Mobilita napříč sítěmi

Eva Hladká, Luděk Matyska, FI MU

V roce 2001 byly na tomto místě prezentovány dva články zaměřené na mobilitu a bezdrátové sítě [1, 2]. V letech, která od publikace obou příspěvků uplynula, se vývoj nezastavil a je na místě se k problematice vrátit a univerzitní veřejnost seznámit se současným stavem podpory mobility v akademických sítích. Stejně jako v původních příspěvcích se omezíme především na podporu mobility v oblasti bezdrátových sítí, protože se jedná o oblast, s níž se každodenně může potkat každý z nás.

Autoři článku mají své domovské pracoviště v areálu FI MU na Botanické 68a, kde byla vybudována první bezdrátová síť v rámci celé Masarykovy univerzity [3] i ostatních vysokých škol (přinejmenším co se rozsahu pokrytí celého areálu fakulty týče). V současné době je v tomto areálu, kde kromě Fakulty informatiky sídlí i Ústav výpočetní techniky a Středisko podpory handicapovaných studentů, zprovozněno několik bezdrátových sítí. Další bezdrátové sítě byly vybudovány i v ostatních lokalitách Masarykovy univerzity [6, 7], která navíc samozřejmě nezůstala jedinou vysokou školou, jejíž pracoviště zajišťují přístup do Internetu tímto způsobem.

Bezdrátová síť již sama o sobě zajišťuje jistou úroveň mobility. V první úrovni umožňuje volný pohyb s trvalým přístupem k Internetu tam, kde je dostupný signál přístupového bodu. Větší prostor může být pokryt soustavou přístupových bodů, které zprostředkovávají dostupnost jednoho síťového segmentu – to je např. případ sítě FI, která v celém areálu vytváří uniformní prostředí z pohledu hierarchie IP sítí. I v tomto případě zůstává problém připojení při vlastním pohybu – nastavení přístupových bodů musí umožňovat dynamické předávání pohybujícího se klienta (např. notebooku). Pokud mobilitu omezíme na možnost přihlásit se kdekoliv v pokrytém areálu (i při omezené pohyblivosti po přihlášení), pak to nevyžaduje žádné dodatečné schopnosti bezdrátové sítě. V celém prostoru je k dispozici jednotný prostor IP adres a přístup do sítě se neliší podle místa připojení.

Problém nastává tam, kde musíme přecházet mezi bezdrátovými sítěmi s různou administrativou. V tomto případě pravděpodobně přecházíme do jiného prostoru z pohledu IP sítě a je pravděpodobné, že mechanismus přístupu k síti – tedy způsob, jak získáme povolení síť používat – se bude lišit. Pokud víme předem, že se v prostoru nové sítě budeme pohybovat, musíme si zpravidla pamatovat nový způsob přihlašování, včetně např. přihlašovacího jména (login) a hesla, ale pokud se v prostoru nové sítě ocitneme neočekávaně, pak zpravidla nejsme schopni ji využít, přestože obecná politika dané sítě tuto možnost nevylučuje.

Existuje celá řada autentizačních mechanismů, které umožňují zpřístupnit bezdrátovou síť předem známým – zaregistrovaným – osobám. Skutečná mobilita však vyžaduje možnost alespoň dočasného využití i sítí organizací, u nichž uživatel není předem registrován. Možným řešením je projití registrační procedurou „na místě“, to však s sebou nese nejméně dva problémy: (i) vlastní registrační proces může být poměrně zdlouhavý a nemusí být tedy vhodný pro skutečně dočasné použití, (ii) hostující organizace si musí vést registrační údaje o všech hostech, což v podstatě zbytečně zatěžuje její administrativu (a v konečném důsledku snižuje ochotu zpřístupnit svou síť návštěvníkům).

