Sítě WLAN dle 802.11 – bezpečnost

Seminární práce na 4IT321, téma K_78

Karel Kohout
karel.kohout@centrum.cz
FIS VŠE, 3. ročník

20. listopadu 2009

Obsah

Seznam tabulek

Seznam obrázků

1 Terminologie

Práce je zaměřena na zabezpečení bezdrátových sítí dle standardu 802.11x z pohledu „běžného“ uživatele. Pokud v práci používám pojmy wi-fi a bezdrátové sítě, jde o bezdrátové sítě dle 802.11x (když uvedeno jinak). V případě, že je to nezbytné pro pochopení textu, zdůrazňuji odlišení běžných „wi-fi“ zařízení a zařízení, které prošly certifikací Wi-Fi Alliance a smí používat logo Wi-Fi. Obdobným způsobem přistupuji ke standardům zabezpečení, kde preferuji běžně známé zkratky (WEP, WPA, WPA2), byť některé z nich jsou označení od Wi-fi Alliance[1] a ne z IEEE 802.11x.

Terminologii takto zjednodušuji, neboť vzhledem k těžišti práce (zabezpečení domácí sítě, připojení k veřejné síti) není pravděpodobné použití bezdrátových sítí dle 802.11, které nejsou alespoň v základních funkcích kompatibilní se zařízeními s certifikací Wi-Fi. Samotným procesem certifikace neprochází všechna zařízení v běžném prodeji[2] – vzhledem k nákladům často jde jen o vybrané nebo dražší modely (patrné zejména u produkce Edimaxu).

Zkratka AP (Access Point) je označení pro bod, ke kterému se připojuje klientské zařízení – klient (někdy označován jako stanice – station). Pokud je v textu určitá technologie označena za bezpečnou, znamená to, že náklady na její napadení jsou (a v příštích třech letech nejspíš budou) pro běžného útočníka[3] za současných poznatků a možností hardware výrazně vyšší než jiné způsoby, jak získat chráněná data.

2 Úvod

Z čistě teoretického hlediska se zabezpečení bezdrátových sítí nijak neliší od zabezpečení „klasických“ sítí, vedených po pevných rozvodech (metalické kabely, optická vlákna a podobně) – šifrování mezi dvěma zařízeními na „poslední míli“ nijak neovlivňuje možnosti případného útočníka odposlouchávat a měnit data dále po cestě. V praxi ale bezdrátová síť, zejména pokud se jedná o wi-fi sítě [4], výrazně snižuje náklady na případný útok a umožňuje ho provést jen s minimálním rizikem odhalení[5] a především s minimálními prostředky (notebook, panelová anténa).

Proto je i v první verzi standardu IEEE 802.11[6] definice šifrování (a omezení přístupu k access pointu) – WEP. Úroveň algoritmu a jeho implementace se může zpětně zdát velmi slabá, ale je třeba mít na paměti výkonové možnosti tehdejších zařízení a samotný účel WEP (viz 3.1). Vlivem implementace, nových poznatků a rozšíření wi-fi sítí přestal být původní WEP považován za bezpečný. Jakožto krátkodobá náhrada byl v roce 2002 navržen „protokol“ WPA (implementující značnou část tehdejšího návrhu IEEE 802.11i). Útok je výrazně obtížnější, přesto ne nemožný. V roce 2004 byl vydán dodatek IEEE 802.11i (WPA 2), od roku 2007 je vyžadována podpora menší části standardu jakožto podmínka pro udělení certifikace Wi-Fi Alliance.

Za jakési formy ochrany bezdrátové sítě je možné považovat i filtrování klientů podle MAC adres, případně skrývání SSID. Jde však o metody, které zastaví jen velmi nekvalifikovaného útočníka (typicky u otevřené bezdrátové sítě, kde má být zabráněno připojení náhodných kolemjdoucích – při krátkém odposlechu však není problém SSID odhalit, respektive zaznamenat

[1] Nezisková organizace – sdružení výrobců bezdrátových zařízení.

[2] Dle nabídky Alza, CzechComputer.

[3] Pracovně útočník s rozpočtem maximálně v řádech desítek tisíc korun.

[4] Lze uvažovat i o jiných typech sítí mimo sítě definované v IEEE 802.11 (pro běžné spotřebitele zejména Bluetooth, mobilní telefony), ale ty jsou mimo téma této práce.

[5] Reálné riziko odhalení je pouze při použití získaných informací (například přihlášení k emailovým účtům), což ale nemá souvislost se samotnými bezdrátovými sítěmi. Pravděpodobnost odhalení je i při agresivních útocích v klasické městské zástavbě s mnoha vysílači skutečně malá (a pravděpodobnost postihu zanedbatelná).

