Všichni chceme Eduroam!

Michal Procházka, ÚVT MU

V dnešní době nepřipadá nikomu nijak výjimečné, že lze volat z mobilního telefonu téměř odkudkoliv a komukoliv na planetě. Nezáleží, ke kterému operátorovi jste připojeni, jednoduše používáte svůj mobilní telefon a o ostatní ať se postará váš domovský operátor. Možnost využívat služby GSM celosvětově zajišťuje tzv. roaming. Jedná se o fyzické ale i smluvní propojení operátorů. Zde se nabízí otázka, proč neumožnit roaming ve světě počítačových sítí? Tuto otázku si položili lidé v ogranizaci *TERENA*[1] *(Trans European Research and Education Networking Association)* a založili skupinu *TF Mobility*[2]. TF Mobility má za cíl vybudovat roamingovou infrastrukturu, která umožní mobilitu uživatelů mezi národními sítěmi tzv. *NREN (National Research and Education Network)* i v rámci nich. Z této skupiny vzešel projekt *Eduroam [1] (Education Roaming)*, který si přiblížíme v tomto článku.

1 Co je to ten Eduroam?

Základní myšlenka Eduroamu je umožnit studentům a akademickým pracovníkům připojit se do počítačové sítě v jiné akademické instituci, aniž by se museli někde registrovat nebo získávat přístupové údaje. Připojení k síti vyžaduje od uživatele pouze uživatelské jméno a heslo, které používá v domovské instituci. V současné době je Eduroam nejvíce rozšířen na poli bezdrátových sítí.

Eduroam v sobě integruje autentizační a autorizační infrastrukturu *AAI (Authentication and Authorization Infrastructure)* a bezpečnost dat. Je to dáno tím, na jakých technologiích je Eduroam postaven. K autentizaci a autorizaci využívá radius servery a protokol 802.1x. Bezpečnost dat se týká bezdrátových sítí, kde se využívají silné šifrovací algoritmy pro přenos dat mezi klientem a přístupovým bodem.

[1] `http://www.terena.nl`

[2] `http://www.terena.nl/activities/tf-mobility`

2 Přístup uživatele k Eduroamu

Na jednoduchém příkladu si ukážeme, jak je jednoduché Eduroam používat k připojení k WiFi sítím podporujícím Eduroam. Uživatel si nejprve zaregistruje eduroam účet ve své domovské instituci. Uživatelské jméno se skládá z volitelného loginu a z tzv. realmu, který identifikuje instituci, např. xnovak@muni.cz. Tyto dva údaje zadá do supplicanta (program, který se stará o připojení k WiFi síti) a od této chvíle se uživatel může připojit do všech sítí podporujících Eduroam. WiFi síť, která podporuje Eduroam, většinou obsahuje ve svém názvu text "eduroam".

3 Co dělá Eduroam Eduroamem

Celá infrastruktura Eduroamu je postavena na Radius serverech a autentizačním protokolu 802.1x. Radius servery umístěné v jednotlivých organizacích spravují své vlastní uživatele. Žádost o připojení uživatele z jakékoliv lokality pokryté Eduroamem znamená vytvoření bezpečného tunelu od klienta přes infrastrukturu Eduroamu až k domovskému radius serveru, který provádí autentizaci.

4 Radius infrastruktura

Radius server (Remote Authentication Dial In User Service) je určen k ověřování identity uživatelů, dále provádí autorizaci uživatelů a accounting na základě informací z přístupového bodu. S radius serverem nekomunikuje přímo uživatel, ale pouze přístupové body. Radius server může také fungovat jako proxy – v tom případě neověřuje identitu uživatelů, ale pouze přeposílá požadavky na jiné radius servery.

Radius servery jsou v Eduroamu hierarchicky seskupeny. Top-level radius servery jsou umístěny v Holandsku, dále každý stát má vlastní národní radius servery a samozřejmě je má i každá připojená instituce. Radius servery v cílových organizacích zajišťují ověření identity vlastních uživatelů. Národní a top-level radius servery se starají o předávání autentizačních požadavků. Pokud na jakýkoliv radius server přijde požadavek o ověření identity uživatele, je z jeho uživatelského jména vyextrahován realm, který určuje, ke které instituci přísluší. Pokud není požadavek

schopen ověřit tento radius server, pak je přeposlán na nadřazený radius server.

5 Řízení přístupu k síti

Možností jak řídit přístup uživatelů do sítě, ať už bezdrátové nebo drátové, je mnoho, většina ale předpokládá sestavené IP spojení nebo ověřování na základě MAC adresy. Eduroam využívá protokol *802.1x*, který umožňuje přístupovým prvkům (switch, přístupový bod WiFi) řídit provoz na jednotlivých portech. Jedná se o protokol, který komunikuje na linkové vrstvě. Protokol 802.1x ve spojení s protokolem *EAP (Extensible Authentication Protocol)* umožňuje bezpečnou výměnu dat mezi klientem a domovským radius serverem přes přístupové body nebo switche a ostatní radius servery. EAP protokol zajistí přenos přihlašovacích údajů až na domácí radius server, který uživatele autentizuje. O výsledku je informován přístupový prvek a poté uživatele vpustí do sítě nebo naopak zamítne přístup.

Důležitou vlastností EAP ve spojení s radius infrastrukturou je ustavení bezpečného (šifrovaného) kanálu mezi klientem a cílovým radius serverem. Je proto vyloučeno, aby jakýkoliv radius server nebo přístupový bod, který předává požadavek dál, viděl uživatelské heslo.

