WiFi sítě a jejich slabiny

Vložil/a cm3l1k1 [1], 17 Březen, 2005 - 18:36

- Hacking [2]
- Networks & Protocols [3]
- Security [4]
- WiFi & Wireless [5]

V tomto článku bych se chtěl zaměřit na podrobný popis WiFi sítí a jejich slabých míst, díky kterým lze již dnes za krátkou dobu uhodnout šifrovací klíč. Vysvětlíme si základní pojmy, historii, specifikaci a nedostatky v používaných protokolech, šifrách a kontrolních součtech.

Každý člověk, který někdy slyšel o WiFi sítích také ví, že to (i v dnešní době) s jejich zabezpečením není nijak slavné. Stále dokola se proto mluví o jejich napadnutelnosti za použití programů AirSnort, aircrack, weplab apod. V médiích se ale nemluví o konkretních problémech, či nedostatcích a proto se chci zaměřit hlavně na tuto problematiku. Mě osobně nezajímá, že airsnort dokáže cracknout heslo po odposlechnutí 100-1000MB dat. Mě zajímá, jakým způsobem on a jemu podobné programy fungují a jakých zranitelností využívají.

Prvopočátky

V roce 1997 byla vydána původní verze standardu 802.11 ("legacy"), která byla taktéž označována jako 802.1y. Tento standard specifikoval přenos dat elektromagnetickým vlněním v bezlicenčním pásmu 2,4-2,4835 GHz, nebo v infračerveném pásmu a to rychlostí 1Mb/s a 2Mb/s. Kvůli masovému rozšíření IrDA se však od infračerveného přenosu upustilo.

U WiFi (Wireless Fidelity) se používa přístupová metoda **CSMA/CA (Carrier Sense Multiple Access /with Collision Avoidance)**. Kolize lze v bezdrátových sítích težko detekovat a proto se nepoužívá CSMA/CD. I když je pásmo v okolí stanice volné, neznamená to, že je volné i v okolí příjemce, kterým je většinou Access Point (AP - přístupový bod). Na AP totiž mohla vyslat požadavek jiná stanice, která není v dosahu první. Proto vysílací stanice nejdříve pošle paket RTS (Request To Send) ve kterém je kromě zdroje uvedena i doba trvání přenosu. Pokud následně přijme **CTS (Clear To Send)** paket, tak zahájí přenos. Okolní stanice, které jsou v dosahu a slyší pakety RST a CTS tím pádem vědí jak dlouho bude médium obsazené a nepokoušejí se vysílat. Jak již všem logicky došlo tak komunikace probíhá half-duplexem. Přenos je vlastně ekvivalentní počítači připojenému do HUBu a s tím souvisí i bezpečnostní rizika.

802.11a

- Tento standard jako jediný pracuje v kmitočtovém pásmu 5 GHz. V EU konkrétně od 5,47 do 5,725 GHz. Teoretická přenosová rychlost je 54 Mb/s. U nás se tento standard moc nepoužívá, protože jeho dosah je menší než u 802.11b a u nás se smí používat pouze v budovách.

802.11b

- Přenos probíhá v pásmu 2,4 až 2,4835 GHz (rozsah 83,5 MHz). Šířka pásma je v ČR rozdělena na 13 kanálů. Aby se signál jednotlivých kanálů nerušil, je nutné nastavit je tak, aby pracovaly minimálně 5 kanálů od sebe (např. 1, 6, 11). Teoretická přenosová rychlost je 11 Mb/s. Tento standard spolu s 802.11g se u nás neuvěřitelně rychle rozšířil a ve vetších městech je již problém s umístěním vlastního AP, aby jste nerušily některé z okolních sítí. Denně vzrůstá počet přístupových bodů. Bohužel drtivá vetšina z nich není dostatečně zabezpečena, či vůbec nepoužívá šifrování.

802.11g

- pracuje ve stejné šířce pásma jako 802.11b a je s ním zpětně komatibilní. Rychlost přenosu je 54Mb/s, ale pokud se k AP, který používá 802.11g, připojí počítač s kartou 802.11b, tak se rychlost přenosu sníží opět na 11Mb/s.

