Standard 802.1x

Technologie pro zlepšení bezpečnosti datových sítí - standard 802.1x (1)

Tento tutoriál navazuje na článek věnovaný zabezpečení lokálních datových sítí proti neoprávněným uživatelům. Objasňuje jeden ze způsobů zabezpečení bezdrátových sítí a LAN sítí vybavených přepínači. Pochopení co přináší specifikace IEEE 802.1x znamená pochopení 3 technologií - PPP, EAP (Extensible Authentication Protocol) a IEEE 802.1x samotné.

Tento tutoriál navazuje na článek věnovaný zabezpečení lokálních datových sítí proti neoprávněným uživatelům. Objasňuje jeden ze způsobů zabezpečení bezdrátových sítí a LAN sítí vybavených přepínači.

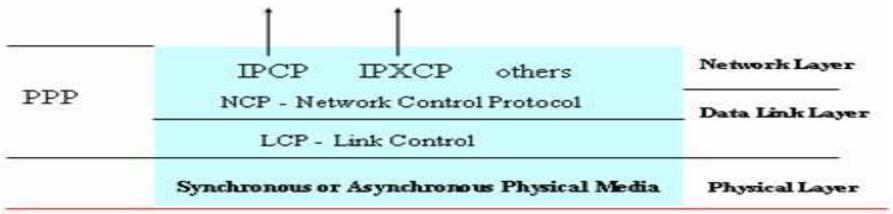
Na tento tutoriál bude navazovat popis 802.11i, což je nová forma specifikace 802.11 pro bezpečnější bezdrátové komunikace. Pochopení co přináší specifikace IEEE 802.1x znamená pochopení 3 technologií - PPP, EAP (Extensible Authentication Protocol) a IEEE 802.1x samotné. PPP a EAP jsou internetové standardy definované prostřednictvím RFC. IEEE 802.1x je IEEE standard postavený na standardu EAP.

Začalo to protokolem PPP...

... a tím, že jeho vlastnosti zabezpečení přestaly postačovat novým nárokům.

Obecně

Protokol PPP (point-to-point protocol) je znám především jako protokol používaný pro přístup k internetu prostřednictvím telefonních linek. Je také používán pro WAN spojení. Někteří ISP jej používají ve formě PPPoE (PPP over Ethernet) pro ověřování uživatelů připojovaných přes xDSL nebo kabelový modem. Protokol PPP je součástí klíčové komponenty bezpečného vzdáleného přístupu implementovaného do OS Windows 2000 - protokolu L2TP.



Komponenty protokolu PPP

PPP je velmi úspěšný protokol. Jeho použití začalo v komutovaných metodách vzdáleného přístupu a dnes jej najdeme na mnoha místech Internetu. Ačkoli má PPP mnoho komponent, které jej přizpůsobují pro použití v různých prostředích (viz. schéma), ve vztahu k diskutovanému tématu nás zajímá pouze část ověřování (součást LCP). Před tím než dojde k čemukoliv na 3. vrstvě OSI (např. IP), zajistí PPP ověření uživatele na vrstvě druhé. Obecně je požadováno (a to znáte např. z přístupu k Internetu) jméno a heslo. Ověření protokolem PPP je použito pro identifikaci uživatele na druhém konci drátu předtím než je mu přístup umožněn. Ověřením na 2. vrstvě je uživatel nezávislý na protokolech vyšší vrstvy (IP, IPX, Appletalk) a může dojít k rozhodnutí jak naložit s protokolem 3. vrstvy OSI. Např. v závislosti na výsledku ověření může uživatel dostat konkrétní IP adresu. Původně byly do PPP implementovány dvě metody - PAP a CHAP. A tady se právě ukázala jedna ze slabin protokolu PPP, již bylo potřeba posílit. PAP i CHAP jsou totiž poměrně slabé ověřovací metody.

PAP

- Password Authentication Protocol – používá jednoduché, jednorázové ověření s přenosem hesla v otevřené formě po síti.

