Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra Informačních Technologií

Bakalářská práce

Mazání dat, nástroje, problematika mazání citlivých dat

Jan Komínek

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci Mazání dat, nástroje, problematika mazání citlivých dat jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 1.dubna 2011 _____

Poděkování

Rád bych touto cestou poděkoval RNDr. Dagmar Brechlerové, Ph.D. za podnětné názory a čas který mi věnovala.

Mazání dat, nástroje, problematika mazání citlivých dat

Deleting data, tools, problems deleting sensitive information

Souhrn

Má bakalářská práce obsahuje informace o technických aspektech mazání dat, shrnuje možnosti uložení dat na různá média. Taktéž uvádí dělení médií dle přepisovatelnosti a způsobu zápisu dat. Shrnuje a porovnává jednotlivé způsoby mazání dat v operačních systémech, likvidaci datových nosičů, mazání dat na internetu, z RAID polí, pamětí RAM a flash pamětí. Taktéž srovnává mazání celých disků s mazáním jednotlivých souborů. Popisuje i možnosti obnovení již smazaných dat. Stěžejní informace jsou obsaženy v kapitolách týkajících se bezpečnosti a mazání citlivých dat. V mé bakalářské praci jsem se zaměřil i na porovnání jednotlivých metod a nástrojů určených pro mazání citlivých dat. Práce obsahuje taktéž přehled všech hlavních metod a postupů pro mazání citlivých dat. V kapitole 4 jsem navrhl metodiku pro mazání menších objemů dat.

Summary

My Bachelor Thesis contains information about the technical aspects of erasing data, summarizes the various data storage media. It also divides media to written and overwritten. Summarizes and compares different ways of erasing data in operational systems, disposal of data media, erasing data on the Internet, RAID, RAM and flash memory. It also compares deletion of entire discs with deleting separate files. It also describes the possibility of restoring data which has been deleted. The core of information is contained in the chapter Safety and Deleting of sensitive information. In my thesis I have focused on comparing different methods and tools for deleting sensitive data. This Thesis also includes an overview of all major methods and procedures for deleting sensitive data. In Chapter 4, I describe a methodology for deleting small amounts of data.

Klíčová slova: Gutmannova metoda, Mazaní citlivých dat, Datové médium, Klasifikace citlivých dat

Keywords: Gutmann method, Deletion of sensitive information, Data medium, Clasification of sensitve infomation

Obsah

1. Úvod

Předmětem mé bakalářské práce je popsat problematiku mazání citlivých dat. Za mazáním dat stojí obvykle dva záměry. Jedním z nich je snaha zamezit úniku citlivých údajů mimo společnost, a to z důvodu jak ochrany osobních údajů, tak i citlivých firemních informací (zákon o ochraně osobních údajů 101/2000 Sb., zákon o utajovaných informacích 412/2005 Sb.….). Druhým důvodem je pak uvolnění místa na datovém nosiči. Mají-li být ochráněna citlivá data i v okamžiku odstranění datových nosičů, jak z důvodu předání do reklamací, vyřazení staré výpočetní techniky, je žádoucí v rámci společnosti přijmout bezpečnostní politiku, kdy by data byla ukládána na datové nosiče již šifrovaná. Již samotné ukládání dat v šifrované podobě má stále větší opodstatnění, protože je velká dostupnost mobilních zařízení a obecně klesá povědomí o způsobu a místu uložení citlivých údajů i mezi vedoucími pracovníky společností. Citlivá data mohou být součástí výstupních sestav, datových rozhraní, lokálně spravovaných databází, emailové korespondence, databázových instancí apod.

Dalším neméně důležitým aspektem je důsledné provedení výmazu dat a zde je potřeba zvážit provádění likvidace vlastními silami, respektive na zakázku. Při uvažovaném výmazu dat je potřeba přistupovat k IT technologii komplexně a nezaměřovat se jen na klasické datové nosiče, diskové jednotky, flash disky, či jiná paměťová media, ale nesmí se zapomínat i na další technologická IT zařízení, která mohou obsahovat citlivá data, jako jsou například paměťová média v tiskárnách, síťových prvcích, atd. Předmětem mazání jsou samozřejmě i bezpečnostní kopie dat ať na diskových polích, páskových archivech. I zde je po uplynutí archivační lhůty potřeba řešit výmaz dat. Mazání dat je tedy komplexní záležitost, která je ovlivněna řadou faktorů jako:

- Technologie zápisu
    - Elektromagnetická
    - Optická
- Forma zápisu
    - Trvalá
    - Přepisovatelná
- Citlivost údajů
- Souborový systém
    - Windows (FAT,FAT32, NTFS)

- Unix, Linux (EXT, EXT2, EXT 3)
- Novell (NVFS-všechny varianty, NSS)
- Mac OS (HFS, HFS+)
- OS/2 (HPFS)
- Palm OS

Pro výmaz dat existuje větší množství standardů pro odstranění údajů z datových médií a jejich použití je dáno citlivostí dat. Citlivost dat je dána klasifikací. V ČR je citlivost dat definována pomocí standardu (zákon o utajovaných informacích 412/2005 Sb., zákon 101…)[1].

DoD 5220.22M byl definován ministerstvem obrany USA. Soubory musí být přepsány trojnásobně - poprvé náhodnými hodnotami, podruhé hodnotami opačnými k hodnotám náhodným a potřetí zcela novými náhodnými hodnotami.

Standard NATO požaduje sedminásobný přepis. Šestkrát se střídají hodnoty 00 a FF, posedmé se zapisují hodnoty náhodné.

VSITR standard také požaduje sedminásobný přepis. Šestkrát se střídají hodnoty 00 a FF, posedmé se zapíše hodnota AA.

Algoritmus Bruce Schneiera doporučuje sedminásobný přepis. Nejprve 00, poté dvakrát FF a zbytek náhodnými hodnotami.

Samozřejmě existuje ještě mnoho dalších standardů, které požadují až 35násobný přepis[2].

2. Cíl práce a metodika

Cílem mé bakalářské práce je seznámení s dostupnými metodami a nástroji pro mazání citlivých dat. Za zásadní v mé práci považuji popis problematiky mazání citlivých dat. Práce přináší ucelený souhrn dané problematiky s ohledem na způsoby uložení dat a typy datových nosičů.

Pro zpracování jsem zvolil metodu literární rešerše. Nejprve jsem se zaměřil na způsoby uložení dat, typy datových médií a důležité technické aspekty. V následující části jsem popsal přehled existujících metod a nástrojů pro mazání citlivých dat. V kapitole 4. jsem navrhl metodu pro mazání menších objemů dat, tedy jednotlivých složek a souborů.

3. Literární rešerše

3.1. Technické aspekty

3.1.1. Koercivita

Koercivita též zvaná koercivní síla. Je to schopnost permanentního magnetu odolávat demagnetizaci externím magnetickým polem a také svým vlastním demagnetizačním polem. Rozlišujeme dva typy koercivity:

- „skutečná“ koercivita, jednoduše zvaná „koercivita“ - znamená magnetické pole, při kterém je celková indukce v magnetu nula.
- „vnitřní“ koercivita - znamená pole, při kterém je celková polarizace nula (vektory polarizace individuálních magnetických domén se vzájemně ruší).

Koercivita se udává v Oerstedech, což je jednotka ze systému CGS (systém jednotek zavedený roku 1874 Britskou Asociací Pokroku ve Vědě) pro intenzitu magnetického pole. 1 Oersted = 1000/(4*π) A/m. Pro praktické užití se dá její velikost vykládat jako obtížnost úplného výmazu dat z magnetického media, tj. čím vyšší je velikost koercivity pro dané magnetické médium, tím více se musíme věnovat zabezpečení jeho výmazu[3].

Přehled některých medií	
3.5“ 1.44MB disketa	700 Oe
HDD před rokem 1980	900-1400 Oe
HDD po roce 1980	1400-2200 Oe
½“ magnetické pásky	300 Oe
DAT pásky	1500 Oe

Tabulka 1. – přehled koercivity medií[3]

3.1.2. CRC - Cyclic Redundancy Check

CRC je hašovací funkce sloužící ke kontrole konzistence uložených či přenesených dat. Pro data před uložením či přenesením je spočítán CRC a přidán k přenášeným datům, či je uložen spolu s daty na disk. Při další aktivitě s daty je spočítán CRC nezávisle a porovnán s uloženým či připojeným kontrolním součtem. Pokud se liší, je zjevné, že data

byla poškozena. Pro detekci úmyslného pozměnění souboru je tento nástroj příliš slabý, dva soubory mohou mít stejný CRC, aniž mají stejný obsah. Porovnáváme pouze se součtem původního souboru, kdy je shoda v případě náhodného poškození vysoce nepravděpodobná[4].

