802.1X – autentizace v počítačových sítích

David Rohleder, Václav Lorenc,ÚVT MU

Bezpečnost patrně nikdy nebyla prioritní otázkou při navrhování počítačových sítí. Bylo to asi způsobeno tím, že k počítačům měly obvykle přístup pouze osoby zodpovědné a řádně vyškolené. Nicméně situace se s postupujícím přibližováním počítačů obyčejným lidem začala postupně měnit. Dodatečně tedy byly zabezpečeny aplikace bezpečnými autentizačními mechanismy, přenos dat po síti začal být šifrován a došlo i na samotné řízení přístupu k datové síti. Tím posledním se v oblasti sítí typu ethernet zabývá standard 802.1X [1], který se vztahuje nejen na pevné (drátové), ale i na bezdrátové sítě WiFi.

Řízení přístupu k počítačové síti je nutné zejména v případě, kdy nemáme pod fyzickou kontrolou všechna možná připojení k datové síti. Zabraňuje tak přístupu neautorizovaných osob bez toho, abychom museli udržovat fyzickou bezpečnost všech přípojek. Navíc v případě bezdrátových sítí je fyzické zabezpečení téměř nemožné. Řízení přístupu zabezpečí přístup pouze oprávněným osobám a neumožní přístup těm, kteří by mohli počítačovou síť zneužít k neoprávněnému přístupu. Nezabezpečená síť totiž dnes díky mnoha různým síťovým protokolům většinou znamená otevřenou cestu pro útočníky, kteří mohou nepozorovaně zneužívat datové připojení, případně provádět další činnosti, jako třeba odposlouchávání provozu nebo vydávání se za někoho jiného.

Standard 802.1X, ačkoliv byl původně určen pro řízení přístupu k drátovým sítím a implementaci v přepínačích, se začal prosazovat s postupným zaváděním bezdrátových sítí, kde bylo řízení přístupu mnohem ožehavější problém než v drátových sítích, ve kterých bylo možné se různými metodami vyhnout riziku zneužití síťových zásuvek. Svou roli zde také sehrála nepřítomnost podpory ze strany rozšířených operačních systémů. Naštěstí situace se v posledních letech výrazně zlepšila, takže je už je reálně možné využít tento standard v praxi.

1 Principy fungování

Celý mechanismus řízení přístupu má celkem tři části. *Supplicant* je aplikace na klientovi, který se snaží připojit do sítě, *autentizátor* – aplikace na síťové straně, jejímž cílem je ověřit klienta, a nakonec *autentizační server* – entita poskytující autentizační informace autentizátoru. Autentizační mechanismus používá standardizovaný protokol EAP (Extensible Authentication Protocol, RFC 3748) zabalený do ethernetových rámců EAPOL (EAP Over LAN). EAP je rozšiřitelný autentizační mechanismus, který umožňuje implementovat různé druhy autentizace (EAP-TLS, EAP-TTLS, EAP-MD5, EAP-OTP, PEAP,...).

Proces ověřování klienta pak probíhá následovně (pro zjednodušení popíšeme drátovou variantu). Ve chvíli, kdy se počítač připojí k síťové zásuvce nebo portu, je síťový port v blokovaném stavu a jediné, co portem prochází, jsou autentizační rámce. Přepínač (v roli autentizátora) vyšle žádost o autentizaci (EAP-Request/Identity) zabalenou do rámců EAPOL. Supplicant na klientovi žádost vyhodnotí (obsahuje např. označení sítě, do které se chce klient připojit) a odpoví zprávou EAP-Response/Identity (MyID). Autentizátor zprávu přijme, vybalí ji z rámce EAPOL, zabalí do datagramu protokolu RADIUS a odešle ji pro ověření RADIUS serveru (autentizační server). Autentizační si zprávou EAP-Request vyžádá prostřednictvím autentizátoru (přepínače) od supplicanta autentizační údaje (opět dochází na přepínači k přebalení datagramů RADIUS do rámců EAPOL). Klient odpoví autentizační zprávou EAP-Response, kterou autentizátor po přebalení opět přepošle autentizačnímu serveru. V případě, že autentizační informace umožňují přístup, autentizační server odpoví zprávou EAP-Success, vrátí klientovi prostřednictvím autentizátoru (přepínače). Přepinač tuto zprávu vyhodnotí, odblokuje port pro komunikaci, nastaví parametry portu (např. přiřazení do VLAN) a přepošle zprávu EAP-Success klientovi. V této chvíli je celý autentizační proces ukončen a klient může bez problému přistupovat k síti (obvykle v této fázi začíná vyjednávání s DHCP serverem o adresách, a pod.). Při ukončování komunikace se sítí může klient vyslat zprávu EAPOL-Logoff, kterou dává na vědomí autentizátoru (přepínači), že už

dále nehodlá komunikovat a přepínač tedy převede port opět do blokovaného stavu. Do blokovaného stavu se port převede i v případě, kdy dojde k odpojení klienta fyzickým vytažením kabelu ze zásuvky nebo vyprší časový limit, během kterého se měl uživatel znovu autentizovat.