Samotný protokol EAP je pouze obálka pro konkrétní autentizační protokoly. V rámci Eduroamu se nejčastěji používá protokol PEAP/MSCHAPv2 nebo TLS. Protokol PEAP vyžaduje od uživatele zadání uživatelského jména a hesla, naopak TLS protokol je postaven na infrastruktuře veřejných klíčů PKI, kde se k autentizaci využívají certifikáty.

6 Bezpečný přenos dat

Všechny bezdrátové sítě, které umožňují přístup přes Eduroam garantují uživateli, že data mezi jeho počítačem a přístupovým bodem jsou šifrována. Eduroam nijak nenařizuje, který typ šifry má být použit. Nejčastěji se setkáváme s šifrováním dat WPA nebo WEP104.

7 Politika Eduroamu

Politika Eduroamu je velice volná. Ten, kdo využívá nebo provozuje Eduroam, musí dodržovat národní politiku pro Eduroam[3]. Česká národní politika pro Eduroam hovoří ve stručnosti o tom, že roaming mezi jednotlivými sítěmi by měl být oboustranně výhodný, a samozřejmě se zabývá postupem při řešení incidentů. Na připojení k Eduroamu není vázán žádný podpis smlouvy, zatím se vše děje "na dobré slovo". V TF Mobility momentálně probíhá vytváření politiky pro Eduroam a současně se v CESNETu vede diskuse nad novou podobou národní politiky pro Eduroam.

Eduroam se naštěstí nijak nepotýká s problémem poskytování osobních údajů o uživatelích, protože jedině domovská instituce zná vazbu uživatelského jména a konkrétní osoby. V případě vzniku incidentu (např. rozesílání nevyžádané pošty, hackerské útoky či jiná nekalá činnost) je do domovské instituce odeslána pouze informace, které přihlašovací jméno incident provedlo a popis incidentu. Domovská instituce musí incident svého uživatele vyřešit a vyrozumět žadatele. Do vyřešení incidentu má uživatel odepřen přístup do sítě. V případě, že domovská instituce incident neřeší, je možné zamezit přístup pro celou instituci, a zároveň tuto informaci odeslat správcům nadřazených radius serverů, kde pak po posouzení dojde ke kompletnímu zablokování hřešící instituce.

8 Eduroam na FI

Na Fakultě informatiky v Laboratoři pokročilých síťových technologií a na Ústavu výpočetní techniky MU již půl roku běží testovací provoz Eduroamu. Jako domácí uživatelé byli vybráni uživatelé *METACentra* a jako autentizační mechanismus byl zvolen TLS, tzn. uživatelé kteří mají platný certifikát vydaný certifikační autoritou CESNET CA. Jak praví politika Eduroamu, domovská instituce je zodpovědna za uživatele, které úspěšně autentizuje. Proto jsme byli nuceni vyvinout úpravu pro radius (konkrétně pro volně dostupnou implementaci freeRadius[4]), kde

[3] http://wiki.eduroam.cz/doku.php?id=cs:roamingova_politika

[4] http://www.freeradius.org

je po úspěšné autentizaci certifikátem provedena ještě autorizace, zda daný certifikát patří uživateli *META Centra*.

9 Eduroam na MU

Pracovníci ÚVT v současné době pracují na zavedení Eduroamu na celé MU. V první fázi se jedná o zprovoznění radius serveru, který umožní využívat Eduroam studentům a zaměstnancům MU všude, kde je Eduroam dostupný. Druhá fáze bude zahrnovat postupnou rekonfiguraci všech WiFi přístupových bodů na MU, aby byl Eduroam dostupný ve většině budov MU.

Zavedení Eduroamu není jednoduché jako přepnutí jednoho tlačítka, jelikož se musí rekonfigurovat jak síťové prvky školy tak i počítače uživatelů. Proto bude dále podporován přístup do sítě přes VPN. Tento duální režim umožní hladký přechod na Eduroam se zachováním všech jeho výhod, což znamená, že se na MU připojí cizí uživatelé a uživatelé z MU se budou moci připojit kdekoliv, kde je Eduroam.

10 Problémy

S příchodem nové technologie jsou vždy spojeny problémy. Od prvopočátků Eduroamu jich bylo již hodně vyřešeno, bohužel však stále ještě některé přetrvávají. Jedním ze zásadních problémů je kompatibilita hardwarových prvků. Na trhu existují dvojice klientských karet a přístupových bodů, které mají problémy se vzájemnou komunikací. Další problém, který se však postupně daří s přibývajícím počtem uživatelů a jejich migrací odstraňovat, jsou nekorektní zásahy do komunikace mezi radius servery. Radius server, který přeposílá požadavek dál, může měnit parametry radius paketů (do obsahu tunelu sestaveného mezi klientem a domácím radius serverem zasahovat nemůže). Při nekorektní konfiguraci radius serveru může dojít k zamezení použití některých autentizačních metod. Nejčastěji je tímto problémem postižena metoda TLS.

11 Závěr

Podrobné informace o Eduroamu lze nalézt na českých stránkách Eduroamu `http://www.eduroam.cz`, kde je také uveden aktuální seznam připojených institucí v ČR. Ke kompletnímu celosvětovému seznamu všech institucí s Eduroamem se lze dostat přes hlavní stránky Eduroamu `http://www.eduroam.org`.

Závěrem bych popřál Eduroamu úspěšný start na MU a chtěl bych také poděkovat těm pracovníkům ÚVT, kteří se na jeho zavedení podílejí.

Literatura

[1] Licia Florio, Klaas Wierenga. *Eduroam, providing mobility for roaming users.* EUNIS Conference. 2005. □