ZPRÁVA O TESTU ZABEZPEČENÍ BEZDRÁTOVÉ SÍTĚ

Autoři článku: **Pavel Kaňkovský, Karel Miko – DCIT, s.r.o.**
http://www.dcit.cz

Článek zveřejněn v časopise **Data Security Management** 1/2004
http://www.dsm.tate.cz

Jak je na tom vaše firma či instituce z hlediska zabezpečení sítě WLAN? To se dozvíte jedině tehdy, když si necháte zabezpečení vaší sítě otestovat. Je až kupodivu, kolik slabin lze během takového testu nalézt. Testování se bohatě vyplatí, což bychom rádi ukázali na výsledcích konkrétního testu sítě WLAN společnosti ABC.

Výchozí situace

Obsah tohoto článku se z velké části opírá o skutečně realizovaný test, který byl proveden pro zákazníka, kterého nechceme přímo jmenovat, nicméně alespoň pro rámcovou představu naznačíme, že se jedná o firmu z oblasti „utility“, která se pravidelně řadí mezi TOP 100 českých společností.

Diskutovaný test byl prováděn v návaznosti na nasazení bezdrátové technologie (konkrétně IEEE 802.11b známá též pod označením Wi-Fi) ve zmíněné společnosti, přičemž testovaná bezdrátová síť byla před vlastním testem zabezpečena s využitím možností provozované technologie. Nejednalo se tedy o zcela otevřenou – někdy s nadsázkou označovanou jako „drive-in“ – bezdrátová síť, u které by podobný test prakticky postrádal smysl.

V době provádění testu již byla publikována řada článků o bezpečnostních slabinách bezdrátových sítí implementovaných podle standardu IEEE 802.11(b). Teoretická pojednání o bezpečnostních slabinách, kterých slyšíte dnes a denně celou řadu, bývají sice zajímavá, ale praktické ověření odolnosti provozované Wi-Fi sítě při simulovaném průniku je velmi cennou informací, u které již není nutno filozofovat, do jaké míry je ten „náš“ systém trpící onou teoretickou slabinou skutečně zranitelný nebo ne.

Pasivní odposlouchávání

V první části testu byla odposlouchávána komunikace mezi bezdrátovými uzly sítě společnosti ABC. Prakticky okamžitě byla pomocí programu Kismet[1] detekována IEEE 802.11b síť na kanálu číslo 10 (2,457 GHz) s BSSID 00:02:04:06:08:0A pracující v infrastrukturním módu. ESSID sítě je ABC. Tento údaj je sice v oznámeních (Beacon)

[1] Výběr software proběhl takto: Prohledli jsme si pár programů, ke kterým byl k dispozici zdrojový kód (aby bylo možné provádět případné úpravy) a které chodily pod Linuxem. V oblasti vyhledávání sítí a odposlechu vypadal nejnadějněji Kismet, v oblasti lámání WEPových klíčů AirSnort. A bylo rozhodnuto.

rozesílaných přístupovým bodem skryt (nahrazen jednou mezerou), nicméně je uveden ve všech požadavcích o připojení k síti (Association Request), kterých bylo při běžném provozu zachyceno cca 5 během jedné hodiny, i ve zprávách vysílaných klienty při hledání přístupového bodu (Probe Request) a odpovědích od něj (Probe Response), kterých bylo zachyceno při běžném provozu průměrně více než 10 za minutu. Pro připojení k síti není vyžadována žádná autentizace, síť je jako provozována jako otevřená, nicméně veškerá přenášená data jsou šifrována.

