Západočeská univerzita v Plzni
FAKULTA PEDAGOGICKÁ
KATEDRA VÝPOČETNÍ A DIDAKTICKÉ TECHNIKY

AUTENTIZAČNÍ PRINCIPY A METODY V POČÍTAČOVÝCH SÍTÍCH

BAKALÁŘSKÁ PRÁCE

Michal Cagáň
Učitelství pro 2. stupeň ZŠ, obor VT-Te

Vedoucí práce: Dr. *Ing. Jiří Toman*

Plzeň, 2013

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 25. červen 2013

……

vlastnoruční podpis

Tímto bych rád poděkoval vedoucímu své bakalářské práce, Dr. Ing. Jiřímu Tomanovi, za maximální vstřícnost a ochotu při konzultování práce a dále za umožnění přístupu k pracovním stanicím.

vlastnoruční·podpis

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta pedagogická
Akademický rok: **2010/2011**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michal CAGÁŇ**
Osobní číslo:	**P08B0505P**
Studijní program:	**B1001 Přírodovědná studia**
Studijní obor:	**Informatika se zaměřením na vzdělávání**
Název tématu:	**Autentizační principy a metody v počítačových sítích**
Zadávající katedra:	**Katedra výpočetní a didaktické techniky**

Zásady pro vypracování:

1. Popište základní principy a pravidla autentizace v počítačových sítích.
2. Charakterizujte princip autentizace v eDirectory.
3. Charakterizujte systémy autentizace v síťových OS MS Srv2008 a OS Linux.
4. Zaměřte se na autentizační systém Kerberos, demonstrujte popisem a ukázkami ve výpočetním prostředí ZČU.
5. Na stanici s volitelným operačním systémem prakticky realizujte, vyzkoušejte a popište konfiguraci systému Kerberos v prostředí ZČU.

Rozsah grafických prací:

Rozsah pracovní zprávy: **30 - 50 stran + CD**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. [s.l.] : Computer Press, 2004. 200 s. ISBN: 80-251-0106-1.

2. Massachusetts Institute of Technology [online]. 2010, 4.8.2010 [cit. 2010-10-18]. Kerberos: The Network Authentication Protocol. Dostupné z WWW: ⟨http://web.mit.edu/kerberos/www/⟩.

3. Novell [online]. 2010 [cit. 2010-10-18]. Novell eDirectory. Dostupné z WWW: ⟨http://en.wikipedia.org/wiki/Novell_eDirectory⟩.

4. ZČU, server uživatelské podpory [online]. 2010 [cit. 2010-10-18]. Kerberos. Dostupné z WWW: ⟨http://support.zcu.cz/index.php/Kerberos⟩.

Vedoucí bakalářské práce: **Dr. Ing. Jiří Toman**
Katedra výpočetní a didaktické techniky

Datum zadání bakalářské práce: **1. listopadu 2010**

Termín odevzdání bakalářské práce: **30. června 2011**

Doc. PaedDr. Jana Coufalová, CSc.
děkanka

L.S.

Doc. Ing. Václav Vrbík, CSc.
vedoucí katedry

V Plzni dne 3. listopadu 2010

OBSAH

1 ÚVOD

Počítačová síť se stala, stejně jako v nedávné době počítače samotné, běžnou, ne-li neodmyslitelnou součástí našeho života. Zásadní vliv na tuto skutečnost má samozřejmě internet, který nabízí den ode dne další možnosti využití. Přistupujeme k vzdáleným datům, poskytujeme osobní údaje, vystupujeme jako skutečná osoba ve virtuálním světě. Ať se jedná o prostou výměnu zpráv, přístup k internetovému bankovnictví, nebo synchronizaci podnikových aktivit, vždy vystavujeme přenášená data, a tedy i sebe samotné, riziku narušení soukromí. Z dosud uvedeného vyplývá potřeba umožnit přístup k těmto datům pouze autorizovaným osobám. Zajistit bezpečnost připojení fyzicky je často neproveditelné, v případě sítě internet nereálné.

Cílem této práce je seznámení se s oblastí ověřování uživatelů a entit počítačových sítí. Práce charakterizuje systémy autentizace v různých prostředích a operačních systémech. Pro lepší pochopení problematiky je zde uveden popis a názorné ukázky autentizace v prostředí ZČU skrze protokol Kerberos. Dále je prostor věnován také jednotlivým metodám ověření identity a obecně používaným autentizačním protokolům.

2 AUTENTIZACE

Počítačová síť je systém, vytvořený propojením počítačů za účelem vzájemné komunikace a výměny informací. Aby nedošlo k neoprávněnému přístupu a následnému zneužití získaných informací, je nezbytné zajistit do síťového systému přístup pouze povolaným subjektům. Proces, který tento požadavek zajišťuje, se nazývá autentizace. Tímto se stává základním bezpečnostním prvkem, jež ověřuje, zda je uživatel či entita skutečně tím, za koho se vydává. Cílem autentizace je zabezpečení virtuální identity uživatele nebo entity a následné určení přístupu ke konkrétním prostředkům systému. Dochází zde tedy nejen k ověření identity ale také rozlišení přístupových práv určitého subjektu. Úmyslně nevolíme slovo „uživatel“, neboť ve smyslu počítačového systému dochází rovněž k autentizaci počítačů, serverů, aplikací a procesů. V této práci, pokud nebude řečeno jinak, bude však slovem „uživatel“ míněna kterákoliv samostatně vystupující entita (počítač, server, proces, apod.)

V rovině operačního systému přistupujeme ke vzdáleným prostředkům nejčastěji skrze určité aplikace. Z výše uvedeného vyplývá potřeba zajistit spolehlivý přístup těchto aplikací k jednotlivým částem subsystému. Vyspělý operační systém by tedy měl zabezpečit komunikaci mezi aplikacemi a hardwarem připojeného počítače (vstupní/výstupní zařízení, paměť apod.). S rostoucí důvěrností přenášených dat pochopitelně roste požadavek na bezpečnost, případně utajení. Řada aplikací vyžaduje konkrétní typy zabezpečení, které byly postupem času implementovány jako součást operačních systémů. Dále není třeba dodatečně řešit zabezpečení formou nadstavby systému a ztěžovat tak práci uživatelům a aplikacím. Tímto je značně redukován výskyt omezení a chyb, případně zanedbání bezpečnosti systému vůbec.

2.1 AUTENTIZAČNÍ ČÁSTI

Prvním krokem k zahájení autentizace je odeslání přihlašovacích údajů (credentials) skrze komunikační mechanismy autentizační autoritě (authentication autority). Tou může být buď lokální pracovní stanice (v případě interaktivního příhlášení) nebo centrální autentizační server (v případě neinteraktivního přihlášení). V praxi to znamená, že autentizační služba (authentication service) vyzve uživatele k zadání přihlašovacích údajů (typicky uživatelského jména a hesla), které následně předá autentizační autoritě, a ta je porovná s údaji verifikační tabulky uloženými ve své databázi (credentials database). Pokud zadané údaje souhlasí s údaji v databázi, povolí autentizační autorita na základě práv přiřazených subjektu přístup do konkrétních částí systému. Tato fáze autentizace se označuje jako login-fáze. Obvykle bývá úspěšně autentizovanému uživateli udělen tzv. token, kterým se uživatel dále prokazuje při žádostech o přístup k dalším zdrojům v systému autorizační autority.

2.2 BEZPEČNOST AUTENTIZAČNÍHO SYSTÉMU

„Systém je nejvýše tak bezpečný, nakolik bezpečné je jeho nejslabší místo.“ Toto pravidlo samozřejmě platí i o systému autentizace. Má-li být autentizace, z bezpečnostního hlediska, klíčovým článkem systému, určuje sílu systému právě úroveň autentizační infrastruktury. Celá tato problematika je součástí bezpečnostní politiky (security policy). Zde se nabízí celá řada aspektů. Mezi ty nejzásadnější patří použité autentizační metody, použité autentizační protokoly a v neposlední řadě způsob uložení přihlašovacích údajů v databázi.

2.3 TYPY AUTENTIZAČNÍCH METOD

S rozšířením síťové komunikace do sfér se zvýšenou cenou přenášených dat (např. bankovnictví) vzrostly logicky nároky na bezpečnost poskytované autentizace. Bezpečnost autentizace je zásadní měrou dána kvalitou přístupových údajů a metodou získání autentizační informace. V případě, že autentizační autorita využívá více než jednu z těchto metod ověření identity, jedná se o tzv. vícefaktorovou autentizaci. Samozřejmě vícefaktorová autentizace poskytuje vyšší míru zabezpečení, je však technicky podstatně náročnější.

Existují tři základní způsoby, jak uživatel může dokázat svou identitu. Je to důkaz znalostí, důkaz vlastnictvím a důkaz vlastností.

2.3.1 DŮKAZ ZNALOSTÍ

„To, co uživatel zná“ je bezpochyby nejpoužívanější a nejrozšířenější autentizační metoda. Důkaz znalostí je typickým příkladem jednofaktorové autentizace, kdy je rozhodující znalost uživatelského jména a hesla, nejčastěji zadaného z klávesnice. Úroveň zabezpečení touto metodou určuje z velké části kvalita hesla. Ideálně je to jeho maximální možná délka a použitá množina znaků.

Hlavní nevýhoda je právě potřeba zapamatovat si příliš složité heslo. Vlivem bezpečnostní politiky se navíc objevuje požadavek na jeho častou změnu. Uživatel se tak nezřídka uchyluje k zapisování hesel na různá místa, čímž dává příležitost potencionálnímu útočníkovi.

Zvláštním typem hesla je tzv. PIN (Personal Identification Number). Nejčastěji je tvořen pouze čtyřmi znaky (čísly). Zabezpečení je zajištěno omezením počtu pokusů ke správnému zadání PINu, obvykle spolu s formou nějakého tokenu (nejčastěji čipová karta).

„Metody založené na znalosti hesla jsou základem pro všechny autentizační protokoly. Ať je totiž autentizační informace získána jakýmkoliv způsobem, v konečné podobě musí být vždy převedena do digitální podoby – jakési obdoby hesla. Z hlediska dalších protokolů nemá přitom smysl rozlišovat, zda se jedná o skutečné heslo, nebo například digitální otisk získaný analýzou otisku prstu.“ (DOSEDĚL, T., 2004, s. 67).

2.3.2 DŮKAZ VLASTNICTVÍM

„To, co uživatel má.“ Tento způsob získání autentizační informace od uživatele je považován za vyšší míru zabezpečení. Důvody jsou zřejmé již z názvu. Podmínkou je vlastnictví určitého předmětu (token), jenž má schopnost nést informace převoditelné do elektronické podoby – např. USB klíčenka, čipová karta, apod. V tomto směru nabízí současné technologie poměrně široké spektrum zařízení, schopných autentizační informaci nejen uchovávat, ale také generovat (smart karta). Díky tomu může být takový token aplikován i na protokol typu

výzva-odpověď. Na rozdíl od lidské paměti má token schopnost pamatovat si mnohem delší a složitější řetězec znaků, a tím spolu s nutností mít tento předmět pro ověření identity u sebe poskytuje onu kýženou úroveň zabezpečení.

Veškerá zabezpečení však ztrácí smysl v případě ztráty nebo odcizení tokenu. Abychom takovému zneužití tokenu zamezili, je vhodné doplnit důkaz vlastnictvím některou z dalších metod ověření (např. čipová karta a PIN). Další nevýhodou je zvýšená cena za bezpečnost, neboť většina tokenů vyžaduje zvláštní zařízení pro jeho připojení (čtečka karet, snímače, apod.).

