Univerzita Hradec Králové
Fakulta informatiky a managementu
KIT - Katedra informačních technologií

Ochrana uživatelských dat na mobilních zařízeních

Bakalářská práce

Autor: Jiří Klouda
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Hana Švecová

Hradec Králové měsíc rok

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne Jiří Klouda

Poděkování:
Děkuji vedoucímu bakalářské práce Ing. Haně Švecové za metodické vedení práce

Anotace

Tato bakalářská práce se zabývá ochranou dat na mobilních zařízeních, zejména pak na laptopech, USB discích, mobilních telefonech a tabletech. V teoretické části je popsána stručná historie informační bezpečnosti. Dále jsou zde uvedeny jak pasivní, tak aktivní metody, které je vhodné použít při ochraně uživatelských dat. Další problematika, kterou se zabývá teoretická část je zaměřena na části bezpečného mazání dat z úložišť a přenosných zařízení.

Praktická část je věnována demonstraci získávání dat ze zařízení, která jsou nezabezpečená a na zařízení, které nebyla vhodně smazána.

Annotation

Title: Protection of user data on mobile devices

This bachelor thesis deals with data protection on mobile devices, especially on laptops, USB drives, mobile phones, and tablets. The theoretical part describes a brief history of information security. There are also both passive and active methods that are suitable for use in protecting user data. Another issue, which is devoted to the theoretical part is, how to securely delete data from the storage of these devices and USB drives.

The practical part is devoted to the demonstration of obtaining data from a device that is not secure and for a device that is not properly deleted.

Obsah

1 Úvod

V dnešní době jsou mobilní zařízení nedílnou součástí společnosti a každodenního života. V kapse každého člověka bychom v současnosti mohli najít chytrý telefon např. na klíčích většiny z nás by se dal najít USB disk a v brašnách přes rameno laptop či tablet.

S rychlým příchodem informačního věku se nám všem otevřelo spoustu možností. Výkony velkých sálových počítačů z 50. let jsou několikanásobně překonány. Rozměry a váhy těchto nových zařízení jsou tak malé, že obyčejný člověk má u sebe hned několik "počítačů". Díky tomu má každý z nás téměř neomezený přístup k jakýmkoliv informacím.

S těmito výhodami ale přišlo také velké riziko. Uživatelé mají na svých zařízeních citlivá data bez jakékoliv ochrany. Smlouvy, osobní údaje, přístupová hesla zapsaná do poznámkového bloku jsou informace, které může útočník snadno zneužít. Často však můžeme najít také citlivé nebo intimní fotografie a automatické přihlášení do různých služeb či aplikací, nezřídka s uloženou platební metodou.

Pro útočníka jsou tato data lákavým cílem. Uživatelé by měli být seznámeni se základními pravidly a principy bezpečnosti a se způsoby, jak mohou své data co nejlépe ochránit.

2 Cíl práce

Teoretická část

Cílem teoretické části bakalářské práce je definování možností ochrany dat na uživatelských zařízeních. Důraz je kladen zejména na fyzickou ochranu, autentizaci a řízení přístupu, kryptologii a bezpečné mazání dat. Součástí teoretické části je také popis škodlivého softwaru, útočníků a druhy útoků.

Praktická část

Cílem praktické části je realizace praktické ukázky zabezpečení dat na uživatelských zařízeních. V této části byl realizován útok na zařízení s různou úrovní zabezpečení, kdy cílem bylo získání citlivých dat. Na základě získaných poznatků bude vytvořen návrh bezpečnostních zásad a doporučeních pro ochranu uživatelských dat na mobilních zařízeních.

3 Metodika zpracování

Teoretická část bude zpracována analýzou odborné literatury a její následnou syntézou. Pro podporu literární rešerše budou využity informace z odborných článků a internetových zdrojů. Praktická část bude vycházet z teoretické části a bude obsahovat praktické ukázky. Nedílnou součástí bude také návrh zásad ochrany dat, který bude vycházet z dosažených poznatků.

4 Ochrana dat

V této teoretické části kvalifikační práce budou charakterizovány základní pojmy týkající se ochrany dat. Je zde popsána fyzická ochrana, autentizace a řízení přístupu a kryptologie. Důraz je kladen na škodlivý software a druhy útoků a útočníků. V této části je také popsaná bezpečná likvidace dat a bezpečnostní normy.

4.1 Ochrana dat

4.1.1 Historie ochrany dat

Informační bezpečnost vzniká spolu s informacemi, které bylo potřeba chránit. Určité mechanismy ochrany informací-především ve formě přeměny otevřeného textu na šifrovaný – začaly vznikat již v antice v podobě kryptologických šifer. Rozvoj šifrování nastal po vynálezu telegrafu v roce 1845 a vyvrcholil za druhé světové války šifrovacími stroji jako byla Enigma. Výrazným milníkem byl vznik moderní kryptografie, jejíž duchovní otec Claude Shannon během 2. světové války vypracoval za účelem bezpečnosti přenosu informací koncept matematické kryptografie [1].

4.1.2 Definice počítačové bezpečnosti

William Stallings ve své knize definuje pojem bezpečnost IT jako ochranu odpovídajících informačních systémů a informací, které jsou v nich uchovávány, zpracovávány a přenášeny [25].

Tomáš Doseděl pak dělí ochranu dat na fyzickou ochranu dat, ochranu před zničením, ochranu logického přístupu a ochranu uložených a přenášených dat [3].

4.2 Fyzická ochrana dat

Fyzická ochrana dat je systém opatření, které mají útočníkovi nebo neoprávněné osobě zamezit v přístupu k uživatelským datům a nosičům s těmito daty, nebo mu tento přístup významně ztížit.

Tato forma ochrany také zabezpečuje data v případě odstávky dodávek elektrické energie, nebo v případě živelné katastrofy, jako je požár nebo povodeň.

Fyzická ochrana dat se skládá s částí:

- zamezení přístupu,
- ochrana před zničením
- ochrana proti výpadkům dodávek energie
- ochrana proti živelným katastrofám.

4.2.1 Zamezení přístupu

Hlavní formou fyzické ochrany dat je zamezení přístupu k zařízení nebo nosiči, který obsahuje citlivá data.

Mobilní zařízení, jako smartphony nebo laptopy, jsou svojí povahou zařízení, která se snadno přenáší a může se s nimi pracovat prakticky kdekoliv. Z toho důvodu je potřeba dodržovat několik pravidel, které útočníkům zamezí v přístupu.

Přístroje by neměli zůstávat bez dozoru na veřejně přístupných místech, jako jsou kavárny nebo restaurace. V takovém případě může snadno dojít k odcizení celého přístroje, nebo infiltraci pomocí škodlivého softwaru.

Pokud ponecháme zařízení nebo nosič na místě, kde může docházet k většímu pohybu osob, jako je třeba kancelářské budovy, je vhodné je uložit do uzamykatelného boxu, nebo při odchodu uzamknout kancelář [3].

4.2.2 Ochrana před zničením

Ke zničení dat může dojít dvěma způsoby – data jsou smazána či poškozena přímo na svém nosiči, nebo jsou fyzicky zlikvidovány vlastní nosiče (HDD, DVD, CD, USB aj). První případ může nastat chybou či zlomyslností uživatele či chybou systému, druhý pak fyzickým útokem či přírodní katastrofou. K oběma případům může dojít, i když jsme dodrželi všechna technicko – organizační opatření v podobě interních doporučení (směrnic) organizace.

