Řízení přístupu

Řízení přístupu je proces autorizace uživatelů, skupinám a počítačům přistupovat k objektům. Předtím než subjekt může získat přístup k objektu, musí se nejprve sám identifikovat bezpečnostnímu podsystému operačního systému. Identita je přítomna v přístupovém žetonu „access token“, který je vždy znovuvytvořen při každém přihlášení. Nežli povolí systém přístup k objektu, ověří, zdali má daný žeton oprávnění k přístupu porovnáním informací z žetonu s bezpečnostními záznamy (Access control entries ACE) daného objektu. ACE může povolovat nebo zakazovat velké množství chování. Například pro soubory může umožňovat čtení, zápis nebo spouštění, tiskárny například možnost tisku, správy tiskárny nebo správy dokumentů v tiskové frontě.

Individuální záznamy ACE tvoří seznamy – ACL (access control list). Bezpečnostní systém prohledává ACL objektu tak dlouho, dokud nenajde ACE záznam patřící danému uživateli nebo skupině, který by povoloval nebo zakazoval přístup nebo neprohledá celý seznam. Pokud dojde až na konec seznamu bez nalezení záznam o požadovaném typu přístupu, bezpečnostní systém zamítne uživateli přístup.

Oprávnění

Oprávnění definují typ přístupu povolující nebo zakazující uživateli nebo skupině přístup k objektu nebo vlastnosti objektu. Například skupině Simpsons povolí oprávnění číst soubor s názvem televizní_program.txt. Pomocí uživatelského rozhraní můžete nastavovat NTFS oprávnění na soubory, objekty Active Directory, registrové záznamy, procesy, atd. Oprávnění mohou být udělena jakémukoli uživateli, skupině nebo počítači. Je vhodné a doporučované přidělovat oprávnění skupinám místo jednotlivým uživatelům nebo skupinám pro lepší přehlednost, správu a výkon během ověřování.

Oprávnění přidělená k objektům závisí na jejich typu. Například oprávnění pro soubory jsou trochu jiná, než oprávnění u registrových záznamů. Nicméně velmi často jsou oprávnění společná, jako například oprávnění Čtení, Zápisu, Modifikace, Smazání.

Když nastavujete oprávnění, určujete úroveň přístupu dané skupiny nebo uživatele. Například uživatel může nechat jednoho uživatele číst obsah souboru, druhého soubor upravovat a měnit a všem ostatním odepřít přístup k souboru kompletně. Obdobně nastavíte oprávnění u tiskáren, několika uživatelům oprávnění spravovat tiskárnu a a ostatním pouze tisknout.

Pokud chcete nastavovat oprávnění na souboru, v průzkumníku klikněte pravým tlačítkem myši na daný soubor, vyberte **Vlastnosti**. Na záložce **Zabezpečení** můžete poté upravovat oprávnění.

Vlastnictví objektu

Každému objektu je při jeho vytvoření přiřazen vlastník. Ve výchozím nastavení vlastníkem je jeho tvůrce. Bez ohledu na oprávnění, jaká jsou nastavená pro daný objekt, jeho vlastník může vždy tato oprávnění upravovat.

Dědičnost oprávnění

Dědičnost umožňuje administrátorům jednoduše spravovat a přidělovat oprávnění. Tato funkce zajišťuje automatické kopírování všech oprávnění, která jsou děditelná, z kontejneru, který obsahuje daný objekt. Například soubor uvnitř složky, když je vytvořen, dědí oprávnění dané složky. Pouze oprávnění označená k dědění budou zděděna. Zděděná oprávnění jsou zobrazována zašedle a a nejdou editovat. Existují tři doporučené způsoby jak upravovat zděděná oprávnění:

- Upravit oprávnění na rodičovském objektu, od něhož jsou oprávnění děděna.
- U daného objektu můžete explicitně uvést povolující (**Allow)** oprávnění, které přepíše zděděný zákaz (**Deny**).
- Zrušit zatržení u „Zahrnout zděditelná oprávnění z nadřazeného objektu“.

Zděděná zakazující oprávnění (Deny) nezabraňují přístupu klientovi k objektu, pokud má na daném objektu explicitně uvedené povolující oprávnění (Allow).

Explicitní oprávnění mají přednost před zděděnými oprávněními, dokonce i před zděděnými oprávněními Odepřít (Deny).