Data se v bezdrátových sítích vysílají všesměrově a tak není težké je odposlechnout. Pokud se tedy najdou tací, kteří šifrování vypnou, lze jednoduše odposlechnout hesla k emailům, ftp serverům, IM účtům apod. a navíc při pasivním odposlechu je téměř nemožné vás odhalit. Přístup na Internet přes WiFi hotspoty je jeden z nejanonymnějších.
Pro zabezpečení bezdrátových sítí normalizační instituce IEEE 802.11 navrhla šifrování v podobě protokolu **WEP (Wired Equivalent Privacy)**, což v překladu znamená "bezpečnost odpovídající drátu". Prioritou lidí z IEEE nejspíše bylo, aby bylo šifrování nenáročné na HW a tak nešťastně použily slabou šifru spolu se slabým 40 bitovým klíčem, který byl v době vzniku daný zákonnými podmínkami o vývozu šifer mimo USA. Asi ani nepočítali s tak obrovským rozšířením WiFi sítí. Níže si popíšeme jaké má WEP fatální nedostatky.

WEP

Zajišťuje šifrování rámců na 2. síťové vrstvě. Šifruje tedy veškeré rámce (blok binárních dat), které vedou od klienta k AP a ne pouze určité služby. Pokud je však AP připojen do Internetu, tak mezi AP a internetovým serverem šifrování neprobíhá. Právě použitá šifra je u WEPu největší problém.
K šifrovaní se používá algoritmus **RC4**, jehož autorem je R. Rivest a zveřejněn byl v roce 1994. Algoritmus používá proudovou symetrickou šifru s délkou klíče 40, 104 a 232 bitů. Již v roce 2001 však bylo v algoritmu objeveno hned několik bezpečnostních nedostatků. Se symetrickým šifrováním je problém v tom, že někde musí mít klient uložený statický klíč, kterým šifruje a zároveň dešifruje komunikaci. Lepší výrobci chrání přístup ke klíči ve speciální paměti síťové karty (NVRAM), ke které lze přistupovat jen pod heslem. Bohužel tímto způsobem to zdaleka nedělají všichni a najdou se i případy, kdy je klíč uložen v registrech a to v otevřené podobě.

Proudová šifra generuje pseudonáhodný stream o stejné délce jakou má zpráva, tzn. délka klíče se podle potřeby nafukuje. Generátor pseudonáhodných čísel, který podle pravidel rozšíří délku klíče se nazývá **PRNG**. Šifrování probíhá jednoduchou operací XOR mezi zprávou a klíčovým streamem a dešifrování probíhá reverzně. WEP bohužel nijak neřeší distribuci klíče a tak je musíme ve většině případů manuálně zapsat do konfigurace zařízení. Tím trochu odpadá podstata šifrování. Útočník sice zatím klíč nezná, ale oprávněný uživatel ano a tak pro něj není složité komunikaci dešifrovat a protože 70% útoků je vedeno zevnitř sítě, tak tento fakt považuji za velký bezpečnostní nedostatek. Ani oprávněný uživatel by o podobě klíče neměl vůbec vědět!

Odesílatel i příjemce musí mít stejný klíč používaný k šifrování/dešifrování komunikace. Pro vyšší bezpečnost je nutné klíč průběžně obměňovat. To ale WEP ani RC4 nijak neřeší a tak jediný možný způsob změny klíče je opětovné nahrazení stávajícího v konfiguraci adaptéru. U distribuce klíčů je problém, protože případný útočník může nový klíč při předání získat. Proto to v dnešních sítích chráněných WEPem vypadá tak, že se jeden rok používá stejný klíč. Přičemž v lepších případech by se měl klíč měnit po několika minutách.
Proč tedy právě tato šifra? Jednoduše proto, že ji lze snadno implementovat do hardwaru bezdrátových adaptérů a díky tomu nemá aktivování šifrování téměř žádný vliv na výkon počítače.

