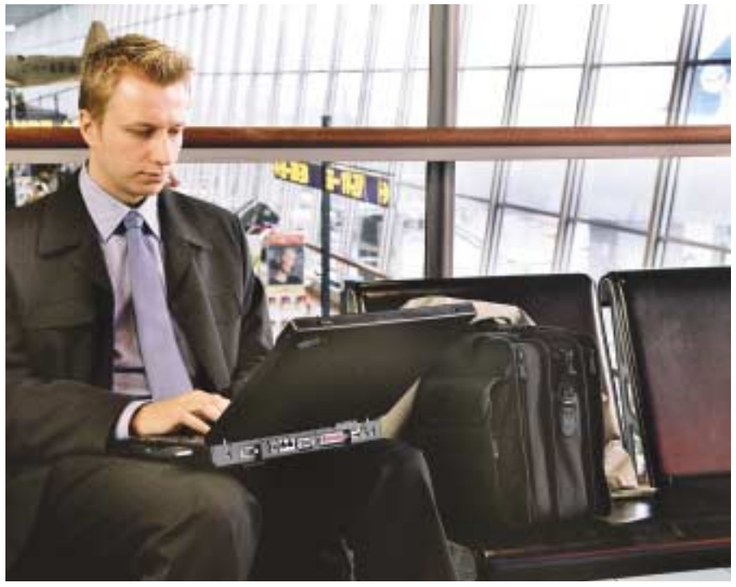
Chystáte se zahodit dráty?

Možnosti a úskalí bezdrátových sítí

PATRIK MALINA

Připojení „bezdrátem“ je skvělé! Nejste k ničemu připoutaní, Wi-Fi je už dostupné na letištích, v hotelech, restauracích a konferenčních místnostech. Sestavení domácí sítě je hračka a stojí to stejně jako s dráty. Prostě jasná volba. Ale prý je to nebezpečné, kdekdo může komunikaci odposlechnout. A také to prý není až tak rychlé, jak bychom potřebovali. Je to všechno pravda?



Pokud dnes říkáme, že používáme bezdrátové připojení, většinou bezděčně směšujeme širokou škálu technologií s různou využitelností, dostupností a technologickým zázemím. Než se pustíme do podrobnějšího výkladu, je žádoucí si ve věci udělat jasno a zřetelně vymezit hřiště, po němž se v tomto článku budeme pohybovat.

V případě komunikace na nejkratší vzdálenost většinou používáme řešení, jež bývají sdružována mezi tzv. „osobní sítě“ (Personal Area Networks, PAN). Jejich působnost bývá měřena na vzdálenost v řádu desítek centimetrů či několika málo metrů a využití bezdrátového přenosu je nasnadě, neboť natahování drátů pro tyto účely je prostě otravné. Jednou z nejproslulejších, prakticky dostupných technologií je Bluetooth, neboli „Modrý zub“, kompletní technologie postavená na využívání rádiových vln (podobně jako dále probírané Wi-Fi). Komunikačním portem tohoto druhu se dnes může pochlubit řada mobilních telefonů a přenosných či kapesních počítačů a odpovídající adaptér snadno zakoupíte i pro pracovní stanici, například pro rozhraní USB. Obdobným řešením je dále známý „infračervený“ přenos, realizovaný ve shodě s názvem pomocí elektromagnetického vlnění z oblasti spektra, jemuž běžně říkáme infračervené. I pro tento typ komunikace, zavedený pod označením IrDA, existuje slušně zavedené a rozšířené kompletní technologické řešení, takže se jedná o běžný typ přenosu například mezi notebooky či mobilními telefony. Přestože tyto komunikační kanály jsou zajímavé a splňují podmínky „bezdrátovosti“, nejedná se o řešení problematiky lokálních sítí v pravém smyslu slova, a proto jej dále do naší pracovní definice bezdrátových sítí nebudeme zahrnovat.

Na opačném konci stojí z hlediska dosahu využití bezdrátové konektivity k řešení problému tzv. poslední míle, tedy připojení účastnických stanic, resp. počítačů, k sítím poskytovatelů internetových služeb. I zde se přenos pomocí rádiových vln (opět viz dále Wi-Fi) prosadil, a to z rozličných důvodů: umožňuje poměrně svobodné budování i rozsáhlejších sítí, jejichž sestavení pomocí kabeláže by bylo finančně neúnosné (u nás např. CZFree.Net, jinak obecně tzv. komunitní sítě), ale též umožňuje komerčním poskytovatelům internetových přípojek překlenout poslední metry ke svému zákazníkovi tam, kde to prostě kabelem či telefonní přípojkou není možné (hádejte, proč je to u nás tak populární metoda...). Ani tato tématika, byť velmi zajímavá a dobrodružná, nebude tentokráte naším cílem, neboť jde často vlastně o druhotné využití technologií původně navržených pro lokální sítě.

Povídat si tedy budeme o komunikaci, jež svým dosahem zůstala „někde uprostřed“: v následujících kapitolách se zaměříme na současné možnosti a komplikace spojené s bezdrátovými lokálními sítěmi s typickými „dosahovými“ vzdálenostmi mezi řádově metry a desítkami metrů. Budeme tedy hovořit o řešeních, jež se snaží nahradit drtivě převládající ethernetovou technologii realizovanou pomocí kabeláže ve zhruba shodných dosazích (cca kolem stovky metrů) – jinými slovy, zaměříme se na praktické otázky kolem sítí typu Wi-Fi v úzkém slova smyslu. Pro účely tohoto článku tedy považujte za bezdrátovou síť tento typ komunikace, jenž v posledních letech zažil nebývalý rozmach.

> Pod pojmem bezdrátové připojení budeme v tomto článku chápat řešení, postavená na technologickém standardu známém jako Wi-Fi, určeném pro lokální sítě malého dosahu zhruba do 100 m. Podrobněji tuto problematiku řeší dále zmíněné normy IEEE 802.11b, IEEE 802.11g a související. Pro úvodní seznámení je možno navštívit stránky Wi-Fi Aliance na adrese www.wi-fi.com.