Vzhledem k tomu, že byla přenášená data šifrována, bylo možno ze zachycené komunikace získat jen omezené informace z řídicích rámců a nešifrovaných záhlaví datových rámců. Během 58 minut (mezi 9:54 a 10:52) bylo zachyceno 181 729 rámců ze 756 různých adres síťových karet (z toho 4 adresy byly identifikovány jako patřící bezdrátovým klientským uzlům). 145 325 rámců (80 %) bylo datových (a šifrovaných), ostatní byly různé řídící zprávy. Většina z datových rámců, konkrétně 141 774 (78 % ze všech resp. 96 % z datových), byla vyslána z pevné sítě ABC a propagována do bezdrátové sítě, z toho 138 449 rámců (76 % ze všech resp. 95 % z datových) bylo rozesíláno všem uzlům či zasíláno na skupinové adresy a lze předpokládat, že většina z nich je generována bez ohledu na počet a aktivitu připojených bezdrátových klientů.

V rámci této části byla provedena namátková kontrola šíření vysílaného signálu mimo budovu společnosti ABC. Bylo ověřeno, že komunikaci lze bez problémů zachytit na nejméně 20 metrů dlouhém úseku ulice před budovou. Na chodníku blízko vchodu do budovy byl dokonce signál podstatně silnější než uvnitř budovy v místnosti, kde byl test prováděn. Je pravděpodobné, že s vhodným vybavením (směrovou anténou a citlivým přijímačem) by bylo možno odposlouchávat i z podstatně větší vzdálenosti.

Kryptoanalytický útok

Standard IEEE 802.11 definuje šifrovací algoritmus WEP (Wired Equivalent Privacy). WEP pracuje následujícím způsobem: Vysílací stanice vygeneruje 24bitový inicializační vektor (IV), ten spojí s tajným klíčem, který sdílí s přijímací stanicí (podle standardu je tento klíč 40bitový, obvykle však zařízení implementují i variantu s 104bitovým klíčem, který je často nesprávně označován jako 128bitový), a výsledkem inicializuje proudovou šifru RC4. Ta pomocí pseudonáhodného generátoru (PRNG) produkuje tzv. klíčovou sekvenci a tato sekvence je pak po jednotlivých bitech sčítána modulo 2 se šifrovanými daty, ke kterým WEP připojuje 32bitový kontrolní součet (ICV). Vyslaný datový rámec obsahuje IV v otevřeném tvaru a data zašifrovaná spolu s ICV (a některé řídící informace). Přijímací stanice přečte IV, dešifruje na základě znalosti IV a sdíleného tajného klíče data a ICV a ověří správnost ICV.

Ve výše popsaném šifrovacím algoritmu WEP byla objevena a v literatuře popsána řada velmi závažných slabin, mj.:

- Útočník může znovu vysílat odposlechnuté rámce a navíc může v zachycených datových rámcích bez znalosti šifrovacího klíče "poslepu" invertovat některé bity a díky linearitě kontrolního součtu (CRC-32) použitého pro ICV upravit odpovídajícím způsobem i kontrolní součet tak, aby byl upravený rámec ostatními uzly akceptován. Toho lze např. využít k zahlcení sítě nebo některého z uzlů, nebo lze úpravou cílových adres přesměrovat zašifrovaná data na útočníkův počítač, kam už budou doručena v otevřeném tvaru.
- Zná-li útočník obsah určitého datového rámce, může vypočítat klíčovou sekvenci (resp. její počáteční část, jejíž délka je stejná jako délka šifrovaných dat) pro daný tajný klíč a použitou hodnotu IV a se znalostí této klíčové sekvence dešifrovat všechny rámce zašifrované stejnou kombinací klíče a IV. IV může nabývat pouze 2^{24} různých hodnot, a proto je prakticky proveditelné, aby útočník mající přístup k otevřenému textu některých rámců (případně mající možnost takové rámce přímo generovat) zjistil hodnoty všech klíčových sekvencí a byl tak schopen dešifrovat veškerou komunikaci

šifrovanou za použití daného tajného klíče. Navíc už se znalostí jediné klíčové sekvence je možné vysílat falešné šifrované rámce.