Základní metodou ochrany proti zničení dat je systematické zálohování [3].

Zálohováním rozumíme proces, v rámci, kterého dochází ke kopírování zálohovaných dat z místa jejich běžného užití do místa odlišného. Při návrhu, tvorbě

či způsobu zálohování pro sestavení plánu záloh v podobě interní směrnice či BCP (Business Continuity Plane) je nutno zvážit důležité skutečnosti:

- co zálohovat
- kam zálohovat (volba média)
- jak často zálohovat
- jak budou zálohy chráněny
- jak bude realizována obnova dat ze zálohy [4].

4.2.3 Ochrana proti výpadkům dodávek energie

Mobilní zařízení jsou proti výpadkům energie poměrně odolné. Často disponují bateriemi, jejichž kapacita vystačí přístroji i několik hodin. Přesto není dobré toto riziko podceňovat.

Existují zařízení, která dokáží zajistit nejen kvalitu dodávaného proudu (tedy stabilitu jeho úrovně), ale i ochranu před neočekávanými špičkami či výpadky. Obecné označení takového zařízení je záložní zdroj, existuje ale více druhů, jako je akumulátorový zdroj a generátor.

4.2.4 Ochrana proti živelným katastrofám

Přírodní katastrofa je přírodním procesem, který je rychlý a zanechal po sobě lidské oběti a materiální škody. Slovo „rychlý“ v této definici má geologický význam. To znamená, že může katastrofický proces může trvat vteřiny, dny i týdny, jeho následky však bývají dlouhodobé. Mezi přírodní katastrofy patří např. požár, záplavy, zemětřesení.

Požár

Protipožární ochranu dnes již podceňuje jen málokdo. Všichni totiž někde viděli požár (což neplatí zdaleka o všech katastrofách). Kromě nehořlavých podložek se instalují samočinné požární hlásiče a komplexní systémy pro hašení vzniklých požárů. Pozor zvláště na to, že elektrická zařízení nelze hasit vodou. Zařízení s citlivými daty by měly být uloženy v nehořlavých skříních, pokud možno vodotěsných a prachotěsných, aby nedošlo k vniknutí hasící látky.

Zemětřesení a podobné katastrofy

Hlavní nepříjemností zemětřesení je borcení budov a následné zasypávání zařízení. Vhodná je tedy již zmíněná prachu vzdornost, na škodu nebude ani pevnost skříně, ve které je zařízení uchováváno [3].

Voda

Může data ohrozit dvojím způsobem buď záplavami, nebo závadami na vodovodních sítích. Důležité protizáplavové opatření je to, že prostory by měly mít vhodnou polohu. Důležitá data by měla být umístěna v horních patrech budovy a místnost by měla být izolována. Izolovány by měly být i počítačové skříně, ve kterých jsou pevné disky s daty umístěny. Při evakuaci budovy je vhodné jak při záplavách, tak i při závadách na vodovodních sítích mít určeno důležitost dat. Je také důležité, v jakém prostředí jsou počítačové komponenty umístěny. Komponenty jsou citlivé na velké změny teplot, prach a vlhkost. To lze vyřešit nainstalováním klimatizace, která obsahuje filtrovací zařízení [4].

4.3 Autentizace a řízení přístupu

Procesem autentizace rozumíme postup, kterým automatizovanému systému prokazujeme identitu. Existují tři základní možnosti, jak identitu prokázat: znalostní, vlastnictvím a vlastností.

Identifikace znalostí předpokládá, že svou identitu prokážete systému tím, že víte něco, co můžete vědět právě jen a pouze Vy (např. heslo).

Vlastnictvím prokazujeme identitu vlastnictvím nějakého fyzického předmětu, který je pro nás unikátní, např. čipová karta. Vlastností prokazujeme identitu systému tím, čím jsme – tedy fyzickou vlastností tělesné části (např. otisk prstu, sken sítnice apod.).

Alternativně je možno k autentizaci použít kombinaci výše uvedených postupů, tedy např. vlastnictvím a znalostí (kreditní karta + PIN) [5].

4.3.1 Důkaz znalostí

Nejstarším a v současné době pravděpodobně nejrozšířenějším způsobem získání autentizační informace je její zadání z klávesnice. Jedná se o různá alfanumerická hesla, numerické PINy, či dlouhé pass phrase [3].

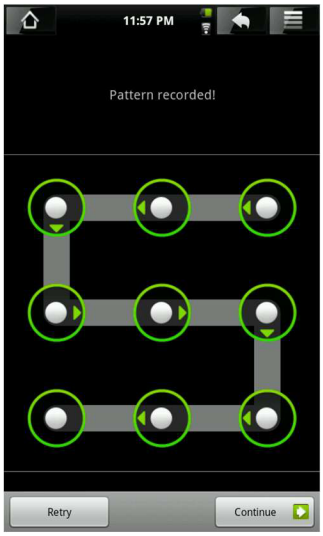
Z hlediska bezpečnosti jsou poměrně problematická gesta. Odemykání pomocí gest funguje tak, že uživateli se zobrazí obrázek a ten odemkne zařízení pohybem po určitých částech takového obrázku. Nedávné studie o použití takových metod však odhalily, že tento typ autentizace není možno považovat za bezpečný. Prvním problémem je samotný display. Lidská kůže má totiž jednu nepříjemnou vlastnost – je mastná. Prakticky to znamená, že všechny dotykové displeje jsou do určité míry „zapatlané“. V těchto šmouhách je pak často možno identifikovat vzory, které pak lze využít pro odemknutí. Druhým problémem je to, že pohyb gesta samotného není náhodný, lze jej také odpozorovat a počet kombinací není nevyčerpatelný, viz srovnání počtu možných kombinací gest a čísel PIN [5].

N	Počet kombinací spojením N bodů	Počet kombinací zadáním N čísel
2	56	100
3	360	1 000
4	2 280	10 000
5	14 544	100 000
6	92 448	1 000 000
7	588 672	10 000 000
8	3 745 152	100 000 000

Tabulka 1: Počet kombinací, gesta vs. PIN (převzato z [6])

Z bezpečnostního hlediska proto není možné použití gest doporučit jako plnohodnotnou náhradu PIN nebo hesel (pass frází) [5].

Fungování zadávání gest na dotykovém displeji je možné si představit z obrázku č. 1.



Obrázek 1: Odemčení pomocí gesta (převzato z [6])

4.3.2 Důkaz vlastnictvím

Autentizace vlastnictvím umožňuje prokázat identitu pomocí vlastnictví nějakého předmětu. Pro tento účel se používají nástroje jako jsou:

- čipové karty (karty s magnetickým páskem),
- čipy (např. RFID),
- průkazy s elektronicky čitelnými údaji,
- tokeny,
- a další [5].

Nevýhodou je už zmiňovaná nutnost nošení předmětu, uživatel nesmí předmět ztratit. Na druhou stranu mají bezpečnostní předměty snesitelný tvar i velikost, v řadě případů se dají připnout na klíče nebo vložit jako plastová karta do peněženky.