Ideálním řešením by se mohl stát jediný bezdrátově pokrytý prostor nejenom v rámci jedné lokality MU či MU jako celku (kde virtuální privátní síť MU již tuto možnost poskytuje), ale celé akademické sítě a případně i celků větších. Je však zřejmé, že tento přístup nemůže být centralistický (s jedinou databází informací o všech potenciálních uživatelích) a je třeba hledat vhodnější přístupy.

Východiskem našich úvah je tedy existence organizací, ochotných v principu zpřístupnit si vzájemně své bezdrátové sítě, ovšem bez administrativní zátěže spojené se sdílením databází přístupových oprávnění.

Projekt EduRoam

Řešením problému uvedeného na konci předchozího odstavce se zabývá aktivita *Mobility Task*

Force sdružení TERENA (organizace sdružující akademické sítě Evropy) [4] od začátku roku 2003. Cílem je výzkum síťových architektur, autentizačních a autorizačních technologií pro transparentní zpřístupnění bezdrátových (a případně dalších) sítí studentům, učitelům a vědeckým pracovníkům participujících organizací tak, aby jednotliví uživatelé mohli bez dalších kroků přistupovat k síti kdykoliv se ocitnou v prostoru pokrytém sítí alespoň jednoho z účastníků (není třeba se dopředu registrovat apod.). Pro tyto účely se řešitelé shodli na označení *EduRoam*, které se současně stalo synonymem pro hostitelskou mobilní infrastruktur (Educational Roaming).

Infrastruktura EduRoam vychází ze základní myšlenky, že autentizační proces konkrétního uživatele je realizován pouze u jedné organizace, nezávisle na tom, kde se uživatel právě nachází. Autentizační infrastruktura musí za zadaných autentizačních informací rozpoznat, kde je ona domovská organizace, té autentizační údaje předá a podle verdiktu (autentizován nebo nikoliv) pak zajistí přístup do lokální sítě. Konkrétně se využívá hierarchicky propojený systém autentizačních serverů RADIUS, neboť ty jsou zpravidla využívány pro autentizace v rámci jednotlivých organizací a podporované protokoly umožňují jejich vzájemné propojení způsobem popsaným výše.

Konkrétní autentizace se pak dělá protokolem 802.1x, případně přes webová rozhraní, podstatný je ale přenos autentizačního dotazu domovské organizaci uživatele. Ta je dána formátem použitého „průkazu“ (credentials), zpravidla pak přihlašovacího jména, jehož součástí je i jednoznačně vymezená identifikace domény (např. `matyska@ics.muni.cz` jako login jméno ukazuje, že autentizaci je nutné provést v doméně `ics.muni.cz`). Aby systém mohl fungovat, musí se jednotlivé organizace předem dohodnout na vzájemné důvěře a tom, že budou takto delegovanou autentizaci uznávat. V současnosti je do aktivity Mobility Task Force připojeno 13 národních sítí, ovšem žádná národní síť nepokrývá všechny byť jen akademické instituce dané země.

EduRoam v české akademické síti

Česká republika se prostřednictvím sdružení CESNET připojila k projektu EduRoam hned v jeho počátku. V rámci výzkumného záměru *Vysokorychlostní síť národního výzkumu a její nové aplikace* byla založena aktivita s cílem vybudovat národní infrastrukturu a připojit ji k ostatním evropským sítím. Výsledkem práce je definice roamingové politiky (tedy kdo, kdy a za jakých podmínek je oprávněn tuto službu používat – zpravidla je taková politika velmi blízká roamingovým politikám, které známe od mobilních operátorů telefonních sítí) a konkrétní implementace EduRoam infrastruktury v České republice [5]. Současně CESNET garantuje propojení národní infrastruktury na evropské úrovni.

Na národní úrovni je do aktivity EduRoam.cz připojena již řada organizací. Kromě sídla CESNETu v Praze na Zikově ulici je třeba zmínit např. UK (rektorát a řada fakult, např. FF, PRF a FAF), FEL ČVUT, UJEP, VŠCHT, ZČU, UHK. Technické podrobnosti o podmínkách provozování RADIUS serverů (jak se k EduRoamu připojit), včetně jejich doporučené topologie, je možné najít na části webu EduRoam určené správcům infrastruktury.

