útoky
  - Narušenie dostupnosti
  - Manipulácia s dátami (duplikácia, modifikácia, injektáž, zničenie dát)
  - Maskovanie
  - Narušenie dôvernosti dát

Bezdrôtové siete sú potenciálnym cieľom ako pasívnych, tak aj aktívnych útokov. Aktívny útok sa líši od pasívneho zásahom útočníka do prebiehajúceho prenosu dát. Pasívny útok je v prípade bezdrôtových sietí nezistiteľný spôsob útoku a je ťažké až nemožné zabrániť mu. Na odpočúvanie môže byť útočník aj niekoľko kilometrov ďaleko od vysielajúcej stanice ak použije silnú prijímaciu anténu, pretože nepotrebuje zasahovať do prebiehajúcej komunikácie. Na analýzu odchytených dát z odpočúvania nepotrebuje byť útočník v dosahu siete vôbec. Akékoľvek dobré zabezpečenie bezdrôtovej siete musí počítať práve s bežným výskytom pasívnych útokov a brániť sa voči nim.

5.2 Ciele útokov

Útočníci majú obvykle viacej dôvodov prečo sa zameriavajú na konkrétnu bezdrôtovú sieť. Môžu chcieť prístup k nedostupným prostriedkom siete (napr. k dôverným materiálom) alebo prístup k prostriedkom, za ktoré by museli za normálnych okolností zaplatiť. Ďalším možným úmyslom útočníka môže byť odoslanie niekoľkých miliónov e-mailov za účelom spamovania, alebo odoslania anonymných vírusov, červov a pod. V neposlednom rade môže byť úmyslom čisto vandalizmus, odplata alebo útok na konkurenciu.

Niekedy môžu byť útoky kombinované. Napríklad útočník môže vyvolať útok na dostupnosť siete voči legitímnej infraštruktúre, aby presmeroval klientov na svoj maskovaný AP a tým získal požadované informácie od klientov alebo im rozosielal falošné informácie pod hlavičkou legitímneho AP.

5.3 XOR

Je veľmi jednoduché získať prúdový kľúč ak poznáme pôvodné aj zašifrované dáta. Zašifrované dáta sa dajú odchytiť jednoducho pomocou dostupných nástrojov z internetu, ale poznať pôvodné dáta je už ťažšie. Ak útočník vie vopred, aké dáta budú odoslané a zachytí ich zašifrované, môže tieto dáta spojiť cez XOR funkciu a dostane prúdový kľúč, ktorý v prípade, že sa bude neskôr opakovať môže použiť na dešifrovanie ďalších paketov.

Niekoľko užitočných rovností:

Zašifrovaný text = Originálny text XOR Prúdový kľúč

Prúdový kľúč = Zašifrovaný text XOR Originálny text

Originálny text = Zašifrovaný text XOR Prúdový kľúč

5.4 Odpočúvanie a analýza prenosu

Útočník musí objaviť cieľovú sieť ešte pred útokom. Toto môže robiť buď stopovaním konkrétnej organizácie alebo používateľa, alebo to môže byť len útok na náhodne vybranú sieť v okolí.

V káblovej sieti môžu odhaliť pasívne útoky detekčné systémy na vniknutie cudzej osoby do siete alebo firewally, avšak v bezdrôtovej sieti sa nedajú tak ľahko, resp. vôbec odhaliť. Môžu existovať detekčné systémy na Probe request/response management rámce, avšak vyžadujú zásah do konkrétnej implementácie stanice alebo AP a už sa nedajú považovať za čisto pasívne útoky, nakoľko vyžadujú odoslanie rámca od útočníka. V prípade AP, ktoré vysiela v pravidelných intervaloch Beacon management rámce dokonca nie je vôbec nutné, aby útočník použil Probe request rámce nakoľko Beacon rámce obsahujú všetky potrebné informácie, a teda ani takto upravený detekčný systém ho pri odpočúvaní nikdy nezachytí.

Počas analýzy sa útočník snaží zistiť, akú šírku vysielacieho pásma, protokoly a zabezpečovacie mechanizmy používa zacielená sieť a kde je jej najzraniteľnejšia oblasť zabezpečenia, aby mohol vybrať, aký postup použije na zdolanie bezpečnosti. Analýzou odchytených paketov môže útočník niekedy objaviť zaujímavé informácie ako napr. používateľské informácie k dôverným informáciám.

Pre sieťového administrátora môže byť analýza paketov užitočná na zistenie správnej konfigurácie siete alebo z bezpečnostného hľadiska môže analyzované pakety použiť aj na zisťovanie útokov na sieť. Takéto zisťovanie je extrémne časovo náročné na ručné spracovanie a tak výsledkom je paleta rôznych nástrojov, z ktorých niekoľko má dokonca open-source kód.

Zvyčajne po pasívnom útoku nasleduje aj aktívny útok. Odchytávanie paketov je napr. veľmi dôležitou fázou pred narušením dôvernosti.

5.4.1 SSID (Service Set Identifier)

SSID je niekedy považovaný za zabezpečovací mechanizmus, avšak nebol vytvorený za týmto účelom. SSID slúži na separáciu bezdrôtových sietí a sú vysielané v Beacon management rámcoch z AP. Nástroje ako Network Stumbler, Kismet a Wellenreiter odpočúvajú a ukladajú záznamy SSID, ktoré zachytia.

Mnoho zariadení má možnosť vypnúť vysielanie Beacon rámcov (tzv. broadcastovanie SSID). Táto možnosť je užitočným zabezpečením voči náhodným okoloidúcim nezameraným na konkrétnu sieť. Avšak veľa nástrojov vystopujú SSID z Association request rámcov, ktoré musia obsahovať aj SSID (v nešifrovanom stave). Ak sa sieť zabezpečí len skrytím vysielania SSID, skúsenému útočníkovi sa nevyhne.

5.4.2 Wardriving

Wardriving je pozorovanie bezdrôtovej siete, typicky z auta. Z minulosti bolo bežným pojmom wardialing, ktorý označoval starú techniku na vyhľadanie počítačových modemov vytáčaním tisícov telefónnych čisiel. Dnes sa už pojem wardriving zaužíval aj v spojitosti s akýmkoľvek odpočúvaním prenosu na bezdrôtovej sieti.

Na wardriving existuje niekoľko jednoduchých nástrojov, ktoré používajú bezdrôtové karty útočníka a automaticky sledujú siete. Stránky ako napr. [25] majú online databázu nezabezpečených bezdrôtových sietí. Tieto programy a databázy sú často prepojené s GPS súradnicami, takže sa dá jednoducho lokalizovať sieť na mape.

5.4.3 Autentifikácia

Open System

Autentifikácia Open System nie je skutočnou autentifikáciou. Autentifikovať sa môže ľubovoľný klient po odoslaní svojej MAC adresy.

Shared Key

Autentifikácia Shared Key (viď Obr. 6) môže poskytnúť útočníkovi dostatok informácií na neskoršie narušenie dôvernosti dát bez nutnosti zásahu do komunikácie počas autentifikácie. Počas autentifikácie môže útočník odchytiť tieto tri dôležité informácie:

- Náhodný text (ďalej správa),
- Zašifrovanú správu,
- IV použité na zašifrovanie správy, pretože je odosielané v nešifrovanom formáte spolu so zašifrovanou správou v hlavičke WEP paketu (viď Obr. 16).

Ako ukážem neskôr, XOR pôvodnej správy a zašifrovanej správy odhalí útočníkovi prúdový kľúč, ktorý mu pomôže spolu s IV narušiť dôvernosť prenosu dát alebo pomôže narušiť autentifikáciu.

Narušenie Shared Key autentifikácie je možné v prípade, že útočník má k dispozícii prúdový kľúč so správnym IV (patriacim k danému prúdovému kľúču). Útočník odošle AP

Authentication request rámec, na základe ktorého mu AP odošle nazad Authentication response rámec s náhodným textom. Náhodný text následne útočník zašifruje pomocou známeho prúdového kľúča a pripojí do hlavičky WEP paketu známe IV. Nakoľko IV si môže autentifikovaná stanica určiť sama, na tento druh útoku postačuje len jediná známa kombinácia prúdového kľúča a IV. Prúdový kľúč, ako som už ukázala vyššie, je jednoduché obdržať napríklad sledovaním Authentication request a Authentication response management rámcov. V ďalších kapitolách ukážem, že prúdový kľúč sa dá získať aj inými spôsobmi.

5.5 Narušenie dostupnosti

Narušenie dostupnosti býva označované termínom DoS (Denial Of Service) a je vážnym problémom sieťovej bezpečnosti. Prerušenie funkčnosti služby môže byť od fyzického zničenia zariadenia až po útoky s úmyslom obsadiť čo najväčšiu šírku pásma. Môže to byť aj pokus o zrušenie prístupu určitého klienta k prostriedkom siete. DoS je problematický najmä v bezdrôtových sieťach kvôli jednoduchosti prístupu k sieti.

DoS útok je pomerne jednoduchý, ako ukážem v ďalších častiach tejto práce, ale s jeho pomocou sa dajú dosiahnuť len limitované ciele. Prístup k sieti by útočníkovi poskytol oveľa viacej možností.

5.5.1 Duration

Jedným z DoS útokov je zneužitie časti rámca Frame Control nazvaný Duration (trvanie prenosu). Útočník môže rozoslať tok paketov s maximálnym Duration (1/30-tina sekundy). Takáto prenosová rýchlosť 30 paketov za sekundu spôsobí obsadenosť siete. Pri prenose 30 paketov za sekundu je maximálna prenosová rýchlosť 352 Kbps ({30 paketov * 1500 B}/1024 B * 8 bitov = 352 Kbps). Momentálne veľa zariadení ignoruje Duration, takže útok nemusí byť vždy úspešný.

5.5.2 Zahltenie siete alebo AP

Zahltenie AP požiadavkami na autentifikáciu je tiež jeden zo spôsobov narušenia dostupnosti. Útočník vytvorí množstvo Authentication request management rámcov a nebude odpovedať na Authentication response rámce. AP musí evidovať všetky vygenerované náhodné texty v pamäti a ak sa pamäť zaplní, AP odmietne autentifikovať ďalších klientov. Ak AP prestane odpovedať na Authentication request rámce, útočník zistí, že dosiahol DoS.

Rovnakým spôsobom sa dá dosiahnuť DoS zaplnením tabuľky asociovaných klientov, pretože AP udržiava informáciu o každej asociovanej stanici. Avšak v tomto prípade je nutné prejsť s každým imaginárnym klientom najskôr cez autentifikáciu, ktorá je pred asociáciou (viď. Obr. 7). Tento útok je jednoduchý len v prípade Open System autentifikácie, kedy na autentifikáciu stačí vygenerovať množstvo rôznych MAC adries imaginárnych klientov.

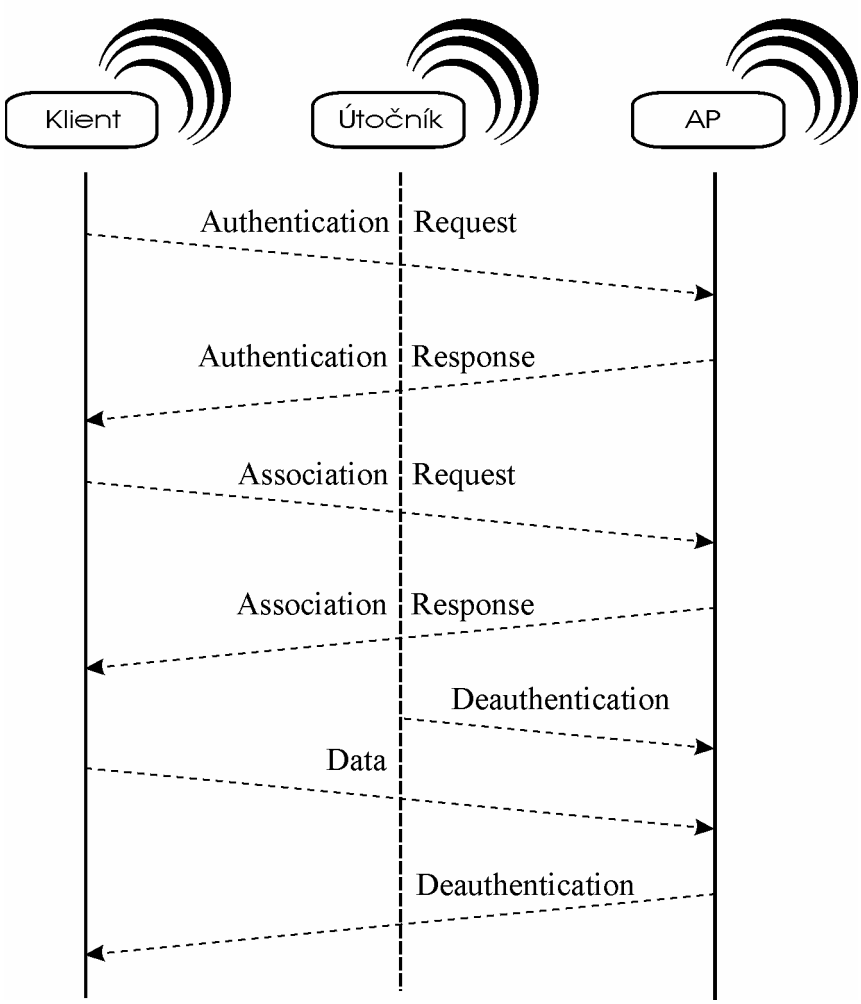
Ďalšie spôsoby zahltenia siete sú popisované v nasledujúcich častiach práce (kap. 5.6).

5.5.3 Deasociačné a Deautentifikačné útoky

Keď sa stanica chce pripojiť k AP, ako prvé si vymení autentifikačné a potom asociačné rámce. Až potom môže stanica využívať prostriedky siete (viď. Obr. 7).

Ako som už vysvetľovala v kapitole 2.6, deasociačné a deautentifikačné rámce sú oznamy, ktoré sa nedajú odmietnuť. Deasociačné aj deautentifikačné rámce môže posielať ako stanica, tak aj AP ku ktorej je stanica autentifikovaná alebo asociovaná.

Útočníkovi stačí napodobniť rámec od klienta, ktorý sa chce (teda korektnejšie – oznamuje, že sa bude) deasociovať, resp. deautentifikovať. AP deasociuje, resp. deautentifikuje klienta, čím spôsobí, že klient nemôže môcť naďalej využívať zdroje siete až pokým sa znovu neasociuje. V prípade, že takýto útok je permanentný, útočník môže jedného alebo viacerých klientov odpojiť zo siete natrvalo a spôsobiť DoS.



Obr. 17 – Deautentifikačný útok

5.6 Manipulácia s dátami

5.6.1 Modifikácia dát – útok na integritu

Prúdové šifry dovoľujú modifikáciu ľubovoľného bitu bez ovplyvnenia zbytku správy. Okrem toho WEP má nebezpečný lineárny kontrolný súčet ICV aj napriek tomu, že je šifrovaný. ICV je počítaný pomocou štandardného CRC-32 algoritmu, ktorý používa len adíciu a násobenie. Zmena jedného bitu správy zmení predpokladaný bit v ICV.

Útočník teda môže zmeniť bit na zašifrovanej správe a vie, ktorý bit sa zmení výsledne v ICV. Nepotrebuje vedieť, aké ICV je, potrebuje vedieť iba ktoré bity treba prehodiť a tým pádom ICV rekalkulovať [17]. Preto ICV nespĺňa svoj účel. Na tento útok nepotrebuje útočník poznať obsah dát.

Keďže ICV môže byť rekalkulovaný aj v zašifrovanej forme, môže útočník vziať čiastočne zrozumiteľnú správu, vymeniť ľubovoľné bity, prepočítať ICV a odoslať ju tak, aby prijímateľ správy nezistil, že bola správa modifikovaná. Aplikácia takéhoto útoku môže byť zmena cieľovej IP adresy správy, aby ju útočník dostal po káblovej sieti na vlastný počítač.

Presmerovanie paketov pomocou zmeny IP adresy

Najjednoduchšou metódou modifikácie cieľovej IP adresy správy je zistenie pôvodnej IP adresy zo zašifrovanej správy a jej úprava pomocou prehodenia bitov a rekalkulácie ICV. Avšak ani v takomto prípade nie je isté, že správa bude prijatá, pretože IP hlavička obsahuje ďalší kontrolný súčet, ktorý je potrebné tiež zmeniť alebo sa mu prispôsobiť.

Ak vieme hodnotu pôvodného kontrolného súčtu, nový kontrolný súčet vypočítame jednoducho cez XOR pôvodného a nového kontrolného súčtu.

Ak hodnotu pôvodného kontrolného súčtu nepoznáme, najjednoduchší spôsob je vyskúšať všetky možnosti a v prípade, že niektorá z nich bude správna, bude správa doručená. Ostatné správy budú zahodené na sieťovej vrstve ISO/OSI modelu.

Poslednou možnosťou je upraviť správu tak, aby nový kontrolný súčet bol rovnaký ako pôvodný. Po úprave cieľovej IP adresy ešte je nutné zmeniť niektoré bity z ostatných rámcov IP hlavičky. Najjednoduchšie je zmeniť bity v IP adrese odosielateľa.

V prípade TCP spojenia je za každým akceptovaným paketom odoslaný TCP ACK paket, ktorý oznamuje odosielateľovi úspešnosť kontrolného súčtu v TCP hlavičky a doručenia paketu. Preto modifikácia TCP paketov je vhodnejšia. Útočník sa dozvie prakticky okamžite, či bola zmena kontrolného súčtu TCP hlavičky úspešná a či bol paket úspešne doručený. TCP ACK aj keď je odosielaný z AP šifrovaný, je jednoducho rozoznateľný svojou dĺžkou. V tomto prípade nemusí byť útočník aktívne pripojený na cieľovej adrese paketu a môže mať iba aktívny nástroj na zbieranie dát, ktoré si neskôr vyzdvihne.