Obrázek 2: Token RSA SecurID SID800 (převzato z [7])

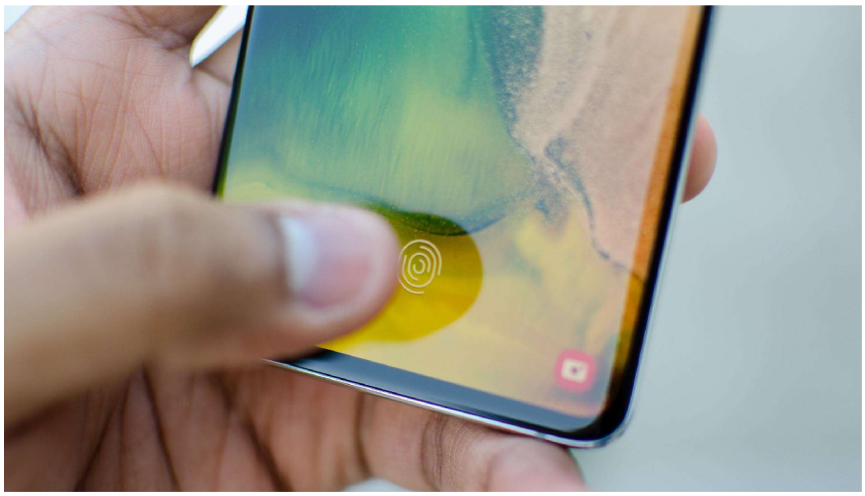
Největší nebezpečí hrozí při ztrátě bezpečnostního předmětu. Kdokoliv tento předmět najde, může se bez problému do informačního systému přihlásit, jako by se jednalo o oprávněného majitele předmětu. Ve většině případů tedy s pouhým důkazem vlastnictví nevystačíme, je nutné ho kombinovat například s předchozím důkazem znalostí [4].

4.3.3 Důkaz vlastností

Autentizace vlastností umožňuje prokázat identitu systému pomocí vlastností lidského těla. Existuje celá řada metod, které spolehlivě umožní identifikovat člověka např. DNA je jednou z nejspolehlivějších metod. Vyhodnocování DNA je však drahé a trvá opravdu dlouho [5].

Pro autentizaci se proto volí takové vlastnosti, které je možno rychle, levně a spolehlivě měřit. Požadavkem zároveň je, že snímací senzor by neměl zabírat příliš mnoho místa. Tedy jaké typy autentizace vlastností se v praxi používají:

- sken siluety ruky,
- snímání otisku prstu,
- sken žilkování na dlani,
- skenování oční duhovky,
- skenování oční sítnice [5].



Obrázek 3: Snímač Samsung Galaxy S10 (převzato z [8])

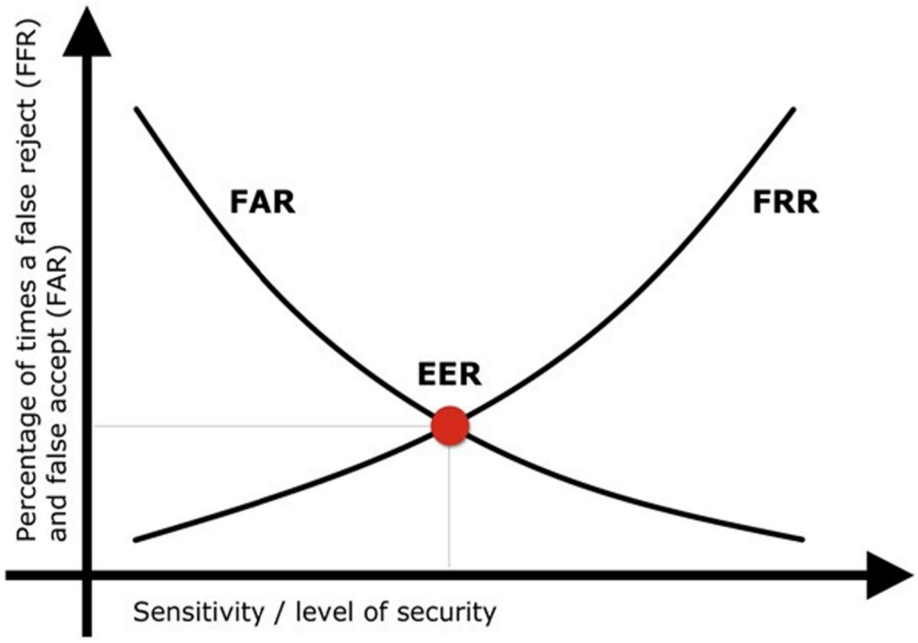
Bohužel se zde vyskytuje několik základních problémů. Jednak je to otázka živosti uživatele. Byly popsány případy, kdy systém pro identifikaci podle obličeje identifikoval naprosto bez problému barevnou fotografii. Japonskému profesorovi se zase podařilo obelstít čtečku otisků prstu modelem vyrobeným z gumových želé medvídků [3].

Dalším problémem je nestoprocentnost spolehlivosti a následná existence dvou chybových stavů, ke kterým může dojít – chyba, při níž je jako platný uživatel označen uživatel, který do systému nemá mít přístup (její pravděpodobnost vyjadřuje tzv. False Acceptance Rate – FAR) a chyba, při které je oprávněnému uživateli odepřen přístup (její pravděpodobnost vyjadřuje False Rejection Rate – FRR) [3].

Otisk prstu	1:500
Oční duhovka	1:100 000
Oční sítnice	1:10 000 000

Tabulka 2: Chybovost jednotlivých metod (převzato ze [5])

Zatímco se zabezpečením systému počet False Acceptance Rate (FAR) klesá, tak naopak počet False Rejection Rate (FRR). Bod, kde se procentuálně FAR a FRR rovná, se nazývá Equal Error Rate (EER) [9].



Obrázek 4: Dopad zabezpečení systému na FRR a FAR (převzato z [9])

4.3.4 Útoky na autentizační protokoly

Všechny autentizační protokoly musí být podrobeny zkoumání z hlediska útoků, které je na ně možné aplikovat. Testování odolnosti je jednak nedílnou součástí práce návrháře autentizačního protokolu, jednak mu bude protokol vystaven v masovém měřítku po svém nasazení do reálného provozu [3].

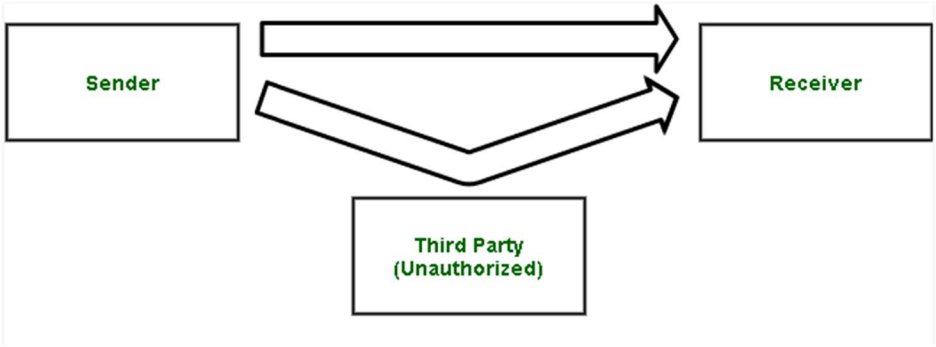
Útoky na autentizační protokoly můžeme rozdělit na:

- útoky opakováním,
- útoky ze středu,
- útoky na hesla,
- útoky na integritu zpráv.

Útok opakováním

Útok opakováním spočívá v odposlechu mezi dvěma autentizujícími se stranami a následném použití odposlechnutých informací k autentizaci útočníka. Hlavním nebezpečím odposlechu je jeho těžká odhalitelnost a snadná proveditelnost.