CHAP

- Challenge Authentication Protocol – používá pro ověření složitější mechanismus; ten je založený na tom, že ověřovací server pošle klientovi náhodně vygenerovaný řetězec (challenge = výzva); klient přidá k řetězci heslo a vytvoří MD5 kontrolní součet vzniklého celku; tento kontrolní součet (nazývaný heš = hash) je odeslán ověřovacímu serveru; ten zná všechny potřebné vstupní údaje (řetězec výzvy, heslo i algoritmus MD5), vypočte si heš a porovná jej s tím co dostal od klienta; výhodou je to, že heslo není přenášeno po síti; CHAP umožňuje i ověřování v průběhu relace (na rozdíl od PAP, kdy ověření proběhne pouze na začátku).

MS-CHAP

Již v minulosti došlo k určitým modifikacím CHAP. Jednou z nich je úprava ověřovacího mechanismu CHAP provedená firmou Microsoft. Základní rozdíl je v tom, že namísto MD5 používá MD4. Novější varianta téhož – MS-CHAP2 zachovává hešovací funkci MD4 a navíc používá obousměrné ověřování.

Co je EAP?

Jak použití PPP narůstalo, lidi našli jeho omezení - jak v pružnosti, tak v úrovni zabezpečení zabudovaných jednoduchých metod ověřování (PAP, CHAP).

Většina podnikových sítí požaduje pro bezpečný přístup zajistit více než jednoduché jméno a heslo. Existovaly dvě cesty jak rozvíjet úspěšný protokol PPP, jenž se stal de facto standardem. První z nich byla změna specifikace protokolu a implementace nového mechanismu ověřování přímo do něj. Druhá byla vytvoření nového protokolu pro ověřování a vyvedení této části mimo PPP, přičemž bude zajištěno provázání obou protokolů.

Zvítězila druhá varianta. Byl vyvinut nový ověřovací protokol nazývaný "rozšiřitelný ověřovací protokol" (Extensible Authentication Protocol) - EAP. Tento protokol byl definován v RFC 2284 a následně revidován v RFC 2284bis. EAP byl původně určen pouze pro protokol PPP. Zajišťuje pro něj rámec (transportní mechanismus) pro všechny druhy ověřovacích metod, nicméně není jeho nedílnou součástí. Na serveru vzdáleného přístupu (RAS) je vytvářen tunel mezi klientem a skutečným ověřovacím serverem. Definice EAP mimo PPP, do samostatného protokolu, umožnilo jeho použití i v jiných prostředích. Např. modifikace EAP definovaná pod specifikací IEEEE 802.1x je v podstatě rozšíření EAP pro sítě typu 802.

EAP je alternativou k proprietárním ověřovacím systémům a umožňuje snadnou práci s hesly, tokeny i PKI certifikáty. Nezajišťuje ověřování jako takové, ale otevřený transportní mechanismus pro ověřovací systémy.

Standardizací EAP se zjednodušila kompatibilita systémů různých výrobců. Například - pokud používáte EAP jako ověřovací technologii pro PPP spojení, RAS nepotřebuje znát podrobnosti o vašem klientském ověřovacím systému. Pouze váš klient a ověřovací server musí být koordinovány. RAS server se na ověřování klienta podílí tím, že přebaluje pakety mezi EAP a RADIUS formátem a posílá je na ověřovací RADIUS server. Výsledek ověření předá RADIUS na RAS a ten jej použije pro pokračování nebo ukončení spojení.

Tak teď již víme co je to PPP a EAP a příště se podíváme podrobněji na IEEE 802.1x.

Technologie pro zlepšení bezpečnosti datových sítí - základní charakteristika IEEE 802.1x (2)

V prvním díle jsme si řekli co je to PPP a EAP a naznačili jsme si i co je IEEE 802.1x. Zjednodušeně řečeno, IEEE 802.1x je standard pro průchod EAP přes bezdrátovou nebo klasickou LAN. Dnes se podíváme na model protokolu 802.1x a základní komponenty.