5.6.2 Injektáž dát

Útočník potrebuje jedinú kombináciu prúdového kľúča s IV na injektovanie paketov, pretože originálny štandard 802.11 dovoľuje odosielateľovi zvoliť si vlastný IV a nezakazuje znovupoužitie IV. Takže útočník môže opakovane použiť rovnaké IV, pre ktoré má prúdový kľúč a injektovať neobmedzené množstvo paketov do siete (v zmysle posielať), čím môže jednoducho spôsobiť zahltenie siete alebo účelne zasielať dáta.

Existuje aj druhá varianta injektáže. V prípade AP, ktoré má zapnuté WEP existuje stále možnosť, že jeho implementácia dovoľuje prijať a spracovať nešifrované broadcast pakety. Ak útočník odošle broadcast paket na AP, v niektorých prípadoch sa mu môže podariť odchytiť zašifrovanú verziu odoslaného paketu dokonca vo väčšom počte naraz v závislosti od počtu asociovaných klientov na AP, ktorým tento paket odošle. Útok sa dá využiť aj na rýchle vytvorenie slovníka prúdových kľúčov neustálym generovaním broadcast paketov.

5.6.3 Duplikácia dát

Inou aplikáciou manipulácie s dátami môže byť pre útočníka odchytenie jednoduchého TCP SYN (TCP Synchronization – TCP synchronizačného) paketu a znovu vo veľkom počte rozoslanie ako SYN flood s tým, že útočník zmení niekoľko málo parametrov každého paketu. Nemohol by rozoslať nezmenené pakety, lebo by boli na vyšších vrstvách ISO/OSI modelu považované za duplikáty a zahodené. Tým pádom by sa minuli účinku. Keďže TCP má fixnú hlavičku, útočník vie, kde v pakete sú polia, ktoré môže náhodne pomeniť na vytvorenie rôznych paketov.

Niektoré protokoly, ako napr. UDP alebo ICMP akceptujú výskyt nezmenených duplikátov, o to je útok ešte jednoduchší.

5.6.4 Zničenie dát

Klient v Power Save móde nemôže prijímať ani vysielať dáta. Preberá sa v pravidelných intervaloch a vyžiada si od AP pomocou PS-Poll rámca pakety, ktoré jej AP medzičasom uschovalo. V prípade, že útočník odošle AP PS-Poll rámec ako prvý, zapríčiní odoslanie uschovaných dát. Keďže klient nemôže v PS móde prijímať dáta, budú nenávratne stratené.

5.7 Maskovanie

5.7.1 Narušenie autentifikácie

Autentifikuje sa len klient. Preto je jednoduché predstierať (maskovať) AP a odpovedať na Authentication request management rámce od legitímnych klientov. Maskované AP v druhom kroku autentifikácie (viď Obr. 6) vymyslí náhodný text a odošle ho klientovi. Klient následne náhodný text zašifruje a odošle ho maskovanému AP spolu s IV potrebným na dešifrovanie. K dokončeniu asociácie klienta na maskované AP potrebuje útočník ešte vymeniť si s klientom asociačné rámce.

Ak bude útočník vychádzať z toho, že obdržal korektné dáta od klienta, má pôvodnú správu, zašifrovanú správu a IV. S týmito tromi informáciami dokáže, ako som už spomínala v kapitole 5.4.3. získať prúdový kľúč a narušiť dôvernosť dát.

5.7.2 Narušenie dostupnosti

Veľmi častou aplikáciou deasociačného alebo deautentifikačného útoku je cielené ukončenie komunikácie s legitímnym AP za účelom asociácie legitímneho klienta na maskovaný AP pod správou útočníka. V prípade, že útočník má lepší signál ako legitímne AP, klient sa bude pokúšať znovu autentifikovať alebo asociovať primárne na maskované AP.

5.7.3 Narušenie dôvernosti

V prípade, že má útočník k dispozícii maskované AP, ku ktorému sú asociovaní legitímni klienti, dokáže odhaliť šifrovanú komunikáciu, a tým narušiť dôvernosť dát. Štandard 802.11 dovoľuje, aby AP volilo IV akýmkoľvek spôsobom, napríklad aj neustále rovnaké IV je akceptované štandardom. V prípade, že má útočník k dispozícii jediný prúdový kľúč s kombináciou správneho IV, môže tieto informácie neustále dookola používať v šifrovanej komunikácii s klientom, pretože ak sa nemení IV, nemení sa ani prúdový kľúč použitý na šifrovanie.

5.7.4 Kontrola prístupu

V originálnom štandarde 802.11 je kontrola prístupu spojená s autentifikáciou, nakoľko asociácia (a teda prístup k zdrojom v sieti) je klientovi povolená až po úspešnej autentifikácii.

Až v štandarde 802.11b bol zavedený dodatočný spôsob kontroly prístupu k Open System autentifikácii filtrovaním MAC adries na strane AP. Asociácia je úspešná len v prípade, ak sa adresa klientskej stanice nachádza v zozname povolených adries.

Ochrana siete povolením konkrétnych MAC adries klientských staníc na AP má dve zásadné vady:

- Ručné zadávanie a obmieňanie každej MAC adresy oprávneného klienta je náročné aj v prípade menšej siete.
- Možnosť maskovania útočníka. Na väčšine klientských zariadení sa dá zmeniť MAC adresa. Pomocou odpočúvacieho nástroja môže útočník zistiť MAC adresu jedného z klientov a skopírovať si ju do MAC adresy svojho klientského zariadenia. Tento útok zároveň môže vyvolať sieťové problémy ak budú naraz obidve zariadenia s rovnakou MAC adresou aktívne.

5.8 Narušenie dôvernosti dát

Sú prinajmenšom štyri možnosti, ako odhaliť dáta chránené pomocou WEP:

- odhalenie prúdového kľúča s korektným IV
- odhalenie kľúča alebo WEP hesla samotného
- vytvorenie slovníka prúdových kľúčov s IV
- hádanie neznámych bitov zašifrovanej správy

Jednou z možností pre útočníka je počkať na opakovanie prúdového kľúča. Inou možnosťou je poznať obsah pôvodných aj zašifrovaných dát a s pomocou XOR z nich dostať prúdový kľúč. Akonáhle útočník pozná všetky prúdové kľúče, môže dešifrovať čokoľvek s daným WEP heslom. Avšak implementácia útoku na WEP heslo je jednoduchšia ako vytvárať slovníky.

5.8.1 Kolízie IV

Princíp WEP spočíva v neustálej obmene prúdového kľúča v RC4 algoritme pre každý odosielaný paket. Prúdový kľúč sa mení len ak sa mení kľúč (spojenie WEP hesla s IV) v KSA. WEP heslo je konštantné do doby, kým sa ručne nevymení u všetkých klientov a na AP (resp. na všetkých staniciach v IBSS móde), takže jediným prvkom algoritmu, ktorý spôsobuje zmenu prúdového kľúča je práve IV.

Keďže IV je odosielané príjemcovi dát v nešifrovanom formáte, detekcia rovnakého prúdového kľúča použitého na zašifrovanie odosielaných dát je jednoduchá. Stačí hľadať rovnaké (tzv. kolízne) IV v hlavičkách prijatých paketov.

Ako som už spomínala, WEP používa 24-bitové IV. Celkový počet rôznych IV je teda 2^{24} = 16 777 216. Takéto množstvo rôznych IV sa môže zdať byť dostatočne veľké na zabránenie kolíziám.

Ak IV je náhodné číslo, v skutočnosti nie je nutné čakať 2^{24} paketov na kolíziu dvoch IV. Dôvodom je tzv. narodeninový paradox [3], ktorého podstata je v tom, že je ľahšie nájsť dve hodnoty, ktoré sa rovnajú, než nájsť zhodu s niektorou konkrétnou hodnotou. Narodeninový paradox sa dá vyjadriť matematickou rovnicou $P \approx 1{,}2 * \sqrt{k}$, kde k je počet všetkých možností. V množine 23 osôb je pravdepodobnosť okolo 50%, že dve osoby majú rovnaký mesiac a deň narodenia (k = 365). To znamená, že v prípade náhodne generovaného IV stačí čakať na 50% pravdepodobnosť zhody len okolo 5 000 paketov ($1{,}2 * \sqrt{2^{24}} = 4915$ paketov). Šanca na kolíziu IV sa zvyšuje na 99% už pri 12 430 paketoch. [28]

Pri priemernej komunikácii 1500 B paketov, môže kolízia nastať už pri prenesení cca 7 MB dát (5 000 paketov * 1 500 B veľkosť paketov ≈ 7 MB dát). Pri maximálnej prenosovej rýchlosti štandardu 802.11 2 Mbps sa 7 MB dát prenesie za 28 sekúnd. (7 MB / {2 Mbps / 8 b/s} = 28 s). 12 430 paketov je približne 18 MB dát, takže v najhoršom prípade stačí čakať pri hustej premávke cca 72 sekúnd. Kolízia IV v prípade plne zaťaženého AP nastane v priebehu 1 minúty. Avšak v realite plne zaťažené AP nebýva. Útočníkovi teda môže stačiť

na odchytenie kolízneho IV len niekoľko málo minút v závislosti od množstva dát tečúcich cez AP.

Pri tak veľkom počte IV je náhodné generovanie IV tak aby sa neopakovali obtiažne. Udržiavať tabuľku o veľkosti približne 48 MB ({3 B veľkosť IV * 2^{24} rôznych IV}/ 1024 B^2 = 48 MB) a sledovať výskyt už použitých IV by bolo príliš náročné a spomaľovalo by komunikáciu, nehovoriac o zvýšení réžie na AP.

Zariadenia od mnohých výrobcov používajú IV inicializujúci sa pri každom zapnutí zariadenia na 0 a inkrementujúci sa o 1 každým paketom. V takom prípade je zrejmé, že kolízia IV nastane po otočení všetkých 2^{24} IV. 802.11 pakety majú veľkosti od 34 B do 2 346 B. Kolízia teda nastane medzi 544 MB ({2^{24} rôznych IV * 34 B}/1024^2 B = 544 MB) a 37 GB ({2^{24} rôznych IV * 2 346 B}/1024^3 B = 37 GB) prenesených dát. Pri maximálnej prenosovej rýchlosti 2 Mbps nastane kolízia medzi 36 minútami a 42 hodinami. V prípade iných verzií štandardov s vyššími rýchlosťami je čas odchytenia kratší nakoľko prenosová rýchlosť ovplyvňuje rýchlosť obdržania dostatočného počtu paketov. V prípade štandardu 802.11b nastane kolízia pri maximálnej prenosovej rýchlosti 11 Mbps do 8 hodín.

Oproti náhodne generovaným IV nastane kolízia v prípade inkrementujúcich sa IV podstatne neskôr. Avšak metóda inicializácie IV od 0 a inkrementácie o 1 napomáha útočníkovi vytvoriť slovník v prípade, že zapnutie zariadení je v určitej dennej dobe bežnou záležitosťou a má istotu, že niekoľko IV v tisíc paketoch bude použitých znova.

Najbezpečnejšou spomedzi bežných implementácií je inicializácia IV na náhodné číslo s inkrementáciou o 1 každým paketom. Najnebezpečnejšou implementáciou je konštantné IV, kedy kolízia nastáva s každým paketom.

Prečo je kolízia IV nebezpečná? Ak poznáme jednu pôvodnú správu a prúdový kľúč, je v prípade kolízie relatívne jednoduché obdržať obsah správ v oboch paketoch s kolíznym IV. Známa pôvodná správa 1 nech je N_1, jej šifrovaný ekvivalent nech je S_1, prúdový kľúč P a neznáma správa 2 s rovnakým IV nech je N_2, resp. S_2 v šifrovanom stave. Potom môžeme použiť nasledujúce rovnosti:

$$S_1 = N_1 \text{ XOR } P$$

$$S_2 = N_2 \text{ XOR } P$$

$$(S_1 \text{ XOR } S_2) = (N_1 \text{ XOR } P) \text{ XOR } (N_2 \text{ XOR } P)$$

$$(S_1 \text{ XOR } S_2) = N_1 \text{ XOR } N_2$$

$$(S_1 \text{ XOR } S_2) \text{ XOR } N_1 = N_2$$

Z rovností vyššie nám vyplýva, že neznámy obsah správy 2 dostaneme s pomocou obidvoch zašifrovaných správ a známeho obsahu správy 1. Prúdový kľúč keby nebol rovnaký, nemohli by sme upraviť 3. rovnosť na tvar 4. rovnosti a tým pádom by sme nemohli odhaliť neznámy obsah správy 2.

5.8.2 Extrakcia kľúča

Pokiaľ by útočník vedel extrahovať kľúč (IV + WEP heslo), resp. WEP heslo, mohol by sa pripojiť do bezdrôtovej siete a stať sa jej legitímnym používateľom.

Existuje niekoľko nástrojov na internete, ktoré sa dajú použiť na extrakciu WEP hesla. Nezávisle od nástroja, takmer všetky používajú rovnaký koncept na jeho vyvodenie. Niektoré nástroje používajú viac komplexnejšie algoritmy na hádanie hesla na rozdiel od štandardnej techniky. Aj napriek tomu, že tieto dosiahnu cieľ skôr, spoliehajú sa viacej na pravdepodobnostné metódy, ktoré môžu viesť k nesprávnym záverom.

Útok je zameraný na trhlinu v KSA RC4 protokolu. Trhlinou je nepatrná štatistická anomália, ktorá spôsobuje, že niektoré heslá s konkrétnou štruktúrou majú tendenciu čiastočne zostať obsiahnuté v kľúči.

V krátkosti, všetky pakety zaslané cez bezdrôtovú sieť obsahujú SNAP hlavičku [16]. Táto hodnota je vždy prvý bajt v odosielanom pakete, ktorý vstupuje do šifrovacej funkcie RC4 s prvým PRGA bajtom na vytvorenie prvého zašifrovaného bajtu. Ako som už ukázala, sú potrebné len dve informácie z troch na dedukciu poslednej v šifrovacej (XOR) funkcii. S touto znalosťou ak vieme pôvodný bajt SNAP hlavičky zašifrovaného paketu, ľahko zistíme bajt prúdového kľúča. Hodnota SNAP hlavičky je 0xAA v prípade IP a ARP komunikácie. V prípade IPX komunikácie má hodnotu 0xFF alebo 0xE0. No v skutočnosti obvykle IP a ARP pakety značne prevyšujú počtom IPX pakety, takže v takom prípade predpokladať hodnotu SNAP hlavičky 0xAA je pomerne logické a je základom k úspešnej extrakcii hesla.

Táto metóda je okrem iného závislá na fakte, že každý paket obsahujúci IV v slabom formáte (tzv. slabé IV) má relatívne vysokú (5%) šancu na odhalenie bajtu WEP hesla [29]. Iba 2000 paketov obsahujúcich slabé IV stačí na vyvodenie WEP hesla. Avšak, na obdržanie toľkých slabých IV je nutné zozbierať niekoľko miliónov paketov. Pri dostatočnom počte paketov (2-5 mil.), je pravdepodobnosť úspešného objavenia hesla značne vysoká a heslo je extrahované s veľmi veľkou presnosťou. [19]

Slabé IV

Formát slabého IV je (B+3, N-1, X), kde B je hľadaný bajt hesla (posunutý o známe 3 bajty kľúča - IV), N je veľkosť stavového poľa a X ľubovoľná hodnota 0-255 (ľubovoľný ASCII znak, číslo alebo hexadecimálna hodnota v dekadickej forme).

Teraz prejdeme cez prvé štyri cykly KSA algoritmu s použitím vybraného IV. Robíme to preto, aby sme zistili hodnoty, ktoré by boli v prípade slabého IV. Takisto tieto hodnoty použijeme neskôr keď sa budeme snažiť o rozbor KSA – aký by použil útočník na zlomenie WEP.

KSA

Prvým krokom RC4 algoritmu je vytvorenie stavového poľa. Pole obsahuje 256 hodnôt, spočiatku v poradí, neskôr poprehadzované. Pre lepšiu orientáciu uvádzam ešte raz kód KSA z kapitoly 3.2.4:

K – pole, v ktorom je uložený kľúč (konštantné)
d – dĺžka kľúča (dĺžka poľa K - pri 40-bit. WEP je dĺžka konštantne rovná 5)
S – stavové pole (256 8-bitových hodnôt, premenné)
m – veľkosť stavového poľa (konštantne 256 hodnôt)
swap(g,h) – funkcia pre zámenu prvkov *g* a *h*

naplnenie stavového poľa hodnotami od 0 do 255

```
for i from 0 to m-1
    S[i] := i
endfor
```

poprehadzovanie stavového poľa s použitím vlastností kľúča

```
j := 0
for i from 0 to m-1
    j := (j + S[i] + K[i mod d]) mod m
    swap(S[i],S[j])
endfor
return S
```

Príprava na prechod cez algoritmus RC4 so slabým IV

Pri vyšetrovaní slabosti WEP je potrebných niekoľko predpokladov na vyšetrenie testovacieho procesu. Pre nás príklad budeme uvažovať, že nasledujúce informácie sú pravdivé:

B = 0 (hľadáme prvý bajt hesla)
IV = B+3,255,7 = 3, 255, 7 (jedno z 256 slabých IV pre hádanie 1. bajtu hesla)
H = 22222 (WEP heslo, pre ilustráciu postačí aj takéto)
K = IV + H = (3,255,7,2,2,2,2,2) (kľúč)
S = (0..255) (stavové pole po prvom cykle KSA algoritmu)

KSA 2. cyklus, krok 1

Počiatočné hodnoty premenných: i = 0, j= 0, (i mod d) = 0, S=(0,1,2,3,4,...,255)
Výpočet nových hodnôt premenných:

Budeme potrebovať K[i mod d] = K[0] = 3
j = (j + S[i] + K[i mod d]) mod m = (0+ 0 + 3) mod 256 = 3
Výmena S[0] s S[3], teda S=(3,1,2,0,4,...,255)

KSA 2. cyklus, krok 2

Počiatočné hodnoty premenných: i = 1, j= 3, (i mod d) = 1, S=(3,1,2,0,4,...,255)
Výpočet nových hodnôt premenných:

Budeme potrebovať K[i mod d] = K[1] = 255
j = (j + S[i] + K[i mod d]) mod m = (3+ 1 + 255) mod 256 = 3
Výmena S[1] s S[3], teda S=(3,0,2,1,4,...,255)

KSA 2. cyklus, krok 3

Počiatočné hodnoty premenných: i = 2, j= 3, (i mod d) = 2, S=(3,0,2,1,4,...,255)
Výpočet nových hodnôt premenných:

Budeme potrebovať K[i mod d] = K[2] = 7
j = (j + S[i] + K[i mod d]) mod m = (3+ 2 + 7) mod 256 = 12
Výmena S[2] s S[12], teda S=(3,0,12,1,4,...,11,2,13,...,255)

Až do tohto momentu KSA nepoužilo žiadnu časť hesla pri prehadzovaní poľa S. To znamená, že každý má možnosť reprodukovať hodnoty generované prvými tromi cyklami KSA.