Co přesně řeší samotné Wi-Fi?

Pokud prakticky nepoučenému uživateli sdělíte cosi o chystaném přechodu na bezdrátovou síť, může to vyvolat všelijaké představy končící třeba obavou, že vše budeme muset odteď dělat jinak: posílat e-maily, stahovat soubory... Dost fantazie a hrůzy, popišme si přesně, co Wi-Fi vlastně zajišťuje.

Kolekce technologií a norem, zahrnutých pod více méně marketingové označení mírně zavádějícího charakteru Wi-Fi (od Wireless Fidelity, asi jako paralela s Hi-Fi) byla vyvinuta s jasným cílem nahradit kabeláž v oblasti lokálních počítačových sítí, tedy typicky uvnitř budov v dosahu několika desítek metrů. Cílem ani výsledkem v žádném případě není změnit způsob práce uživatelů, neboť příslušné technologie řeší tzv. 1. a 2. vrstvu síťového modelu. Srozumitelněji řečeno, Wi-Fi má nahradit kabeláž rádiovými vlnami tak, aby vše ostatní běhalo normálně, tedy asi jako byste v případě ethernetu vyměnili starší koaxiální kabely za nové v podobě kroucené dvojlinky. I proto se někdy Wi-Fi označuje jako bezdrátový ethernet, což navíc souvisí i s hlubšími aspekty tohoto řešení. Důsledkem uvedené skutečnosti je, že potřebujete zásadně odlišné síťové karty (adaptéry), neboť ty právě řeší onu „1. a 2. vrstvu“, příslušné ovladače pro vás operační systém, ale jinak aplikace pochopitelně běhají jako dosud.

> Standardy a technologie zahrnované pod průmyslové označení Wi-Fi se zaměřují na řešení tzv. první a druhé vrstvy síťového přenosu. V praxi to znamená, že jejich cílem je zastoupit provoz po kabelu, nikoliv však nahrazovat či měnit práci se sítěmi např. typu TCP/IP. Na aplikace či způsob uživatelské práce nemá zavedení bezdrátové infrastruktury v zásadě žádný významný vliv.

Protože Wi-Fi síťový adaptér je vlastně vysílačem a přijímačem s nezanedbatelným výkonem, je potřeba si ujasnit otázku licencování vysílacích frekvencí, neboť ty podléhají státní kontrole. Obrovskou výhodou při vývoji Wi-Fi byl fakt, že státní legislativa většiny zemí (včetně ČR) uvolnila pro tuto technologii frekvenci kolem 2,4 GHz (jde o pásmo určité šíře) podle speciální bezplatné generální licence: za využití se nic neplatí, ale nesmíte překračovat povolený vysílací výkon, takže zařízení musejí mít homologaci a měla by se chovat mravně. V mnoha mimoevropských zemích bylo pro stejný účel uvolněno i pásmo kolem 5 GHz, takže jsou k mání i zařízení pro tyto frekvence, ovšem zde se mějte na pozoru: evropská legislativa toto nepřipouští, neboť si pásmo drží pro vlastní očekávaný standard HiperLAN, čili dnes je využití pásma i u nás pro tento účel nepřípustné. Naštěstí se drtivá většina podobných komponent na náš trh ani příliš nedováží, takže při koupi v tuzemsku zřejmě nepochybíte.

Stručně řečeno, Wi-Fi technologie skutečně řeší nahrazení „kabelové“ fyzické a linkové vrstvy za vysílání víceméně volným prostorem, jež vám ušetří ono připojování konektorů a natahování drátů. To, co běžně využíváte, funguje tak, jak jste zvyklí.

Co je vlastně 802.11b a 802.11g?

Již výše jsme naznačili, že běžné označení Wi-Fi je víceméně průmyslovým či marketingovým standardem, což by technologům samozřejmě nestačilo, i když v praxi bylo založení stejnojmenné aliance pro rozvoj velmi zásadní. Řešení typických lokálních bezdrátových sítí je tedy přesněji popsáno pomocí norem standardizační organizace IEEE. Dvě výše zmíněná čísla označují dokumenty, jež popisují dnes nejvíce rozšířené varianty, známé právě jako typické Wi-Fi. A proč jsou vlastně dvě? Ve skutečnosti jsou alespoň tři... Ale postupně.

Norma 802.11b popisuje o něco starší standard, jenž je v podstatě první prakticky realizovanou normou pro Wi-Fi zařízení. Vyznačuje se především skutečností, že teoretická maximální přenosová rychlost je 11 Mb/s, což je srovnatel-

▲ **Nejnovější modely síťových adaptérů zvládají i komunikaci podle normy IEEE 802.11b, v případě přístupových bodů (AP) je samozřejmostí podpora obou norem pro zpětnou kompatibilitu.**

▶ **Nad zaváděním Wi-Fi technologií a inovací do praxe bdí průmyslová asociace Wi-Fi Alliance, jejímž přičiněním mimo jiné získaly bezdrátové lokální sítě toto pojmenování.**

né s nejpomalejší ethernetovou variantou po klasickém kabelu. Standard existuje od roku 1999 a první zařízení Wi-Fi, jež jsou dodnes ve většině, pracují právě podle něj. Nejen rychlost byla důvodem, proč se vývoj nezastavil: v červnu 2003 byla schválena norma 802.11g, jež mimo jiné nabízí teoretickou maximální rychlost 54 Mb/s, což je někde na půli cesty k dnes nejběžnějšímu ethernetu, jehož rychlost je 100 Mb/s. I zařízení dle této normy jsou již běžně dostupná, a co je veledůležité, většinou jsou zpětně kompatibilní s 802.11b typy. Jenže, něco za něco: pokud se v síti s mnoha „géčkovými" kartami objeví jedno „béčko", budou si sice rozumět, ale všechny „spadnou" na nižší normovanou rychlost, což je škoda. Standard, který nemůžete v tuzemsku využít díky nedostupnosti pásma kolem 5 GHz, je pak označován jako 802.11a: síťová zařízení s tímto označením nekupujte, nemá to u nás smysl.