- Slabina v inicializaci PRNG v RC4 umožňuje pro určité tzv. slabé hodnoty IV útočníkovi odvodit ze znalosti prvního bajtu výstupu PRNG, který je zároveň použit jako první bajt klíčové sekvence, částečnou informaci o jednom bajtu tajného klíče. První bajt klíčové sekvence lze určit ze znalosti prvního bajtu dat, a tuto datovou hodnotu je prakticky vždy možné odhadnout (obsah většiny datových rámců začíná záhlavím LLC SNAP a to má první bajt fixní – 0xAA). Útočník, který zachytí dostatečné množství rámců se slabým IV, pak může vypočítat tajný klíč. Známých slabých hodnot IV je cca 3000 pro 40bitové klíče resp. cca 9000 pro 104bitové klíče.

První dvě slabiny jsou detailněji popsány např. v knize J. R. Walkera [1], třetí slabina byla publikována v článku S. Fluhera, I. Mantina a A. Shamira, viz [2]. Poznamenejme, že efektivita útoku na první a druhou slabinu není nijak ovlivněna délkou tajného klíče a složitost útoku na třetí slabinu roste s délkou klíče pouze zhruba lineárně.

Prakticky demonstrován byl útok na třetí uvedenou slabinu za použití programu AirSnort. Pro nalezení tajného klíče je třeba shromáždit zhruba 100 šifrovaných datových rámců se slabým IV pro každý bajt klíče – konkrétní hodnota pro daný klíč se však může lišit. Bylo vypozorováno, že klienti i AP generují IV sekvenčně, přičemž první bajt je nejméně významný (little-endian). Nově připojení klienti začínají IV generovat od nulové hodnoty, což bylo z hlediska útoku relativně výhodné, protože klient pak musel po svém připojení procházel oblast s vyšší hustotou slabých IV (navíc by tato vlastnost zvýšila efektivitu útoku na kolize IV). Aby však bylo možné nalézt dostatečný počet požadovaných rámců v krátkém čase, byl provoz v bezdrátové sítí uměle zvýšen na přibližně 500 rámců za sekundu vysíláním zpráv ICMP Echo z pevné sítě na vybraný bezdrátový uzel, který následně generoval na tyto zprávy odpovědi.

Po zhruba 3 hodinách bylo odposlechnuto přes 3 milióny datových rámců a nalezeno přes 3000 slabých hodnot IV (pro obě délky klíčů), a z těch se podařilo celý tajný klíč rekonstruovat. Nalezený klíč byl 40bitový, byl sdílen všemi pozorovanými bezdrátovými uzly a byl tvořen ASCII kódy znaků v řetězci „heslo“. Je třeba upozornit, že podobně konstruovaný krátký klíč (omezeným výběrem znaků byla efektivní délka zkrácena o cca 7 bitů) lze s běžně dostupným výpočetním výkonem odhalit i z malého množství odposlechnutých zašifrovaných dat během několika desítek hodin za použití hrubé síly.

Dolní odhad běžného provozu na bezdrátové síti ABC je cca 130 tisíc datových rámců za hodinu. Budeme-li uvažovat pouze pracovní dobu, tj. 8 hodin denně, lze každý den odposlechnout přes milión datových rámců. Je tedy pravděpodobné, že tento útok by bylo i bez uměle generovaného provozu možné úspěšně dokončit během jednoho týdne. Časový odhad by se příliš nelišil ani v případě užití 104bitového tajného klíče místo 40bitového díky vyšší hustotě slabých IV pro delší klíč (pouze by se poněkud zvýšily nároky na útočníkův výpočetní výkon).

Po zjištění šifrovacího klíče byla úspěšně dešifrována data zachycená během předchozí části testu obsahující mj. informace o výskytu IP telefonu Cisco IP Phone 7960 s IP adresou 10.1.2.3, heslo pro směrovací protokol OSPF, jména a adresy doménových řadičů ABC01DC, ABC02DC a EML01DC a HTTP komunikaci uživatele Zelenka z počítače P118 se serverem *portal.oracle.com* týkající se registračních údajů ABC na tomto portálu. Se znalostí ESSID a klíče se také bylo možné do bezdrátové sítě připojit a v ní bez problémů komunikovat a vzhledem k povaze zachycených dat se jeví velmi pravděpodobné, že by tak byl získán přímý přístup do vnitřní sítě ABC.

