VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

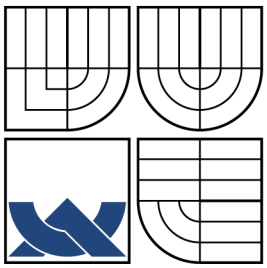
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

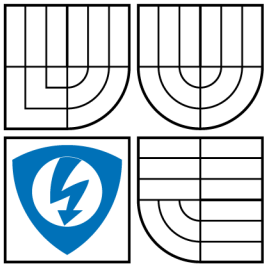
ZABEZPEČENÍ OPERAČNÍHO SYSTÉMU APPLE OS X

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE JOSEF HOŠEK
AUTHOR



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND
COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

ZABEZPEČENÍ OPERAČNÍHO SYSTÉMU APPLE OS X

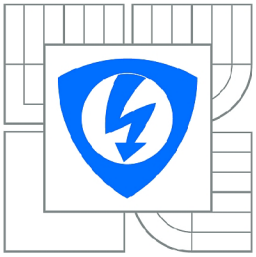
SECURITY OF OPERATING SYSTEM APPLE OS X

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — JOSEF HOŠEK
AUTHOR

VEDOUCÍ PRÁCE — Ing. JAN HAJNÝ, Ph.D.
SUPERVISOR

BRNO 2013



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Josef Hošek	***ID:***	134499
Ročník:	3	***Akademický rok:***	2012/2013

NÁZEV TÉMATU:

Zabezpečení operačního systému Apple OS X

POKYNY PRO VYPRACOVÁNÍ:

Téma je zaměřeno na využití bezpečnostních prvků operačního systému OS X Mountain Lion. Cílem práce je nastudovat strukturu operačního systému OS X a analyzovat bezpečnostní mechanismy na této platformě. Výstupem projektu bude zhodnocení použitých mechanismů z pohledu kryptografie a demonstrace na reálných scénářích použití v síťové bezpečnosti a řízení přístupu. Součástí výstupu je také implementace pokročilých metod filtrace síťového provozu a benchmarky šifrovacího subsystému.

DOPORUČENÁ LITERATURA:

[1] STALLINGS, William. Cryptography and Network Security: Principles and Practice (5th Edition). USA : Prentice Hall, 2010. 744 s. ISBN 0136097049.

[2] Mac OS X: Security Configuration. [online]. roč. 2010 [cit. 2012-10-09]. Dostupné z: http://images.apple.com/support/security/guides/docs/SnowLeopard_Security_Config_v10.6.pdf

Termín zadání:	11.2.2013	***Termín odevzdání:***	5.6.2013

Vedoucí práce: Ing. Jan Hajný, Ph.D.
Konzultanti bakalářské práce:

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Práce se zabývá rozborem bezpečnosti operačního systému Mac OS X ve verzi 10.8 „Mountain Lion“. Bezpečnost je probírána z pohledu prvků a nástrojů, které jsou v systému implementovány a používány. Všechny používané prvky a nástroje jsou dále podrobně popsány z pohledu jejich funkce. V praktické části práce jsou obsaženy postupy pro konfiguraci bezpečnostních prvků systému, otestování vlivu šifrování na rychlost systému, nastavení a popis komplexního firewallu vytvořeného pomocí IPFW. Jako poslední je popsán a zprovozněn scénář s přesměrováním a překladem adres pomocí NATD mezi dvěma OS X.

KLÍČOVÁ SLOVA

Bezpečnost operačního systému, Apple, Mac OS X, Mountain Lion, šifrování, firewall, IPFW, NATD, FileVault,

ABSTRACT

Project deals with the analysis of the security of Mac OS X version 10.8 „Mountain Lion“. Security is discussed in terms of components and tools that are used in this system. All used components and tools are described in terms of their function. The practical part of the bachelor thesis contains procedures for configuring security features of the system, testing the influence of encryption on the speed of the system, comprehensive description of the firewall created by IPFW. At the end is described scenario for forwarding and address translation by NATD.

KEYWORDS

Security of operating system, Apple, Mac OS X, Mountain Lion, encrypting, firewall, IPFW, NATD, FileVault

HOŠEK, Josef *ZABEZPEČENÍ OPERAČNÍHO SYSTÉMU APPLE OS X*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. 60 s. Vedoucí práce byl Ing. Jan Hajný, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „ZABEZPEČENÍ OPERAČNÍHO SYSTÉMU APPLE OS X“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

(podpis autora)

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu semestrální práce panu Ing. Janu Hajnému, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

(podpis autora)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic

http://www.six.feec.vutbr.cz

PODĚKOVÁNÍ

Výzkum popsaný v této bakalářské práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .

(podpis autora)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

OBSAH

SEZNAM OBRÁZKŮ

1 ÚVOD

Téma mé práce je zaměřeno na využívání bezpečnostních prvků v operačním systému od firmy Apple, OS X „Mountain Lion“. Při vypracování práce jsem se zaobíral zkoumáním a popisem veškerých bezpečnostních prvků a nástrojů používaných v tomto operačním systému. Probírána je vlastní struktura systému, jeho historie a obecný popis šifrovacích procesů, které jsou dnes používány. Dále jsou ve třech kapitolách podrobněji popsány prvky používané při práci s uživatelskými účty, šifrováním a síťovou bezpečností.

V praktické části práce jsou tyto prvky popsány z hlediska reálného používání. V první části jsou vypracovány jednoduché postupy, které ukazují jednotlivé kroky pro správné nastavení těchto prvků. V další části je otestován vliv šifrování na práci v systému. Následně je vypracován a popsán komplexní firewall vytvořený pomocí IPFW. A jako poslední úsek praktické části je popsán a zprovozněn scénář s přesměrováním a překladem adres v rámci dvou OS X systémů.

1.1 Historie Mac OS

Mac OS je operační systém navržený firmou Apple, pro jejich počítače Macintosh. Systém je založený již od počátku vývoje na ovládání pomocí grafického rozhraní. Proto má právě Mac OS zásluhu na zpopularizování ovládání počítače pomocí grafického rozhraní a tím i na celkovém zjednodušení ovládání počítačových systémů. Apple se od začátku snažil tento operační systém dělat co nejvíce uživatelsky přívětivý a jednoduše ovladatelný, což byl rozdíl například oproti MS-DOS, který byl více technicky náročný na ovládání.

První operační systém byl představen v roce 1984 v počítačích Macintosh, kde nebyl pojmenován, a proto byl nazýván jednoduše Systém. Takto se nazýval až do verze 7 a jako Mac OS byl poprvé označen až ve verzi 7.5 [7].

První verze Mac OS [1] byly kompatibilní pouze s počítači Macintosh založenými na mikroprocesorech Motorola 68000, které se v polovině 80. let začaly používat jak v osobních počítačích, tak například v laserových tiskárnách. Když Apple uvedl počítače s PowerPC hardwarem, operační systém byl portován na tuto architekturu. Verze 8.1 byla poslední, která podporovala procesory Motorola 68K. Mac OS X, který nahradil dřívější Mac OS, byl kompatibilní pouze s PowerPC procesory, a to od verze 10.0(„Cheetah“) do verze 10.3 („Panther“). PowerPC a Intel procesory byly podporovány pouze ve verzi OS X 10.4 („Tiger“) a OS X 10.5 („Leopard“). Od verze 10.6 tento systém podporuje pouze procesory firmy Intel [2].

Klasický Mac OS ve verzích 7, 8 a 9 je v základu takřka totožný. Oproti předchozím verzím už byly tyto verze plně 32bitové a funkce Finder byla plně nahrazena novější verzí (MultiFinder). Systém 7, který byl vydán v roce 1991, byl na svou dobu skutečně velmi vyspělým systémem, a proto byl používán až do roku 1997, kdy byl nahrazen osmou verzí. Tato verze byla velmi podobná svému předchůdci, ale navíc do ní byly začleněny některé technologie z Coplandu (OS) a ve verzi 8.1 byla přidána podpora Carbonu (vývojové prostředí), která se používá dodnes. Mac OS 9 byl představen v roce 1998, kdy už měl Apple jasné plány s další verzí systému. Proto hlavním úkolem této verze, bylo připravení platformy Macintosh k přechodu na verzi systému nazvanou Mac OS X.

Mac OS X je poslední verze systému od firmy Apple, který začal vznikat v polovině 90. let minulého století. V této době byly na trhu další operační systémy, jako uživatelsky přátelský systém Windows 95 od Microsoftu a také unixové systémy, které vynikaly svou stabilitou. V této době začal Apple ztrácet, protože jeho systém nevyhovoval v mnoha ohledech, od prakticky neexistujícího multitaskingu po poměrně značnou nestabilitu (Mac Extension Hell, což byla jakási obdoba modré obrazovky smrti na Windows). A tak bylo jasné, že Apple potřebuje nový operační systém. V této době Apple vyzkoušel mnoho různých projektů, jako byly například Copland, BeOS, TalOS nebo dokonce portování Windows NT na Macintosh s PowerPC architekturou. Ale jen málo z těchto projektů bylo více než pouhým pokusem.

V únoru roku 1997 kupuje Apple společnost NeXT, kterou vlastnil v té době zakladatel firmy Apple Steve Jobs. Systém vycházející ze získaného NeXTu byl pojmenován Rhapsody a po jeho spojení s Mac OS a několika unixovými technologiemi byl v březnu 1999 vydán jako Mac OS X Server 1.0 a zároveň jeho unixový základ pod smíšenou Open Source licencí Darwin 1.0. První uživatelsky orientovaný Mac OS X vyšel v roce 2000 a po půl roce byl v březnu 2001 následován první prodávanou finální verzí, nazvanou Mac OS X 10.0 "Cheetah". Ta ovšem měla mnoho nedostatků a tak šest měsíců poté vyšla verze 10.1 "Puma". Mnohdy za přelomovou je ale považována až verze 10.3 "Panther", která byla skutečně první dospělý Mac OS X. Kromě perfektní stability a rychlosti, obsahovala také řady vylepšení jak uživatelského rozhraní, tak samotných funkcí systému. Funkce jako Exposé nebo FileVault nebyly dlouho k vidění na jiných systémech.

Dnes je podíl Mac OS X na trhu v celosvětovém měřítku zhruba 7,2 %. U nás je to pouze 2,7 %, což je poněkud méně oproti celosvětovému podílu.

1.2 Bezpečnost operačních systémů

Způsobů jak zajistit požadovaný stupeň ochrany v rámci operačního systému je řada. Za nejoptimálnější řešení můžeme považovat vývoj zcela nového systému, kde si stanovíme bezpečnostní požadavky již na začátku vývoje, a proto je můžeme lépe implementovat. Avšak tato možnost je složitá a náročná, proto se užívají spíše další možnosti zajištění úrovně bezpečnosti jakou požadujeme. Jednodušším způsobem je odpovědné konfigurování všech funkcí některého ze stávajících operačních systémů. A také dostatečně časté využívání záplat a různých aktualizací, které můžou zajistit lepší funkci a možnosti bezpečnostních nástrojů. Dnes mají operační systémy své bezpečnostní nástroje implementovány. Samozřejmě je možné systém doplnit dalšími nástroji, případně některý z integrovaných nástrojů nahradit. Může jít například o antivirus, antispamové nástroje, šifrovací nástroje nebo firewall.

Antivirové programy nebývají vždy integrovány v systému, a proto si je občas musí doplnit sám uživatel. Tento typ programu kontroluje soubory na disku a také veškerou aktivitu programů. A v obou těchto funkcích se snaží identifikovat infekci, kterou poté odstraní nebo umístí do karantény. Nebezpečné programy označujeme malware nebo spyware. Spyware je program, který po svém vniknutí do počítače, začne odesílat různé typy dat a informací o uživateli svému autorovi a to bez svolení uživatele. Tohoto škodlivého programu je mnoho typů a každý je možné identifikovat pomocí určitého příznaku. Malware je oproti tomu program, který není určen k odesílání dat, ale k poškození funkce a obsahu počítače, nebo případnému převzetí kontroly nad systémem. Proti těmto a mnoha dalším nebezpečím je třeba se bránit a to tak, že se budeme vyhýbat programům a webovým stránkám, ze kterých by mohl útok přijít.

Rozsáhlé využívání výpočetní techniky v dnešní době, vede ke stále zvětšujícímu se objemu zpracovávaných a ukládaných dat. A to nejen v rámci lokální sítě, ale i internetových úložišť. Proto šifrování nejen našich soukromých dat, ale také naší komunikace v rámci internetu je velmi důležité. Zabezpečení dat šifrováním je proto samozřejmostí v každém bezpečném operačním systému. Mac OS proto obsahuje defaultně FileVault, který v nejnovějších verzích šifruje celý disk oproti dřívějšímu šifrování pouze domovských adresářů. Windows integruje svůj Encrypting File System (EFS) a BitLocker, kde BitLocker šifruje celý disk podobně jako FileVault a EFS slouží k šifrování jednotlivých složek a souborů. Také Linux má své šifrovací nástroje, jako například dm-crypt. Šifrování je samozřejmě možné provádět i pomocí externích multiplatformních nástrojů, jako je například TrueCrypt.

Bezpečnost sítě má mnoho úhlů pohledu a v první řadě záleží na tom, jakým potencionálním útokům může být vystavena. Druhů útoků dnes existuje nepřeberné množství a mezi nejzákladnější patří například falšování IP adres, odposlech paketů

nebo útoky s odepřením služeb. Naproti tomu na straně uživatele připojeného k síti je důležité dbát na ochranné prvky. Tyto ochranné prvky jsou dnes součástí každého operačního systému již při jeho nainstalování. Pro řízení a zabezpečení síťového provozu používají všechny operační systému svůj firewall. Firewallů existuje více typů, a to paketový, aplikační a stavový. Stavový firewall je rozšířením a vylepšením nejjednoduššího paketového firewallu (např. ACL používaný v Mac OS). Rozdíl mezi nimi je takový, že stavový firewall si oproti paketovému ukládá již povolené spojení pro jednodušší rozhodnutí při dalším spojení. Aplikační firewally existují dvojího typu, host-based nebo network-based a pracují na sedmé aplikační vrstvě OSI modelu.

1.3 Kryptologie

Se zabývá všemi typy šifrování, které se dnes používají nebo se používaly dříve. Má dvě hlavní disciplíny, a to kryptografii a kryptoanalýzu.

Kryptografií můžeme označovat postupy, kterými se různé informace a data mění tak, aby je mohl přečíst pouze ten, kdo vlastní určité specifické znalosti nebo klíče. Původ slova kryptografie je v řeckých slovech *kryptós (skrytý)* a *gráphein (psát)*. Šifrování se používá a vyvíjí již po staletí a to stále k větší složitosti, protože nároky na šifrování různých dat jsou neustále větší. Tyto nároky jsou v dosti velké míře ovlivňovány historickými událostmi. Kryptografii je možné teoreticky dělit na dvě hlavní části, a to na klasickou a moderní. Kde za klasickou můžeme považovat dobu před započetím používání výpočetní techniky a to je období přibližně do poloviny 20. století. Moderní kryptografie je charakteristická vznikem sofistikovaných přístrojů díky kterým mohly být postupy šifrování složitější. Dnes se doba posunula od používání zvláštních přístrojů k užívání softwaru na počítačích.

Kryptoanalýza vychází z řeckých slov krypós (skrytý) a analýein (uvolnit). A oproti kryptografii se zaobírá postupy, jak ze zašifrovaných dat získat původní informaci bez přístup ke klíči. Šifrou můžeme označit algoritmus, který slouží k zašifrování čitelné zprávy nebo dat do takové podoby, kterou nikdo bez specifického klíče nepřečte. Proto je klíč velmi důležitý a měli by se k němu dostat pouze uživatelé, kterých je to dovoleno.

1.3.1 Symetrická šifra

Je takový šifrovací algoritmus, který k šifrování i dešifrování užívá stejný klíč. Výhodou tohoto typu šifrování je značná výpočetní nenáročnost. Oproti tomu nevýhodou je potřeba sdílení tajného klíče, proto se musí odesílatel a příjemce předem domluvit

na tajném klíči. Symetrické šifrování je často použito společně se šifrou asymetrickou a to z důvodů lepší bezpečnosti. A je to provedeno tak, že text je zašifrován šifrou symetrickou s náhodným klíčem a poté tento klíč zašifrujeme pomocí veřejného klíče asymetrické šifry. Takže získat šifrovaná data může pouze majitel, který vlastní tajný klíč asymetrické šifry. Symetrické šifrování rozdělujeme na proudové šifrování (FISH, RC4), které zpracovává text po jednotlivých bitech a šifrování blokové (AES, Blowfish, DES, IDEA atd.), které rozdělí text na bloky stejné velikosti a doplní vhodným způsobem poslední blok na stejnou velikost. U většiny šifer se používá blok o 64 bitech, AES používá 128 bitů.

Advanced Encryption Standart (AES) je specifikace pro šifrování elektronických dat stanovená úřadem pro standardizaci (NIST) v roce 2001 v USA. Když dva belgičtí autoři šifru přihlásili do soutěže o federální šifrovací algoritmus AES, jmenovala Rijindael. Později byla tato šifra vyhlášena jako nejvhodnější ze všech návrhů v soutěži. AES je první šifra dostupná pro veřejnost, která byla zároveň povolena Národní bezpečnostní agenturou (NSA) k šifrování nejtajnějších dokumentů. Dnes se používá pří zabezpečení například Wi-Fi sítí v rámci zabezpečení WPA2 ve standardu IEEE 802.11.