Zašifrování stejné zprávy symetrickou šifrou totiž pokaždé generuje stejnou šifrovanou zprávu a tím pádem je mnohem jednoduší klíč uhodnout. Proto je součástí WEP ještě **inicializační vektor** (IV), který se mění s každým paketem a doplňuje klíč o dalších 24 bitů. Při použití WEPu s klíčem dlouhým 128 bitů má klíč pouze 104 bitů + 24 bitů IV. Generování IV zajišťuje vysílací strana, která ho nejenom použije k sestavení šifrovaného streamu, ale přidá ho v otevřené podobě i do záhlaví rámce. Tím by se mohlo zdát, že se pokaždé použije "jiný klíč" a šifra je tím bezpečnější, ale není tomu tak. Unikátních IV je pouze 224 a pokud se tedy odešle 224 paketů, začne se IV opakovat. Inicializačním vektorem se tedy nic nevyřeší a šifra je stále napadnutelná řadou útoků. Navíc

prodloužení klíče má k délce jeho luštění lineární závislost => pro 2x delší klíč je potřeba pouze 2x více času k dešifrování.
Integritu šifrované zprávy zajišťuje známá funkce **CRC-32 (Cyclic Redundancy Check)**, jejíž hodnota je společně s daty zašifrovaná v těle zprávy. Bohužel však díky lineárnosti funkce CRC32 ji lze obelstít určitou formou záměny bitů, které nedokáže odhalit.

WPA není záchranou

WPA (WiFi Protected Access) je novější bezpečnostní mechanizmus a původně měl opravit chyby, kterých se WiFi Aliance dopustila u WEPu. Sice nešťastně používá stejný šifrovací algoritmus RC4, kvůli jednoduchému upgradu firmwaru stávajících zařízení, ale určite sebou přináší řadu vylepšení. Standardně používá 128 bitový dynamický klíč, který se mění každých 10 000 paketů. Dalším zlepšením je MIC (Message Integrity Check), jež je používán současně s CRC32 a tím řeší jeho nedostatky, díky kterým bylo možné změnit zprávu při zachování stejného kontrolního součtu. Zabezpečením WiFi sítí se budu zabývat v jiném článku. Raději nyní přejdu dál a v popisu metod útoků uvedu i jednu zranitelnost WPA ve spojení s PSK.

První bezpečnostní otřesy

Programátoři Scott Fluhrer, Itsik Mantin a Adi Shamir publikovali zprávu „Weakness in the Key Scheduling Algorithm of RC4“ (slabina v algoritmu plánování klíčů RC4), která popisuje metodu (FMS) umožňující prolomit řídící WEP klíč. Prvním programem, který dokázal pasivním odposloucháváním komunikace derivovat šifrovací klíč byl AirSnort. **AirSnort** byl uveřejněn o víkendu 17. srpna 2001 i se zdrojovými kódy a tehdy poprvé se začalo o slabé bezpečnosti WiFi sítí mluvit v širším měřítku. Autoři programu (Jeremy Bruestle a Blake Hegerle) uvádějí, že jim sestavení programu trvalo zhruba 24 hodin. AirSnort využíval metodu FMS (Fluhrer-Mantin-Shamir) podle jmen autorů, jejíž podmínkou bylo odposlechnutí obrovského množství paketů. Dalším problémem bylo, že klíč lze cracknout jen za pomocí "slabých" paketů s unikátním inicializačním vektorem (IV). Podle mých (ne)přesných počtů je to +- 1 paket z 500. Takže v prvopočátcích byl AirSnort po velkém úsílí účinný. Dnes již však existují mnohem efektivnější a promyšlenější metody derivace klíče.

AirSnort se v dnešní době moc nepoužívá a na řadu nastupují nástroje nové generace, kterými jsou např. aircrack a WepLab. Tuto "novou éru" odstartoval dne 8. srpna 2004 hacker jménem KoreK se svojí novou metodou statistické kryptoanalýzy, která se zhmotnila v nástroji **chopper**. Tato metoda změnila celou podstatu útoku FMS a již nebylo zapotřebí slabých paketů. Základní složkou útoku je zachycení velkého množství paketů se stejným inicializačním vektorem. Útok je často možný po odposlechnutí řádově statisíců paketů. Tato metoda byla samozřejmě poupravena a portována do programů aircrack a WepLab. Pokud chcete shlédnout výsledky úspěšnosti některých programů, tak vás odkážu na článek, který vyšel na portálu SecurityFocus pod názvem "WEP: Dead Again, Part 1". Teď konečně přejdeme k jednotlivým scenářům útoku, kde se budu snažit uvést jak slabiny protokolů samotných, tak i modely špatné konfigurace přístupového bodu (AP).

