Bezdrôtové pripojenia a bezpečnosť

V tejto časti článku by sa mal záujemca o bezpečnosť bezdrôtových sietí oboznámiť so základnými princípmi fungovania týchto sietí, aby mohol pochopiť bezpečnostné potreby, ktoré tieto siete vyžadujú.

Zaujímavé je, že prvá skutočné fungujúca bezdrôtová sieť LAN vznikla 4 roky pred zrodom eternetu, a to na University of Hawaii a prsty v tom mala firma Xerox. Bolo to v roku 1969. Ustanovením štandardu 802.3 sa preniesla aj hlavná tvorivá snaha na túto platformu. Rozširovanie používania bezdrôtových prenosov na eternete však začalo ježiť chlpy administrátorom systémov a bezpečnostným správcom sietí. Bezdrôtové prenosy so sebou doniesli dedičstvo v podobe nových bezpečnostných problémov a na ich pochopenie bolo treba vedomosti z oblasti rádiofrekvencií. Dátová vrstva bezdrôtových prenosov je totiž zásadne odlišná od oveľa rozšírenejšieho vodičového variantu.

V súčasnosti používané bezdrôtové technológie môžeme približne rozdeliť na tri kategórie:

- **WPAN** (*Wireless Personal Area Network*) – technológie združené v štandarde 802.15, ako Bluetooth, HomeRF alebo IrDA, s vysielacím výkonom niekoľko jednotiek mW a dosahom niečo nad 10 m;
- **WLAN** (*Wireless Local Area Network*) – technológie združené v rodine štandardov 802.11 s povoleným vyžarovacím výkonom 100 mW, prípadne 1 W a dosahom bez externých antén niekde medzi 100 m až 1 km.
- **WWAN** (*Wireless Wide Area Network*) – rôzne celulárne a im príbuzné technológie, ako GSM, GPRS, CDPD, TDMA a pod., ktorých prevádzka väčšinou vyžaduje udelenie licencie príslušného úradu, ktoré však majú spravidla dosah 10 – 30 km.

Takéto rozdelenie však nie je úplne jednoznačné, pretože 802.11b pri vytvorení linky point-to-point vie fungovať aj na vzdialenosť 20 – 30 km a Bluetooth vie tiež dosiahnuť až do 100 m, ak je vhodné fyzikálne prostredie a chýbajú interferencie.

Bezpečnosť WWAN je silne závislá od typu linky a nastavení a hardvéru prevádzkovaného u providera. Hlavná bezpečnostná zásada je pristupovať aj k linkám WWAN ako k nezabezpečeným verejným sieťam a zaistiť vhodné oddelenie sietí a bezpečnosť gateway. Autentifikácia a dátové šifrovanie by malo byť konzultované s providerom linky z dôvodu možného filtrovania určitých protokolov alebo ich služieb. Bezpečnosť WLAN a WPAN je zvyčajne v kompetencii spoločnosti alebo jednotlivca. Preto si viac WWAN nebudeme všímať.

Bezpečnosť bezdrôtových sietí je výnimočná v tom, že expert z oblasti sieťovej prevádzky IT sa stretne s množstvom nových skutočností a funkcií z oblasti rádiotechniky. Okrajovo spomeniem tie hlavné, ktoré by sa mali spriateliť s bezpečnosťou:

SPRAVNY NAVRH SIETE – o bezpečnosti treba uvažovať už pri prvotnom návrhu bezdrôtovej siete. Stratégie typu „však to nejako zazichrujeme" tu vedú väčšinou ku sklamaniam alebo pre tých, ktorí sa ani nenamáhajú skontrolovať, čo nainštalovali, vedú väčšinou k výdychu: Hurá! Funguje to! Bezdrôtové siete majú ešte stále nižšiu priepustnosť ako ich metalickí bratia, a preto sú z dôvodu nesprávnej konfigurácie oveľa citlivejšie na útoky DoS, najmä ak sa na nich prevádzkuje ešte aj VPN.

NEED TO ACCESS PRINCÍP – bezdrôtová sieť má umožniť konektivitu, keď ju používateľ potrebuje, a nie inokedy. Sieť má byť projektovaná a inštalovaná tak, aby maximálne pokrývala požadovanú oblasť a aby na druhej strane mimo tejto oblasti vyžarovala čo najmenej. Tento princíp zminimalizuje príležitosť pre „náhodne okoloidúcich sniffujúcich chodcov". Prípadný snaživec by sa musel priblížiť do tesnej blízkosti budov a tam by už mala pomôcť CCTV.