Vyhodnocení výsledného oprávnění

Oprávnění se sčítají podle skupin, kterých je uživatel členem. Pokud bude uživatel členem např. 3 skupin, kde každá bude mít jiná oprávnění ke stejnému objektu, výsledná oprávnění uživatele budou součtem všech oprávnění těchto skupin k danému objektu. Toto neplatí pro oprávnění Deny. Toto oprávnění je nadřazeno všem ostatním. Pokud byť v jediné skupině by bylo použito oprávnění Deny k některé akci, bude tato akce danému uživateli zakázána, i kdyby byla ve všech ostatních skupinách, jejichž je členem, povolena. Nicméně existuje výjimka i na toto pravidlo právě s již zmíněnou dědičností, tedy explicitními a zděděnými oprávnění. Uplatňují se tedy v tomto pořadí:

1) explicitní odepřít
2) explicitní povolit
3) zděděné odepřít
4) zděděné povolit

Pro snadné vypočtení výsledných oprávnění obsahuje systém Windows kalkulátor NTFS oprávnění, který bere v potaz členství uživatele ve všech skupinách. Ve **vlastnostech** daného objektu, záložce **Zabezpečení** klikněte na tlačítko **Upřesnit**. V novém okně na záložce **Skutečná oprávnění** můžete určit účet, jehož výsledná oprávnění vás zajímají a a systém vám je zobrazí.

Přehled NTFS oprávnění

NTFS oprávnění jsou základní a rozšířená a a stejné oprávnění se jinak chová pro složku a a jinak pro soubor. Základní oprávnění se poté skládají z kombinace více oprávnění rozšířených. V následující tabulce jsou vypsána oprávnění, která lze nastavit, nebo naopak odepřít a složení základních oprávnění z rozšířených.

Special Permissions	**Full Control**	**Modify**	**Read & Execute**	**Read**	**Write**
Traverse Folder/Execute File	X	X	X		
List Folder/Read Data	X	X	X	X	
Read Attributes	X	X	X	X	
Read Extended Attributes	X	X	X	X	
Create Files/Write Data	X	X			X

Create Folders/Append Data	X	X			X
Write Attributes	X	X			X
Write Extended Attributes	X	X			X
Delete Subfolders and Files	X				
Delete	X	X			
Read Permissions	X	X	X	X	X
Change Permissions	X				
Take Ownership	X				
Synchronize	X	X	X	X	X

Sdílení

Umožňuje využívat prostředky vzdáleného systému tak, jako by byli přístupné lokálně. U sdílení souborů rozlišujeme 3 typy sdílení – běžné, administrativní, skryté. Administrativní sdílení je skryté sdílení, jejž mohou využívat pouze členové skupiny Administrators. Administrativně jsou sdíleny složky Windows (ADMIN$), pevné disky (C$) a IPC$.

Skryté sdílení umožňuje přístup pouze, když zadám úplnou UNC cestu (nemohu se k němu proklikat - browse). Skryté sdílení končí vždy dolarem $.

Postup při přístupu na sdílení: Nejdříve firewall ověří, zda je povoleno sdílení. V druhém kroku je ověřeno, zda má uživatel právo přístupu k počítači ze sítě. Pokud má právo přístupu ze sítě, ověří se oprávnění sdílení. Nakonec se ověří oprávnění NTFS.

U oprávnění sdílení platí stejná pravidla jako u oprávnění NTFS. Pokud je uživatel ve více skupinách, je výsledné oprávnění sjednocením oprávnění jednotlivých skupin. Deny je silnější než allow – pokud má v jedné skupině právo read allow, ale v druhé skupině má právo read deny je výsledkem read deny.

Výsledné oprávnění je průnikem oprávnění sdílení a oprávnění NTFS. Například, pokud mám oprávnění sdílení read allow, ale u NTFS nemám read uvedeno, je výsledkem, že nemohu číst danou složku.

Microsoft považuje za dobrou praxi, nastavit skupině Authenticated Users nebo Everyone oprávnění Full Control pro sdílená oprávnění a následně spoléhat na NTFS oprávnění, která budou mít standardní konfiguraci, která se uplatní jak lokálně, tak i na všechny přístupy po síti (oprávnění přístupu přes síť se netýká funkce Vzdálené plochy). Tento postup je považován za efektivní způsob řízení přístupu k místním a síťovým datům. Poskytuje také dobrou strategii při zálohování, změně názvu nebo umístění.