2.3.3 DŮKAZ VLASTNOSTÍ

„To, čím uživatel je.“ Tato metoda získání autentizační informace spočívá v sejmutí některé z biometrických vlastností uživatele – otisk prstu, obraz oční duhovky nebo obličeje, apod. Tyto údaje jsou u každého člověka jedinečné. Na rozdíl od hesla nebo tokenu, který může použít kdokoliv, je tento způsob bezprostředně svázán s konkrétním uživatelem. Pomineme-li „drastické“ získání autentizační informace, můžeme mít teoreticky jistotu, že se skutečně autentizuje příslušný uživatel, nikoli útočník skrze počítač. Stejně jako předchozí metody má i tato své úskalí.

Z technologického hlediska je získání autentizační informace touto metodou relativně náročný a nákladný proces. Protože se fyzické charakteristiky každého člověka mohou lišit jen nepatrně, je důležitá vysoká rozlišovací schopnost snímacího zařízení. Ani poté nemusí být zaručena pravost sejmutého vzorku – tzv. živosti (liveness-test). Aby nemohlo dojít k úspěšné autentizaci podstrčením například uměle vytvořeného otisku prstu nebo modelu tvaru obličeje, zahrnují se do procesu ověření další fyziologické vlastnosti uživatele – puls, teplota či elektrický odpor pokožky. S tím ale přirozeně roste cena technologie.

BEHAVIOMETRIKA

Dalším důkazem vlastností uživatele je tzv. behaviorální charakteristika. Stejně jako jsou jedinečné některé biometrické vlastnosti uživatele, je unikátní i jeho chování. Je možné kontrolovat počet úderů, dynamiku, případně rytmiku při psaní na klávesnici. Dále existuje forma elektronického podpisu, kde sledujeme

rychlost, dynamiku, držení stylusu (obdoba elektronické tužky), jeho přitlačení k podložce v různých fázích podpisu atd.

Výhodou behaviometriky je získávání údajů po celou dobu přístupu do systému a tím průběžná odezva, zda skutečně v systému pracuje oprávněný uživatel. Oproti biometrice je tato metoda fyzicky nenapodobitelná.

U obou metod může nastat komplikace, neboť s postupem času nebo stavu uživatele se některé, ať behaviorální nebo biometrické, vlastnosti mění. Je tedy třeba nastavit tomuto systému toleranci. S tím souvisí jistá nespolehlivost a vznik dvou chybových stavů. Zaprvé je to případ, kdy je oprávněnému uživateli zamítnut přístup (tzv. False Rejection Rate – FRR). Druhá chyba nastane, když je přístup povolen neoprávněnému uživateli (tzv. False Acceptance Rate – FAR). Proto se oba způsoby zároveň doplňují o další metodu ověření, nejčastěji heslem nebo PINem.

2.4 AUTENTIZAČNÍ ALGORITMY SÍŤOVÝCH SLUŽEB

Protože autentizace uživatele probíhá skrze otevřené (nezabezpečené) síťové prostředí, jsou přenášená data v potenciálním nebezpečí. Proto je vzhledem k povaze autentizačních údajů (hesla, PIN-kódy apod.) nezbytné zajistit bezpečnost jejich přenosu k autentizační autoritě a zabránit tak možnému zneužití pro neoprávněný přístup do vzdáleného systému v případě odposlechu. Jako řešení, které by tuto podstatnou část ověřování obstaralo, se nabízí šifrování autentizačních dat. Ač poskytuje tato metoda poměrně velký prostor k utajení tajemství, např. formou jednosměrné šifrovací funkce – hashování, není sama o sobě ideálním řešením. Pro úspěšnou autentizaci do systému může totiž případnému útočníkovi stačit i pouze odposlechnutý hash nebo šifrovaná autentizační data.

2.4.1 ZÁKLADY KRYPTOGRAFIE

Kryptografické metody zajišťují utajení obsahu zprávy pomocí tajné informace. Tou je tzv. šifrovací klíč. Kryptografie dělíme na dvě základní skupiny:

Symetrická kryptografie - využívá k zakódování i dekódování zprávy stejný klíč. Obvyklá délka klíče v současných kryptografických protokolech je mezi 128 a 256 bity. Nejznámějšími šiframi, dosud považovanými za bezpečné, jsou 3DES (Tripple Data Encryption Standard) a AES (Advanced Encryption Standard). Výhodou symetrické kryptografie je rychlost (de-)kódování, ta ke standardně až tisíckrát větší než u srovnatelně bezpečných asymetrických metod. Nevýhodou je pochopitelně potřeba znalosti klíče u obou stran komunikace.

Asymetrická kryptografie - využívá dvojice klíčů - tzv. veřejný a privátní klíč. Pomocí veřejného klíče jedna strana komunikace zašifruje zprávu a druhá strana ji privátním klíčem dešifruje. Jak již název napovídá, veřejný klíč je volně dostupný, naproti tomu privátní klíč je nutné držet v tajnosti. Bezpečnost asymetrické kryptografie spočívá v principu složitosti prvočíselného rozkladu násobku dvou velkých prvočísel nebo počítání diskrétního logaritmu. Délky klíčů se pohybují v rozmezí 1024 až 2048 bitů. Nejznámější asymetrickou šifrou je RSA (dle iniciálů autorů Rivest, Shamir, Adleman). (PIPER, F., MURPHY, S., 2002, s.33).

2.4.2 AUTENTIZAČNÍ PROTOKOLY

Autentizační protokoly pracují spolu s využitím kryptografických metod na principu výzva-odpověď. Díky implementaci tohoto způsobu komunikace je možné zajistit více bezpečnostních faktorů procesu ověřování, záleží na konkrétním typu použitého protokolu. Typicky je to odpověď na jedinečný dotaz, kdy sledujeme správnost tvrzení a tedy znalost sdíleného tajemství. Zde se patrně nejvíce uplatní metod symetrického a asymetrického šifrování a hashovacích funkcí. Pomocí hashů lze rovněž prokázat autentičnost a integritu přijatých dat. Dále se nabízí možnost využití tzv. časových razítek zpráv a tím eliminovat rizika v případě útoku opakováním hesla. Protože autentizační protokol obstarává hlavní komunikační kanál mezi klientem a autentizační autoritou, je většina útoků mířena právě na něj. Správně vytvořený autentizační protokol nesmí odesílat otevřenou sítí heslo ve formátu prostého textu (plain-textu), ale pouze hash hesla. (DOSEDĚL, T., 2004, s. 75).

Protokolů zajišťujících autentizaci existuje velké množství, liší se pro svůj účel i způsobem šifrování. V jednotlivých kapitolách této práce se budu zabývat protokoly, které jsou implementovány v systémech eDirectory, Server 2008 a Unix.

Příklady některých obecně využívaných autentizačních protokolů

SSL a TLS

SSL (Secure Sockets Layer) a TLS (Transport Layer Security) jsou v zásadě stejné protokoly (TLS je nástupce SSL) a jsou běžnou součástí skupiny protokolů TCP/IP (hlavní protokol světové sítě internet), kde zajišťuje šifrování přenosu a autentizaci obou stran komunikace. Ověřením identity uživatele a serveru dojde k vytvoření zabezpečené relace (session). SSL je rovněž využíván jako rozšiřující součást protokolu HTTP-S.

Princip ověření identity pomocí protokolů SSL/TLS spočívá v použitém algoritmu asymetrické kryptografie (standard pro systémy založené na veřejném klíči x.509) a metodou výzva odpověď. Každá strana komunikace tedy vlastní jeden pár šifrovacích klíčů – soukromý a veřejný. Samotná komunikace je šifrována společným klíčem relace (symetrická kryptografie), který je vytvořen během autentizace.

Zjednodušené schéma komunikace:

1. První spojení logicky zahajuje klient formou nezabezpečeného kanálu. Odešle tedy serveru požadavek na vytvoření relace - zprávu s údaji o verzi SSL, typem šifry apod.
2. Server pošle uživateli odpověď spolu se svým certifikátem veřejného klíče.
3. Uživatel dle certifikátu veřejného klíče ověří autentičnost serveru. Dále vygeneruje náhodné číslo tzv. pre-master secret, které zašifruje tímto veřejným klíčem a odešle jej zpátky serveru.
4. Server zjistí pomocí svého soukromého klíče obsah zprávy. Obě strany komunikace mají v tuto chvíli pre-master secret, z kterého vygenerují hlavní klíč relace. Tímto klíčem bude šifrována následná komunikace [1].

RADIUS

Obecný protokol pro vzdálené přihlašování (Remote authentiaction for dial-in user service). Klient A se přihlašuje na autentizační server B (RADIUS server). Autentizaci zahajuje klient zasláním svého požadavku (s hashem hesla). Server odpovídá jednou ze tří možných zpráv: odmítnutím či přijetím autentizačního požadavku, nebo požadavkem na další komunikaci podle zvoleného protokolu (většinou výzva-odpověď). RADIUS tak může poskytovat autentizační služby dalšímu protokolu. (DOSEDĚL, T., 2004, s. 75).

Mezi nejsilnější vlastnosti patří jeho vysoká bezpečnost, protože komunikace mezi klientem a RADIUS serverem je autentizována pomocí sdíleného tajemství, které není nikdy posíláno přes síť. Všechna uživatelská jména jsou přes síť zasílána šifrovaně. Uživatelské heslo je přenášeno metodou založenou na RSA Message Digest algoritmu MD5 [2].

3 KERBEROS

Kerberos je síťový autentizační protokol umožňující vzájemné ověření totožnosti entit v nezabezpečeném síťovém prostředí, konkrétně v aplikacích typu klient/server. Rovněž dokáže zajistit integritu přenášených dat. Systém Kerbera je postaven na principech Needham-Schroeder Symmetric Key protokolu, vytvořeném v roce 1978. Jak už předchozí věta napovídá, jeho bezpečnost je založena na symetrickém šifrování. Za svůj vznik vděčí výzkumnému institutu MIT (Massachusetts Institute of Technology), který Kerberos vyvinul pro univerzitní účely v rámci projektu Athena. V roce 1993 se objevila pátá verze protokolu, určená pro veřejnost. Právě verze 5 je předmětem této práce. MIT dává k dispozici zdrojový kód pod licencí velmi podobné licenci BSD. Protokol je integrován jako součást mnoha aplikací (např. Active Directory) a je výchozím bezpečnostním protokolem systémů Microsoft Windows 2000 (a vyšších verzí). Kerberos je multiplatformní. Jeho implementaci nalezneme i v platformách na bázi Unix. Své jméno získal tento protokol podle tříhlavého psa řecké mytologie - Kerbera, který střeží vchod do podsvětí.

Celý systém tvoří tři hlavní části: uživatel, aplikace (služba) podporující Kerberos a konečně autentizační server Kerberos. První dvě jmenované části nesou jednoznačné označení, tzv. principal a jsou registrovány na serveru Kerbera. Podporované aplikace autentizují uživatele na základě přihlašovacích údajů Kerbera - tzv. credentials.

Autentizace mezi uživatelem a službou není založena na vzájemné důvěře, ale na důvěře třetí straně. Třetí stranou je myšlen právě server Kerberos – tzv. Key Distribution Center (dále jen KDC). Zde je soustředěna infrastruktura celého systému Kerberos, která se dále větví na dvě části. Tou první je Autentizační Server (dále jen AS), jež obstarává ověření identity obou stran komunikace. Druhou částí KDC je Ticket-Granting Server (dále jen TGS). Jak již název napovídá, hlavním účelem této služby je poskytování tzv. Ticket Granting Ticket (dále jen TGT), pomocí kterých se obě strany komunikace vzájemně prokazují. Ověření tedy nespočívá v odeslání hesla nebo certifikátu, což je zásadním bezpečnostním

prvkem. Tikety dále obsahují časové razítko tzv. Time-Stamp (dále jen TS), ty znesnadňují případnému útočníkovi prolomení zabezpečení komunikace, neboť mají omezenou dobu platnosti. Tikety se během komunikace mění podle právě prováděné akce. KDC i klient-principal vlastní svůj vlastní klíč. Tyto klíče má uložen KDC formou hashe a slouží k šifrování komunikace a prokázání identity (viz. níže). Kerberos samozřejmě podporuje mezi servery systém jediného přihlášení - SingleSignOn (dále jen SSO) [3][4].