[6] IEEE 802.11-1997

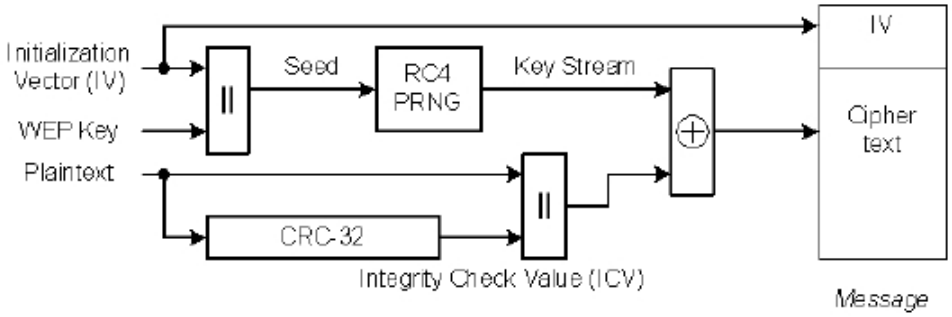
MAC adresu a změnit ji u vlastního zařízení). Proto tyto formy zabezpečení v práci dále nerozebírám. Mnohem účinnější je nasazení zařízení podporující některý ze standardů zabezpečení, definovaných v IEEE 802.11x.

3 Standardy zabezpečení

3.1 WEP

WEP[7] byl definován v IEEE 802.11-1997 jakožto „metoda“ na ochrany dat před náhodným odposlechem mezi autorizovanými uživateli bezdrátové sítě”[8]. Implementace byla nepovinná. Z definice a názvu je zřejmé, že ani v době návrhu nemělo jít o dokonalé zabezpečení.

Jako základ klíče se používají řetězce (sdílené všemi autorizovanými uživateli) o velikosti 40 bitů (WEP-40) nebo 104 bitů (WEP-104), použitý algoritmus je proudová šifra RC4. Integrita dat se ověřuje přes CRC-32 pouze nad nezašifrovanými daty. Jako „seed“ je pro generátor pseudonáhodných čísel pro RC4 použit základ klíče, ke kterému se přidává 24 bitů (IV, initialization vector; náhodné číslo, vygenerované pro každý síťový rámec zvlášť), čímž vzniknou klíče o velikosti 64 bitů (WEP-40[9]) a 128 bitů (WEP-104). IV se přenáší rámci každého síťového rámce a je, spolu s velikostí klíče a použitou šifrou, největší slabinou WEP.



Obrázek 1: WEP - šifrování (Zdroj: Figure 43a [1])

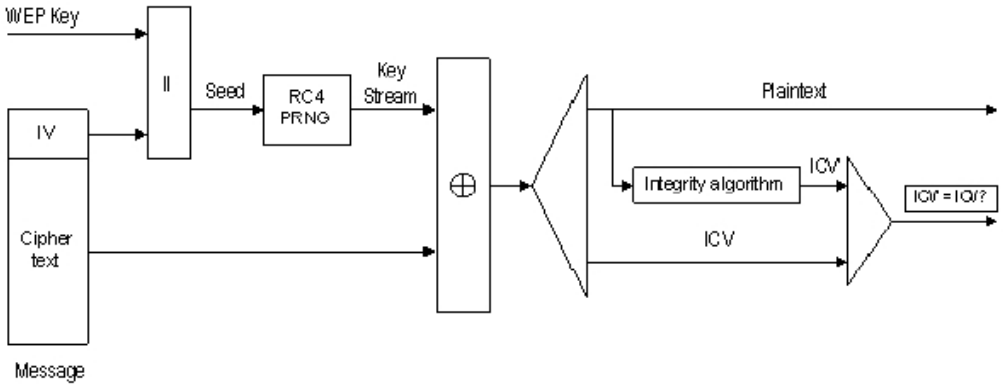
Autorizace uživatelů u WEP probíhá dvěma možnými způsoby:

Open system Asociace klienta a AP proběhne bez jakéhokoliv ověření. Při následné komunikaci může být použit WEP k šifrování.

Shared key Klient před asociací musí prokázat, že zná daný WEP klíč (dle [1], 8.2.2.3):

1. Klient odešle AP požadavek o autorizaci.
2. AP vygeneruje náhodná data (přes generátor pseudonáhodných čísel ve WEP) o velikosti 128*8 bitů a odešle klientovi („challenge“).
3. Klient náhodná data zašifruje WEP klíčem a odešle zpět.
4. AP dešifruje data od klienta a porovná je s daty z kroku 2. Pokud se shodují, umožní klientovi asociaci.