Již jsme naznačili, že IEEE norem je vlastně více. Ty další už neřeší námi zmiňovaný problém, tedy přenos na úrovni fyzické a linkové vrstvy. Ale nebojte se, dojde na ně dále. Důležitým závěrem je fakt, že při koupi síťových karet si u nás momentálně můžete vybrat ze dvou standardů 802.11b a 802.11g a že oba dva jsou ve fázi praktického, běžného využívání.

Drtivá většina v tuzemsku dostupných zařízení standardu Wi-Fi jsou homologována podle dvou norem, 802.11b a 802.11g. Důležitou skutečností je, že novější „géčka" jsou řádově pětkrát rychlejší a v případě potřeby zpětně kompatibilní s „béčky". Tuzemská legislativa prozatím nedovoluje použití zařízení podle normy 802.11a, takže je v zahraničí „výhodně" nenakupujte.

Jistou potíž však způsobuje fakt, že ačkoliv se výrobci snaží normy zavádět co nejlépe, ne vždy se to bezezbytku podaří. Starší standard 802.11b je na trhu přece jen delší dobu a je to rozhodně znát na vzájemné kompatibilitě hardwaru, tedy karty a přípojné body (access pointy) různých výrobců jsou schopny spolu často bez obtíží komunikovat. Znatelně větší dobrodružství nastává v případě budování sítě podle novějšího standardu 802.11g. Ačkoliv výrobci dodávali na trh zařízení již před rokem před definitivním schválením normalizační komisí, i v současné době nelze než vřele před definitivním utracením peněz doporučit důkladné otestování plánované sestavy. Nejsou výjimkou případy, že ani dvě zařízení téhož výrobce si spolu pořádně nerozumí. Na druhou stranu, funkční kombinace rozhodně nalézt lze a stojí to za námahu.

Jak rychle to opravdu poběží?

Možnost volného pohybu s počítačem a plynulé připojování do sítě bez kabeláže je výhoda, za níž je potřeba někde zaplatit. Jedním z kritických parametrů je přístupová rychlost, kde stále přetrvává znatelný hendikep ve srovnání s natažený-mi dráty. Jak jsme již uvedli výše, bývá zvykem uvádět maximální teoreticky dosažitelnou rychlost u zařízení podle příslušné normy, což obzvláště v případě „géčka" vyvolává dojem, že nejsme tak daleko třeba za běžným ethernetem na 100 Mb/s. Je však potřeba se na věci podívat střízlivě a říci na rovinu, že tak růžové to není.

V první řadě, u bezdrátových spojů vstupuje do hry fakt, jenž se u kabelových variant běžně nevyskytuje: v případě horší dostupnosti signálu mezi rádiovými stanicemi dojde k řízenému „přeskoku" na nižší přenosovou rychlost, jež je v dané chvíli možná. V praxi to znamená, že při větší vzdálenosti (třeba přes 20 m) či při zastínění (stačí kvalitní kovová zárubeň) okamžitě maximální rychlost v závislosti na oslabení signálu poklesne, a to dosti rapidně, třeba o polovinu či čtvrtinu.

Druhou zásadní skutečností je způsob, jak uživatelé sdílejí rádiové pásmo. Pokud je skupina příjemců připojena na stejný přístupový bod a nacházejí se tak fyzicky na jednom síťovém segmentu, což je typický případ, musejí se o kapacitu linky podělit stejně, jako tomu bylo v období raného ethernetu, jenž přežívá dodnes v podobě sdílení linky pomocí obyčejného rozbočovače (hubu). Účastníci komunikace se tedy vlastně přetlačují o vysílací prostor a při řešení vzniklých kolizí tak dochází k dalšímu výraznému snížení přenosového výkonu, jako u ethernetu bez přepínačů (switchů). Mezních hodnot lze tak dosahovat pouze při bezprostředním přiblížení bezdrátových síťových karet a při komunikaci „jeden na jednoho".

Třetí významnou skutečností, u níž se pozastavíme, je nezbytné vyplýtvání přenosové kapacity na nutnou režii protokolů vyšších vrstev. Jednoduše řečeno, když posíláte dopisy, i ta obálka něco váží a poštovní auto či letadlo musí unést nejen vaše čisté myšlenky v podobě milostného psaní, ale též onen fyzický nosič v podobě papíru, obálku, známku a třeba i velké poštovní pytle. Na první pohled to vypadá zanedbatelně, ale ve skutečnosti ona režie na protokoly vyšších vrstev představuje významnou poměrnou část a skutečná šíře pásma, určená pro čistá data, tak opět povážlivě klesá.

▲ **Ačkoliv i operační systém vám ukáže při navázání spojení nominální rychlost technologie, s níž pracujete, s takto vysokou rychlostí v praxi nepočítejte.**

Normovaná maximální rychlost zůstává v reálných sítích spíše těžko dostižným ideálem. Za běžných situací dochází k poměrně častému rušení signálu a režie přenosu si také „vyžádá" svůj podíl, a proto je skutečná rychlost většinou nejvýš poloviční oproti deklarovanému maximu, často bohužel i nižší. Významným faktorem je zde samozřejmě počet současně připojených uživatelů.