3.1 KERBEROS A DALŠÍ MOŽNOSTI AUTENTIZACE

Vzhledem k množství typů aplikací a služeb bylo třeba zajistit další možnosti získávání tiketů.

Forwardable - pro potřeby získání přístupu ze vzdáleného počítače. Uživatel pošle na KDC žádost obsahující adresu počítače a TGT tiket, čímž zajistí stejný relační klíč pro komunikaci s požadovaným počítačem.

Proxiable - opět mohou být přeposlány na jiný počítač, avšak slouží pouze pro přístup ke službě. Není možné získat plnohodnotný TGT tiket.

Renewable - lístky nesou dvě doby platnosti. Standardní doba platnosti je opakovaně prodloužitelná do chvíle, než vyprší maximální, tzv. vyměnitelná doba platnosti.

Postdated - umožňuje získat přístup k aplikacím, které se budou používat v určitou dobu. Tento tiket, podobně jako předchozí, obsahuje časová razítka s dobou platnosti typu od/do.

Volitelně je možné nainstalovat také následující balíčky pro podporu kerberizovaných klientů (ftp, telnet, ssh):

- krb5-clients
- ssh-krb5

3.2 POPIS A SCHÉMA OVĚŘENÍ PROTOKOLU KERBEROS

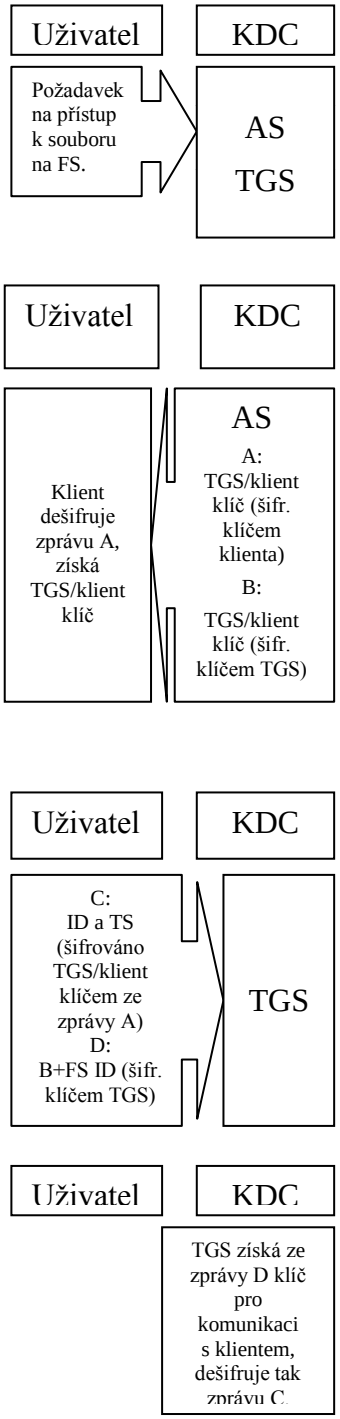


Diagram 1, Schéma ověření Kerberos 1.část

Uživatel pošle KDC serveru skrze klienta požadavek na přístup k souboru umístěného na cílovém serveru FS (file server). Tento požadavek je směřován na AS. AS vrátí klientu dvě zprávy - A a B.

A- Zpráva A obsahuje klíč pro komunikaci mezi klientem a TGS, tato zpráva je zašifrována soukromým klíčem klienta.

B- Zpráva B je v podstatě TGT. Ten obsahuje ID a síťovou adresu klienta, dále TS a klíč pro komunikaci mezi klientem a TGS, tentokrát šifrovaný klíčem TGS.

Klient dešifruje zprávu A svým soukromým klíčem a tím získá klíč pro komunikaci s TGS. Pochopitelně nemůže dešifrovat zprávu B, protože nezná klíč TGS.

C- Protože klient získal klíč pro komunikaci s TGS z předchozího kroku, použije jej pro šifrování zprávy obsahující jeho ID a TS (časové razítko).

D- Zprávu z kroku B, zašifrovanou klíčem TGS, klient doplní o identifikátor adresářové služby, tzv. File service ID a odešle spolu s C-zprávou TGS.

TGS dešifruje zprávu D svým klíčem a zjistí tak ID klienta, jeho síťovou adresu, TS a konečně klíč pro komunikaci mezi klientem a TGS. Tento klíč použije TGS k dešifrování zprávy C. Získá tak dvě časová razítka (TS), ID klienta ze zprávy C a ze zprávy D. Dále TGS porovná obě ID, čímž si ověří identitu klienta. Zároveň zkontroluje, zda rozdíl časových údajů na TS

nepřekročil stanovenou hodnotu, tedy zda nevypršela platnost časového razítka.

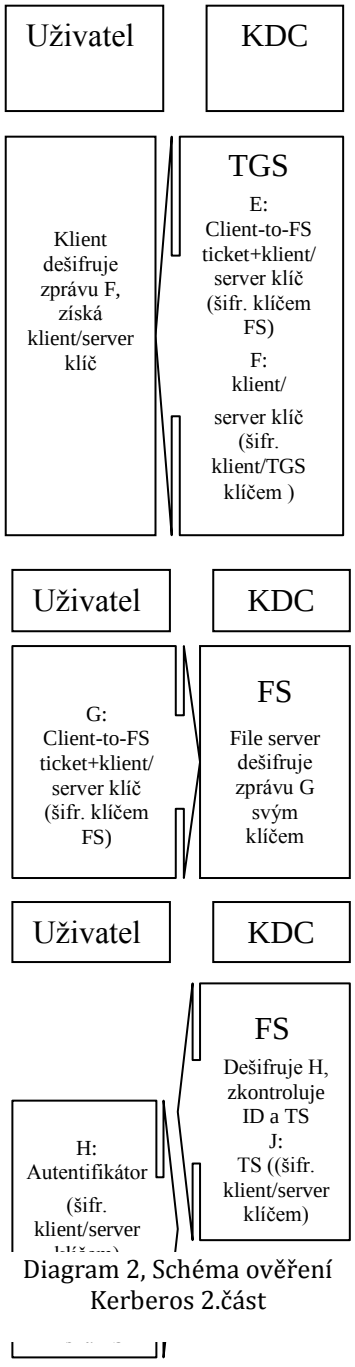


Diagram 2, Schéma ověření Kerberos 2.část

E- TGS pošle klientu tzv. Client-to-FS ticket. FS je cílový server, se kterým si hodláme vyměňovat data. Tento tiket obsahuje ID klienta, síťovou adresu, TS a Klient-Server klíč. To vše šifrováno soukromým klíčem FS.

F- Klient obdrží ještě jednu zprávu, která rovněž obsahuje Klient-Server klíč. Tentokrát je ale šifrována klíčem pro komunikaci mezi klientem a TGS. Tento klíč klient získal ze zprávy A, tedy může zprávu F dešifrovat a Klient-Server klíč zpřístupnit.

G- Klient přepošle Client-to-FS ticket (zpráva E) serveru FS.

H- Dále vytvoří tzv. Authentificator, obsahující ID klienta společně s TS, zašifrovaný Klient-Server klíčem, získaným ze zprávy F.

I- FS dešifruje pomocí svého tajného klíče zprávu G. Získá ID klienta, síťovou adresu, TS a konečně Klient-Server klíč. Tím dešifruje Authentificator, tedy zprávu H, porovná obě ID a zkontroluje platnost TS.

J- FS pošle zpět zprávu potvrzující ověření identity klienta a ochotu poskytovat uložená data. Tato zpráva také obsahuje TS uloženého ve zprávě H, zvětšeného o hodnotu 1 a nakonec zašifrovaného Klient-Server klíčem.

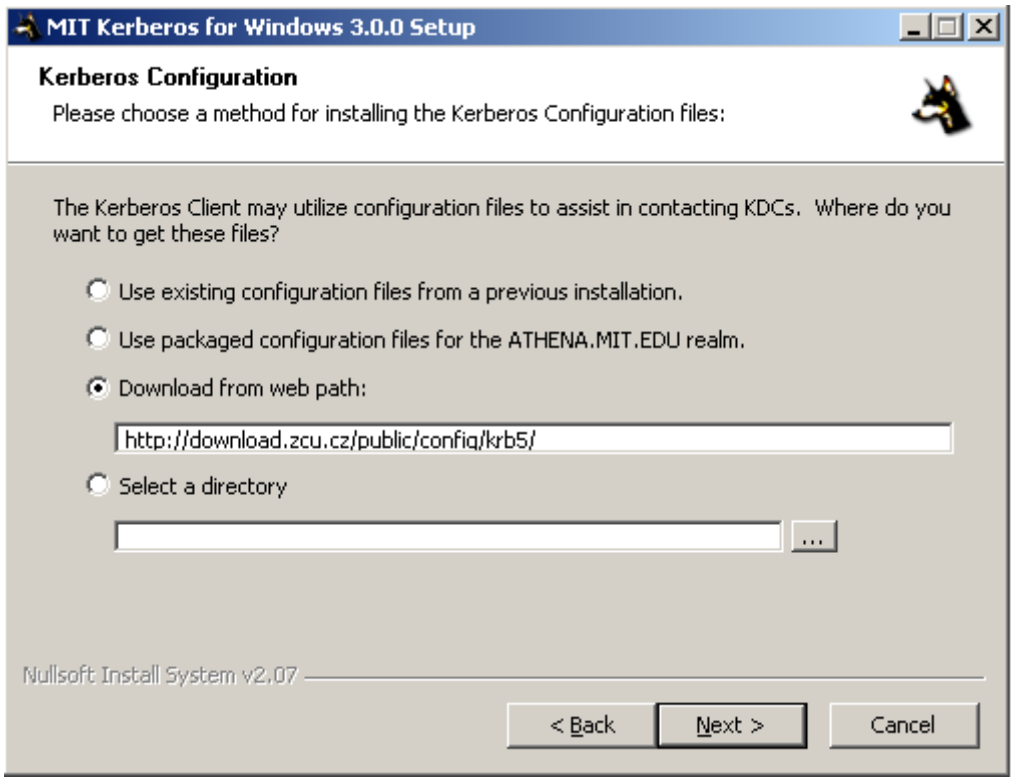
Klient zkontroluje, zda je hodnota skutečně zvětšena o 1. V případě že ano, může důvěřovat FS.

Tímto je ověření obou stran komunikace ukončeno [4].

3.3 PRAKTICKÁ ČÁST – KERBEROS V PROSTŘEDÍ ZČU

3.3.1 ÚVOD DO PRAKTICKÉ ČÁSTI

Následující kapitola popisuje systém Kerbera přímo tak, jak je implementován v prostředí sítě ZČU. Dále obsahuje popis práce s klientem protokolu Kerberos. V tomto případě bylo třeba nastavit připojení k doméně ZCU.CZ. Samotná tvorba konfiguračních souborů je mimo rámec této práce, proto jsem využil možnosti volného stažení příslušných souborů, a to přímo z oficiálních stránek[1] ZČU.



Obrázek 1, Výběr konfiguračních souborů Kerbera

3.3.2 KERBEROS INFRASTRUKTURA ZČU

KDC SERVERY

Vybudování sítě pro účely virtualizace univerzity vyžaduje spolehlivé a bezpečné řešení. Server KDC v prostředí sítě ZČU je proto rozdělen na čtyři servery - tzv. Master server a tři geograficky různě rozmístěné repliky. Administraci a s ní spojené služby zajišťuje Master server. Dále se stará o replikaci databáze na

[1] viz. http://download.zcu.cz/public/config/krb5/krb5.conf.

zmíněné kopie Master serveru. Samotnou autentizaci a poskytování pověření zajišťují tyto KDC repliky [5].

POVĚŘENÍ

Po úspěšném ověření zašle KDC replika uživateli vytvořeným zabezpečeným kanálem TGT lístek. Pomocí TGT lístku je pak možné získat další pověření na jednotlivé služby.