INTERFERENCIE, prekrývanie signálu a neautorizované zariadenia

Na pochopenie interferencie si povedzme o rozostretom spektre komunikácie. Rozostreté spektrum spočíva na širokej frekvencii s nízkym vysielacím výkonom, čo je v protiklade s úzkopásmovým prenosom, ktorý používa len práve potrebné spektrum na prenos signálu a má veľmi vysoký pomer odstupu šumu. Obidve normy, 802.11 a 802.15, definujú technológiu rozostretého pásma. Táto technológia bola pôvodne vyvinutá počas druhej svetovej vojny, pričom bezpečnosť bol primárny hnací faktor. Hocikto, kto prechádzal cez vysielacie frekvencie so širokopásmovým skenerom a nevedel, ako sú dáta prenášané a ktoré jednotlivé frekvencie sú použité, prijímal len signál podobný bielemu šumu. V posledných rokoch boli implementované dva základné spôsoby prenosu signálu:

- *preskakujúca frekvencia – Frequency hopping spread spectrum – FHSS,*
- *priamo následné – Direct sequence spread spectrum – DSSS.*

FHSS používa psedonáhodnú postupnosť frekvencií a ich zmien (hops), ktoré sú vykonávané všetkými zariadeniami participujúcimi v bezdrôtovej sieti. V súčasnosti používa tento typ prenosu Bluetooth. Ten je veľmi odolný proti interferenciám dovtedy, kým signály nepokryjú celé pásmo ISM. Toto pásmo sa dá vyplniť mobilným telefónom s bluetoothovým rozhraním, PDA alebo notebookom a potom sa tieto zariadenia môžu stať prostriedkami na vedenie útoku DoS. Teoreticky možno do siete PAN pripojiť 26 bluetoothových zariadení, ktoré skackajú na rozdielnych frekvenciách prenosového rozsahu. Prax neodporúča používať viac ako 15 zariadení naraz. Dnes to ešte nehrozí, ale vývoj rýchlo napreduje.

V predchádzajúcich riadkoch som spomenul nový termín: pásmo ISM. Moderné bezdrôtové siete operujú v ISM (Industrial/Scientific/Medical) na frekvenciách medzi 2,4 a 2,5 GHz (teda na vlnovej dĺžke medzi 12,5 – 12,0 cm) a v UNII (Unlicensed National Information Infrastructure) na frekvenciách 5,15 – 5,35 a 5,725 – 5,825 GHz (vlnová dĺžka 5,8 – 5,6 a 5,24 – 5,15 cm). Zariadenia podľa noriem 802.11, 802.11b a 802.11g a Bluetooth používajú pásmo ISM, zatiaľ čo pásmo UNII je používané zariadeniami podľa 802.11a.

Vysielacie výkony sú riadené v USA FCC, v Európe to má na starosti ETSI. Tieto predpisy sú aplikované aj slovenským telekomunikačným úradom. WLAN a WPAN síce fungujú na voľnej frekvencii, ale predpis sa môže porušiť neprimerane veľkým vysielacím výkonom.

Pri vysielacích výkonoch sa zvyknú udávať dve hodnoty: International radiator (IR), ktorá zahŕňa transmiter a celú kabeláž, ale nezahŕňa anténu, a Equivalent isotropically radiated power (EIRP), čo je výkon vysielaný anténou. Pre pásmo 2,4 – 2,5 GHz pripúšťa FCC v prevádzke point-to-multipoint maximum 4 W EIRP, pre Bluetooth je obmedzenie 100 mW. V prevádzke point-to-point je to rozdielne v každej krajine. Regulácie pre pásmo UNII sú trochu komplexnejšie. V tomto pásme existujú tri podpásma. Dolné pásmo UNII (5,15 – 5,25 GHz) je rezervované na prevádzku v rámci budov a podľa FCC je vysielací výkon ohraničený na max. 50 mW EIRP. Stredné pásmo (5,25 – 5,35 GHz) môže byť použité na prevádzku v rámci budovy alebo mimo budov na kratšie vzdialenosti a povoľuje výkon 250 mW. Vrchné pásmo (5,725 – 5,825 GHz) je určené na vonkajšiu prevádzku a povoľuje vysielací výkon 1 W. Zaujímavosť je obmedzenie IEEE, ktoré znížili vysielací výkon pre každé podpásmo o 20 %.