3.1.3. Degauser

Degauser je zařízení sloužící k odmagnetování magnetického média. Pro dané médium je známa schopnost odolávat odmagnetování - tzv. koercivita. Bezpečnostní standardy udávají, jak velké pole musí působit pro certifikované vymazání daného datového nosiče. V současné době se používají degausery o výkonu cca 12000 Gaussů. Při skartaci dat pomocí odmagnetování narážíme na problém s poškozením továrních údajů. Zvláště u pevných disků pak dochází k takovému poškození, že již není možné jejich další užití. Pro pevný disk je tato metoda i metodou fyzické likvidace. U pevných disků je dalším problémem i samotný obal disku, který slouží jako stínění a pro větší jistotu je lepší odmagnetovávat přímo fyzicky vyjmuté diskové plotny, místo celých disků i s obalem, jelikož ten nenese žádné informace a dá se likvidovat odděleně. I pokud bychom nezničili disk při rozebírání, po odmagnetování je již nepoužitelný a tak je jen velmi tenká hranice mezi odmagnetováním a likvidací disku. Záleží pouze na finančních možnostech vlastníka příslušného hardware, zda použije odmagnetování, či fyzicky zničí disk. Samozřejmě při kombinaci více metod se šance na obnovení dat neustále snižuje[5,6].

3.2. Způsoby uložení dat

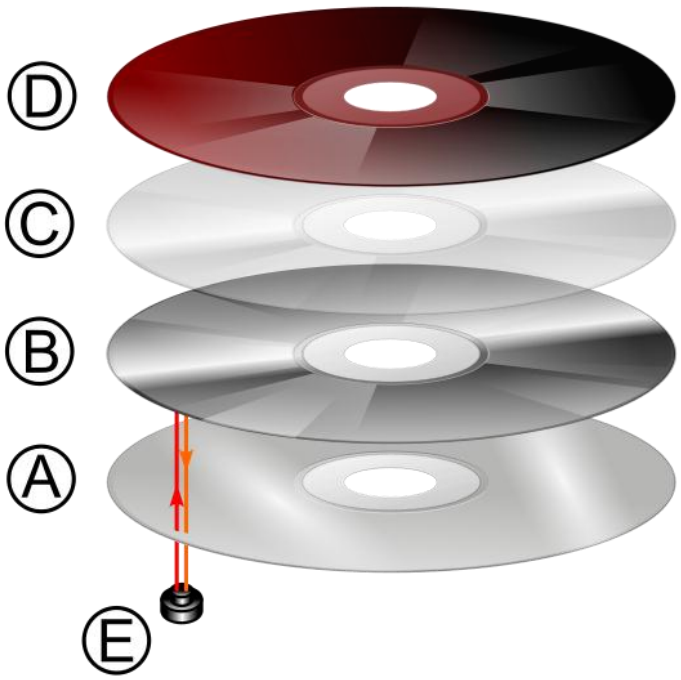
Pro pochopení problematiky mazání dat je nutno nejprve nastínit způsoby jejich uložení. Ne všechna datová média však umožňují jiný než destruktivní způsob odstranění obsahu. Datová média můžeme dělit podle fyzikálních principů, na nichž fungují na tři základní typy:

- **Optická** - CD, DVD, Blue ray, HD DVD
- **Magnetická** – HDD, disketa, pásky (například WHS,DAT)
- **Elektronická - flash paměť** – paměťové karty, USB flash disky [7]

3.2.1. Způsob zápisu dat na disk CD/DVD

Pro zápis na optické disky používáme laseru. Jednotlivé vrstvy CD jsou uspořádány z pohledu laseru následovně: první vrstvou je průhledná ochranná vrstva (na obrázku č.:1. je označena A), následuje neodrazivá vrstva B. Třetí v pořadí je odrazivá vrstva C. Vrstva D je ochranná vrstva, bránící mechanickému poškození datového nosiče. Při vypalování dat se laserovým paprskem odstraní vrstva B, která pohlcuje laserové záření a vznikne tak bit obsahující jedničku. Pokud zanecháme vrstvu B na svém místě, dojde při čtení k pohlcení paprsku a čteme tak 0.

Dle popisu principu zápisu DVD a CD se dá velice snadno navrhnout metoda jejich ničení. Pokud odstraníme odrazivou a neodrazivou vrstvu, dostaneme nosič bez informací. Při tomto postupu se snažíme o maximální fyzickou destrukci těchto vrstev. U přepisovatelných optických medií můžeme tento postup vylepšit o prvotní smazání souborů z disku pomocí laseru. Dochází tak k obnově nosiče do továrního stavu, kdy by neměl obsahovat žádná data. Nesmí se ovšem jednat o takzvaný rychlý výmaz, kdy je přepsána pouze úvodní sekce s hlavičkami. Při úplném formátování disku dochází k přemazání všech bitů na optickém disku[9].



Obrazek 1. – skladba CD/DVD[8]

3.2.2. Přepisovatelná a nepřepisovatelná média

Základní fyzikální rozdělení (optická, magnetická a elektronická) nicméně nedokáže identifikovat média, které lze použít k opětovnému zápisu dat. U medií bez možnosti dalšího zápisu je nejefektivnějším řešením fyzická likvidace média, vyjma

případů, kdy cena likvidace převyšuje potencionální ztrátu při úniku obsažených dat. U nepřepisovatelných médií je však ve většině případů jejich likvidace otázkou jednoduchého použití síly – např.: CD/DVD – stačí seškrábat a následně zlikvidovat povrch obsahující uložené informace, magnetické pásky se dají odmagnetovat. Oba popsané druhy médií nevydrží větší teplotu bez úplné destrukce.

U přepisovatelných médií v zásadě rozlišujeme výmaz dat a výmaz souborů. Výmaz souborů znamená pouhé odstranění informace o uložení na disku. Z pohledu operačního systému dojde k uvolnění místa na disku, nicméně data zůstávají na disku. Při výmazu dat dojde k výše popsanému procesu, navíc je proveden jejich fyzický přepis bit po bitu, kdy je každá hodnota nahrazena výchozí či náhodnou hodnotou. Takto odstraněná data je již velmi obtížné obnovit – pro jejich obnovení musíme rozpoznávat jejich magnetický obtis, což je zbytkový obraz původních dat uložených na disku.

Pro samotné mazání dat ve většině používaných systémů dojde k jedné z následujících akcí – přesunutí souborů do „koše“, kdy nedochází k fyzickému odstranění dat z disku, pouze nejsou dostupná přes původní lokaci – jsou přesunuta ve speciálním adresáři. Druhou nejčastější akcí je pouhé označení sektorů, v nichž se nacházel soubor, jako prázdné – dochází tak k recyklaci místa na disku. Pro uvolnění místa je tato akce více než dostatečná. Pokud však bylo naším cílem zlikvidovat data, je tento postup nedostatečný. Již poměrně jednoduché programy a postupy jsou schopné takto smazaná data obnovit. Takto jednoduchý postup obnovy je však možný jen po časově omezenou dobu, ta není vždy stejně dlouhá. Jde o časový úsek mezi změnou označení sektoru z obsazeného na prázdný a fyzickým zaplněním sektoru novými daty. K fyzickému přepsání sektoru může dojít během několika sekund, ale i během několika týdnů. Až do fyzického přepsání informací se dá zajistit jejich přečtení poměrně jednoduchými nástroji[10].

3.2.3. Systémy souborů

Pro mazání je podstatné i samotné uložení dat, téměř každý operační systém má svůj souborový systém a je nutno toto brát v potaz při implementaci nástrojů na bezpečné mazání dat. Pro klasické mazání není nutno příliš brát v úvahu rozdíly v souborových systémech, krom odlišností v konkrétních příkazech pro mazání. Mezi nejrozšířenější systémy na osobních počítačích patří Windows, Linux/UNIX a MAC OS. Používají

rozdílné souborové systémy i formátování disků, nejčastěji se dnes setkáme s FAT32, NTFS, HFR, EXT, EXT2, EXT3.

Souborový systém je způsob ukládání dat na médium, kterým je ve většině případů pevný disk. Data jsou organizována do souborů a ty se pak organizují do adresářů. Mimo souborů může obsahovat i na první pohled jiné objekty (metadata, i-uzly a jiné), ve skutečnosti jde však opět o soubory[11].

3.2.3.1. Unixový souborový systém

Unixový souborový systém je připojen do adresáře, buď do jiného souboru systému, či přímo do kořenového adresáře značeného /. Můžeme zde nalézt tři druhy souborových systémů:

- Lokální - EXT2,XFS….
- Síťový - NFS, AFS, SAMBA
- Virtuální - /proc, /sys, devfs

Základem jsou lokální systémy a těmi se budeme dále zabývat. Lokální souborový systém pracuje na blokovém zařízení, ve většině případů se jedná o pevný disk. Na tomto záznamovém zařízení najdeme v různých podobách tyto položky:

- Hlavička souborového systému
- Seznam volných bloků
- Hlavičky souborů - i-uzly (i-nodes)
- Adresáře
- Vlastní data souborů
- Případně i tzv. Žurnál (viz. Seznam pojmů).