Soubory offline (Offline Files)

Speciální typ synchronizace. Umožňuje přistupovat k souborům na síti, i když k této síti není uživatel připojen. Nejde o nic jiného než vytvoření kopií těchto souborů na lokálním počítači a jejich neustálé synchronizaci. Pro zpřístupnění souborů offline je nejprve potřeba globálně povolit tuto službu, následně označit požadované soubory jako přístupné offline a nakonec pomocí **Centra synchronizace** provést synchronizaci, aby byly tyto soubory přeneseny na cílové zařízení. Ve

Windows 7 došlo k integraci globálního nastavení **Souborů offline** do **Centra synchronizace**, kde je přístupné skrz Spravovat soubory offline v levém panelu **Centra synchronizace**.

Soubory offline tvoří obousměrné partnerství pro synchronizaci, takže zde může docházet ke konfliktům. Protože tyto soubory mohou být důvěrné a jsou často synchronizovány na mobilní zařízení, je zde velké nebezpečí jejich odcizení odcizením daného zařízení. Pro zabezpečení těchto dat lze tyto data šifrovat pomocí systému EFS a tím zabránit jejich zneužití.

Encrypting File System (EFS)

Nejčastější ochranou dat v systémech Windows je využití možností zabezpečení NTFS souborového systému. Soubory mají definovány přístupové oprávnění a systém při každém přístupu k těmto datům kontroluje, zda přihlášený uživatel má oprávnění provádět vyžadovanou operaci. V tomto případě ale nejde o ochranu na úrovni dat, ale na úrovni přístupu k datům, samotná data nejsou nijak chráněna. Pokud útočník získá fyzický přístup k datům, např. získá pevný disk, může tento disk připojit k jinému počítači, kde má oprávnění modifikovat přístupová práva (má účet s administrátorskými právy), nebo kde jednoduše vůbec k ověřování práv nedochází (např. jiný operační systém jako Linux s adekvátními ovladači NTFS souborového systému).

EFS poskytuje ochranu na úrovni dat, takže data jsou čitelná pouze pro uživatele vlastnící validní dešifrovací klíč. **EFS** není služba systému Windows, ale služba souborového systému NTFS, takže lze šifrovat pouze soubory na oddílech naformátovaných jako NTFS. Výhodou **EFS** je transparentnost, veškeré šifrování a dešifrování probíhá na pozadí a uživatel ani nemusí vědět, že je soubor, se kterým pracuje, zašifrován.

EFS využívá pro svou činnost kombinaci symetrické a asymetrické kryptografie. Symetrická kryptografie využívá jediný klíč pro zašifrování i dešifrování dat, zatímco asymetrická kryptografie využívá klíče dva - veřejný klíč pro zašifrování dat a privátní klíč pro dešifrování dat, u systému EFS jsou tyto klíče ve formě certifikátu. Při šifrování dat se nejprve vygeneruje klíč (FEK – File Encryption Key), kterým se pomocí symetrické kryptografie zašifrují data. Poté se pomocí veřejného klíče uživatele zašifruje asymetricky tento vygenerovaný klíč. Při dešifrování se nejprve dešifruje FEK a poté se tímto klíčem dešifrují data.

Kombinace těchto dvou technik poskytuje řadu výhod. Symetrická kryptografie je velice rychlá[1], což je výhodné pro šifrování velkého množství dat, ovšem představuje riziko z hlediska ochrany samotného klíče pro šifrování. Asymetrická kryptografie je pomalá, což je ovšem při šifrování malého objemu dat (u **EFS** pouze FEK) zanedbatelné, ale zato velice bezpečná. Také tento způsob umožňuje jednoduše realizovat přístup více uživatelů k zašifrovaným datům, stačí pouze zašifrovat FEK veřejným klíčem dalšího uživatele a přiložit tento zašifrovaný řetězec k souboru.

Je důležité pamatovat na to, že **EFS** poskytuje ochranu na úrovni dat. Pokud útočník nemá dešifrovacím klíč, nedostane se k datům, ovšem stejná situace může nastat i z pohledu uživatele, pokud ztratí svůj certifikát, který obsahuje dešifrovací klíč. Je tedy vhodné mít tento certifikát zálohovaný a bezpečně uložený pro případ ztráty. Windows 7 poskytuje průvodce, které umožní uživateli jednoduše zálohovat nebo obnovit svůj certifikát. Protože uživatelé často opomíjejí zálohování svých certifikátů, poskytuje Windows 7 také možnost vytvoření tzv. **Agenta Obnovení**

[1] Často se uvádí, že symetrická kryptografie je až 1000x rychlejší než asymetrická

(Recovery Agent, RA), který má schopnost dešifrovat jakákoliv data zašifrovaná pomocí EFS. Princip fungování **Agenta Obnovení** je jednoduchý, jak již bylo zmíněno dříve, ke každému zašifrovanému souboru lze přidat další uživatele, kteří mohou soubor dešifrovat, systém tedy pouze přidá **Agenta Obnovení** jako dalšího uživatele, který má právo soubor dešifrovat při každém šifrování souboru, které na počítači v budoucnu proběhne. Soubory před vytvořením **Agenta Obnovení** pro něj ale **nebudou** přístupné, pro zpřístupnění lze ovšem využít nástroj **cipher**, který umožňuje aktualizovat zašifrované FEK jednotlivých souborů a dodat potřebná data pro zpřístupnění souborů **Agentovi Obnovení**.