Doporučení

V daném případě byla doporučena následující opatření, řadu z nich lze do jisté míry považovat za obecně platná doporučení při zabezpečování Wi-Fi sítí:

- Použití další kryptografické ochrany vedle WEPu pro komunikaci ve wireless síti – např. IPsec či jinou technologii šifrované VPN. Jinými slovy: považovat wireless komunikaci za nezabezpečenou a pro připojení z wireless sítě do vnitřní sítě využívat šifrované VPN kanály.
- Oddělit bezdrátovou síť od pevné lokální sítě směrovačem či jiným zařízením, které omezí únik dat (zvl. broadcastů a multicastů) z pevné sítě do bezdrátové.
- Používat pro WEP co nejdelší (běžný hardware obvykle podporuje 104bitové) a netriviální (nejlépe náhodné) klíče. Zvážit možnosti, jak zajistit rychlou obměnu těchto klíčů.
- Zjistit, zda nelze změnou konfigurace nebo výměnou firmware na používaných zařízeních potlačit užití slabých IV.
- Zvážit použití různých klíčů pro různé klienty resp. skupiny klientů (pomocí tzv. keymappingu).
- Překonfigurovat AP tak, aby požadoval autentizaci klientů a to pokud možno jinou metodou, než je standardní shared-key authentication v IEEE 802.11.
- Zvážit omezení úniku signálu mimo budovu vhodně umístěnou a orientovanou sektorovou anténou případně jinými metodami (stíněním).
- Zvážit změnu ESSID na nějakou nic neříkající hodnotu (např. WLAN, INTER) aby nebyla na první pohled zjevná skutečnost, že se jedná o síť společnosti ABC.
- Výhledově doporučujeme technologii IEEE 802.11b opustit a nahradit některým z jejích následovníků (bohužel v současné době není žádná technologie dostatečně zavedena, aby bylo možno ji jednoznačně doporučit).

Nutno podotknout, že zdaleka ne všechna opatření byla v případě firmy ABC jednoduše realizovatelná, přičemž překážky nebyly finanční, nýbrž vesměs omezení plynoucí z technologických limitů provozovaných komponent.

Shrnutí

V případě průnikových testů nebývá obvykle diskuse nad možnými dopady nijak složitá, ve světle praktické demonstrace možného útoku administrátoři i manažeři velmi rychle pochopí možné důsledky – sami vědí mnohem lépe než externí konzultanti, jak cenná data a systémy mají.

Výsledkem popisovaného testu byl závěr, že přes všechna aplikovaná nastavení je provozovaná síť zranitelná, související rizika byla dle našeho názoru neakceptovatelná. Hlavními problémy byla možnost pasivního odposlechu komunikace příp. aktivní komunikace útočníka ve vnitřní síti, se kterou byla bezdrátová síť propojena.

Motivovaný útočník s dostatečnou technickou znalostí a patřičným vybavením (přitom požadované znalosti i vybavení jsou běžně dostupné) by s velmi vysokou pravděpodobností byl schopen provést útok stejným či obdobným způsobem, tj. detekovat existenci sítě, odhalit šifrovací klíč (ať už sofistikovaným kryptoanalytickým útokem nebo prostou hrubou silou) a následně zachycovat a dešifrovat veškerý provoz na bezdrátové síti, nebo se dokonce do sítě připojit a získat tak konektivitu na stejné úrovni jako mají oprávnění uživatelé této sítě (což nemusí nutně znamenat plný přístup do celé komunikační infrastruktury). Další „úspěchy“ v rámci útoku by závisely pouze na odolnosti přístupných interních komponent vůči napadení.