Základem jsou takzvané i-uzly, každá položka adresáře je svázána s tímto uzlem. Jedná se o datovou strukturu obsahující metadata – práva, vlastník atd. a seznamy, které popisují umístění souboru na disku. Tyto seznamy obsahují seznam adres bloků souboru a mohou být použity k efektivnějšímu mazání dat. Adresáře jsou v podstatě soubory, které obsahují seznam jmen souborů a čísel jim příslušejících i-uzlů. Při vyhledávání souborů je pak nutno v nejhorším případě přečíst všechny položky adresáře. Vyhledávání je možno implementovat i pomocí hašovací tabulky (viz. Slovník pojmů), či vyhledávacího stromu (viz. Slovník pojmů). Obě zmíněná vylepšení zjednodušují i implementaci mazání dat[12].

3.2.3.2. Souborový systém NTFS

Naproti tomu NTFS je odlišným souborovým systémem, který je spjatý s WINDOWS. Známe ho už z Windows NT, posléze se rozšířil i do domácích instalací a dnes je zcela ekvivalentní FAT32. Tento souborový systém je postaven přímo na atributech souborů. I obsah souboru je vlastně jeho atributem. Téměř všechny datové struktury tohoto systému jsou reprezentovány pomocí souborů. Například bootsektor disku je reprezentován jako soubor v seznamu souborů. Všechny soubory jsou udržovány v seznamu souborů. Atributy těchto souborů můžeme najít buď přímo v tomto seznamu, nebo je nalezneme pomocí odkazů na jiných místech disku. Při alokaci volného místa dochází k zachování většího prostoru kolem některých datových struktur (je to zřejmě výsledkem snahy o zvýšení výkonu). Tento prostor je však zmenšen v případě nedostatku místa pro běžná data. Jak již bylo zmíněno, systém byl původně vytvářen pro Windows NT, ale tento systém jej nedokázal plně využít. Větší využití tohoto systému souvisí s rozšířením systémů určených pro běžné uživatele s podporou NTFS [13].

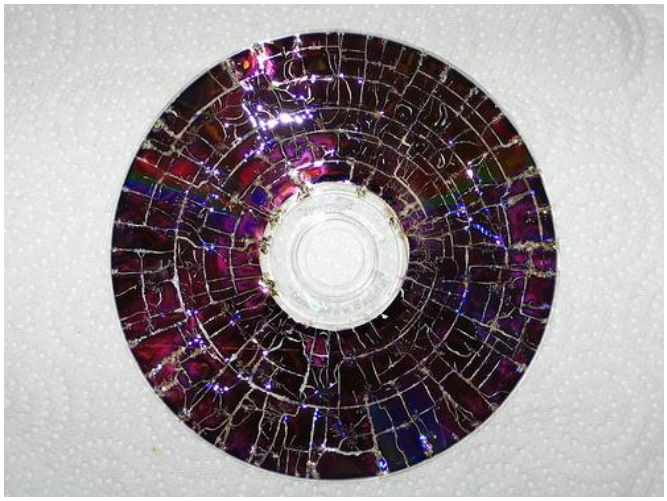
3.2.3.3. Souborový systém FAT, FAT32

Souborový systém FAT se výrazně podobá Unixovému souborovému systému, nemá ale i-uzly. Ty jsou nahrazeny umístěním do položek adresáře a v období bitmapy volných bloků, kterou nazýváme File Allocation Table. Z této alokační tabulky vznikl i celý název souborového systému, jedná se o seznam všech bloků, kde každá položka obsahuje buď informaci o následujícím bloku, nebo hodnotu označující konec souboru, nepoužitelný blok nebo prázdný blok. Při poškození této tabulky nejde souborový systém připojit, či začne způsobovat problémy. Systém FAT32 se od FAT liší v maximální velikosti souboru a maximální velikosti, na kterou lze formátovat pevný disk. Ve FAT je možné uložit soubor o velikosti až 2GB a naformátovat disk o velikosti až 4GB. Fat32 umožňuje uložit soubory o velikosti až 4GB a naformátovat disk o velikosti až 2TB[14].

3.3. Principy mazání dat

3.3.1. Destruktivní ničení datových nosičů - mimo HDD

U optických médií cena poklesla natolik, že nemá smysl se zabývat přepisovatelnými nosiči a tedy výmazem jako takovým. Zvláště pak u DVD a CD nosičů je nejjednodušší varianta jejich fyzická likvidace. Samotný nosič se skládá z polykarbonátového disku, datové vrstvy, vrstvy s potiskem a svrchní ochranné vrstvy. Při zápisu/čtení se laserový paprsek dostává skrze polykarbonátový disk a odráží se od datové vrstvy, kde dochází k odrazu v případě čtení nebo ke změně struktury v případě zápisu. Pro fyzickou likvidaci nás tedy zajímá pouze tato datová vrstva, ostatní mohou být vyhozeny do běžného tříděného odpadu. Jelikož jde o mechanickou formu zápisu, tak pro základní ochranu stačí disk zlomit, pro vyšší úroveň bezpečnosti existují skartovače CD a DVD, které médium rozřežou na malé kousky. Už samotným řezáním se ztratí obrovské množství informací. A samotné kousky jsou velice špatně čitelné, pokud vůbec. Odtržením datové vrstvy se poškodí ještě více a obnova dat je téměř nemožná. Mezi domácí postupy likvidace patří i zničení média v mikrovlnné troubě, kdy dochází k totální destrukci. Ovšem je nutné si uvědomit, že jde o riskantní způsob z hlediska možného zničení přístroje [16].



Obrázek 2. – CD po použití mikrovlnné trouby[15]

3.3.2. Mazání dat z flash pamětí a pamětí RAM

Každý typ média má specifické uložení dat a stejně tak je i specifický způsob jejich bezpečného mazání, u pamětí typu RAM bude stačit nechat dostatečně dlouho odpojené napájení. Při běžné teplotě to jsou řádově minuty, pokud by však teplota výrazně poklesla, je možné přečíst obsah paměti i po hodinách až dnech. Problém nastává v dnešní době především s nástupem paměťových karet, SSD disků a jim podobným zařízením, kdy již není možné aplikovat metody jako je odmagnetování. Jedinou možností krom fyzické likvidace disku je opakovaný přepis celého disku. U paměti typu RAM můžeme prodloužit

či zkrátit dobu uchování informace pomocí snížení či zvýšení teploty. Například při teplotě kolem -60°C se dají data přečíst i v rámci horizontu týdne a při teplotě 140°C je s jistotou nečitelná už v řádu minut. Čím nižší teplotě je vystavena paměť RAM tím déle trvá její paměťový efekt. Tedy jak již bylo zmíněno, může v paměti RAM zůstat i déle než několik hodin [17,18].

3.3.3. Mazání dat v internetu, RAIDu…

Zvláštním případem je mazání dat ve sdílených sítích, kdy smazat data na jedné lokaci je problém se stejnou obtížností, jako smazat data na osobním počítači. Jiný případ ovšem nastává při snaze smazat informaci, která se může šířit samovolně. Typickým případem je dokument umístěný na internet. Každým přenosem tohoto souboru z úložiště ke koncovému uživateli se násobí počet lokací, přes něž prošel a tím i potencionální počet míst, kde zůstane uložen. To vše za předpokladu, že není šířen ještě záměrně na další lokace uživateli, i bez této pomoci se šíří lavinovitě a po vypuštění je téměř nemožné ho ze všech míst průchodu odstranit a daří se tedy pouze dílčí odstranění. Jedinou spolehlivou metodou je do takto sdílených sítí nevypouštět soubory, jež bychom nechtěli distribuovat, případně je alespoň před odesláním zašifrovat.

Další problematiku představuje mazání v RAIDových polích (viz Slovník pojmů), kdy je nutno počítat s principem RAIDu. RAID je stavěn s maximálním důrazem na zachování dat a snaha o jejich úplný výmaz jde přímo proti tomuto principu a je tedy nutné podniknout více operací než při mazání na izolovaném disku. Pokud není třeba již mít RAID k dispozici, zjednodušíme problém rozebráním disků a přepisem každého zvlášť. V případě mirroringu stačí dokonce přepisovat jeden disk a další budou přepisovány jako jeho identické kopie. V případě nutnosti zachování dat uložených na RAIDu vyvstává problém, jak jednoznačně zjistit, kde je ten který soubor na discích uložen. Jedna z možností je dočasně vypnout RAID, smazat všechny výskyty daného souboru a pak několikrát přepsat uvolněné místo. Většinou se toto neřeší až do doby, kdy se některý z disků či celý RAID vyřazuje a v tomto případě se postupuje stejně jako u běžného pevného disku. RAIDová pole jsou uložena v serverových místnostech, což je nejvíce střežená místnost v rámci počítačové sítě a případná ztráta kontroly není pak již riziková z pohledu smazaných souborů, ale z hlediska ztráty stále uložených informací [19].

3.3.4. Mazání celých disků x jen některých dat, problematika magnetického otisku a jiné technické aspekty

Při mazání disku se setkáváme s problémem, který pro nás představují špatné sektory disku.