Když si výše uvedené skutečnosti shrneme, je nasnadě, že teoretických maximálních kapacit nelze dosáhnout. Počítejte v praxi s tím, že za velmi dobrých podmínek se maximální šířka pásma pro užitečný datový náklad pohybuje někde kolem poloviny nominálních hodnot, tedy asi 5 Mb/s u „béčka" a 25 Mb/s u „géčka", při zhoršení podmínek (typicky stínění) bývá mnohem hůř! Připomeňme, že při použití kabeláže lze dnes pomocí běžné výbavy pro „stovkový ethernet" dosáhnout v přepínané síti, jež obsahuje switche, přenosy poměrně blízké teoretickému maximu. A to především proto, že když na jeden drát připojíte na každém konci jeden adaptér, tak vám zkrátka nikdo přenos narušovat nebude, což v éteru nemáte šanci stoprocentně zařídit.

Je lepší používat přístupový bod?

Tradiční sítě Wi-Fi nabízejí při svém provozu plně v souladu s původním návrhem dva režimy propojení účastníků komunikace. První z nich je označován jako „ad hoc" a jedná se vlastně o náhodné propojení typicky dvou komunikujících počítačů pomocí Wi-Fi přenosu. Velkou výhodou je zde skutečnost, že nepotřebujete kromě klientských síťových adaptérů žádný další hardware, spojení mezi koncovými body vzniká velmi snadno (až nebezpečně snadno) a spojení i rozpojení je podle potřeby snadné. Velmi jednoduše tak můžete například pohotově přenášet soubory. Zásadní nevýhodou je skutečnost, že se takto můžete „asociovat" do bezdrátového sbratření s kýmkoliv, kdo se vyskytne v dostatečné blízkosti, aniž byste o to měli zájem, z čehož plyne poměrně vysoké riziko.

▶ **Přístupové body (AP) kromě základní funkce – připojení bezdrátových klientů do síťové infrastruktury – nabízejí řadu dalších možností, jako napojení na internetovou linku (WAN) a routování, ochranu sítě firewallem či připojení více ethernetových portů.**

V zásadně odlišném režimu pracuje tzv. infrastrukturní mod, jenž právě vyžaduje onu komponentu, označovanou jako „ápéčko", tedy přístupový bod neboli access point. Ten pracuje jako prostředník, za jehož účasti komunikují všichni přítomní tím, že přes něj proudí všechny datové toky mezi klienty sítě. Jeho použití má především tu výhodu, že lze podle možností nastavení filtrovat či kontrolovat provoz, včetně zpřístupnění sítě různým klientům. Na straně uživatele pak dochází k přepnutí síťového rozhraní do tohoto režimu, což zaručuje eliminaci náhodných pokusů o sestavení ad hoc spojení – veškerý tok musí směřovat na AP, což síť může zásadně ochránit.

Přístupový bod není rozhodně nutný, pokud považujete bezdrátové spojení například za příležitostný mechanismus propojení dvou zařízení. Na druhou stranu, budujete-li byť malou domácí síť s více než dvěma účastníky či hodláte sdílet třeba internetovou konektivitu do prostoru domácnosti či malé kanceláře, bez přístupového bodu se neobejdete a získáte tím značné možnosti zabezpečení. V neposlední řadě ve prospěch přístupového bodu hovoří skutečnost, že tuto funkci dnes řada výrobců slučuje do „krabiček", jež následně slouží také jako router, přepínač pro kabelový ethernet a typicky též modem pro některé z širokopásmových internetových připojení (ADSL, kabelový internet apod.).

Přístupový bod (access point, AP) je komponenta, jež umožňuje provozovat bezdrátovou infrastrukturu v pokročilejším, tzv. infrastrukturním režimu. Nabízí lepší řízení, pokročilejší možnosti zabezpečení a vzhledem k cenové dostupnosti AP zařízení je vhodný i pro malé, domácí sítě.

Na kolik že taková síť přijde?

Pokud jste dosud žili v představě, že sestavení bezdrátové sítě je cosi luxusního a v porovnání s klasickým ethernetem po drátu též nevkusně rozmařilého, tak jste, s odpuštěním, zaspali dobu. Pořízení základních dostatečně výkonných komponent je cenově srovnatelné s kabelovou variantou a výběr je bohatý.

Koupě základního kamene, tedy síťové karty pro jeden počítač, vás přijde podle provedení na necelých 1 000 Kč u nejlevnějších variant pro normu 802.11b. K mání jsou varianty interní pro PCMCIA sloty či externí typicky pro USB rozhraní a za 3 000–4 000 Kč již můžete získat špičkové karty pro rychlejší standard 802.11g. Budujete-li „pořádnou" síť, jež si žádá přístupový bod (AP), počítejte podle výbavy s cenou od zhruba 2 000 Kč výše. V případě pořízení kombinovaného zařízení, jež bude zahrnovat například router (směrovač) mezi sítěmi a také přepínač ní. Na druhou stranu, budujete-li byť malou domácí síť s více než dvěma účastníky či hodláte sdílet třeba internetovou konektivitu do prostoru domácnosti či malé kanceláře, bez přístupového bodu se neobejdete a získáte tím značné možnosti zabezpečení. V neposlední řadě ve prospěch přístupového bodu hovoří skutečnost, že tuto funkci dnes řada výrobců slučuje do „krabiček", jež následně slouží také jako router, přepínač pro kabelový ethernet a typicky též modem pro některé z širokopásmových internetových připojení (ADSL, kabelový internet apod.).

Cena již rozhodně není při volbě bezdrátové sítě limitujícím faktorem. Komponenty lze zakoupit za srovnatelných podmínek, jako v případě klasických ethernetových řešení.

pro zapojení další infrastruktury pomocí ethernetového kabelu, očekávejte ceny mezi 2 000 a zhruba 6 000 Kč podle možností a výrobce. V případě, že stávající možnosti potřebujete rozšířit, bude jednou z komponent zřejmě externí anténa. Použitelné zařízení tohoto druhu pořídíte rovněž od zhruba 2 000 Kč nahoru.