BitLocker

Nová možnost šifrování dat od Windows Vista, podporován pouze v edicích Enterprise a Ultimate. **BitLocker** se od **EFS** odlišuje několika klíčovými vlastnostmi:

- Šifruje celý systémový oddíl, včetně souborů všech uživatelů a souborů systému (**EFS** neumožňuje šifrování systémových souborů)
- Chrání počítač ihned po startu, před tím než naběhne operační systém. Po startu operačního systému je již kompletně transparentní
- Poskytuje šifrování na úrovni počítače, ne na úrovni uživatele. Pro zabezpečení souborů proti jiným nepovolaným uživatelům je potřeba využít systému **EFS**
- Umožňuje chránit integritu operačního systému, čímž napomáhá chránit proti rootkitům a offline útokům (externí modifikace systémových souborů)
- Šifruje pouze systémový oddíl, šifrování dat na jiných oddílech lze provést pouze pomocí systému **EFS**

BitLocker vyžaduje pro svou činnost dva oddíly NTFS, první obsahující operační systém a druhý obsahující alespoň 1,5GB volného místa, které bude použit jako bootovací oddíl. Existují dvě možnosti kde skladovat symetrický klíč používaný pro šifrování dat:

- **TPM** (Trusted Platform Module) čip – obsažen přímo v počítači
- **USB flash disk** – vyžaduje připojení při každém startu počítače nebo přechodu z hibernace

Pokud počítač obsahuje **TPM** čip, jsou k dispozici dva režimy činnosti:

- **Pouze TPM** – Transparentní uživateli, během startu počítače **BitLocker** ověří u **TPM** integritu počítače a operačního systému. Pokud **TPM** není nalezeno, pevný disk byl přesunut nebo došlo ke změně startovacích souborů, přejde **BitLocker** do režimu obnovení (recovery mode) a bude po uživateli požadovat klíč pro obnovení (recovery key) nebo připojit USB flash disk obsahující tento klíč. **BitLocker** zde poskytuje pouze ochranu proti krádeži pevného disku.
- **TPM s klíčem pro start** – Kromě ověření u **TPM** bude **BitLocker** navíc požadovat po uživateli klíč pro start (startup key). Klíč pro start může být zadán přímo ve formě hesla nebo obsažen na USB flash disku. **BitLocker** zde poskytuje jak ochranu proti odcizení pevného disku tak celého počítače.

Pokud není **TPM** k dispozici, lze pro uložení symetrického klíče použít USB flash disk. Pokud dojde ke ztrátě tohoto disku, lze pro obnovu dat použít klíč pro obnovení (recovery key), který je sdělen uživateli při aktivaci **BitLockeru**.

Hlavním cílem **BitLockeru** je co nejlépe ochránit symetrický klíč pro šifrování obsahu disku, tzv. Full Volume Encryption Key (**FVEK**). **FVEK** je uložen na **TPM** čipu, případně na USB flash disku (jenž ale ve srovnání s **TPM** čipem neposkytuje tak vysokou bezpečnost). **TPM** čip obsahuje sadu registrů, tzv. PCRs (Platform Configuration Registers), jejichž obsah je při spuštění počítače vynulován. Obsah těchto registrů může být změněn pouze speciální funkcí **`extend`**, jenž nastaví hodnotu registru na hash předchozí hodnoty registru a předaného datového řetězce. Tedy cílová hodnota je hash přes všechny předané datové řetězce a jediný způsob jak získat identickou hodnotu je provést stejnou sekvenci volání **`extend`**. Pro získání / uložení **FVEK** klíče poté slouží funkce **`unseal`** / **`seal`**. Funkce **`seal`** zašifruje **FVEK** klíč na základě hodnoty PCR registrů, funkce **`unseal`** naopak dešifruje **FVEK** klíč, pokud je hodnota PCR registrů totožná s hodnotou, jakou měly v době šifrování klíče.