Získaný lístek má následující vlastnosti:

- Standardní doba platnosti je 8 hodin
- Standardní doba, po kterou je možné obnovovat platnost lístku, je 14 dní
- Lístek je možné forwardovat

3.3.3 SPRÁVA SYSTÉMU KERBEROS

NETWORK IDENTITY MANAGER

Správu pověřování, tedy poskytování tiketů, práci s hesly a zajišťování AFS tokenů v protokolu Kerberos obstarává aplikace Network Identity Manager (dále jen NetIdMgr). Grafické rozhraní uživateli přehledně prezentuje správu síťových identit a jejich pověření. Pro přístup ke všem propojeným síťovým účtům v rámci jediného přihlášení disponuje NetIdMgr podporou metody SSO. Další výhodou NetIdMgr je automatická obnova pověření v případě skončení platnosti.

Klíčovou vlastností NetIdMgr je však podpora ze strany aplikací, neboť právě ty musejí umět zpracovat poskytnuté pověření. NetIdMgr je koncipován jako obecný nástroj, který je nezávislý na konkrétním typu identity a typu pověření. Příslušné typy identit a pověření jsou podporovány díky zásuvným modulům ve formě DDL knihoven (plugin). Tyto moduly jsou dodávány jako součást balíku Kerberos for Windows. Pro NetIdMgr jsou vyvinuté i další pluginy a to plugin AFS (jako součást balíku OpenAFS for Windows) a KCA (samostatně od Secure Endpoints Inc.).

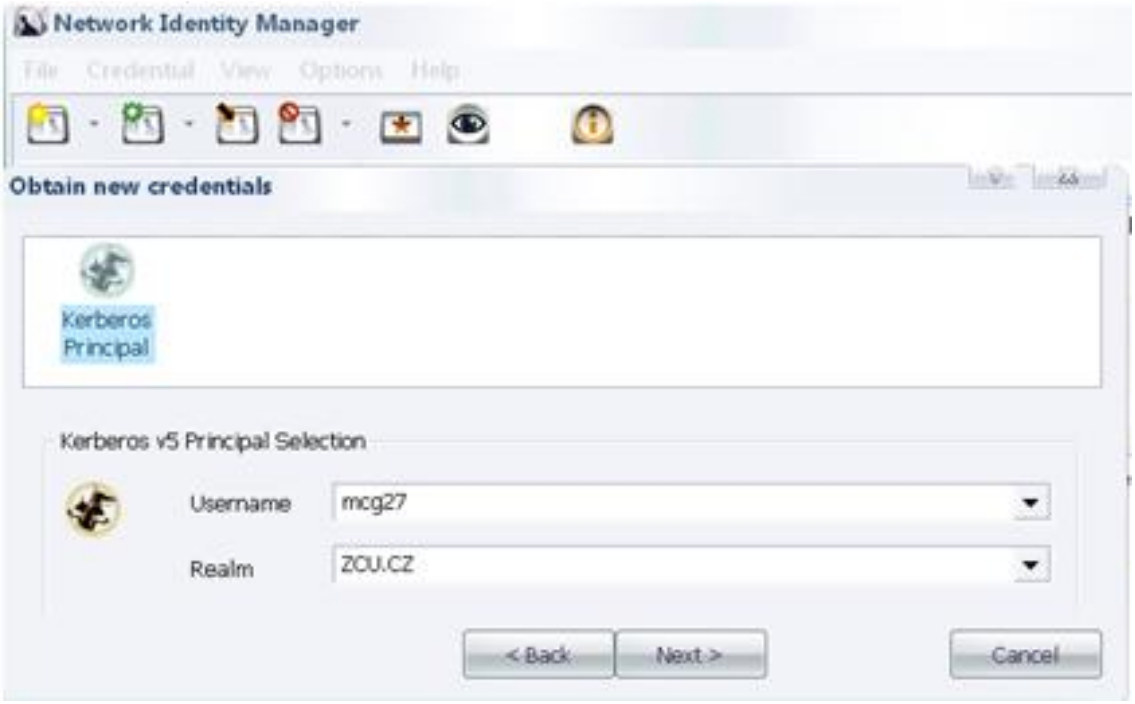
Identita v Network Identity Manageru je definována jako jedinečná identifikace uživatele, která je vhodná pro použití nějakou síťovou službou. Pověření, které je spravováno NetIdMgr je vždy mapováno na jednu identitu, v případě, že je více pověření mapujících se na jednu stejnou identitu, pak všechny tyto pověření náleží k dané identitě.

„NetIdMgr podporuje dva hlavní typy pluginů:

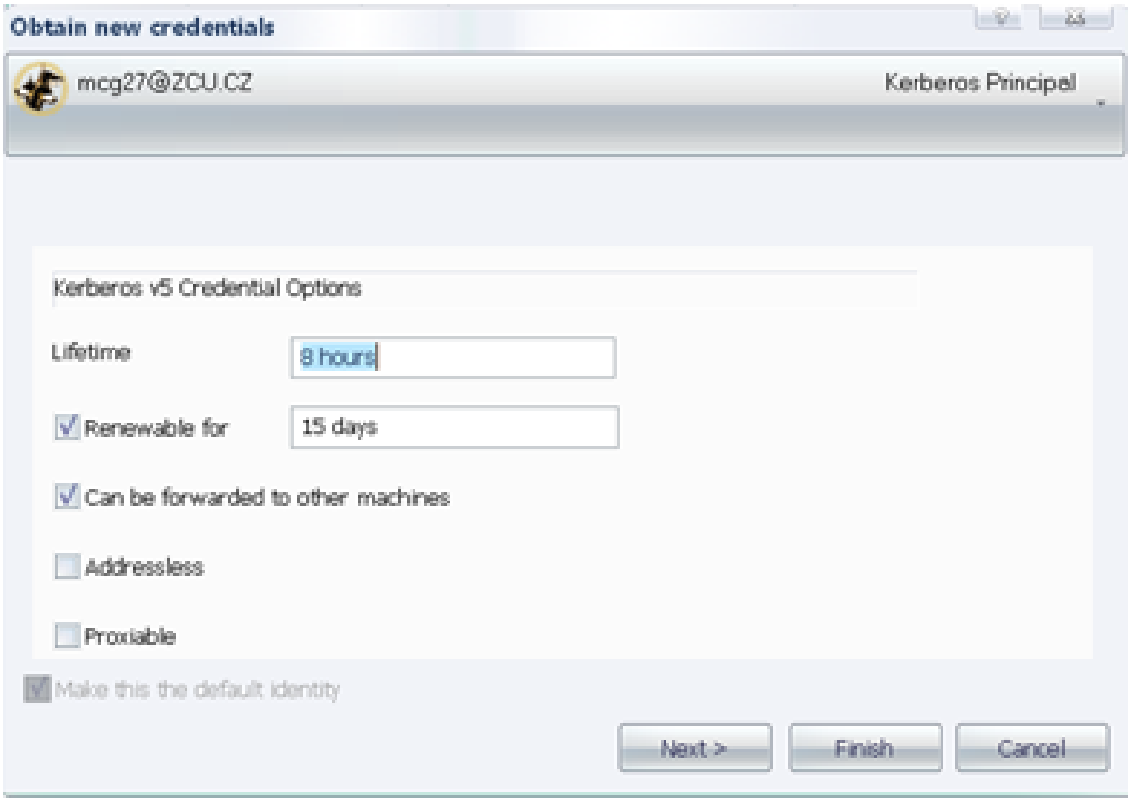
Identity provider - Tento typ pluginu se stará o identitu, její atributy, název a konfiguraci. Plugin registruje do NetIdMgr svůj typ identity a registruje funkce, které implementují funkcionalitu a reakce na zprávy zasílané NetIdMgr.

Credential provider - Tento plugin se stará o pověření, registruje svůj typ pověření, specifické atributy pověření (např. datum a čas vydání pověření, doba platnosti, fyzické umístění, aj.) a také registruje funkce, které reagují na zprávy zasílané z NetIdMgr. Tyto funkce implementují potřebnou funkcionalitu specifickou pro daný typ pověření, např. podporu pro manipulaci s nimi (mazání, obnovování,

konfiguraci nastavení, aj.) Pluginy dále mohou registrovat vlastní konfigurační a zobrazovací panely do aplikace. Pluginy také mohou definovat vzájemné závislosti mezi sebou (např. AFS je závislý na Kerberos).„ [6]



Obrázek 2, Volba uživatele a domény



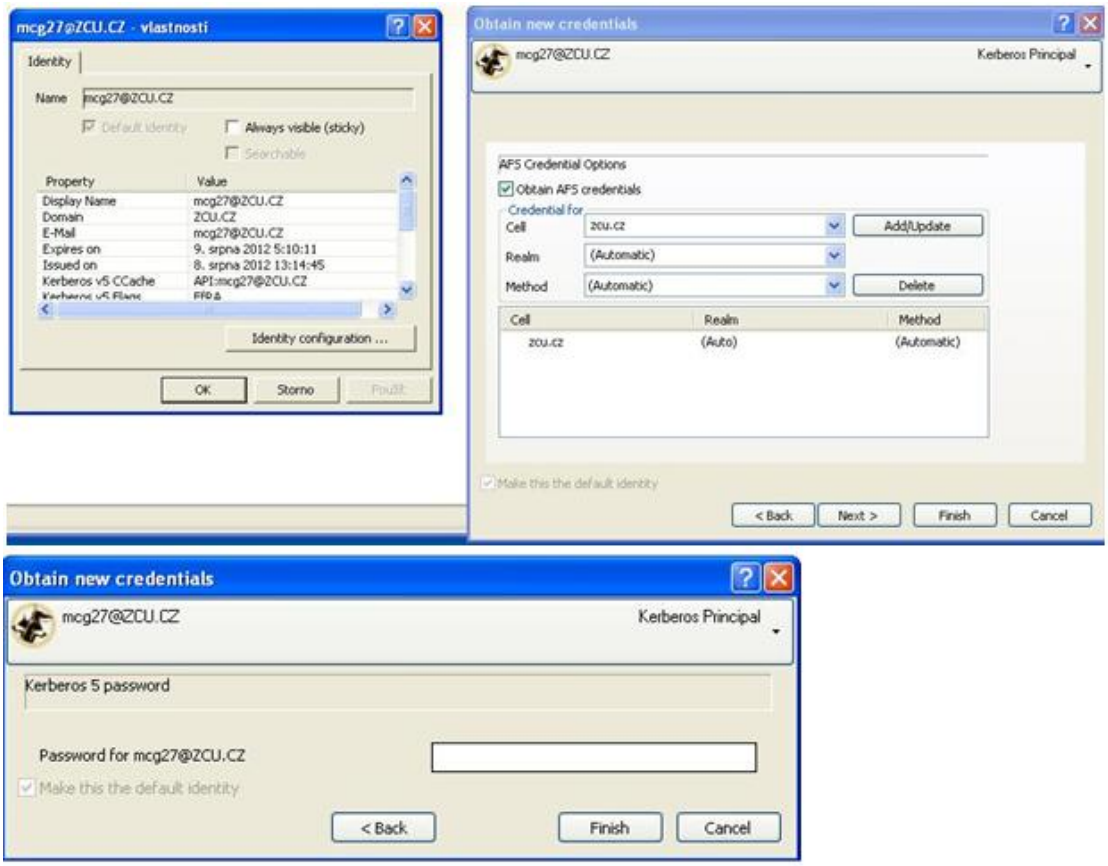
Obrázek 3, Nastavení pověření

Obrázek 4, Získané tikety a token

Získání tokenů

Pro přístup například do domovského adresáře je třeba být autorizován. Token pro přístup lze získat v Network Identity Manageru vyvoláním příkazu New Credentials. Uživatel se tedy nejprve autentizuje v rámci služby Kerbera, načež získá tiket. Tímto tiketem se poté prokáže systému a získá AFS token.