Mezi aspekty, které ovlivňují náročnost vymazání dat, můžeme počítat:

- Délku existence záznamu na magnetickém nosiči. Pokud skladujeme magnetické pásky při zvýšené teplotě, či po dlouhou dobu s jedním záznamem je téměř nemožné spolehlivě smazat tato data. Pro určení není směrodatné stáří média, ale záznamu. V podstatě stejné vlastnosti bude vykazovat dva roky starý disk a nově koupený, pokud na oba zapíšeme data ve stejnou dobu.
- Závislost na teplotě zápisu. Pokud je během zápisu menší teplota a koercivita je tak velmi nízká, dojde k velmi trvanlivému zápisu do datového média. Pří následném pokusu o přepsání při vyšší teplotě a výrazně vyšší koercivitě je pak mnohem obtížnější permanentně přepsat všechna data. Toto je velmi důležité u pevných disků, kde dochází k zahřívání provozem. Pak je třeba sledovat čas běhu disku, případně dobu kdy probíhala aktivita u disků s podporou úspory energie.
- Dalším problémem jsou samoopravné kódy a error kódy na disku, pomocí nichž je možno obnovit již vymazaná data. Jedná se především o **ECC – error correction code.** Typický disk má 512 bytů dat, 4 byty CRC a 11 bytů ECC na jeden sektor, díky tomu mohou být obnovena i data, jež byla spolehlivě smazána, pro větší pravděpodobnost úplného výmazu dat je nutno mazat i opravné kódy, především ECC[2].

Jak uvádí Peter Gutmann[2], nejlepším způsobem, jak bezpečně smazat data, je zabezpečit, aby se nikdy nezapsala na disk. Kupříkladu klíč pro šifrování se může dostat na disk při výpisu chyb v paměti, tedy i data, o nichž si myslíme, že již dávno na disku nejsou, se zde mohou při podrobném zkoumání objevit. Mnohem horší situace však může nastat, když jsou tato data stránkována přes síť a téměř kdokoliv na síti je může odposlechnout a uložit. Pro předcházení takovýmto situacím je možno zamezit stránkování na disk či přes

síť. Po provedení defragmentace disku dojde k přepsání prázdných – tj. již smazaných míst ať již částečně či úplně. Při částečném přepisu dojde k narušení souvislosti těchto oblastí.

I při používání základního příkazu **Delete** můžeme snížit naději na obnovení dat okamžitým provedením defragmentace disku. Plánovanou defragmentaci můžeme provádět periodicky, kdy sice zůstane disk relativně zranitelným mezi smazáním a defragmentací, ale zkrátíme pravděpodobný čas přepisu daných sektorů. Nicméně i tak nejde o sofistikovaný nástroj, ale spíše o náhradu z nouze. Největším problémem je nepředvídatelnost tohoto procesu. Například dojde-li k odmazání souboru v celku, tak nemusí v extremním případě dojít k přepisu dané oblasti. Sice není pravděpodobnost takové situace veliká, ale jakmile dovolíme vstup náhody v oblasti bezpečnosti, tak se blížíme stavu, kdy daná bezpečnostní politika přestane být účinná. Defragmentaci je vhodné provést po každém vymazání citlivého souboru, čím více byl soubor fragmentován, tím větší je i efektivnost defragmentace jako nástroje pro zamezení obnovení dat.

3.3.5. Mazání dat v prostředí Windows

V prostředí Windows je nejčastěji užívanou funkcí pro výmaz dat **odstranit (delete)**, tato funkce však neslouží k výmazu dat v pravém slova smyslu. Po provedení příkazu/nabídky **odstranit (delete)** dojde k přesunutí souboru do koše, ale fakticky na data dále existuje ukazatel. Tento ukazatel není však již běžně přístupný z původní adresářové lokace. Tento stav jde vrátit zpět do výchozího stavu. Teprve při použití nabídky **vysypat koš** dojde k výmazu ukazatele na daný soubor/složku, do té doby se při přesunu dat zpět na disk neprovádí obnovení souboru v pravém slova smyslu.

Při užití klávesové zkratky **Shift+Delete** dojde k vymazání ukazatele na daný soubor/složku. Při pokusu obnovit takto smazaná data je nutno využít speciální nástroje. Na internetu je možno nalézt nepřeberné množství těchto programů. Obě popsané metody se však hodí maximálně k uvolnění místa na disku, první z nich dokonce místo ani neuvolní, pouze není soubor na první pohled vidět. Použití **Shift+Delete** je často mylně pokládáno za dostatečné odstranění dat z pevného disku, nicméně teprve fyzickým přepisem dat dojde k nečitelnosti dat na disku pomocí softwarových nástrojů. Tento přepis však již není standardní součástí funkcí systému Windows.

V souvislosti se zmíněnými funkcemi je vhodné uvést též rozdíl v mazání dat a v mazání souborů. Celá řada uživatelů si pod těmito dvěma pojmy představí téměř totéž. Základní rozdíl je však větší, než se může na první pohled zdát a je pomyslným předělem mezi mazáním užitým pro uvolnění místa a tím, které již přináší alespoň minimální ochranu před zneužitím dat, jež se vyskytovala na daném disku. K mazání souborů se užijí dvě výše popsané funkce, mazání dat vyžaduje již sofistikovaný postup v podobě výmazu každého bitu daných dat. Každý jednotlivý bit je pak nastaven na náhodnou hodnotu. Tímto postupem se zamezí softwarové obnově dat, jakákoliv další obnova je již možná pouze pomocí analýzy analogového signálu a je nutný fyzický přístup k pevnému disku[20].

3.3.6. Porovnání efektivnosti mazání x zničení HDD

V této a dalších kapitolách se budeme věnovat mazání dat pouze jako nástroji pro zabezpečení úniku citlivých informací. V tomto úhlu pohledu se jeví zničení pevného disku jako alternativa k odstranění dat. Fyzická likvidace datového nosiče přináší téměř stoprocentní jistotu zničení dat – výjimky tvoří neodborně provedené likvidace – ať již záměrně, kdy místo znehodnocení
hardware dochází k jeho rozprodeji, nebo nedodržením technologického procesu či selháním lidského faktoru. U optických médií je likvidace poměrně jednoduchou záležitostí, kterou zvládne každý doma. Pro odstranění dat z nich stačí seškrábat datovou vrstvu a případně zničit ohněm, vrstvu zničit na malé kousky atd. U magnetických pásek a disket se dá provést tzv. demagnetizace – jelikož je nosné médium volně přístupné, tak i tento proces lze provést i v improvizovaných podmínkách. Fyzické zničení nosné vrstvy se dá provést pomocí běžně dostupných ostrých nástrojů. Jiná situace nastává při pokusu o fyzickou likvidaci pevného disku, u klasického HDD se dá s úspěchem použít opět klasická hrubá síla – prezentovaná například úhlovou bruskou – kdy se odstraní horní vrstvy jednotlivých diskových ploten a naprosto se tak

Obrázek 3. – degauser[23]

znemožní jakákoliv analýza média a případná záchrana dat, či jejich zneužití. V porovnání s pouhým smazáním přináší likvidace zvýšení obtížnosti případného čtení dat z daného média, nejlepší je samozřejmě kombinace obojího. U dat kategorie C4 (více v kapitole 3. 3. 10), které mají přímý dopad na společnost, se dá předpokládat likvidace média jako jediné východisko nakládání s vyřazovanými médii. Tento přístup se však dá uplatnit pouze v případě likvidace celého média. Není příliš vhodný pro průběžné mazání dat – výjimku tvoří data takové důležitosti, jejichž případná ztráta, či škoda způsobená zneužitím, je neporovnatelná s cenou disku. Pro domácí užití a menší firmy tedy tento postup nepřichází v úvahu, naopak u velkých společností se v interních předpisech setkáváme s nařízeními o likvidaci disku místo reklamace – pokud obsahuje nebo obsahoval data kategorie C2 (více v kapitole 3. 3. 10). Nemluvě o likvidaci veškeré výpočetní techniky pomocí specializovaných firem – dodržujících normy a certifikáty NBÚ, ISO 9001, ISO 14001 a ISO 27001[1]. Bohužel stále ne všechny firmy dbají důsledně na tyto postupy a ne všechny mají implementované i interní kontrolní mechanismy. Likvidace má jako taková smysl pouze tehdy, je-li důsledně provedena. Při požadavku na minimalizaci rizika úniku dat z vyřazených médií opouštějících kontrolovaný prostor, pak vede ke spolehlivějším výsledkům v porovnání s výmazem[22].

3.3.7. Mazání dat v Unixu

Podobně jako v systému Windows zde existuje příkaz pro jednoduchý výmaz, tedy uvolnění místa, tím je **rm**. Příkaz **rm** způsobí, že **i-uzly**(viz Slovník pojmů) odkazující na soubor, jsou uvolněny, ale soubor samotný existuje na disku dále. Pro obnovu takto smazaných dat stačí vzdálený přístup k datovému médiu, není tedy nutno pronikat ochranou budovy, krást médium. Pro obnovu stačí použít nástroje jako je **unrm** nebo **lazarus** a ve většině případů se obnova podaří. Tento postup je opět omezen možností náhodného přepsání dat, tedy čím dříve po smazání se útočník k disku dostane, tím je větší jeho šance na obnovu dat – nebereme v potaz absolutní čas, ale čas strojový (není důležité, kolik času stráví disk v PC, ale jak dlouho PC je zapnutý a tedy je vystaven riziku přepsání dat).