Z výše uvedených údajů je patrné, že sestavení bezdrátové sítě není ve srovnání s kabelovými sourozenci nijak závratně drahé a jde o zcela srovnatelné řešení, tedy alespoň z hlediska nákladů.

Někteří výrobci a dodavatelé Wi-Fi zařízení

SMC *www.compexdata.cz/produktsmc.phtml*
D-Link *www.dlinknet.cz*
Edimax *www.edimax.com*
Linksys *www.linksys.com*
Proxim *www.proxim.com/products/wifi*
U.S.Robotics *www.usr-emea.com/products/p-networking-menu.asp?loc=czec*
Belkin *www.belkin.com*
Planet *www.planet.com.tw*
Proxim*www.proxim.cz*

▲ Základním rysem bezdrátových sítí je skutečnost, že přenosový kanál může kdokoliv nejen objevit, ale při nedostatečné ochraně rovnou použít. To se vám u kabelového rozvodu tak snadno nestane.

Je Wi-Fi náchylnější k útokům než ethernet?

Poměrně velké publicity se dostalo sítím Wi-Fi v dosti nelichotivých souvislostech, neboť již od počátku používání bylo zřejmé, že jsou poměrně náchylné k řadě útoků a narušení bezpečnosti. Zde je na místě upozornit, že jde částečně o nepochopení, v čem nebezpečí vězí, a proto se na problém podíváme blíže.

Hlavním principem jak ethernetu, tak Wi-Fi zařízení je v zásadě sdílení přenosového média. V případě kabelů je však mnohem obtížnější se k přenosové lince dostat a „napíchnout" se za účelem odposlechu. Útočník by zkrátka musel najít nechráněný port na rozbočovači (hubu), přepínači (switchi) či například v kanceláři v podobě síťové zásuvky. A to je mnohem obtížnější než v případě „bezdrátu", i když samozřejmě stále možné. U Wi-Fi přenosů není datový tok vázán na pevný, spoutaný drát, a proto lze volně „ze vzduchu" přenosy vylovit a pokusit se o odposlech. V zásadě je tedy nebezpečnost potenciálně stejná: když se vám někdo dostane k ethernetové přípojce, může napáchat stejnou škodu jako útočník proti Wi-Fi, neboť ethernet není ve své podstatě také nijak chráněn proti odposlechu a ten lze rutinně provádět. U Wi-Fi přenosů tedy prostě nelze spoléhat na to, že vás nikdo „nenapíchne", neboť „volné zásuvky" jsou všude ve vzduchu kolem vašeho zařízení, a to při dobré anténě útočníka i ve vzdálenosti několika stovek metrů.

Je třeba tedy říci, že bezdrátové sítě skutečně náchylnější na odposlech být mohou, ovšem jen a pouze proto, že jejich tvůrci ignorují základní principy a podceňují související nebezpečí.

Rozlišujte mezi autentizací a šifrováním

Jedním z problémů, jenž zůstává při budování bezpečných bezdrátových sítí často nepochopen, je zabezpečení dvou v podstatě nezávislých mechanismů: ověření účastníka komunikace (autentizace) a šifrování přenášených užitečných dat. Možná způsobila zamlžení této problematiky samotná implementace první podoby prakticky použitelného Wi-Fi, neboť tam se pro realizaci obou činností mimo jiné používá mechanismus WEP. Protože se jedná o důležité funkce, pozastavíme se u nich blíže.

Autentizace neboli ověření uživatele, resp. účastníka komunikace má zajistit, že se ve vaší bezdrátové síti neobjeví nikdo, kdo tam nemá co dělat. Ačkoliv je to velmi zásadní, řada uživatelů tento mechanismus podceňuje a vůbec nepoužívá, případně ve velmi omezené podobě. Původní podoba Wi-Fi totiž nabízí dvě možnosti, z nichž první, příznačně nazývaná open-system, v podstatě pracuje podle hesla „přijď a snadno se k nám připoj". Druhá možnost využívá silnější mechanismus v podobě vynucení tzv. sdíleného klíče (přesněji možná ověřovacího tajemství

▲ I konfigurace v operačním systému Windows XP vám napovídá, že autentizace a šifrování přenosu dat jsou dva nezávisle konfigurovatelné parametry.

či kódu), jehož podobu musejí znát obě komunikující strany, jinak k asociaci (navázání spojení) mezi bezdrátovými adaptéry nedojde. Právě tato silnější varianta je chráněna mechanismem WEP, jenž nabízí alespoň nějakou šifru, ovšem pohříchu je využíván pramálo.

Za mnohem důležitější považují uživatelé obecně šifrování samotného obsahu přenášených dat. Připojení nežádoucího účastníka se většinou nebojíme, vyzrazení obsahu už ano. V základní variantě Wi-Fi je opět použit mechanismus WEP, jenž nabízí pro tento účel mírně problematickou šifru RC4 s poměrně krátkými klíči (40 či 104 bitů). Největší bolestí, jak si ještě řekneme dále, je skutečnost, že klíče není možné

Procesy ověření uživatele a šifrování přenášených dat jsou dvě zcela odlišné procedury, jež lze realizovat různými postupy. Ochranu přenášených informací lze zajistit i zcela jinými technologiemi, než jaké nabízí Wi-Fi, třeba klasickým aplikačním šifrováním (PGP, S/MIME, SSL) či na úrovni síťové vrstvy (IPSec).

automaticky během komunikace obměňovat na obou stranách a uživatelé to musí provádět ručním nastavením. V současné době byly možnosti šifrování dat posíleny díky implementaci standardu WPA (viz dále) a také prodlužováním šifrovacích klíčů z iniciativy výrobců zařízení, takže lze běžně použít například 256 bitový, průběžně automaticky vytvářený a dojednávaný klíč.

Zásadním faktem zůstává, že procedury autentizace a šifrování obsahu jsou nezávislé a je potřeba řešit oba problémy: do vaší sítě by se neměl připojovat nikdo neoprávněný a rovněž citlivý obsah není ničím, co by měli cizí uživatelé spatřit.