[7] Wired equivalent privacy
[8] Překlad z 8.2.1.1 (WEP overview), [1]
[9] Velikost klíče byla pro export mimo USA omezena na 40 bitů, zrušeno na konci roku 1996: Executive Order 13026



Obrázek 2: WEP - dešifrování (Zdroj: Figure 43b [1])

Zásadní slabinou WEP je IV o velikosti 24 bitů. Pro zajištění bezpečnosti u proudové šifry RC4 by neměl být šifrovací klíč použit více jak jednou; vzhledem k malému prostoru 24 bitů a vzhledem ke slabinám generátoru (pseudo)náhodných čísel[7] je vysoká pravděpodobnost, že ke kolizi–opakování IV (a tím pádem celého klíče) – dojde již po řádově tisících zachycených packetech. Následné nalezení klíče je při dostatečném množství dat obvykle otázkou minut, v nejhorším případě desítek minut výpočtů (na dnes běžném počítači).

WEP jako takový v původní podobě již nepředstavuje pro útočníka zásadní překážku[2], pokud bude schopný zachytit dostatek dat, respektive pokud bude útočník schopný si data vygenerovat s pomocí vhodných nástrojů typu balíčku *aircrack-ng* (ARP replay) a komoditního hardware.

Určitou ochranu poskytuje tzv. WEP Cloaking[3], fungující na principu vysílání „atrap“ síťových rámců, které mají zmást případného útočníka – existují však nástroje, které podobné atrapy umí odhalit a proto jde v podstatě jen o zpomalení útoku (navíc na úkor přenosové kapacity sítě). Některé firmy používají (použily) nestandardní úpravy (WEP2, WEPplus, Dynamic WEP), vycházející z WEP, žádná z nich ale není rozšířená.

3.2 WPA

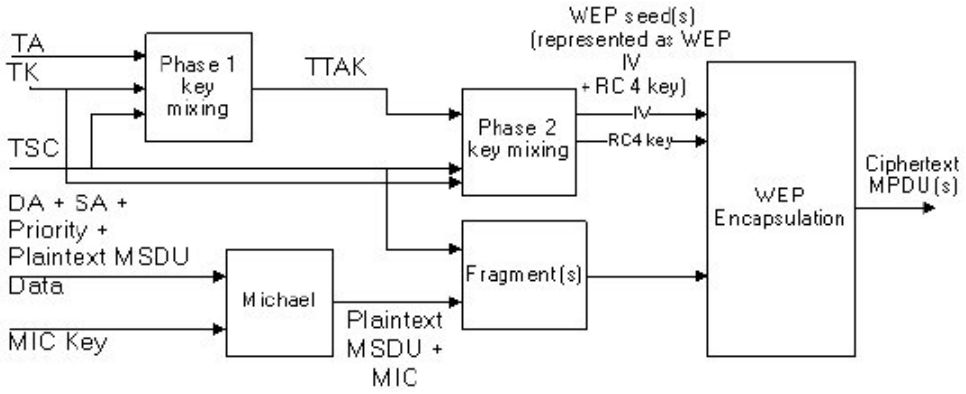
WPA[10] je název Wi-Fi Alliance pro protokol WEP s implementovaným TKIP[11]. Byl navržen jako přechodný stadard, než bude přijat (a než se rozšíří) dodatek IEEE 802.11i (schválen 2004) – proto WPA používá obdobné postupy jako WEP (proudová šifra RC4) a u části síťových karet je implementace otázkou nahrání nového firmware (nebo ovladačů), byť na úkor vyšší zátěže zařízení; u AP je situace složitější a zpětná kompatibilita je problémová. Podpora WPA je od roku 2003 povinná pro udělení certifikace a možnosti používat logo Wi-Fi.

Vyšší odolnost vůči útokům je u WPA zajištěna několika metodami. Klíč pro zašifrování daného síťového rámce není získán pouze spojením WEP klíče a IV, ale na základě řady náhodných proměnných[12], čímž je zajištěna vysoká pravděpodobnost, že každý síťový rámec je zašifrován jedinečným klíčem (o velikosti 128 bitů). Ochranu proti úpravě a „přehrávání“ (replay) poskytuje kontrolní součet MIC (MICHAEL; Message Integrity Check, 64 bitů), zlepšující integritu síťového rámce (v rámci možností zpětné kompatibility); u AP se sleduje počet chybných kontrolních

[10] Wi-Fi Protected Access
[11] Temporal Key Integrity Protocol
[12] Přesný výčet a popis je mimo rozsah této práce. Lze ho nalézt v 8.3.2.1.1 TKIP encapsulation v [1]

součtů pro detekci případného útoku.