KSA 2. cyklus, krok 4

Počiatočné hodnoty premenných: i = 3, j= 12, (i mod d) = 3, S=(3,0,12,1,4,...,11,2,13,...,255)
Výpočet nových hodnôt premenných:

Budeme potrebovať K[i mod d] = K[3] = 2 (prvý bajt WEP hesla)
j = (j + S[i] + K[i mod d]) mod m = (12+ 1 + 2) mod 256 = 15
Výmena S[3] s S[15], teda S=(3,0,12,15,4,...,11,2,13,14,1,16,...,255)

V tomto kroku cyklu KSA priradí do S[3] vždy jeden bajt WEP hesla. S pravdepodobnosťou 5% sa už hodnoty S[0]..S[3] v ďalších krokoch cyklu nezmenia [29]. V tomto momente už môžeme skončiť krokovanie 2. cyklu KSA algoritmu a pozrieť sa na funkčnosť PRGA algoritmu so stavovým poľom S=(3,0,12,15,...).

PRGA

PRGA je druhý z algoritmov RC4. Štartuje inicializáciou dvoch premenných i,j a potom tieto premenné použije spolu s hodnotami v poli S na vytvorenie prúdového kľúča. Pre lepšiu orientáciu uvádzam ešte raz kód PRGA z kapitoly 3.2.5:

L – dĺžka požadovaného prúdového kľúča
P – pole o veľkosti L, v ktorom bude uložený prúdový kľúč
S – stavové pole (256 8-bitových hodnôt)
m – veľkosť stavového poľa (konštantne 256)
swap(g,h) – funkcia pre zámenu prvkov *g* a *h*

```
i := 0
j := 0
for k from 0 to L-1
    i := (i + 1) mod m
    j := (j + S[i]) mod m
    swap(S[i],S[j])
    P[k] := S[(S[i] + S[j]) mod m]
endfor
return P
```

PRGA krok 1

Počiatočné hodnoty premenných: i = 0, j= 0, S=(3,0,12,15,...)
Výpočet nových hodnôt premenných:

i = (i + 1) mod 256 = (0 + 1) mod 256 = 1
j = (j + S[i]) mod 256 = (0 + S[1]) mod 256 = 0
Výmena S[1] s S[0], teda S=(0,3,12,15,...)
P[0] = S[(S[i] + S[j]) mod 256] = S[(0 + 3) mod 256] = S[3] = 15

V tomto momente sme obdržali prvý bajt prúdového kľúča, ktorý vstupuje do šifrovacej funkcie XOR s prvým bajtom pôvodných dát. V tomto prípade bude 1. bajt zašifrovaných dát 15 XOR OxAA = 15 XOR 170 = 160.

Kroky útočníka

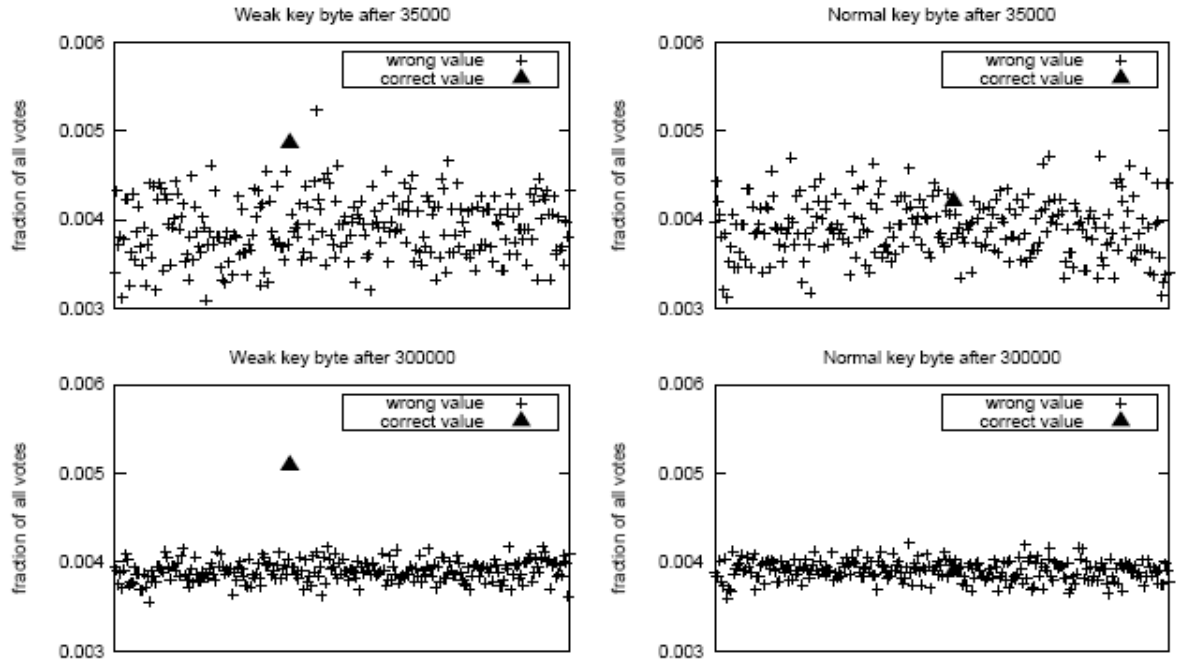
Predchádzajúce časti ukázali, ako zo známych hodnôt algoritmy KSA a PRGA produkujú hodnoty prúdového kľúča. Teraz sa položíme do role útočníka. Útočník v KSA kroku 4 nepozná hodnotu prvého bajtu WEP hesla.

Pre neho sú známe iba tieto fakty:

- IV = 3,255,7
- bajt šifrovaného textu je 165

Útočník potrebuje postupovať opačne. Z 1. bajtu zašifrovaných dát dostane 1. bajt pôvodných dát, teda P[0] = 165 XOR 0xAA = 165 XOR 170 = 15. Ďalej útočník vie, že P[0] = S[3] a vie prejsť prvými tromi krokmi 2. cyklu KSA bez nutnosti použitia hesla.
V závere 3. kroku 2. cyklu KSA má teda tieto informácie: i = 3, j = 12, (i mod d) = 3, S = (3,0,12,1,4,...,11,2,13,...,255). Keďže S[3] = P[0] = 15 na konci 4. kroku 2. cyklu KSA, ľahkou dedukciou zistí, že nastala výmena S[3] a S[15] a že hodnota j = 15. Keďže hodnota j sa počíta j = (j + S[i] + K[i mod d]) mod m a útočník pozná i = 3, S[3]=15 a j = 15, dostaneme, že prvý bajt hesla K[3] = 2.

Útok sa spolieha na veľké množstvo odchytených zašifrovaných dát a pozerá sa na pakety, v ktorých má kľúč slabú štruktúru. Musím však ešte raz poznamenať, že tento postup nefunguje vždy s každou hodnotou. Úspešnosť je stále len 5%. Napríklad IV 3,255,10 by nevyprodukovalo správny bajt hesla. Z tohto dôvodu potrebuje útočník veľké množstvo (v stovkách) zaujímavých paketov so slabým IV, aby postupne odhaľoval bajty kľúča. Medzičasom slabý bajt sa bude ukazovať viacej častým výskytom ako ostatné hodnoty a bude jednoducho identifikovateľným ako je vidieť na obrázku nižšie [12]. Z obrázku je zrejmé, že čím viac zaujímavých paketov útočník obdrží, tým je väčšia šanca odhaliť správny bajt hesla.



Obr. 18 – Odhalenie bajtu WEP hesla pravdepodobnostnou metódou

5.8.3 Slovníkové útoky

Schopnosť útočníka dešifrovať pakety pomocou slovníkového útoku je úmerná kompletnosti slovníka prúdových kľúčov pre jedno WEP heslo. Ak má útočník kompletný slovník, môže dešifrovať akýkoľvek zašifrovaný paket kým sa nezmení WEP heslo. Toto je ekvivalentné

znalosti WEP hesla, dokonca efektívnejšie nakoľko na dešifrovanie potrebuje útočník v prípade slovníka len vyhľadávajúcu funkciu pre spárovanie IV s prúdovým kľúčom a šifrovaciu funkciu - XOR. Dômyselný útočník môže ukladať pakety, ktorých obsah nepozná v prípade, že nepozná prúdový kľúč na dešifrovanie tohto paketu, ale predpokladá, že v budúcnosti tento prúdový kľúč bude mať a bude vedieť paket dešifrovať bez nutnosti byť v dosahu BSS.

Slovník všetkých prúdových kľúčov, ktoré sú 1500 B dlhé má približne 24 GB (1500 B * 2^{24} rôznych IV = 24 GB) a dá veľa námahy pozbierať toľko dát na vytvorenie kompletného slovníka.

V prípade väčšieho WEP hesla je slovníkový útok rovnako obtiažny, nakoľko sa vytvára slovník kombinácií prúdových kľúčov s IV a nie WEP heslami. Takže v konečnom dôsledku bude slovník rovnako veľký.

Okrem slovníkových útokov popísaných v kap. 5.5.2 a 5.8.1 existujú ďalšie typy útokov, ktoré popíšem v tejto kapitole.

Poznať pôvodný obsah dát

Získať pôvodné dáta sa dá donútením používateľa prijať alebo odoslať predvídaný paket. Na zabezpečenie môže poslúžiť chat alebo e-mail so známym obsahom pre útočníka. Avšak táto metóda môže byť tiež náročná, nakoľko sa k prenášaným dátam pripájajú hlavičky z vyšších sieťových vrstiev ISO/OSI modelu s neznámym obsahom a iné mätúce informácie. V takomto prípade, ak má byť útočník úspešný, potrebuje odoslať správu, ktorá zvyšuje šance odhaliť kľúč. Napríklad e-mail s prázdnym obsahom, dlhý text z rovnakých písmeniek, spam alebo ICMP ping napomôže k úspešnému odhaleniu. Ak útočník pošle známy e-mail používateľovi, bude mať 3 informácie: pôvodné dáta, IV a zašifrované dáta, z ktorých dostane pomocou XOR prúdový kľúč. Útočník môže posielať takýchto dát množstvo a tak vytvoriť si slovník prúdových kľúčov.

Ak má útočník prístup do siete, môže si nainštalovať odchytávací nástroj a odchytávať dáta ešte pred zašifrovaním. Potom by tie isté dáta mohol odchytávať aj bezdrôtovo a porovnávať ich cez XOR, čím by vytváral slovník prúdových kľúčov. Avšak to je už nepodstatné, pretože akonáhle má útočník prístup do siete, nepotrebuje vytvárať slovník.

Načrtla som niekoľko spôsobov extrakcie prúdového kľúča, avšak v praxi sú veľmi ťažko implementovateľné. Aj keď je možné extrahovať čistý text zo zašifrovanej informácie pomocou niekoľkých XOR funkcií, počet takto obsiahnutých informácií je limitovaný. Útočník by musel zahltiť bezdrôtovú sieť, dokiaľ by obdržal všetky IV kombinácie. Následne by musel vytvoriť program, ktorý by dešifroval každý zašifrovaný paket XOR-ovaním s jeho pôvodným obsahom a vytváral slovník.

Generátory WEP hesla

Silnejšie WEP heslá sú 104-bitov alebo 26-hexadecimálnych číslic dlhé (štandard 802.11b). Keďže WEP heslá sa zvyknú zadávať ručne, niekoľko výrobcov vyvinulo metódu založenú na zadaní hesla v alfa-numerických znakoch a následne prepočítanú hashovacím algoritmom na potrebný tvar 40 alebo 104 bitov. Na zabezpečenie kompatibility existuje štandard na

hashovací algoritmus. Nanešťastie tento algoritmus redukuje počet WEP hesiel, ktoré môžu byť zvolené a otvára možnosti pre slovníkové útoky. [8]

Tim Newsham [31] predviedol nástroj wep_crack, ktorý vie zlomiť heslá generované hashovacím algoritmom z alfa-numerických znakov. Jednou technikou, ktorú to používa je prejdenie všetkých slov v klasickom slovníku cez hashovací algoritmus. Najskôr nájde zašifrovaný paket, potom sa snaží ho dešifrovať pomocou klasického slovníka. Ak ICV paketu je správne, nástroj vie, že dešifroval správne a s vysokou pravdepodobnosťou našiel WEP heslo.

Newsham tiež prišiel na to, že algoritmus na generovanie 40-bitového hesla dovolí vytvoriť len 2^{21} (2 mil.) možných WEP hesiel bez ohľadu na dĺžku alebo komplexnosť hesla prechádzajúceho cez hashovací algoritmus. S takýmto počtom rôznych hesiel by trvalo útočníkovi len niekoľko minút na dešifrovanie paketov pomocou útoku hrubou silou (brute-force). Newsham napísal aj nástroj wep_decrypt, ktorý dešifruje odchytené pakety mimo dosahu BSS zo súboru s pomocou známeho WEP hesla. Tento nástroj samozrejme nie je závislý od metódy obdržania WEP hesla.

5.8.4 Hádanie bitov

Ďalšou metódou je predvídať známe komunikačné hlavičky. Pakety prechádzajúce cez bezdrôtovú sieť obsahujú niekoľko známych hodnôt, akými sú bezpochyby IP hlavičky, IPX hlavičky, SNAP hlavičky a mnoho ďalších, vďaka ktorým útočník dokáže odvodiť časti hesla zo zašifrovaných dát Takáto slabina vyústila v naprogramovaní niekoľkých nástrojov, ktoré dedukujú známy obsah paketov.

Reakčný útok [23]

Útočník môže uhádnuť hodnotu bitu, ktorý nepozná. Tým, že TCP/IP hlavičky sú čiastočne predvídateľné, môže útočník prehodiť niektoré bity správy, znovu odoslať správu a pozrieť, či paket má správny TCP/IP kontrolný súčet jednoduchým zachytením zašifrovaného TCP ACK paketu. Aj napriek tomu, že je zašifrovaný, je TCP ACK paket odhaliteľný svojou dĺžkou.

Pri dodržaní podmienky P_i XOR $P_{i+16} = 1$ v pôvodnej správe ostane TCP kontrolný súčet nezmenený. Teda prítomnosť TCP ACK odpovede nám prezradí jeden nový bit z neznámej časti zašifrovanej správy. Opakovanou procedúrou niekoľko alebo všetky kľúče pre konkrétne IV môžu byť odhalené.

Induktívny útok [36]

Ďalším z dômyselných útokov na kľúč je metodické skúšanie a chybovanie. Predpokladajme, že útočník začne s konkrétnym množstvom n (v zmysle známej dĺžky) kľúčov pre konkrétne IV a heslo. Môže obdržať prvý kľúč sledovaním ľahko uhádnuteľného paketu, ako napr. DHCP request alebo podstrčením známeho obsahu. Teraz útočník začne induktívny útok. Vytvorí paket (napr. ICMP ping alebo ARP request ktorý žiada odpoveď), zvolí dĺžku paketu aj s 802.11 kontrolným súčtom na n+1. Útočník však pozná len n bajtov z kľúča, takže musí uhádnuť n+1. byte. Spraví to odoslaním 256 verzií paketov so všetkými možnosťami posledného bajtu. AP odstráni 255 zlých paketov, ale správny paket má korektný kontrolný

súčet a bude prijatý + vyšle sa potvrdzujúca odpoveď o prijatí paketu. Tým pádom útočník odhalí postupne každý ďalší bajt až po celú dĺžku kľúča pre konkrétne IV.

5.9 Zhrnutie

V tomto bode môže byť už pre čitateľa zrejmé, že WEP je slabým protokolom na zabezpečenie bezdrôtovej siete a existuje mnoho pomerne jednoduchých postupov na jeho oslabenie. Hlavným dôvodom sú nezabezpečené management rámce, ktoré sa dajú veľmi ľahko zneužiť a slabá implementácia RC4 algoritmu.

Na lepšie zabezpečenie dôvernosti dát by postačoval akýkoľvek automatický manažment distribúcie a obmeny WEP hesiel po odoslaní 2^{24} paketov, pretože sila RC4 algoritmu spočíva práve v neopakovaní sa prúdových kľúčov, resp. v náhodnom malom počte. Počet rôznych IV je príliš malý. Ďalšou možnosťou by mohlo byť použitie väčších IV, a tým pádom by kolízie IV nastali zriedkavejšie.

Spomínané útoky v tejto kapitole nezávisia od veľkosti použitého WEP hesla. Väčšie heslo iba predĺži čas, ktorý potrebuje útočník na zdolanie bezpečnosti, avšak nespôsobí radikálnu zmenu zabezpečenia. Nakoľko obmena WEP hesla je pre ručné spracovanie vo väčšine sietí extrémne časovo náročná, je zrejmé, že nebude dostatočne často realizovaná a v prípade úspešného zdolania dôvernosti dát môže útočník dlhšie sledovať dôverné informácie.

Slovníkové útoky trvajú podstatne kratšie ako útoky hrubou silou. V prípade 104-bitového WEP-hesla je útok hrubou silou s dnešnou bežne dostupnou výpočtovou silou nemožný.

6 Experimentálna časť

V tejto časti práce chcem ukázať niektoré aspekty komunikácie staníc v štandarde IEEE 802.11, niektoré typy útokov na bezpečnosť štandardu a podrobnosti použitia vybraných nástrojov. Použila som len voľne šíriteľné nástroje .