Na počítačích v systému Orion dojde po přihlášení k získání AFS tokenu automaticky.

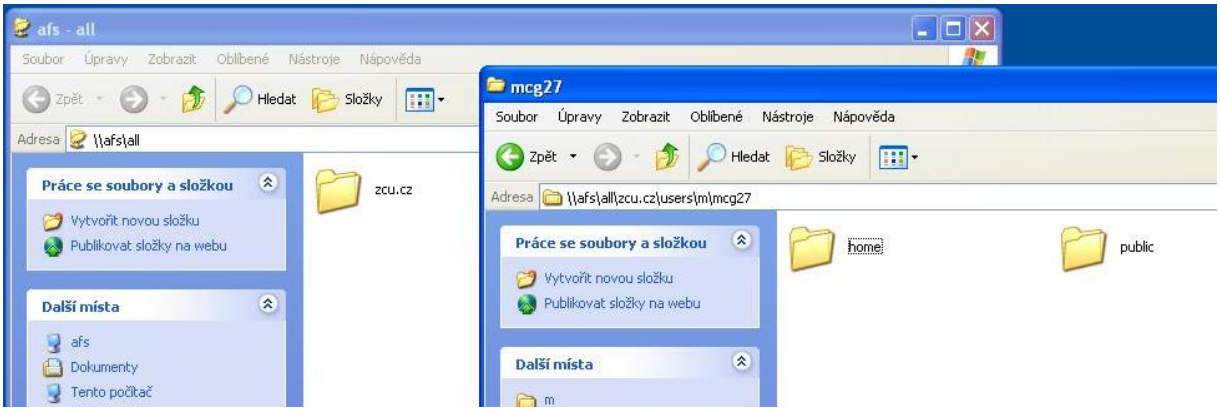


Obrázek 5, Získání přístupu: AFS token

OPEN AFS

Open AFS klient je aplikací, která v prostředí Windows umožňuje klientské stanici pracovat se souborovým systémem AFS. Uživatel se po získání AFS tokenu může pohybovat v adresářovém systému tak, jako by měl data přímo ve svém počítači. Samozřejmě s patřičnými přístupovými právy. AFS řeší přístup k jednotlivým adresářům seznamem přístupových práv tzv. ACL (Access Control List). Ten obsahuje jména uživatelů a jejich přístupová práva.

"*Kořenem souborového stromu je adresář /afs. Základní jednotkou AFS je buňka (cell). Je to zpravidla několik administrativně sloučených serverů, které v rámci AFS vystupují jako jednotný souborový systém. Tyto buňky mohou být lokální (na stejné síti; zde je připojen i váš počítač) nebo vzdálené. Typickým příkladem AFS buňky je sada serverů, které používají stejné Internetové doménové jméno. V našem případě budeme mluvit o AFS buňce zcu.cz.*" [7]



Obrázek 6, Adresářový systém AFS - ZČU

4 EDIRECTORY

Adresářová služba eDirectory je produktem společnosti Novell. Byla vyvinuta jako nástupce NDS (Novell Directory Services) a roce 2000 se poprvé objevila v síťovém operačním systému Novell NetWare 5.1. I nadále je standardní součástí vyšších verzí operačních systémů Novell. Protože se jedná o multiplatformní adresářovou službu, je možná její implementace v dalších operačních systémech (Linux/Unix a MS Windows). Koncepce služby eDirectory je založena na celosvětovém standardu X.500 [8].

4.1 KONCEPCE EDIRECTORY

Služba eDirectory umožňuje v počítačových sítích správu entit (uživatelských účtů apod.), aplikací a síťových prostředků a zajišťuje také jejich autentizaci a autorizaci. Data jednotlivých součástí systému jsou formována do objektů (např. uživatelé a skupiny uživatelů, servery, tiskárny, licence, aplikace apod.), které jsou umístěny do tzv. partitionů.

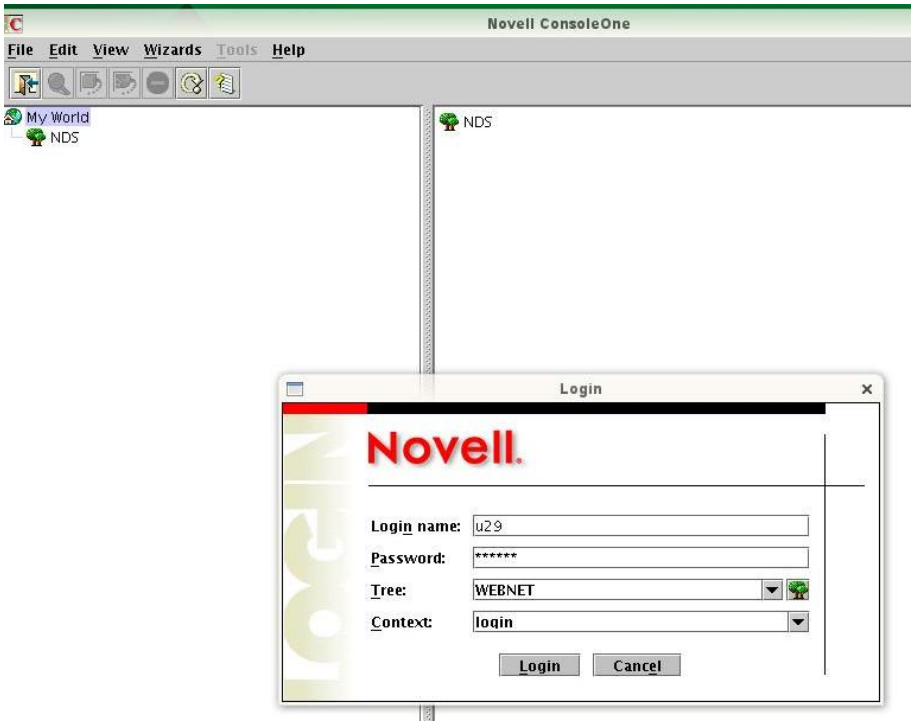
Jednotlivým objektům jsou přiřazována tzv. ACL, což je seznam přístupových práv. Uživatelům, operačnímu systému, administračním nástrojům či kompatibilním aplikacím je na základě ACL práv umožněno (nebo znemožněno) s těmito objekty pracovat. Pověřeným entitám se říká trustee.

„K základním rysům eDirectory patří objektovost, otevřenost, hierarchičnost, globálnost, distribuovatelnost a multiplatformnost. Zmíněnou objektovostí se rozumí skutečnost, že informace o součástech sítě jsou udržovány ve formě objektů a jejich vlastností. Množina typů těchto objektů a jim příslušných vlastností (tzv. schéma eDirectory) je přitom otevřená, lze ji tedy rozšiřovat a upravovat dle potřeby. Jednotlivé definované objekty jsou umísťovány do hierarchické struktury nazývané strom eDirectory. Jejich pozice v této struktuře pak není bezvýznamná, vhodné umístění usnadňuje uživatelům přístup k síťovým prostředkům, ovlivňuje čerpání licencí apod. eDirectory má také globální platnost, takže objekty, jež jsou v ní definovány, platí v prostředí celé sítě a nikoli jen na hostitelském serveru. Databázi eDirectory lze též distribuovat. Jednak je možné ji udržovat ve formě několika vzájemně synchronizovaných kopií na různých

serverech a zvýšit tak její zabezpečení před haváriemi, jednak ji lze rozdělit na několik menších vzájemně souvisejících částí a snížit tím zatížení sítě od režijní komunikace (důležité především v sítích WAN).“ [9]

4.2 PŘÍSTUPOVÝ SYSTÉM V EDIRECTORY

Každý objekt má nadefinované vlastnosti, mimo jiné i přístupová práva konkrétních uživatelů. Přestože se tedy uživatel úspěšně autentizuje do adresářového stromu systému eDirectory, neznamená to, že má v tomto stromu neomezený přístup ke všem jeho položkám (výjimkou samozřejmě může být uživatel typu administrátor apod.). To ale neznamená, že bychom měli umožnit přístup do adresářového stromu komukoliv.



Obrázek 7, Příhlášení do prostředí ConsoleOne

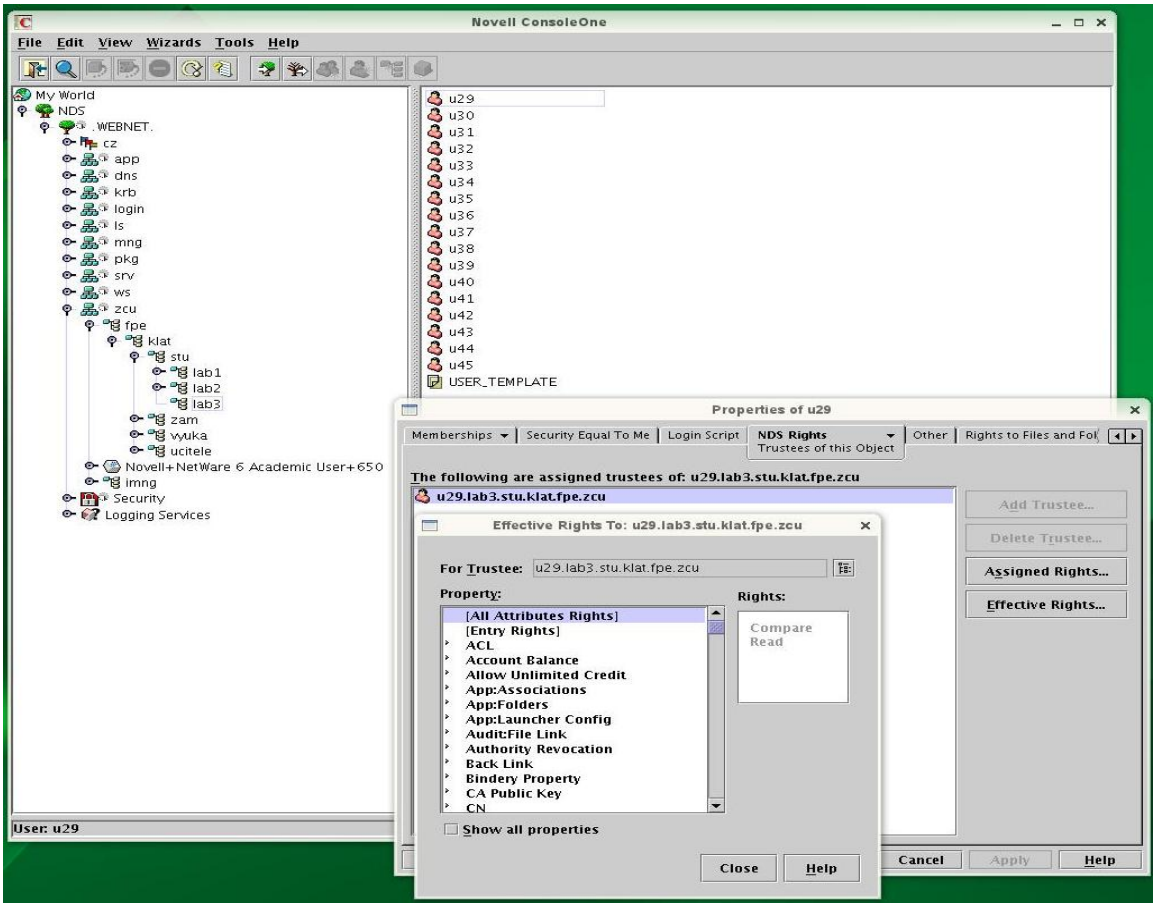
Správu přístupových práv k objektům lze provádět přímo ve „stromu“ eDirectory, a to pomocí nástroje Novell Console One. Po výběru příslušného objektu můžeme zobrazit aktuálně přiřazená práva viz. obrázek níže. K objektům se nastavují pověřenci, tzv. trustees (definují právo uživatele ke konkrétnímu objektu) a práva. Obecně existují dva typy práv – práva k objektům a k souborům adresářům.