Novinkou u WPA je podpora pro EAP[13] kromě již existujícího PSK (pre-shared key) pro autentizaci mezi AP a klientem. Protokol je oproti WEP výrazně bezpečnější, přesto sám o sobě, zejména v módu PSK, nevyhovuje (Beck-Tews: chop-chop – rozšíření útoku z WEP, Ohigashi-Morii[8] – man in the middle).



Obrázek 3: WPA-TKIP - šifrování (Zdroj: Figure 43c [1])

3.3 WPA 2

V rámci dodatku IEEE 802.11i-2004[14] byla přijata opatření, ve stejném roce shrnutá WI-FI Alliance pod označení WPA 2. Oproti WPA nezachovává vůbec zpětnou kompatibilitu a proto došlo k úpravám, které umožňují WPA 2 označit, podle současných poznatků, za bezpečný standard plnící funkci „chránit bezdrátové připojení před běžným útočníkem“.

Základem standardu je RSN[15], respektive RSNA[16], kde jsou definovány dva protokoly zabezpečení – TKIP, který je ve standardu chápán z pohledu zpětné kompatibility, a CCMP.

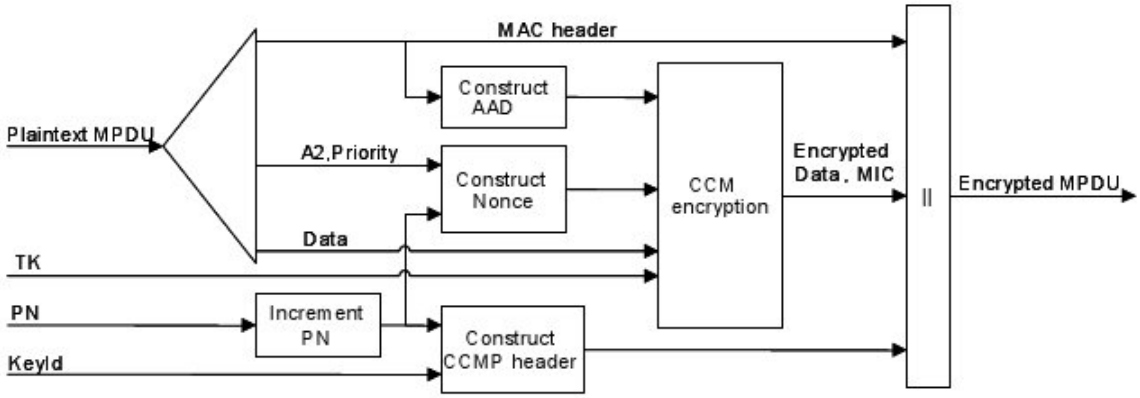
3.3.1 CCMP

Zásadní rozdíl spočívá v použitém šifrovacím algoritmu – proudová šifra RC4 je nahrazena algoritmem Rijndael, přijatým jako AES[17]; AES se rovněž používá k ověření integrity přenesených síťových rámců. Ověření AP a klienta vůči sobě používá „4 way handshake“ (viz [1]).

3.3.2 EAP

EAP[18] je framework pro ověřování uživatelů pomocí řady metod – je možné ho použít i pro sítě LAN, point-to-point sítě a podobně. Následující tabulka obsahuje výčet metod, které EAP používají (v rámci WPA/WPA 2 se používá pět z nich). Podrobnosti lze nalézt v [5]. Některé

[13] IEEE 802.1X/Extensible Authentication Protocol; podrobnosti viz 3.3.2.
[14] Později začleněn do IEEE 802.11-2007
[15] Robust Security Network
[16] Robust Security Network Authentication
[17] Advanced Encryption Standard, bloková šifra s variantami AES-128, AES-192 and AES-256 (dle velikosti klíče). V CCMP jsou použity klíč a bloky o velikosti 128 bitů.
[18] Extensible Authentication Protocol



Obrázek 4: WPA2 – CCMP - přehled (Zdroj: Figure 43o [1])

z uvedených metod EAP dle [5] implementují jen z části. EAP je možné použít i nad WPA. Wi-Fi Alliance pro udělení certifikace nevyžaduje implementaci EAP (označováno jako WPA 2 – Enterprise), pouze implementaci doporučuje.