Základní princip fungování **BitLockeru** je poté následující. Během startu počítače sledují **PCR** registry kód, jenž se vykonává, a na jeho základě modifikují svůj obsah. Při normálním startu dosáhnou hodnoty **PCR** registrů stejných hodnot, jakých nabývaly při šifrování **FVEK** klíče a lze tedy **FVEK** klíč úspěšně dešifrovat. V případě nastartování jiného operačního systému bude hodnota **PCR** registrů odlišná a nebude možné tedy disk dešifrovat (přesněji nebude možné dešifrovat systémový oddíl disku původního operačního systému, jiné operační systémy mohou normálně startovat, jen nebudou mít přístup k tomuto oddílu disku).

Více v detailu dochází při startu počítače nejprve k spuštění kódu BIOSu. První část tohoto kódu je neměnná a zajišťuje rozšíření PCR BIOSu (volání funkce **`extend`**) o celý kód BIOSu. Pokračuje se vykonáváním kódu BIOSu, jenž následně načte MBR disku a použije obsah sektoru s MBR k rozšíření **PCR** zaváděcího sektor (Boot Sector **PCR**) a spustí kód uložený v MBR. Dále dochází ještě k několika takovýmto iteracím, kdy se načtený kód vždy nejprve použije k rozšíření nějakého **PCR** registru a následně se vykoná. Volání funkce **`extend`** nijak neovlivňuje start jiných operačních systémů, ty obsah **PCR** registrů ignorují.

Samotné šifrování obsahu disku využívá AES-CBC algoritmus + Elephant diffuser. AES-CBC podporuje klíče délky 128 a 256 bitů. Elephant diffuser je proprietární implementace algoritmu, jenž zajišťuje tzv. *diffusion* vlastnost. Tato vlastnost zajišťuje, aby neuniformní distribuce písmen v původním textu byla redistribuována v mnohem složitější neuniformní distribuci v šifrovaném textu, neboli bity šifrovaného textu by měly velice složitě záviset na bitech původního textu. Jakmile se tedy změní jediný bit původního textu, mělo by dojít ke kompletní změně odpovídajícího šifrovaného textu. Diffusery pracují v obou směrech, jak ve směru úpravy původních dat na šifrovaná, tak opačně. **BitLocker** využívá celkem dva diffusery, oba jsou navrženy tak, aby měly dobré *diffusion* vlastnosti v jednom směru na úkor špatných vlastností v opačném směru. Oba pak poskytují dohromady dobré vlastnosti v obou směrech.

BitLocker To Go

Rozšíření **Bitlockeru** o možnosti šifrování úložných zařízení připojených přes USB. **Bitlocker To Go** podporuje celkem dva způsoby odemykání (dešifrování obsahu) zařízení, buď na základě zadání hesla nebo vložením smart karty.

Princip fungování **Bitlockeru To Go** je velice podobný **Bitlockeru**. Využívá celkem tři klíče:

- USB disk je zašifrován pomocí **VFEK** klíče, jenž opět využívá algoritmus AES-CBC s Elephant diffuser, ve výchozím nastavení je délka klíče 128 bitů
- **VFEK** je pak zašifrován pomocí 256 bitového klíče založeného na AES, tzv. **VMK** klíč (Volume Master Key)
- **VMK** je nakonec zašifrován heslem zadaným uživatelem nebo přítomným na smart kartě

Další novinkou je možnost konfigurace **Bitlocker To Go** pomocí politik, kde je možné například zakázat používání USB zařízení, jenž nemají **Bitlocker To Go** povolen, povolit možnost využití **Agenta Obnovení** pro dešifrování obsahu nebo nastavit délku klíče AES-CBC algoritmu.

LAB1 – NTFS Oprávnění

V následujícím cvičení si ukážeme uplatňování NTFS oprávnění, dědičnost oprávnění, její rušení a také přebírání vlastnictví souborů a složek.

Prerekvizity: win7-base a uživatelské účty **Homer** (Administrators), **Bart** (Users), **Lisa** (Users), skupina **Simpsons** (**Homer**, **Bart**, **Lisa**).