Možná očekáváte alespoň zobecněné odstrašující informace o tom, které všechny klíčové systémy byly v daném případě v ohrožení. U průnikových testů z externího prostředí (což je případ testu wireless sítě) ovšem jako externisté obvykle nedostáváme podrobné informace, které konkrétní systémy byly v ohrožení a jaké konkrétní dopady by reálný útok mohl mít (a vzhledem k omezenému rozsahu testu to ani nebylo zkoumáno).

Závěr

Pořídit levný plug&play Access Point a připojit ho do volného ethernetového portu je sice lákavé, efektní a jednoduché, nicméně vězte, že po standardní instalaci v drtivé většině případů spouštíte zcela otevřenou (nezabezpečenou) bezdrátovou síť a všem náhodným kolemjdoucím otevíráte dokořán virtuální dveře do Vaší sítě. Ale i v případě, že se svou bezdrátovou síť pokusíte zabezpečit za použití standardních bezpečnostních mechanismů, může důkladnější zkoumání odhalit řadu problémů vyplývajících ze slabin těchto mechanismů nebo z jejich chybného použití.

Literatura:

[1] J. R. Walker: *Unsafe at any key size; An analysis of the WEP encapsulation*, IEEE Document 802.11-00/362, Oct. 2000.

[2] S. Fluher, I. Mantin, A. Shamir: *Weaknesses in the Key Scheduling Algorithm of RC4*, Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

Box 1: Terminologická poznámka šéfredaktora

V rámci WLAN se rozlišují dva způsoby komunikace mezi stanicemi:

- infrastrukturní, kdy spolu stanice (např. notebooky) komunikují přes tzv. přístupový bod (AP, Access Point); tento mód bývá také označován jako managed nebo ESS (Extended Service Set);
- ad-hoc, kdy spolu stanice komunikují přímo bez přístupového bodu; pro ad-hoc sítě se používají i dva další názvy a to peer-to-peer sítě a IBSS (Independent Basic Service Set).

Když WLAN operuje v infrastrukturním módu, jeho přístupový bod a k němu připojená zařízení tvoří tzv. BSS (Basic Service Set). Každá BSS má svůj 48bitový identifikátor BSSID (Basic Service Set Identifier), obvykle je to MAC adresa přístupového bodu. Kromě toho má každá síť v infrastrukturním módu přiřazeno jméno o délce max. 32 znaků označované jako ESSID (Extended Service Set Identifier), někdy jen krátce jako SSID. Pokud je v jedné síti více přístupových bodů, pak používají stejný ESSID a odlišují se různými BSSID.

ESSID používají stanice při přihlašování k přístupovým bodům a znalost ESSID je nezbytná k tomu, aby se stanice mohla připojit k AP (nikoli však k tomu, aby mohla odposlouchávat přenášená data – pokud nejsou šifrována). Zjištění ESSID je tedy jedním z hlavních úkolů útočníka hledajícího sítě, do kterých by se mohl přípojit (tato aktivita bývá označována jako *wardriving*, resp. *warchalking* pokud je zároveň spojena s označováním míst, ze kterých je možno se k nalezeným sítím připojit). Někteří administrátoři sítí proto ESSID ve výzvách přístupového bodu eliminují (mohou místo něj zvolit mezeru anebo ESSID nakonfigurovat jako *any*, tj. cokoliv). Nemá to ovšem velký smysl, protože tento údaj je v řídích zprávách, pomocí kterých se stanice připojují k AP, v otevřeném nezašifrovaném tvaru. Útočník si tudíž může ESSID odposlechnout, kdykoli se do do sledované sítě přihlašuje nová stanice, jak to nakonec ukazují výsledky testu. Někteří administrátoři zase ponechávají v platnosti defaultní ESSID a si to stačí jen ověřit (Cisco má defaultní ESSID „tsunami“, 3Com „101“ atd.).