AES je rychlé šifrování a oproti svému předchůdci neužívá Feistelovu síť. AES má přesně určené velikosti jak bloku tak klíče a to 128 bitů pro blok a 128, 192 nebo 256 bitů pro klíč. Pro srovnání Rijindael má specifikovanou velikost bloku i klíče jako násobky 32 bitů, kde oba mají minimum 128 bitů a maximum 256 bitů. AES s maticemi pracuje ve více krocích a v těchto krocích provádí postupy jako prohození řádků nebo přidání podklíče. Asymetrická kryptografie je souhrn takových metod, ve kterých je pro šifrování a dešifrování používáno odlišných klíčů. To je hlavním rozdílem oproti symetrickému šifrování, kde je použit pouze jeden klíč.

1.3.2 Asymetrická šifra

Je také používána pro tzv. elektronický podpis. Šifrovací klíč pro asymetrickou šifru se skládá ze dvou částí, kde jedna část je používána pro šifrování zprávy a příjemce zprávy tuto část znát nemusí. A druhá část je určena pro dešifrování zprávy a naopak s touto částí odesílatel zprávy být seznámen nemusí. Proto je jasně viditelné, že odesílatel a příjemce spolu nemusí sdílet žádné privátní informace a z tohoto důvodu je použití asymetrického šifrování výhodné. Je zřejmé, že oba klíče spolu musí být nějakým matematickým způsobem svázány, avšak musí být prakticky nemožné pomocí jednoho z klíčů vypočítat klíč druhý. Asymetrická šifra je založena na tzv. jednocestných funkcích, což jsou operace, které lze lehce provést pouze v jednom směru. A to znamená, že ze vstupu na výstup se dopočítáme snadno, ale opačně je to velmi složité.

Elektronický podpis je obdobou ručně psaného podpisu na písemných dokumentech. Zaručený elektronický podpis je takový podpis, který nezaručuje pouze autentizaci autora dokumentu, ale i jeho neporušenou integritu. U některých podpisů je navíc vyžadován určitý typ certifikace. Zaručený elektronický podpis tedy deklaruje autenticitu, což znamená, že můžeme ověřit identitu majitele elektronického podpisu. Deklaruje také integritu dokumentu, takže je zaručeno, že podepsaný dokument nebyl změněn ani poškozen. Tento podpis také může zaručovat nepopíratelnost dokumentu a též může obsahovat časové razítko pro určení času, kdy došlo k podepsání dokumentu.

Elektronický podpis je založen na principu asymetrické šifry a z toho důvodu je použita právě tato šifra. Algoritmy pro vytváření elektronického podpisu mohou být asymetrické algoritmy s veřejným klíčem a to nejčastěji *RSA (Rivest-Shamir-Adleman)* a *DSA (Digital Signature Algorithm).* Anebo algoritmy jednocestné (neboli hašovací funkce) jako *MD5 (Message Digest 5)* spolu s *RSA* a *SHA (Secure Hash Algorithm).*

Z důvodů zjednodušení práce šifrujeme místo celého dokumentu pouze jeho tzv. hash, který je výstupem hašovácí funkce a označujeme ho např. jako výtah, miniatura, otisk, fingerprint či hash. Při vytváření zmíněného hashe dokumentu, pomocí hašovací funkce, jsou používány takové algoritmy, že je dnes prakticky nemožné změnit kteroukoliv část dokumentu takovým způsobem, aby se zároveň nezměnil jeho výstupní hash.

Hašovací funkce je algoritmus určený pro převod dat na vstupu do relativně malého čísla na výstupu. Mezi hlavní vlastnosti této funkce patří schopnost, z jakkoli velkého množství dat na vstupu. Vytvořit vždy stejně dlouhý hash na výstupu a také jakákoliv nepatrná změna na vstupu je na výstupu reprezentována takovým způsobem, že je viditelná na první pohled. Za další vlastnosti hašovací funkce považujeme to, že z výstupního hashe je prakticky nemožné získat původní zprávu, která byla na vstupu této funkce. Také je v praxi téměř nemožné, aby dvěma různým zprávám odpovídal stejný výstupní hash. Jinými slovy, pomocí výstupního hashe můžeme identifikovat pouze jednu unikátní zprávu, ze které hash vznikl.

Kryptografické hašovací funkce jsou používány právě k ochraně proti úmyslnému znehodnocení či úpravě dat. Zde není prvořadá rychlost, ale kryptografické vlastnosti. Nejdůležitějšími vlastnostmi této funkce jsou ty, které určují náročnost napadení této hašovací funkce. Náročnost je vlastně výpočetní složitost, která by měla být v dnešní době mimo reálné možnosti. Zmíněné vlastnosti jsou dány:

- odolností proti získání předlohy,
- odolností proti nalezení kolize,
- a dalšími požadavky, jako například ošetření vstupních a výstupních bitů kvůli

znemožnění statistické kryptoanalýzy.

Message-Digest algorithm je oblíbená MD5, která je používána v mnoha aplikacích pro kontrolu integrity souborů nebo pro ukládání hesel. Tento algoritmus vytváří hash o velikost 128 bitů. Byl vytvořen v roce 1991, aby nahradil původní a méně bezpečný MD4. Již v roce 1996 byla nalezena vada i v MD5 algoritmu a i když tato chyba nebyla nijak zásadní, začaly se vyhledávat nové a bezpečnější algoritmy. V roce 2004 byl tento algoritmus prolomen úplně a postup pro nalezení kolizního páru zpráv byl zveřejněn. Ale i přesto je dnes tento algoritmus používán při přenosu souborů a pro kontrolu neporušení dat při jejich přenosu (md5sum).

Další hašovací funkce se jmenuje *Secure Hash Algorithm (SHA)*, která byla navržena organizací NSA a vydána Národním institutem pro standardy (NIST) jako americký federální standard (FIPS). Ve skupině SHA je obsaženo pět algoritmů a to SHA-1, SHA-224, SHA-256, SHA-384 a SHA-512. Poslední čtyři algoritmy se obecně označují jako SHA-2. Délka vytvořeného hashe je u SHA-1 160 bitů a u skupiny SHA-2 je délka viditelná z označení každého algoritmu. SHA je používáno v různých typech aplikací a protokolů a to včetně TLS, SSL nebo IPSec, ale také pro kontrolu integrity souborů. Tento algoritmus je bezpečnějším nástupcem výše zmíněného MD5.

Bezpečnost SHA-1 byla zpochybněna a prolomena a v roce 2005 byl zveřejněn algoritmus, který umožňuje nalézt kolizi podstatně rychleji než hrubou silou. Výpočetní náročnost je ovšem stále mimo současnou techniku. Skupina SHA-2 je součástí FIPS PUB 180-2 a používá podobné algoritmy jako SHA-1. Proto je zde snaha o vylepšení těchto hašovacích funkcí. A proto byla v roce 2007 vyhlášena výběrová soutěž pro novou SHA-3 funkci. V říjnu tohoto roku byla vybrána funkce Keccak [14] jako vítěz této výběrové soutěže.

Tiger je další hašovací funkce, která byla navržena v roce 1995. Tato funkce produkuje hash o délce 192 bitů, případně lze zkrácením původní délky dosáhnout délky 128 či 160 bitů u verzí Tiger/128 a Tiger/160. Také je používána pro kontrolu integrity souborů nebo ukládání hesel. Tiger2 je varianta původní funkce Tiger, u které se používá stejné zakončení vstupních dat jako u funkcí MD5 nebo SHA-1, oproti mírně odlišnému způsobu zakončení u původní funkce Tiger. Tato hašovací funkce se používá například v P2P (*Peer-to-peer*) aplikacích.

2 BEZPEČNOST MAC OS X

2.1 Úvod do bezpečnostní architektury OS X

Ať už tento systém bude používat jakýkoliv uživatel, jistě potřebuje zabezpečit důvěryhodnost a integritu svých dat. Zabezpečit tyto podmínky je v Mac OS X velmi jednoduché, protože je navržený tak, aby prvky zajišťující tyto podmínky byly integrovány a zároveň byly jednoduše ovladatelné a nastavitelné. Pro další zvýšení bezpečnosti vašeho počítače nabízí systém následující funkce:

- Nabízí moderní bezpečnostní architekturu, která podporuje standardy pro vývoj softwaru. To umožňuje vývoj bezpečného softwaru, ať už ze strany Applu nebo jiných vývojářů.
- Již při prvním použití OS X je systém defaultně nastaven tak, že splňuje bezpečnostní nároky požadované v mnoha prostředích. Proto má i nezkušený uživatel zajištěnu určitou úroveň bezpečnosti.
- OS X obsahuje nástroje jako FileVault, který chrání naše data na disku pomocí důvěryhodného šifrování. Integrovaný VPN klient nám umožnuje bezpečný přístup k síti a také silný firewall, který chrání naši síť. Díky těmto nástrojům nemusíme mít obavy z používání tohoto operačního systému.
- Základ systému v open source metodologii (OSS - *Open Source Software*) dělá tento systém na jednu stranu bezpečnějším, ale na druhou stranu i více zranitelným. Protože jakékoli chyby v systému mohou být identifikovány a opraveny Applem nebo velkou open source komunitou, ale také tyto chyby mohou identifikovat a zneužít potencionální útočníci. Obecně je ale OSS považován za věc prospěšnou a přínosnou.
- Rychlé řešení chyb je důležité pro zachování bezpečnosti, proto Apple spolupracuje s CERT (*Computer Emergency Response Team*). Z důvodu rychlejší identifikace potencionálních hrozeb a poté jejich rychlé opravy a distribuce oprav mezi uživatele.

Bezpečnostní architektura OS X je založena na dvou open source standardech. První je BSD (*Berkeley Software Distrubution*), což je forma UNIXu, která poskytuje základní služby, jako například přístupová oprávnění k souborům. Druhým je CDSA (*Common Data Security Architecture*), který poskytuje řadu bezpečnostních prvků, jako například specifičtější přístupová oprávnění, autentizace uživatelů, šifrování nebo zabezpečování datových úložišť.

Jádro (neboli kernel) OS X je postaven také na BSD, ale navíc i na Mach což je jádro, které bylo vyvinuto na Carnigie Mellon University. BSD poskytuje souborový systém, síťové služby a implementuje identifikaci uživatelů a skupin pomocí ID.

A pomocí těchto identifikačních ID skupin a uživatelů umožňuje omezení přístupových oprávnění k souborům a systémovým zdrojům. Mach navíc poskytuje správu paměti, kontrolu vláken (thread), propojení s hardwarem a komunikaci mezi procesy. Spojení BSD a Machu představuje podstatnou složku v bezpečnosti systému OS X.

Přístupová oprávnění jsou důležitou součástí počítačové bezpečnosti protože to, zda je oprávnění uděleno či nikoliv, je zásadním rozdílem. Oprávnění jsou udělována na úrovních složek, podsložek, souborů a aplikací. Oprávnění jsou také přidělována pro data v souborech nebo pro specifické funkce aplikací. Udělené oprávnění jsou kontrolovány na mnoha úrovních a to od součástí jádra až po vyšší úrovně operačního systému.

2.1.1 Autorizace versus Autentizace

Autorizace je proces, při kterém uživatel nebo počítač získává oprávnění k provedení určité operace, kterou by bez těchto oprávnění nemohl provést. Autorizace také může odkazovat na vlastní získaný souhlas jako „Anna má autorizaci ke spuštění tohoto programu“. Autorizace obvykle obsahuje i autentizaci uživatele, podle čehož může rozhodnout o správnosti přidělených oprávnění.

Autentizací rozumíme proces, při kterém dochází k ověření zda entita (neboli uživatel) je opravdu tím, kým tvrdí že je. Například, pokud určitý uživatel zadává soukromé heslo, může dojít k autentizaci dané osoby. Autentizace obvykle bývá součástí autorizačního procesu a některé aplikace nebo systémy mohou používat svou vlastní autentizaci.

2.1.2 Security Framework (Bezpečnostní rámec)

V Mac OS X je bezpečnostní rámec implementací CDSA architektury (*Common Data Security Architecture*), což je sada bezpečnostních služeb a kryptografických rámců které, poskytují infrastrukturu pro zabezpečení aplikací. Obsahuje rozšiřitelnou sbírku kryptografických algoritmů k provádění „code signing“ (podepisování aplikací) a šifrování operací pro zachování bezpečnosti kryptografických klíčů. Také obsahuje knihovny pro výklad X. 509 certifikátů.

CDSA kód je používán systémem jako keychain (klíčenka) a k ochraně přihlašovacích údajů při přístupu na web. Apple postavil OS X na OSS jako FreeBSD, Apache, Kerberos a další. OSS je podrobován testování během mnoha let používání uživateli. A to je hlavní výhodou open source softwaru, každý si může prohlédnout zdrojový kód a nalézt případné zranitelné místa. Poté tyto místa posílit a tím posílit i celý software. Apple se aktivně účastní tím, že uvolňuje pravidelně aktualizace

Mac OS X. Právě tyto aktualizace jsou podrobovány neustálému přezkoumávání ze strany nezávislých vývojářů a uživatelů.

Zabezpečení Mac OS X je postaveno na vrstvené obraně a to z důvodu zajištění co nejvyšší možné úrovně ochrany. Aplikování nabízených možností zabezpečí data na všech úrovních a to od operačního systému až k aplikacím a sítím.

- Zabezpečení komunikace přes internet zajistí aplikační nebo IPFW firewall a kontrola e-mailů, která pomůže odfiltrovat software, který by mohl ohrozit počítač.
- Bezpečnost aplikací je zajištěna pomocí šifrovaných obrazů disku a FileVaultu, který šifruje veškeré data na počítači v reálném čase.
- Bezpečnostní síťové protokoly - *Secure Socket Layer* (SSL) je protokol, který se nejčastěji používá pro zajištění bezpečné komunikace s internetovými servery pomocí HTTPS. SSL funguje na principu asymetrické šifry, což znamená, že každá strana ma dvojici šifrovacích klíčů. Kerberos oproti tomu zabezpečuje například autentizaci uživatele v nezabezpečené síti a to většinou pomocí symetrické kryptografie (potřebuje třetí důvěryhodnou stranu). V dílčích částech svých procesů může také využívat kryptografii asymetrickou.
- Bezpečnostní služby - autentizace používá tzv. keychain (klíčenka) společně s oprávněními POSIX a ACL. Kde standard POSIX (*Portable Operating System Interface*) zajišťuje kompatibilitu mezi operačními systémy a také definuje rozhraní pro programování aplikací (API - *Application Programming Interface*). A v ACL (*Access control list*) jsou přidělena jednotlivá přístupová práva pro uživatele.
- Průvodce nastavením hesla (*Password utility*) pomáhá nastavit co nejbezpečnější heslo na nejnižší vrstvě systému. A tím brání v přístupu k důvěrným informacím i pokud útočník získá fyzický přístup k počítači.

Zabezpečení transportní vrstvy používá *Secure Socket Layer* (SSL) a *Transport Layer Security* (TLS). Tyto protokoly zajišťují zabezpečenou komunikaci přes síťovou vrstvu. Firewall poté může filtrovat komunikace přes TCP/IP protokol, pomocí povolení nebo zamítnutí přístupu k počítači nebo síti.

Klíčenky (keychains) jsou používány pro ukládání hesel, klíčů, certifikátů a dalších dat umístěných do klíčenky uživatelem. Díky citlivé povaze těchto informací je klíčenka šifrována společně s klíčem k dešifrování. Mac OS X umožňuje vytvářet klíčenky a bezpečně ukládat položky klíčenky.
Po vytvoření klíčenky můžeme přidávat, mazat nebo upravovat její položky. Uživatel také může odemknout klíčenku pomocí autentizace, například použitím hesla, digitální známky (*digital token* - což je typ bezpečnostní známky, která provádí ověření pomocí například elektronického podpisu) nebo biometrické čtečky. Poté mohou

aplikace použít klíčenku pro uložení nebo obnovení dat jako jsou hesla.

2.2 Zabezpečení uživatelských účtů

Před samotným zabezpečením uživatelských účtů je nutné definovat, jak budou účty používány a jak vysoká úroveň zabezpečení bude nutná. Když definujeme účet pro uživatele, musíme specifikovat informace, pomocí kterých bude uživatel prokazovat svoji identitu. Tyto informace jsou reprezentovány uživatelským jménem, metodou autentizace (heslo, bezpečnostní známka, smart card nebo biometrická čtečka) a identifikačním číslem uživatele. Informace v účtu uživatele mohou být dotazovány různými službami k upřesnění jaký uživatel je přihlášen a poté mohlo dojít k případné personalizaci uživatelského prostředí.

2.2.1 Typy uživatelských účtů

Pro přihlášení do systému je možné použít běžný nebo administrátorský účet. Hlavní rozdíl mezi těmito účty je ten, že běžný účet je omezen bezpečnostními mechanismy, aby nemohl provádět úpravy v systému, které by mohly ohrozit jeho funkčnost nebo narušit bezpečnost. Administrátorský účet oproti běžnému nemá tento typ omezení. Dále můžeme specifikovat oba typy účtů a to pomocí dalšího přidělení výsad a omezení.

Tab. 2.1: Typy uživatelských účtů

Uživatelský účet	**Uživatelský přístup**
Host účet	Omezený uživatelský přístup (defaultně vypnutý)
Standardní účet	Neomezený uživatelský přístup
Spravovaný účet	Omezený uživatelský přístup
Administrátorský účet	Plný přístup ke konfiguraci počítače
Systémový root účet	Neomezený přístup k počítači

Pokud není administrátorský přístup potřebný k systémové údržbě, kterou nelze vykonat při přihlášení na běžném účtu nebo autentizací na administrátorský účet z účtu běžného, měl by být vždy používán běžný účet. V případě že není administrátorský účet používán, měl by být odhlášen, aby nedošlo k jeho narušení. Běžné aktivity jako je prohlížení internetu nebo kontrola e-mailů, by měly být vždy prováděny z běžného účtu.