1) Přihlaste se na **win7-base** pod účtem **Homer**.
2) Vytvořte složku **C:\Simpsons**. Na nové složce otevřete **Vlastnosti** -> **Zabezpečení** -> **Upravit** (Properties -> Security ->Edit). Přidejte oprávnění **Číst**, **Číst a spouštět**, **Zobrazovat obsah složky** (Read, Read & execute a List folder kontent) členům skupiny **Simpsons**.
3) Přihlaste se postupně pod všemi účty rodiny Simpsonů a vytvořte si domovský adresář s odpovídajícím jménem. Zkontrolujte, zda se zdědila oprávnění pro skupinu Simpsons.
4) Pod účtem **Lisa** si nyní vytvořte adresář **C:\Simpsons\Lisa\Secrets**.
5) Na složce **Secrets** vyberte **Vlastnosti** -> **Zabezpečení** -> **Upřesnit** -> **Změnit oprávnění** (Properties -> Security -> Advanced -> Change Permission).
6) **Zrušte** zatržení u „**Zahrnout zděditelná oprávnění z nadřazeného objektu**“ (Include inheritable permissions from this object's patent). V následném dotazu zvolte **Přidat** (Add).
   - Lisa si nepřeje, aby jí kdokoli další zasahoval do tajného adresáře, proto potřebuje zrušit zděděná oprávnění.
7) Nyní upravte seznam oprávnění -> OK:
   - Odstraňte všechna oprávnění kromě SYSTEM.
   - Přidejte povolující oprávnění **Úplné řízení** účtu **Lisa** (Allow Full Controll).
8) V okně „Upřesnit nastavení zabezpečení“ (Advanced Security Settings) se na kartě **Skutečná oprávnění** (Effective Permissions) přesvědčte o tom, zda opravdu Bart ani Homer nemají přístup k adresáři.
9) Přihlaste se z ostatních účtů a ověřte, že nemohou přistupovat k obsahu.
10) Přihlaste se zpět jako **Lisa** a mezi oprávnění přidejte následující položky (Lisa je trochu paranoidní):
    - Bart – **Odepřít Úplné řízení** (Deny Full Control)
    - Homer – **Odepřít Úplné řízení** (Deny Full Control)
11) Nyní vytvořte v adresáři Secrets soubor **denik.txt** s nějakým obsahem.
12) Ověřte pro ostatní účty, že se nemohou dostat k obsahu adresáře **Secrets** ani k souboru **denik.txt**:
    - pomocí nástroje Skutečná oprávnění (Effective Permissions)
    - přihlášením pod daným účtem
    - Pokuste se otevřít v poznámkovém bloku soubor specifikováním celé cesty.
13) Přihlaste se zpět jako **Lisa**. Vytvořte v adresáři **Secrets** nový soubor **tajny.txt**. Udělte **Bartovi** oprávnění **Čtení**. Opakujte předchozí krok, Bart by měl být schopen otevřít soubor v poznámkovém bloku.
    - Lisa s Bartem si budou chtít do tohoto souboru ukládat společné tajnosti tak, aby je Homer nezjistil.

14) Přihlaste se jako **Homer**. Na složce **Secrets** vyberte **Vlastnosti** -> **Zabezpečení** -> **Upřesnit** -> **Vlastník** -> **Změnit** (Properties -> Security -> Advanced -> Owner -> Edit). Vyberte účet **Homer** -> OK.
    - Homer nemůže najít svoje pivo a dobře ví, že před ním Lisa s Bartem něco schovávají. Využije tak svých administrátorských oprávnění a převezme vlastnictví složky a souboru tajny.txt.
15) Upravte si oprávnění pro možnost čtení. Tento postup opakujte pro možnost čtení souboru tajny.txt.

LAB2 – Šifrování souborů pomocí EFS a záloha certifikátu

Poté, co se Lisa dozvěděla o tom, co Homer udělal, rozhodla se šifrovat soubor pomocí EFS. Čili v tomto cvičení se seznámíte s odlišnostmi mezi šifrováním a NTFS přístupovými oprávněními, jak zálohovat certifikát pro dešifrování souborů.

1) Přihlaste se na **win7-base** jako **Lisa**.
2) U souboru **tajny.txt** vyberte **Vlastnosti** -> **Obecné** -> **Upřesnit** (Properties -> General -> Advanced).
3) Zatrhněte Šifrovat obsah a zabezpečit tak data (Encrypt contents to secure data)
    - Pokud uživatel ještě nemá vytvořen certifikát pro EFS (sada privátního a veřejného klíče využívaného asymetrickou kryptografií pro šifrování FEK, viz. EFS), bude automaticky vytvořen operačním systémem.
4) Potvrďte OK a v zobrazeném dialogu vyberte Zašifrovat pouze soubor (Encrypt file only)
5) Přihlaste se jako **Homer** a ověřte, že ani uživatel s administrátorskými oprávněními nezobrazí obsah zašifrovaného souboru
    - Nezapomeňte, že v případě zabezpečení souboru pomocí NTFS přístupových práv by takovýto uživatel mohl data přečíst, ať již přímo nebo po převzetí vlastnictví souboru.
6) Přihlaste se zpět jako uživatel **Lisa.**
7) Otevřete Uživatelské účty (User Accounts) v Ovládacích panelech (Control panel) a vyberte Spravovat šifrovací certifikáty souborů (Manage your file enctyption certificates).
8) U výběru šifrovacího certifikátu zvolte Použít tento certifikát (Use this certificate).
9) Zvolte Zálohovat certifikát a klíč nyní (Back up the certificate and key now), specifikujte cílový souboru pro zálohování (např. **C:\Simpsons\efscert.pfx**) a heslo (např. **aaa**) a pokračujte.
10) U aktualizace zašifrovaných souborů zvolte Všechny logické jednotky (All Logical Drives) a pokračujte
    - Aktualizace zajistí schopnost dešifrování dat, které byly zašifrovány před vytvořením tohoto certifikátu, ale pouze dat, ke kterým má daný uživatel přístup (tzn., může je např. dešifrovat pomocí jiných certifikátů apod.)

