Bezdrátová síť Fakulty informatiky

Luděk Matyska, FI a ÚVT MU

Vidina možného využití bezdrátových technologií v prostorech MU, kterou byl zakončen půl roku starý příspěvek o mobilním počítání [1], se koncem roku 2001 stala skutečností. Fakulta informatiky MU nechala v prostorách budovy na Botanické 68a instalovat celkem 14 přístupových bodů s nástěnnými anténami. Radiovým signálem (je použit systém podle normy IEEE 802.11b, tedy s maximální přenosovou kapacitou 11 Mb/s) jsou pokryty všechny volné prostory v nadzemní části budovy včetně vnitřního átria, všechny posluchárny, pracoviště odborných laboratoří a významná část kanceláří pedagogů. Instalace sleduje dva základní cíle:

- Zpřístupnit Internet co největšímu počtu studentů a pro tento účel využít jak „hluché“ veřejné prostory budovy, v nichž nelze instalovat standardní drátové přípojky, tak i volné, přednáškami v daném období neobsazené posluchárny.
- Otevřít prostor pro nové styly práce, a to jak studentů samotných, tak i při vlastní pedagogické a výzkumné práci. Bezdrátové připojení umožňuje v principu např. tvorbu ad-hoc skupin, které se mohou scházet prakticky na libovolném místě fakulty (např. ve volné posluchárně) a pracovat společně na nějakém problému, který vyžaduje trvalé připojení k Internetu.

1 Zpřístupnění a bezpečnost provozu

Zprovoznění bezdrátové sítě vyžaduje vyřešení dvou základních problémů:

1. Efektivní rozmístění přístupových bodů.
2. Zpřístupnění sítě, vymezení oprávněných uživatelů a zajištění bezpečnosti provozu.

Zatímco první z uvedených bodů je v podstatě jednorázovou záležitostí, přístup k řešení druhého bodu velmi významným způsobem ovlivňuje použitelnost sítě. Vzhledem k primárnímu určení sítě pro studenty fakulty bylo nutné zajistit, aby zabezpečení nebránilo i případně velmi širokému použití v podstatě značně heterogenní studentskou komunitou.

Bezdrátová síť je svou podstatou sdílené médium, což je ovšem z bezpečnostního hlediska velmi nepříjemné. K síti je možno se připojit všude, kde je k dispozici dostatečně silný signál, což samozřejmě situaci dále komplikuje. Kdokoliv, kdo má k dispozici vhodné technické vybavení (notebook s administrátorským přístupem), je schopen odposlouchávat veškerý provoz na síti. Jediným řešením je šifrování všech přenášených dat, otázkou však zůstává, na jaké vrstvě síťových protokolů. Na úrovni technických prostředků (jednotlivé karty) je k dispozici protokol WEP (Wired Equivalent Privacy), který přenášená data šifruje algoritmem RC4. Toto řešení má však podstatné nevýhody:

1. Karty podporují pouze 4 různé klíče (hesla), což nutně znamená sdílení hesel mezi větší komunitu uživatelů. A sdílení hesla v takto heterogenní skupině je v podstatě ekvivalentní jeho zveřejnění.
2. Vlastní šifrování, přestože je realizováno v hardware karet, představuje určité zatížení. To je zanedbatelné u koncových zařízení, ale může se negativně projevit na přístupových bodech, které v daném okamžiku komunikují s větším počtem připojených stanic.
3. V současné době je WEP k dispozici v provedení s klíčem 40 bitů a s klíčem 104 bitů dlouhým. Zejména první varianta, ve spojení s kryptovacím algoritmem RC4, dnes již nepředstavuje významnou ochranu proti „proražení“ klíče hrubou silou (podrobnosti viz. `http://sourceforge.net/projects/airsnort/`).

Tyto důvody vedly k rozhodnutí zajistit důvěrnost dat až na vyšších vrstvách, tj. důsledným doporučením programů a protokolů, přenášejících data v šifrované podobě (např. `ssh` či kerberizovaný `telnet` pro přístup ke vzdáleným počítačům, `pop3s` a `imaps` pro přístup k poštovním serverům a `https` pro přístup k Internetovým stránkám).