Mechanismus 802.1X přináší jak výhody, tak i nevýhody. Mezi výhody patří možnost blokovat přístup neautorizovaných osob k síti nebo blokovat osoby, které mají z nějakých důvodů přístup k síti zakázaný (např. za šíření virů). Tento mechanismus navázaný na další síťové technologie umožňuje např. umístění klienta do karanténní VLAN, kde má přístup pouze k minimu služeb a nemůže nakazit ostatní, nicméně mu zůstává možnost přistupovat ke zdrojům nutným k odvirování počítače.

Mezi nevýhody tohoto přístupu patří to, že s počítači připojenými na neautorizovaný port není možné komunikovat, což může být nevýhodné pro vzdálenou správu počítačů. Někdy se využívá pro údržbu počítačů nočních hodin, kdy si vzdálená managementová stanice probudí počítač pomocí wake-on-lan rámce, provede např. zálohování a po zazálohování dat počítač opět vypne. Tato možnost je bohužel kvůli blokování portů znemožněna (ačkoliv existují metody, jak se tomuto omezení vyhnout).

Dále je nutné připomenout, že 802.1X je pouze mechanismem pro řízení přístupu k portu počítačové sítě. Neřeší další problematiku bezpečnosti a tak by se tento protokol dal přirovnat ke hradbám, za kterými je schována počítačová síť. Jakmile se útočník dostane za hradby, tak má volné pole působnosti a protokol 802.1X sám o sobě žádnou další bezpečnost nezajistí. O tu se musejí postarat další bezpečnostní mechanismy v síti.

2 802.1X na MUNI

V prostředí Masarykovy univerzity je 802.1X již nějakou dobu nastaveno a používáno zejména v bezdrátových sítích. Uživatelé federativní sítě Eduroam [2], ať už vědomě nebo nevědomě, 802.1X používají pro přístup k Internetu.

Pro drátové přípojky tomu tak ve většině případů není. Aby se zamezilo připojování osob, které s univerzitou nemají žádný vztah, jsou jednotliví zájemci o volnou ethernetovou zásuvku nuceni vytvořit si VPN [3] tunel. Ačkoliv to na první pohled nevypadá jako zásadní omezení, několik nevýhod to s sebou přeci jen nese. Z pohledu uživatelů je to rozhodně operace navíc, kterou je třeba po každém připojení k přístupovému bodu provést. Ze strany správců to přináší vícenásobné vytížení VPN serverů, neboť po drátových přípojkách je možné přenášet data mnohem rychleji, než v současných dostupných bezdrátových sítích.

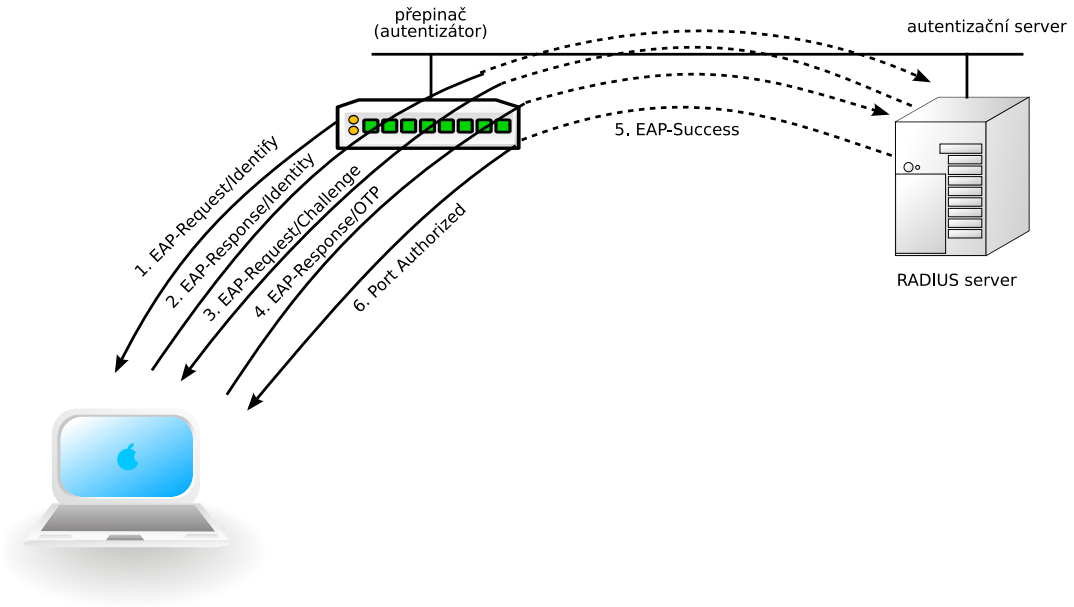
Právě toto by mohlo funkční 802.1X v původní variantě pro drátové přípojky vyřešit, byť to vyžaduje celou řadu změn, ať už na straně síťové infrastruktury, nebo na zařízeních jednotlivých uživatelů.