LAB3 – Sdílení šifrovaných souborů

Lisa a Bart stále chtějí sdílet soubor tajny.txt. Ukážeme si tedy jak toto zařídit. V tomto případě si Bart vytvoří vlastní klíč pro šifrování a Lisa tento klíč použije k povolení přístupu k souboru tajny.txt.

1) Přihlaste se na **win7-base** jako **Bart**.
2) Vytvořte si v domovském adresáři textový soubor a ten zašifrujte.
    - Bart si potřebuje vytvořit nový certifikát pro EFS.

3) Přepněte se na účet **Lisa**. U souboru **tajny.txt** otevřete -> **Vlastnosti** -> **Obecné** -> **Upřesnit** -> **Podrobnosti** (Properties -> General ->Advanced -> Details).
4) Nyní pomocí **Přidat** (Add) přidejte Bartův certifikát.
5) Ověřte, že Bart je nyní opět schopen číst soubor pomocí poznámkového bloku při zadání přesného umístění.

LAB4 – Sdílení šifrovaných souborů

Druhý způsobem sdílení šifrovaných souborů je import certifikátu, který jsme ve 2. cvičení exportovali. Tím však zpřístupníme všechny zašifrované soubory.

1) Přihlaste se jako uživatel **Homer** a spusťte uložený certifikát **efscert.pfx**, zobrazí se Průvodce importem certifikátu (Certificate Import Wizard).
2) Pokračujte dále s ponecháním výchozího nastavení až do části Heslo (Password), kde zadejte dříve specifikované heslo pro ochranu certifikátu a pokračujte.
3) Jako Úložiště certifikátu (Certificate Store) ponechte výchozí automatický výběr a pokračujte.
4) Potvrďte import certifikátu pomocí Dokončit (Finish).
5) Ověřte, že nyní již uživatel **Homer** může otevřít a přečíst soubor **tajny.txt**.

LAB5 – Vytvoření Agenta Obnovení

Nyní si ukážeme postup vytvoření Agenta obnovení pro potřeby dešifrování šifrovaných souborů v případě ztráty certifikátu.

1) Přidělte Studentovi oprávnění **Číst** soubor **tajny.txt**.
2) Přihlaste se jako uživatel **Student.**
3) Spusťte **Příkazový řádek** např. příkazem **cmd.**
4) Vytvořte certifikáty pro **Agenta Obnovení** příkazem **cipher /R:racert**, jako heslo zvolte **aaa**
5) Otevřete Editor místních zásad skupiny (Local Group Policy Editor) např. příkazem **gpedit.msc**
6) Vyberte Konfigurace počítače -> Nastavení systému Windows -> Nastavení zabezpečení -> Zásady veřejných klíčů (Computer Configuration -> Windows Settings -> Security Settings -> Public Key Policies).
7) Klikněte pravým tlačítkem na Šifrování systému souborů (Encrypting File System) a zvolte Přidat Agenta obnovování dat … (Add Data Recovery Agent …).
8) U Výběru agentu obnovení (Select Recovery Agents) zvolte Procházet složky … (Browse Folders …) a lokalizujte soubor **racert.CER**, vytvořený dříve pomocí nástroje **cipher**, a potvrďte instalaci certifikátu.
9) Pokračujte dále a potvrďte vytvoření **Agenta obnovení** pomocí Dokončit (Finish)
   - Tento krok nevytvoří přímo **Agenta obnovení**, ale pomocí tohoto certifikátu bude zašifrován každý FEK jakéhokoliv souboru, který bude od tohoto okamžiku šifrován, tedy jakýkoliv uživatel vlastnící privátní klíč tohoto certifikátu se stane **Agentem obnovení**
10) Importujte certifikát **racert.PFX**, vytvořený dříve pomocí nástroje **cipher**
    - Importováním tohoto certifikátu získá uživatel **Student** privátní klíč certifikátu, kterým jsou zašifrovány všechny FEK a stane se tedy **Agentem obnovení**
11) Zkuste otevřít soubor **tajny.txt**.