6.1 Vybrané zariadenia

Odchytávanie a časti analýzy paketov som robila na notebooku HP NX9420 s procesorom Intel Core 2 Duo, 2,16 GHz s 1 GB RAM a operačným systémom Slackware Linux alebo Windows XP (označený ako NB 1). Ostatnú analýzu som robila na notebooku Prestigio Nobile 151C s procesorom Intel Pentium Mobile, 1,4 GHz s 512 MB RAM s operačným systémom Slackware Linux (označený ako NB 2) a simuláciu bezdrôtovej komunikácie (sťahovaním obrovského súboru) som robila na notebooku HP Omnibook XE3 s procesorom Intel Pentium 3, 930 MHz s 512 MB RAM s operačným systémom Windows XP (označený ako NB 3).

Na odchytávanie paketov z bezdrôtovej komunikácie som musela použiť bezdrôtové zariadenie do NB 1. Chipsety najčastejšie používané a podporované na odpočúvanie sú Prism2 (používané v zariadeniach Linksys, D-link, SMC, a i.), Orinoco (používané v zariadeniach Lucent), a Aironet (používané v zariadeniach Cisco). Mojím výberom bola bezdrôtová PCMCIA karta Orinoco Gold.

Ostatné použité bezdrôtové zariadenia v rámci experimentov použité na rolu klientov alebo AP boli všetky od výrobcu D-com. Ako AP som použila zariadenie WX-1590 a ako klientov striedavo zariadenie WP-102 a dve zariadenia WX-1590.

6.2 Vybrané nástroje

Nástroje na odpočúvanie musia zvládnuť minimálne tri základné funkcie:

- odchytiť pakety
- analyzovať užitočné pakety
- zobraziť informácie obsiahnuté zo zachytených paketov

Množstvo nástrojov môže napomôcť k zmapovaniu sietí. Sú dostupné na rôzne operačné systémy (Linux, Windows, Macintosh, BSD, a i.) a na veľa druhov chipsetov a zariadení, ako aj laptopy a PDA. Niektoré z týchto nástrojov sú zadarmo a majú open-source kód. Komerčné nástroje majú obvykle viacej funkcií užitočných na stopovanie a zisťovanie trhlín v zabezpečení siete.

Na sledovanie dostupných sietí som použila Kismet a Netstumbler, na odpočúvanie som vybrala Tcpdump, Ethereal, Kismet, AirSnort a na analýzu dát som použila nástroje AirSnort, Wepcrack, WEPlab a WEP Attack. Nasleduje ich podrobný popis funkcií.

6.2.1 Netstumbler

Autor: Marius Milner

Popis:
Nástroj na zobrazovanie informácií o dostupných bezdrôtových sieťach. Netstumbler je jedným z prvých voľne šíriteľných sledovacích nástrojov. Zobrazuje rôzne informácie o bezdrôtových sieťach, ako napr. silu signálu, ESS ID, vysielací kanál, spôsob šifrovania, druh podporovaného štandardu a i. Má podporu GPS, takže sa siete dajú ľahko lokalizovať pomocou ďalších nástrojov do máp.

Netstumbler je viac ako len nástroj vďaka interaktívnej webovej stránke [25], na ktorej sa dajú ukladať a vyhľadávať MAC adresy a lokality naskenovaných AP. Na webovej stránke existuje skript, ktorý prekonvertuje dáta do súborov čitateľných pre mapový nástroj Map Point 2002.

Program je veľmi užitočným a obľúbeným nástrojom pod operačným systémom Windows. Existuje aj verzia pre vreckový počítač alebo mobilné zariadenia s názvom MiniStumbler.

Operačné systémy: Windows

6.2.2 Kismet

Autor: Mike Kershaw

Popis:
Nástroj na identifikáciu a sledovanie bezdrôtových sietí. Kismet je voľne šíriteľný nástroj s bohatou funkcionalitou. V porovnaní s Netstumbler-om je bohatší o zachytávanie paketov, kreslenie grafu počtu paketov v priebehu času, analýzu siete , ukladanie paketov do súborov pre iné nástroje, grafické znázornenie zachytených sietí a i.

Verzia 2.0 obsahuje navyše vzdialenú prácu s nástrojom, čo rozširuje jeho možnosti použitia pre systémových administrátorov, ako aj útočníkov. Na prácu s nástrojom nie je teda nutný fyzický prístup k zariadeniu, na ktorom je nainštalovaný.

Kismet je zrejme najobľúbenejším nástrojom na sledovanie sietí a zachytávanie paketov pod operačným systémom Linux, BSD a MacOS. S inštaláciou vo Windows sú mierne ťažkosti, preto dajú používatelia radšej prednosť NetStumbler-u.

Operačné systémy: Linux, BSD, MacOS, Windows (Cygwin)

Ethereal (Wireshark)

Autor: Gerald Combs

Popis:
Nástroj na zachytávanie, analýzu a prehliadanie prenášaných dát v sieti. Ethereal je jeden z najpopulárnejších voľne šíriteľných nástrojov na analýzu paketov. Dôvodom je, že podporuje množstvo operačných systémov, dokáže analyzovať pakety zo súborov, ktoré vytvorili iné odpočúvacie nástroje (Tcpdump, NetXray a i.), dokáže pakety aj ukladať do súborov pre neskoršiu analýzu inými nástrojmi, filtrovať pakety, rekonštruovať hlavičky viac ako 260 rôznych protokolov a zachytávať pakety na rôznych médiách (ethernet, PPP, token ring, X-25, a i.).

Grafické rozhranie Ethereal-u v rôznych operačných systémoch je to isté. V hlavnom okne sa nachádzajú 3 podokná:

- Okno 1: zoznam odchytených paketov
- Okno 2: detail vybraného paketu
- Okno 3: hexadecimálny a ASCII výpis hlavičky vybraného paketu

V okne 1 sa nachádzajú len niektoré informácie k zachytenému paketu: poradové číslo, čas zachytenia, zdrojová a cieľová adresa, protokol a vybrané informácie k paketu závislé od protokolu.

Program je veľmi užitočným nástrojom ako pre systémového administrátora, tak aj pre útočníka a mal by byť súčasťou arzenálu nástrojov každého sieťového odborníka.

Operačné systémy: UNIX, BSD, Windows, AIX, MAC OS, Solaris a i.

6.2.3 AirSnort

Autor: The Shmoo Group

Popis:
Nástroj na lámanie WEP hesla na princípe slabých IV z kap. 5.8.2. AirSnort je schopný pasívneho sledovania prevádzky v sieti, ukladania paketov a ich analýzy v reálnom čase. Airsnort síce nebol jedným z prvých nástrojov na lámanie WEP, ale aspoň boli do neho zakomponované neskoršie zistené metódy postupného odhaľovania WEP hesla, čím spravili z tohto nástroja jeden z najefektívnejších. AirSnort je veľmi obľúbeným nástrojom aj z dôvodu jeho jednoduchosti použitia. Je to kompletný nástroj, ktorý vie bezdrôtovú kartu prepnúť na odchytávanie a má kvalitne spracované prostredie. Dokáže odhaliť 104-bitové heslo s použitím cca 1,5 mil. zašifrovaných paketov.

Verzia 2 má funkciu lámania WEP hesla automaticky zapnutú popri zachytávaní paketov na rozdiel od pôvodnej verzie. Obidve verzie obsahujú možnosť urýchliť lámací proces zadaním inej úrovne na úkor presnosti hádania hesla alebo naopak.

AirSnort je najlepší nástroj na zlomenie WEP hesla. Aj keď neobsahuje toľko funkcií ako iné nástroje, je veľmi obľúbeným a rýchlym nástrojom na zachytávanie paketov a lámanie v reálnom čase.

Operačné systémy: Linux, Windows

6.2.4 WEPCrack

Autor: Anton Rager, Paul Danckaert

Popis:
Nástroj na lámanie WEP hesla. WEPCrack bol prvým verejne uvoľneným spomedzi nástrojov na zlomenie WEP hesla po zverejnení [29] trhlín v implementácii RC4 algoritmu v roku 2001. Tým, že bol vyvíjaný ako jeden z prvých nástrojov, nie je najrýchlejší a potrebuje veľké množstvo paketov. WEPCrack je kolekciou viacerých nástrojov – Prism-getIV.pl, WEPCrack.pl a WeakIVGen.pl.

WEPCrack obsahuje 3 Perl skripty:

- Prism-getIV.pl – skript načíta súbor s odchytenými paketmi (napr. z Ethereal) a hľadá v ňom slabé IV, ktoré ukladá do IVFile.log súboru. Skript môže byť pustený s aktívnym Ethereal v reálnom čase.
- WEPCrack.pl – skript vezme IVFile.log súbor, z ktorého pomocou metódy opísanej v kap. 5.8.2 prepočíta prvé tri cykly KSA/PRGA algoritmu a použije slabé IV na reverzný proces zisťovania WEP hesla bajt za bajtom. Napokon používa štatistickú metódu na zistenie správneho WEP hesla. V prípade malého počtu slabých IV môže skript vyprodukovať nesprávne WEP heslo. WEP heslo ukazuje v hexadecimálnej podobe.
- WeakIVGen.pl – skript, ktorý po zadaní WEP hesla (5 alebo 13 bitového) vygeneruje všetky slabé IV do IVFile.log súboru.

WEPCrack nedokáže odchytávať pakety, takže potrebuje externý nástroj na zlomenie WEP. Na istotu zlomenia WEP hesla je odporúčané [8] zozbierať aspoň 7 GB dát.

Operačné systémy: Linux, BSD s podporou Perl

6.2.5 WepLab

Autor: José Ignacio Sánchez Martín

Popis:
Weplab implementuje niekoľko pasívnych útokov na WEP (útok hrubou silou, slovníkový útok aj útok na extrakciu kľúča pravdepodobnostnou metódou). Je schválne písaný bez optimalizácie kódu pre edukačné účely, aby čitateľ kódu pochopil jeho princíp. Ale aj napriek neoptimálnemu kódu patrí medzi najefektívnejšie nástroje na zlomenie WEP hesla.

WepLab sa pokúša zdolať WEP heslo s použitím týchto druhov útokov:

- Útok hrubou silou – skúšaním všetkých kombinácií možných WEP hesiel a overovanie ich správnosti. Je možné obmedziť základňu hesiel

hexadecimálnymi podmnožinami, napr. 7F:7F:7F… obmedzí heslo na ASCII znaky.

- Slovníkový útok – pomocou súboru, v ktorom sú uložené možné WEP heslá
- Extrakcia kľúča pravdepodobnostnou metódou – s použitím metódy popísanej v kap. 5.8.2, avšak s použitím aj iných ako klasických slabých IV a útokom na prvý aj druhý bajt hesla. V tejto metóde sú už zaimplementované zložitejšie analýzy, ktoré potrebujú oveľa menej paketov. Na zlomenie 64-bitového kľúča je potrebných približne 100 000 paketov.

Operačné systémy: BSD, Linux, MacOS, Windows

6.2.6 WEP Attack

Autor: Dominik Blunk, Alain Girardet

Popis:
Nástroj na lámanie WEP hesla pomocou externého slovníka, z ktorého postupne testuje, či pre konkrétne WEP heslo je správny kontrolný súčet. Ak je kontrolný súčet v poriadku pre takmer všetky pakety, heslo je správne. Na spustenie nástroja stačí jediný odchytený paket, avšak pre zabezpečenie istoty správneho hesla je potrebných viacej paketov, na ktorých bude testovať kontrolný súčet.

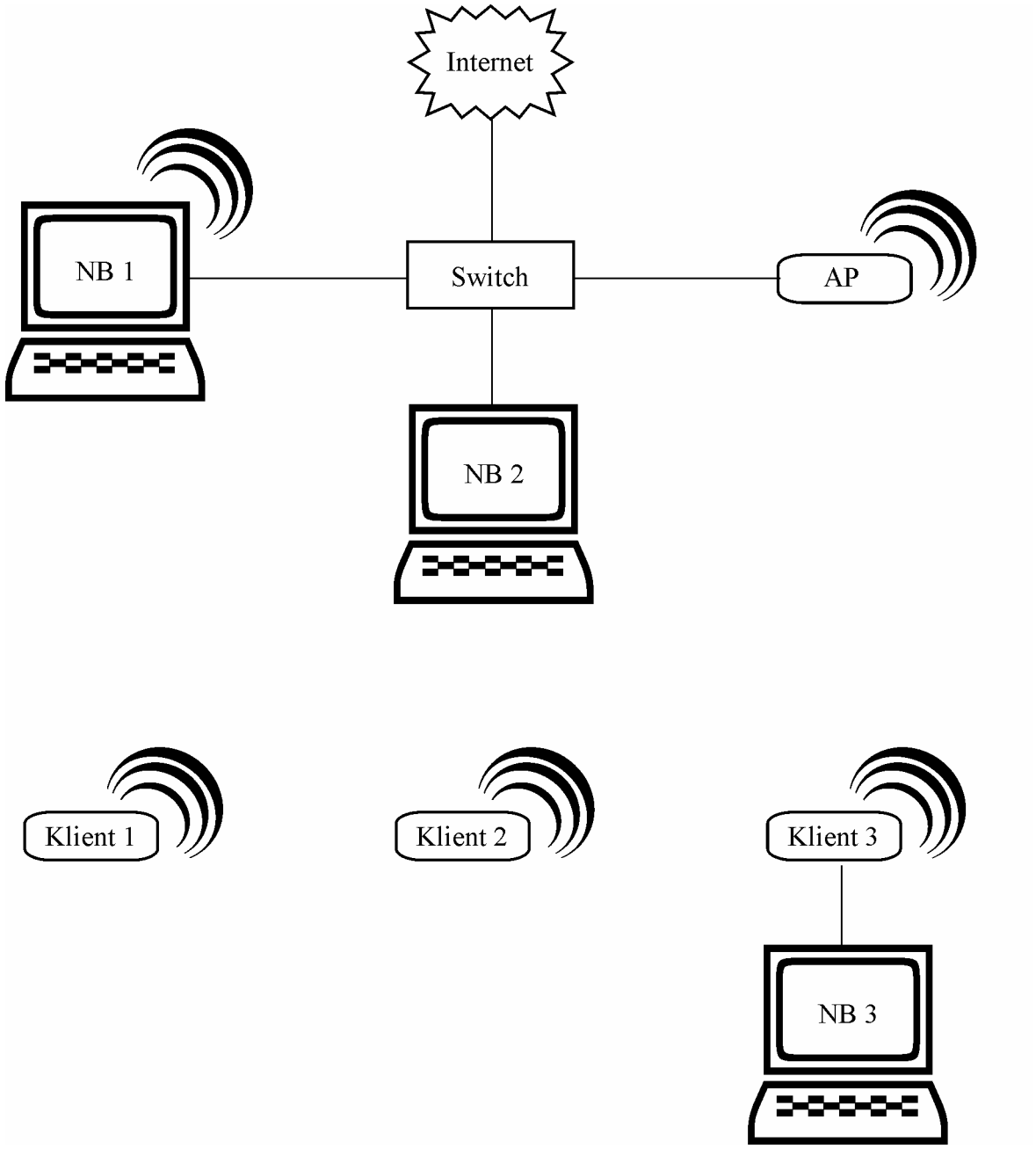
Operačné systémy: Linux

6.3 Nastavenia

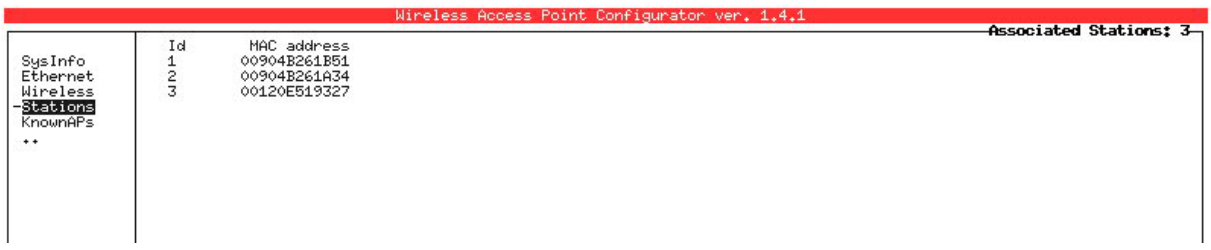
Rozmiestnenie zariadení z kap. 6.1 je zobrazené na Obr. 19. Klientské stanice boli počas experimentu prehadzované, takže na NB 3 bolo pripojené zariadenie WP-102 aj zariadenie WX-1590 podľa potreby. V prípade funkčného prepojenia AP s Klientom 3 mali všetky počítače prístup do siete Internet.