Zkratka	Význam	Poznámky	Bezpečný
LEAP	Lightweight Extensible Authentication Protocol	Autor: Cisco	Ne
EAP-TLS	EAP-Transport Layer Security	Požadavek na certifikát u klienta	Ano
EAP-MD5	-	Pouze ověření klient → AP; slabiny MD5	Ne
EAP-PSK	EAP - pre-shared key	Klíče pro komunikaci dohodnuty na základě sdíleného „hesla“	Ano
EAP-TTLS	EAP-Tunneled Transport Layer Security	-	Ano
EAP-IKEv2	EAP - Internet Key Exchange Protocol version 2	Komplikovaný systém klíčů	Ano
PEAPv0/EAP-MSCHAPv2	-	Eduroam na VŠE (WPA);	Ano
PEAPv1/EAP-GTC	-	Cisco; alternativa k PEAPv0	Ano
EAP-FAST	Flexible Authentication via Secure Tunneling	Cisco; náhrada LEAP	Ano

Tabulka 1: WPA 2 – módy (Zdroj: Tabulka 1, str. 7 [10])

Z pohledu běžného uživatele provozujícího malou domácí síť není pravděpodobné, že by použil některý ze zmíněných protokolů (nepotřebuje provozovat speciální server s databází uživatelů pro ověření). Ve větších sítích je častý PEAPv0/EAP-MSCHAPv2 (například Eduroam na VŠE[19], ověření probíhá přes jméno a heslo na RADIUS serveru). Zřejmě nejbezpečnější, ale na implementaci nejnáročnější, je EAP-TLS (klientské certifikáty), jehož nasazení pro samotné zabezpečení WI-FI sítě je relativně nákladné – uvažovat by se o něm dalo, pokud by osobní certifikáty byly používány k dalšímu zabezpečení (podepisování nebo šifrování elektronické pošty, přihlašování přes SSH a podobně).

Standard	**Povinná implementace pro certifikaci Wi-Fi**
WEP	4/2000
WPA	9/2003
WPA 2	3/2006 (Personal); Enterprise (EAP) jen doporučený

Tabulka 2: Zdroj: Tabulka 1, [11]

3.4 Další vývoj

V blízké budoucnosti se nechystají tak převratné změny jako bylo zavedení WPA / WPA 2. Předpokladem je postupné vyřazování zařízení zvládajících jen WEP, což však může trvat ještě několik let. Z pohledu domácí sítě je zajímavá aktivita Wi-Fi Alliance směrem k Wi-Fi protected setup (viz níže) i pro sítě „ad-hoc“ (což odpovídá třeba propojení mobilního telefonu s počítačem na synchronizaci kontaktů, kde je wi-fi rychlejší a spolehlivější než Bluetooth).

V další části práce se zabývám možnostmi zabezpečení při použití veřejného připojení (například wi-fi v restauraci) a zajištění domácí sítě. Je nutné zmínit, že předpokládám bezchybnou implementaci WPA 2 (tj. AES, generátoru náhodných čísel a podobně) u AP i klienta. Tento předpoklad se může zprvu jevit jako přehnaný, ale rozhodně nejde o nepravděpodobný případ – stačí si vzpomenout na balíček OpenSSL v Debianu (problém generátorem náhodných čísel při tvorbě klíčů[20]). Podobná chyba může existovat, aniž bude veřejně známa či opravena (v případě hardwarové chyby je navíc obtížně opravitelná); v této seminární práci ji však neuvažuji.

4 Veřejný přístupový bod

„Veřejné“ wi-fi připojení se dnes stává standardem v mnoha prostorách (restaurace, knihovny, konektivita zdarma v Czfree.net) a tudíž je i stále používanější. Podobné připojení však přináší bezpečnostní rizika, která je ne vždy možné eliminovat. Z hlediska provozovatele musí takovýto veřejný bod splňovat zásadní podmínku – nesmí vyžadovat na straně klienta žádné složité nastavení. Připojení je obvykle poskytováno zdarma nebo za mírný poplatek (často jako součást platby za jídlo, ubytování a podobně), proto nepřipadá v úvahu zajišťovat v místě kvalifikovaný personál, který by konfiguroval zařízení klientů. Z podmínky plyne omezení pro použité zabezpečení – je možné použít pouze sdílený klíč (mód PSK), žádný klíč a přihlašování přes webový

[19] Teoreticky jde o bezpečné připojení (klient má v počítači certifikáty z „důvěryhodného“ zdroje, zde z webu VC VŠE), v praxi bude ale bezpečnost řešení nižší – na Eduroam je možné se z linuxových systémů (minimálně z Debian Sid a novejšího Ubuntu) připojit pouze pokud nedochází k ověření certifikátu AP (zřejmě kvůli problému s certifikátem GTE CyberTrust Global Root).