Práva k objektům (NDS rights) se dále dělí na:

- *Efektivní práva* (Effective rights) jsou skutečná práva, kterými uživatel disponuje. Umožňují nastavit práva na konkrétní operace s objektem.
- *Děděná práva* (Inherited rights filters) nabízí možnost aplikovat již vytvořená práva na další objekty.

Implicitně je každému objektu přiřazeno právo Browse, čili procházet stromem. Další práva (compare, read, write, addSelf) lze nastavit.

Explicitní – „výslovně“ zadaná práva mají vyšší prioritu než práva zděděná. Každý uživatel může sám sobě zapisovat a ukládat do login scriptu.



Obrázek 8, Správa přístupových práv v eDirectory

4.3 AUTENTIZAČNÍ MECHANIZMY EDIRECTORY

Konkrétní typy autentizačních mechanizmů se liší podle implementace eDirectory v různých prostředích. Za účelem autentizace existuje pro eDirectory široká škála podporovaných rozšíření. Obecně tak lze vybrat a nastavit způsob ověření pro konkrétní situaci.

NOVELL MODULAR AUTHENTICATION SERVICE (NMAS)

NMAS (Novell Modular Authentication Service) je rovněž produktem firmy Novell. Jedná se o nadstavbový modul, který podporuje všechny tři metody získání přihlašovacích údajů včetně jejich kombinace.

K dispozici jsou metody:

- Heslo - standardní autentizace NDS heslem založena na pricipu výzva-odpověď. Existuje několik druhů přenosu hesla - Plain text, SHA-1 a MD-5.

- Token, karta - fyzické zařízení obsahující čip, který je schopný generovat heslo či uchovávat formu kryptografické funkce.
- Biometrika - dynamická (behaviorální) či statická (otisk prstu apod.)

K dispozici jsou i pokročilejší způsoby autentizace - právě kombinací zmíněných metod:

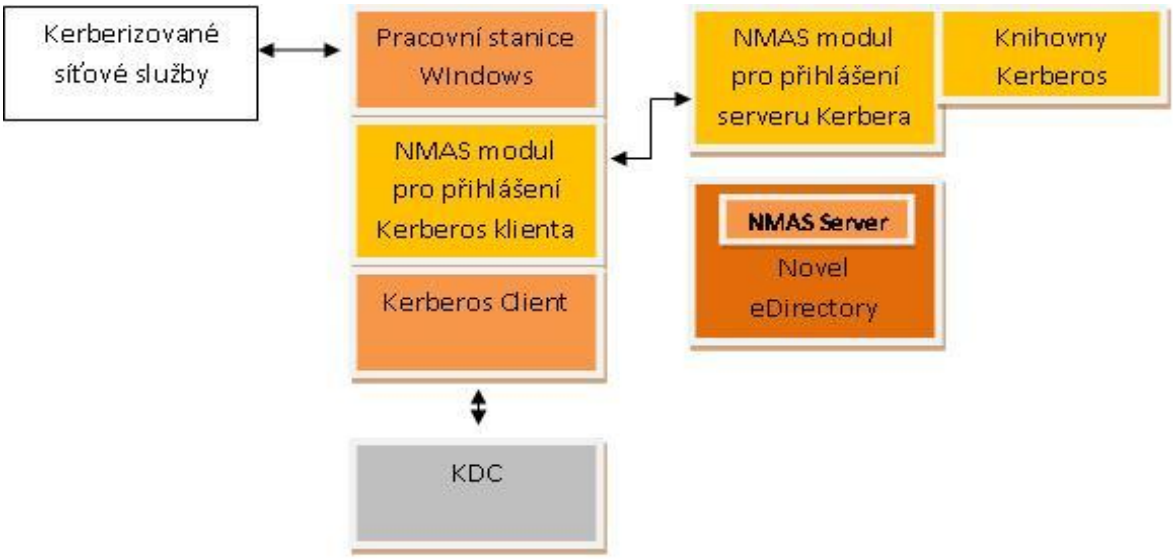
- Výzva-odpověď - při přihlašování server vyzve uživatele k zadání identifikačních údajů. Uživatel zadá PIN kód nebo ID na server, který pak vydá výzvu --- náhodné číslo, které odešle pracovní stanici uživatele. Uživatel dešifruje toto číslo pomocí svého tokenu a odešle zpátky na server. Ten porovná získaný údaj s údaji ve své databázi, když hodnoty souhlasí, autentizace je úspěšná.
- Časová synchronizace (Time-synchronous auth.) - metoda je podobná předchozímu způsobu. Speciální algoritmus vytváří na serveru i na tokenu uživatele identická čísla, která se během doby mění. Uživatel pošle na server svůj PIN spolu s aktuální hodnotou tokenu.
- X.509 certifikát - autentizace založená na asymetrické kryptografii pomocí veřejného certifikátu.

Zajímavým doplňkem je tzv. gradovaná autentizace, kdy se v přístupu k různě „citlivým“ datům vyžaduje odpovídající úroveň zabezpečení [10].

NMAS A KERBEROS

V síťovém prostředí, kde je vyžadována autentizace zvlášť pro přístup k službám eDirectory a zvlášť k službám, vyžadujícím ověření skrze protokol Kerberos, je jediný uživatel nucen vystupovat v rámci dvou identit. Tedy jedna identita má přístup k tzv. „kerberizovaným“ aplikacím a druhá k aplikacím služby eDirectory. Uživatel se proto musí nejen dvakrát autentizovat, ale také si pamatovat dvě hesla pro přístup. Musejí být tedy udržována dvě hesla, ale také je třeba zajistit dva přihlašovací procesy, což pochopitelně zvyšuje riziko útoku.

Metoda NMAS Kerberos řeší tento problém povolením používání přihlašovacích údajů Kerbera pro autentizaci do eDirectory. Opět se jedná o způsob jednotného přihlášení SingleSign-On. Ověření uživatele probíhá na základě jeho lístku Kerberos (ticketu). Metoda se skládá z klientské a serverové části. Klient je nainstalován na pracovní stanici uživatele a serverovská součást je nainstalován na serveru NMAS v eDirectory. Dispozice eDirectory je rozšířena pro uložení Kerberos dat (ticketů, hesel, cíle stromu Kerberos apod.). Identita Kerberos uživatele je spojena s uživatelským objektem eDirectory.



Obrázek 9, Architektura NMAS Kerberos

SCHÉMA AUTENTIZACE METODY NMAS KERBEROS:

1. Uživatel spustí klienta Novell a zadá své uživatelské jméno (eDirectory), vybere „strom“ a server NMAS.
2. V dalším kroku uživatel zvolí metodu Kerberos z přihlašovacího dialogu NMAS.
3. Kerberos klient odešle všechny tyto informace na server NMAS.
4. NMAS Server vrátí seznam Kerberos principals (jedinečné identity, kterým Kerberos může poskytnout tikety) spojených s daným uživatelem.
5. Klient tento seznam zobrazí uživateli. Ten si zvolí požadovanou identitu, kterou chce autentizovat.

6. Klient odešle vybranou Kerberos identitu NMAS serveru.
7. NMAS server vrátí informace o doméně (KDC hostname/jméno uzlu a port pro komunikaci se zvolenou Kerberos identitou).
8. Klient vyzve uživatele k zadání svého Kerberos hesla.
9. Poté klient autentizuje uživatele k serveru KDC a poskytne TGT tiket.
10. Klient odešle tento tiket serveru KDC s žádostí o poskytnutí tiketu pro přístup k eDirectory. Rovněž odešle eDirectory service tiket serveru NMAS jako součást autentizace.
11. Autentizace je hotova. Uživatel může nyní využívat všechny povolené aplikace eDirectory, aniž by musel zadávat heslo pro přístup k eDirectory [11].

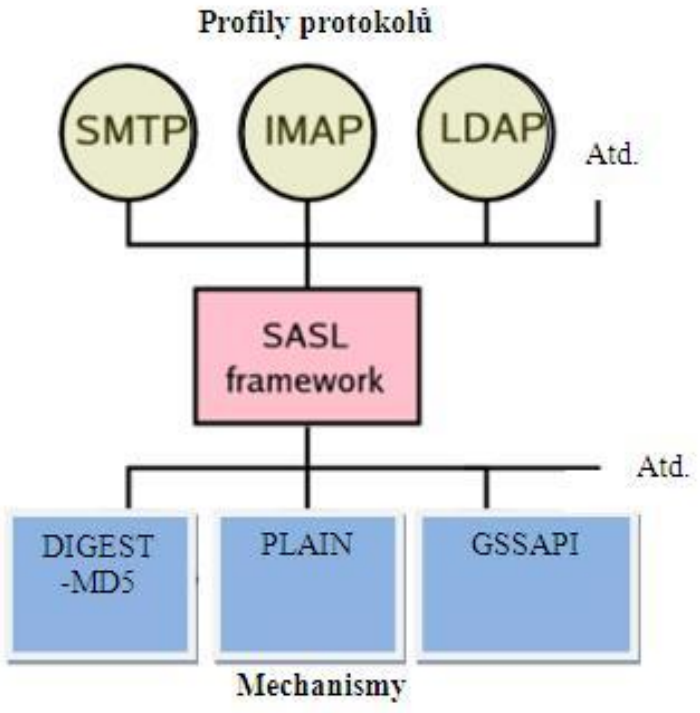
4.3.1 SOUVISEJÍCÍ MECHANISMY

AUTENTIZACE DO ADRESÁŘOVÝCH SLUŽEB - LDAP/OPENLDAP

Protokol, určený k přístupu a správě adresářových služeb. V plném znění Lightweight Directory Access Protocol je protokol, určený k přístupu a správě adresářových služeb, jako jsou databáze a stromově strukturované adresáře. Typickým příkladem jsou hierarchicky uspořádané skupiny (např. oddělení firmy), jejich podskupiny (zaměstnanci), další o řád nižší úrovně (informace o zaměstnancích) atd. Jednotlivé úrovně reprezentují položky nesoucí atributy s předem nadefinovanou hodnotou a DN (distinguished name – rozlišovací jméno). Protokol LDAP funguje na bázi klient – server. Existuje také ve verzi OpenLDAP, což je multiplatformní open source verze.

Bezpečnostní služby autentizace však obstarává jiná programová vrstva - framework SASL (Simple Authentication and Security Layer). Jedná se o mechanismus umožňující volbu autentizační služby a zabezpečení přenosu dat formou klient-server protokolů. SASL koriguje výzvy a odpovědi mezi oběma stranami a způsob šifrování komunikace. Představuje tak přizpůsobitelné rozhraní mezi protokoly a jejich mechanizmy. Teoreticky lze v rámci kompatibility SASL

uplatnit libovolný autentizační mechanismus v jakémkoliv aplikačním protokolu [12].



Obrázek 10, LDAP>SASL. Schéma systému přizpůsobení různých mechanismů libovolnému protokolu.

Autentizaci v LDAP je možné provést několika způsoby, které se od sebe liší ve výsledném přístupu k adresářovým službám.

Autentizace pomocí tzv. Bind operace

Bind operace obstarávají výměnu autentizačních informací mezi klientem a serverem za účelem autorizace. Žádost Bind-request určuje požadovanou identitu uživatele. Některé typy operace Bind umožňují uživateli volbu poskytnutí identity.

1. Anonymní autentizace - Můžeme tak například získat přístup k adresářovému stromu, aniž bychom se serveru identifikovali. Nemůžeme však provádět ty operace, které jsou umožněny pouze pověřeným (autentizovaným) uživatelům.
2. Neautentizovaná přístup – uživatel zadá na server požadavek k přístupu k určitému objektu - DN. Autorizační služba zkontroluje oprávnění k danému objektu, a buď přístup povolí, nebo zamítne.