Konfigurácia AP bola realizovaná pomocou nástroja apconfig (Wireless Access Point Configurator) verzie 1.4.1 určeného pre tento typ zariadení. Nástroj umožňuje okrem bežných nastavení aj prezeranie zoznamu asociovaných staníc (viď. Obr. 20). Na AP boli tieto nastavenia:

- Režim Access Point
- SSID strecnianska-vychod2
- Prenosová rýchlosť 2 Mbps
- Topológia Infrastructure
- Vysielací kanál 1
- Zakázané vysielanie Beacon rámcov
- Autentifikácia povolená aj Open System aj Shared Key
- WEP heslo EF:CA:FF:EF:CA



Obr. 19 – Rozmiestnenie zariadení počas experimentov



Obr. 20 – Zoznam asociovaných staníc na AP

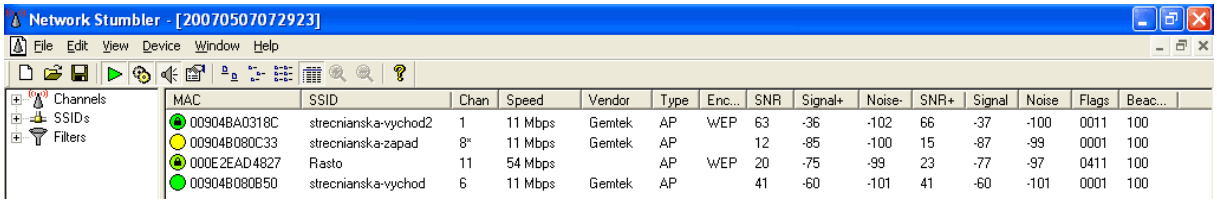
Na klientskej stanici boli takéto nastavenia:

- Access Point Client
- SSID strecnianska-vychod2
- Prenosová rýchlosť 2 Mbps
- Topológia Infrastructure
- WEP heslo EF:CA:FF:EF:CA (viď. Obr. 21 pre zariadenie D-com WP-102)
- Autentifikácia bola menená v priebehu experimentu

Obr. 21 – Nastavenie WEP hesla do zariadenia D-com WP-102

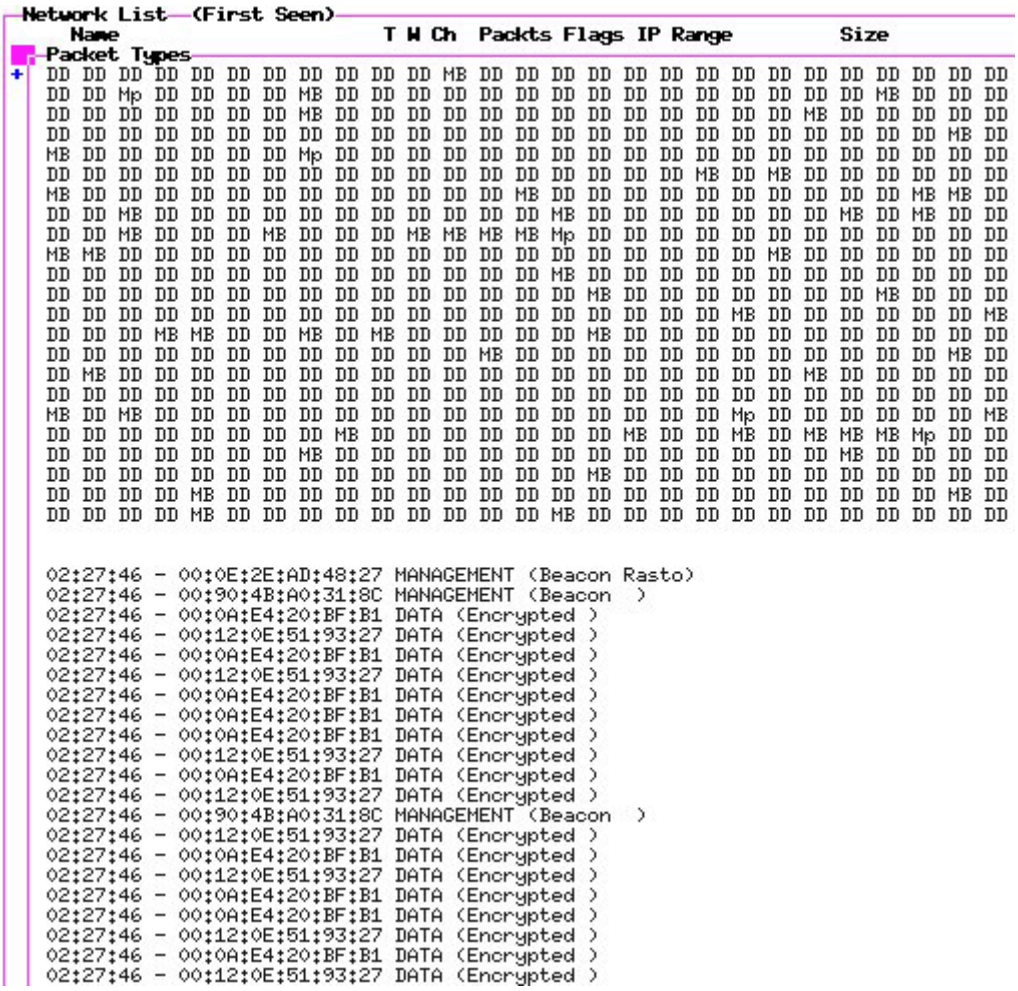
6.4 Pasívne útoky

Ako prvý som vyskúšala nástroj Netstumbler (Obr. 22) pod Windows. Úspešne našiel a zobrazil informácie o experimentálnom AP ešte v režime odosielania Beacon rámcov, ako aj o iných sieťach, ktoré zhodou okolností sú dostupné v mieste vykonávania experimentu. Keď boli Beacon rámce vypnuté, Netstumbler AP nenašiel.



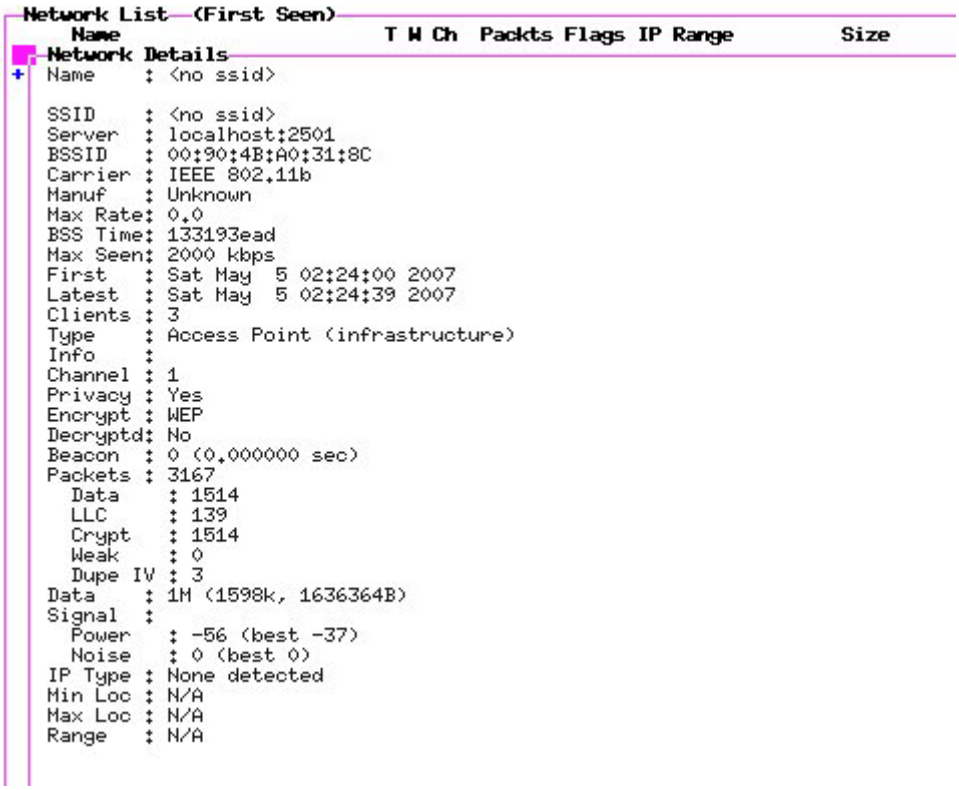
Obr. 22 – Netstumbler – výpis zoznamu dostupných AP

Druhým vyskúšaným nástrojom bol Kismet pod Linux. Okrem výpisu veľmi podobného Netstumbler-u poskytol informácie ako o zachytených paketoch počas skenovania dostupných sietí (Obr. 23), tak aj o sieti (Obr. 24).



Obr. 23 – Kismet - výpis zachytených paketov

Kismet už nepotreboval, aby boli zapnuté Beacon rámce na AP. Pozorný čitateľ si určite všimol prázdnu položku SSID vo výpise o sieti. Vo výpise zachytených paketov ma pomerne prekvapilo, že AP namiesto umlčania Beacon rámcov vysielalo Beacon rámce s prázdnym SSID (viď. Obr. 23), ktoré sú ľahko identifikovateľné pomocou MAC adresy AP 00:90:4B:A0:31:8C.



Obr. 24 – Kismet - výpis informácií o sieti

Posledným z pasívnych útokov bola analýza dát s nástrojom Ethereal, pomocou ktorého som skúmala (podobne ako s Kismet) výpis zachytených paketov v reálnom čase. Ethereal však ukazuje oveľa viac informácií k paketom ako Kismet a tak poslúžil na detailné preskúmanie komunikácie AP s klientmi.

6.5 Autentifikácia a Asociácia

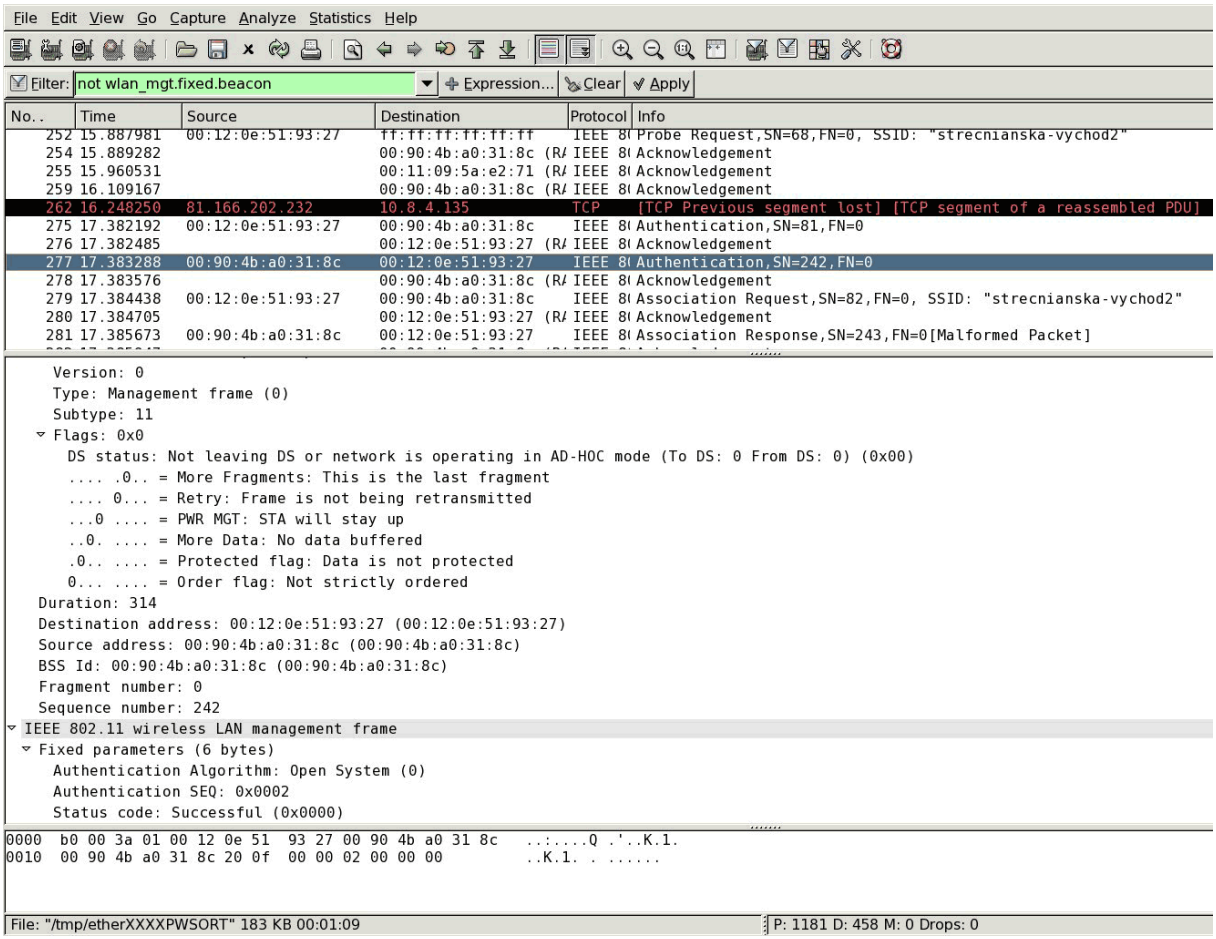
V prvom rade ma zaujímal spôsob autentifikácie klienta k AP. Stanice majú v nastaveniach na výber tieto možnosti autentifikácie:

- Open system
- Shared key
- Automatic

V základnom nastavení zariadení je autentifikácia Automatic. Vyskúšala som teda sledovať, ako bude prebiehať takáto autentifikácia a zistila som, že ľubovoľný klient sa snažil primárne autentifikovať cez Shared key autentifikáciu a až po neúspešnej výmene rámcov sa autentifikoval cez Open system. Neúspšená výmena rámcov prebiehala nasledujúco:

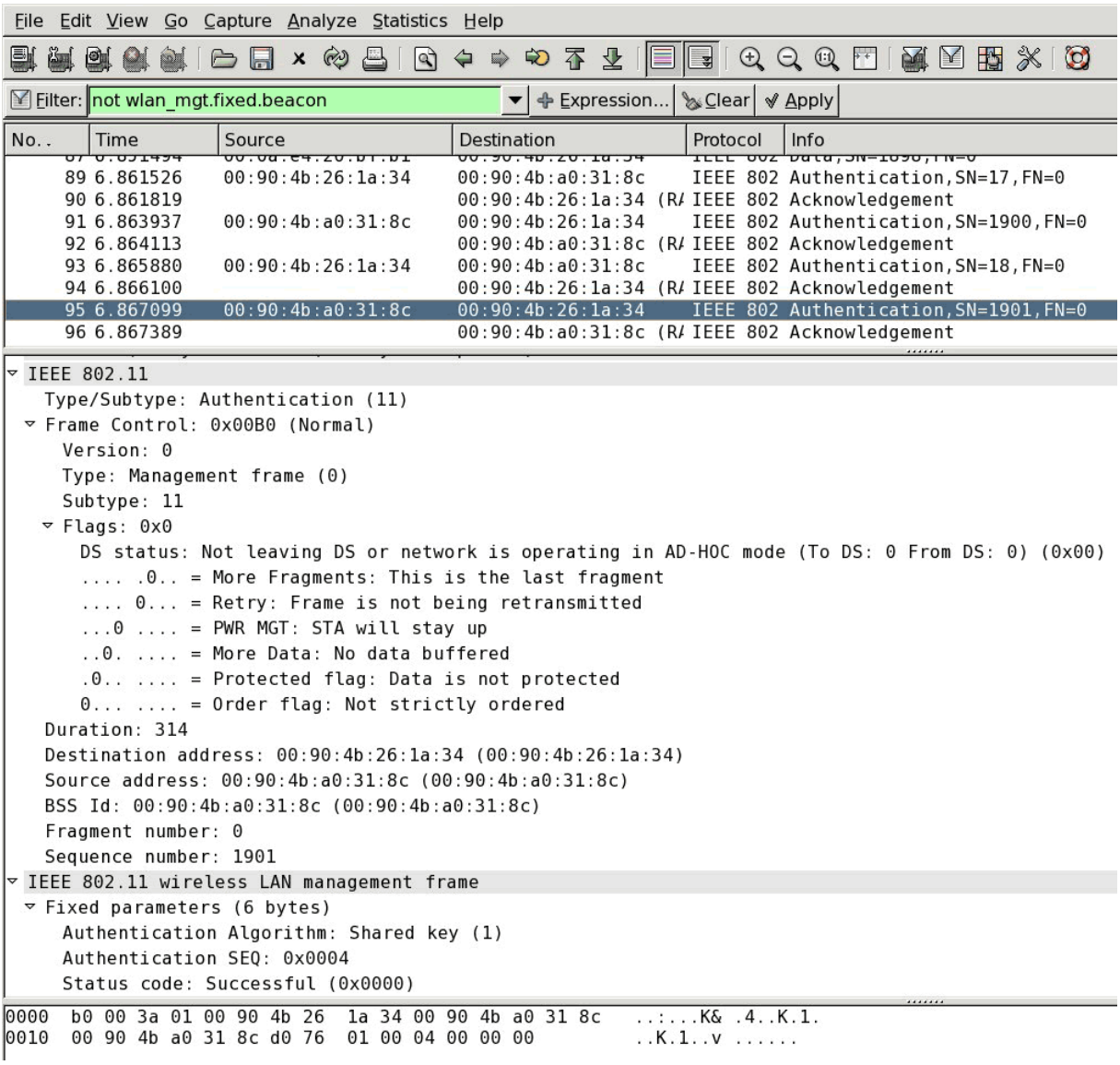
- Klient poslal AP Authentication request
- AP poslalo klientovi Authentication response s náhodným textom
- Klient odoslal AP Authentication rámec 3 so zašifrovaným náhodným textom
- AP odmietlo autentifikáciu

Dôvod odmietnutia bol jednoduchý – zadala som zlé WEP heslo do klienta a preto po autentifikácii pomocou Open system a následnej asociácii (viď. Obr. 25) nebolo aktívne ani pripojenie do Internetu na NB 3. Prekvapením pre mňa bolo, že klient nehlásil žiadnu chybu v pripojení, takže nie príliš skúsený používateľ nemal šancu zistiť, kde spravil chybu pri nastavovaní klienta.