Při vytváření uživatelských účtů musíme dodržovat určitá pravidla:

- Každý účet by měl být užíván právě jedním uživatelem a to jak účet běžný, tak administrátorský. A to hlavně pro zjednodušení mapování aktivit uživatelů.
- Uživatel, který potřebuje administrátorský přístup, musí mít jak běžný účet, tak účet administrátorský. Administrátorský účet by měl používat pouze k účelům, u kterých je potřeba tohoto oprávnění a k normální práci užívat účet běžný. Tím se snižuje riziko například náhodného přenastavení systému a narušení bezpečnosti.

Uživatelské ID je číslo identifikující unikátně každého uživatele. Systém používá tato ID ke zjištění, jaké složky a soubory daný uživatel vlastní. Protože když uživatel vytvoří složku nebo soubor, jeho ID je uloženo jako podpis tvůrce a tento uživatel má defaultně oprávnění pro čtení a zápis. Uživatelské ID jsou řetězcem čísel v rozmezí 500 a 2 147 483 648.

Samozřejmě je riskantní přidělit více uživatelům stejné ID, protože tito uživatelé by mohli přistupovat jak do složek a souborů svých, tak i do složek a souborů uživatelů se stejným ID. Nicméně každý uživatel má unikátní GUID (*Globally unique identifier*), který je generován pří vytváření účtu. A ke GUID jsou asociovány ACL oprávnění, která jsou nastavena u složek a souborů. A právě přiřazování těchto oprávnění na základě GUID řeší problém více uživatelů se shodným ID.

Nulová hodnota uživatelského ID je rezervována pro root uživatele. ID s hodnotou pod 100 jsou vyhrazeny pro systémové účely. Tyto ID nemohou být smazány a upravovány, pouze může být upraveno přístupové heslo root uživatele. Pokud nechceme, aby se náš účet zobrazoval na přihlašovací obrazovce, musíme mu přidělit ID s hodnotou nižší než 500 a v okně Terminálu zadat příkaz pro skrytí tohoto účtu.

Jakmile je ID přiděleno a uživatel začne vytvářet složky a soubory, není možné jeho unikátní ID změnit. Jediná výjimka je možná pouze v případě přenosu uživatelských účtů z jiného serveru a tím pádem možného vzniku shod ID uživatelů.

2.2.2 Zabezpečení host (guest) účtu

Host účet je používán k přidělení dočasného přístupu k počítači. Pokud ho chceme použít, musíme ho povolit, protože defaultně je vypnut. A to z důvodu, že pro přihlášení není třeba žádného hesla. Proto by tento účet měl zůstat vypnut. Pokud ho i přes jeho nezabezpečenost potřebujeme použít, musíme ho bezpečně nakonfigurovat, aby nemohlo dojít k ohrožení bezpečnosti počítače. Tím je myšleno například zakázání přístupu do sdílených složek na počítači.

2.2.3 Zabezpečení běžných účtů

Máme dva typy běžného účtu. První z nich je standardní účet, který nemá administrátorská práva a ani nemá aktivní rodičovskou kontrolu, která by mohla nějak dále omezovat jeho možnosti. Naopak druhý spravovaný účet (řízený rodičovským dohledem)také nemá administrátorská práva, ale rodičovskou kontrolu má aktivní, což pomáhá kontrolovat uživatele a zabránit případnému zneužití počítače. Při vytváření těchto účtů, bychom měli omezit účet tak, aby byl schopen provádět jen akce, které potřebuje.

Rodičovská kontrola slouží k omezování oprávnění používat různé aplikace a provádět různé činnosti na účtu. Například můžeme odepřít možnost instalovat software nebo omezit přístup k určitému softwaru. Při nastavování těchto omezení máme široké možnosti.

2.2.4 Zabezpečení externích účtů

Externí účet je mobilním typem účtu, což znamená, že jeho domovská složka je uložena na externím disku. Když přihlásíme externí účet do systému, je možné vidět pouze tento jeden účet (ostatní jsou skryty). Externí účty jsou podporovány od verze 10.6 „Snow Leopard“ a potřebují disk formátovaný jako Mac OS X Extended formát (HFS Plus). Při použití tohoto typu účtu je nutné použití FileVaultu, kvůli ochraně našich dat při ztrátě.

2.2.5 Zabezpečení directory-based účty

Tento účet je uložen na adresářovém serveru, který obsahuje evidenci uživatelských účtů a důležitá data pro autentizaci uživatelů. Pokud je počítač připojen k adresářovému serveru, můžeme přidat složku uživatelů a udělit jim oprávnění. Tento účet je možné omezit pomocí rodičovské kontroly. Přístup k adresářovému serveru je obvykle hodně omezen z důvodu ochrany dat na tomto serveru.

2.2.6 Zabezpečení administrátorských účtů

Každý administrátor by měl vlastnit dva účty. Jeden běžný účet pro denní práci a druhý administrátorský pro administrátorský přístup. Běžný účet by měl používat pro většinu denní práce, obzvlášť pokud přistupuje do sítě a na internet. Administrátorský účet by měl užívat, jen pokud to je jediná možnost jak vykonat určitou úlohu. K zachování bezpečnosti těchto účtů musíme omezit jejich počet a také jejich používání. Uživatelský účet s administrátorskými výsadami může provádět úlohy jako

standardní uživatel i jako administrátor (vytváření účtů, změna master hesla FileVaultu, povolení sdílení, operace s firewallem, instalovat systémový software a další).

2.2.7 Zabezpečení systémového root účtu

Nejmocnější účet v Mac OS X je právě systémový root účet. Defaultně je tento účet zakázán a je doporučeno toto nastavení neměnit. Root účet je primárně určen k provádění Unixových příkazů. Obvykle akce obsahující systémové soubory potřebují oprávnění root. Pokud je administrátor přihlášen na administrátorském účtu může provádět příkazy jako root a to pomocí příkazu `sudo`. Systém zaznamenává činnosti provedené pomocí příkazu `sudo`, proto aby bylo možné snadným způsobem odhalit zneužití tohoto příkazu. Bezpečnější je ponechat root účet zakázaný a pro akce, které vyžadují root oprávnění použít administrátorských účtů a příkazu `sudo`. Protože root účet není nijak kontrolován, tak u něj nelze zjistit, jaký uživatel provedl danou činnost.

2.2.8 Directory Domains (adresář domén)

Uživatelské účty jsou skladovány právě v adresáři domén. Preference a atributy účtu jsou nastaveny podle informací uložených v adresáři domén. Místní účty jsou umístěny v lokálním adresáři domén a při přihlášení probíhá autentizace k místnímu adresáři domén. Místní účet má také domovský adresář, kam jsou ukládány lokálně soubory.

Síťové účty jsou hostovány v síťovém adresáři domén a to pomocí *Lightweight Directory Access Protocol* (LDAP) nebo *Network Information Service* (NIS). Při přihlašování k síťovému účtu probíhá autentizace právě k síťovému adresáři domén. Tyto účty mají síťový domovský adresář, takže soubory ukládané do tohoto adresáře odesíláme přes síť na server.

Mobilní účty ukládají údaje k autentizaci a správě preferencí do mezipaměti (*cache*) počítače. Takže tyto informace jsou zachovány v síťovém adresáři domén, ale také jsou uloženy v mezipaměti místního počítače. Proto se uživatel může přihlásit pomocí stejných údajů, i když není připojen k sítí. Uživatelé s tímto účtem mají tzv. přenosný domovský adresář, který je kombinací domovského adresáře na počítači a na serveru. Tento přenosný adresář je synchronizován s podmnožinou účtů uživatele v místní síti a na serveru.

Na počítači můžeme nastavovat síťové adresáře domén pomocí *Adresářové utility*. Zde můžeme nastavovat typ adresářového vyhledávání, druh používaného protokolu a zásady vyhledávání údajů k ověření totožnosti a kontaktů. Všechny tyto informace používají různé části operačního systému.

2.2.9 Používání silné autentizace

Při autentizaci je ověřována identita uživatele. Mac OS X podporuje místní i síťový druh autentizace z důvodu zajištění přihlašování pouze uživatelů s platným pověřením. Heslo je proto potřebné k přihlášení, k probuzení počítače ze spánku a ze spořiče obrazovky, ale také k instalaci aplikací nebo ke změně systémového nastavení. Rovněž jsou podporovány různé druhy autentizace jako smart cards, digitální známka nebo biometrické čtečky. Silná autentizace je tvořena použitím kombinací následujících možností.

- Co ví uživatel, např. heslo nebo PIN kód.
- Co má uživatel, např. one-time-password (OTP) nebo smart card.
- Co uživatel je, např. otisk prstu nebo vzorek DNA.

Kombinací těchto možností vytvoříme autentizaci více důvěryhodnou a identitu uživatele potvrzenou s větší jistotou.

Při vytváření hesel je dobré používat průvodce nastavením hesla (*Password Assistant*). Tento průvodce analyzuje složitost hesel nebo hesla vytváří. Při vytváření můžeme určovat délku hesla a typ hesla. Můžeme vybírat z těchto druhů hesel:

- manuální - vložíme heslo a asistent nás informuje o síle hesla a případně nám nabídne možnost jak zvýšit bezpečnost hesla.
- Zapamatovatelné - podle našeho požadavku na délku hesla, asistent vytvoří seznam zapamatovatelných hesel.
- Písmena a čísla - podle našeho požadavku na délku hesla, asistent vytvoří seznam hesel, skládajících se z kombinací písmen a čísel.
- Pouze čísla - podle našeho požadavku na délku hesla, asistent vytvoří seznam hesel, skládajících se pouze z čísel.
- Náhodné - podle našeho požadavku na délku hesla, asistent vytvoří seznam hesel, skládajících se z náhodných znaků.
- Kompatibilní s FIPS-181 (*Federal Information Processing Standard*) - podle našeho požadavku na délku hesla, asistent vytvoří heslo, které bude FIPS-181 kompatibilní. Což znamená, že bude obsahovat malá i velká písmena, interpunkci a čísla.

Kerberos

Tento autentizační protokol je používán k jednoduchému systémovému přihlášení. To umožňuje autentizaci ve více službách v jeden čas a to bez opětovného zadávání hesel a jejich odeslání přes síť. Mac OS X používá Kerberos ke zjednodušení sdílení mezi počítači, proto není potřeba server pro sdílení klíče, když jde o dva počítače se systémem Mac OS X. Když se připojíme k počítači podporující Kerberos, je nám

poskytnuta vstupenka, která nám umožňuje dále používat systém. Vstupenka je časově omezená, takže musí být obnovena, pokud nechceme přijít o přístup.

2.3 Zabezpečení dat a šifrování

Nejcennější částí počítače jsou naše data, proto je potřeba ochrana šifrováním proti případným útokům, nebo pro případ krádeže počítače. A to pomocí nastavení globálních oprávnění, šifrování disku a také šifrování přenášených dat. Také je důležité používání bezpečného vymazání dat pomocí nástroje, který je součástí systému.

K ochraně našich souborů a složek slouží nastavení přístupových oprávnění. Mac OS X podporuje dvě možnosti nastavení oprávnění k jednotlivým souborům a složkám. A to jsou:

- **Portable Operating System Interface (POSIX)** oprávnění, která jsou používaná standardně v Unixových operačních systémech.
- **Access Control Lists (ACLs)**, což je doslova seznam pro řízení přístupu. Je používán v Mac OS X a také je kompatibilní s Microsoft Windows.

ACL používá POSIX oprávnění, když potřebuje ověřit oprávnění ke složkám a souborům. Postup při použití ACL, ke zjištění zda je akce povolena nebo zakázána, obsahuje i ověření tzv. položek pro řízení přístupu (*Access Control Entries* - ACEs). Pokud nejsou žádné položky ACE k dispozici, standardní POSIX pravidla určují oprávnění k přístupu.

Nastavení oprávnění na POSIX standardu je možné provádět pro adresáře a soubory, kde můžeme přidělovat čtyři druhy oprávnění: čtení a zápis, pouze čtení, pouze zápis a žádné oprávnění. Máme definovány tři základní kategorie: majitel, skupina nebo všichni. Majitel souboru má veškeré oprávnění a také může spolu s administrátorem přidělovat oprávnění k dané složce nebo souboru. Do skupiny můžeme přiřadit uživatele, kteří potřebují mít přístup ke stejným složkám a souborům a poté jim přidělit potřebná oprávnění.

Zjištění POSIX oprávnění můžeme provést pomocí terminálu nebo zobrazením informací o dané složce nebo souboru. POSIX oprávnění je interpretováno prvními deseti bity v dlouhé výstupní informaci souborů a složek. První písmeno symbolizuje zda jde o složku nebo soubor a následujících devět bitů rozdělíme vždy na trojici bitů a každá tato trojice určuje oprávnění pro jednu ze tří kategorií (majitel, skupina a všichni).

Pro větší flexibilitu při konfiguraci a kontrole oprávnění souborů obsahuje Mac OS X právě ACL. Každá položka pro řízení přístupu (ACE) obsahuje tyto komponenty:

1. Uživatel - majitel, skupina nebo ostatní.
2. Akce - čtení, zápis nebo provedení.
3. Oprávnění - povolení nebo zakázání akce.

ACL může nastavit oprávnění pro přístup k adresáři nebo souboru pro více uživa-

telů a také pro skupiny, což je výhoda oproti POSIX oprávnění. Toto zjednodušuje nastavení sdílení souborů při spolupráci mezi více prostředími.

Každý soubor a složka získá po svém vytvoření POSIX oprávnění a tyto oprávnění jsou přiřazeny pomocí Umask. Což je nastavení implicitní masky práv nově vytvořeným souborům a složkám.

2.3.1 Zabezpečení domovského adresáře uživatele

K zabezpečení domovského adresáře je třeba změnit přístupové oprávnění tak, aby tento adresář mohl být přečten a vyhledán pouze jeho majitelem. Při zakázaném FileVaultu jsou oprávnění k domovské složce nastaveny tak, že i ostatní uživatelé mohou prohlížet obsah tohoto adresáře. Složky, které jsou používány pro sdílení, musí být nastaveny tak, aby je bylo možné vyhledat a číst jinými uživateli. Ale pokud není sdílení používáno, oprávnění k těmto složkám můžeme omezit.

Mac OS X obsahuje **FileVault 2** (trezor souborů), který šifruje celý disk tak, aby tento disk nebyl čitelný nikomu, kdo nezná správný dešifrovací klíč. Kódování celého disku (FDE - *Full Disk Encryption*) by mělo splňovat tyto kritéria:

- uživatel by neměl nic nastavovat a proces šifrování by měl být transparentní a nezjistitelný během běžné práce,
- šifrování by mělo být chráněno proti neautorizovanému přístupu,
- použití šifrování by nemělo nijak zpomalit ani omezit funkce počítače.

FileVault 2 za správných okolností splňuje tyto tři kritéria. FileVault by měl být užíván v přenosných počítačích a v počítačích u kterých nemůžeme dostatečně garantovat jejich fyzickou bezpečnost.

V dřívějších verzích mohla být šifrována pouze domovská složka uživatele, ale od verze 10.7 „Lion“ je možné šifrovat celý disk. Nyní je používáno kódování XTS-AES 128 oproti dřívějšímu kódování AES 256 a právě použití tohoto „řidšího“ kódování umožnuje šetření místa na disku. FileVault 2 konvertuje celý disk v zašifrovaný svazek (*volume*). Dále je vygenerován silný šifrovací klíč, který je přístupný pouze z účtu určitého uživatele, kterého můžeme konfigurovat při startu počítače. Šifrovací 24místný klíč, který je vygenerovaný při zapnutí FileVaultu je možné zálohovat na server Applu a jeho pozdější získání je provázeno zodpovězením tří otázek, které si definujeme při ukládání hesla.

Při zapnutém FileVaultu jsou všechna data na disku převedena na nesrozumitelné bity při každém vypnutí počítače. Data jsou znova čitelná až při zapnutí počítače a přihlášení určitého uživatele. Proto je bezpečnější počítač vypínat, pokud ho nepoužíváme a fyzicky se od něj vzdalujeme, než ho jen uvádět do režimu spánku. Z tohoto jasně plyne, že FileVault dosahuje své plné účinnost jen při vypínání počítače namísto používání režimu spánku.

Pomocí FileVaultu je možné šifrovat i externí disky a umožnuje také vymazat veškerá data z počítače.

2.3.2 Bezpečné mazání dat

Když smažeme určitá data, tak smažeme informaci, kterou systém používá pro nalezení určitého souboru. Takže při smazání souboru je jeho místo označeno jako volné místo, a pokud není toto místo přepsáno jinými daty, je stále možné již vymazaný soubor obnovit i s jeho obsahem. Proto Mac OS X poskytuje tři druhy bezpečného mazání dat:

- zero-out vymazání,
- 7-pass vymazání,
- 35-pass vymazání.

Zero-out vymazání použité bity nastaví na hodnotu 0. Zatímco 7-pass a 35-pass mazání používá algoritmus pro přepis disku. I když je zero-out mazání nejméně bezpečné, je nejrychlejší vzhledem k dalším dvěma typům. Typ 35-pass je nejbezpečnější, ale také časově a výpočetně nejnáročnější. Při použití druhých dvou typů mazání je prováděno 7 kroků algoritmu (postupné přepisování pomocí stejného znaku, nul, stejného znaku, různých znaků, nul, stejného znaku a nakonec různých znaků), které brání právě nechtěnému obnovení již vymazaných dat. V systému si můžeme nastavit, aby byly data vždy vymazávány bezpečně.