Jednoduchou ochranou je použití časového razítka či metody výzva odpověď, kdy jedna strana vyzve otázkou druhou stranu k poskytnutí správné odpovědi, aby mohlo dojít k autentizaci přístupu.



Obrázek 5: Replay attack (převzato z [10])

Útok ze středu

Útok ze středu je založen na přítomnosti útočníka mezi oběma komunikujícími stranami a jeho kontrole nad celou komunikací. Útočník odposlouchává jednotlivé zprávy autentizačního dialogu a postupně navazuje spojení s oběma stranami A a B tak, že pro stranu A se jeví být stranou B, a naopak straně A odpovídá tak, jak by činila strana B.

Obrázek 6: Útok ze středu (vlastní zpracování)

Útok na hesla

Jedná se o situaci, při níž útočník nějakým způsobem získá uživatelovu autentizační informaci – heslo.

Cest se nabízí hned několik. Uložení všech hesel v centrální databázi značně zvyšuje motivaci k útokům. Se vzrůstajícím výpočetním výkonem moderních počítačů je

zase možné provádět testy všech možných hesel metodou hrubé síly či propracovaný slovníkový útok.

Vhodnou obranou je důkladná ochrana zařízení, na kterých jsou citlivé údaje uloženy, nebo nastavení maximálního počtu neúspěšných pokusů o autentizaci.

Útok na integritu zpráv

Útok na integritu zpráv souvisí s nedokonalým návrhem protokolu. Protokoly sice mohou řešit všechny nestandartní situace vzniklé například podvržením expirované odposlechnuté zprávy, zprávy zašifrované nesprávným klíčem a podobně, nemusí už ale kontrolovat například situaci, kdy je velikost jednoho pole zprávy nastavena na hodnotu, jež přesahuje velikost celé zprávy. V tomto případě není chování protokolu nijak definováno [3].

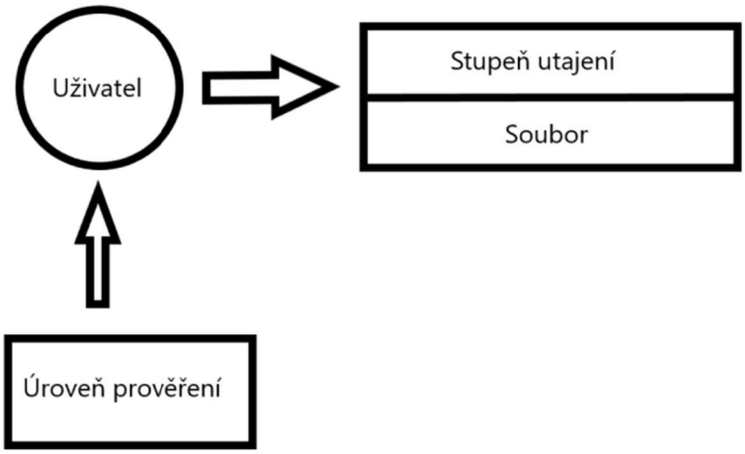
4.3.5 Řízení přístupu

Řízení přístupu je ochrana informačních zdrojů nebo služeb před přístupem nebo využíváním ze strany nepovolaných entit (organizací, lidí, strojů, procesů). Můžeme tedy říci, že řízení přístupu zabraňuje neautorizovanému využívání určitého zdroje (tzn. tato služba kontroluje a určuje, kdo má přístup, k jakým zdrojům, za jakých podmínek k nim může přistupovat a jakým způsobem je může využívat) [11].

Povinné řízení přístupu (Mandatory Access Control)

Základním principem tohoto druhu řízení přístupu je dělení dat podle stupně utajení, kterému podléhají. Různí uživatelé mají přístup k datům s různým stupněm utajení. Důležité je zajistit, aby uživatel neměl přístup k datům, které jsou na vyšší úrovni utajení, než k jaké má uživatel přístup.

Důležitou vlastností je, že uživatel nemůže sám měnit přístupová práva. Nemůže dokonce ani vytvořit kopii objektu s vyšším stupněm utajení a přiřadit ji nižším stupněm.

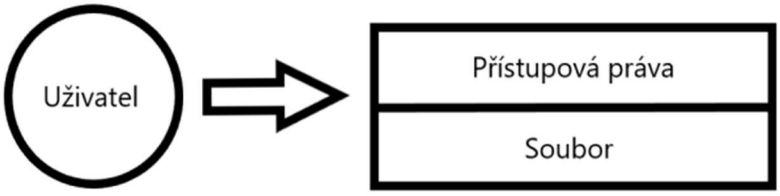


Obrázek 7: Povinné řízení přístupu (převzato z [3])

Nepovinné řízení přístupu (Discretionary Access Control)

Jedná se o řízení přístupu ve smyslu, jak ho chápe většina uživatelů. Každý uživatel má v tomto systému přiřazena jistá přístupová práva k jednotlivým objektům, uživatelé mohou, ale nemusí být řazení do skupin. Systém při pokusu o přístup k objektu hlídá, zda má uživatel dostatečná oprávnění k dané činnosti.

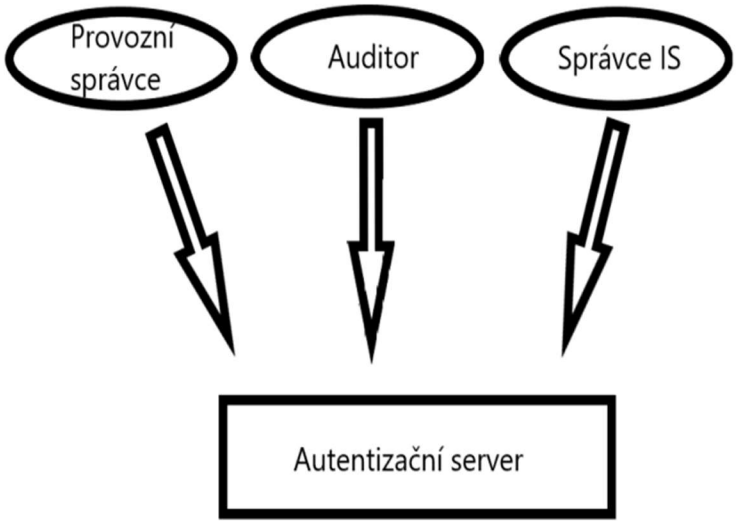
V systému musí existovat jeden správce, který má možnost měnit přístupová práva jednotlivým uživatelům. Většinou však může práva do jisté míry měnit každý uživatel, minimálně u objektů, které sám vytvořil a jejichž je vlastníkem.



Obrázek 8: Nepovinné řízení přístupu (převzato z [3])

Oddělení rolí

Systémy v nejjednodušší podobě mají všechny uživatele na stejné úrovni privilegovanosti. Všichni jsou ve své podstatě správci. Pokročilejší systémy od sebe odlišují správce a běžné uživatele, správce je však v systému v podstatě všemocný. Na nejvyšší úrovni jsou systémy, které rozlišují více druhů správců.



Obrázek 9: Oddělení rolí (převzato z [3])

Je samozřejmé, že role jednotlivých správců se mohou prolínat, jeden člověk může provádět více činností. U zvláště důležitých a citlivých operací je ale vhodné zavést pravidlo čtyř očí. K provedení této operace je pak nutné, aby ji odsouhlasilo více na sobě nezávislých správců. Je důležité zajistit, aby ke spáchání bezpečnostního incidentu bylo potřeba spolupráce více lidí [3].