Druhý spôsob prenosu – DSSS – je používaný aj pôvodnou normou 802.11, ale aj následnými 802.11b, 802.11g a 802.11a. V porovnaní s FHSS, ktoré používa šírku nosnej frekvencie 5 MHz, v prenosoch DSSS sú použité širšie kanály. 802.11b/g používa 22 MHz a 802.11a 20 MHz šírku kanála. Väčšia šírka prenosového kanála umožňuje vyššie prenosové rýchlosti. Napriek tomu, že DSSS používa len jeden kanál z pásma, je oproti FHSS viac zraniteľné cez interferencie a rušenie. Jednoduché počty nám ukážu, že v pásme od 2,4 GHz do 2,5 GHz sa nám zmestí ani nie celkom 5 kanálov. Keďže to nestačí, kanály sú usporiadané tak, že rozdiel medzi nimi je 5 MHz. Z toho vyplýva, že sa musia prekrývať. V USA sa používa na normálnu prevádzku 11 kanálov. To značí, že sa neprekrývajú len kanály č. 1, 6 a 11. V Európe sa používa 13 kanálov a všetkých 14 sa používa len v Japonsku. Zaujímavý môže byť kanál 6, ktorý dosť výrobcov používa ako default továrenské nastavenie.

■

Treba rozlišovať bezpečnostný incident od iných príčin, prečo sieť nefunguje, rozhodnúť, ako má byť zabránené nežiaducemu príjmu signálu – napríklad či ide o rádiovú interferenciu alebo niekto skúša útok DoS. Prichádzajú SYN TCP pakety, pretože vysielajúci host nemôže prijať SYN-ACK správne, alebo je to „packet kiddie" skúšajúci zahltiť váš server? Odkiaľ pochádza toľko fragmentovaných paketov v sieti? Použil útočník *nmap –ffff / hping –f* alebo bola upravená hodnota LAN MTU, lebo sa často opakovalo vysielanie veľkých paketov? Väčšina problémov je vystopovateľná v sieti, niektoré z nich môžu spôsobiť aj susedné bezdrôtové siete. Dve susediace bezdrôtové siete nemôžu vysielať na rovnakej frekvencii z dvoch dôvodov: pre interferenciu a možný príjem dát v susednej sieti.

Ďalšia zaujímavá kapitola sú antény pre bezdrôtové siete. Staršie ročníky iste ovládajú túto problematiku, keď bolo úspechom zachytiť na 9 dB anténu Yagi vysielanie Ö3 na vzdialenosť 200 km, a to stereo. Dnešné ceny antén nie sú vysoké a treba si odpovedať, či je účelné míňať čas na výrobu vlastných antén. Myslím, že len pre veľmi zapálených nadšencov alebo pri neštandardných riešeniach. Antény spomínam z dôvodu, že je to dôležitý bezpečnostný člen, ako ovplyvniť vyžarovací výkon a hlavne smer signálu, aby bola pokrytá najmä žiadaná oblasť a oblasť mimo záujmu ostala odtienená. Kto chce správne inštalovať zabezpečené bezdrôtové siete, musí bezpodmienečne poznať, ako sa kalkulujú vyžarovacie výkony. Na uľahčenie života sa na internete dajú nájsť rôzne nástroje a pomôcky. Možno sa divíte, čo za vzťah je medzi akceptovateľným vyžarovaným výkonom a bezpečnosťou bezdrôtových prenosov. Jednoducho taký, aby ste negenerovali interferencie a nenašli sa na druhej strane barikády podobne ako hľadači bezdrôtových pripojení, teda crackeri. Na tej druhej strane je to však jednoduchšie, načo sa starať o vyžiarený výkon, čím viac, tým lepšie a tým väčšia je možnosť úspešnej konektivity.

Na základe takýchto aktivít sa rozvinula ďalšia komodita, a to wireless IDS (Intrusion Detection Systems), ktoré vedia vyhodnotiť prívaly alebo iné anomálie v kvalite bezdrôtového signálu.