Obr. 25 – Open System autentifikácia s následnou asociáciou

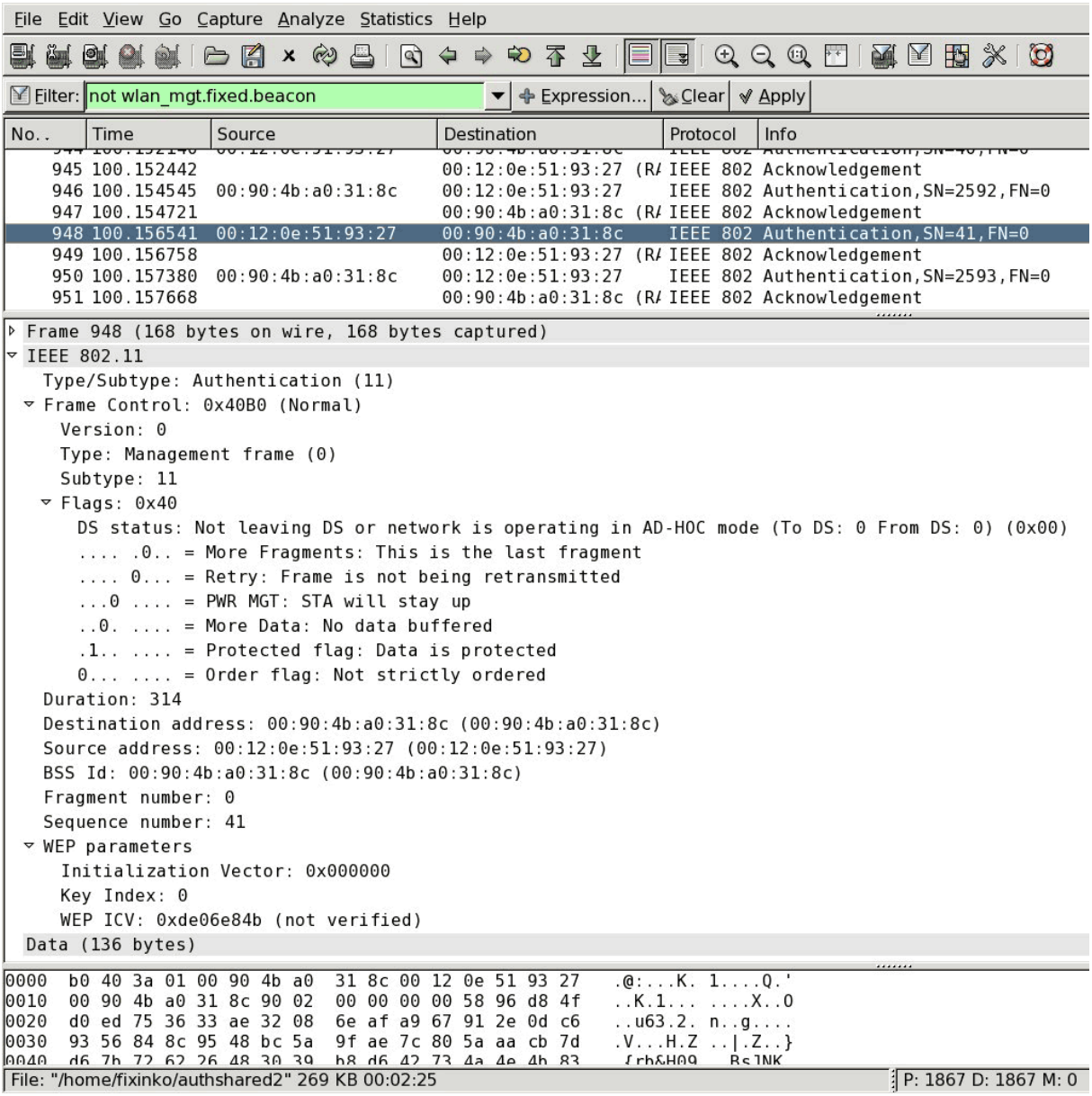
Ďalším experimentom bolo vyskúšanie kompletnej Shared Key autentifikácie. Na klientovi som nastavila správne WEP heslo a komunikácia prebehla podľa štandardu. Po správnom zašifrovaní náhodného textu bol z AP odoslaný paket potvrdzujúci autentifikáciu a nastala výmena asociačných rámcov (viď. Obr. 26).



Obr. 26 – Shared Key autentifikácia

V rámci tohto experimentu ma aj zaujímalo, aké IV zvolí klient na zašifrovanie náhodného textu. Všimla som si, že klient WX-1590 posielal náhodne generované IV, ale klient WP-102 posielal po každej autentifikácii IV = 0,0,0 (viď. Obr. 27).

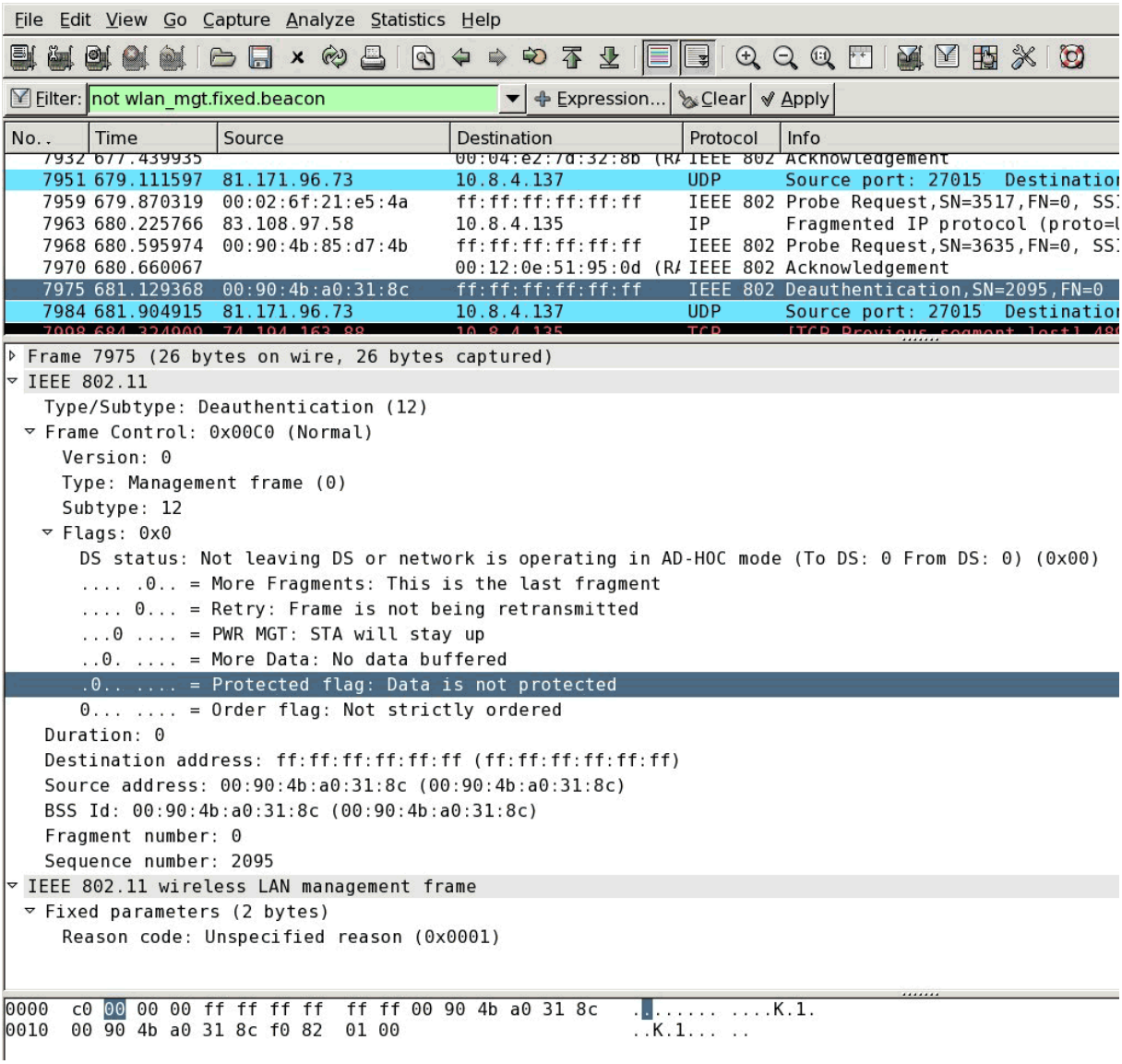
Posledný experiment bolo nastavenie rozdielnej kombinácie autentifikácií na AP a na klientovi. V takomto prípade vždy po prijatí Authentication request rámca odoslalo AP nazad Authentication response s odmietnutím autentifikácie a klient sa neustále snažil autentifikovať. Stav klienta v tomto prípade bol neustále Scanning.



Obr. 27 – Shared key autentifikácia s klientom WP-102

6.6 DoS útok

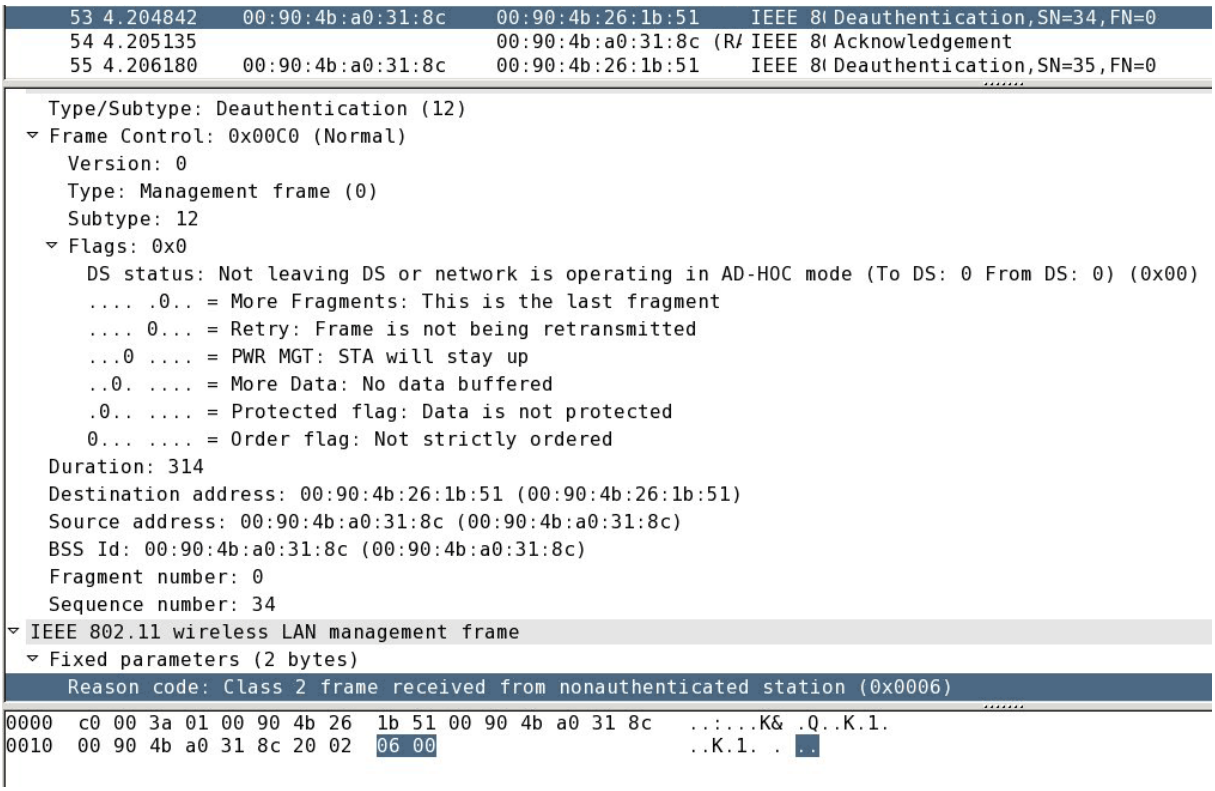
Jedným z experimentom bolo aj prevedenie DoS útoku. Konkrétne sa jednalo o deautentifikačný útok na všetkých klientov. Na Obr. 28 je deautentifikačný paket, ktorý pre všetkých klientov (broadcast) oznamuje ukončenie autentifikácie s AP. Po tomto kroku sa všetky stanice snažili znovu autentifikovať a následne asociovať, aby mohli ďalej využívať sieťové prostriedky.



Obr. 28 – Deautentifikácia broadcast pre všetkých klientov

Posledným z DoS útokov bola simulácia deautentifikačného útoku smerom na stanicu. Pokúsila som sa odoslať deautentifikačný rámec s SA jednej z klientských staníc smerovaný na AP. Po tomto pakete boli ešte stále na AP prijímané dáta, ktoré však AP odmietlo odoslaním deautentifikačného paketu s dôvodom prijatia nepovoleného rámca od neautentifikovanej stanice (viď. Obr. 29).

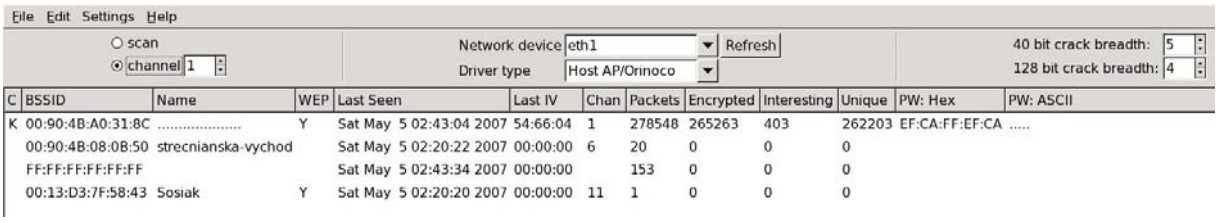
Prekvapilo ma, že AP odpovedalo na všetky prijaté dátové pakety, z čoho som presvedčená, že by sa dal spraviť útok na dostupnosť. Ak by som zahltila AP obrovským množstvom dátových paketov, zrejme by nestíhalo čítať hlavičky a odosielať deautentifikačné pakety na každý prijatý paket, čo by spôsobilo zvýšenú réžiu a používatelia by pocítili zníženú QoS, resp. úplné prerušenie dátovej komunikácie s AP. Tento útok sa už bohužiaľ zrealizovať nepodaril z časových dôvodov.



Obr. 29 – Deautentifikačný paket s dôvodom nepovoleného rámca

6.7 Lámanie WEP hesla

Poslednými experimentmi boli útoky na WEP. Na tieto účely som použila nástroj AirSnort, ktorým som nielen zachytávala pakety, ale zároveň v reálnom čase lámala WEP heslo. Pri WEP hesle EF:CA:FF:EF:CA potreboval AirSnort nastavený na 3. úrovni 877 zaujímavých paketov, ktoré obdržal z celkového množstva cca 540 000 paketov. Na 5. úrovni potreboval už len 403 zaujímavých paketov z celkového množstva cca 280 000 paketov (viď. Obr. 30). Verím tomu, že zvýšenie úrovne (na úkor presnosti lámania hesla) pomohlo k rýchlejšiemu, ale stále správnemu zlomeniu WEP hesla z pomerne malého počtu paketov.



Obr. 30 – AirSnort po zlomení WEP hesla EF:CA:FF:EF:CA

Ďalším skúšaným nástrojom bol WepLab na ten istý počet paketov ako AirSnort v prvom pokuse (nakoľko som pakety z AirSnort po zlomení WEP hesla uložila do súboru a tento súbor následne načítala ako vstup do WepLab). Zistila som, že na rozdiel od AirSnort zachytil WepLab pomocou pravdepodobnostnej metódy až 282 000 zaujímavých paketov z celkového

počtu cca 570 000 paketov a úspešne našiel WEP heslo (viď. Obr. 31). Hneď na to som úspešne zlomila heslo aj s pomocou druhého súboru z AirSnort s celkovým počtom cca 280 000 paketov. Skúsila som aj metódu brute-force, avšak v priebehu 24 hodín sa nepodarilo zlomiť heslo, čo spôsobilo môj nezáujem o ďalšiu prevádzku tejto metódy na denne používanom notebooku.

```
asterix[pts/5]:/usr/src/weplab-0.1.5>./weplab -k 64 -r /home/fixinko/kismet/log-5-4.pcap
weplab - Wep Key Cracker Wep Key Cracker (v0.1.5).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>

Not BSSID specified.
 Detected one packet with BSSID: [00:90:4B:A0:31:8C]

Total valid packets read: 286011
Total packets read: 572092

 282573 Weak packets gathered:
Statistical cracking started! Please hit enter to get statistics.
It seems that the first control data packet verifies the key! Let's test it with others....


Key: ef:ca:ff:ef:ca
Right KEY found!!
Key cracked in 2 seconds
```

Obr. 31 – WepLab po zlomení WEP hesla EF:CA:FF:EF:CA

6.7.1 Zmena hesla

Po týchto pokusoch som sa pokúsila zmeniť WEP heslo na číselné, a to konkrétne 82601. Výsledky boli zaujímavé. AirSnort na úrovni 3 obdržal 334 zaujímavých paketov z celkového množstva cca 285 000 paketov a podarilo sa mu na tomto množstve úspešne zlomiť WEP heslo (viď. Obr.32).

File Edit Settings Help

scan / channel 1 — Network device eth1 — Refresh — Driver type Host AP/Orinoco — 40 bit crack breadth: 3 — 128 bit crack breadth: 6

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
K	00:90:4B:A0:31:8C	.....	Y	Sat May 5 15:39:47 2007	92:33:03	1	285755	265403	334	262200	38:32:36:30:31	82601
	00:0E:2E:AD:48:27	Rasto	Y	Sat May 5 15:04:58 2007	00:00:00	11	2	0	0	0		
	00:13:D3:7F:58:43	Sosiak	Y	Sat May 5 15:04:58 2007	00:00:00	11	1	0	0	0		
	00:90:4B:08:0B:50	strecnianska-vychod		Sat May 5 15:37:05 2007	00:00:00	6	73	0	0	0		
	00:90:4B:08:0C:33	strecnianska-zapad		Sat May 5 15:05:00 2007	00:00:00	8	3	0	0	0		
	FF:FF:FF:FF:FF:FF			Sat May 5 15:39:27 2007	00:00:00		497	0	0	0		
	00:90:4B:A0:0A:C8			Sat May 5 15:34:15 2007	00:00:00		2	0	0	0		

Obr. 32 – AirSnort po zlomení WEP hesla 82601

WepLab bol taktiež úspešný na rovnakom počte paketov pomocou pravdepodobnostnej metódy.

Ako ďalší nástroj som na to isté číselné heslo 82601 použila WEP Attack - slovníkový útok. Na veľmi malom počte paketov sa mu podarilo objaviť správne heslo v úžasnom čase 1,6 sekundy (viď. Obr. 33). Čas bol, ako som postupne skúšala, vždy rovnako malý bez ohľadu na množstvo paketov (začínajúc od rozumnej hodnoty okolo 100 až po milióny kusov paketov).

Obr. 33 – WEP Attack po zlomení hesla 82601

Posledným zo skúšaných nástrojov na zlomenie WEP hesla bol WEPCrack. Avšak pri všetkých mojich pokusoch bol výsledok nesprávny (viď. Obr. 34) alebo žiadny. Zrejme potreboval podstatne väčší počet zachytených paketov, než ostatné nástroje. Počas skúšania 285 000 paketov boli iba prvé 2 bajty hesla správne. V ostatných bajtoch hesla sa už bohužiaľ mýlil.