Autentizace pomocí jména a hesla – klient zašle Bind-request požadavek v podobě jména DN spolu s hashem přístupového hesla. Autorizační služba zkontroluje, zda zadané heslo odpovídá s některým z hesel vztahujícím se k danému DN. Následně umožní, nebo zakáže přístup [13].

5 OS LINUX

OS Linux je systém odvozený od UNIXu (komerční OS). Zásadní měrou se Unixové systémy uplatnily při vzniku internetu - vývoji počítačových sítí a modelu klient-server. Byly též vyvíjeny společně s protokolem TCP/IP. Linux byl od svého vývoje využíván jako operační systém pro servery a pracovní stanice, je však využitelný i jako OS pro osobní počítače. V základu instalace obsahuje řadu serverových aplikací jako například www a ftp servery. Výhodou je také podpora propojení s MS Windows servery a klienty. Linux existuje v několika různých distribucích. Vzhledem k otevřené povaze Unixových systémů je na výběr velké množství způsobů autentizace. Pochopitelně závisí také na typu síťových služeb a jejich vzájemné podpoře.

5.1 PAM - SPRÁVA AUTENTIZAČNÍCH MECHANISMŮ

Linux-PAM (Pluggable Authentication Modules for Linux) je systém zásuvných autentizačních modulů, které nahrazují interní autentizační mechanizmy aplikací. Funkční stránka programů je tak odlehčena od té bezpečnostní. Aplikace se stávají nezávislé na konkrétních autentizačních postupech. Již neřeší, jak bude ověření provedeno, ale jaký je výsledek ověřování.

Systém PAM tvoří připojitelné autentizační moduly, ke kterým aplikace přistupuje skrze vrstvy. První vrstvu stvoří systémová knihovna. Ta je připojena k programu a má za úkol zpřístupnit autentizační služby. Další vrstvou je systémová konfigurace. Jak již z názvu vyplývá, umožňuje nastavení PAM – autentizaci uživatele, kontrolu účtu, správu relace atd. PAM sám o sobě není autentizačním systémem. Pomocí zásuvných knihoven však dokáže zprostředkovat autentizaci uživatele vůči programům např. využitím protokolu Kerberos [14].

5.2 AUTENTIZACE POMOCÍ KLÍČŮ METODOU OPENSSH.

Pro účely ověření identity v Unixových systémech byl vyvinut bezpečnostní balík openSSH (Secure shell), který obsahuje SSH server (sshd) a klient (ssh). Autentizace uživatele skrze protokol SSH (součást openSSH) probíhá výměnou veřejných klíčů metodou asymetrického šifrování RSA. Bezpečnost spočívá v absenci zasílání přístupového hesla. K šifrování přenosu dat se používá

symetrické šifrování (např. 3DES, či AES). OpenSSH je standardní součástí všech současných Linuxových distribucí.

Při přihlašování server poskytne svůj veřejný klíč (SSH host key). Ten si můžeme ověřit zobrazením tzv. fingerprintu. Klient si také udržuje databázi veřejných klíčů serverů pro případnou kontrolu. Po ověření serveru je na řadě uživatel. I ten je ověřován pomocí veřejného klíče. Je proto nezbytné, aby server tento klíč znal [15].

To je zařízeno následovně. Součástí SSH je speciální program (ssh-keygen), kde si uživatel vygeneruje dvojici klíčů - veřejný (public) a soukromý (private). Soukromý klíč je dále šifrován tzv. passphrase, což je heslo chránící zneužití tohoto klíče. Získaný veřejný klíč uživatel uloží do svého domácího adresáře na serveru, ke kterému se chce přihlašovat. Na serveru tedy není uloženo heslo a autentizaci uživatele podmiňuje znalost jeho soukromého klíče, resp. passphrase [16].

Protože je ve své podstatě systém Linux otevřenou licencí, je možné implementovat nejrůznější prostředky poskytující autentizaci. Mezi již uvedené bychom mohli rovněž zařadit i systém Kerberos, tomu je prostor věnován v samostatné kapitole.

6 OS MS SRV2008

Windows Server 2008 je operační systém od společnosti Microsoft. V počítačových sítích se využívá jako OS pro servery. Systém vychází ze stejného kódu jako Windows Vista. Oproti verzi Srv 2003 obsahuje například vestavěnou virtualizaci serverů, různá vylepšení správy, podporu IPv6 nebo nativní podporou bezdrátových sítí. Co se týče bezpečnosti, došlo rovněž k několika změnám. Nově může uživatel zasahovat do bezpečnostní politiky hesel, rozšířit systém ověřování o další bezpečnostní služby atd.

Windows Server 2008 R2 (druhé vydání) dále obsahuje balík rozšíření (Negotiate authentication protocol package), jež umožňuje volbu dalších zprostředkovatelů zabezpečení - autentizaci a šifrování. Jeho úkolem je vyjednat, který autentizační protokol má být použit na základě protokolů podporovaných na klientském počítači a na serveru [17].

MS Srv2008 standardně nabízí dva základní autentizační systémy. Jsou to NTLMv2 a Kerberos (verze 5). Přestože je třeba zajistit komunikaci s autentizačním serverem KDC a nutná je i další konfigurace na úrovni domény a konkrétních služeb, upřednostňován je právě protokol Kerberos.

Obrázek 11, přihlašovací obrazovka MS Server 2008

6.1 NTLMv2 v SRV 2008

NTLM (NT LAN Manager) je soubor autentizačních a bezpečnostních protokolů integrovaných v síťových systémech Windows jako SSO mechanismus. Je vyvinut společností Microsoft. I přes řadu let je v rámci dalších implementací stále podporován, zejména kvůli zpětné kompatibilitě.

Fungování systému MS Server 200x je spjato se službou Active Directory, přístup do systému je řízen řadičem domény (DC - Domain Controller). Přihlášení probíhá na základě uživatelského účtu a hashe hesla pomocí protokolu NTLM. Ten zadané údaje porovná s údaji v lokální databázi nebo se obrací na řadič domény (např. Active Directory). V případě shody se vytvoří relace a získané údaje využívají také při neinteraktivní autentizaci. Protože bylo ve verzi NTLMv1 zjištěno mnoho bezpečnostních nedostatků a je ve Window Server 2008 zakázán, budeme se zabývat následující verzí NTLMv2. (RUSSEL, CH.,CRAWFORD, S., 2009, s.787; 1030).

NTLMv2 je založen na ověřovacím mechanismu výzva-odpověď, kdy uživatel prokazuje svoji identitu, aniž by odesílal serveru své heslo.

Průběh NTLMv2 autentizace:

1. Klient zašle na server požadavek na autentizaci (Authentication Request). Součástí této zprávy je také seznam funkcí podporovaných klientem.
2. V odpovědi serveru je seznam dohodnutých funkcí a dále výzva - náhodně vygenerované číslo (NTLM výzva)
3. Klient odpoví tzv. NT zprávou – NTLM výzva zašifrovaná NT hashem klienta + samotná NTLM výzva
4. Server přepošle zprávu č.3 řadiči domény (DC). DC zašifruje NTLM výzvu rovněž NT hashem klienta, který má uložený ve své databázi. Poté porovná obě hodnoty, tj. výsledek hashování DC s hashem ze zprávy č. 3. Výsledek odešle zpět serveru, který na jeho základě buď povolí, nebo odepře přístup. Tato forma ověření se nazývá NTLM pass-through.

Verze NTLMv2 již používá jen NT hash, tedy metodu šifrování HMAC-MD5[2]. Výsledkem je navýšení doby potřebné k prolomení hashe (oproti LM hash – metoda DES). Bezpečnost dále zvyšuje metoda solení a použití časových razítek [18].

[2] použití kryptografické hašovací funkce v kombinaci s tajným šifrovacím klíčem

6.2 KERBEROS V SRV 2008

Kerberos je od OS MS Windows 2000 implementován jako výchozí autentizační protokol. To především kvůli jeho univerzálnosti a rychlosti ověřování. Rovněž podporuje bezpečnostní prvky, jako jsou časová razítka, integrita přenášených dat a šifrování přenosu, vzájemná autentizace obou stran, či tzv. tranzitivní důvěra v doménách využívajících stejný protokol. Oproti NTLM je Kerberos považován za bezpečnější a podporuje asymetrické i symetrické šifrování.

Důležitou roli hraje Kerberos také systému adresářových služeb. V OS MS Server 2008 je adresářovou službou Active Directory (AD). AD Umožňuje přístup a správu k serverům, aplikacím, zdrojům a dalším síťovým prostředkům. AD je součástí systému MS Server již od verze 2000. Jako protokol pro přístup používá LDAP. Ověřování Kerberos podporuje zabezpečení pomocí veřejných i soukromých klíčů a používá stejný model podpory seznamu řízení přístupu ACL (access control list) jako systém Windows Server 2008. (RUSSEL, CH.,CRAWFORD, S., 2009, s.49; 1071; 1246).

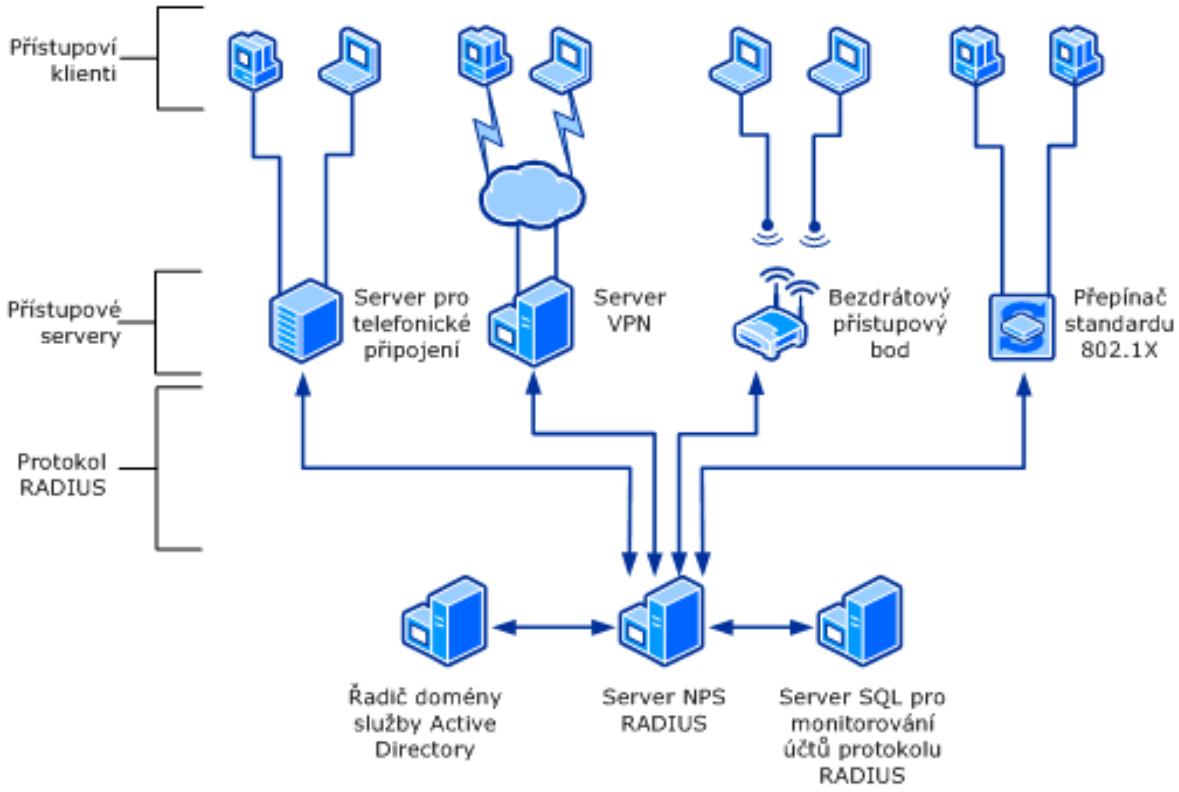
V systému Windows Server 2008 R2 navíc Kerberos podporuje kryptografii eliptických křivek (ECC)[3] pro přihlášení pomocí smart card, která používá certifikáty X.509. Přitom není nutné dodatečně konfigurovat Kerberos.