2.4 Zabezpečení síťových služeb

Bezpečná konfigurace síťových služeb je velmi důležitou součástí zabezpečení počítače proti útokům ze sítě. Organizace i uživatelé jsou závislí na komunikaci jak v místních privátních sítích, tak v sítích velkých. Nesprávné nastavení síťových služeb může ohrozit tuto komunikaci a způsobit nemalé problémy. Mac OS X nabízí služby a nástroje, které mohou být rychle a lehce konfigurovány. A právě z důvodu takto jednoduché konfigurace musíme mít vždy přehled nad tím, kdo přistupuje k počítači. Většina služeb může být také zabezpečena pomocí užití silného hesla, nebo pokud není služba používána, můžeme ji vypnout.

2.4.1 Zabezpečení síťové komunikace

Použití firewallu k filtrování síťového provozu mezi jednotlivými počítači nebo sítěmi je důležité a může zabránit útočníkům, aby získali přístup k našemu počítači nebo k naší celé síti.

Firewall je software, který chrání systém před neoprávněným přístupem. Při jeho zapnutí dojde k pomyslnému postavení zdi kolem našeho systému, která kontroluje přístup k našemu počítači. Kontrola probíhá na úrovni síťového provozu a pomocí určitých pravidel je přijetí paketů povoleno nebo zakázáno. Také můžeme omezit přístup k síti jakékoli služby běžící na našem počítači. Firewallu můžeme také povolit zápis tzv. logů, což znamená, že do určitého souboru bude zapisována aktivita firewallu jako například, jaké připojení byly blokovány.

OS X má zabudované dva firewally, první je **aplikační firewall** a druhý je **IPFW firewall**. Pokud zapneme některou službu sdílení, jako je sdílení souboru, právě aplikační firewall ověří, zda se jedná o aplikaci podepsanou firmou Apple a posléze povolí její přístup k síti. Uživatel sám může v nastavení sdílení určovat jaké služby a aplikace budou moci přistupovat k síti. Pokud některá služba získá přístup k síti, ale zároveň se neobjeví v nastavení sdílení, může se jednat o systémovou aplikaci nebo službu. Tyto programy je možné blokovat až po jejich manuálním přidání do seznamu firewallu. A samozřejmě blokování přístupu k sítí může značně omezit funkčnost programu a také služeb, které na tomto programu závisí.

2.4.2 Aplikační firewall

Tento typ firewallu umožňuje kontrolu připojení na základě aplikací namísto dřívější kontroly na základě portů. Umožňuje uživateli jednodušeji využívat výhod bezpečnosti firewallu a také zamezit, aby nežádoucí aplikace převzaly kontrolu nad síťovými porty, které by měly využívat pouze autorizované aplikace. Firewall je aplikován na TCP, UDP a většinu běžně používaných protokolů. Toto neovlivňuje například AppleTalk, ale firewall je možné nastavit k blokování těchto příchozích ICMP (*Internet Control Message Protocol*) zpráv a to povolením tzv. Tajného módu (*Stealth mode*) v pokročilém nastavení firewallu.

Dřívější verze IPFW technologie jsou stále přístupné z příkazového řádku v Terminálu. Aplikační firewall nepotlačí pravidla nastavené IPFW technologií a pokud IPFW blokuje příchozí paket, aplikační firewall to nezpracuje.

Pokud je aplikační firewall vypnutý, systém nemůže blokovat příchozí spojení k počítači. Když firewall zapneme, začne blokovat neoprávněné aplikace a služby před přijetím příchozích připojení. Aplikační firewall má tyto módy:

- **blokování všech příchozích připojení** - toto je nejkonzervativnější mód. Blokovány jsou všechny připojení, až na nastavený seznam základních služeb pro operační systém a také ty služby a aplikace, které si uživatel sám povolí. Systémové služby, které mají stále povoleno přijímat příchozí připojení jsou:
  - `config`: implementuje DHCP a ostatní nastavení síťových služeb,

  - `mDNSResponder`: implementuje Bonjour (protokol pro zjišťování služeb v sítích),
  - `racoon`: implementuje Internet Key Exchange (IKE, což je protokol používaný k nastavení přidruženého zabezpečení (SA) v IPSec protokolu).
- **Automatické povolení podepsanému softwaru přijímat příchozí připojení** - tento mód je defaultně nastaven. Aplikace podepsané platnou certifikační autoritou mají povoleny služby přistupující ze sítě.
- **Povolení neviditelného režimu** (*Stealth mode*) - tento mód brání počítači, aby reagoval na ICMP (ping) žádosti. A skrývá ho před skenováním sítě.

Také můžeme manuálně nastavit přístup specifických služeb a aplikací, a to výběrem, zda má být povoleno nebo zakázáno příchozí připojení pro jakoukoli aplikaci v systému. Po přidání aplikace do seznamu, můžeme vybrat, zda má povoleno nebo zakázáno příchozí připojení a také jestli je tato aplikace digitálně podepsána systémem. Pokud je aplikace později upravena, uživatel je vyzván k povolení nebo zakázání příchozího síťového připojení. Většina aplikací se sama neupravuje a proto je tento bezpečnostní prvek užitečný právě díky těmto upozorněním při úpravě.

Neviditelný režim neboli „Stealth mode“ je obrana proti hackerům, kteří skenují síť, aby objevili případné počítače, na které by mohli zaútočit. Tento režim znemožňuje počítači na takové skenování odpovědět. Pokud je tento režim povolen, počítač neodpovídá na ICMP ping zprávy a také neodpovídá na pokusy o připojení ze zavřených portů TCP a UDP. Právě toto ztěžuje útočníkům najít náš počítač.

2.4.3 IPFW2 Firewall

Mac OS X obsahuje open source software, který se jmenuje IPFW2 a je používán jako alternativa firewallu. Při použití příkazu `ipfw` k filtrování paketů je použito pravidel, podle kterých se rozhoduje jaké pakety povolit a jaké odepřít. Firewall skenuje příchozí pakety a ty přijímá nebo odmítá na základě souhrnu filtrů a pravidel, které uživatel nastavil. Můžeme omezit přístup k jakékoli IP službě běžící na počítači a také můžeme přizpůsobit filtr pro všechny adresy nebo pro určitý rozsah IP adres. IPFW zpracovává pakety na nejnižší síťové vrstvě oproti firewallu aplikačnímu, který funguje na vyšší vrstvě. Proto jsou jeho pravidla upřednostňována před pravidly aplikačního firewallu.

IPFW firewall umožňuje vytvářet komplexní a silné filtrovací sady. Nastavení firewallu může být složité a také může narušit síťovou komunikaci při nesprávném nakonfigurování. Proto je potřebné psát pravidla zodpovědně a systémem se musí tyto pravidla načítat při jeho startu. Sada pravidel pro IPFW je vytvořena tak, aby při shodě paketů došlo k odpovídající akci. Pravidla jsou vyjádřena číselně

od hodnoty 0 do hodnoty 65 535. Paket, který projde k firewallu je porovnáván s každým pravidlem a pokud dojde ke shodě, je provedena odpovídající akce.

Zabezpečit můžeme také data, které posíláme přes nezabezpečenou síť (internet) a to použitím zabezpečeného síťového připojení. Toto brání neoprávněnému přístupu k našim datům. Zabezpečit vzdálený přístup do jiných sítí můžeme použitím VPN (Virtuální Privátní Síť). VPN je propojením několika počítačů prostřednictvím nedůvěryhodné sítě, ale pomocí soukromého spojení, které přenáší zabezpečená data. Toto spojení simuluje místní připojení, jako by byly počítače připojeny do místní sítě LAN. Existují tři druhy zabezpečení transportního protokolu: *Layer Two Tunneling Protocol and Secure Internet Protocol* (L2TP/IPSec), *Point-to-Point Tunneling Protocol* (PPTP) a *Cisco* IPSec.

Bonjour je protokol, který umožňuje vyhledávání souborů, tiskáren, sdílení hudby a ostatních služeb v síti. Poslouchá dotazy služeb ostatních počítačů a poskytuji jim informace o dostupných službách. Uživatel může rychle zjistit, jaké služby jsou k dispozici v místní síti na ostatních počítačích. Tato výměna informací je vhodná pro zjištění služeb, ale také podstupuje bezpečnostní risk. Bonjour odesílá všem (broadcast) v síti informace o dostupných službách. Bezpečnostní riziko je podstupováno díky potenciálnímu výskytu chyb, které umožňují útočníkům vzdáleně přistoupit k našemu systému. Nicméně Bonjour zmírňuje tato rizika implementací sandboxingu.

Pokud Bonjour vypneme, musíme manuálně nastavovat síťové tiskárny. Také funkčnost dalších aplikací může být ovlivněna. Například odesílání kontaktních informací, fotek a hudby pomocí aplikací, která Bonjour používají, může být omezeno.

2.4.4 Vzdálený přístup

Vzdálený přístup umožňuje uživateli připojení ke svému počítači pomocí *Secure Shell* (SSH). Povolením vzdáleného přístupu aktivujeme také bezpečné verze běžně používaných nástrojů. Defaultně je vzdálený přístup vypnut a zapínat by se měl, pouze pokud bude používán. Přístup může být povolen pouze určitému uživateli. Připojení pomocí SSH nahradilo používání starších protokolů jako: Telnet, slogin nebo scp. SSH podporuje používání hesel, klíčů a Kerberos autentizace. Zabezpečení pomocí klíčů je bezpečnější než zabezpečení pouze pomocí hesel.

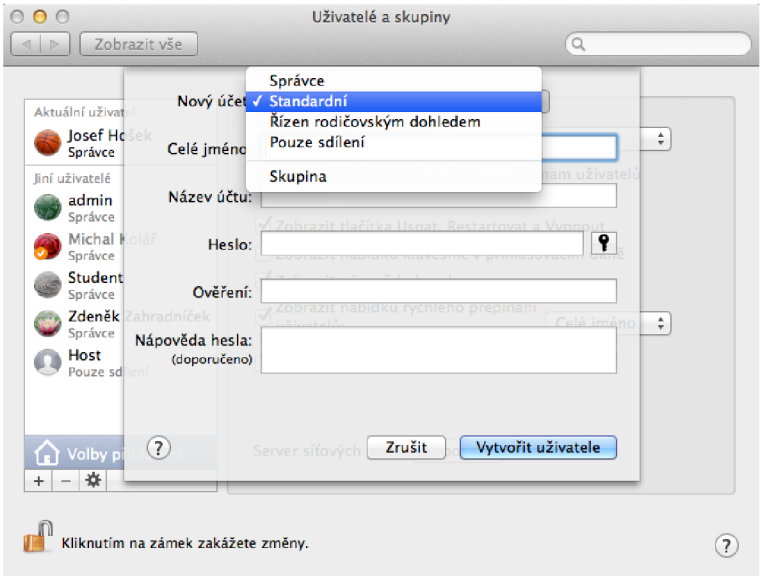
3 PRAKTICKÁ ČÁST PRÁCE

První část je interpretována vytvořením postupů pro konfiguraci určitých bezpečnostních prvků. Postupy jsou vypracovány jak pro Mac OS X, tak i pro Microsoft Windows a to z důvodu srovnání těchto postupů v rámci více platforem. V další části je otestován systém OS X z pohledu vlivu šifrování na jeho rychlost. Jako další je vypracován a popsán komplexní firewall pomocí IPFW. V poslední části je popsán a zprovozněn scénář s přesměrováním a překladem adres pomocí NATD mezi dvěma OS X.

3.1 Návody pro nastavení základních prvků v Mac OS X „Mountain Lion“

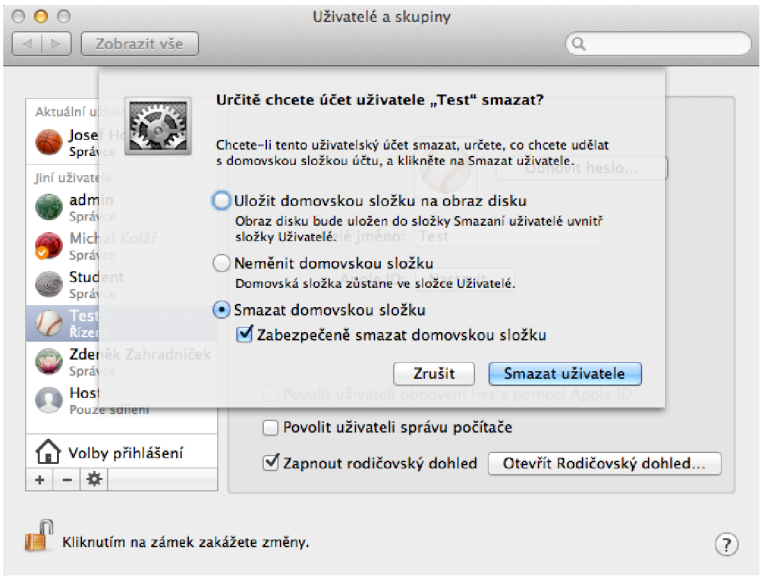
3.1.1 Vytváření a nastavení uživatelských účtů

První věc, kterou je potřeba provést před samotným vytvářením nebo upravováním účtů, je povolení změn tak, že po kliknutí na zámek v levém dolním rohu zadáme administrátorské heslo. Vytváření i úpravy stávajících uživatelských účtů a skupin se provádí v Předvolbách systému/Uživatelé a skupiny. Při vytváření nového účtů můžeme volit z možností, které jsou viditelné na obrázku 3.1. Dále zadáváme jméno uživatele, název účtu, heslo, jeho ověření a případnou nápovědu pro heslo. Pro vytvoření bezpečného hesla můžeme použít průvodce nastavením hesla, který je reprezentován znakem klíče.



Obr. 3.1: Okno vytvoření uživatelského účtu

Rodičovský dohled je možné zapnout i u existujícího účtu a ne jen při vytváření nového účtu. U účtů řízených rodičovským dohledem je možné omezit a nastavit mnoho věcí. Například omezení určitých aplikací nebo webových stránek, omezení doby užívání počítače a také zákaz změny hesla. Každému uživateli můžeme nastavit aplikace, které se budou automaticky zapínat po přihlášení. Při mazání účtu uživatele je možné ponechat jeho domovskou složku beze změny, uložit ji na obraz disku nebo tuto složku bezpečně smazat (viz Obr 3.2).

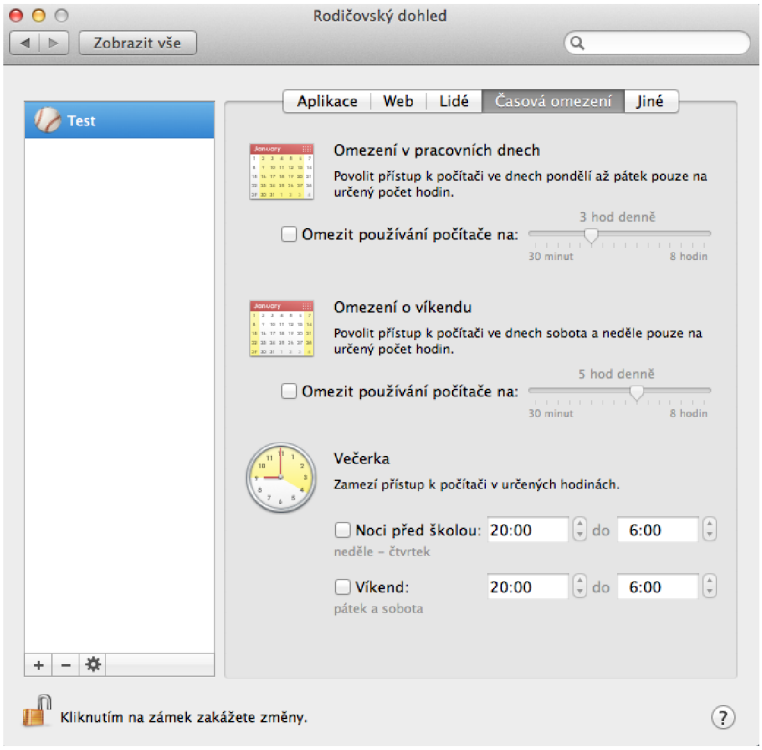


Obr. 3.2: Okno odstranění uživatelského účtu

Postup pro vytvoření účtu se zapnutým Rodičovským dohledem

1. Najedeme do Předvoleb systému a zde v části systém do Uživatelských účtů a skupin.
2. Dále musíme v levém dolním rohu okna povolit změny a to kliknutím na zamčený zámek a následovným zadáním administrátorského hesla. Změny jsou povoleny, pokud je zámek odemčen.
3. Pomocí znaku plus, pod seznamem již existujících účtů, vyvoláme dialog pro vytvoření nového účtu (viz Obr. 3.1). Zde vybereme typ účtu standardní, poté zadáme celé jméno a název účtu. Heslo můžeme zadat vlastní nebo pomocí průvodce nastavením hesla, který je reprezentován klíčem vedle řádku pro zadání hesla. Samozřejmě je žádoucí zadat i nápovědu pro případné zapomenutí hesla.
4. Po vyplnění všech údajů a následovném potvrzení vytvoření uživatele vidíme v seznamu uživatelů i námi vytvořený účet.