Lze klíče mechanismu WEP snadno rozluštit?

Jednou z často zmiňovaných slabin původního návrhu bezdrátových přenosů pomocí technologie Wi-Fi je možnost šifrování pomocí postupu označovaného jako WEP (Wireless Equivalent Privacy). Tato technologie byla navržena jako víceméně provizorní ochranná výbava a poměrně brzy se přišlo na to, v čem spočívají její zásadní slabiny, jichž je několik. U řady Wi-Fi zařízení je WEP dosud jediným ochranným prostředkem a pokud nemáte na výběr jiný postup, je potřeba tuto možnost využívat co nejlépe.

Z praktického hlediska nás budou zajímat pouze některé aspekty, jež můžeme ovlivnit. Základní provedení šifrování WEP nabízí dvě délky klíčů, a proto je potřeba vždy zvolit tu vyšší, abychom byli schopni lépe odolávat případným pokusům o útok. Druhou zásadní okolností je fakt, že klíč (přesněji vámi zvolená fráze) zůstává po zadání neměnný do té doby, než ho sami nezměníte, a to na obou stranách zabezpečeného kanálu. A dlouhodobé používání stejného klíče znamená smrt pro téměř každou šifru, tedy pro WEP určitě. Pokud bude chtít potenciální útočník vaši šifru zlomit, velmi mu to usnadníte tím, že klíč nebudete měnit. K definitivnímu průlomu je totiž potřeba odchytit dostatečné množství dat, jež byla šifrována stejným klíčem, a to může trvat i desítky hodin či několik dnů, kdy je nutně průběžné přenosy odposlouchávat. Pokud si zvyknete jednou za dva až tři dny klíč k šifře WEP měnit, nesmírně tím zvýšíte své šance na ochranu síťového přenosu. Pokud by se útočníkovi přece jen podařilo klíč odhalit, bude mu po několika hodinách či málo dnech k ničemu, pokud budete důslední.

Šifru WEP lze skutečně reálně prolomit, ovšem za příznivé souhry okolností. Útočník mu-

sí být vybaven vyhovující bezdrátovou kartou, jež si rozumí s potřebným softwarem (náklady cca 4 000–6 000 Kč), dále kvalitní anténu pro případný dálkový odposlech (kolem 5 000–6 000 Kč) a programem (bezplatně, open source), jenž vše zařídí. Ze strany uživatelů je potřeba určité „vstřícnosti": velmi pomůže volba slabšího klíče WEP s kratší délkou, jeho již zmíněná neměnnost

▲ Prvním předpokladem k úspěšnému útoku na jakoukoliv bezdrátovou síť je její nalezení a zevrubné prozkoumání. Skvělým nástrojem pro tyto účely je NetStumbler, dostupný zdarma na internetu.

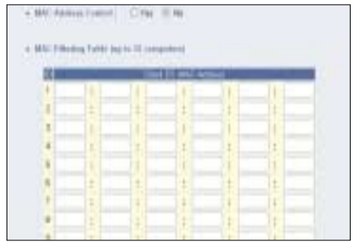
Mechanismus WEP, poskytující základní šifrování pro Wi-Fi, není kdovíjak silným nástrojem. Zajištění maximální bezpečnosti vyžaduje velké administrátorské úsilí a v rozsáhlejších sítích se jedná téměř o nerešitelný problém, pokud nepoužijeme jiné pokročilejší možnosti.

po delší dobu a také silný provoz, generující velké množství jednotek přenosu (paketů), neboť úspěšnost prolomení závisí právě na počtu paketů, jež má útočník k dispozici. V praxi to pak znamená několik hodin až málo dnů odposlechu, jež vás mohou ohrozit. Tedy šifru úspěšně prolomit lze, ovšem je možné se tomu alespoň nějak účinně bránit.

Je filtrování MAC adres dostatečné?

Protože ověřování účastníků připojujících se do bezdrátové infrastruktury bylo dosti problematické, rozhodli se výrobci zařízení zavést zajímavý mechanismus, jehož možnosti jsou s dílčími úspěchy využívány i jinde. Bývá označován jako filtrování MAC adres a protože kolem něj panují některé nejasnosti, vysvětlíme si jeho princip.

Vtip tohoto řešení spočívá ve faktu, že každý účastník komunikace v lokální síti (nejen bezdrátové, ale i ethernetové) je vybaven jedinečnou informací, jejíž použití je pro zdárný síťový



▲ Filtrování MAC adres je jednoduchý mechanismus, založený na prostém porovnávání seznamu s údaji o přistupujících počítačích. Jeho použití patří k dobrému zvyku. Současná zařízení tuto funkci běžně nabízejí.

přenos nezbytné. Číslo, označované jako MAC adresa (Media Access Control), slouží ke vzájemné komunikaci síťových adaptérů na linkové vrstvě, a to jak v případě Wi-Fi, tak na ethernetu (síťové IP adresy či jména počítačů jsou využívána až druhotně pro jiné účely). Podle platných dohod je MAC adresa jedinečné číslo (v celém vesmíru) a každý zakoupený adaptér tedy bezděčně disponuje nezaměnitelným identifikátorem.

Filtrovací procedura spoléhá právě na fakt, že klient má svou MAC adresu pevně přidělenu, neboť ta je typicky napevno „vypálena" v čipu adaptéru a při snaze o datový přenos ji musí poskytnout. Při konfiguraci tedy zadáme na přístupovém bodu bezdrátové sítě do tabulky povolené MAC adresy, příslušející oprávněným počítačům, ostatní účastníci budou považováni za nežádoucí. Ačkoliv je takto vše jasné a v praxi často i poměrně účinné, celá věc má háček, či spíše hák: s MAC adresou při komunikaci pracuje operační systém a jeho prostřednictvím lze svou MAC identifikaci záměrně změnit. Pomocí jednoduchého programku tedy může útočník vnutit svému systému jiné MAC označení, čímž bude původní hodnota z adaptéru potlačena, a vydávat se tak za legálního účastníka sítě.