EduRoam řeší problém hostujících účastníků v síti zcela přirozeným způsobem. K autentizaci stačí autentizace uživatelským jménem a heslem ze své domovské organizace.

Rizika spojená s provozováním EduRoamu

Jak jste si možná všimli, mezi národními organizacemi zapojenými do aktivity EduRoam nebyla zmíněna Masarykova univerzita v Brně. Jedním z důvodů je standardní problém těch, kteří začali příliš brzy – bezdrátové sítě na MU jsou staršího data a používají autentizační mechanismy, které nejsou jednoduše propojitelné s požadavky EduRoam. Dalším, podstatnějším důvodem je ale právní nevyjasněnost – člen EduRoam musí zpřístupnit svou síť uživatelům z ostatních organizací. To ovšem znamená přizpůsobit bezpečnostní a přístupovou politiku požadavkům EduRoam, což v případě MU není jednoduché rozhodnutí, mimo jiné opět proto, že na MU mají formálně ustavené politiky přístupu k síti jednu

z nejdelších tradic v rámci akademického prostředí ČR. V rámci realizace politiky je pak třeba ošetřit případy, kdy jednotlivec – „návštěvník“ – poruší její pravidla. Má se v takovém případě zakázat přístup všech uživatelů ze stejné domovské organizace? Pokud ne, pak jakým způsobem budou drženy údaje o „nežádoucích“ uživatelích – nebudeme si muset vytvářet vlastní databáze, jejichž existenci a správě jsme se chtěli vyhnout?

Nejproblematičtějším místem sjednocení politik je otázka přístupu k vnitřním zdrojům univerzity. EduRoam sám nedefinuje, jakou IP adresu (ve vztahu k adresnímu prostoru hostující organizace) „návštěvník“ získá, nicméně jednoduché a často používané řešení přiděluje IP adresu přímo z rozsahu IP adres hostující organizace. To ovšem v dnešním světě, kde je stále řada přístupů kontrolována na základě IP adresy, znamená, že takový uživatel získá přístup ke stejným službám a informačním zdrojům jako vlastní student nebo zaměstnanec. Tím zpravidla dojde k rozporu s licenční politikou třeba elektronických databází – MU má zakoupeno právo přístupu vlastních studentů a zaměstnanců, nikoliv však studentů a zaměstnanců ostatních vysokých škol či dalších akademických institucí. Tento problém lze řešit vyčleněním bezdrátové sítě z rozsahu sítí, zpřístupňujících takové zdroje – pokud ovšem stejnou síť použije oprávněná osoba, pak rovněž ztrácí možnost přístupu (nebo ten musí byt realizován dalším stupněm autentizace, což je samozřejmě pro vlastní uživatele nepohodlné).

Použití Virtuální privátní sítě tento problém může řešit, vyžaduje však netriviální technickou podporu všech účastníků aktivity EduRoam a ochotu implementovat příslušné nástroje. Dalším možným řešením je zlepšení mechanismů *autorizace*, tedy oprávnění přistupovat ke konkrétním zdrojům.

Autorizace – jak na ni?

Autorizace logicky následuje za autentizací – poté, co máme potvrzenu identitu konkrétního uživatele rozhodneme, co smí či nesmí v síti dělat. Ovšem aktivita EduRoam je založena na předpokladu, že lokální síť vlastně identitu nezná – pouze dostane od domovské organizace (které věří) potvrzeno, že ta konkrétního žadatele zná. Jak ovšem v takovém prostředí zajistit odpovídající autorizaci? Tato otázka zatím nemá jednoznačnou odpověď, nicméně v posledních letech se zdá, že by možným řešením mohl být systém Shibolleth [8], který původně vznikl v USA (jakou součást aktivit kolem Internetu2) pro autorizaci přístupu k rozsáhlým elektronickým knihovním zdrojům.