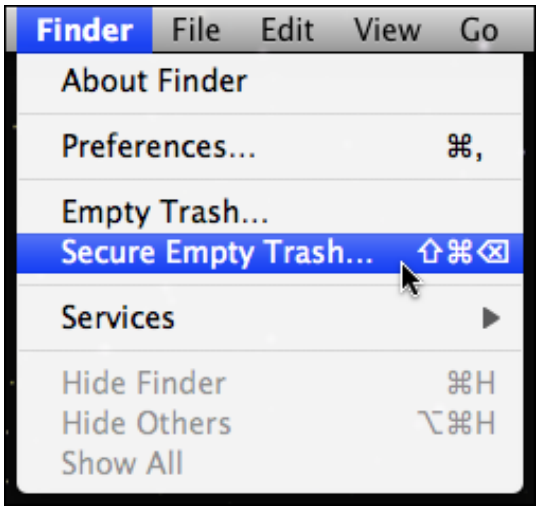
Dalšími příkazy pro smazání by se daly nazvat **mkfs** a **newfs**. Slouží k vytvoření nového Unixového souborového systému, v podstatě je to něco jako příkaz formát. Ve

skutečnosti nesmaže žádná data, ale pouze definuje strukturu souborového systému pro operační systém. Jednou z nevýhod je to, že smažeme v podstatě data na celém oddílu (viz. Slovník pojmů) v jeden okamžik a stejně tak i to, že podobně jako u **rm** se dají použít nástroje **unrm** a **lazarus** k obnově dat.

Poslední možností tak zůstává příkaz pro formátování disku, každá distribuce unixu/linuxu má buď obecně užívaný, nebo svůj nadstavbový nástroj – například **Solaris** má **format utility.** Tyto příkazy provedou kontrolu celého disku, označí špatné sektory a všechny sektory přepíší, díky tomu již není možné použít jednoduché nástroje jako je **unrm** a **lazarus**. Pro další získání je nutno použít již MFM nebo STM. Stále zůstává nevýhoda mazání celého média najednou, nicméně v porovnání se zničením, je to stále akceptovatelné. Pro běžné užití je to dostatečná metoda, jde v podstatě o implementaci dále popisované tzv „Rychlé metody výmazu“[2].

3.3.8. Mazání v Mac OS

Dalším poměrně rozšířeným operačním systémem je MAC OS, tento systém stejně jako oba předchozí, nabízí funkci smazání. Při standardním smazání dojde k přesunutí souboru do „odpadkového koše“ a následně při vyprázdnění dojde k smazání pointeru na tento soubor. Opět se dá použít celá řada nástrojů pro bezpečné odstranění, stejně jako ve výše jmenovaných systémech. Ovšem v Mac OS se vyskytuje i možnost bezpečného smazání dat z „odpadkového koše“, kdy se přes data přepíšou náhodná data. Jde sice o jeden přepis, nicméně je to zdaleka nejlepší přímo vestavěný nástroj. Mac OS skýtá možnost nastavit defaultně toto bezpečnější mazání, případně se dá pouze vybrat u souborů, u nichž chceme minimalizovat riziko obnovení[22].



Obrázek 4. – „odpadkový koš“ Mac OS[23]

3.3.9. Možnosti obnovení smazaných dat

Mnoho uživatelů se domnívá, že stačí data smazat, či zformátovat disk a veškerá data, jsou navždy zničena. Tento fakt dokládá i několik praktických studií, kdy se skoupí řada disků z aukčních serverů a provede se jednoduchá analýza a obnovení dat – provádí se pouze základní obnova tj. pouze pomocí software. I tak však často dochází k objevení minimálně citlivých, ne-li tajných informací. Mezi nalezenými informacemi jsou nejčastěji PIN od kreditní karty, údaje od účtu apod. Výjimečně se daří získat i tajné vládní dokumenty.

Při prohledání internetu je snadné nalézt celou řadu firem nabízejících obnovu dat z datových médií. Většinou je jejich nabídka omezena na obnovení poškozených či omylem smazaných medií. Nikdo neposkytuje obnovu záměrně vymazaných nosičů, kdy dojde k jejich výmazu pomocí dále popsaných metod. Největší nebezpečí tak představují nedůsledně smazaná data - kdy není dodržen předepsaný postup a data jsou pouze zformátována rychlým formátováním, či dokonce je disk pouze označen jako vymazaný.

Často zmiňovaný je například výzkum realizovaný studenty Massachusetts Institute of Technology (MIT) z roku 2002[24]. Ze 158 pevných disků získaných z různých bazarů, hromadných výprodejů velkých firem a dalších podobných zdrojů hned 28 disků obsahovalo zcela nesmazaná data, 60 % testovaných disků bylo sice zformátováno, ale jen necelých 10 % z celkového počtu bylo opravdu bez dat. Z 90 % disků se tedy nějaká data získat dala. Studenti MIT tehdy na discích našla spoustu opravdu zajímavých dat, např. hesla, pornografii, lékařské zprávy, osobní a firemní data, e-maily apod. Kardinální úlovek představoval pevný disk z bankomatu, který obsahoval soubor s kompletním výpisem výběrů (časy, data, čísla karet, částky apod.) za celý rok provozu.

V Unixu pro záchranu dat můžeme využít takzvaný **The Coroner's Toolkit (TCT)**. Jde vlastně o balíček nástrojů pro administrátory, který obsahuje mimo jiné nástroje **unrm** a **lazarus**. Pomocí **unrm** se přistupuje k nealokovaným diskovým oblastem a ty jsou jako surová data překopírována do výstupního souboru. Následuje analýza těchto dat pomocí **lazarus**u a jejich rekonstrukce. Lazarus je nejčastěji užíván se souborovými systémy FAT32, EXT2, UFS a NTFS (viz. Slovník pojmů), nicméně je použitelný s jakýmkoliv

souborovým systémem. Původně zamýšlené určení těchto nástrojů bylo na pomoc administrátorům, při hledání souborů, které mohl útočník smazat, aby zahladil stopy. Nicméně, to co může použít administrátor, může použít i útočník k obnovení dat smazaných úmyslně. Vzhledem k poměrně jednoduché obsluze je tento nástroj o to nebezpečnější[25].

3.4. Bezpečnost a dopady v případě ztráty dat

Problém mazání citlivých dat spadá do oblasti nazývané počítačová bezpečnost. Větší firmy mají vlastní procesy řízení rizik a tedy i počítačové bezpečnosti. Pro posouzení rizik spojených s užíváním počítačů je nutné především znát potencionální hrozby. Tedy to, jak velkou škodu může způsobit únik dat. Například DVD disk, obsahující platové výměry společnosti o několika desítkách zaměstnanců, který unikne mimo společnost, způsobí řádově menší škodu, než adekvátní údaje z nadnárodní společnosti.

Z tohoto důvodu je velice důležité zaměřit se na bezpečné nakládání s daty a datovými nosiči. Obzvláště s těmi nosiči, které jsou určeny k likvidaci, či prodeji. Pro firmu může mít ztráta i jednoho disku nedozírné následky. Nehrozí pouze přímé finanční ztráty, naopak tyto ztráty nejsou zdaleka největší. V celé řadě případů je hlavní ztráta reputace, důvěryhodnosti atd. Pro peněžní ústavy je naprosto stěžejní si právě tyto vlastnosti udržovat ve vztahu ke klientům.

Ve své praxi jsem se setkal s firmou, která měla založený byznys na vlastnictví obrovské databáze. Tato databáze ji jednoznačně zvýhodňovala před všemi konkurenty na trhu a vytvářela z ní téměř monopol. Na rozdíl od výše zmíněného se nevěnovala dostatečná pozornost zabezpečení dat a došlo k jejich úniku na nesmazaném disku, který obsahoval téměř celou databázi. Tím, že se k této databázi dostala konkurence, ztratila firma výhodu na trhu a přišla o více než 50% svých zákazníků. Tento případ uvádím pouze pro ilustraci toho, jak důležité je nakládání s daty.

3.4.1. Klasifikace citlivých dat

Národní bezpečnostní úřad na svých internetových stránkách uvádí odkaz na zákon, v němž je uvedena tato klasifikace utajovaných skutečností:

a) Přísně tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky.

b) Tajné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky.
c) Důvěrné, jestliže její vyzrazení neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky.
d) Vyhrazené, jestliže její vyzrazení neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky[1].

Ve své práci v bankovním sektoru se setkávám s mezinárodními definicemi citlivých dat, které se užívají v Evropské Unii:

- C1 – Public
- C2 – Restricted
- C3 – Confidential
- C4 – Secret

Každá společnost si musí upravit následné nakládání s daty dle příslušnosti do jednotlivých kategorií a tedy dle faktického dopadu na provoz firmy. Jinak se bude chovat společnost, jež ztrátou dat kategorie C1 ztratí stovky tisíc euro a jinak ta, jejíž ztráta bude dosahovat pouze stovek eur.

Pro zacházení s daty kategorie C1 ve většině firem neplatí žádná speciální nařízení, dala by se charakterizovat například jako instalace software, běžné dokumenty, jako je ceník kancelářských potřeb – volně stažitelný z internetu a vůbec všechny volně dostupné dokumenty.