V prvním díle jsme si řekli co je to PPP a EAP a naznačili jsme si i co je IEEE 802.1x. Zjednodušeně řečeno, IEEE 802.1x je standard pro průchod EAP přes bezdrátovou nebo klasickou LAN. 802.1x balí EAP do Ethernet rámců a nepoužívá PPP. Zajišťuje transportní mechanismus pro ověřování - nic víc.

Model protokolu - komponenty

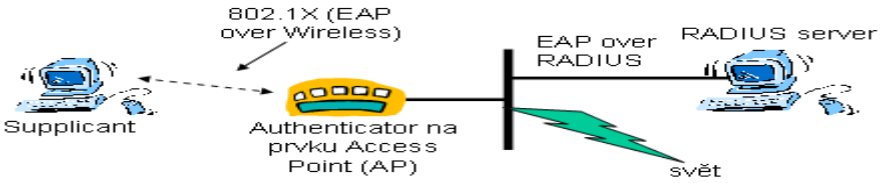
IEEE 802.1x používá 3 komponenty, které mají své pojmenování (jsem zvědav na jakých výrazech se jednou překlad ustálí a byť jsem si dovolil vznést návrh na pojmenování, nebudu výrazy používat a nechám je v dalším textu v originálu :-)

supplicant - uživatel nebo klient, který chce být ověřen ***(navrhuji výraz prosebník)***;

authentication server - ověřovací server, typicky RADIUS server;

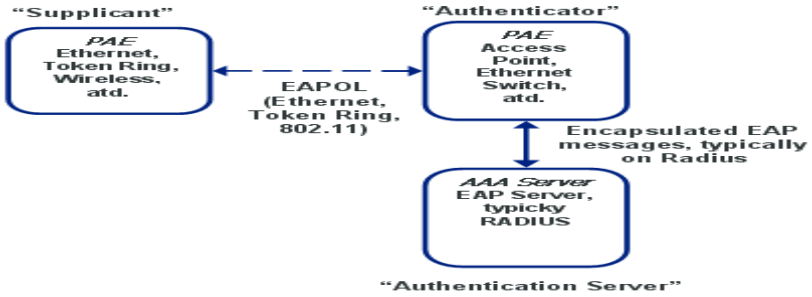
authenticator - zařízení mezi klientem a ověřovacím serverem; buď Access point nebo přepínač; ***(navrhuji výraz ověřovatel)***.

PAE (Port Access Entity) - (doplňková entita modelu, která je zmiňována pouze v části dokumentů) protokolová jednotka přičleněná k portu. Může podporovat funkčnost komponent Supplicant, Authenticator nebo obou.



Jednou z klíčových vlastností 802.1x je to, že ***authenticator*** může být jednoduchý a hloupý. Veškerá inteligence je v klientovi a ověřovacím serveru. To je ideální pro access pointy, protože jsou typicky poměrně jednoduché s malou pamětí a výkonem procesoru. Ovšem s tou jednoduchostí to nesmíme brát tak úplně doslova, protože kdyby byl ***authenticator***skutečně úplně hloupý, postrádal by 802.1x významnou část svého smyslu (viz. dále)!

Ještě jeden pohled na komponenty EAP.

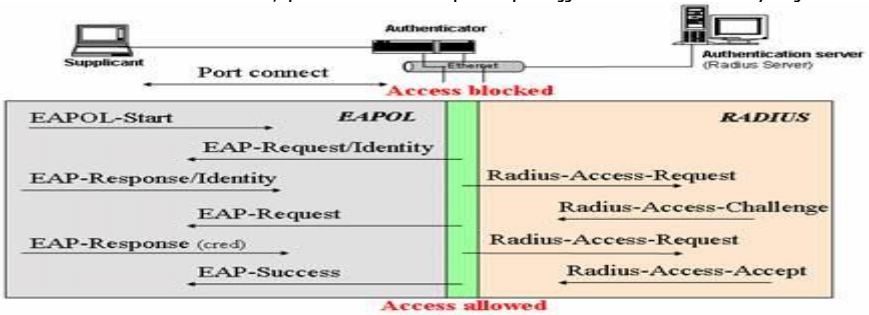


Příště se již podíváme na průběh ověřování.