Bezdrôtové siete boli pôvodne konštruované na obmedzenú veľkosť sietí a krátke vzdialenosti point-to-point prepojení. No v súčasnosti sa používajú aj pre korporátne siete. Na toto použitie sú však projektované bezpečnostné vlastnosti nedostatočné. Operačný mód bezdrôtových sietí je podobný ako pri eternete. Pretože radio transceiver môže v jednom okamihu buď vysielať, alebo len prijímať, bezdrôtové siete sú v zásade v režime half-duplex. Prístupový bod siete – access point – je bridge medzi bezdrôtovou časťou a „drôtovou", správa sa ako hub, čo uľahčuje sniffing. Z pohľadu riešenia kolízií je použitý algoritmus CSMA/CA (Carrier Sense Media Access/ Collision Avoidance) oproti klasickému eternetovému CSMA/CD (.../ Collision Detection). CSMA/CA je založený na pozitívnom ACK pre každý úspešný prenos. Ak sa ACK neprijme, prenos sa opakuje. Na pevných sieťach, keď sa zapojí kábel do zásuvky alebo aktívneho zariadenia, používateľ je so sieťou asociovaný. Na bezdrôtových sieťach to nie je možné, pretože ak access point stratí konektivitu, nasleduje vykonávanie asociácie, posielajú sa framy s požiadavkou a odpoveďou. V tomto období by mechanizmus CSMA/CD nefungoval.

Bluetooth môže fungovať v dvoch módoch: v circuit-switching (hlasová komunikácia) a packet-switching (TCP/IP). Pretože Bluetooth je relatívne nová špecifikácia (1999), myslí sa v špecifikácii aj na zabezpečenie. Pre záujemcov o podrobnejšie informácie o štruktúre komunikácie medzi bluetoothovými zariadeniami odporúčam *Robert Morrow: Bluetooth-Operation and Use* (McGraw-Hill Professional, 2002).

Najväčší problém s protokolmi bezdrôtových komunikácií na 2. vrstve, a to pre 802.11 a 802.15, je ten, že riadiace framy nie sú ani šifrované, ani autentifikované. Každý ich môže logovať, analyzovať a vysielať bez toho, aby bol asociovaný s cieľovou sieťou. Ešte raz upozorňujem, že hovorím o riadiacich framoch. Dajú sa z nich vyčítať informácie ako sieťová ESSID, adresa MAC bezdrôtového hosta, DSSS LAN číslo kanála, vzorka FHCC preskakovaných frekvencií atď. Aj Bluetooth vysiela jedinečné ID v textovom formáte. Na druhej strane informácie ponúkané v riadiacich framoch tvoria len nepatrnú časť celej komunikácie. No ten, kto pracuje s bezdrôtovými sieťami, vie, že prípad-

ný útočník môže poslať deautentifikačný a deasociačný frame. Následne možno umiestniť v sieti neautorizovaný AP a spoofingom skutočného AP (adresa MAC a IP) presmerovať prevádzku cez takýto AP.

Defaultná autentifikačná metóda v 802.11 bola open system authentication. To značí, že sa mohol prihlásiť každý, ak mal správny kanál a ESSID. Na dátové šifrovanie a autentifikáciu klientov pre štandardy 802.11a/b/g sa začal používať WEP (Wired Equivalent Privacy). WEP šifruje rétžiu a CRC symetrickým spôsobom cez RC4 (viac informácií na ***www.rsasecurity.com/rsalabs/faq/3-6-3.html***). Pôvodne bola veľkosť kľúča 64 bitov z dôvodu amerických exportných zákonov. Dnes sa používa 128-bitový kľúč. WEP môže byť použitý na autentifikáciu bezdrôtových hostov, ak je povolená metóda „ shared key authentication". Pri takejto autentifikácii vysiela AP na klienta výzvu. Klient odpovedá zašifrovaním výzvy a poslaním späť na AP. AP dešifruje výzvu kľúčom WEP a porovná ju s pôvodnou hodnotou. Ak sú zhodné, host je autentifikovaný. Dnes je známych viac bezpečnostných nedostatkov WEP. Problémy WEP sa dajú rozdeliť do dvoch kategórií:

1. správa kľúčov,

2. nedostatky šifrovania.