4.4 Kryptologie

Kryptologie je vědecká disciplína věnující se ochraně dat před neoprávněným čtením [3].

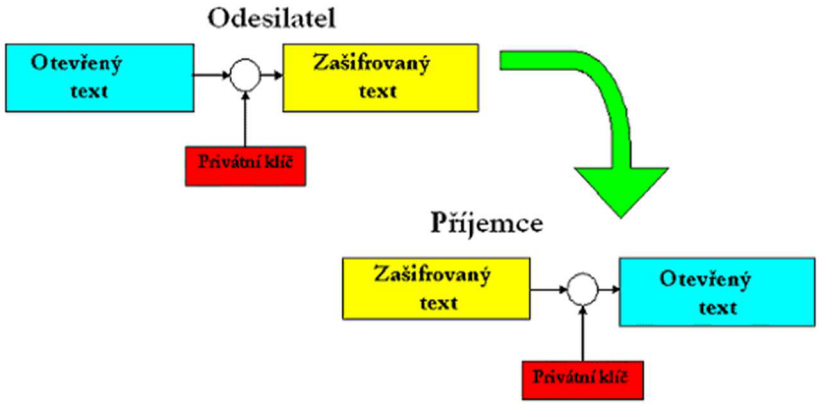
Hlavními disciplínami kryptologie jsou kryptografie a kryptoanalýza. Kryptografie studuje šifrovací algoritmy, kryptografické nástroje, hardwarové implementace šifrovacích algoritmů a kryptografické protokoly. Kryptoanalýza se zabývá luštěním šifer. V poslední době její význam získává stále více na váze, díky odhalování teoretických slabin běžně používaných šifer.

V kryptologii rozlišujeme 2 důležité pojmy – **šifrování** a **kódování.** Oba termíny popisují proces transformace určité informace z jedné podoby do druhé, ale kódování při něm nevyužívá žádné utajované informace, na rozdíl od šifrování. Typickým příkladem kódování jsou kódy ASCII, latin 2 nebo UNICODE.

Proces transformace, který převede text na šifrovaný text se nazývá šifrovací algoritmus [12].

4.4.1 Symetrická kryptografie

Algoritmy symetrické kryptografie pracuje s jedním klíčem, který je společný dvěma komunikujícím stranám. Jeden klíč je používán pro šifrování a dešifrování textu. Výhoda této metody je její velká rychlost, nevýhodou pak nároky na počet klíčů a jejich správu [3].

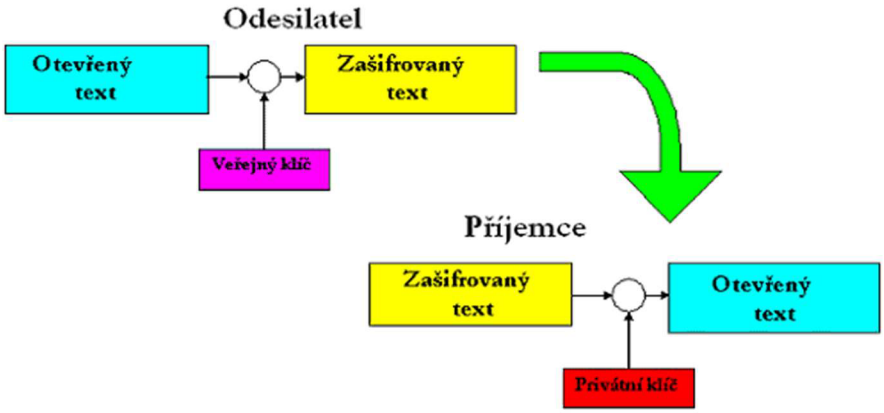


Obrázek 10: Symetrické šifrování (převzato z [13])

Problematické jsou zejména situace, kdy mezi sebou provádí komunikaci stovky či tisíce lidí. V tomto případě je nutné pro každý komunikující pár vytvořit tajný symetrický klíč. V systému N uživatelů tedy vzniká N2/2 klíčů. Kromě toho, při porušení důvěrnosti kteroukoliv pracovní stanicí, získá záškodník přístup ke všem klíčům tohoto uživatele a může odesílat jakoby jeho jménem, zprávy všem abonentům, s kterými si "oběť" dopisovala.

4.4.2 Asymetrická kryptografie

Základním znakem asymetrické kryptografie je existence klíčového páru pro každého uživatele. Vlastností tohoto páru je skutečnost, že text zašifrovaný jedním klíčem z páru je možné dešifrovat pouze druhým klíčem ze stejného páru [3]. To znamená, že se znalostí šifrovacího klíče a zašifrovaného textu je nemožné obnovit původní zprávu – je možné jej přečíst pouze s pomocí druhého klíče – dešifrovacího klíče. Z tohoto důvodu není nutné šifrovací klíč při komunikace skrývat. Proto se šifrovací klíč v asymetrických systémech nazývá "otevřeným klíčem“ a dešifrovací klíč musí příjemce zpráv uchovávat v tajnosti – nazývá se "zavřeným klíčem".



Obrázek 11: Asymetrické šifrování (převzato z [13])

Další podmínkou pro asymetrické šifrování je, aby se díky znalosti otevřeného klíče nebylo možné spočítat uzavřený klíč.

4.4.3 Šifrování dat

Úkolem šifrování je změnit data tak, aby je nemohla přečíst neoprávněná osoba. Šifrování tedy zajišťuje důvěrnost dat [3].

Šifrování disku

Šifrování disku je fyzickou ochranou dat a uživatele nijak neochrání v případě, kdy je šifrovaný disk nebo oddíl připojený a na stroj se naboural útočník ze sítě.

Narozdíl od šifrování souborů nebo zpráv se u celého disku šifruje velké množství dat (v dnešní době až jednotky TB). Šifrovaná data a datové struktury mají očekávané charakteristiky, které, při špatném zvolení šifrovacího módu, mohou usnadnit kryptoanalýzu.

Při použití šifrovaných a nešifrovaných souborových systému je nutné zajistit, aby šifrovaná data neprosakovala v nešifrované podobě mimo šifrované souborové systémy.

Kromě značných výhod přináší diskové šifrování i celou řadu nevýhod. Je velmi jednoduché přijít o šifrovaná data (stačí zapomenout heslo). Diskové šifrování také zkomplikuje veškeré záchranné operace v případě HW problémů s médiem. Chyba v jediném bitu způsobí minimálně ztrátu celého bloku. Šifrování také o něco zpomaluje diskové operace (čtení/zápis), respektive činí je závislými na CPU. Vyšší

zátěž CPU znamená větší spotřebu a vyšší teplotu, což se podepíše třeba na životnosti baterie laptopu [14].

4.5 Bezpečné mazání dat

Po vymazání dat z pevného disku, v prostředí Windows přesunutím do koše a jeho vyprázdněním, soubor zmizí z původní složky. Ve skutečnosti však není odstraněn, ale je stále na pevném disku. Prostor, na kterém byl uložen, je označen jako volný a čeká na další soubor, který zaujme jeho místo. Totéž se děje při formátování pevného disku. Celý jeho povrch je označen jako volný, ale ve skutečnosti se na něm stále nachází data [22].

V případě magnetickým pevných disků je potřeba věnovat pozornost zejména souborovému systému. SSD a jiné disky z flash paměťovými buňkami obsahují ochranné hardwarové prostředky, které zabraňují opakovanému zápisu dat do stejných buněk a tím i předčasnému poškození disku.