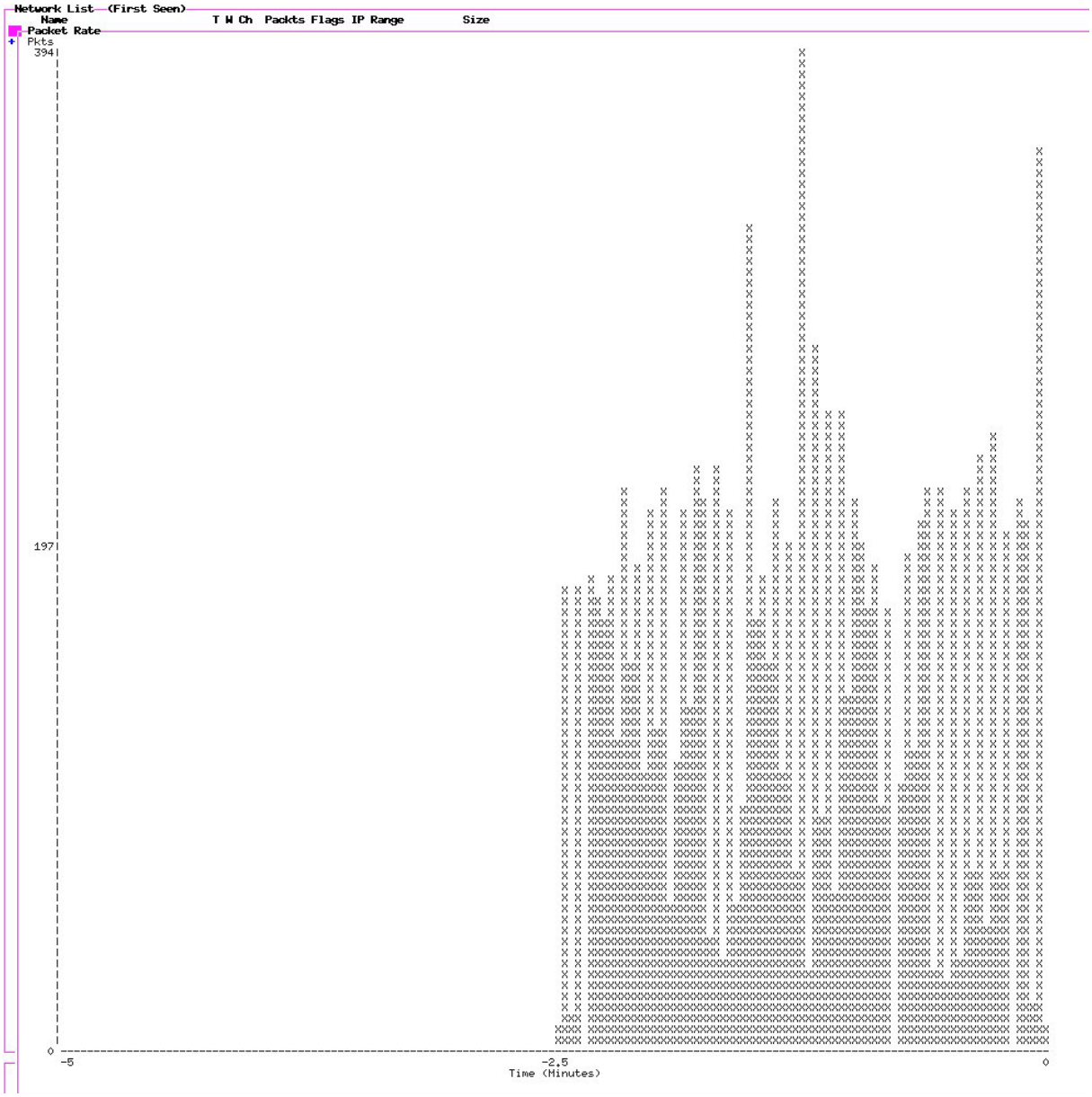
Obr. 34 – WEPCrack po neúspešnom hádaní WEP hesla

6.8 Zhrnutie

Počas experimentov sa mi podarilo zoznámiť sa s rôznymi nástrojmi, z ktorých som len niektoré (obvykle najobľúbenejšie alebo najznámejšie) použila na predvedenie kompatibility implementácií so štandardom IEEE 802.11.

Snažila som sa názornými ukážkami uviesť čitateľa do problematiky bezpečnosti bezdrôtovej siete. Ukážky boli smerované práve na jednoduchosť zdolania bezpečnosti rôznymi spôsobmi – od pasívneho odchytávania dát po aktívne DoS útoky.

Počas experimentov som prišla aj na to, že WEP redukuje maximálnu prenosovú rýchlosť pri plnej záťaži z 2 Mbps na približne 1,5 Mbps alebo aj menej. Dôkazom je graf z Kismet (viď. Obr. 35), ktorý ukazuje zhustený počet paketov za sekundu okolo polovičnej prenosovej rýchlosti (cca 120 paketov za sekundu je pri max. veľkosti paketu 1500 B prenosová rýchlosť 1400 Kbps). Tento pokles je relatívne malý, avšak používatelia ho môžu pociťovať na znížení QoS. Samozrejme, pokles záleží od vybraného bezdrôtového zariadenia, záťaže siete a počtu aktívnych používateľov.



Obr. 34 – Graf prenosovej rýchlosti počas WEP šifrovania z Kismet

Nasleduje tabuľka s údajmi o experimentoch na lámanie WEP hesla.

WEP heslo	Celkový počet paketov	Nástroj	Počet zaujímavých paketov	Úspešnosť	Poznámka
EF:CA:FF:EF:CA	40 000	AirSnort	64	Nie	Úroveň 3
EF:CA:FF:EF:CA	280 000	AirSnort	403	Áno	Úroveň 5
EF:CA:FF:EF:CA	280 000	WepLab	140 000	Áno	Pravdepod.
EF:CA:FF:EF:CA	540 000	AirSnort	877	Áno	Úroveň 3
EF:CA:FF:EF:CA	570 000	AirSnort	917	Áno	Úroveň 3
EF:CA:FF:EF:CA	570 000	WepLab	282 000	Áno	Pravdepod.
EF:CA:FF:EF:CA	570 000	WepLab		Nedokončil	Hrubou silou

EF:CA:FF:EF:CA	40 – 570 tis.	WEPCrack		Nie	
EF:CA:FF:EF:CA	ľubovoľný	WEP Attack		Nie	
82601	540 000	AirSnort	877	Nie	Úroveň 3
82601	540 000	WepLab	262 000	Áno	Pravdepod.
82601	540 000	Wep Attack		Áno	1,6 sek.
82601	540 000	WEPCrack		82xxx zle	21 sek.
82601	250 000	AirSnort	290	Nie	Úroveň 3
82601	250 000	WepLab	121 000	Nie	Pravdepod.
82601	250 000	Wep Attack		Áno	1,6 sek.
82601	250 000	WEPCrack		Nie	
82601	285 000	AirSnort	334	Áno	Úroveň 3
82601	285 000	WepLab	147 000	Áno	Pravdepod.
82601	285 000	Wep Attack		Áno	1,6 sek.
82601	285 000	WEPCrack		Nie	

Tab. 4 – Výsledky lámania WEP hesla

Z vykonaných pokusov lámania WEP hesla som bola najspokojnejšia s nástrojom WepLab, ktorý poskytuje v porovnaní s ostatnými najlepšie výsledky. WepLab (aspoň podľa mojich experimentov) potreboval najmenší počet paketov na správne uhádnutie hesla vynímajúc slovníkový útok s pomocou WEP Attack. Páčilo sa mi aj, že WepLab dokáže previesť až 3 rôzne spôsoby útokov a jeho kód je písaný naozaj prehľadne.

Slovníkový útok WEP Attack je použiteľný len na pomerne jednoduché slovné alebo číselné heslá, ale s jeho rýchlosťou sa ho oplatí ešte pred ostatnými nástrojmi aspoň na malom počte odchytených paketov vyskúšať. Páčilo sa mi, že slovník sa dá editovať a dajú sa do neho dopĺňať slová, avšak v abecednom poradí, nakoľko jeho rýchlosť a korektnosť závisí od utriedenosti slovníkového súboru.

AirSnort by som považovala za druhý najlepší nástroj na lámanie WEP hesla po WepLab. Páčilo sa mi jeho príjemné grafické prostredie, jednoduché použitie a automatické lámanie WEP hesla v reálnom čase bez nutnosti spúšťania ďalšieho procesu. Navyše od WepLab má možnosť zachytené dáta uložiť do súboru čitateľného pre množstvo ďalších nástrojov.

Najviac ma sklamal nástroj WEPCrack. Vedela som, že bol jedným z prvých voľne šíriteľných nástrojov na lámanie WEP hesla, ale odradilo ma zbieranie niekoľkých miliónov paketov na vyskúšanie jeho funkčnosti. Autori mohli pouvažovať nad rozšírením tohto nástroja o nové techniky a umožniť (podobne ako WepLab) porovnanie viacerých spôsobov lámania WEP hesla.

Nástroje ako Kismet, NetStumbler a MiniStumbler som používala už dávnejšie a sú pre mňa nevyhnutnou základnou výbavou operačných systémov Slackware Linux, Windows alebo Windows CE.

Záver

Pri zrode WEP sa predpokladalo, že bude dostatočným zabezpečením proti útočníkom, avšak ako sa bezdrôtový prenos stával značne rozšíreným, skupina vedcov [29] odhalila chybu v samotnom algoritme WEP protokolu, čo spôsobilo prakticky okamžite nárast nástrojov na jeho oslabenie.

Pôvodným úmyslom mal byť bezdrôtový prenos ekvivalentný bezpečnosti káblového prenosu. Dizajnéri protokolu akceptovali fakt, že existujú potenciálne trhliny v protokole, ale mysleli si, že spravili útoky aspoň tak ťažkými ako fyzicky sa dostať do káblovej siete. Vyšlo najavo, že ich závery boli chybné a útočníci napísali množstvo nástrojov a postupov na oslabenie WEP protokolu dostupné pre širokú verejnosť.

Vo všeobecnosti je obtiažne korektne implementovať silnú šifru. Aj v prípade, že predajca implementuje šifru, ktorá je známa ako veľmi silná, často implementácia môže oslabiť šifru alebo zneefektívniť ju. Omyl pri implementácii môže byť jednoduchý, ako napríklad nezabezpečené ukladanie šifrovacieho kľúča, slabý generátor náhodných čísiel, alebo chyba v generovaní šifrovacích kľúčov. Všetky tieto funkcie môžu jednoducho oslabiť šifru alebo odhaliť kľúč.

RC4 je bezpečný algoritmus a mal by aj ostať niekoľko ďalších rokov bezpečným. Avšak v tomto špecifickom prípade keď sa jedná o bezdrôtovú implementáciu algoritmu do WEP s použitím iniciačného vektora je nedostatočný.

Chybou v implementácii WEP je príliš malý IV vektor, neurčený spôsob obmeny IV, veľké množstvo známych častí prenášaných správ v komunikácii prostredníctvom IP protokolu, žiadny systém distribúcie a obmeny kľúčov (čo ústí do problému zdieľaného kľúča pre všetkých používateľov), veľmi slabá ochrana integrity paketov, neprítomnosť ochrany opätovného vysielania informácie a chybný autentifikačný systém.

Cieľom tejto práce bolo poskytnúť analýzu techník zabezpečenia, alebo oslabenia bezpečnosti štandardu IEEE 802.11. Zároveň bolo mojim cieľom poskytnúť široký prehľad a kategorizáciu nástrojov týkajúcich sa vybranej problematiky.

Spomínané ciele sa mi podarilo v práci dosiahnuť. Navyše som pridala do práce experimentálnu časť, ktorou som chcela ukázať funkčnosť najpoužívanejších nástrojov a zároveň prakticky overiť komunikáciu medzi bezdrôtovými zariadeniami pracujúcimi v rozoberanom štandarde.

Práca je určená hlavne pre sieťových administrátorov, pretože znalosťou útokov dokáže dobrý administrátor lepšie naplánovať a vyvinúť bezpečnosť pre konkrétny účel použitia bezdrôtovej siete.

Príloha – Nástroje

Nasleduje rozsiahly zoznam nástrojov, ktoré som zhodnotila za užitočné v oblasti bezpečnosti bezdrôtových sietí štandardu IEEE 802.11 a jeho ďalších verzií. Táto príloha v abecednom poradí slúži na vyhľadania vhodného nástroja podľa krátkeho popisu a operačného systému.

Aerosol

Autor: Sniph
Popis: Nástroj na sledovanie bezdrôtových sietí písaný v jazyku C.
Operačné systémy: Windows

Airbase

Autor: Johnny Cache
Popis: Zbierka viacerých nástrojov na lámanie WEP hesla. Je postavený na báze AirCrack.
Operačné systémy: UNIX

AirCrack

Autor: AirCrack Team
Popis: Zbierka viacerých nástrojov na sledovanie bezdrôtových sietí a lámanie WEP hesla metódou z kap. 5.8.2. Dokáže odchytávať, analyzovať pakety a robiť aj injektáž paketov.
Operačné systémy: Linux, MacOS, Windows

Airfart

Autor: Dave Smith
Popis: Nástroj na sledovanie siete, identifikovanie bezdrôtových zariadení a zobrazovanie sily signálu. Je písaný v jazyku C/C++.
Operačné systémy: Linux, UNIX

AirJack

Autor: Abaddon
Popis: Balíček AirJack obsahuje nástroj zvaný essid_jack, ktorý implementuje deautentifikačný útok na objavenie sietí, ktoré nevysielajú svoje SSID. Deasociáciou klienta útočník dosiahne, že klient pošle sondovací paket s SSID. Variantou k AirJack je wlan_jack, alebo fata_jack – tento pošle nekorektné požiadavky o autentifikáciu zahltením legitímnych klientov a spôsobí tým, že AP deasociuje reálneho klienta.
Operačné systémy: Linux

AirMagnet

Autor: AirMagnet Inc.
Popis: Komerčná sada nástrojov na plánovanie zabezpečenia, analýzu a celkovú obranu bezdrôtovej siete s veľmi pekným grafickým rozhraním.
Operačné systémy: Windows

AiroPeek NX

Popis: AiroPeek NX je komerčný produkt na podrobnú analýzu paketov v reálnom čase. Obsahuje tiež filtre, nástroje na detekciu útokov a i. funkcie.

Operačné systémy: Windows

Airsnarf

Autor: The Shmoo Group

Popis: Airsnarf je nástroj na nastavenie maskovaného AP a na demonštráciu, ako maskované AP môže kradnúť prihlasovacie heslá z verejných hotspotov. Presmeruváva DNS a HTTP komunikáciu z AP.

Operačné systémy: Linux

AirSnort

Autor: The Shmoo Group

Popis: Nástroj na lámanie WEP hesla na princípe slabých IV z kap. 5.8.2. AirSnort je schopný pasívneho sledovania prevádzky v sieti, ukladania paketov a ich analýzy v reálnom čase. Airsnort síce nebol jedným z prvých nástrojov na lámanie WEP, ale aspoň boli do neho zakomponované neskoršie zistené metódy postupného odhaľovania WEP hesla, čím spravili z tohto nástroja jeden z najefektívnejších. AirSnort je veľmi obľúbeným nástrojom aj z dôvodu jeho jednoduchosti použitia. Je to kompletný nástroj, ktorý vie bezdrôtovú kartu prepnúť na odchytávanie a má kvalitne spracované prostredie. Dokáže odhaliť 104-bitové heslo s použitím cca 1,5 mil. zašifrovaných paketov.

Operačné systémy: Linux, Windows

AirTraf

Autor: Elixar

Popis: Nástroj na sledovanie a zachytávanie bezdrôtovej komunikácie.

Operačné systémy: Linux

AP Hopper

Autor: Matthew Davidson, Jeffrey Strube

Popis: Nástroj na identifikovanie dostupných bezdrôtových sietí, preskenuje pásmo, pokúsi sa pripojiť na všetky dostupné bezdrôtové siete a získať v nich IP adresu.

Operačné systémy: Linux, BSD, UNIX

AP Hunter

Autor: Jim Carter

Popis: Nástroj na vyhľadávanie sietí a pripájanie sa k nim.

Operačné systémy: Ľubovoľný s podporou Perl

APSniff

Autor: Frederic Bret-Mounet

Popis: Nástroj na zachytávanie Beacon rámcov a zobrazovanie dostupných sietí.

Operačné systémy: Windows

APTools

Autor: Kirby Kuehl

Popis: Nástroj na vyhľadávanie AP na káblovej sieti.

Operačné systémy: Windows, UNIX

BSD-AirTools

Autor: Dachb0den Labs

Popis: Nástroj na kompletný audit bezdrôtových sietí. Bsd-airtools balíček obsahuje niekoľko nástrojov. Dstumbler je komponent na sledovanie sietí s podobným rozhraním ako NetworkStumbler aj s podporou GPS. Dwepdump odchytáva pakety a dwepcrack používa dumpy na zlomenie WEP hesla.

Operačné systémy: FreeBSD

Chopchop

Autor: KoreK

Popis: Nástroj na zlomenie WEP hesla na základe IP/ARP komunikácie s AP.

Operačné systémy: rôzne

ClassicStubler

Autor: alksoft

Popis: Nástroj na sledovanie bezdrôtových sietí podobný NetStumbleru.

Operačné systémy: MacOS

DMZS-Carte

Autor: DMZ Services, Inc.

Popis: Nástroj na nanášanie výsledkov vyhľadávania sietí z NetStumbler-u do mapového podkladu zo satelitu.

Operačné systémy: Ľubovoľný s podporou Perl

Driftnet

Autor: Chris Lightfoot

Popis: Nástroj na odchytávanie a zbieranie komunikácie v bezdrôtovej sieti – vyberá a ukladá obrázky a audio záznamy z komunikácie.