Princip Shibollethu je obdobný principům, na nichž je založen EduRoam – definujeme autorizační skupiny (např. uživatelé konkrétní elektronické databáze) a na těchto skupinách se dohodneme s partnery. Autorizační požadavek pak opět řeší domovská organizace – té hostující předá autentizační údaje klienta a požadavek, aby domovská organizace potvrdila příslušnost k určité skupině (např. skupině zahrnující uživatele oprávněné používat konkrétní elektronickou databázi). Domovská organizace udělá kompletní ověření (autentizaci a následnou autorizaci) a hostující organizaci sdělí pouze výsledek: *ano* či *ne*. Hostující organizace si opět nemusí budovat vlastní databázi oprávnění, uživatel se nemusí předem registrovat, ...

Systém Shibolleth je dimenzován s ambicí sloužit celé akademické veřejnosti USA, v současné době je používán řadou univerzit s velmi dobrým ohlasem. I v ČR se začíná uvažovat o jeho experimentálním nasazení, ovšem plná implementace bude vyžadovat součinnost jak univerzit, tak i vlastních poskytovatelů obsahu a je to tedy běh na dlouhou trať.

Závěr

Jak je z popsaného patrné, podpora mobility postupně přerůstá z řešení čistě technických problémů do roviny politik, definujících oprávnění přístupu jak k síti, tak jednotlivým zdrojům touto sítí zprostředkovaným. Rostoucí počet případů zneužití volného přístupu k Internetu nutí i vysoké školy a další akademická pracoviště, aby ve zvýšené míře dbaly na nástroje a metody kontroly používání počítačové sítě. V příspěvku zmíněné přístupy se snaží překlenout

rozpor, který je mezi snahou zpřístupnit Internet co největšímu počtu (akademických) uživatelů a snahou minimalizovat nebezpečí, která z neomezeného přístupu plynou. Aktivity EduRoam i Shibolleth jsou příkladem škálovatelných řešení, schopných pokrýt velmi rozsáhlé oblasti s minimem administrativy a byrokracie. Akademické sítě se snaží rozvíjet podporu mobility, nemohou však ignorovat problémy, které mobilita přináší. Je možné, že z projektu EduRoam vyroste v budoucnu jeden velký prostor pokrývající akademické prostředí a my budeme moci přecházet z jedné sítě do druhé bez ruční přeregistrace a bez obav z bezpečnosti (a provozovatelé sítí budou ochotni je otevírat, protože budou schopni vždy identifikovat případné narušitele provozu). Nepochybně se časem i MU připojí k aktivitám EduRoamu, aby svým zaměstnancům a studentům umožnila využití bezdrátových sítí i v dalších lokalitách, a aby současně vytvořila přívětivé prostředí pro své hosty. K tomu však bude ještě třeba kromě technických problémů vyřešit právě i otázky autorizace přístupu k licencovaným či jinak chráněným informačním a dalším zdrojům.

Literatura

[1] L. Matyska, E. Hladká. „Mobilní počítání.“ *Zpravodaj ÚVT MU*. 2001, roč. 11, č. 4 s. 1–3.

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

[3] L. Matyska. „Bezdrátová síť Fakulty informatiky.“ *Zpravodaj ÚVT MU*. 2002, roč. 12 č. 3, s. 5–7.

[4] „TERENA mobility initiative“ `http://www.terena.nl/tech/index_mobility.html`

[5] „Projekt EduRoam České akademické sítě“ `http://www.eduroam.cz`

[6] D. Rohleder. „Bezdrátové sítě v prostředí MU.“ *Zpravodaj ÚVT MU*. 2004, roč. 14, č. 3, s. 18–19.

[7] J. Morávek, R. Peša. „VPN server Masarykovy univerzity.“ *Zpravodaj ÚVT MU*. 2003, roč. 14, č. 2, s. 10–12.

[8] „Shibolleth—authorization“ `http://shibboleth.internet2.edu/` □