Bezpečná distribúcia šifrovacích kľúčov je všeobecný problém implementácie symetrického šifrovania. V pôvodnom návrhu WEP bol myslený pre ohraničenú veľkosť sietí, kde sa nikto nezamýšľal nad distribúciou kľúčov, pretože nebolo ďaleko ku každému bodu. Tento problém sa objavil až rozrastaním sietí, kde sa manuálna distribúcia stala problémovou. WEP vykonáva autentifikáciu orientovanú na zariadenia, nie na používateľov. Stratené alebo ukradnuté PDA alebo notebook znamená ohrozenie siete a nevyhnutné následné administrátorské zásahy.

Všetci používatelia na jednej sieti majú rovnaký kľúč WEP. Sniffing v bezdrôtových sieťach je preto jednoduchší ako v klasických. Menej skúsení čitatelia si to môžu vyskúšať známymi pomôckami, ako Hunt, Dsniff, Ettercap alebo iné, skúseným radiť netreba. A ešte jedna vec, používateľ vnútri siete môže byť rovnako nebezpečný ako vonkajší útočník, keďže AP je bridge, a nie router a používatelia zdieľajúci rovnaký kľúč WEP patria do rovnakej dátovej domény napriek tomu, že sieť môže byť rozdelená do viacerých IP podsietí alebo VLAN.

Nedostatky šifrovania spočívajú v tom, že „shared key" a 24-bitový inicializačný vektor (IV) sú prenášané po sieti nešifrované. V modernej kryptológii je navyše 24 bitov veľmi malé číslo. Rovnaký IV sa používa pre rôzne dátové pakety. Po pozbieraní dostatočného množstva framov s rovnakým IV môže byť identifikovaný „shared key".

Praktiky a odporúčania na zvýšenie bezpečnosti

V tomto odseku si povieme zatiaľ o základných odporúčaniach. Jedným zo základných spôsobov je filtrovanie adries MAC. Každé modernejšie zariadenie ho podporuje. Môže zastaviť útoky v angličtine označované ako „script kiddie" na asociáciu so sieťou. Dá sa však obísť, ak útočník vynúti deasociovanie hosta bez čakania na dobu, kým host príde do stavu off-line, pričom vie získať adresu MAC. V niektorých prípadoch pomôže filtrovanie protokolov, ale to väčšinou len v sieťach, kde sa napr. požaduje len prístup na web a k mailom. HTTPS, S/MIME a prípadne SSH môžu byť vhodnou náhradou. Odvtedy, ako sa stali zraniteľnosti WEP dobre známymi, wireless komunita sa začala opierať o štandard 802.11i.

Záujemcovia o podrobnejšie informácie môžu nalistovať databázu RFC a príslušné štandardy (***www.rfc-archive.org***).

Boli navrhnuté nové protokoly na šifrovanie prevádzky:

- **TKIP** (Temporal Key Integrity Protocol) sa považuje za upgrade WEP, ktorý rieši jeho známe bezpečnostné nedostatky. Používa 48 bitov dlhý IV, aby sa neopakovalo znovupoužitie a umožňuje miešanie IV, aby sa znížila možnosť vystopovania závislosti medzi šifrovanou správou a hodnotou kľúča. Takisto implementuje jednosmerný hash MIC (Message Integrity Code) namiesto málo bezpečného CRC-32. TKIP nie je povinný pri prevádzke v štandarde 802.11i, je spätne kompatibilný s WEP a nepotrebuje hardvérový upgrade. Spolu s 802.1x sa TKIP stal základom pre prvú verziu WPA (WiFi Protected Access), v súčasnosti aj vo verzii WPA2 sú najviac podporované väčšinou výrobcov.

- **CCMP** používa AES (Advanced Encryption Standard, Rijndael) šifrovanie. Dĺžka kľúča definovaného štandardom 802.11i je 128 bitov. Používa 48 bitov dlhý IV.