3.5. Problematika mazání citlivých dat.

Na tuto oblast se dá pohlížet ze dvou úhlů pohledu:

1. Jde o výmaz médií před jejich likvidací nebo před prodejem, či darováním.
2. Vymazání dat, která již nejsou žádoucí či nutné dále uschovávat.

Pokud se jedná o výmaz dat z fyzického média, jež je určeno k prodeji, či likvidaci a tedy opouští bezpečnou oblast, je nutné použít certifikovanou technologii pro odstranění. Jelikož jde o vyřazení majetku, není nutné zachovat již žádná data a tím pádem se nám

otevírá celé spektrum možností výmazu. Pokud nemažeme jedinou existující kopii dat, nejsme limitování zákonem o Archivnictví a spisové službě č. 499/2004 Sb.

Jiný případ ovšem nastává při odstranění nepotřebných nebo nechtěných souborů, zde jsme již omezováni celou řadou okolností – výše zmíněným zákonem počínaje a technickými omezeními konče[1,2].

3.5.1. Hrozba

Pokud se soustředíme pouze na data smazaná sofistikovanější technologií než je pouhé vložení do Koše a podobně, zjistíme, že je nutný fyzický přístup k médiu samotnému. To samo o sobě na první pohled zmenšuje pravděpodobnost takového jednání, nicméně při podrobnějším prozkoumání této problematiky narazíme hned na několik aspektů, které se mohou zdát málo podstatné:

- Reklamace pevných disků
- Vyřazení staré techniky
- Odprodej techniky zaměstnancům
- Krádež nebo ztráta přenosného disku, notebooku…

Všechny výše jmenované eventuality mají společné to, že se jim nedá zabránit pomocí vymazání obsahu, či elektronické ochrany dat. Můžeme však minimalizovat škody pomocí hardwarového šifrování přenosných disků, důsledné likvidaci nepotřebných datových nosičů.

Při reklamaci opouští disk monitorovanou oblast a dostává se do rukou neautorizovaných osob, kdy není přesně evidován přístup k médiu – ve vztahu mezi standardním zákazníkem a servisem. Poškozený disk není možno obvykle důsledně vymazat před předáním do servisu a v případě výměny za nový bezvadný kus nedochází standardně k návratu hardwaru zákazníkovi, jelikož vlastníkem disku se stává dodavatel nebo servis. Záleží pak na jeho uvážení, jak s ním naloží a zda ho nechá bezpečně zlikvidovat. Tomuto nebezpečí předchází firmy, jež musí udržovat bezpečnost na určité úrovni pomocí dohod s dodavateli o náhradě poškozených disků pouze na základě kontroly hardwaru na místě, kdy poškozený disk neopouští bezpečnou oblast.

Daleko častějším jevem je vyřazení staré či nepoužívané techniky, kdy se snažíme minimalizovat další náklady spojené s její likvidací. Pokud však dojde k prodeji této techniky do rukou útočníka, má tak k dispozici legálně držený datový nosič a není způsob, jak ho o něj připravit. Likvidaci techniky by měla provádět firma schopná splnit certifikáty a normy NBÚ, ISO 9001, ISO 14001 a ISO 27001[1], tedy alespoň pevných disků. U ostatních součástí počítače nehrozí takové nebezpečí úniku dat.

Do výše zmiňované kategorie náleží i odprodej techniky zaměstnancům, bohužel v tomto případě nedochází k její likvidaci, ale volnému pohybu na trhu. I při smluvním ošetření nakládání s takovou technikou roste riziko úniku na volný trh a tím i riziko možného obnovení dat. Základním řešením je použít některou z certifikovaných metod výmazu pro minimalizaci rizika, například Gutmanovu metodu, či metodu U. S. DoD, metodu dle standardu DoD 5220.22-M[26].

Zvláštní kapitolou je krádež či ztráta disku, notebooku, flash disku – v tomto případě nejde o mazání. Důsledné mazání nepotřebných dat u těchto médií napomůže minimalizaci škod.

3.5.2. Útok

Útokem v tomto případě nerozumíme samotné proniknutí do sítě, nýbrž samotné proniknutí na disk či k disku. Často se nejedná ani o narušení bezpečnosti naší sítě, pokud dojde k vyřazení či odprodeji techniky a disk se dostane mimo naše pole působnosti.

3.5.3. Přehled existujících metod pro mazání citlivých dat

- **Rychlá metoda –** lze nalézt různé názvy pro tento postup, nicméně jde především o technologické řešení a nikoliv název. Fakticky jde o jednoprůchodové mazání, kdy je soubor náhodným vzorkem dat - náhodně generovaný proud nul a jedniček. Jedná se o základní zabezpečení, nejrychlejší vymazání dokumentů, ale zároveň nejmenší spolehlivost.

- **U. S. DoD metoda** – metoda amerického Ministerstva obrany, podle standardu DoD 5220.22-M od NSA. Metoda užívá pro vyčištění disku 3 přepisů dat. Obvyklá implementace je následující: Při prvním průchodu je disk přepsán nulami a je také ověřeno, zda byl zápis úspěšný. Následuje druhý průchod, kdy je přepsán celý disk jedničkami a opět je provedeno ověření zápisu. Při posledním třetím zápisu se zapisují náhodné znaky, následně se provede ověření, že zápis proběhl úspěšně a disk může být označen za vymazaný. Dle všech předpokladů je toto mazání schopno odolat všem pokusům o obnovu pomocí software, neboť dojde prokazatelně k třem přepisům uložených dat. Pro získání smazaných dat by byl již nutný fyzický přístup k disku a využití hardwarových metod obnovy dat[1].
- **Gutmanova metoda –** Metoda publikovaná roku 1995 Peterem Gutmannem byla přijata odbornou veřejností za jakýsi standard bezpečnosti při mazání dat, ze všech zde uváděných metod je nejpomalejší a používá nejvíce přepisů disku. Při celkem 35 průchodech se přepisuje jak pomocí náhodných vzorků, tak i jasně definovaných vzorků. Celý návrh se snaží maximálně minimalizovat riziko obnovení dat, bez ohledu na předchozí způsob uložení dat a použitou technologii pro obnovení. Teoreticky je resistivní jak vůči MFM tak FTM a s jistotou i proti softwarovým pokusům. Pro úplnou jistotu se používá její kombinace s degauserem a případně i fyzickou likvidací[3].

  Gutmannova metoda počítá s 35 přepisy disku, kdy první a poslední čtyři jsou přepisy pomocí náhodných dat (viz následující tabulka). Krom těchto osmi přepisů je zbývajících dvacetsedm přesně definováno. V následující tabulce je uvedeno i na které modulační schéma je tento přepis zaměřen. Zaměření na jedno určité schéma modulace neznamená nefunkčnost přepisu u jiného, znamená jinou efektivnost. Každý přepis dat snižuje šanci na jejich obnovení jakoukoliv metodou. Sám Gutmann v Epilogu[3] uznává, že není nutno provádět všech 35 přepisů. Podle Gutmmana stačí provést ty, které se týkají použité modulace při zápisu na konkrétním disku.

Přepisování dat				
Průch. č.	**Zapisovaná data** **V hex. kódu**	**Modulace zápisového signálu na disk**		
1.	**Náhodná**			
2.	**Náhodná**			
3.	**Náhodná**			
4.	**Náhodná**			
5.	**55 55 55**	**(1,7)RLL**		**MFM**
6.	**AA AA AA**	**(1,7)RLL**		**MFM**
7.	**92 49 24**		**(2,7)RLL**	**MFM**
8.	**49 24 92**		**(2,7)RLL**	**MFM**
9.	**24 92 49**		**(2,7)RLL**	**MFM**
10.	**00 00 00**	**(1,7)RLL**	**(2,7)RLL**	
11.	**11 11 11**	**(1,7)RLL**		
12.	**22 22 22**	**(1,7)RLL**		
13.	**33 33 33**	**(1,7)RLL**	**(2,7)RLL**	
14.	**44 44 44**	**(1,7)RLL**		
15.	**55 55 55**	**(1,7)RLL**		
16.	**66 66 66**	**(1,7)RLL**	**(2,7)RLL**	

17.	**77 77 77**	**(1,7)RLL**		
18.	**88 88 88**	**(1,7)RLL**		
19.	**99 99 99**	**(1,7)RLL**	**(2,7)RLL**	
20.	**AA AA AA**	**(1,7)RLL**		
21.	**BB BB BB**	**(1,7)RLL**		
22.	**CC CC CC**	**(1,7)RLL**	**(2,7)RLL**	
23.	**DD DD DD**	**(1,7)RLL**		
24.	**EE EE EE**	**(1,7)RLL**		
25.	**FF FF FF**	**(1,7)RLL**	**(2,7)RLL**	
26.	**92 49 24**		**(2,7)RLL**	**MFM**
27.	**49 24 92**		**(2,7)RLL**	**MFM**
28.	**24 92 49**		**(2,7)RLL**	**MFM**
29.	**6D B6 DB**		**(2,7)RLL**	
30.	**B6 DB 6D**		**(2,7)RLL**	
31.	**DB 6D B6**		**(2,7)RLL**	
32.	**Náhodný**			
33.	**Náhodný**			
34.	**Náhodný**			
35.	**Náhodný**			