Dalším problémem je napojení bezdrátové sítě na Internet. Pokud by byla připojena k Internetu přímo, pak by umožnění přístupu k ní prakticky bez omezení představovalo závažné porušení pravidel provozu sítě MU (do budovy má přístup veřejnost a kdokoliv by se tak mohl připo-

jit a síť používat třeba pro komerční účely). Bezdrátová síť proto tvoří oddělenou síť (analogie VPN, tedy Virtual Private Network), oddělenou od Internetu směrovačem, který umožňuje přístup k Internetu pouze autentizovaným uživatelům.

V praxi to znamená, že zatímco připojení do vlastní bezdrátové sítě není nijak omezeno (stačí v podstatě znát jméno této sítě, které je snadno zjistitelné např. odposlechem přenášených dat), přístup do Internetu vyžaduje další krok, kterým je autentizace uživatele. Pro zajištění univerzálních podmínek přístupu bylo pro tento účel zvoleno webové rozhraní. Uživatel se po připojení do bezdrátové sítě, kdy je mu (protokolem DHCP) přiděleno IP číslo této sítě, musí připojit k webovému prohlížeči (na adrese `https://thetis1.fi.muni.cz/auth/system/wireless/login.mpl`) a tam se autentizovat zadáním svého uživatelského jména a hesla. Teprve po úspěšné autentizaci je pro koncovou stanici, z níž byla autentizace provedena (přesněji pro její IP a MAC adresu, tedy vlastní adresu použitého bezdrátového rozhraní), „otevřena“ cesta do Internetu. Toto zpřístupnění je však časově omezeno (v současnosti na 10 hodin) a nejpozději na konci této doby se uživatel musí autentizovat znovu.

Další zvýšení bezpečnosti je zajištěno systémem trvalé kontroly připojení: jakmile je autentizovaná stanice na více jak pět minut nedostupná, je jí příslušející oprávnění přístupu do Internetu zrušeno a stanice (resp. její uživatel) se musí před dalším přístupem znovu autentizovat.

Počítače připojené prostřednictvím bezdrátové sítě se ani po autentizaci nestávají rovnocennými počítačům interní sítě FI – důvodem je poměrně snadná možnost převzetí identity autentizovaného stroje jiným. Zatímco dva stroje se stejnou IP adresou by byly okamžitě detekovány, může potenciální narušitel čekat, až se skutečný uživatel odpojí ze sítě (to zjistí podobným mechanismem, jakým je hlídáno připojení původního počítače na síti) a poté (dříve, než je odpojení detekováno jako přetrvávající neaktivita) převezme jeho identitu. Z tohoto důvodu bylo nezbytné nepovolit služby, autentizované pouze internetovou adresou (IP), jako je např. sdílení souborů protokolem NFS, neautentizovaný přístup na síťové tiskárny apod.[1] Na druhé straně je počítač připojený prostřednictvím bezdrátové sítě stále součástí sítě MU a podléhá tak odpovídajícím pravidlům provozu sítě. Podrobné podmínky připojení a z nich vyplývající omezení je možno nalézt na webu FI (`http://www.fi.muni.cz/wireless`).

2 Technické vybavení

Zpřístupnění bezdrátové sítě je zajištěno přístupovými body ORiNOCO AP-1000 firmy Lucent Technologies, vybavených PCMCIA kartami stejné značky. Jedná se o tzv. stříbrné karty (Silver Cards), které mají pouze 11 ze 13 kanálů definovaných standardem IEEE 802.11b (ty dva zbývající nepatří v řadě zemí k nelicencovaným, tj. nesmí se používat) a podporují klíče pouze 40 bitů dlouhé v rámci algoritmu WEP (na rozdíl od zlatých karet, podporujících silnější 104 bitové šifry). Použití pouze stříbrných karet však nijak neovlivňuje funkcionalitu sítě (zejména s ohledem na rozhodnutí nepoužívat WEP protokol) a umožnilo snížit celkové náklady. Všechny přístupové body mají prostor pro dvě PCMCIA karty, instalována je však vždy pouze jedna, což vytváří dostatečný prostor pro až dvojnásobné zvýšení výkonu (počtu připojitelných uživatelských stanic) bez nutnosti dalších investic do vlastních přístupových bodů (které tvoří nejnákladnější položky celé instalace). S výjimkou přístupového bodu pokrývajícího vnitřní volné prostranství (átrium) fakulty je v ostatních případech instalována všesměrová anténa Omni-6 s výkonem 6 dBi, pokrytí átria zajišťuje pak jedna všesměrová anténa s výkonem 10 dBi.