Zařízení, jako jsou smartphony nebo tablety lze snadno uvést do továrního nastavení, ze kterého lze ale data snadno obnovit. Bezpečné odstranění dat z těchto zařízení vyžaduje přímý přístup k vnitřnímu úložišti [23].

4.5.1 Bezpečné mazání HDD

Přesné umístění a typ uložených souborů jsou zaznamenány v centrální tabulce systému souborů. V souborovém systému FAT se tento záznam nazývá alokační tabulkou, v systému NTFS nese název Master File Table (MFT). Jakmile dojde ke smazání souboru, Windows fyzicky nevymažou sekvenci jeho nul a jedniček z plotny pevného disku, jen jej ve zmíněné tabulce označí jako smazaný. Do okamžiku, než dojde k přepsání dat na plotně HDD jinými daty, lze smazaný soubor snadno obnovit.

Pokud tedy dojde k přepsání starých dat novými, nemělo by být možné je obnovit ani ve specializované laboratoři. Musí ale dojít k přepsání všech dat, uložených na pevném disku [23].

4.5.2 Bezpečné mazání FLASH

U SSD neřídí zápis bitů a bajtů operační systém, ale řadič samotného disku rozhoduje, jaké paměťové buňky ukládanými daty zaplní. Ačkoliv to nemá velký vliv na obnovu smazaných dat, bezpečné mazací programy jako je Eraser už nemohou zařídit, aby byly všechny smazané buňky spolehlivě přepsány jinými daty. Místo toho jsou buňky označeny v MFT jako smazané a řadič pak data, která do nich měla směřovat, uloží do jiných buněk, aby nedocházelo k jejich zbytečnému opotřebování. Úložný prostor SSD, většinou i s vyhrazeným rezervním prostorem, lze snadno přepsat tak, že se do řadiče disku pošle ATA příkaz "Secure Erase". Jelikož se jedná o ATA příkaz, měl by být SSD připojen přes rozhraní SATA, Externí USB disky musí podporovat konverzi SCSI příkazů do ATA. [23]

4.5.3 Bezpečné mazání smartphonů

Systém Android nabízí možnost obnovy do továrního nastavení. Data se při resetu vymažou, nejsou ale přepsána jinými daty, a proto je lze obnovit.

Mobilní zařízení s operačním systémem Android mohou používat dva druhy úložišť, interní flash paměť a externí paměťové karty. SD karta nepředstavuje z hlediska mazání dat problém, lze jí vložit do čtečky paměťových karet a vzhledem k tomu, že bývá většinou naformátována na systém FAT, lze s daty pracovat pomocí nástrojů jako je Eraser. Mazání dat z interní paměti, která je zpravidla naformátována na linuxový systém ext4, je o něco složitější, protože pro přístup k paměťovým buňkám vyžaduje administrátorská práva. Proto nelze spolehlivé smazání ve smartphonu nebo tabletu provést prostřednictvím operačního systému Windows, ani za pomocí specializovaných aplikací pro Android.

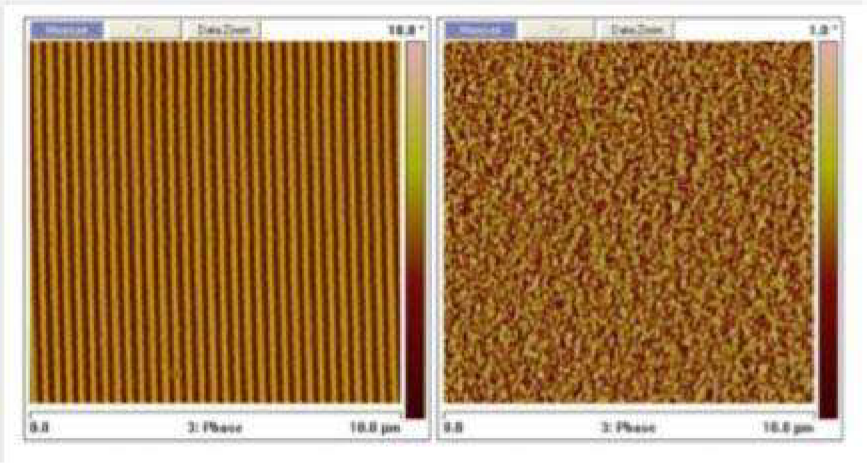
Nástroje určené pro mazání dat musí mít přímý přístup k souborovému systému, což je možné pouze prostřednictvím Andriod Debug Bridge (ADB). Pomocí ADB a kombinací aplikací určených pro Windows i Andriod je možné přesunout fyzickou image interní paměti tabletu nebo smartphonu do PC, kde je možné ji upravit [23].

4.5.4 Demagnetizace

Demagnetizace (degaussing), je metoda odstranění dat, kterou lze považovat za trvalou. Tato metoda je účinná pouze v případě magnetickým médií, jakou jsou

pevné disky či magnetické pásky. Silné magnetické pole, vytvořené demagnetizačním přístrojem, do nějž se média vkládají, dokáže vytvořit magnetické pole o intenzitě 11 000 Gauss.

Demagnetizátor umožňuje trvalé odstranění magneticky zapsaných dat s tím, že disk či páska nemusí být v danou chvíli v provozu. Data lze tedy odstranit jak z pevného disku s poruchou, ale i z funkčního média, které je tímto krokem zničeno, data jsou nenávratně smazána a médium je nepoužitelné [24].



Obrázek 12: Pevný disk před a po degaussingu (převzato z [24])

4.5.5 Fyzická likvidace

Fyzické zničení je vhodná metoda zejména u médií, která se se svými rozměry nevejdou do zásuvky degausseru. Může se jednat například o tablety nebo staré serverové disky.

Při ničení je možné využít pákový destroyer, který disk probodne a zdeformuje tak, že již není možné data obnovit. Pokud dochází k likvidaci velkého počtu médií, používá se skartovačka. Například Shredder ProDevice DGX02, používaný odborníky na certifikovanou likvidaci dat, splňuje požadavky evropské normy DIN 66399H5, což umožňuje pracovat na úrovni bezpečnosti H5, kde maximální rozměry vzniklé drtě jsou od 10 mm^2 do 320 mm^2.

4.6 Škodlivý software

Škodlivý software, označující se též jako malware, je počítačový program nebo jakýkoliv kus programového kódu vytvořeného za účelem napadení – vniknutí do systému za účelem jeho poškození, odcizení dat nebo sledování uživatele [17].

4.6.1 Spyware

Spyware je druh škodlivého kódu, který bez vědomí uživatele v systému, v němž je nainstalován, shromažďuje odesílaná data. Spyware sám sebe v drtivé většině případů nekopíruje, nepoškozuje uložená data, nepřesouvá, ani jej nemaže.

4.6.2 Adware

Je škodlivý kód, který má během své činnosti za úkol zobrazovat reklamu v jakékoliv formě. Povětšinou není nikterak nebezpečný, je spíše obtěžující. Bývá distribuován společně s jinými programy. Adware neshromažďuje data ani je nikam neodesílá, v některých případech může reklamu cílit na základě informací nashromážděných spywarem.

4.6.3 Rootkit

Rootkit je soubor nástrojů, kterými lze maskovat činnost škodlivých kódů v systému. Maskování může probíhat skrýváním adresářů s malwarem, skrýváním klíčů v registrech, skrýváním běžících procesů, síťových spojení a dalších systémových služeb tak, že je činnost škodlivého kódu běžnými systémovými prostředky těžko odhalitelná [17].