[20] Viz například `http://www.debian.org/security/2008/dsa-1571`, `http://digitaloffense.net/tools/debian-openssl/`

formulář při připojení k síti, nebo provozovat zcela otevřený, nekontrolovaný přístupový bod[21].

Celkově tedy lze říci, že u veřejného přístupového bodu není možné očekávat žádné zabezpečení. Zároveň, i pokud bude takovýto bod dostatečně zabezpečený (vhodný mód EAP[22]), nezaručuje sebelepší nastavení, že správce bodu (například technik, který AP v restauraci nastavoval) nakládá s daty bezpečným způsobem a nezaznamenává je. Navíc nejde ověřit, zda se klient připojuje k AP, které je skutečně v restauraci a provozované restaurací („rogue AP“ – útočník si vytvoří vlastní AP s SSID rámcově odpovídajícím názvu legitimního přístupového bodu)[23]. Z útoků, přicházejících v úvahu, je nepochybně nejnebezpečnější odposlech; pokročilé útoky man-in-the-middle jsou spíš akademického charakteru[24].

Pro našeho „běžného uživatele“ z výše uvedeného plynou následující doporučení:

- považovat jakékoliv informace, přenesené přes veřejný přístupový bod, za zcela veřejné, pokud nejsou dostatečně chráněné (šifrované)
- pro jakékoliv důležité informace používat dostatečnou ochranu – ideální je VPN, SSH tunel na bezpečné místo, SSL/TLS[25] u HTTP protokolů[26].

Pro normálního uživatele je však nereálné se připojovat přes VPN například domů (navíc mnohá zařízení typu mobilních telefonů toto neumožňují) a drtivá většina služeb, které používá (e-mail, webové stránky) není proti odposlechu buď chráněna vůbec nebo chrání pouze přihlašovací údaje a ne samotná data. Rozumné je tedy používat veřejné připojení pouze pro nedůležitá data[27].

5 Zabezpečení domácí sítě

U domácí sítě je nutné uvést dva další předpoklady: v práci se nezabývám zabezpečením samotného počítače a předpokládám, že internetové připojení uživatele, vedené po pevných rozvodech (ADSL, kabelová televize a podobně) je dostatečně bezpečné proti běžnému odposlechu (například by takový odposlech vyžadoval viditelně narušit vybavení ISP). Zároveň předpokládám, že uživatel nepoužívá připojení k internetu přes wi-fi (kde se ze zkušenosti problém mění na veřejný přístupový bod[28]). Řeším tedy, jak zabezpečit například v rámci domu připojení mezi („bezpečným“) notebookem a („bezpečným“) ADSL routerem přes nebezpečné wi-fi v rámci malé bezdrátové sítě (složené z jediného AP-routeru a několika klientů – počítačů, notebooků a mobilních telefonů).

[21] Což může přivést provozovatele do značných potíží, pokud jeho připojení někdo zneužije k nelegálním aktivitám.

[22] Příklad: v hotelu vazba číslo pokoje + náhodné heslo a ověření oproti RAIDUS serveru.

[23] Ověření u restaurace by bylo možné například zveřejněním otisku certifikátu AP na jídelním lístku, u knihovny na nástěnce (...), je ale otázka, kolik procent uživatelů bude schopno shodu certifikátů zkontrolovat.

[24] Dalo by se o nich uvažovat u cíleného útoku na konkrétní firmu, jejíž zaměstnanci pravidelně chodí do konkrétní restaurace na obědy a jednání a pravidelně se připojují do firemní sítě nebo k firemním službám.

[25] V době psaní seminární práce byla objevena zranitelnost u SSL/TLS, umožňující man-in-the-middle útoky, riskantní právě u WI-FI sítí.

[26] Což je obtížné, protože z přihlašovací stránky mnohdy není vůbec zřejmé, zda bude k odeslání formuláře použito HTTP nebo HTTPS.

[27] Ještě zajímavější situace je u internetových kaváren, kde je potenciálně nebezpečný i software a hardware na klientské stanici (keylogger).