Operačné systémy: Linux, UNIX

Ethereal (viď. Wireshark)

Ettercap

Autor: Alberto Ornaghi, Marco Valleri

Popis: Nástroj slúžiaci na sledovanie sieťovej komunikácie cez maskované AP a jej následnú analýzu. Dokáže spraviť rozbor pre množstvo protokolov (aj šifrovaných).

Operačné systémy: Linux, BSD, MAC OS, Windows, Solaris

FakeAP

Autor: Stuart Stock & Ken Beames, Black Alchemy Labs

Popis: Nástroj na vytvorenie veľkého množstva klamlivých AP, slúži na zamaskovanie a zmätenie tých reálne používaných pred očami prípadného útočníka.

Operačné systémy: Linux, BSD

Hotspotter

Autor: Max Moser, Joshua Wright

Popis: Nástroj slúžiaci na kompromitáciu počítačov so systémom Windows XP pripojených cez bezdrôtové siete. Počítače s týmto operačným systémom

vysielajú Probe request rámce na všetky uložené (niekedy navštívené) AP. Hotspotter odpovedá na tieto rámce a robí maskované AP.

Operačné systémy: Linux, UNIX

iStumbler

Autor: Alf Watt

Popis: Nástroj na sledovanie bezdrôtových sietí, obdoba Netstumbler-a pre MacOS.

Operačné systémy: MacOS

KisMAC

Autor: Michael Rossberg

Popis: Nástroj na sledovanie bezdrôtových sietí, obdoba Netstumbler-a pre MacOS pracujúci pasívne (bez Probe request rámcov), tak aby nebol vystopovateľný. Nástroj je určený pre skúsenejších používateľov.

Operačné systémy: MacOS

Kismet

Autor: Mike Kershaw

Popis: Nástroj na identifikáciu a sledovanie bezdrôtových sietí. Kismet je voľne šíriteľný nástroj s bohatou funkcionalitou. V porovnaní s Netstumbler-om je bohatší o zachytávanie paketov, kreslenie grafu počtu paketov v priebehu času, analýzu siete , ukladanie paketov do súborov pre iné nástroje, grafické znázornenie zachytených sietí a i.

Operačné systémy: Linux, BSD, MacOS, Windows (Cygwin)

LibRadiate

Autor: Packetfactory

Popis: Nástroj na zachytávanie, injektáž a odosielanie modifikovaných paketov.

Operačné systémy: Linux

LORCON: Loss Of Radio CONnectivity

Autor: Joshua Wright, dragorn

Popis: LORCON (Loss of Radio Connectivity) je nástroj na zachytávanie, injektáž a odosielanie modifikovaných paketov.

Operačné systémy: Linux, UNIX

MacStumbler

Autor: Korben

Popis: Nástroj slúžiaci na zobrazovanie informácii o dostupných bezdrôtových sieťach podobne ako NetStumbler.

Operačné systémy: MacOS

MiniStumbler

Autor: Marius Milner

Popis: Netstumbler pre vreckový počítač.

Operačné systémy: Windows CE

Mognet

Autor: Sean Whalen

Popis: Nástroj na sledovanie komunikácie v bezdrôtových sieťach napísaný v Java. Zobrazuje zachytené pakety v reálnom čase aj v ich hexadecimálnej alebo ASCII podobe.

Operačné systémy. Ľubovoľný s podporou Java

Musatcha Advanced WiFi Mapping Engine

Autor: Brad Isbell

Popis: Nástroj slúžiaci na zobrazovanie a ukladanie informácií o dostupných bezdrôtových sieťach podobne ako Kismet, pracujúci so zariadeniami Linksys WAP54G a WRT54G.

Operačné systémy: Windows

NetChaser

Autor: Michael A. Waldron

Popis: Nástroj na vyhľadávanie hotspotov pre vreckové počítače s Palm OS.

Operačné systémy: PalmOS

NetStumbler

Autor: Marius Milner

Popis: Nástroj na zobrazovanie informácií o dostupných bezdrôtových sieťach. Netstumbler je jedným z prvých voľne šíriteľných sledovacích nástrojov. Zobrazuje rôzne informácie o bezdrôtových sieťach, ako napr. silu signálu, ESS ID, vysielací kanál, spôsob šifrovania, druh podporovaného štandardu a i. Má podporu GPS, takže sa siete dajú ľahko lokalizovať pomocou ďalších nástrojov do máp.

Operačné systémy: Windows

Omerta

Autor: Mike Schiffman

Popis: Nástroj na deasociáciu a deautentifikáciu klientov. Tento nástroj počúva pakety a zasiela ku každému z nich deautentifikačné pakety.

Operačné systémy: UNIX

Packetyzer

Autor: Network Chemistry

Popis: Ovládač na vytvorenie sieťového rozhrania slúžiaceho na zachytávanie komunikácie v sieťach a ich následnú analýzu z nástroja Ethereal.

Operačné systémy: Windows

PocketWarrior

Autor: DataWorm Labs

Popis: Nástroj na vyhľadávanie bezdrôtových sietí pre vreckový počítač.

Operačné systémy: Windows CE

PrismStumbler

Autor: Jan Fernquist

Popis: Nástroj na pasívne sledovanie a zachytávanie Beacon rámcov v bezdrôtovej sieti.

Operačné systémy: Linux, BSD

SMAC

Autor: KLC Consulting
Popis: Nástroj na zmenu MAC adries sieťových rozhraní pod Windows.
Operačné systémy: Windows

Sorwep

Autor: Andrea Bittau
Popis: Nástroj na zlomenie WEP hesla
Operačné systémy: UNIX

SSIDsniff

Autor: Kostas Evangelinos
Popis: Nástroj na sledovanie, ukladanie a analýzu sieťovej komunikácie v bezdrôtových sieťach.
Operačné systémy: Linux

StreetStumbler

Autor: kg4ixs
Popis: Nástroj na vykreslenie výsledkov meraní z NetStumbler-a na mapové podklady.
Operačné systémy: Windows

StumbVerter

Autor: Michael Puchol, Sonar Security
Popis: Nástroj na vykreslenie výsledkov meraní z NetStumbler-a na mapové podklady.
Operačné systémy: Windows

Tcpdump

Popis: Nástroj na odchytávanie paketov. Obsahuje filtre, ale funguje len v textovom režime. Verzia pre Windows má názov WinDUMP.
Operačné systémy: UNIX

Void11

Autor: Reyk Floeter
Popis: Nástroj na vykonávanie autentifikačných a deautentifikačných útokov na klientov bezdrôtovej siete. Obsahuje deautentifikačný útok opísaný v kap. 5.5.3 a útok na zahltenie AP autentifikačnými paketmi opísaný v kap. 5.5.2.
Operačné systémy: Linux

Wavelan Tools

Autor: Cyrus Durgin
Popis: Nástroj na vyhľadávanie bezdrôtových sietí a služieb.
Operačné systémy: Linux, BSD

WaveMon

Autor: Jan Morgenstern
Popis: Nástroj na sledovanie vlastností pripojenia k bezdrôtovej sieti (sily signálu, šumu, štatistiky prenesených dát a chýb pri prenose).

Operačné systémy: Linux

WaveStumbler

Autor: Patrik

Popis: Nástroj na vyhľadávanie bezdrôtových sietí ako NetStumbler pre Linux.

Operačné systémy: Linux

WebStumbler

Autor: Frank Echanique

Popis: Nástroj na prevod výstupov z NetStumbler-a do html súborov.

Operačné systémy: Windows

WellenReiter

Autor: Michael Lauer

Popis: Nástroj na vyhľadávanie, sledovanie a audit bezdrôtových sietí. Má podporu GPS a je viacej graficky orientovaný ako Kismet. Má možnosť uloženia stavu, ale nie zachytených paketov.

Operačné systémy: UNIX, BSD s podporou Perl

WepAttack

Autor: Dominik Blunk, Alain Girardet

Popis: Nástroj na lámanie WEP hesla pomocou externého slovníka, z ktorého postupne testuje, či pre konkrétne WEP heslo je správny kontrolný súčet. Ak je kontrolný súčet v poriadku pre takmer všetky pakety, heslo je správne. Na spustenie nástroja stačí jediný odchytený paket, avšak pre zabezpečenie istoty správneho hesla je potrebných viacej paketov, na ktorých bude testovať kontrolný súčet.

Operačné systémy: Linux

WEPCrack

Autor: Anton Rager, Paul Danckaert

Popis: Nástroj na lámanie WEP hesla. WEPCrack bol prvým verejne uvoľneným spomedzi nástrojov na zlomenie WEP hesla po zverejnení [29] trhlín v implementácii RC4 algoritmu v roku 2001. Tým, že bol vyvíjaný ako jeden z prvých nástrojov, nie je najrýchlejší a potrebuje veľké množstvo paketov. WEPCrack je kolekciou viacerých nástrojov – Prism-getIV.pl, WEPCrack.pl a WeakIVGen.pl.

Operačné systémy: UNIX, BSD s podporou Perl

WepLab

Autor: José Ignacio Sánchez Martín

Popis: Weplab implementuje niekoľko pasívnych útokov na WEP (útok hrubou silou, slovníkový útok aj útok na extrakciu kľúča pravdepodobnostnou metódou). Je schválne písaný bez optimalizácie kódu pre edukačné účely, aby čitateľ kódu pochopil jeho princíp. Ale aj napriek neoptimálnemu kódu patrí medzi najefektívnejšie nástroje na zlomenie WEP hesla.

Operačné systémy: BSD, UNIX, MacOS, Windows

WEPWedgie

Autor: Anton Rager

Popis: Nástroj na odchytávanie prúdových kľúčov a následnú injektáž paketov do bezdrôtovej siete. WEPWedgie obsahuje aj firewall logiku, skenovanie portov a i.

Operačné systémy´: Linux, UNIX

WEP_Tools

Autor: Tim Newsham

Popis: Balíček dvoch nástrojov. Wep_crack slúži na lámanie WEP hesla zo súboru zachytených paketov a druhý nástroj Wep_decrypt slúži na dešifrovanie súboru paketov s pomocou známeho WEP hesla. Nástroje sa dajú použiť nezávisle. Wep_crack láme heslo slovníkovým útokom, pričom kontroluje kontrolný súčet. Ak je kontrolný súčet v poriadku pre takmer všetky pakety, našiel správne heslo.

Operačné systémy: Linux, UNIX

Wi-Find

Autor: Eric Olinger

Popis: Nástroj na vyhľadávanie bezdrôtových sietí a zobrazonie relevantných informácií ako NetStumbler písaný v jazyku C.

Operačné systémy: Linux

Wicrawl

Autor: Aaron Peterson, Jason Spence, Peter Kacherginsky, Brian Johnson

Popis: Nástroj na selektívne vyhľadávanie AP podľa zaujímavých paketov umožňujúci pomocou ďalších nadstavieb získavať a zaznamenávať rôzne informácie o sieti a zariadeniach v nej zapojených.

Operačné systémy: Linux

WiFiFoFum

Autor: Malcolm Hall

Popis: Nástroj na vyhľadávanie bezdrôtových sietí s GPS pre vreckové počítače

Operačné systémy: PocketPC 2003

WifiScanner

Autor: Jérôme Poggi

Popis: Nástroj na vyhľadávanie bezdrôtových zariadení (AP aj klientov). Má zabudovaný detekčný systém na zistenie potenciálneho útoku.

Operačné systémy: Linux

Wifitap

Autor: Cédric Blancher

Popis: Nástroj umožňujúci presmerovať komunikáciu bezdrôtových klientov cez svoje maskované AP a IP komunikáciu následne ukladať alebo modifikovať pri prenose.

Operačné systémy: Linux, UNIX

WinDump

Autor: Loris Degioanni

Popis: Nástroj na zachytávanie a analýzu komunikácie na sieti, obdoba tcpdump.

Operačné systémy: Windows

Wireshark (Ethereal)

Autor: Gerald Combs

Popis: Nástroj na zachytávanie, analýzu a prehliadanie prenášaných dát v sieti. Ethereal je jeden z najpopulárnejších voľne šíriteľných nástrojov na analýzu paketov. Dôvodom je, že podporuje množstvo operačných systémov, dokáže analyzovať pakety zo súborov, ktoré vytvorili iné odpočúvacie nástroje (Tcpdump, NetXray a i.), dokáže pakety aj ukladať do súborov pre neskoršiu analýzu inými nástrojmi, filtrovať pakety, rekonštruovať hlavičky viac ako 260 rôznych protokolov a zachytávať pakety na rôznych médiách (ethernet, PPP, token ring, X-25, a i.).

Operačné systémy: UNIX, BSD, Windows, AIX, MAC OS, Solaris a i.

WiStumbler

Autor: Isao Seki

Popis: Nástroj na vyhľadávanie bezdrôtových sietí na princípe Netstumbler pre NetBSD.

Operačné systémy: NetBSD

Wscan

Autor: Portland State University

Popis: Nástroj na vyhľadávanie bezdrôtových sietí a grafické zobrazovanie sily signálu.

Operačné systémy: Linux, FreeBSD

Zoznam bibliografických odkazov

[1] A. Klein: *Attacks on the RC4 stream cipher*, Designes, Codes and Cryptography, 2007, http://cage.ugent.be/~klein/RC4/RC4-en.ps

[2] A. Stubblefield, J. Ioannidis, A. Rubin: *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, Proc. Symposium on Network and Distributed System Security, San Diego, California, 2001

[3] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: *Handbook of applied cryptography*, CRC Press, 1996 ISBN 0-8493-8523-7

[4] Andrea Bittau, Mark Handley, Joshua Lackey: *The Final Nail in WEP's Coffin,* http://tapir.cs.ucl.ac.uk/bittau-wep.pdf

[5] ArcFour algoritmus, http://www.mozilla.org/projects/security/pki/nss/draft-kaukonen-cipher-arcfour-03.txt

[6] Bezpečnosť 802.11, súvisiace články a materiály, http://www.drizzle.com/~aboba/IEEE/

[7] Brian Carter, Russell Shumway: *Wireless Security End to End*, Wiley Publishing, Inc., 2002 ISBN 0-7645-4886-7

[8] Cyrus Peikari, Seth Fogie: *Maximum Wireless Security*, Sams, 2002 ISBN 0-672-32488-1

[9] Články o zdolaní WEP, http://smallnetbuilder.com

[10] Články o zdolaní WEP, http://www.securityfocus.com

[11] Doc. RNDr. Peter Mederly, CSc.: *Introduction to Computer Networks*, FMFI UK, Bratislava, 1997

[12] Erik Tews, Ralf-Philipp Weinmann, Andrei Pyshkin: *Breaking 104 bit WEP in less than 60 seconds*, Technische Universität Darmstadt, http://eprint.iacr.org/2007/120.pdf

[13] Frank Ohrtman, Konrad Roeder: *Wi-Fi Handbook: Building 802.11b Wireless Networks*, McGraw-Hill, 2003 ISBN 0-07-141251-4

[14] IEEE 802.11Working Group, http://grouper.ieee.org/groups/802/11/index.html

[15] J. Bellardo, S.Savage: *802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions*, Proceedings od the USENIX Security Symposium, Washington, D.C., 2003, http://www.cs.ucsd.edu/users/savage/papers/UsenixSec03.pdf

[16] J. Postel, J. K. Reynolds: *Standard for the transmission of IP datagrams over IEEE 802 networks,* RFC 1042, IETF, 1988, http://www.rfc-archive.org/getrfc.php?rfc=1042

[17] J. Walker: *Overview of 802.11 security*, 2001, http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3-Overview-of-802-11-Security.ppt

[18] J. Walker: *Unsafe at any key size: an analysis of the WEP encapsulation*, Tech. Rep. 03628E, IEEE 802.11 committee, 2000, http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

[19] K. Sankar, S. Sundaralingam, A. Balinsky, D. Miller: *Cisco Wireless LAN Security, Expert guidance for securing your 802.11 networks*, Cisco Press, 2005 ISBN 1-58705-154-0

[20] LAN MAN Standards Committee of the IEEE Computer Society: *Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE Standard 802.11,* 1999 ISBN 0-7381-1810-9

[21] Matthew Gast: *802.11 Wireless Networks: The Definitive Guide,* O'Reilly, 2002 ISBN 0-596-00183-5

[22] Merritt Maxim, David Pollino: *Wireless Security*, McGraw-Hill/Osborne, 2002 ISBN 0-07-222286-7

[23] N. Borisov, I. Goldberg, and D. Wagner: *Intercepting Mobile Communications: The Insecurity of 802.11*, 2001, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[24] Nástroje, http://www.wardrive.net/wardriving/tools/

[25] Netstumbler, http://netstumbler.com

[26] R. K. Nichols, P. C. Lekkas: *Wireless Security: Models, Threats, and Solutions*, McGraw-Hill, 2002 ISBN 0-07-138038-8

[27] Rámce IEEE 802.11, http://www.wi-fiplanet.com/tutorials/article.php/1447501

[28] Robert E. Mahan: *Security in Wireless Networks*, SANS Institute, 2001

[29] Scott Fluhrer, Itsik Mantin, Adi Shamir: *Weaknesses in the Key Scheduling Algorithm of RC4*, http://www.crypto.com/papers/others/rc4_ksaproc.pdf

[30] Štandardy IEEE, http://standards.ieee.org/

[31] Tim Newsham: *Cracking WEP Keys Applying known techniques to WEP Keys*, 2001, http://www.lava.net/~newsham/wlan/WEP_password_cracker.pdf

[32] Úvod do IEEE 802.11, http://www.informit.com/articles/article.asp?p=24411&seqNum=1&rl=1

[33] Úvod do IEEE 802.11, http://www.intelligraphics.com/articles/80211_article.html

[34] Wi-Fi Alliance, http://www.wifialliance.com , http://www.wi-fi.org

[35] Wikipedia, http://www.wikipedia.org/

[36] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan: *Your 802.11 Wireless Network has No Clothes*, 2001, http://www.drizzle.com/%7Eaboba/IEEE/wireless.pdf

[37] Zbierka materiálov k bezdrôtovým sieťam, http://www.raulsiles.com/resources/wifi.html