Technologie pro zlepšení bezpečnosti datových sítí - průběh ověřování 802.1x (3)

Protokol 802.1x je také nazýván zkratkou EAPOL - tedy EAP over LANs. Je definován pro protokoly 802, tedy např. pro Ethernet (802.3), včetně bezdrátového 802.11 i pro sítě založené na technologii token ring (i pro FDDI - 802.8). EAPOL není zvláště složitý a v základní implementaci není úplně bezpečný - zejména u bezdrátových sítí.

Protokol 802.1x je také nazýván zkratkou EAPOL - tedy EAP over LANs. Je definován pro protokoly 802, tedy např. pro Ethernet (802.3), včetně bezdrátového 802.11 i pro sítě založené na technologii token ring (i pro FDDI - 802.8). EAPOL není zvláště složitý a v základní implementaci není úplně bezpečný - zejména u bezdrátových sítí. Na následujícím obrázku je popis práce protokolu. A abychom se do toho nezamotali, představíme si princip nejjednodušší metody s jednocestným ověřením.



0) **Supplicant** může nezávisle na tom zda dostal od **authenticator** požadavek poslat informaci o tom, že je zde a chce se přihlásit do sítě ("EAPOL-Start").

1) **Authenticator** posílá na **supplicant** požadavek na ověření totožnosti kleinta ("EAP-Request/Identity") v okamžiku, kdy dostane požadavek ("EAPOL-Start") nebo detekuje aktivní link

- v případě bezdrátové technologie se na access point snaží připojit nový klient (supplicant);
- v případě přepínače se stav portu (s aktivovaným 802.1x ověřováním) změnil z down na up.

2) **Supplicant** posílá na **authenticator** informaci o své totožnosti ("EAP-Response/Identity"); ten ji přebalí z EAP do RADIUS protokolu a posune ji na **authentication server** (RADIUS server).

3) **Authentication server** posílá zpět na **authenticator** výzvu pro ověření (challenge) - to je v podstatě řetězec znaků. **Authenticator** přebalí paket z formátu RADIUS do EAPOL a posílá jej na **supplicant** . Rozdílné ověřovací metody mají různé množství paketů v této části procesu (tzn. nemusí být pouze jednoduchý proces zobrazený na obrázku). EAP podporuje jak jednoduché ověření klienta tak i silné vzájemné ověřování. Pro použití v bezdrátových je vhodnější (slabý výraz), nutné vzájemné ověřování.

4) **Supplicant** na výzvu odpovídá **authenticatoru** (např. tak, že k výzvě přidá své heslo, provede hash a ten použije jako odpověď). Ten posunuje odpověď na **authentication server**.
5) Jestliže se **supplicant** prokáže řádnými údaji, **authentication server** odpoví zprávou o úspěšnosti, která je přeposlána na **supplicant**. **Authenticator** umožní přístup do sítě - s možností restrikcí na základě atributů od **authentication server**. Například přiřadí**supplicant** do konkrétní VLAN nebo nastaví filtrovací pravidla.
EAPOL má další možnosti, např.:

- zpráva ukončení práce od **supplicant** ("LOGFF"); pokud se supplicant odhlásí nekorektně (např. link na přepínači jde do stavu down nebo access point ztratí spojení s klientem), je na aktivním prvku ukončeno oprávnění a **supplicant** se musí opět ověřit;
- 802.1X také umožňuje definovat časovou prodlevu pro opětovné ověřování; **supplicant** se tak musí periodicky prokazovat.