Filtrace MAC či hardwarových adres je metoda, jež může mírně posílit zabezpečení vaší infrastruktury, ovšem pouze v součinnosti s dalšími postupy. Sama o sobě je poměrně bezzubým mechanismem, který lze snadno obejít.

Ačkoliv je tedy podvržení MAC adresy možné, doporučujeme používání jejich filtrace. Sám o sobě je sice tento ochranný mechanismus napadnutelný a prolomitelný, avšak v kombinaci s ostatními možnostmi alespoň mírně posiluje ochranu. Útočník totiž musí při průzkumu sítě mimo jiné vhodné MAC adresy vypátrat a případně vyzkoušet, což mu lze rovněž ztížit, a jakékoliv významné zdržení představuje zisk pro legální uživatele.

Co dokáže ochrana pomocí WPA?

V předchozích odstavcích jsme se již pozastavili nad problémy, jež jsou spojeny se snahou o zabezpečení bezdrátové komunikace. Zcela nové možnosti vnáší do této oblasti implementace technologie WPA, s níž se již dnes můžete běžně setkat, a proto si řekneme o jejích výhodách více.

Bezpečnostní řešení WPA neboli Wi-Fi Protected Access vzniklo jako reakce Wi-Fi Aliance na známé bezpečnostní problémy, jež tížily uživatele a správce sítí, a lze je víceméně označit jako „z nouze ctnost". Protože standardizační instituce IEEE pracovala již dlouho na nové normě pro zásadní posílení bezpečnosti a konec byl v nedohlednu, rozhodly se zúčastněné firmy pro zásadní krok: z nově připravované komplexní normy si Wi-Fi Aliance vypůjčila některé užitečné části a definovala „prozatímní" průmyslový standard, označený právě jako WPA, po němž výrobci rychle sáhli a začali jej zavádět do svých zařízení, takže je dnes téměř samozřejmostí. Pro úplnost dodejme, že schválení uvedené – rozsáhlé bezpečnostní normy IEEE 802.11i bylo v době psaní článku na spadnutí a ve chvíli, kdy toto čtete, jde zřejmě již o schválenou normu.

Zavedení WPA řeší některé zásadní potíže původního návrhu Wi-Fi sítí. Velmi zajímavou vymožeností je průběžná automatická výměna dynamicky vytvářených klíčů pro šifrovací proceduru, což řeší výše zmíněnou zásadní slabinu v podobě zapisovaní statických klíčových frází. Pro tu-

▲ Použití technologie WPA přináší značné posílení zabezpečení, a to jak při ověřování, tak při šifrování přenosu dat. Zvolíte-li například ve Windows XP ověření pomocí WPA se sdíleným klíčem, zpřístupní se vám i možnost použití silnějších šifrovacích postupů.

Poměrně nový standard WPA dovoluje zásadně posílit bezpečnost bezdrátové komunikace. Protože již přes rok je součástí např. klientských operačních systémů Microsoftu, nesmlouvavé žádejte při koupi nových hardwarových komponent tuto funkcionalitu a důsledně ji ihned při nasazení otestujte, obzvláště s ohledem na kompatibilitu s dalšími strukturami v síti.

to činnost je v rámci WPA použit protokol TKIP (Temporal Key Integrity Protocol), jenž byl právě „zapůjčen" z chystané normy 802.11i. Jeho práce je v zásadě prostá: v případě, že šifrujete bezdrátový přenos, kontroluje počet zaslaných paketů s daty a po určitém počtu provede z bezpečnostních důvodů výměnu nových klíčů mezi účastníky komunikace a koloběh může pokračovat. Potenciálnímu útočníkovi tak chybí to nejdůležitější – dostatečné množství dat šifrovaných stejným způsobem, což jeho možnosti značně oslabuje.

Druhým zajímavým vylepšením, s nímž při praktické implementaci WPA tvůrci zařízení přišli, je zvětšení délky klíče pro používané šifrování na hodnotu až 256 bitů. Jedná se o řádově zcela jinou úroveň, než v případě původní technologie WEP. Přínos pro zabezpečení je dosti zásadní.

Potřebuji k něčemu protokol 802.1x?

Při popisu použití novější bezpečnostní technologie WPA jsme se zmínili rovněž o protokolu 802.1×, jeho význam je pro bezpečné provozování bezdrátových sítí zcela zásadní. Na jedné straně se jedná o dobrou možnost, jak bezpečnost síťové infrastruktury celkově výrazně zvýšit, na straně druhé jej není jednoduché nasadit, neboť je pro to potřeba zajistit odpovídající podmínky. Podívejme se blíže, co nám nabízí a co od nás jeho zavádění žádá.

Protokol 802.1× byl definován již dříve a se samotným bouřlivým vývojem Wi-Fi sítí není nijak těsně spjat. Tvůrci pokročilých bezdrátových řešení však v pravou chvíli rozpoznali jeho potenciál pro komunikaci v éteru a přijali jej takřka za svůj. Jedním z úkolů protokolu je umožnit ověření (autentizaci) připojujícího se klienta, a to v zásadě v jakékoliv lokální síti (ethernet, Wi-Fi) na úrovni tzv. linkové vrstvy. Jednoduše řečeno to znamená, že pokud se pomocí bezdrátové či ethernetové síťové karty budete snažit připojit do stávající infrastruktury, jako první reakci obdržíte výzvu pro zaslání ověřovací informace. Pokud tak učiníte a budete rozpoznáni jako oprávnění uživatelé, kabelem či éterem vám bude umožněna komunikace a zapojení do síťových struktur. Pakliže se prokázat nedokážete, dojde k zablokování síťového přístupu, a to právě na úrovni oné linkové vrstvy, což je zcela zásadní: v praxi to znamená totéž, jako by vás někdo odpojil od síťové zástrčky nebo odstínil od přístupového bodu, protože s neověřenými klienty se nekomunikuje a přístupový port se jim fakticky uzavře. Zůstává jediná možnost: zaslat platné přihlášení a pak se připojit.