Podvržení MAC adresy

Pokud není AP úplně nezabezpečený, tak filtrování MAC adres je taková první "překážka", kterou lze obejít během několika sekund. Teď nebudeme uvažovat o šifrovaném AP, ale o takovém, který pouze podle MAC adres povoluje přístup a tím rádoby řeší autentizaci. My jednoduše odposlechneme jednu z používaných adres a přiřadíme ji své wifi kartě. Pod Windows lze MAC adresu změnit programem SMAC nebo windowsáckým /etc -> registry. Spusťte "regedit" a vyhledejte tento klíč: HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/Class/4936E972-xxxx-xxxx, kde jsou další podklíče síťových adaptérů ve tvaru 0001, 0002 atd. Vyhledejte adapatér vaší síťové karty a vytvořte novou řetězcovou hodnotu REG_SZ s názvem "networkaddress". Pokud chceme například MAC adresu 11-22-33-44-55-66, tak zapíšeme hodnotu 112233445566.

Pod Linuxem jednoduše za použití nástroje ifconfig:

```
ifconfig eth0 down
```

```
ifconfig eth0 hw ether 00:00:00:00:00:00
ifconfig eth0 up
```

Za předpokladu, že eth0 je rozhraní wifi karty a 00-00-00-00-00-00 je nová MAC adresa. Pokud však budete chtít využít tento způsob, tak musíte zajistit, aby počítač s vámi podvrženou adresou nevysílal. Buď si počkáte až ho majitel odpojí, nebo počítač DoSnete (útok odepření služby) a tím nebude dočasně přijímat regulerní pakety. Až budeme chtít přistupovat např. na Internet, tak se nemusíme bát, že pakety dorazí i na druhý stroj, který o ně nežádal, protože reakce systému by mohly být nepředvýdatelné.

Shared Key Authentication

Jedná se o autentizační mechanismus, kterým se ověřuje klient při připojení k AP. Pokud se chce klient připojit, tak mu AP odešle náhodně vygenerovaný text (challenge string). Klient ho zašifruje svým klíčem a odešle zpět. AP text zašifruje taky a pokud se shoduje s tím, co dostal od klienta, tak mu je povolen přístup. Tato metoda otevírá malá bezpečnostní dvířka, protože dokážeme odposlechnout vygenerovaný text a poté jeho zašifrovanou podobu. Derivovat klíč, pokud známe původní a šifrovanou podobu zprávy, je totiž mnohem snazší. Takže je paradoxně bezpečnější využití standardního mechanismu ověřování klienta přístupovým bodem (Open Key Authentication), při kterém se žádné autentizační údaje nepředávají. Autentizace je jednoduše zajištěna tím, že AP i klient mají stejný šifrovací klíč. Jinak by nesouhlasil ICV (Integrity Check Value) a AP by provoz blokoval.

Induktivní derivace klíče

U symetrické kryptografie má odesílatel i příjemce stejný klíč. U bezdrátových sítí s WEP šifrováním se ještě přidává 24 bitů inicializačního vektoru (IV). Pokud zašifrujeme klíčem určitá data, tak budou mít určitou podobu. Díky IV můžou mít stejná data 224 podob, než se IV začne opakovat. Potřebovali bychom stejná data poslat hned několikrát, zašifrovaný tvar odposlechnout a derivovat klíč. Když to samé uděláme s použitím dalších 223 různých IV, budeme moct dešifrovat veškerou komunikaci. Teď je problém, jak zasílat stejná data, když nemáme do bezdrátové sítě přístup? Pokud budeme mít štěstí, budou klientským stanicím přidělovány veřejné IP adresy. Potom už můžeme z jiného počítače připojeného k Internetu posílat na počítače v bezdrátové síti nějaká (nám známá) data, odposlechnout jejich zašifrovanou podobu a pokusit se derivovat klíč.

Derivace klíče díky CRC32

Jak jsem již několikrát uvedl, tak u WEPu se používá kontrolní součet CRC32. Nyní si popíšeme jednoduchý příklad, jak toho využít. O nedostatcích CRC32 se ví již dlouho. Záměnou určitých bitů zůstane kontrolní součet stejný. Takže pokud bity zaměníme a odešleme, paket projde přes kontrolu integrity a předá se do vyšší vrstvy. Tam paket způsobí chybu, protože data nebudou dávat smysl a odešle se zpět ICMP zpráva s chybovým hlášením. Její podobu můžeme odhadnout a tím odvodit i šifrovací klíč pro daný IV.