Stav portů v procesu ověřování

V procesu ověřování se z hlediska logiky věci dělí porty na:

- controlled port - přijímá pakety od ověřených zařízení;

a

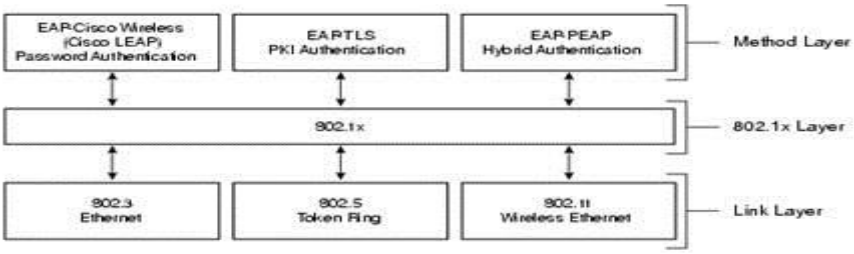
- uncontrolled port - přijímá pouze 802.1x pakety pro ověřování.

Přechod mezi stavy je dán výsledkem procesu ověření (z uncontrolled do controlled) a odhlášení nebo odpojení uživatele (z controlled do uncontrolled).

Typy ověřování

Již bylo řečeno, že EAP protokol zajišťuje pouze transportní mechanismus pro ověřování. Umožňuje to poměrně snadno vytvářet nové modifikace protokolu - ten se v principu nemění, pouze ověřovacímu mechanismu musí rozumět **supplicant** a **authentication server** . Uvádím ty nejznámější a nejzajímavější.
Architekturu se lze představit podle následujícího obrázku. Má tyto vrstvy:

- Linková vrstva - uzpůsobení konkrétní LAN technologii (definice specifických rámců);
- 801.1x vrstva - zajištění pravidel pro komunikaci komponentami systému (**supplicant**, **authenticator** a **authentication server);**
- vrstva ověřovací metody - řeší konkrétní metodu ověření uživatele; příslušných metod je mnoho, na obrázku je jich jmenována část, další jsou v popisu metod;



EAP-MD5 - (RFC 1994, RFC 2284); pro ověřování je používáno uživatelské jméno a heslo; ty jsou pro zajištění pravosti hashovány pomocí MD5; jde o původní specifikaci s jednocestným ověřováním; tento způsob se nejvíce blíží tomu co bylo představeno na schématu; další alternativy používají složitější mechanismus výměny informací a v navazovací sekvenci je více kroků.
EAP-OTP - (FRC 2289) One-Time Password; pro ověřování je použit některý ze systémů typu CRYPTOCard Token, RSA SecureID, SecureComputing SafeWord Token…
EAP-GTC - (Generic Token Card) - obdoba EAP-OTP.
EAP-TLS - (RFC 2716) Transport Level Security; pro ověřování použito PKI a SSL; mechanismus ověřování je založen na použití certifikátů, umožňuje vzájemné ověření klienta a sítě (tedy i síť prověřuje klientovi svou pravost); klíče jsou generovány dynamicky; tento verze byla zvolena jako základní pro implementaci ve Windows (2000 a XP).
O TLS se můžete více dozvědět v tutorialu SSL protokol a jeho akcelerace na odkazu http://www.svetsiti.cz/tutorialy.asp?id=177.
EAP-LEAP - (Lightweight Extensible Authentication Protocol); proprietární ověřovací mechanismus fy Cisco; podporuje vzájemné ověření klienta a sítě; je obdobou EAP-TLS, ale namísto certifikátů používá jméno a heslo; zajišťuje mechanismus dynamického generování klíčů pro WEP.
EAP-TTLS - (Tunneled TLS); rozšíření modifikace EAP-TLS, používá TLS pro navázání spojení s ověřovacím serverem a vytvoření tunelu pro druhý ("vnitřní") ověřovací algoritmus, ten je libovolného typu - PAP, CHAP...
EAP-PEAP- (Protected EAP); podobný TTLS, zajišťuje TLS k vytvoření tunelu pro druhý ověřovací algoritmus, ten je typu EAP.
Dále uvádím výčet některých používaných modifikací EAP:

- EAP AKA - Authentication and Key Agreement; připraveno pro použití v UMTS sítích;
- EAP SKE - Shared Key Exchange;
- EAP GPRS - modifikace pro GPRS

Technologie pro zlepšení bezpečnosti datových sítí - nasazení v praxi (4)
Jednou z důležitých možností 802.1x je schopnost nastavit WEP (Wired Equivalent Privacy) klíč pro bezdrátově připojené uživatele. Některé ověřovací metody (např. TLS, TTLS, LEAP…) vytvářejí "sdílené tajemství" jako vedlejší efekt ověřování. V dalším se pak podíváme na proprietární mechanismy Cisco a doporučení pro nasazení v praxi.
Vztah mezi ověřováním uživatele a šifrováním dat
Jednou z důležitých možností 802.1x je schopnost nastavit WEP (Wired Equivalent Privacy) klíč pro bezdrátově připojené uživatele. Některé ověřovací metody (např. TLS, TTLS, LEAP…) vytvářejí "sdílené tajemství" jako vedlejší efekt ověřování. Toto sdílené tajemství lze použít jako základ klíče pro WEP. Ovšem pozor - TLS tunel je při navazování spojení vytvořen mezi komponentami **supplicant** a **authentication server**. A WEP šifrování je zajištěno mezi komponentami **supplicant** a **authenticator**. **Authentication server** tedy musí posunout sdílené tajemství na **authenticator**.
Ověřování metodou 802.1x pomáhá zmírnit rizika používání WEP. Například hodně velkou slabinu WEP, jíž je dlouhodobá životnost klíčů a jejich sdílení mezi uživateli. Při použití 802.1x jsou unikátní WEP klíče generovány pro každé spojení. Authenticator (access point) také může mít nastavenu pravidelnou změnu klíčů s vyšší frekvencí - např. každých n minut a/nebo m rámců.

Nasazení 802.1x samo o sobě negarantuje zlepšení bezpečnosti, ale nabízí silný potenciál, který při správné implementaci zlepšení zajistí.

Proprietární mechanismy Cisco

Základní rozdíl mezi dnes běžně dostupnými prvky levných výrobců a značkovými produkty výrobců zaměřených na podnikovou sféru je především v úrovni bezpečnosti. Levní výrobci těží ze standardů, které se snaží dodržovat, ale nerozvíjejí je a spoléhají na mechanismy, které jsou již dávno překonané. Progresivní výrobci (a i když zde uvádím pouze Cisco, protože jeho produkty znám nejlépe, je to záležitost širší škály) se snaží implementovat mechanismy, které odstraňují známé problémy na základě nových standardů (802.1x), případně definují nové mechanismy, které mají potenciál stát se základem dalších standardů. A nebo alespoň při podílu na trhu a tím i masovosti nasazení mechanismu, dochází k jejich přejímání dalšími výrobci a tím i dalšímu nárůstu množství produktů podporujících „nestandard" a tím zmírnění negativních vlastností používání nestandardu (viz. např. LEAP).

Proprietární mechanismus fy Cisco nazývaný **TKIP** (Temporal Key Integrity Protocol) zajišťuje zlepšení bezpečnosti šifrování dat na bezdrátových sítích – tedy snaží se eliminovat základní nedostatky protokolu WEP. Jeho lepší bezpečnost je zajištěna použitím těchto mechanismů:

- **PPK** (*per-packet key hashing*), umožňuje změnu klíče pro každý paket; tím je odstraněna slabina standardní definice WEP, jež pracuje se statickým klíčem, ten se během spojení nemění (a není-li použit protokol 802.1x se vynuceným pravidelným ověřováním, nemění se dlouhodobě);
- **MIC** (*Message Integrity Check*), je v podstatě digitální podpis nesený v každém paketu; tím je odstraněna možnost útoku nazývaného "man-in-the-middle", tedy takového útoku, kdy útočník zachytává pakety od vysílajícího, modifikuje je a posílá příjemci;
- **rotace broadcastových klíčů** ; PPK zajišťuje změnu klíčů pro unicastovou komunikaci; protože je 802.11 založen (jako všechny 802.x sítě) na broadcastovém mechanismu, je nutné zajistit změnu i klíčů používaných pro broadcasty a multicasty.