Nabízí se například otázka – je každé síťové zařízení schopno spolupracovat s 802.1X? Bohužel ne. Ať už se jedná o bezdrátové přístupové body (AP), nebo koncové přepínače, tedy zařízení, k nimž se budou jednotliví uživatelé přímo připojovat, je nutné používat taková zařízení, která s podporou protokolu 802.1X pro autentizaci uživatelů počítají.

Takové prvky jsou nainstalovány například v CPS (Centrální počítačové studovně), kde již v pilotním provozu funguje 802.1X i na ethernetových zásuvkách pro notebooky. Takto zkonfigurované zásuvky v případě řádné 802.1X autentizace umožňují přenášet data rychlostí až 1 Gb/s bez dalších výraznějších omezení.

Současně je potřeba mít připravenou celou řadu dalších serverů, které poskytují autentizační službu a mají za úkol rozhodnout, jsou-li poskytnutá jména a hesla, případně další autentizační informace, v pořádku a platná. I tato část je v současnosti bezproblémově splněna, neboť infrastruktura připravená pro původní řešení s VPN je díky šikovnosti správců připravena i pro autentizaci pomocí 802.1X.

Druhá podstatná otázka v souvislosti s nasazováním 802.1x v nehomogenním prostředí univerzity zní – umí každé uživatelské zařízení spolupracovat s 802.1X? Ani v tomto případě nebude odpověď kladná. S rozrůstající se škálou zařízení, která disponují některou z variant připo-



Obrázek 1: Postup autentizace v protokolu 802.1X

jení k Internetu (ať již bezdrátově nebo pomocí ethernetového kabelu), se objevuje celá řada problémů. Ty nemusí být spojeny jen s hardwarem, často nespolupracuje správně buď samotný operační systém, nebo některá z aplikací, která se stará o připojování do sítě. Tento trend však není vzestupný, naštěstí je tomu spíše naopak. 802.1X je natolik rozšířeným standardem, že moderní operační systémy v moderních zařízeních často podporují i několik autentizačních metod z tohoto standardu.

Pochopitelně není možné omezit připojení k síti pouze pro zařízení, která jsou víceméně moderní. I uživatelé, jejichž operační systém nebo zařízení protokol 802.1X nepodporuje, mají možnost se připojit. Vhodnou konfigurací aktivních prvků je zajištěno, že je v platnosti i původní mechanismus připojování přes VPN – a to bez ohledu na použité přenosové médium, tedy drát či bezdrát.

S přibývajícím množstvím notebooků a uživatelů, kteří nejsou primárně vzděláváni v oblasti zabezpečování svých počítačů, s přibývajícími chybami v aplikacích a operačních systémech a s přibývajícími útočníky, ať už zkušenými nebo náhodnými začátečníky, je každý drobný pokrok v zabezpečení sítě před nezvanými hosty důležitou součástí mozaiky.

Do budoucna, podaří-li se vyřešit všechny související problémy, to s sebou může nést i další klady – menší nutnost konfigurace aktivních prvků při přesunování pracovišť mezi jednotlivými lokalitami univerzity (např. kampusem), a i v případě přechodu z autentizace jménem a heslem na autentizaci pomocí čipové karty či nějakého jiného tokenu, jsou již všechny protokoly a zařízení ze strany serverů a sítě připraveny.

Literatura

[1] `http://www.ieee802.org/1/pages/802.1x-2004.html`
[2] `http://www.eduroam.cz/`
[3] `http://vpn.muni.cz/` □