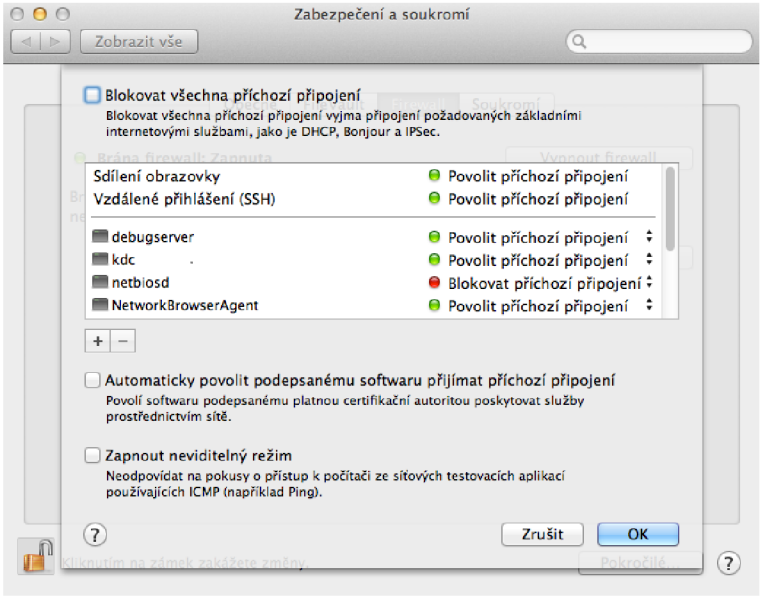
5. Označením našeho účtu se dostaneme k jeho podrobnějšímu nastavení. Zde můžeme nastavit Apple ID a obnovit heslo. Také můžeme tomuto účtu povolit správu počítače a tak z něj udělat účet správce. Hned pod tímto zapneme rodičovskou kontrolu účtu zaškrtnutím checkboxu a hned si otevřeme Rodičovský dohled pomocí tlačítka vedle.
6. V tomto nastavení je v levé části obrazovky viditelné pro které účtu je kontrola aktivní. V pravé části je umístěno pět záložek (viz Obr 3.3), pomocí kterých náš účet omezíme a to například nastavením doby, kdy je možné počítač používat. Toto omezení nastavíme v záložce časová omezení. Další omezení můžeme vybírat pomocí ostatních záložek.



Obr. 3.3: Okno rodičovské kontroly s nastavením časového omezení užívání počítače

3.1.2 Nastavení firewallu

Pokud není odemčena možnost provádění změn, je třeba tuto možnost opět zpřístupnit pomocí administrátorského hesla. Nastavení firewallu najdeme v Předvolbách systému/Zabezpečení a soukromí/záložka Firewall. Zde je možné firewall zapínat a vypínat. Pokud je zapnut, můžeme se dostat do „Voleb firewallu“, kde dále specifikujeme, jak bude firewall fungovat. Je možné blokovat všechna připojení, povolit příjem příchozích připojení podepsanému softwaru či zapnout neviditelný režim (viz Obr. 3.4).

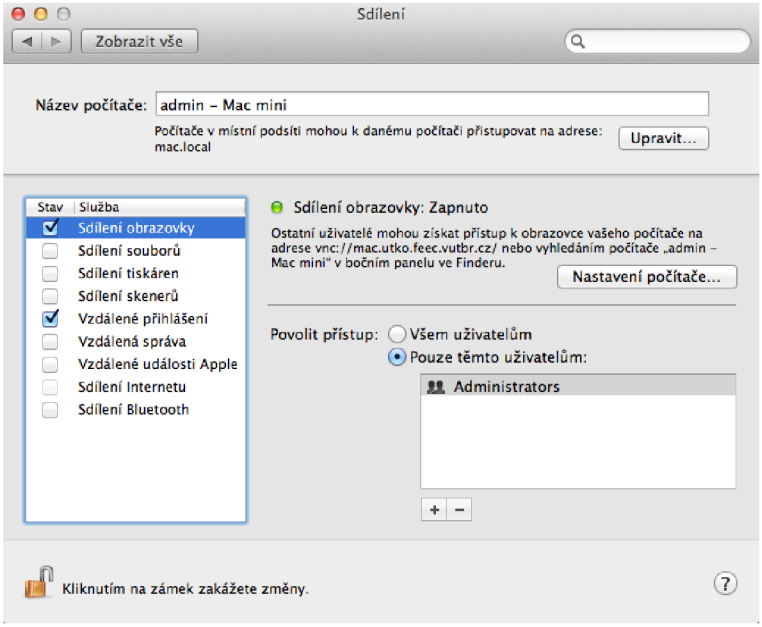


Obr. 3.4: Volby nastavení firewallu

V tabulce výjimek je možné povolit nebo blokovat určitá připojení. Samozřejmě je možné různá připojení do tohoto seznamu přidávat, ale i stávající odebírat, a to pomocí dvou tlačítek pod tímto seznamem. První dva řádky tohoto seznamu není možné měnit v tomto menu, ale je potřeba přejít zpět do Předvoleb systému a poté do menu sdílení (Obr. 3.5). Zde měníme sdílení různých periferií i vzdálené přihlášení. Pokud zde jednu z položek povolíme, systém sám přidá výjimku do seznamu firewallu, aby mohlo ke sdílení dojít.

Postup zapnutí firewall a správa jeho seznamu výjimek

1. Firewall najdeme v Předvolbách systému, část okna Osobní, kde vybereme Zabezpečení a soukromí a v horní části nového okna označíme Firewall.
2. Dále musíme v levém dolním rohu okna povolit změny a to kliknutím na zamčený zámek a následovným zadáním administrátorského hesla. Změny jsou povoleny, pokud je zámek odemčen.
3. Teď klikneme na tlačítko Zapnout firewall a hned vidíme, že se dialog nalevo od tlačítka změnil na Brána firewall: Zapnuta.
4. Další nastavení budeme provádět po otevření okna pomocí tlačítka Volby firewallu (Obr. 3.4). Pokud nebudeme chtít blokovat veškerá připojení, až na základní internetové služby, ponecháme první zaškrtávací políčko prázdné. Dále můžeme spravovat následující seznam aplikací, pomocí kterého povolíme či zakážeme přístup určité aplikace. Pokud potřebujeme omezit aplikaci, která není v seznamu zobrazena, vybereme plus pod tímto seznamem a v následují-



Obr. 3.5: Okno nastavení sdílení

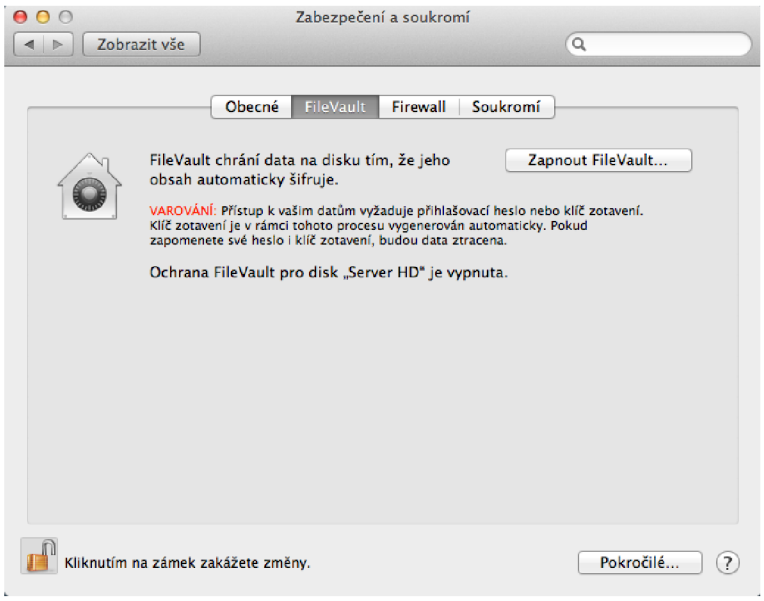
cím okně najdeme a označíme námi požadovanou aplikaci a potvrdíme výběr.

5. Další volby v okně jsou zaškrtávací políčka pro zapnutí neviditelného režimu a automatického povolení podepsanému softwaru.
6. Pokud bychom potřebovali povolit nebo zakázat přístup z určitého portu, musíme použít terminál a ipfw2 firewall.
7. Terminál najdeme ve složce utility, která je umístěna mezi aplikacemi. Po jeho spuštění můžeme psát příkazy, pomocí kterých povolíme nebo zakážeme komunikaci skrze námi definované porty. Příkaz pro povolení komunikace skrze port 5060 (což je port pro protokol SIP, který je užívaný například aplikací iChat) může vypadat takto:
   `sudo ipfw add 15000 allow udp from any to any dst-port 5060`.

3.1.3 Šifrování disku pomocí FileVault

Samozřejmě i pro změny v nastavení FileVault je potřeba mít odemčenou možnost změn. Tyto nastavení najdeme v Předvolbách systému/Zabezpečení a soukromí/záložka FileVault (Obr. 3.6). Zde můžeme FileVault zapnout, poté se objeví klíč zotavení, kterým je možné odemknout zašifrovaný disk i když ztratíme přístup k účtu. V dalším kroku si můžeme kopii tohoto klíče zálohovat na sever Applu, pro případ, že bychom klíč ztratili. Pokud tuto možnost využijeme, je nutné definovat tři otázky, pomocí kterých je tento klíč možné získat.

V dalším kroku jsme vyzváni k restartu počítače. Po restartu a přihlášení započne



Obr. 3.6: Záložka pro nastavení FileVaultu

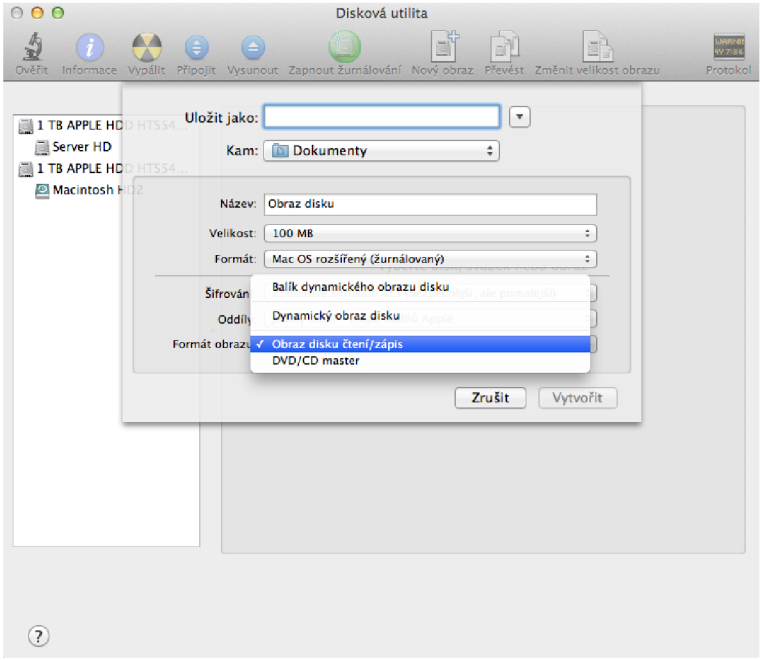
šifrování celého disku.

3.1.4 Zašifrování jednotlivých složek a souborů

Toto je možné provést pomocí Diskové utility, kterou najdeme mezi aplikacemi ve složce utility. Zde zvolíme „Nový obraz“ v horní části obrazovky. Poté co potvrdíme náš výběr, jsme dotázáni na umístění nového obrazu, jeho název, velikost, formát, šifrování, oddíly a formát obrazu (viz Obr. 3.7).

Formát je možné zvolit i kompatibilní s Windows. Výběr šifrování mezi 128bit AES a 256 AES volíme podle potřeb. Formát obrazu je možné ponechat, nebo změnit na Dynamický obraz disku, což znamená, že obraz bude na disku zabírat právě tolik prostoru, kolik je v tomto obrazu uloženo dat. A to nezávisle na velikosti, kterou volíme při vytváření obrazu.

Po nastavení všech parametrů obrazu můžeme potvrdit jeho vytvoření a pokud jsme zvolili některý typ šifrování, budeme vyzváni k zadání hesla k tomuto obrazu. Toto heslo si můžeme uložit do klíčenky. Po vytvoření obrazu jej můžeme vidět v levém sloupci diskové utility. A zde tento obraz můžeme otevřít pomocí hesla, které jsme definovali při vytváření obrazu. Posléze se zobrazí oddíl tohoto obrazu, pokud tento oddíl otevřeme, můžeme do něj přetažením umístit jakékoli soubory a složky, které chceme mít v tomto obrazu zašifrované.



Obr. 3.7: Dialog pro vytvoření nového obrazu

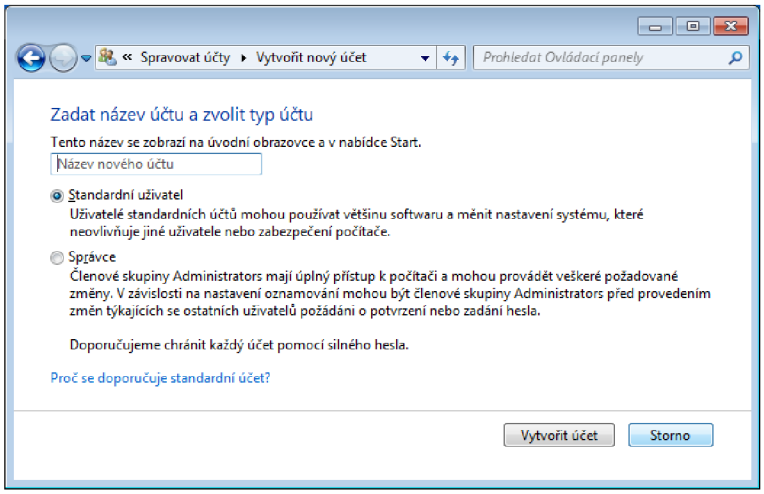
Postup pro individuální zašifrování dokumentů

1. Ve Finderu si najedeme do všech aplikací a poté do složky Utility, kde najdeme Diskovou utilitu.
2. Po spuštění tohoto nástroje vidíme okno, kde vybereme v horní části položku Nový obraz a při tomto výběru nesmíme mít v seznamu obrazů nic vybráno.
3. V dialogu pro nový obraz (Obr. 3.7) vybereme kam a pod jakým názvem chceme náš obraz uložit. Pokud nevíme přesně kolik dat budeme šifrovat, zvolíme velikost obrazu raději větší. Formát a Oddíl ponecháme na nastavené předvolbě a zvolíme 256bitové AES šifrování. Formát obrazu změníme na dynamický obraz disku.
4. Po nastavení všech parametrů obrazu potvrdíme jeho vytvoření a poté vyplníme dialog, který se nás dotazuje na heslo k obrazu a jeho ověření. Samozřejmě můžeme k vytvoření hesla použít Průvodce nastavením hesla.
5. Teď vidíme v seznamu obrazů v levé části okna i námi vytvořený obraz. Obraz je již připojen a tak nemusíme pro jeho otevření zadávat heslo, které jsme definovali v předchozím kroku.
6. Následně si tento obraz otevřeme pomocí pravého tlačítka, nebo si ho vyhledáme pomocí Finderu a do otevřeného okna vložíme přetažením dokumenty určené k zašifrování.
7. Poté obraz zavřeme a vysuneme, aby při dalším otevření bylo třeba zadat heslo.

3.2 Návody pro nastavení základnách prvků ve Microsoft Windows 7

3.2.1 Vytvoření a nastavení uživatelských účtů

Veškeré úpravy v rámci uživatelských účtů můžeme provádět v Ovládacích panelech/Uživatelské účty. Při vytváření nového uživatelského účtu máme k dispozici dva typy, a to Standardní uživatel a Správce (viz Obr. 3.8). Rozdíl mezi těmito dvěma typy je zřejmý. Pro vytvoření účtu stačí zadat název účtu, protože další parametry účtu, jako heslo nebo nastavení rodičovské kontroly, nastavujeme až po jeho vytvoření.



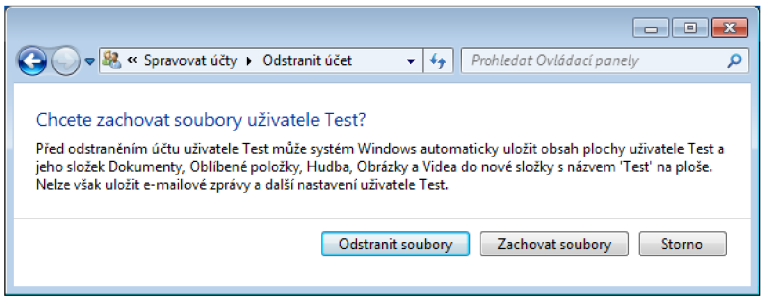
Obr. 3.8: Okno pro vytvoření nového uživatelského účtu

Hned po vytvoření jakéhokoliv účtu je nutné definovat přístupové heslo a pro standardní účet také nastavit rodičovskou kontrolu. Pomocí rodičovské kontroly je možné určit časové limity pro používání počítače, nastavení her a povolení či blokování určitých programů. Při konfiguraci účtů je možné nastavit i upozornění na změny v počítači, které je defaultně nastaveno tak, aby upozorňovalo na všechny změny, jaké se program pokouší provést. A samozřejmě je k povolení určitých akcí potřeba administrátorského hesla.

Při odstranění účtů jsme dotázáni, zda chceme zachovat dokumenty a obsah plochy uživatele nebo tyto data smazat (viz Obr. 3.9). Pokud soubory zachováme, budou uloženy do složky s názvem účtu na naši plochu.