Tabulka 2. – Guttmanova metoda [2]

- **Mazání z flash paměti –** Doporučované řešení při použití flash pamětí je zašifrování celého disku, případně jednotlivých dokumentů pomocí klíče a bezpečné vymazání klíče jako takového. Pro šifrování je užívána symetrická šifra.
- **Secure delete** - Tato metoda je definována s jedním přepisem, kdy se zapisují binární jedničky či nuly. Jde o velice rychlou metodu, její hlavní výhoda je, že přepis se provádí přímo pomocí diskových příkazů a není potřeba implementovat kontrolní mechanismy. Kontrolu zápisů provádí přímo hardware disku, a pokud se někde setká s neúspěchem, sám se postará o nápravu. Při jejím spuštění máme jistotu, že dojde opravdu k přepisu celého disku a nezůstane nám tedy žádné nepřepsané místo, kde by mohlo dojít k uchování nechtěných informací.
- **NCSC-TG-025 US NATIONAL SECURITY AGENCY –** tato metoda je prakticky shodná s DoD 5220.22-M. Stejně tak i její implementace jsou v podstatě totožné.
- **AFSSI-5020 – US Air force** Při této metodě dochází opět ke třem zápisům, první se zapisují jedničky, následují nuly a vše je uzavřeno zápisem náhodných dat. Hlavní rozdíl proti DoD 5220.22-M je ověřování zápisu, ke kterému dochází pouze po posledním zápisu a nikoliv po každém.
- **AR 380 – 19 – US Army** Opět jde o metodu s třemi zápisy, během prvního je zapsán náhodný znak (0,1), druhý zápis provedeme pomocí pevně určeného znaku – ve většině případů je tímto zvoleným znakem nula. Poslední třetí zápis je proveden doplňkem ke znaku zapsanému v předchozím kroku – doplňkem je nula nebo jednička. Posledním krokem je opět ověření zápisu.
- **NAVSO P-5239-26 US Navy** Opět jde o tříprůchodovou metodu. Při prvním průchodu je zapsán specifikovaný znak – obvykle jednička, při druhém je zapisován doplněk – obvykle tedy nula a naposledy dochází k zápisu náhodného znaku a ověření zápisu.
- **RCMP TSSIT OPS-II Canada** Tříprůchodová metoda, při prvním průchodu se zapíše jednička nebo nula, při druhém se zapíše doplněk první hodnoty a nakonec dojde k zápisu náhodného znaku a ověření zápisu.
- **HMG IS5 UK** Při prvním průchodu provedeme zápis nul, při dalším průchodu zapisujeme jedničky, při posledním průchodu provedeme zápis náhodného znaku, nakonec ověříme úspěšnost zápisu.

- **ISM 6. 2. 92 Australia** Jeden průchod se zápisem náhodného znaku, pro disky menší než 15GB požaduje metoda tři průchody se zápisem náhodného znaku.
- **NZSIT 402 New Zeland** Jedna z nejslabších metod, požaduje pouze jeden přepis disku náhodným znakem NZIST 402. Tyto programy přepisující pouze volné místo na disku, nemohou být použity pro odstranění citlivých dat.
- **VSITR Germany** Tento standard charakterizuje sedm průchodů, kdy se střídá zápis nul a jedniček. Při posledním průchodu je zapisován náhodný znak.
- **GOSTR 50739-95 Russia** Tato metoda má obvykle dvě různé implementace. První je dvouprůchodová. Prvním průchodem zapisuje jedničky, při druhém průchodu dojde k zápisu náhodného znaku. Druhá implementace provádí pouze jeden zápis a to náhodného znaku.
- **Schneier** - Jde o metodu doporučující k vyčištění disku použití sedmi přepisů, jde tedy opět o metodu poměrně časově náročnou. Při prvním průchodu zapisuje nuly, při druhém jedničky, následuje pět zápisů náhodného znaku.
- **Pfitzner** Pfitznerova metoda se v podstatě nejvíce podobá Gutmmanově metodě, kdy požaduje třicetři násobný přepis pevného disku. Na rozdíl od Gutmannovy metody však nebere v potaz různé modulace při ukládání dat, přepisuje třicetřikrát náhodným znakem. Ve své podstatě, každé přepsání zvyšuje bezpečnost, při použití Gutmannovy metody však dochází k daleko větší efektivnosti. Tedy disk smazaný Guttmanovou metodou bude při použití i nižšího počtu mazání smazaný lépe. Například pokud použijeme jen průchody určené pro modulace signálu, který byl použit při zápisu dat.
- **Random Data** Metoda zápisu náhodných dat nemá žádnou pevnou specifikaci, nejvíce se používá, pokud chceme specifikovat vlastní schéma. V popisu se uvažuje jeden až více přepisů celého disku. Finální počet mazání při implantaci záleží jen na tom, kdo dané schéma navrhuje, či implementuje.
- **Write Zero** Je metoda, která nemá pevnou specifikaci. Obvyklé nastavení je jeden přepis disku se zápisem nul. Dají se ovšem nalézt i implementace provádějící ověření zápisu či používající i jiný znak než nulu.

[26]

3.5.4. Porovnání metod užívaných k mazání citlivých dat

Většina z výše zmíněných metod se sobě velmi podobá, tedy i jejich efektivnost je podobná. Počet průchodů diskem se liší od jednoho až po třicetpět, kdy častým číslem jsou dva a sedm průchodů. Některé metody kladou nároky i na data, jimiž je disk přepisován, jiné se spokojí s náhodnými. Pro obranu před softwarovými nástroji obnovy dat stačí bohatě jeden přepis. Pro ochranu před hardwarovými metodami brání dle specifikací jednotlivých metod už sedm přepisů, jediný Gutmann však uvádí i věrohodnou studii a vysvětlení, na jaké bázi brání jeho přepisovací vzorec přečtení dat pomocí MFM a FTM. Sám Gutmann však v pozdější revizi svého textu přijímá názor, že oněch třicetpět přepisů je zbytečných a naddimenzovaných. [3]

Porovnávat jednotlivé nástroje implementující tyto metody nemá smysl, zajímavé je pouze porovnání jednotlivých metod a následně popsání, jak se ten který nástroj vyrovnává s jejich implementací. V případě správné implementace dané metody bude výsledkem porovnání shoda. Není možné, aby správně implementovaná metoda mohla dát rozdílné výsledky.

4. Návrh metodiky mazání menších objemů dat

Ne vždy, když chceme bezpečně smazat určitá data, máme možnost přemazání celého disku, a přesto chceme docílit alespoň nějaké úrovně bezpečnosti. Všechny výše jmenované metody jsou navrženy na smazání celého disku a jeho kompletní vyčištění, jsou však nepoužitelné, jakmile jde o smazání jednoho souboru. Cílem této části mé bakalářské práce je zhodnotit možnosti, které nám pro řešení této situace nabízí současná technika a navrhnout metodu, která by odpovídala bezpečnostním standardům.

První podmínkou je možnost přístupu přímo k fyzické adresaci disku, kdy je nutno mít seznam všech adres, kde je soubor uložen. Nicméně ani to nebude stačit pro eliminaci bezpečnostních rizik. Snaha o smazání určitého souboru před nás staví několik zásadních otázek:

1. Nemůže být soubor uložen i na jiném místě na disku?
2. Není soubor aktuálně natažen v operační paměti?

Pro úspěšný výmaz je nutno několikrát přepsat místo uložení souboru na disku. Abychom zamezili přepisování souboru na jiná místa disku, než kde daný soubor leží, je nutno zamezit defragmentování disku a stránkování paměti na disk. Tohoto nejlépe docílíme tak, že nástroj používající navrhovanou metodu, implementujeme do vlastního buildu Linuxu schopného bootu z CD/DVD mechaniky, či přímo z USB. Sestavíme si vlastní build Linuxu, který obsahuje nástroje pro mazání. Nejjednodušší pro takto vytvářené médium je vzít volně šiřitelný operační systém a ten si upravit dle potřeb. Tím se nám podaří spustit nezávislý systém, který bude mít ovšem práva pro zápis do systému, jejž budeme chtít upravovat. Problém nastane, pokud byl disk v nedávné době defragmentován a tedy soubory byly původně uloženy na jiných lokacích, než se nachází teď. V podstatě již samotná defragmentace zajistí alespoň jeden přepis těch míst, jež jsou zabrána ostatními soubory. Je nutno však pamatovat na diskové sektory, jež jsou v tu chvíli prázdné a ty, které aktuálně obsahují mazaný soubor či adresář. Tím, že přepíšeme celé volné místo včetně místa právě uvolněného, dosáhneme zamezení možnosti obnovy smazaných dat pomocí softwarových metod. Zbývá nám ještě možnost obnovy pomocí mikroskopických metod.