[28] ISP se u wi-fi připojení obvykle věnují jen autentizaci uživatele kvůli omezení rychlosti nebo přenesených dat; síť buď není šifrována vůbec nebo je používáno nejnižší možné šifrování (WEP) a sdíleno krátké heslo (často essid, název firmy), které zabrání připojení „nezkušených kolemjdoucích“, ale vzhledem k provozu v síti (a tedy množství dat k analýze) nezastaví dostatečně motivovaného útočníka.

Cílem je, aby:

1. wi-fi bylo dostupné jen autorizovaným uživatelům
2. provoz nebyl odposlouchávatelný ani při dlouhodobém (v řádu měsíců) zaznamenávání síťových rámců
3. uživatelé měli jistotu, že se připojují ke správnému AP[29]
4. přidání nového zařízení bylo jednoduché a nevyžadovalo složité úkony.

Lze vyřadit zabezpečení typu skrytí SSID, omezení na konkrétní MAC adresy (nesplňuje 2). Obdobně není možné použít WEP (v delším období, zejména u sítě na jediném místě, je možné témeř vždy odchytit dostatek dat i u mimořádně dlouhých klíčů – nesplňuje 2). Pokud to technické vybavení umožňuje, chceme se vyhnout WPA, u něhož mohou být objeveny další závažné slabiny.

Jako ideální se potom pro domácí použití jeví WPA 2-PSK. U zdatnějších uživatelů[30] by připadalo v úvahu EAP-TLS, jehož podpora na některých zařízeních však nemusí být dostupná nebo využitelná (především mobilní telefony a jiné „komunikátory“). Nezbytným krokem je změna SSID zařízení (kvůli „rainbow tables“), změna hesla u webového rozhraní u routeru, pokud jím disponuje a volba silného hesla pro samotné WPA 2[31].

5.1 Wi-Fi protected setup

Konfiguraci domácí sítě usnadňuje[32] technické vybavení podporující Wi-Fi Protected Setup. Jde o nepovinný standard pro Wi-Fi certifikovaná zařízení[33] určený pro segment domácností a malých firem, který specifikuje vybrané postupy zabezpečení sítě. Používá WPA 2-PSK.

Obrázek 5: Logo pro zařízení s certifikací Wi-Fi protected setup (Zdroj: [10])

Velmi bezpečný je nepovinný mód NFC (Near Field Communication). U módu PBC (Push Button Configuration) existuje (velmi malé) riziko, že v krátkém okamžiku, kdy se přidává do sítě nové klientské zařízení, se připojí další, nežádoucí zařízení útočníka. Systém eliminuje tvorbu hesel uživateli, což je nejslabší článek u všech výše zmíněných standardů. Bohužel zařízení s tímto certifikátem obvykle patří mezi dražší modely [34]

[29] Podmínky 2 a 3 zabraňují MITM útokům, které u domácí sítě představují významné riziko (uživatel obvykle zachovává určitou rutinu, provozuje v obdobné časy obdobné síťové služby a útočník – „zvídavý soused“ – se tak může dobře připravit).

[30] A pokud nahradíme běžný SOHO router „chytřejším“ zařízením typu Mikrotik.

[31] Síla hesla není nad určitou hranicí kritická, protože pro samotné šifrování se používá (po úpravách) hash z hesla.

[32] Na takovou úroveň, aby bylo možné domácí síť bezpečně nastavit bez pochopení jakýchkoliv podrobností.

[33] Zařízení pro udělení tohoto certifikátu musí zvládat WPA a WPA 2.

[34] V ČR routery s Wi-Fi protected setup stojí od 1500 Kč výš. Úplný seznam zařízení: `http://www.wi-fi.org/search_products.php?search=1&lang=en&filter_company_id=&filter_category_id=&filter_cid=&selected_certifications[]=23&x=34&y=8`

Krok	PIN	PBC	NFC (nepovinné)
1	Uživatel aktivuje AP	Uživatel aktivuje AP	Uživatel aktivuje AP
2	Uživatel aktivuje klientské zařízení	Uživatel aktivuje klientské zařízení	Uživatel aktivuje klientské zařízení
3	SSID je náhodně vygenerováno; AP začíná vysílat	SSID je náhodně vygenerováno; AP začíná vysílat	SSID je náhodně vygenerováno; AP začíná vysílat
4	Uživatel přistoupí k AP přes webové rozhraní	Uživatel stiskne tlačítko zároveň na AP a na klientském zařízení	Uživatel přiblíží klientské zařízení k AP
5	Uživatel zadá PIN z klientského zařízení		

Tabulka 3: Wi-Fi protected setup – kroky, které musí uživatel provést pro bezpečné připojení nového zařízení do sítě (Zdroj: Tabulka 1, str. 7 [10])