Postup vytvoření standardního účtu s aktivovanou rodičovskou kontrolou

1. Otevřeme okno uživatelských účtů, které najdeme v Ovládacích panelech.



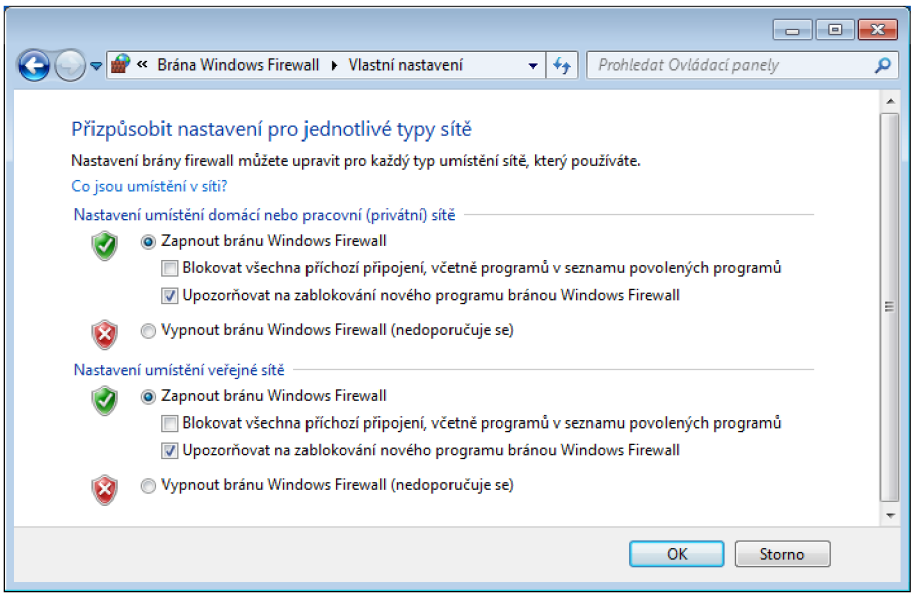
Obr. 3.9: Okno pro odstranění uživatelského účtu

2. Poté zvolíme možnost spravovat jiný účet, kde v novém okně pod nabídkou účtů najdeme možnost Vytvořit nový účet.
3. Zadáme jméno účtu a ponecháme volbu Standardního uživatele (Obr. 3.8).
4. Po potvrzení vytvoření účtu uvidíme námi vytvořený účet v seznamu účtů a pokud na tento účet klikneme, dostaneme se do jeho nastavení. Zde zvolíme možnost vytvořit heslo, zadáme heslo, jeho potvrzení, také nápovědu pro heslo a potvrdíme vytvoření hesla.
5. Zpět v nastavení námi vytvořeného účtu zvolíme možnost nastavit rodičovskou kontrolu. A v okně rodičovské kontroly vybereme náš účet a následně zvolíme možnost „Zapnuto, vynutit aktuální nastavení“.
6. Následně můžeme nastavit časové intervaly, kdy budeme moci účet používat. Toto nastavení provádíme pomocí tabulky všech dnů týdne a postupným označováním vybraných časů každého dne, kdy chceme povolit používání.

3.2.2 Nastavení Windows Firewallu

Tyto nastavení se provádí v Ovládacích panelech/Brána Windows Firewall. V tomto okně můžeme vidět základní nastavení firewallu a to pro režim domácí nebo veřejné sítě. Pro jakoukoli základní změnu stačí v levém sloupci vybrat možnost Zapnout nebo vypnout bránu Windows Firewall. Zde je možné zapnout či vypnout firewall pro oba režimy, zapnout blokování veškerých příchozích připojení a to včetně seznamu povolených programů nebo upozornění na zablokování nového programu firewallem (viz Obr. 3.10). Povolení programům komunikovat skrz firewall můžeme definovat v nastavení Povolené programy, které též vybereme v levém sloupci okna.

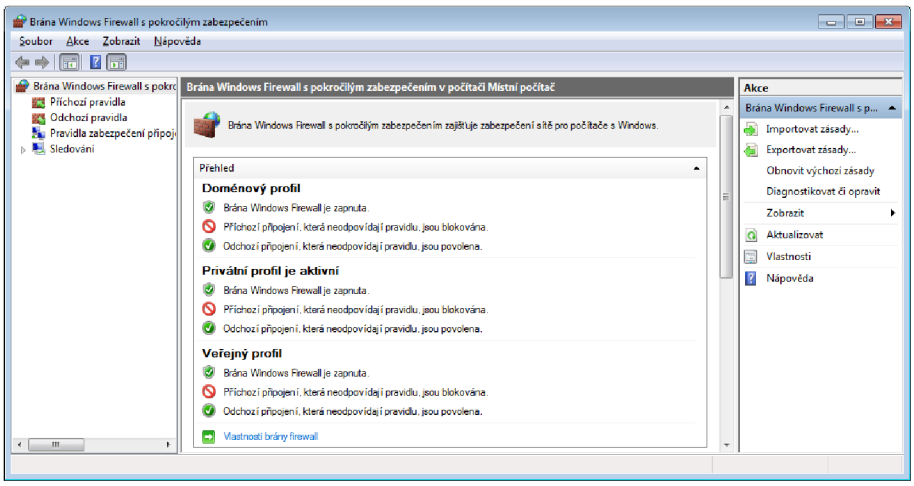
Pokud bychom chtěli provést pokročilé nastavení firewallu, musíme v levém sloupci vybrat Upřesnit nastavení. Otevře se nám nástroj s názvem Brána Windows Firewall s pokročilým nastavením . Zde můžeme vidět i definovat příchozí i odchozí pravidla, pravidla zabezpečení připojení a sledování (viz Obr. 3.11).



Obr. 3.10: Okno pro nastavení firewallu

Postup zapnutí firewallu a jeho následné nastavení

1. K nastavení firewallu se dostaneme opět pomocí Ovládacích panelů a položky Brána Windows Firewall.
2. Zde zvolíme možnost v levé části okna Zapnout nebo vypnout bránu Windows Firewall.
3. V tomto okně (Obr. 3.10) zapneme firewall pro oba typy umístění sítě a také u obou zaškrtneme políčka u „upozornění při zablokování nových programů“.
4. Po nastavení v předchozím kroku a jeho následném potvrzení se vrátíme zpět do základního okna firewallu.
5. Dále zvolíme možnost „povolit programu nebo funkci průchod bránou firewall“ v levé části okna. Zde můžeme provádět individuální nastavení pro všechny programy v rámci obou síťových umístění. Pokud hledaný program není v seznamu, zvolíme možnost pod tímto seznamem „Povolit jiný program a vybereme požadovaný program“.
6. Po potvrzení předchozího kroku se dostaneme zpět do základního okna, kde vybereme možnost „upřesnit nastavení“ v levé části obrazovky.
7. V nově otevřeném okně pokročilého nastavení firewallu (Obr. 3.11) vytvoříme nové pravidlo pro odchozí spojení. A před vytvořením nového pravidla vyzkoušíme `ping www.vutbr.cz` v příkazovém řádku. Tento příkaz by měl momentálně fungovat.
8. Poté pravým tlačítkem klikneme na odchozí spojení a vybereme Nové pravidlo. V průvodci nastavením zvolíme vlastní pravidlo.



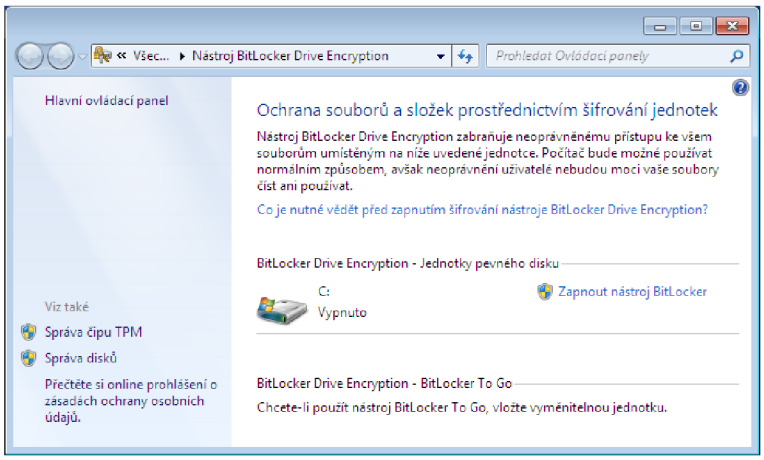
Obr. 3.11: Okno pokročilého nastavení firewallu

9. V dalším kroku ponecháme nastavené všechny programy. A v příštím kroku vybereme protokol ICMPv4 a v dalších krocích už jen ponecháme nastavení pro všechny IP a blokování připojení. Jako poslední zadáme název našeho nového pravidla.
10. Po vytvoření našeho pravidla, ho můžeme najít v seznamu odchozích pravidel a případně toto pravidlo zakázat nebo ponechat povolené.
11. Nyní otestujeme správnou funkci vytvořeného pravidla. A to zapnutím příkazového řádky a opět použitím příkazu `ping www.vutbr.cz`. Pokud je po potvrzení vypsána hláška „obecná chyba“, je pravidlo nastaveno správně a z našeho počítače není možné použít `ping`. Obdobné pravidlo je možné vytvořit pro příchozí spojení.

3.2.3 Šifrování disku pomocí BitLocker

Pro šifrování celého disku ve Windows existuje nástroj BitLocker, který je obsažen pouze v edicích Ultimate a Enterprise u Windows 7 a ve Windows 8 již od verze Professional a výše. Tento nástroj najdeme pomocí vyhledávače, poté můžeme zapnout šifrování kteréhokoli disku (viz Obr. 3.12). Po ověření zda k šifrování může dojít, nám nástroj oznámí, že zašifruje disk a zároveň aktivuje TPM (Trusted Platform Module), který je použit k ochraně klíče šifrování. V dalším kroku bude počítač restartován poté, co odpojíme veškeré připojené periferie.

Tento nástroj je aktivován administrátorem a je aktivní pro celý počítač tzn. pro všechny uživatelské účty.



Obr. 3.12: Okno pro nastavení nástroje BitLocker

3.2.4 Šifrování složek a souborů pomocí EFS

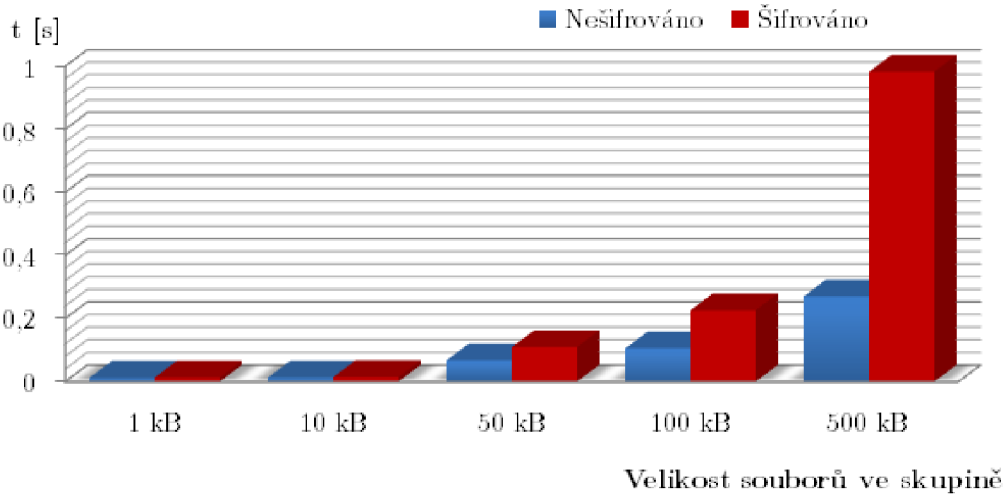
K šifrování samostatných složek a souborů je možné použít EFS (Encrypting File System), který je obsažen od verze Windows 7 Professional výše. Tímto systémem nelze nahradit BitLocker, protože EFS nemůže šifrovat boot operačního systému. K nastavení šifrování složky nebo souboru musíme pomocí pravého tlačítka vybrat Vlastnosti a poté Upřesnit v dolní části okna. V následujícím okně zaškrtneme možnost „Šifrovat obsah a tak zabezpečit data“. Pokud jsme toto zvolili pro soubor, budeme po potvrzení dotázáni, zda chceme šifrovat pouze soubor nebo i jeho nadřazenou složku. Oproti tomu při šifrování složek jsme dotázání, zda chceme šifrovat pouze složku nebo i její podsložky a soubory.

Tento nástroj může používat každý uživatel nezávisle na ostatních a tak si šifrovat své osobní data.

3.3 Testování Mac OS X „Mountain Lion“ a komplexní práce s ním

3.3.1 Měření časů kopírování souborů mezi nešifrovanými a šifrovanými složkami

Prováděl jsem měření reálných časů kopírování souborů v OS X pro kopírování mezi nešifrovanými složkami a pro kopírování ze složky do zašifrovaného kontejneru (obraz disku s 256bitovým AES šifrováním) vytvořeného pomocí diskové utility a to na školním serveru Mac OS X pomocí vzdáleného přístupu. Cílem měření bylo zjistit, jaký je rozdíl mezi časy kopírování a tak určit zda je výhodné využívat šifrování v rámci běžné práce se systémem. Měření jsem prováděl vždy pro skupinu 100 souborů, které měly stejnou velikost. Těchto skupin jsem proměřil celkem deset. Postupně jsem zvyšoval velikost použitých souborů. Použité soubory jsem generoval pomocí programu tak, aby měly všechny přesně požadovanou velikost a také byl každý unikátní.



Obr. 3.13: Graf závislosti velikosti souborů na čase kopírování - první část

Každou skupinu jsem kopíroval vždy minimálně pětkrát z důvodu reálnějších časových výsledků, které získám díky zprůměrování časů více měření téhož. Pro tento úkon jsem použil určité příkazy terminálu (např. `cp`, `time`) a ty jsem pro jednoduchost uložil do skriptu, který vždy požadovaný postup měření provedl pětkrát souvisle po sobě. Po doměření jsem tento skript spustil několikrát po sobě, abych se opravdu ujistil o změřených hodnotách.

V následujících tabulkách 3.1 a 3.2 jsou uvedeny maximální a minimální hodnoty času kopírování pro všechny skupiny, spolu s průměrnou hodnotou a směrodatnou

odchylkou pro každou skupinu. Dále jsou v grafech 3.13 a 3.13 zobrazeny závislosti velikosti souborů na průměrném čase za jaký byly zkopírovány a to pro oba typy měřeného kopírování. Tabulky a grafy jsou vypracovány zvlášť pro polovinu skupin s menší velikostí souborů a zvlášť pro druhou polovinu skupin s větší velikostí souborů, a to z důvodu lepší přehlednosti a směrodatnosti jak tabulek, tak hlavně grafů.

Tab. 3.1: Časy kopírování souborů

Velikost souborů	*t[s]*	**Nešifrované kopírování**	**Šifrované kopírování**
1 kB	max	0,014	0,016
	min	0,011	0,011
	ø	0,012	0,013
	σ	0,0011	0,0022
10 kB	max	0,016	0,016
	min	0,012	0,012
	ø	0,0132	0,0142
	σ	0,0016	0,0015
50 kB	max	0,123	0,207
	min	0,02	0,052
	ø	0,0678	0,11
	σ	0,049	0,0631
100 kB	max	0,202	0,642
	min	0,063	0,02
	ø	0,105	0,226
	σ	0,0558	0,26
500 kB	max	0,687	2,12
	min	0,152	0,113
	ø	0,271	0,983
	σ	0,233	0,337

U prvních pěti měřených skupin jsou zpočátku časové rozdíly mezi oběma druhy kopírování minimální. S postupným zvětšováním souborů ve skupinách ale rozdíl v časech kopírování narůstá. Z grafu 3.13 je viditelné, že kopírování mezi nešifrovanými složkami je při nejmenších velikostech souborů dokonce časově skoro stejně náročné jako kopírování do šifrovaného kontejneru. Samozřejmě u takto malých souborů jsou časy daleko menší než sekunda a tak jsou rozdíly opravdu minimální. A je zde samozřejmě i možnost chyby měření díky práci na vzdáleném serveru, na kterém pracuje více studentů současně.