Pro posílení této metody je vhodné šifrování celého disku pomocí alespoň základního symetrického šifrování. Tento přídavný požadavek sám o sobě neovlivňuje náročnost obnovení dat z hlediska samotného čtení médií, ale ztěžuje interpretaci dat

získaných pomocí analýzy analogového signálu z disku. Sice bychom mohli předpokládat umístění disků, pro něž je tato metoda určena, v zabezpečeném prostředí, ale je lepší počítat i s možnou ztrátou kontroly nad oblastí a tím i fyzickou ztrátou média. I minimální zabezpečení pomocí šifrování výrazně snižuje pravděpodobnost obnovení dat. Obnovovat smazanou zašifrovanou složku nebo smazaný zašifrovaný soubor, je úkol obtížnější, než obnovit smazaný soubor z nešifrovaného disku. Při obnově šifrovaných informací je nutno nejen obnovovat informaci jako takovou, ale zároveň provádět i dešifrování.

Celou techniku je nutno vylepšit i defragmentováním disku a tedy přesunem dat tam a zpět. Pokud přidáme defragmentaci, dochází ke ztrátě informace, kde původní soubor ležel. Jakmile není možno jednoduše lokalizovat původní uložení souboru, je mnohem obtížnější provádět obnovu. Výhodou v tomto ohledu může být i předchozí fragmentace souboru, čím více bylo původních částí souboru, tím obtížněji se hledají.

Navrhovaná metoda se dá shrnout následovně:

1. Vymazání souboru
2. Přepis celého volného místa, tedy úplné zaplnění diskového média daty
3. Následná defragmentace

Pro zvýšení efektivity této metody je nutné použít šifrování disku. Šifrování disku snižuje možnosti interpretace dat získaných z analýzy analogového signálu.

5. Závěr

V práci byly popsány technické aspekty uložení a mazání dat, uvedl jsem zde i nejpoužívanější metody pro mazání citlivých dat. Symbolem této problematiky je již od svého publikování Gutmannova metoda. Tato metoda je považována za maximálně bezpečnou, vyžaduje taktéž největší počet přepisů média, než můžeme toto médium prohlásit za smazané. Ostatní metody jsou však pro ochranu před softwarovým obnovením dat stejně bezpečné a není tedy třeba vždy používat Gutmannovu metodu.

V zásadě se dá říci, že důkladné smazání dat není tak jednoduché jak by se mohlo na první pohled zdát. Je nutno provést celou řadu podstatných úkonů, než si můžeme být jisti, že soubor nepůjde obnovit. Nejde to provést jen přesunutím souboru na ikonku koše, jak se mylně domnívá velká část laické veřejnosti a dokonce i část odborné. Problém nastává v případě, kdy si koncový uživatel neuvědomuje hrozbu plynoucí z faktu, že si daný soubor uloží na disk. Jediný 100% spolehlivý způsob jak zajistit, že nikdo na našem disku nenajde pozůstatky daného souboru, je nikdy ho tam neuložit. Z tohoto důvodu je nutné zavádět nejen metodiky a standardy pro mazání dat, ale zavádět též monitorování datových toků. Pokud budeme mít efektivní nástroje na mazání, ale nebudeme vědět, kde všude byla data uložena, nebude nám to nic platné. Jak bylo již zmíněno výše je nutno též monitorovat a minimalizovat počet míst využívaných k uložení dat.

6. Slovník Pojmů

CGS – systém jednotek zavedený roku 1874 Britskou Asociací Pokroku ve Vědě, postupně nahrazovaný systémem MKS. MKS je systém založený na používání metru, kilogramu a sekundy [18]

DOD – Department of Defense – Americké ministerstvo obrany

FAT32, EXT2, UFS a NTFS – souborové systémy užívané operačními systémy Windows, UNIX, Mac OS.

Hašovací tabulka – jde o datovou strukturu o dvou záznamech hašovacího klíče a záznamu. Hašovací klíč je generován hašovací funkcí přímo z dat záznamu. Hašovací funkce je navržena tak, aby byla minimální pravděpodobnost vygenerování stejného klíče pro různé záznamy.

I-uzel – datová struktura uchovávající metadata o souborech a adresářích (např.: definici přístupových práv, čas poslední změny,…)

Oddíl – diskový oddíl slouží k rozdělení fyzického disku na logické či fyzické části, s nimiž pak můžeme volně manipulovat.

RAID - Redundant Array of Inexpensive/Independent Disks – vícenásobné diskové pole levných/nezávislých disků. Jde o metodu používanou pro zvýšení spolehlivosti uložení informací. Technické řešení spoléhá na více pevných disků, na něž jsou data ukládána buď po částech – při stripingu (RAID 0), nebo jako identické kopie při mirroringu (RAID 1). Oba tyto postupy se dále kombinují pro vznik dalších typů RAID polí,

Vyhledávací strom – datová struktura usnadňující vyhledávání. Nejčastěji užívaným stromem je BVS – binární vyhledávací strom. BVS má jeden kořen, ten může mít dva syny. Stejně tak každý uzel, který je synem vrcholu může mít dva syny. V levém synovi je uložena hodnota nižší než hodnota uzlu, v pravém je naopak uložena hodnota vyšší než uzlu.

7. Seznam zkratek

CD, DVD, HD DVD – optické datové nosiče

CRC - Cyclic Redundancy Check

CGS – systém jednotek zavedený roku 1874 Britskou Asociací Pokroku ve Vědě

DAT – Digital Audio Tape, formát datových pásek definovaný roku 1989 Sony a Hewlett Packard

ECC – error correction code

EXT,EXT2,EXT3 – souborová systémy užívané Linuxem

FAT,FAT32,NTFS – souborové systémy užívané ve Windows

HDD – hard disk drive – pevný disk

HFS,HFS+ - souborové systémy Mac OS

HPFS – souborový systém operačního systému OS/2

NVFS,NSS – souborové systémy užívané systémy Novell

Oe – jednotka intenzity magnetického pole v systému CGS,v jednotce SI definován jako $1000/4\pi$ (≈ 79.5774715) ampérů na metr.

RAID - Redundant Array of Inexpensive/Independent Disks

SSD – Solid State Drive – pevný disk, bez pohyblivých částic

USB – universal serial bus

8. Seznam literatury

[1] http://www.nbu.cz/_downloads/pravni-predpisy/container-nodeid-604/412-2005-po-11-2011---.pdf (21. 12. 2010)

[2] http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html (12. 1. 2011)

[3] http://hyperphysics.phy-astr.gsu.edu/hbase/solids/magperm.html (15. 2. 2011)

[4] http://www.ciphersbyritter.com/ARTS/CRCMYST.HTM (6. 2. 2011)

[5]]http://nobelprize.org/educational/physics/microscopes/scanning/index.html (3. 1. 2011)

[6] http://www.fujifilmusa.com/shared/bin/Degauss_Data_Tape.pdf (12. 1. 2011)

[7] http://www.articlesbase.com/software-articles/3-types-of-data-storage-mediaa-guide-to-selecting-media-for-storing-backing-up-computer-data--1374591.html (12. 1. 2011)

[8] http://en.wikipedia.org/wiki/CD (20. 2. 2011)

[9] Pohlmann, Kenneth C. (1992). The Compact Disc Handbook. Middleton, Wisconsin: A-R Editions. ISBN 0-89579-300-8

[10] http://www.osta.org/technology/cdqa.htm (20. 1. 2011)

[11] Tanenbaum, Andrew S.; Woodhull, Albert S. (2006). Operating Systems: Design and Implementation (3rd ed.). Prentice Hall. ISBN 0131429388.

[12] Marshall Kirk McKusick, Keith Bostic, Michael J. Karels, and John S. Quarterman (1996). "Local Filesystems". *The Design and Implementation of the 4.4BSD Operating System*. Addison-Wesley. ISBN 0-201-54979-4

[13] Custer, Helen (1994). Inside the Windows NT File System. Microsoft Press. ISBN 155615660X.

[14] http://technet.microsoft.com/en-us/library/cc738068%28WS.10%29.aspx (13. 1. 2011)

[15] http://www.wikihow.com/Destroy-a-CD-or-DVD (13. 1. 2011)

[16] http://www.likvidace-dat.cz/ (13. 2. 2011)

[17] http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-536.pdf (6. 1. 2011)

[18] http://portal.acm.org/citation.cfm?id=1364813.1364832 (14. 1. 2011)

[19] http://www-2.cs.cmu.edu/~garth/RAIDpaper/Patterson88.pdf (20. 1. 2011)

[20] http://www.computer.org/portal/web/csdl/doi?doc=doi/10.1109/MSP.2009.89 (21. 1. 2011)

[21]http://www.ibas.com/data-erasure/degausser/ (20. 1. 2011)

[22] http://pcsupport.about.com/od/toolsofthetrade/tp/erase-hard-drive.htm (23. 1. 2011)

[23] http://www.askdavetaylor.com/how_to_secure_securely_delete_files_mac_os_x.html (22. 1. 2011)

[24] http://web.mit.edu/newsoffice/2003/diskdrives.html (19. 12. 2010)

[25] http://www.cse.sc.edu/~okeefe/tutorials/cert/i046.03.html (15. 1. 2011)

[26] http://pcsupport.about.com/od/toolsofthetrade/g/data-sanitization-method.htm (19. 1. 2011)