Autentizaci pomocí systému Kerberos je věnován prostor v samostatné kapitole této práce.

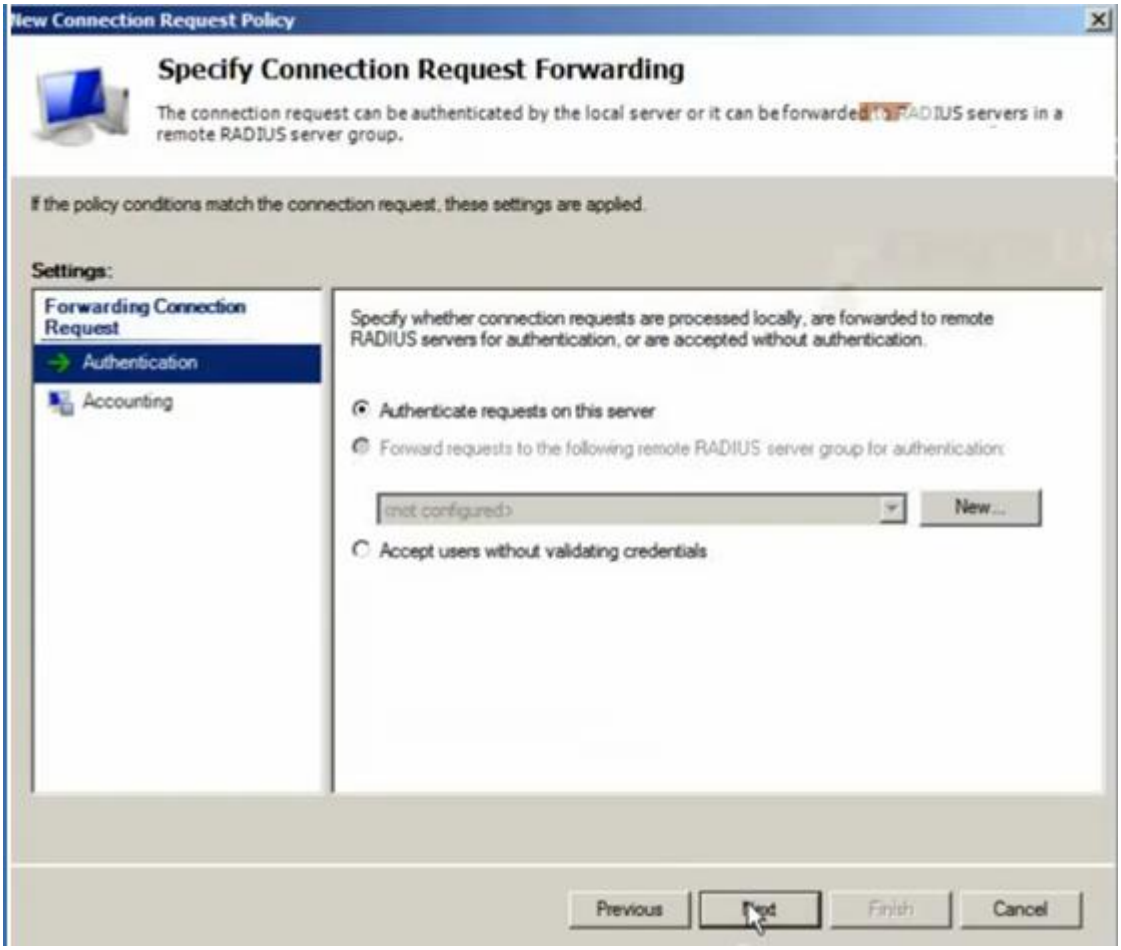
[3] Kryptografie eliptických křivek (ECC) je metoda šifrování veřejných klíčů založená na algebraických strukturách eliptických křivek nad konečnými poli. Snižuje nároky na přenos i místo.(http://cs.wikipedia.org/wiki/Kryptografie_nad_eliptick%C3%BDmi_k%C5%99ivkami)

6.3 RADIUS V SRV 2008

Mimo výše zmíněných způsobů ověření existuje u Srv200x ještě možnost autentizace u internetového autentizačního serveru RADIUS. U verze Srv2008 doznala tato služba několika změn. Server RADIUS provádí ověřování, autorizace a správu účtů pro bezdrátová připojení, vytáčená vzdálená spojen, spojení VPN (Virtual Private Network) nebo proxy server RADIUS. K ověřování credentials může použít server RADIUS například doménu služby Active Directory. (RUSSEL, CH.,CRAWFORD, S., 2009, s.838).



Obrázek 12, server RADIUS pro různé typy přístupových klientů, dle technet.microsoft.com



Obrázek 13, volba způsobu autentizace

7 ZÁVĚR

Práce se pokusila představit problematiku ověřování entit v počítačovém světě sítí. Byly popsány obecné principy ověřování pomocí hesel, certifikátů či tiketů. Zvláštní pozornost byla věnována autentizačnímu protokolu Kerberos, který je v prostředí počítačových sítí velice rozšířen. Pomocí názorných ukázek byl popsán způsob autentizace do prostředí Západočeské univerzity skrze klienta NIM protokolu Kerberos. V návaznosti na toto téma bylo uvedeno několik, v praxi hojně používaných, řešení, a to jak v rámci hotových komplexních systémů, tak i jako dílčích nástrojů sloužících k poskytování služeb ověřování identity. O vyspělosti popsaných způsobů autentizace svědčí i jejich podpora moderních technologií poskytování identifikačních údajů. Všechny uvedené způsoby poskytují bezpečné zajištění autentizace. Zásadním problémem, kdy by mohla být narušena ona bezpečnost, se zdá být snad jen selhání lidského faktoru, tedy politika správy hesel. Probírané systémy se od sebe liší především typem distribuce, a tedy i cenou za implementaci síťového řešení. Přestože nabízí zhruba srovnatelné kvality, ať už z hlediska bezpečnosti nebo správy systému. Klíčovou vlastností v rozhodování, který systém zvolit, dále zůstává podpora aplikací třetích stran.

Při zpracování práce jsem si rozšířil znalosti počítačových sítí a distribuovaných systémů, metod šifrování a principů fungování síťových autentizačních protokolů a celkově si tak prohloubil a ujasnil vědomosti získané během studia.

8 RESUMÉ

This work introduces general problems and its solutions of authentication in non-secure websites, especially internet. It describes methods of verifying all computer entits with authentication protocols and its implementations in server's operation systems. Individual part of this work is given to show how Kerberos authentication protocol works on website of University of West Bohemia. Because of its universal application, Kerberos is used like a main part of secure solution in many server-type OS and website applications. Kerberos and other kinds of verifying are defined in the rest of this work. It contains a description of OS Windows Server 2008, eDirectory services and Linux OS authentication.

9 SEZNAM LITERATURY

Knižní zdroje:

- **DOSEDĚL, T**. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. 190 s. ISBN: 80-251-0106-1
- **PIPER, F. – MURPHY, S**. *Kryptografie*. Praha: Dokořán, 2006. 157 s. ISBN: 80-7363-074-5
- **RUSSEL, Ch. - CRAWFORDOVÁ, S.** *MS Windows Server 2008 - Velký průvodce administrátora.* Brno: Computer Press, 2009. 1271 s. ISBN 978-80-251-2115-3
- **PŘIBYL, J.** *Informační bezpečnost a utajování zpráv*. Praha: Vydavatelství ČVUT, 2004. 239 s. ISBN: 80-01-02863-1
- **JIROUŠEK, R**. *Principy digitální komunikace.* Voznice: Leda, 2006. 309 s. ISBN: 80-7335-084-X

Internetové zdroje:

[1] RFC 5246. The Transport Layer Security (TLS) Protocol [online]. T. Dierks, E. Rescorla. August 2008 [cit. 2012-06-10]. Dostupné z <http://tools.ietf.org/html/rfc5246#page-16>

[2] RSA. Wikipedia [online]. San Francisco (CA): Wikimedia Foundation. 11.3.2012 [cit. 2012-06-10]. Dostupné z <http://cs.wikipedia.org/wiki/RSA>

[3] MIT Kerberos [online]. MIT. 6.11.2010 [cit. 2012-12-1]. Dostupné z <http://web.mit.edu/kerberos/www/>

[4] RFC 4120. The Kerberos Network Authentication Service (V5) [online]. C. Neuman, T. Yu, S. Hartman. July 2005 [cit. 2012-12-1]. Dostupné z <http://www.ietf.org/rfc/rfc4120.txt>

[5] Kerberos [online]. ZČU - Server uživatelské podpory. 4.2.2013 [cit. 30.1.2013]. Dostupné z < http://support.zcu.cz/index.php/Kerberos#Odkazy>

[6] Integrace gridových autentizačních metod do prostředí MS Windows [online]. Závodný, T. 2007 [cit. 28.1.2013]. Dostupné z <http://is.muni.cz/th/39400/fi_m/dp-xzavodny.txt>

[7] AFS [online]. ZČU - Server uživatelské podpory. 2.7.2010 [cit. 30.1.2012]. Dostupné z <http://support.zcu.cz/index.php/AFS>

[8] Adresářová služba Novell eDirectory [online]. O. Přichystal. 2011 [cit. 14.5. 2012]. Dostupné z < http://www.novell.cz/cs/aktuality/technicke-clanky/adresarova-sluzba-novell-edirectory.html>

[9] Adresářová služba Novell eDirectory [online]. O. Přichystal. 5/2006 [cit. 14.5. 2012]. Dostupné z <http://www.prichystal.cz/Archiv_c/NovNews/eDir_nn/edir_nn.htm>

[10] NMAS Functionality [online]. Novell.com. 2012 [cit. 19.5. 2012]. Dostupné z <http://www.novell.com/documentation/nmas23/?page=/documentation/nmas23/admin/data/a53s8fw.html>
[11] AppNote: NMAS and Kerberos [online]. Novell.com. 21.9.2005 [cit. 17.5. 2012]. Dostupné z <http://www.novell.com/coolsolutions/appnote/11468.html>
[12] RFC 4422. Simple Authentication and Security Layer (SASL) [online]. A. Melnikov, K. Zeilenga. June 2006 [cit. 21.4. 2012]. Dostupné z <http://tools.ietf.org/html/rfc4422>
[13] RFC 4513. LDAP: Authentication Methods and Security Mechanisms Simple Authentication and Security Layer (SASL) [online]. R. Harrison. June 2006 [cit. 11.3. 2012]. Dostupné z <http://tools.ietf.org/html/rfc4513#page-14>
[14] PAM – Správa autentizačních mechanismů [online]. B. Bobčík. 19.9.2000 [cit. 19.5.2012]. Dostupné z: <http://www.root.cz/clanky/pam-sprava-autentizacnich-mechanismu/>
[15] OpenSSH FAQ [online]. OpenBSD. 21.4.2012. [cit. 1.6.2012]. Dostupné z: <http://www.openssh.org/faq.html>
[16] OpenSSH - bezpečně a pohodlně [online]. ABClinuxu, Šimerda P. 21.8.2007 [cit. 21.4.2012]. Dostupné z: < http://www.abclinuxu.cz/clanky/bezpecnost/openssh-bezpecne-a-pohodlne>
[17] Introducing Extensions to the Negotiate Authentication Package [online]. Technet.microsoft.com. 3/2009 [cit. 1.6.2012]. Dostupné z: <http://technet.microsoft.com/cs-cz/library/dd560645%28v=ws.10%29.aspx>
[18] NTLM Authentication Protocol and Security Support Provider [online]. Sourceforge.net. Glass E. 2006 [cit. 2.6.2012]. Dostupné z: <http://davenport.sourceforge.net/ntlm.html#ntlmVersion2>

10 SEZNAM OBRÁZKŮ

11 SEZNAM DIAGRAMŮ