Tab. 3.2: Časy kopírování souborů

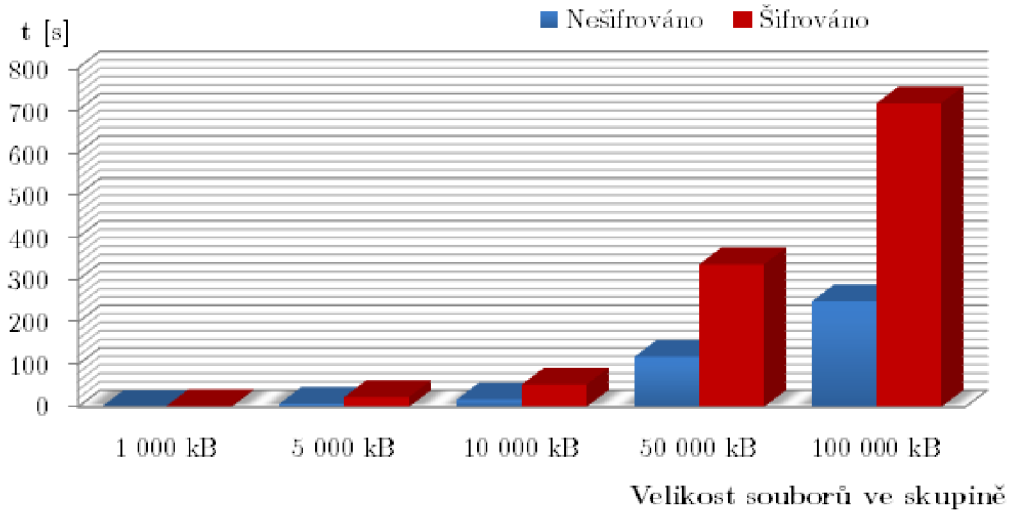
Velikost souborů	*t[s]*	**Nešifrované kopírování**	**Šifrované kopírování**
1 000 kB	max	1,04	4,069
	min	0,59	0,461
	ø	0,84	2,639
	σ	0,2053	1,445
5 000 kB	max	11,261	25,754
	min	6,129	21,558
	ø	7,439	23,314
	σ	2,162	1,667
10 000 kB	max	24,584	53,837
	min	15,286	51,254
	ø	17,814	52,734
	σ	3,971	1,199
50 000 kB	max	122,54	338,06
	min	110,36	333,16
	ø	118,28	336,19
	σ	4,786	1,964
100 000 kB	max	257,98	736,59
	min	236,36	701,77
	ø	249,33	717,06
	σ	8,02	12,73

Ve druhé části, kde měřené skupiny obsahují soubory o větší velikosti, je z tabulky 3.2 viditelné, že kopírování do šifrovaného kontejneru je ve všech případech časově náročnější. Po zhlédnutí výsledného grafu 3.14 můžeme říci, že šifrované kopírování trvá zhruba třikrát déle než kopírování nešifrované. Rozdíl průměrných hodnot měření je poměrově stálý a se zvětšující se velikostí souboru se nemění.

Na závěr můžeme říci, že výsledky měření dopadly podle očekávání. V první části měření se z počátku rozdíly mezi kopírováními skoro nelišily, ale se zvětšující se velikostí souborů už rozdíl mezi oběma měřeními narůstal podle očekávání. Při opakovaném měření téhož, některé výsledné časy poměrně vybočovaly oproti ostatním hodnotám, ale to je dané opravdu malými výslednými časy a možnými chybami měření z důvodu práce na vzdáleném serveru.

Naproti tomu ve druhé části měření se očekávaný výsledek projevil již při prvním měření. Rozdíl mezi oběma kopírováními byl tím pádem značný. Tento rozdíl nenarůstal se zvětšující se velikostí souborů, ale pohyboval se v rozmezí 2,8 a 3,1

násobku. Z těchto výsledků můžeme usoudit, že pokud nebudeme kopírovat opravdu velké soubory, tak nás šifrování souborů nebude zásadně časově omezovat i když je šifrované kopírování časově náročnější. A pro uchování a přenos osobních a citlivých souborů je zcela jistě vhodné šifrování využívat.



Obr. 3.14: Graf závislosti velikosti souborů na čase kopírování - druhá část

3.3.2 Měření časů spuštění systému a vybraných aplikací při nešifrovaném a šifrovaném běhu systému

Cílem tohoto měření bylo zjistit jak moc ovlivňuje šifrování celého systému OS X jeho rychlost v rámci uživatelského používání. Šifrování se provádělo pomocí funkce FileVault, která toto provádí v reálném čase. Měření jsem opět prováděl na školním serveru pomocí vzdáleného přístupu na něj. Na serveru jsem si nainstaloval VMware Fusion 5, což je nástroj pro virtualizaci v Mac OS X. Je v něm možné virtuálně spouštět jak OS X, tak Windows nebo Linux. Pracoval jsem na virtuálním stroji z důvodu větší objektivnosti měření, díky nově nainstalovanému systému, na kterém nebyl připojený žádný další uživatel, a tak jsem mohl kontrolovat všechny spuštěné programy a také je dobře regulovat vzhledem k mým potřebám.

Všechna měření jsem provedl minimálně v 10ti opakováních, abych dosáhl co nejobjektivnějších výsledků. Pro měření jsem zvolil několik základních a běžně používaných aplikací spolu se zapínáním a vypínáním samotného systému Mac OS X. Počítal jsem, že běžně k počítači přistupuje více uživatelů a tak jsem měřil čas od zapnutí systému po načtení přihlašovací obrazovky a od zadání hesla po kompletní načtení uživatelské plochy a docku. A samozřejmě také v opačném pořadí kdy se uživatel odhlašuje a poté případně vypíná celý systém.

Tab. 3.3: Časy startování/vypínání systému a přihlašování/odhlašování uživatele

Úkon	*t[s]*	**Vypnutý FileVault**	**Zapnutý FileVault**
Zapnutí do přihlašovací obrazovky	ø	31,19	7,71
	σ	2,11	1,33
Příhlášení	ø	5,32	27,54
	σ	0,46	2,14
Odhlášení	ø	2,62	3,45
	σ	0,23	0,29
Vypnutí	ø	22,77	21,7
	σ	1,31	1,67

U každého měření jsem si zvolil pevný bod, který jsem pří načítání ať už systému nebo jednotlivých aplikací sledoval a tím jsem určil přesný bod úplného načtení a tím i ukončení mého měření. Měření jsem prováděl tímto manuálním způsobem, abych mohl určit reálný bod úplného načtení z pohledu uživatele. To znamená bod po kterém, je například v prohlížeči kompletně načtená internetová stránka nebo je přihlašovací obrazovka systému zcela načtena a je možné zvolit uživatelský účet a zadat heslo.

Tab. 3.4: Časy startování běžně používaných aplikací

Aplikace	*t[s]*	**Vypnutý FileVault**	**Zapnutý FileVault**
Mail	ø	1,95	2,4
	σ	0,37	0,39
Safari	ø	2,35	2,45
	σ	0,29	0,46
iTunes	ø	1,76	2
	σ	0,0,26	0,13
AppStore	ø	5,55	5,48
	σ	1,07	0,88
Zprávy	ø	2,09	2,02
	σ	0,26	0,2
Disková utilita	ø	1,96	1,75
	σ	0,33	0,13

Samotné výsledky jsem rozdělil do dvou tabulek, kde v první tabulce (3.3) jsou uvedeny časy zapnutí systému a přihlášení uživatele a naopak také odhlášení uživatele a následovné vypnutí sytému. Ve druhé tabulce (3.4) jsou uvedeny časy

pro spouštění jednotlivých aplikací. U všech měření jsem uvedl průměrnou hodnotu a směrodatnou odchylku časů.

Po zhodnocení výsledků v první tabulce (3.3) můžeme říci, že hodnoty při vypnutém FileVaultu se dosti liší oproti hodnotám, kdy je FileVault zapnutý. Samotné zapnutí systému je v prvním případě časově náročnější, ale přihlášení uživatele je oproti tomu rychlejší než u šifrovaného systému. Z tohoto lze usoudit, že pokud je systém šifrovaný, načtení přihlašovací obrazovky po startu systému je rychlé, ale následovné přihlašování trvá déle. Takže systém provádí více úkonů až po autentizaci uživatele, naproti tomu při nešifrovaném systému, se tyto úkony provádějí již při startu systému a načítání přihlašovací obrazovky. Díky výsledným časům měření vidíme, že pokud sečteme čas zapnutí systému a přihlášení uživatele u obou typů měření a tyto časy následně porovnáme. Tak výsledné hodnoty se budou v obou případech pohybovat kolem 35 sekund. Při odhlašování uživatele a následném vypínání systému už nejsou znatelné rozdíly mezi šifrovaným a nešifrovaným systémem. Rozdíly v časech těchto postupů jsou minimální.

Z druhé tabulky (3.4), ve které jsou uvedeny časy spouštění základních aplikací jako jsou Mail, Safari, iTunes a další, můžeme říci, že hodnoty při nešifrovaném systému se nijak zásadně neliší oproti hodnotám v systému šifrovaném. Samozřejmě jsou zde mírné rozdíly, ale ty se pohybují maximálně v rozmezí půl sekundy a proto jsou pro běžného uživatele nepostřehnutelné.

FileVault je tedy užitečný bezpečnostní prvek systému OS X, který mírně ovlivňuje start systému a následovné přihlašování, kdy jde poznat zda je zapnutý. Ale při další práci v systému tento prvek pracuje na pozadí a běžného uživatele nijak neovlivňuje.

3.3.3 Nastavení komplexního firewallu pomocí IPFW

Samotnou práci jsem opět prováděl na virtuálním stroji umístěném na školním serveru a to z důvodu neomezování práce ostatních studentů při mém nastavování pravidel firewallu a s tím spojeného omezování síťového provozu.

Přehled základních příkazů pro práci s IPFW [11]

Základní příkaz, je samozřejmě příkaz pro přidání pravidla do seznamu firewallu:

`sudo ipfw add NUMBER SPECIFIKACE_PRAVIDLA`.

Pro případné mazání jednotlivých pravidel v našem seznamu lze jednoduše použít příkaz

`sudo ipfw -q delete NUMBER`,

nebo pro zobrazení jednotlivých pravidel

`sudo ipfw show NUMBER`.

Samozřejmě nemusíme znát přesné označení námi chtěného pravidla a tak využijeme příkaz pro zobrazení všech aplikovaných pravidel v seznamu:

`sudo ipfw list`.

Pomocí toho příkazu je možné zobrazit také například veškerá dynamická pravidla a to jak používaná, tak nepoužívaná. Je třeba přidat pouze parametr k předchozímu příkazu:

`sudo ipfw -d -e list`.

A pokud bychom chtěli smazat veškerá pravidla v námi vytvořeném seznamu, je třeba použít příkaz

`sudo ipfw -f flush`.

V systému jsem jako první vypnul aplikační firewall pomocí grafického rozhraní. Poté jsem otestoval funkčnost mnou požadovaných služeb, jako SSH, ping, apache, telnet, vzdálenou správu a samozřejmě přístup na internetové stránky pomocí prohlížeče Safari. Po tomto kroku jsem zjistil jaká pravidla jsou aktuálně obsažena v seznamu firewallu IPFW. A to pomocí příkazu:

`sudo ipfw list`,

u kterého je možné vidět, že při provádění jakéhokoliv příkazu spojeného s IPFW je třeba použít administrátorských práv pomocí `sudo`. Zjistil jsem, že v seznamu je použito pouze deufaltní pravidlo, které je vždy obsaženo a má za úkol vše povolit a také je neměnné. Takže pokud uživatel nepoužívá IPFW firewall, ale pouze aplikační firewall ovládaný z grafického prostředí, není možné, aby IPFW firewall jakýmkoliv způsobem omezoval síťový provoz. Toto deufalní pravidlo má tvar:

`65535 allow ip from any to any`.

Kde číslo na začátku určuje pořadí v seznamu pravidel, toto defaultní pravidlo je v tomto seznamu na úplně posledním místě. S tím, že firewall funguje tak, že porovnává veškerý provoz se seznamem pravidel tím způsobem, že začne od pravidla číslo 1 a jde postupně až k poslednímu pravidlu, které má hodnotu právě 65 535 a je to zmíněné defaultní pravidlo. Pokud dojde při porovnávání ke shodě, kde pravidlo definuje právě tento určitý druh provozu, je provedeno, to co pravidlo definuje a dále se neporovnává. Proto pokud nedojde ke shodě, je vše automaticky povoleno díky poslednímu pravidlu.

Pro vytvoření komplexního firewallu, který bude filtrovat opravdu veškerý provoz a povolí jen námi požadované, je třeba použít logiku obrácenou, tzn. defaultním pravidlem zakážeme veškerý síťový provoz. Poté postupně pomocí jednotlivých pravidel povolujeme jen námi požadované služby. Tímto způsobem získáme mnohem lepší kontrolu nad firewallem a celkovým síťovým provozem v našem systému. Naše pravidlo, které vše zakáže, vložíme před defaultní pravidlo a tak můžeme zvolit číslo například 10 000 a stále nám zůstane dostatečné množství prostoru pro další pravidla před tímto umístěním.

`sudo ipfw add 10000 deny log logamount 500 all from any to any`.

Tento příkaz jednoduše přidá do seznamu pravidlo, které odepře přístup veškerému příchozímu i odchozímu provozu a zároveň je zadán parametr `log`, který po zamítnutí jakéhokoli provozu vytvoří záznam o této činnosti do souboru *system.log* umístěného ve složce */var/log/*. K tomuto příkazu přísluší i parametr `logamount`, který upřesňuje maximální délku záznamu jaký je možné zaznamenat do *system.log*.

Nyní je možné začít vkládat pravidla pro povolení jednotlivých služeb a funkcí, které potřebujeme. Jako první vytvoříme pravidlo pro *localhost*, který je možné využít v případě potřeby otestování například apache.

`sudo ipfw add 100 allow all from any to any via lo0`

Začneme postupně od přidání pravidla pro fungování `pingu`. Toto lze povolit obecně tak, že povolíme veškeré ICMP pakety, ale pro naše potřeby zprovoznění jen `pingu`, nám bude stačit povolit jen určité typy ICMP paketů, které jsou potřeba pro jeho funkci.

`sudo ipfw add 300 allow log icmp from any to any icmptype 0,8 out...`

`...via en0 keep-state`

Tímto příkazem tedy přidáme pravidlo, které povolí ICMP pakety typu 0 (*echo reply*) a 8 (*echo request*) pouze v odchozím směru, tzn. `ping` na náš počítač stále nebude funkční. V příkazu je pravidlo definováno pouze pro jedno síťové rozhraní en0, což je pro nás Ethernet. A příkaz `keep-state` vytváří pravidlo v dynamické tabulce, díky kterému je možné přijímat odpověď na odchozí `ping` z jakékoliv adresy a portu. Tento parametr je spojený s dalším parametrem `check-state`, který si přidáme a vysvětlíme později.

Další povolovanou funkcí je SSH, která pracuje na port 22 a proto je třeba otevřít právě tento port. Chceme, abychom SSH mohli využívat, jak z našeho počítače, tak odněkud přistupovat zpět na náš počítač, proto povolíme provoz v obou směrech.

`sudo ipfw add 400 allow tcp from any to any dst-port 22 out...`

```
...keep-state setup

sudo ipfw add 410 allow tcp from any to me dst-port 22 in...

...keep-state setup
```

U obou pravidel je opět povoleno vytváření dynamické tabulky a také parametr `setup`, který identifikuje start relace při žádosti o určité TCP pakety. Následně povolíme i příchozí připojení pomocí telnetu, které bude mít podobný tvar jako pravidlo pro SSH, až na jiné číslo portu. A také povolíme jen příchozí pakety z důvodu možného přístupu pouze ve směru k nám.

```
sudo ipfw add 420 allow tcp from any to me dst-port 23 in...

...keep-state setup
```

Následujícími pravidly povolíme vzdálený přístup a tím i vzdálené ovládání plochy. Jako první musíme povolit ARD, což je *Apple Remote Desktop Protocol*, který pracuje na portu 3283.

```
sudo ipfw add 430 allow udp from any to me 3283 in via en0...

...keep-state

sudo ipfw add 431 allow udp from any to any 3283 out via en0...

...keep-state
```

A pro úplnou funkci musíme povolit také Apple VNC, které pracuje na portu 5900.

```
sudo ipfw add 440 allow tcp from any to me 5900 in via en0...

...keep-state setup
```

Po povolení všech těchto funkcí a vzdáleného přístupu ve sdílení v nastavení systému můžeme bez omezení vzdáleně ovládat náš počítač. Další velmi důležitá součást běžné práce na počítači je prohlížení internetových stránek pomocí prohlížeče. Proto musíme povolit protokoly HTTP (port 80) a HTTPS (port 443).

```
sudo ipfw add 500 allow tcp from any to any 80 out via en0...

...keep-state setup

sudo ipfw add 510 allow tcp from any to any 443 out via en0...

...keep-state setup
```

Nyní je možné načíst internetové stránky, ale ještě nebude fungovat překlad doménových jmen pomocí DNS serveru, který funguje na portu 53 a proto ho musíme také

povolit pokud chceme, aby fungoval. A samozřejmě je třeba povolit provoz v obou směrech.

```
sudo ipfw add 520 allow udp from me to any dst-port 53
```

```
sudo ipfw add 530 allow udp from any 53 to me
```

Po přidání těchto pravidel už je prohlížení internetových stránek plně funkční.