6 Závěr

Je třeba zdůraznit, že přes pokroky v zabezpečení bezdrátových sítí (zejména standard WPA 2) nelze wi-fi sítě považovat za bezpečné. Jedinou skutečnou ochranu představuje silné šifrování od jedné stanice až k druhé (u webových stránek například SSL s certifikáty podepsanými důvěryhodnou CA). U domácího připojení je možné použitím šifrování účinně „povýšit“ Wi-Fi na úroveň bezpečnosti klasických pevných rozvodů, které brání odposlechu od náhodného útočníka (například souseda). V případě veřejného přístupového bodu vstupuje do hry ještě důvěryhodnost zařízení provozovatele sítě a proto i přes použití zabezpečení je toto připojení o řád méně bezpečné. V obou případech, bez ohledu na použité šifry a standardy, je možné vždy maximálně dosáhnout úrovně zabezpečení, jaké poskytuje přenos po pevných rozvodech a nikdy vyšší (pokud se nejedná o přenos výhradně mezi dvěma zařízeními v modu „ad-hoc“).

Doporučení pro uživatele proto je veškerá důležitá data přenášet pouze bezpečným způsobem a ostatní data považovat za veřejná bez ohledu na zabezpečení na „poslední míli“[35].

6.1 Přiložený článek

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., and Wetherall, D. 2009. **“When I am on Wi-Fi, I am fearless”: privacy concerns practices in everyday Wi-Fi use**. In Proceedings of the 27th international Conference on Human Factors in Computing Systems (Boston, MA, USA, April 04 - 09, 2009). CHI ’09. ACM, New York, NY, 1993-2002. DOI= `http://doi.acm.org/10.1145/1518701.1519004`

Text mě zaujal rozebráním zabezpečení wi-fi z pohledu uživatele, přesněji popisem, jak neškolení uživatelé vnímají dosah wi-fi signálu (podceňují, protože je rozdíl mezi schopností připojit se k AP a zaznamenat data z něj) a jak chápou zabezpečení a možnost odposlechu. Z výzkumu plyne, že většinou mají jen matné představy o způsobu šifrování signálu a nejsou schopni odhadnout, jaká data takto o sobě šíří a jak je možné takováto data agregovat. Paradoxně považují za

[35] Jednoznačně vždy dochází k zaznamenání části dat u ISP, což ukládá zákon.

nebezpečné provádět přes wi-fi bankovní transakce (které *by měly být* v případě dobré implementace zcela bezpečné) a naopak se neomezují u služeb (z hlediska bezpečnosti) na okraji zájmu (email), které jsou jen nedostatečně chráněné (nebo nechráněné – jak uvádím v práci, často je chráněno jen přihlašování, nikoliv přenášený obsah).

Článek mimo jiné do značné míry potvrzuje, že nejslabším místem jakéhokoliv zabezpečení je vždy člověk a jeho motivace (ať už pozitivní nebo negativní) chránit informace.

Reference

[1] IEEE, Dodatek IEEE 802.11i-2004, 2004 http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[2] BECK, Martin, TEWS, Erik, Practical attacks against WEP and WPA http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[3] AirDefense Inc., WEP Cloaking – Maximizing ROI from Legacy Wireless LAN http://www.advisetech.com/pdf/wep_whitepaper.pdf

[4] Wi-Fi Alliance, WPA deployment http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf

[5] Extensible Authentication Protocol (EAP); RFC 3748, The Internet Society, 2004 http://tools.ietf.org/html/rfc3748

[6] Wikipedia, Temporal Key Integrity Protocol, Wi-Fi Protected Access, Extensible Authentication Protocol (pouze pro zorientování v problematice), http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol, http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access, http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

[7] Fluhrer, Mantin and Shamir attack http://en.wikipedia.org/wiki/Fluhrer,_Mantin,_and_Shamir_attack

[8] OHIGASHI, Toshihiro, MORII, Masakatu, A Practical Message Falsi[U+FB01]cation Attack on WPA, Hiroshima University, Kobe University, Japan http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf

[9] WONG, Stanley, *The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards*. GSEC Practical v1.4b, May 20, 2003

[10] Wi-Fi Alliance, Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup™: Easing the User Experience for Home and Small Office Wi-Fi® Networks http://www.wi-fi.org/files/kc/20090123_Wi-Fi__Protected_Setup.pdf

[11] Wi-Fi Alliance, The State of Wi-Fi® Security, 9/2009 http://www.wi-fi.org/knowledge_center_overview.php?docid=4582