Nasazení v praxi

Bezdrátové sítě

Samozřejmě záleží na místě kde je síť použita. Pokud si pořídím bezdrátovou síť domů, asi bude požadované zabezpečení na jiné úrovni než když budu používat bezdrátovou síť v korporátní síti.

V prostředí domácnosti se pokusím aplikovat co nejvíc integrovaných metod zabezpečení (nestandardní ssid, vypnutí broadcastingu ssid, MAC filtering, WEP) a nastavím si oprávnění na OS (příp. s použitím personal firewallu). Tím jsem udělal asi maximum - těžko předpokládat, že si domů pořídím RADIUS server a access point s podporu 802.1x.

Bezdrátové sítě v podnikové sféře by měly používat ověřování s použitím 802.1x a některou z metod vzájemného ověřování s generováním klíče pro WEP (např. EAP-TLS, PEAP nebo LEAP)! Případně se vyplatí jít do proprietárního řešení některého ze silných výrobců s významným podílem na trhu (viz. např. již zmiňované Cisco).

Více o problematice zabezpečení, včetně popisu slabiny WEP je popsáno v dokumentu "Doporučení pro konfiguraci WiFi sítí".

LAN síť postavená na přepínačích

Použití moderních aktivních prvků se stanicemi vybavenými vhodným operačním systémem umožní zabezpečit přístup do sítě LAN pouze pro oprávněné uživatele. Neoprávnění uživatelé mohou skončit ve VLAN "karanténa" nebo nejsou do sítě vpuštěni vůbec (port na němž se pokoušejí přihlásit je zablokován a přijímá pouze rámce 802.1x).

Na rozdíl od bezdrátových sítí, kde je doporučováno vzájemné ověření uživatele a sítě, navíc vytvářejícího předpoklad generování klíče pro WEP, stačí v případě ověřování na přepínači jednoduché ověření (např. výše popisované ověřování MD5). Stavy ukončení pokusu o autorizaci mohou v závislosti na konfiguraci přepínače a oprávněnosti uživatele být:

- vpuštěn do sítě - pokud na portu přepínače není zapnuto ověřování 802.1x (bez ohledu na stav 802.1x klienta, ten totiž většinou bere ověření jako vstupenku na koncert – pokud ji nikdo nechce, vstoupí zadarmo);
- port zablokován
- - pokud je na portu přepínače ověřování zapnuto a klient je oprávněn;
- - pokud je ověřování na přepínači zapnuto, ale klient jej nepodporuje;
- - pokud je ověřování na přepínači zapnuto, a klient nemá oprávnění.

Uzly nepodporující 802.1x - např. tiskárny..., mohou být zapojeny do speciální VLAN, jejíž spojení s okolním světem je omezeno filtrovacími pravidly na aktivních prvcích. Např. pouze na definované tiskové servery s definovaným protokolem - ve většině sítí totiž není nutné aby stanice viděli přímo na tiskárny - a navíc např. v definovaném směru navazování komunikace (od serveru s frontou k tiskovému serveru).

Doplňkovou funkcí ověřování pomocí 802.1x může být např. přiřazení uživatele do VLAN na základě výsledku ověření (tím pádem i IP adresa a filtry zajišťující omezení přístupu klienta do ostatních částí sítě).

Technologie pro zlepšení bezpečnosti datových sítí - na co je potřeba si dát pozor; přehled produktů (5)

Zejména na zvolený formát a podporu na vybraném produktu. Např. LEAP je proprietární technologie fy Cisco a těžko ji hledat na produktech jiných výrobců (byť se najdou výrobci, kteří tento formát podporují). V závěru si uvedeme přehled produktů podporující 802.1x.