Všechny přístupové body jsou připojeny na 100 Mb/s páteř fakultní počítačové sítě a tvoří virtuální síť, jejíž směrování je zajištěno mechanismem popsaným výše. Vlastní směrování pak zajišťuje fakultní router, což je dvouprocesorový osobní počítač s operačním systémem Linux, webový server (Apache) pro autentizaci uživatelů běží na dalším osobním počítačem s Linuxem. Zatímco návrh rozmístění přístupových

[1] Na druhé straně je na místě upozornit, že tento typ autentizace je obecně nedostatečný a představuje významnou bezpečnostní díru.

bodů a jejich instalace byly svěřeny externí firmě, zajištění provozu je již zcela v kompetenci Centra výpočetní techniky FI. Síť zajišťuje roaming, tj. připojení na Internet je funkční i při pohybu koncového zařízení (notebook) jak v rámci jednoho přístupového bodu, tak i při pohybu mezi nimi. Je tedy možno se připojit např. bezprostředně po vstupu do budovy a pak se po ní volně pohybovat, aniž by došlo ke ztrátě spojení či změně jeho parametrů (např. IP adresa notebooku).

3 První zkušenosti

Síť byla instalována na přelomu roku 2001/2002 a experimentálním provozem byla zpřístupněna v druhém lednovém týdnu. V současné době je v síti zaregistrováno celkem 27 karet, jejichž uživatelé síť používali alespoň 45 minut. Celkově nejdéle připojená karta byla on-line více jak 1 plný den (přesně 1445 minut). K 23. lednu možnosti vypůjčit si kartu využilo 15 studentů, řada dalších má karty vlastní. Ostatní karty jsou buď zaměstnanců nebo studentů, kteří kartu dostali v rámci práce výzkumných skupin, nejméně jeden další student projevil zájem připojit do sítě i PDA (Personal Digital Assistent) typu Compaq iPaq nebo HP Jornada. Vynořil se i zájem o pokrytí suterénních prostor, kde jsou umístěny některé menší učebny, vhodné jako útočiště spolupracujících skupin studentů.

Zkušenost za prvních čtrnáct dní experimentálního provozu potvrzuje předpoklad, že o podobné zpřístupnění Internetu je skutečný zájem jak mezi zaměstnanci, tak i studenty. Již krátkou dobu po zprovoznění sítě bylo vytvořeno de facto (za spoluúčasti studentů) dalších cca 20 přístupových míst k Internetu a je možné očekávat další růst tohoto počtu bez dalších dodatečných nákladů fakulty a zejména bez nutnosti zajištění nových prostor. Bezdrátová síť bude k dispozici i účastníkům mezinárodních konferencí, které FI v tomto roce organizuje. Zajištění provozu vyžaduje mimo jiné i průběžné řešení současně se vynořujících technických problémů, např. kolísání signálu, překryv signálu z více přístupových bodů, „nepochopitelné“ radiové stíny apod. Takto získané praktické zkušenosti pak budou moci být využity i pro případnou instalaci podobného systému v jiných areálech MU, jako jsou např. koleje, ale lákavá je i představa úplného pokrytí plánovaného univerzitního kampusu v Bohunicích bezdrátovým signálem. Na to si ale budeme muset ještě nějakou dobu počkat, až bude možno zkušenosti FI dostatečně zevšeobecnit.

Literatura

[1] L. Matyska, E. Hladká. *Mobilita v malém*. Zpravodaj ÚVT MU, 2001, roč. 11, č. 5, s. 1–4. □