Zranitelnost EAP-MD5 a LEAP

EAP-MD5 a LEAP jsou metody šifrované autentizace v sítích standardu 802.1X. Větší zranitelnost je u EAP-MD5, protože nemá podporu dynamicky generovaných WEP klíčů pro každou relaci. Obě metody trpí náchylností ke slovníkovým útokům, pokud uživatel nepoužije dostatečně kvalitní heslo. **LEAP** (narozdíl od **PEAP (Protected Extensible Authentication Protocol)**) nevytváří šifrovaný tunel mezi klientem a autentizačním serverem. Z toho vyplívá, že LEAP přenáší autentizační informace v nezašifrovaném formátu. Technologie LEAP dále v kombinaci s autentizací dle MAC adres na jednom RADIUS serveru, je dírou do systému. Stačí totiž použít MAC adresu místo přihlašovacích údajů a přístup je povolen. (podrobnosti tohoto útoku bohůžel neznám a sám jsem ho nikdy nevyzkoušel)

WPA v kombinaci s PSK

Autentizace sdíleným klíčem **PSK (Pre-Shared Key)** je alternativa ke správě klíčů v rámci 802.1X. PSK je 256 bitové číslo nebo heslo (fráze) o délce 8 až 63 Bytů. Právě pokud je PSK generováno na základě fráze a má míň jak 20 znaků, tak je PSK náchylné ke slovníkovým útokům, které mohou mít vyšší úspěšnost než u obyčejného WEPu.
Každá stanice může mít vlastní PSK v závislosti na MAC adrese. Většina výrobků ale používá jeden PSK pro celou ESS. **ESS (Extended Service Set)** je velká síť, která vznikne spojením menších (třeba kancelářních) BSS sítí. Dále tu máme **PMK (Pairwise Master Key)**, který řídí 4-Way Handshake při požadavku o připojení. PMK je taktéž 256 bitové číslo, které lze vypočítat z PSK a to vzorcem:
PMK = PBKDF2(heslo, ssid, delka_ssid, 4096, 256)

PBKDF2 je metoda z PKCS #5 v2.0 (Password-based Cryptography Standard) a znamená to, že spojení řetezce hesla, SSID a hodnoty délky SSID je 4096-krát hashováno a z toho je vygenerována 256 bitová hodnota PMK.
Teď se dostáváme k jádru věci. Máme PSK a PMK pro řízení 4-Way Handshake a teď na řadu nastupuje PTK (Pairwise Transient Key), které je generováno z prvních dvou paketů 4-Waye za pomocí funkce HMAC-MD5, náhodným číslem (nonces) a použitou šifrou. PTK je jedinečné pro každé spojení a PMK řídí celou jeho klíčovou hierarchii. Jak si lze odvodit, pokud tedy známe PSK, tak můžeme, po odposlechnutí důležitých paketů handshaku, dešifrovat spojení mezi klientem a přístupovým bodem. Zároveň, pokud je PSK stejné pro celou ESS, tak je možné kompromitovat celou síť. Tato zranitelnost byla poprvé popsána v dokumentu "Weakness in Passphrase Choice in WPA Interface" od Roberta Moskowitze.

Podvržení přístupového bodu

Jestliže používáte GNU/Linux, tak jste určitě slyšeli o ovladači **HostAP**. Tento ovladač dokáže z obyčejné síťové karty, založené na čipové sadě Prism, udělat přístupový bod (AP). Představme si situaci, kdy se klient přihlašuje do sítě přes šifrované stránky uložené na AP. Nakonfigurujeme na našem počítači HostAP, okopírujeme design a formu stránek na kterých se uživatelé autentizují, spustíme Apache a ke kartě připojíme silnou anténu. Anténa vysílající na stejném kanále a se stejným SSID, jako pravý AP, musí mít vyšší zisk a tím se uživatel, místo na pravé AP, připojí k nám. Otevře se mu stránka, kam zadá login a heslo, které si uložíme do databáze a je hotovo. Máme login a heslo a můžem se přihlásit jako běžný uživatel.
Další možností je nabídnout uživateli přesně to co chce. Tím myslím překrýt signálem pravé AP, nechat klienta se připojit a povolit mu jen port 80 pro surfování na internetu. Některým čtenářům jistě dochází co mám na mysli. Povolili jsme port 80, ale ne port 443, který se používá k zabezpečenému přístupu na webové stránky pomocí SSL (Secure Socket Layer). Takže uživatel si bude číst emaily, nakupovat kreditní kartou v eshopu atp. a my v roli prostředníka mezitím můžeme odposlechnout veškeré soukromé informace.