- **WPA2** (WiFi Protected Access 2) spočíva na metóde WPA, ale vykonáva silnejšiu ochranu dát a kontrolu sieťového prístupu. Prostrediu podnikovej sféry, ale aj spotrebným používateľom zaručí, že do bezdrôtovej siete bude mať prístup len autorizovaný používateľ. Vo WPA2 je implementované NIST (National Institute of Standards and Technology) FIPS 140-2 AES šifrovanie a autentifikácia založená na štandarde 802.1x. Existujú dve verzie WPA2, personal a enterprice. WPA2 personal chráni neautorizovaný sieťový prístup použitím set-up hesla, WPA2 Enterprice verifikuje sieťového používateľa pomocou servera. WPA2 je spätne kompatibilný s WPA. Tak ako WPA aj WPA2 je vytvorený na ochranu všetkých zariadení spĺňajúcich štandard 802.11 vrátane 802.11b/a/g.

Štandard 802.1x bol pôvodne vytvorený na implementáciu autentifikácie používateľov na druhej vrstve v klasických sieťach. V bezdrôtových sieťach môže byť 802.1x použité aj na dynamickú distribúciu kľúčov WEP. Asociácia medzi klientom a AP sa v bezdrôtových sieťach považuje za network access point a AP za autentifikátora, ktorý však potrebuje autentifikačný server. To môže spĺňať RADIUS server, doplnený vhodnou formou databázy používateľov, napr. natívny RADIUS, LDAP, NDS alebo Active Directory. Niektorí výrobcovia toto riešenie ponúkajú ako appliance.

Autentifikácia používateľov v 802.1x na druhej vrstve je vykonávaná pomocou EAP (Extensible Authentication Protocol, RFC 2284). EAP je zdokonalená náhrada CHAP na PPP. Existujú rôzne implementácie EAP. Najznámejšie sú:

- **EAP-MD5** je základná úroveň EAP, podporovaná zariadením vyhovujúcim 802.1x. Pretože EAP-MD5 nepodporuje serverovú autentifikáciu, je zraniteľný útokom využívajúcim pomoc neautorizovaného autentifikátora/autentifikačného servera. Takým je napr. útok zvaný *man-in-the-middle*.

- **EAP-TLS** je postavený na protokole SSLv3 a vyžaduje použitie certifikačnej autority. Windows XP podporuje štandardne tento spôsob. Podrobné inštrukcie ohľadom implementácie EAP-TLS nájdete na ***www.microsoft.com/WindowsXP/pro/techinfo/deployment/wireless/80211corp.doc***.

Na implementáciu v prostredí otvorených unixových systémov využite ***www.missl.cs.umd.edu/wireless/eaptls***.

EAP-LEAP je Cisco proprietárny EAP typ implementovaný v Aironetoch. Informácie sa nachádzajú na ***www.cisco.com/warp/public/707/accessregistrar_leap.html***. Podporuje aj posledné verzie FreeRADIUS, signalizujúc, že toto riešenie neostalo len riešením jedného výrobcu. Nanešťastie však EAP_LEAP používa modifikovaný MS-CHAPv2 s nezabezpečeným MD4 hashingom a slabé kľúče DES na posielanie výzvy a prijímanie odpovede bezdrôtového klienta. Preto odporúčam použiť v prípade implementácie skutočne silné heslá.

Iné, menej často sa vyskytujúce varianty EAP sú PEAP (Protected EAP) a EAP-TTLS (Tunneled Transport Layer Security EAP). EAP-TTLS podporuje niekoľko starších autentifikačných metód, ako PAP, CHAP, MS-CHAP, MS-CHAPv2 a EAP-MD5. Použitím EAP-TTLS bezpečným spôsobom vzniká tunel TLS, v ktorom fungujú staršie, menej bezpečné protokoly. EAP-PEAP je podobný na EAP-TTLS, ale nepodporuje PAP a CHAP. Obidva vyžadujú certifikát servera a kópia certifikátu servera je distribuovaná na klienta.

Medzi ďalšie odporúčania na zvýšenie bezpečnosti bezdrôtových sietí teda patrí náhrada WEP bezpečnejším spôsobom, správna autentifikácia používateľa v bezdrôtovej sieti a zavedenie detekcie prienikov na sledovanie abnormalít v prevádzke. O tomto poslednom odporúčaní si viac povieme v niektorom z ďalších článkov.

MILOSLAV ĎURČIK,
mdurcik@infoware.sk

Miloslav Ďurčík vyštudoval technickú kybernetiku na Technickej univerzite Ilmenau v Nemecku. V súčasnosti vedie spoločnosť RSN Systems, s. r. o.