Kromě popsané schopnosti dokáže protokol 802.1× realizovat i další důležitý úkol, kterým je distribuce klíčů pro šifrování síťového provozu. O nebezpečí statického, v čase neměnného klíče jsme se zmínili již v části o WEPu, takže je zřejmé, jak je pravidelná automatická distribuce šifrovacích klíčů důležitá. V rozsáhlejším prostředí je prakticky vyloučeno, aby administrátoři zajistili v dostatečně krátkých intervalech pravidelnou obměnu ručně zadávaných klíčů a jejich dynamická výměna znamená pro mnoho typů útoků principiální bariéru. I tato funkce protokolu 802.1× je tedy dobrým argumentem pro jeho nasazení.

Význam použití protokolu 802.1× byl velmi rychle doceněn, a proto byl implementován do průmyslových výrobků mimo jiné jako součást či podmnožina technologie WPA, o níž byla výše řeč. Jeho použití však vyžaduje pokročilejší síťovou infrastrukturu, takže nasazení je téměř výhradně myslitelné ve větších, typicky firemních sítích. Onou zásadní podmínkou, jíž musíte splňovat, je dosažitelnost funkčního serveru služby RADIUS. Drobný problém spočívá totiž v tom, že

▲ Ověřování a distribuce tajných informací pomocí protokolu 802.1x patří prozatím k tomu nejsilnějšímu, co z hlediska zabezpečení můžeme použít. Jak je z obrázku patrné, pro sestavení infrastruktury je nezbytný server se službou RADIUS.

Zajímavé zdroje na internetu

Wi-Fi Alliance
www.wi-fi.com
Zdroj zajímavých materiálů
wireless.ittoolbox.com
Stránky s řadou zajímavých článků
www.wi-fiplanet.com
Stránky Microsoftu o Wi-Fi ve Windows
www.microsoft.com/wifi
Výborné univerzitní stránky s technickými informacemi
www.kjhole.com/Standards/Intro.html
Weblog Patricka Zandla
www.marigold.cz

du, protože s neověřenými klienty se nekomunikuje a přístupový port se jim fakticky uzavře. Zůstává jediná možnost: zaslat platné přihlášení a pak se připojit.

Kromě popsané schopnosti dokáže protokol 802.1× realizovat i další důležitý úkol, kterým je distribuce klíčů pro šifrování síťového provozu. O nebezpečí statického, v čase neměnného klíče jsme se zmínili již v části o WEPu, takže je zřejmé, jak je pravidelná automatická distribuce šifrovacích klíčů důležitá. V rozsáhlejším prostředí je prakticky vyloučeno, aby administrátoři zajistili v dostatečně krátkých intervalech pravidelnou obměnu ručně zadávaných klíčů a jejich dynamická výměna znamená pro mnoho typů útoků principiální bariéru. I tato funkce protokolu 802.1× je tedy dobrým argumentem pro jeho nasazení.

Význam použití protokolu 802.1× byl velmi rychle doceněn, a proto byl implementován do průmyslových výrobků mimo jiné jako součást či podmnožina technologie WPA, o níž byla výše řeč. Jeho použití však vyžaduje pokročilejší síťovou infrastrukturu, takže nasazení je téměř výhradně myslitelné ve větších, typicky firemních sítích. Onou zásadní podmínkou, jíž musíte splňovat, je dosažitelnost funkčního serveru služby RADIUS. Drobný problém spočívá totiž v tom, že protokol 802.1× dokáže přenášet od klientů ověřovací informace a vracet jim rozhodnutí, ale sám se nedokáže nikoho přímo zeptat, zda ten či onen uživatel do sítě patří. To za něj právě musí udělat služba RADIUS: je to její specialita, takže to umí velmi dobře, navíc dokáže zajistit i další služby kromě ověřování. Zprovoznění služby RADIUS rozhodně není začátečnické téma a navíc s sebou nese potřebu provozování síťového serveru a případně další dodatečné náklady, takže se vyplatí spíše v rozsáhlejším prostředí. Přestože by se nám protokol 802.1× hodil i v malých sítích, s jeho jednoduchým použitím z výše uvedených důvodů příliš nepočítejte. Naopak v rozsáhlejších sítích jej lze považovat za velmi významný prvek ochrany.

Posílení zabezpečení pomocí protokolu 802.1× je dnes jednou z nejsilnějších možností, jaké máme. Jeho nasazení má své opodstatnění, ovšem díky požadavku na běžící službu RADIUS pro ověřování klientů je její místo především v rozsáhlejších, většinou firemních sítích.

Shrnutí

Bezdrátové sítě typu Wi-Fi dnes představují dobře zvládnutou technologii, jež nabízí řadu zajímavých možností tam, kde nasazení klasické ethernetové kabeláže není možné. Ačkoliv absolutní srovnání rychlosti přenosu prozatím jasně vyhrává kabel, pokud jej nechcete, máte k dispozici spolehlivou a životaschopnou alternativu, jíž se nemusíte obávat. Náklady na vybudování bezdrátové lokální sítě nejsou oproti ethernetu nijak vyšší a možnosti zabezpečení je možné v současné době označit za mírně uspokojivé se světlejší budoucností. Správa malé domácí bezdrátové sítě rozhodně není nad síly přiměřeně pokročilých uživatelů a jejího sestavení se není třeba obávat. V případě, že používáte běžně přenosné počítače, je použití Wi-Fi více než vhodnou vymožeností. 4 0363/FEL ❑