Známé útoky

WiFi síť si lze představit jako počítač připojený kabelem do HUBu. S tím souvisí i útoky známé v lokálních sítích, jako únos relací (hijacking), nebo MiM (Man-in-the-Middle) útoky. U session hijacking je možné do stavajícího datového toku vkládat vlastní informace a tím i přesměrovat legitimní provoz na svůj stroj. Jeden z typických příkladů MiM útoku je popsán výše v odstavci "Podvržení přístupového bodu". V podstatě jde o to, že útočník hraje roli prostředníka mezi klientem a cílovým serverem, tím pádem může odposlouchávat a v případě bezpečného přenosu i dešifrovat data.

DoS útoky

Zahltit bezdrátové sítě je mnohem jednoduší než u ethernetových sítí. K odepření služby stačí např. neustálé posílání RTS (Request To Send) paketů, takže AP nám pořád bude přidělovat právo k

vysílání a ostatní budou muset čekat. Tato chyba byla již u některých AP vyřešena. Co ale určitě nejde vyřešit je rušení pásma 2,4 GHz na kterém WiFi běží. Pásmo 2,4 GHz může rušit spousta přístrojů, např. bezdrátové domácí telefony, mikrovlnky, dálkové odemykání apod. Pokud pásmo budeme záměrně nějakým zařízením či anténou rušit, tak klienti nebudou schopni komunikovat.

Zranitelnosti hloupého administrátora

- Napadá mě hned několik variant. Většina dnešních přístupových bodů je pro zjednodušení spravovatelná přes webové rozhraní. I v dnešní době se najdou AP, které nemají změněné standardní heslo administrátora. Takže může být zabezpečení jakékoliv, ale my si upravíme politiku podle sebe.
- Dalším problémem může být nepovolené AP, které si tam např. pro vlastní potřebu připojil některý ze zaměstnanců. Pokud administrátor nekontroluje, zda v jeho síti nepřibyly AP bez jeho vědomí, tak má útočník otevřenou bránu. Zaměstnanci totiž většinou jen připojí AP, bez jakéhokoliv zabezpečení, do sítě a pokud vše funguje, tak se o něj dál nestarají.
- Pokud administrátor zablokoval vysílání SSID (názvu přístupového bodu) a tím aktivoval tzv. "neviditelný režim", tak se nic neděje. Tento pokus o zabezpečení je samozřejmě úplně k ničemu, protože SSID lze získat pasivním odposlechem.
- WiFi a interní síť by měli být jednoznačně odděleny firewallem. Pokud administrátor neučiní jinak, tak není složité zkoumat firemní intranet a tím pádem se dostat k interním informacím, topologii sítě, sdíleným prostředkům atp.
- Existují také WiFi sítě, okolo kterých jen projdete, automaticky dostanete IP adresu od DHCP serveru a můžete surfovat na internetu. V případě, že je povolený pouze port 80 (http), tak tunneling rulez.

Závěrem
Doufám, že jsem zde shrnul nejčastější bezpečnostní mezery bezdrátových sítí. Jen bych chtěl upozornit, že i když to může vypadat s bezpečností WiFi sítí žalostně, tak mezi teorií a praxí je velký rozdíl a zdaleka ne vše je tak jednoduše prolomitelné, jak by se mohlo zdát. V některém z příštích článků bych se naopak chtěl věnovat novým technologiím a postupům zvyšujícím bezpečnost WiFi sítě.

URL článku: https://security-portal.cz/clanky/wifi-s%C3%ADt%C4%9B-jejich-slabiny

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/networks-protocols
[4] https://security-portal.cz/category/tagy/security
[5] https://security-portal.cz/category/tagy/wifi-wireless