Zejména na zvolený formát a podporu na vybraném produktu. Např. LEAP je proprietární technologie fy Cisco a těžko ji hledat na produktech jiných výrobců (byť se najdou výrobci, kteří tento formát podporují). V závěru si uvedeme přehled produktů podporující 802.1x.

Je tedy potřeba zvážit možnosti všech systémů zúčastněných v procesu:

supplicant - ne všechny klienti podporují všechny metody; dokonce některé klíčové prvky nepodporují EAP ani WEP (typickým příkladem jsou PTC používané ve skladovém hospodářství);

authenticator - ne každý prvek podporuje EAP; některé sice tyto pakety přenášejí, ale nejsou schopni s EAP smysluplně pracovat (a na co je nám přenesený paket, když nedojde k zastavení neoprávněného návštěvníka na vstupu);

authentication server - ne každý RADIUS server podporuje EAP a pakliže ano, nemusí podporovat zvolenou ověřovací metodu (GTC, TLS, TTLS, LEAP…).

Produkty podporující 802.1x

Nutno podotknout, že seznam není úplný. Ovšem na druhou stranu – u starších produktů a levných výrobců je pravděpodobnost podpory malá.

RADIUS Servery

- Microsoft
- OS Support: Windows 2000 Server, Windows .NET Server

- EAP Methods: EAP-MD5, EAP-TLS
- Cisco Secure ACS v3.0 For Windows
- OS Support: Windows NT Server 4.0, Windows 2000 Server
- EAP Methods: Cisco LEAP, EAP-CHAP, EAP-TLS
- Funk Odyssey
- OS Support: Windows 2000 Server, Solaris, Netware
- EAP Methods: EAP-TLS, EAP-TTLS, EAP-MD5, Cisco LEAP
- Interlink
- OS Support: Solaris, HP-UX, Tru64 Unix, Red Hat Linux
- EAP Methods: EAP-MD5, Cisco LEAP
- FreeRadius
- OS Support: Linux, Solaris, HP-UX, AIX, OS/2, MINGW32
- EAP Methods: EAP-MD5

RADIUS server fy Funk Software byl dodáván i pod označením Nortel Networks BaySecure Access Control (BSAC).

Wired/Wireless Supplicants

- Microsoft
- OS Support: Windows XP
- EAP Methods: EAP-MD5, EAP-TLS
- Meeting House Data Communications
- OS Support: Win 98/ME, Win NT, Win 2000, Linux
- EAP Methods: EAP-MD5, EAP-TLS
- Funk Odyssey Client
- OS Support: Windows XP/NT/2000/98/ME
- EAP Methods: EAP-MD5, EAP-TLS, EAP-TTLS, Cisco LEAP
- University of Maryland Open1X
- OS Support: Linux, FreeBSD
- EAP Methods: EAP-TLS
- Cisco 802.1x Supplicant
- OS Support:Win XP/NT/2000/98/95/ME/CE, Linux, Mac OS 9.X
- EAP Methods: Cisco LEAP, PEAP, EAP-TLS, EAP-MD5

Ethernet Switch Authenticators

- HP
- Products: ProCurve 25xx, 410x, 530x
- Cisco
- Products: Catalyst 2950, 3550, 4000, 5000, 6000 (pouze některé verze IOS a HW moduly)
- Enterasys
- Products: Matrix E7/E6 Blades Firmware 5.02.03
- Nortel
- Products: BayStack 450, BayStack 470, BayStack 425, Business Policy Switch, produkty s BoSS 3.0

802.11 AP Authenticators

- Cisco
- Products: Aironet 350, Aironet 1100, Aironet 1200
- Enterasys
- Products: RoamAbout R2
- Agere System Orinoco
- Products: AP-2000 Access Point
- Symbol
- 3Com
- Products: WLAN Access Point 8000