Nyní přidáme před všechna naše pravidla ve kterých je použito `keep-state` další pravidlo, které je právě s tímto parametrem svázáno. To znamená, že pokud toto pravidlo umístíme na začátek seznamu, vždy budou první prohledány dynamicky tvořené tabulky a v případě shody použito dané pravidlo. Pokud ke shodě nedojde, pokračuje standardní porovnávání s námi vytvořenými statickými pravidly.

```
sudo ipfw add 200 check-state
```

Po přidání tohoto posledního pravidla otestujeme za pomocí NMAPu jaké porty jsou otevřeny a také jestli všechny námi požadované funkce pracují tak jak mají.

```
PORT     STATE         SERVICE
22/tcp   open|filtered ssh
80/tcp   open|filtered http
88/tcp   open|filtered kerberos-sec
631/tcp  open|filtered ipp
5900/tcp open|filtered vnc

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.03 seconds
           Raw packets sent: 1344 (53.760KB) | Rcvd: 2339 (93.560KB)
```

Obr. 3.15: Výsledek otestování otevřených tcp portů pomocí NMap

```
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
88/udp   open|filtered kerberos-sec
123/udp  open          ntp
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
3283/udp open|filtered netassistant
5353/udp open|filtered zeroconf

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 16.72 seconds
           Raw packets sent: 1828 (52.823KB) | Rcvd: 2822 (108.507KB)
```

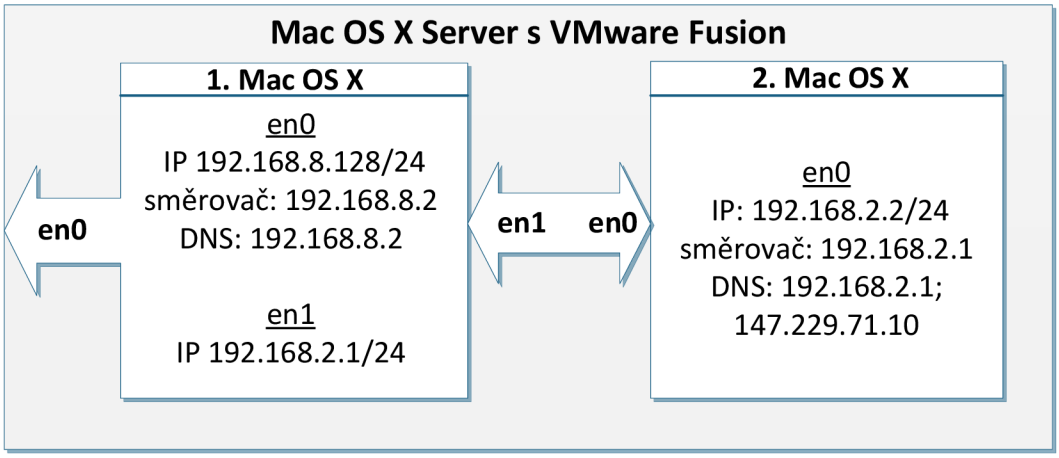
Obr. 3.16: Výsledek otestování otevřených udp portů pomocí NMap

Z výsledků NMapu je viditelné, že všechny námi otevřené porty jsou opravdu otevřeny. A při testování UDP vidíme otevřeny ještě další systémové porty.

3.3.4 Nastavení překladu adres mezi dvěma Mac OS X za pomocí NATD

Práce byla prováděna opět v rámci školního serveru a VMware Fusion 5, na kterém byly nainstalovány dva virtuální systémy Mac OS X „Mountain Lion“. Cílem práce bylo zprovoznění přesměrování a překladu adres mezi dvěma vytvořenými virtuálními systémy pomocí integrované funkce OS X, která se nazývá **NATD** a používá se pro tyto potřeby. První OS X má vytvořeno rozhraní pro přístup k veřejné síti přes fyzický stroj na kterém běží. Naopak druhý systém takové rozhraní vytvořené nemá a proto nemá možnost přistupovat do sítě. Proto je třeba nastavit spojení mezí těmito dvěma systémy a poté za pomocí NATD zprovoznit, aby druhý OS X mohl přistupovat do sítě. Právě díky přesměrování a překladu adres na prvním OS X.

A tak se v rámci řešení projektu vytvoří u obou systému privátní rozhraní a tím i spojení mezi nimi. Nyní má tedy první OS X dvě ethernetové rozhraní, kde pomocí jednoho (*en0*) přistupuje přes VMware a následně fyzický stroj do sítě a pomocí druhého (*en1*) do privátní sítě v rámci VMwaru. Druhý OS má vytvořeno pouze jedno ethernetové rozhraní (*en0*), které je připojeno do privátní sítě VMwaru. Všechno toto nastavení je viditelné na blokovém schématu 3.17.



Obr. 3.17: Schéma prostředí dvou virtuálních systémů s nastaveními pro jednotlivá rozhraní

Rozhraní ethernet0 (*en0*) u prvního virtuálu má síťové nastavení přiděleno VMwarem díky tomu, že sdílí připojení s fyzickým strojem (funkce ve VMwaru: Internet Sharing - Share with my Mac). U rozhraní ethernet1 (*en1*) je ale třeba manuálně nastavit námi požadované síťové nastavení, tzn. zvolit určitou IP adresu a masku

podsítě. Zvolíme IP adresu 192.168.2.1, která je defaultně užívána pro sdílení internetu v OS X.

U druhého virtuálního stroje je třeba nastavit pouze jedno rozhraní které má a to ethernet0 (*en0*). Chceme, aby oba systémy byly ve stejné privátní síti a tak zvolíme IP adresu 192.168.2.2. Aby tento počítač přistupoval do sítě přes první virtuál je třeba nastavit směrovač právě jako IP adresu prvního OS X. Stejnou IP adresu zadáme také jako DNS server a ještě přidáme školní DNS server (viz. 3.17).

Nyní máme nastaveny všechny síťové rozhraní na obou virtuálech podle našich požadavků. Ještě je potřeba zprovoznit přesměrování a překlad adres, aby druhý virtuál mohl přistupovat do sítě. A tak na prvním virtuálu jako první povolíme přesměrování v rámci sítě a k tomu použijeme příkaz, který přepíše hodnotu 0 v konfiguračním souboru na 1.

```
sudo sysctl -w net.inet.ip.forwarding=1
```

Teď když máme povoleno přesměrování je třeba povolit NATD i v rámci firewallu. A tak použijeme následující příkaz, který přidá pravidlo do seznamu a tím povolí NATD na rozhraní *en0* a v rámci jakékoliv IP adresy nebo portů.

```
sudo ipfw add divert natd ip from any to any via en0
```

Parametr příkazu `divert natd` vlastně povolí „odklánění“ síťového provozu v rámci zadaného rozhraní. Nyní už zbývá jen uvést do provozu samotný NATD, protože vše ostatní je připraveno. Pokud se podíváme na stránku manuálu k NATD [9], zjistíme že, je možné použít mnoho parametrů při spouštění NATD. Vybereme ty, které jsou pro nás užitečné a poté můžeme potvrdit příkaz a tím spustit překlad adres.

```
sudo natd -alias_address 192.168.8.128 -interface en0...

...-use_sockets -same_ports -unregistered_only -dynamic...

...-clamp_mss -enable_natportmap -natportmap_interface en1
```

Samozřejmě je třeba tento příkaz provést za pomocí administrátorských práv a proto provedeme příkaz s pomocí `sudo`. První dva parametry po samotném příkazu `natd` nám specifikují IP adresu a rozhraní, na které se provádí přesměrování, tzn. bod přes který oba počítače přistupují do veřejné sítě. Následující parametr `-use_sockets` zajišťuje úspěšné spojení i pokud dojde ke konfliktu mezi porty. Díky parametru `-same_ports` dochází k dodržování portů při změně odchozích paketů, proto je větší šance, že komunikace přes většinu protokolů bude funkční. Další parametr `-unregistered_only` povoluje změnu paketů pouze s privátní (neregistrovanou) adresou. Parametr `-dynamic` společně s parametrem `-interface` zajišťuje monitorování provozu na rozhraní, které je zvolené a pokud dojde ke změně IP adresy

tohoto rozhraní, dojde k dynamické upravě v parametru `-alias_address` a tak se nepřeruší komunikace. `-clamp_mss` povoluje úpravu maximální velikosti některých segmentů (*MSS - Maximum Segment Size*), což může být potřebné pokud je při TCP spojení maximální přenosová jednotka (*MTU*) menší než standardní velikost segmentů Ethernetu. Poslední dva parametry uvedené v našem příkazu povolují přesměrování portů za pomocí NATPMP protokolu na rozhraní *en1*. Tento protokol byl představen firmou Apple a to jako náhrada za IGD (*Internet Gateway Device Protocol*).

Po provedení celého tohoto postupu je překlad adres funkční a druhý virtuální stroj může bez problémů přistupovat k internetu. Pokud otestujeme z druhého virtuálu příkaz `traceroute` na adresu například `www.vutbr.cz` zjistíme, že provoz jde jako první přes první virtuální stroj a poté na fyzický stroj jak bylo zamýšleno.

```
Pep-MAC:desktop pep$ traceroute www.vutbr.cz
traceroute to piranha.ro.vutbr.cz (147.229.2.90), 64 hops max, 52 byte packets
 1  192.168.2.1 (192.168.2.1)  10.602 ms  27.697 ms  0.382 ms
 2  192.168.8.2 (192.168.8.2)  0.701 ms  0.496 ms  0.607 ms
```

Obr. 3.18: Výsledek otestování provozu pomocí traceroute

4 ZÁVĚR

Cílem práce bylo nastudování struktury operačního systému Mac OS X „Mountain Lion“ a analyzování bezpečnostních prvků a mechanismů, které tento systém používá. Veškeré prvky systému jsem studoval z velké části pomocí literatury přímo od výrobce tohoto systému. Během studia jsem si všechny své teoretické zjištění prakticky ověřil pomocí vzdáleného přístupu na školní server se systémem OS X ve verzi 10.8 „Mountain Lion“.

Všechna teoretická zjištění a popisy jednotlivých prvků systému jsou uvedeny v teoretické části mé práce. Ověření teoretických znalostí je reprezentováno vypracováním praktické části, ve které jsou jako první popsány postupy pro konfiguraci bezpečnostních prvků systému (uživatelské účty, šifrování a síťová bezpečnost). Konkrétně je v těchto postupech popsáno nastavení rodičovské kontroly při vytváření uživatelských účtů, nastavení firewallu a definování jeho specifických pravidel pomocí grafického rozhraní systému a jako poslední je popsán postup jak nastavit šifrování celého disku a jednotlivých složek a souborů. Tyto postupy jsem vypracoval pro OS X a také pro Microsoft Windows. Proto je možné teoretické srovnání prvků a jejich nastavení u obou těchto systémů. Z mého subjektivního pohledu, dlouholetého uživatele systému Windows, je používání Mac OS X v některých ohledech jednodušší, přehlednější a to již po krátké době jeho užívání. Naproti tomu je zde pro vykonání některých pokročilejších akcí zapotřebí znalostí, které běžný uživatel nemusí mít. Například pro komplexnější nastavení firewallu je třeba znalost příkazů terminálu (viz kapitola 3.3.3 o nastavení firewallu pomocí IPFW).

V dalších částech práce jsem již testoval a konfiguroval pouze Mac OS X. Jako první jsem otestoval vliv šifrování jednotlivých složek na rychlost kopírování oproti běžnému kopírování mezi složkami nešifrovanými. Tento vliv je zobrazen v grafech 3.13 a 3.14 pro různé velikosti souborů. Z těchto grafů je znát určitý vzorec podle kterého je viditelné, že šifrované kopírování od určité velikosti souborů trvá 2,8 - 3,1 krát déle. Proto můžeme usoudit, že šifrované kopírování je opravdu časově náročnější, ale zhruba trojnásobné snížení rychlosti je při běžném kopírování přijatelné. A pro šifrování osobních a citlivých souborů, které nemají velké velikosti, ale spíše textový charakter, je jistě na místě šifrování využívat.

Další část je také zaměřena na testování vlivu šifrování na rychlost systému, ale tentokrát je to při šifrování celého disku v reálném čase pomocí FileVault. Měřil jsem časy provedení systémových akcí, ale i časy spuštění běžně užívaných aplikací. Výsledky veškerých měření jsou uvedeny v tabulkách 3.3 a 3.4. U první tabulky ve které jsou uvedeny výsledky pro testování samotného systému je viditelné, že se značně liší jen čas startu systému a následného přihlášení. Ale pokud tyto dva úkony vezmeme jako celek (přihlašování většinou probíhá po startu systému) a je-

jich časy sečteme, tak zjistíme že v obou případech se dostaneme na čas okolo 35 sekund. Takže při zapnutí systému a následném přihlášení není uživatel šifrováním časově ovlivněn. K ovlivnění by došlo pouze pokud by přihlášení probíhalo nezávisle na startu systému, potom je u šifrovaného systému doba přihlášení pětkrát delší. Rozdíly mezi časy při odhlašování uživatele a vypnutí systému se nijak zásadně neliší. Ve druhé tabulce jsou uvedeny časy pro spouštění jednotlivých aplikací a hned na první pohled je viditelné, že šifrování systému neovlivňuje tuto činnost takovým způsobem, abychom ji byly schopni zaznamenat. Nakonec tedy můžeme říci, že ve většině případů šifrování celého disku pomocí FileVaultu neovlivňuje chod systému takovým způsobem, aby to uživatel zaznamenal při běžné práci.

Jako další jsem vytvořil a popsal komplexní firewall vytvořený pomocí IPFW, který filtruje veškerý síťový provoz a povoluje pouze vybrané základní funkce systému. Veškeré prováděné kroky a příkazy jsou popsány v kapitole 3.3.3. Tento vytvořený firewall povoluje ping, SSH, telnet, vzdálené ovládání plochy a samozřejmě plně funkční prohlížení internetových stránek. U příkazů je implementována i možnost vytvářet dynamickou tabulku pravidel, která mnohdy zjednoduší práci s firewallem. Po uvedení vytvořeného seznamu pravidel do provozu jsem otestoval otevřené porty pomocí NMap. Výsledky tohoto testování jsou zobrazeny na obrázcích 3.15 a 3.16. Je viditelné, že jsou otevřeny ty porty, které jsme pomocí pravidel otevřít chtěli pro naše potřeby. Ale jsou zde i některé další systémové porty, například 88 (Kerberos - zabezpečuje autentizaci uživatele), 123 (NTP - *Network Time Protocol*) a 5353 (slouží pro Multicast DNS). Po následném manuálním otestováním veškerých zprovozněných služeb jsem nenarazil na chybu v jejich funkčnosti.

Posledním úsekem mé praktické části je zprovoznění přesměrování a překladu adres pomocí SNAT mezi dvěma systémy Mac OS X. Komunikaci mezi oběma systémy jsem nastavil v rámci dvou virtuálních strojů ve VMwaru. Blokové schéma popisující mnou zvolené síťové nastavení obou systému je na obrázku 3.17. Zde je viditelné, že první stroj má vytvořeny rozhraní jak pro komunikaci s fyzickým strojem tak s privátní sítí v rámci VMwaru. Oproti tomu druhý stroj má rozhraní pouze pro komunikaci v privátní síti. Po přidělení síťových parametrů oběma strojům je třeba povolit přesměrování v konfiguračním souboru a také přidat pravidlo do IPFW firewallu. Jako poslední krok je je třeba uvést do provozu samotný NATD. Příkaz pro jeho spuštění má více parametrů z důvodu zajištění provozu i při například různých změnách portů nebo IP adres. Nyní je síťový provoz na druhém stroji plně funkční. Pro ujištění, že vše pracuje tak jak bylo zamýšleno, jsem otestoval `traceroute` ven z privátní sítě. Na výsledku, který je na obrázku 3.18 je jasně viditelné, že provoz z druhého virtuálního stroje prochází jako první přes první virtuální stroj (192.168.2.1) a následně teprve přes fyzický stroj (192.168.8.2), který má přístup k internetu.

LITERATURA

[1] *Apple History Timeline.* [online]. [cit. 2012-12-09]. Dostupné z URL: <http://applemuseum.bott.org/sections/history.html>.

[2] *Apple to Use Intel Microprocessors Beginning in 2006.* [online]. [cit. 2012-11-09]. Dostupné z URL: <http://www.apple.com/pr/library/2005/06/06Apple-to-Use-Intel-Microprocessors-Beginning-in-2006.html>.

[3] *How to Configure a Firewall for Mac OS X: ipfw for Snow Leopard.* THE UNIVERSITY OF NORTH CAROLINA. [online]. [cit. 2013-04-30]. Dostupné z URL: <http://help.unc.edu/help/how-to-configure-a-firewall-for-mac-os-x-ipfw-for-snow-leopard/>.

[4] JEPSON, Brian, Ernest E ROTHMAN a Brian JEPSON. *Mac OS X Tiger for Unix geeks.* 3rd ed. Sebastopol, CA: O'Reilly, 2005, 395 s. ISBN 05-960-0912-7.

[5] KISSELL, Joe. *Mac security bible.* Indianapolis: Wiley Publishing, 2010, 900 s. ISBN 978-0-470-47419-8.

[6] *Macintosh: System Software Version History.* [online]. [cit. 2012-11-09]. Dostupné z URL: <http://support.apple.com/kb/TA31885?viewlocale=en_US>.

[7] *Mac OS Timelines.* [online]. [cit. 2012-12-09]. Dostupné z URL: <http://www.guidebookgallery.org/timelines/macos>.

[8] *Mac OS X: Security Configuration.* [online]. roč. 2010 [cit. 2012-11-11]. Dostupné z URL: <http://images.apple.com/support/security/guides/docs/SnowLeopard_Security_Config_v10.6.pdf>.

[9] *NATD(8) BSD System Manager's Manual.* [online]. [cit. 2013-05-24]. Dostupné z URL: <https://developer.apple.com/library/mac/documentation/Darwin/Reference/ManPages/man8/natd.8.html>.

[10] *OS X: About FileVault 2.* [online]. [cit. 2013-04-30]. Dostupné z URL: <http://support.apple.com/kb/ht4790>.

[11] *IPFW(8) BSD System Manager's Manual.* [online]. [cit. 2013-05-24]. Dostupné z URL: <https://developer.apple.com/library/mac/documentation/Darwin/Reference/ManPages/man8/ipfw.8.html>.

[12] STALLINGS, William. *Cryptography and network security: principles and practice.* 5th ed. Boston: Prentice Hall, 2010, 744 s. ISBN 01-360-9704-9.

[13] SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii.* Praha: Dokořán, 2003, 382s. ISBN 80-865-6918-7.

[14] *The Keccak sponge function family.* [online]. [cit. 2012-11-09]. Dostupné z URL: <`http://keccak.noekeon.org/`>.

[15] *Well known TCP and UDP ports used by Apple software products.* [online]. [cit. 2013-04-31]. Dostupné z URL: <`http://support.apple.com/kb/ts1629`>.