4.6.4 Počítačový vir

Počítačový virus je program nebo část kódu, která se spustí na vašem PC bez vašeho vědomí nebo svolení. Některé viry pouze znepříjemňují uživateli život. Většina virů je ale navržena tak, aby získala kontrolu nad napadeným systémem a prováděla destruktivní akce [18].

Zvláštním druhem počítačového viru je červ, škodlivý kód, který se replikuje do počítačových systémů pomocí počítačových sítí [17].

4.6.5 Trojský kůň

Trojským koněm je označován škodlivý kód, který je ukryt v počítačovém programu a který se na první pohled může tvářit neškodně. Často využívá legitimní a důvěryhodné zdroje, jako e-mailová zpráva s přílohou vytvářející domnění že pochází například od společnosti vyvíjející antivirové programy.
Narozdíl od počítačového viru se zpravidla nesnaží o další šíření, jeho hlavním účelem je získávání hesel, manipulaci se soubory nebo ovládání běžících systémů.

4.6.6 Ransomware

Ransomware (alias rogueware nebo scareware) omezuje uživatelům přístup k jejich počítačovému systému nebo souborům. Za obnovení přístupu požaduje program zaplacení výkupného.
Systém se může nakazit prostřednictvím webového prohlížeče, náhodnou návštěvou webu, který je tímto typem malwaru infikován nebo pokud uživatel spustí zavirovanou přílohy emailu. Může se také šířit přes počítačovou síť [19].

4.6.7 Antivirový program

Jedná se o speciální software sloužící k ochraně zařízení před viry a dalším malwerem, jejich detekováním, eliminaci jejich činností a úplným odstraněním ze systému. Moderní antivirové programy vykonávají mnoho činnosti najednou – rezidentní štít, ochrana zařízení proti virům, rychlá ochrana proti epidemiím nebo automatická aktualizace virových knihoven jsou jen některé funkce [17].

4.7 Útoky a útočníci

Na jakýkoliv počítačový systém může zaútočit člověk ze zlými úmysly. Takovou osobu označujeme útočník. Útočníky můžeme rozdělit podle odbornosti, nebo podle logické polohy vzhledem k napadnutému systému [3].

4.7.1 Vnitřní útočník

Jedná se o osobu, která je připojena do vnitřní sítě, ve většině případů se jedná o interního zaměstnance firmy [3].

Aby byl útok zvenčí úspěšný, musí projít několika vrstvami ochrany sítě a aktiva, na které je útočeno, pokud je však útok realizován zevnitř organizace, ochranné vrstvy na vnějším perimetru sítě útok nemohou zachytit.
Motivací pro takový útok mohou být peníze – některá firemní tajemství, jakou jsou například obchodní tajemství nebo technická schémata, mohou být dobře zpeněžitelné u konkurence.
Druhým typem motivace může být zjištění nějaké nepřístojnosti v organizaci, kterou daný člověk řeší vynesením informací na veřejnost. Takové lidi označujeme jako whistle blowery a nemusí se nutně jednat o kriminální akt.
Posledním motivem, který vnitřní útočník může mít, je pomsta. Pomsta, jako motivační faktor, je obzvláště nebezpečná, protože je většinou dlouhodobě naplánována s cílem ve finále způsobit maximální škody [5].

4.7.2 Vnější útočník

Jedná se o osobu, která nemá fyzický přístup k vnitřní síti. Při svém útoku musí překonat všechny nástrahy, které mu správce sítě klade [3].
Z hlediska motivace rozlišujeme hackery „podle klobouků“, v tomto smyslu můžeme hackery rozlišovat:

- **white hat** – bílý klobouk – bezpečnostní specialista (etický hacker), často najímaný organizacemi pro nalezení slabých míst v zabezpečení, zabývá se penetračním testováním a konzultační činností
- **black hat** – černý klobouk – zabývá se prováděním útokům na systémy za účelem dosažení vlastního prospěchu,
- **gray hat** – většinou etický hacker, ale někdy může jít „přes čáru“ ať už úmyslně nebo neúmyslně [5].

4.7.3 Amatéři

Jedná se o nejméně nebezpečné útočníky. Za použití dostupných nástrojů zkouší využít popsanou bezpečnostní díru. Častou motivací je pouhá zvědavost. K ochraně

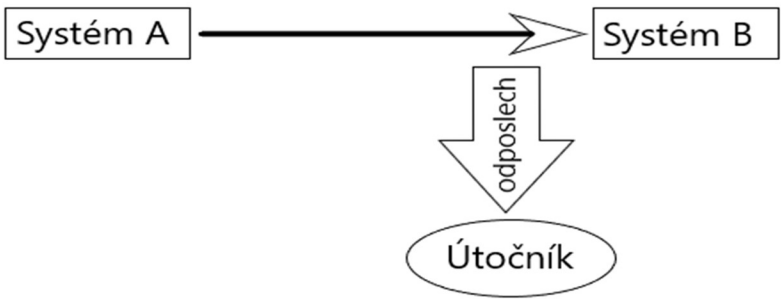
systému proti jejich útokům dostačují levná a jednoduchá bezpečnostní opatření, například pravidelné aktualizace [3].

4.7.4 Profesionálové

Jejich útoky se řadí mezi nebezpečnější a často se vymykají všem známým postupům. Jsou vybaveni dobrými znalostmi, dostatečnými prostředky i časem.
Jejich motivace může být různá. Do této skupiny spadají nájemní zločinci a teroristé.

4.7.5 Útoky

Útoky můžeme rozdělit na pasivní útoky, útoky na převzetí moci, Dos a DDos útoky a sociální inženýrství.
O pasivním útoku mluvíme v případě, kdy se útočník nesnaží nijak modifikovat probíhající komunikaci. Hlavní nebezpečí tedy spočívá v tom, že je nesnadno identifikovatelný.
Trojský kůň – jedná se většinou o program, který umožňuje zaznamenávat přenášená data či stisky kláves. Tento program může být do systému oficiálně nainstalován, nebo tuto funkci plní některý jiný program, takzvaný trojský kůň.
Fyzický odposlech – útočník musí získat fyzický přístup k jednomu z komunikujících zařízení. V případě fixních sítí je třeba fyzicky připojit odposlechové zařízení, u mobilních plně dostačuje, aby se přijímač nacházel v dosahu signálu [3].



Obrázek 13: Pasivní útok (vlastní zpracování)

Útoky na převzetí moci

V některých případech není převzetí kontroly prostředkem ale přímo cílem. Útočník se například snaží získat data uložená na příslušném zařízení či je zničit.

Nejjednodušší je samozřejmě získání fyzického přístupu k počítači a provedení útoku přímo. Někdy se podaří uživatele donutit, jindy je špatně zabezpečená fyzická ochrana a k zařízení se dostane kdokoliv. Vhodnou obranou je zajištění kvalitní fyzické ochrany a zavedení autentizace uživatelů.