- Obsah souboru nepůjde zobrazit, protože byl zašifrován ještě před vytvořením **Agenta obnovení**

12) Přihlaste se jako uživatel **Lisa** a spusťte příkaz **cipher /U**
13) Přihlaste se zpět jako uživatel **Student** a zkuste nyní otevřít soubor **tajny.txt**

- Nyní již soubor půjde zobrazit, protože nástroj **cipher** aktualizoval zašifrované soubory uživatele a doplnil zašifrované FEK pomocí klíče **Agenta obnovení**

LAB6 – Sdílení

V následujícím cvičení si ukážeme pokročilejší možnosti nastavení sdílení v MS Windows.

1) Přihlaste se na **win7-base** jako uživatel **Student.**
2) Vytvořte složku **C:\smlouvy**. Ve složce vytvořte soubor **sprava.txt**.
3) Na složce smlouvy otevřete **Vlastnosti** ->**Sdílení** -> **Rozšířené možnosti sdílení** (Properties -> Sharing->Advanced Sharing).
4) Zatrhněte **Sdílet tuto složku** (Shared this folder). Nastavte:
   - Název sdílené složky (Share name): **Firma**
   - Komentáře (Comments): **Firemní smlouvy**
   - Oprávnění (Permissions): **Everyone** povolit **Úplné řízení** (Allow Full Control)
5) Přihlaste se lokálně na **win7-domain** (uživatelské jméno **win7-domain\student**) a otevřete sdílený z průzkumníka zadáním UNC cesty \\win7-base\Firma
6) Vytvořte nové sdílení na složce smlouvy (opakuj krok 4), klikněte na tlačítko **Přidat** (Add) a nastavte:
   - Název sdílené složky (Share name): **data**
   - Oprávnění (Permissions): **Everyone** povolit **Úplné řízení** (Allow Full Control), **Administrators** odepřít **Číst** (Deny Read)
7) Ověřte, že účet patřící do skupiny administrators nemůže číst při přístupu ze sítě (účet Student).
8) Složku smlouvy nasdílejte jako skryté sdílení s názvem **tajne** (opakuj krok 4), klikněte na tlačítko **Přidat** (Add) a nastavte:
   - Název sdílené složky (Share name): **tajne$**
   - Omezit současný počet uživatelů na: **1**
   - Oprávnění (Permissions): **Everyone** povolit **Číst** (Allow Read)
9) Ověřte, že sdílení není viditelné v průzkumníku.
10) Zadejte plnou cestu a přistupte na skryté sdíleni.

LAB7 – Offline soubory

Cílem tohoto cvičení je zpřístupnit si obsah složky offline, ověřit dostupnost souborů ve složce a vyřešit konflikty.

1) Ve složce **C:\Smlouvy** vytvořte soubor **offline.txt** s obsahem **Version 1**
2) Přihlaste se lokálně na **win7-domain** (uživatelské jméno **win7-domain\student**) a otevřete sdílený adresář **Firma**.

3) Zakažte veškeré síťové adaptéry a zkuste otevřít soubor **offline.txt**
   - Soubor nebude možné otevřít z důvodu nedostupnosti cílového sdílení.
4) Povolte lokální síťový adaptér (**LAN2**) a obnovte (Refresh) sdílený adresář **Firma**.
5) Klikněte pravým na sdílený adresář **Firma** a zvolte Vždy přístupné offline (Always Available Offline), počkejte na dokončení synchronizace.
6) Opět zakažte veškeré síťové adaptéry a zkuste otevřít soubor **offline.txt**
   - Soubor nyní bude možné otevřít, jelikož je již uložen lokálně.
7) Změňte obsah souboru **offline.txt** na obou místech (Původní soubor i offline kopii)
8) Opět povolte lokální síťový adaptér (**LAN2**).
9) Otevřete vlastnosti (Properties) souboru **offline.txt** a přejděte na záložku Soubory offline (Offline Files).
10) Zvolte Synchronizovat nyní... (Sync now...).
11) Vyberte Zachovat obě verze (Keep both versions).
12) Ověřte, že adresář **C:\Smlouvy** nyní obsahuje obě upravené verze souborů.