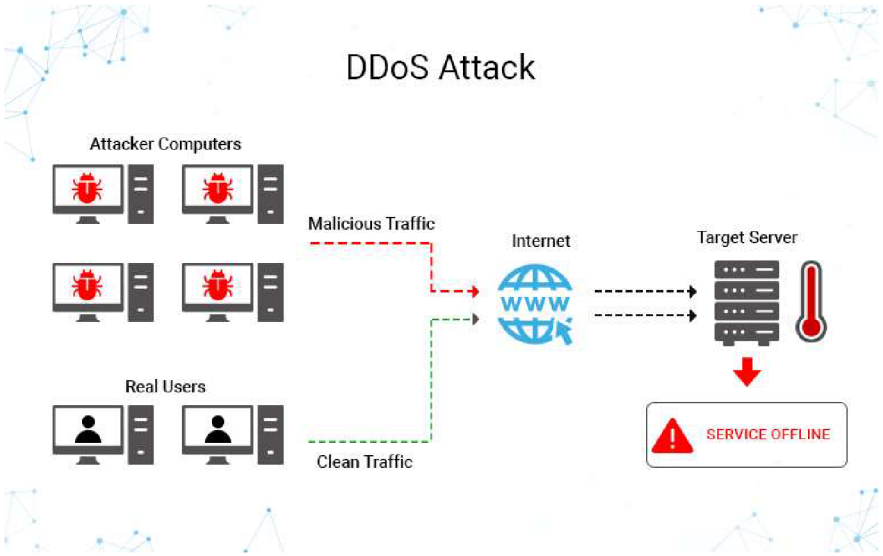
O něco složitější je vzdálený útok. Útočník musí nějakým způsobem instalovat a spustit program, kterému mu umožní provést útok na dálku. Toho může docílit například pomocí trojského koně, zaslaného emailem. Tento program pak může bez problému kopírovat do souboru všechna zadávaná hesla nebo otevírat vybrané porty. jednoduchým řešením je nastavení pravidla, které přímo na poštovním serveru zablokuje všechny spustitelné soubory.

Pokud se útočníkovi nepodaří nainstalovat žádný program, může využít známých chyb již nainstalovaného softwaru. Tyto útoky bývají většinou automatizované, útočníkovi tedy nic nebrání procházet postupně vybranou část adres a zkoušet, jak je které zařízení zabezpečeno [3].

DoS a DDoS

Útoky typu Denial of Services (DoS) a Distributed Denial of Services (DDoS) jsou jedněmi z nejčastěji prováděných útoků, které mohou vést k úplnému a dlouhodobému odstavení IT služeb poskytovaných napadeným prostředkem IT.

Systém poskytuje své služby na základě zaslaného požadavku. Požadavky na poskytnutí služby si dané zařízení zařazuje do fronty požadavků, kterou postupně v rámci svých možností vyřizuje.



Obrázek 14: DDoS útok (převzato z [15])

Kapacita fronty tedy není bezedná. V okamžiku, kdy je požadavků více než může zařízení vyřídit jsou některé požadavky odmítány.

Základní rozdíl mezi útoky typu DoS a DDoS je místo provedení. Útok DoS je realizován obvykle z jednoho nebo několika málo míst. To nám dává možnost tato místa identifikovat a preventivně, např. pomocí firewallu, síťový provoz z těchto míst blokovat. Oproti tomu je útok DDoS silně distribuován – zdrojů útoku je tak příliš mnoho, aby je bylo možné jednoduše blokovat. Jednoduché řešení takového útoku pak není možné [5].

Sociální inženýrství

Hlavní myšlenkou sociálního inženýrství je, že je zbytečné používat hrubou sílu na prolomení hesla. Mnohem jednodušší je donutit oběť, aby nám tuto informaci

sama sdělila. Největší nebezpečí sociálního inženýrství je, že si oběť často ani sama neuvědomí, že předala útočníkovi důvěrné informace.

Do této skupiny patří řada postupů, které lze využít pro získání citlivých informací nebo získání přístupu do jinak nepřístupných (bezpečných) lokací [5].

Phising – jedná se o nejrozšířenější techniku emailového podvodu. Jedná se o zaslání generického emailu, který zneužívá známe služby (nejčastěji banky). Podobné techniky jsou pak *Smishing* (vylákání informací pomocí falešných SMS) a *Vishing* (vylákání informací pomocí telefonického hovoru).

Pretexting – Tato technika je založena na zneužití falešné identity, kdy se útočník vydává za IT podporu, či za vedoucího zaměstnance, nebo například za nového investora společnosti. Díky postavení dané osoby je zneužito nepřímého nátlaku, či úrovni postavení dané osoby (útočníka), a tím je oběť zmanipulována a je ochotna vydat citlivé údaje.

Scareware – je technika na počítačích i na mobilních platformách, kdy útočník doručí oběti aplikaci, službu, či internetovou stránku, která obsahuje podvodnou informaci o tom, že počítač oběti byl napaden nebo zneužit škodlivým kódem, a je nutné stáhnout nějaký specializovaný software, který nákazu odstraní. Po jejím stažení a instalaci, pak útočník získá často neomezený přístup k danému zařízení a instaluje další malware do kompromitovaného zařízení.

Baiting – je kombinovaná technika, kdy je často využívána technika USB Dropping. Je postavena na zvědavosti lidí, za pomoci „nalezených“ USB disků, CD-ROM, či jiných médií. Popřípadě se může jednat o různé typy placeného software dostupného na veřejném úložišti, který si uživatel ze zvědavosti nainstaluje, ale tím zanese do zařízení i malware nebo backdoor, který útočník do aplikace umístil [16].

4.8 Normy

V dnešním globálním světě potřebují komunikovat všichni se všemi. Aby se mezi sebou domluvily systémy používané například ve Spojených státech a Evropě, je třeba omezit svobodu vývojářů a zavést pravidla [3].

4.8.1 Bezpečnostní normy

Existuje celá řada národních i mezinárodních organizací, které se vydáváním norem zabývají profesionálně. České úřady tyto normy v některých případech přebírají.

- **ISO – International** Organization for Standartisation
- **IEC – International** Electrotechnical Commision
- **ITU – Mezinárodní** telekomunikační unie

Kromě nadnárodních organizací existují i národní úřady, které část těchto norem přebírají.

- ANSI – American National Standards Institute
- DIN – Deutsche Institut for Normung

V České republice se normalizací zabývá normalizační institut. Normy vydávané tímto úřadem nesou označení ČSN. Pokud se jedná o normu převzatou od mezinárodní organizace, zůstává i původní označení. Normy jsou potom ve tvaru ČSN ISO/IEC XXXXX [3].

4.8.2 Standardy

Schvalování oficiálně vydaných norem je zdlouhavý proces, který rozhodně nedostačuje rychlému rozvoji internetových protokolů a služeb. Bylo teda potřeba zavést de facto standardy. Tyto normy nejsou oficiálně schválené a byly vytvořeny skupinou odborníků a zveřejněny na internetu.
Zvláštní postavení mají normy, které vydá významná společnost v oboru společně s novou technologií. Z pozice síly se pak snaží konkurenty v oboru přesvědčit

k používání této normy, což, v případě úspěchu, znamená obrovský náskok ve vývoji.

4.8.3 Důležité normy

ISO/IEC 27001 Management bezpečnosti informací

ISO/IEC 27001 je mezinárodní norma pro řízení bezpečnosti informací. Definuje, jak zavést nezávisle oceňovaný a certifikovaný systém řízení bezpečnosti informací. Norma se zaměřuje na ochranu a bezpečnost dat a informací, tedy minimalizuje pravděpodobnost, že někdo získá nelegální či neautorizovaný přístup k těmto datům [20].

ISO IEC 20000-1 Management služeb pro informací technologie

Je soubor standardů pro poskytovatele IT služeb, který shrnuje osvědčené postupy pro zachování bezpečnosti, poskytování konzistentních služeb a přijímání nových technologií. Tato norma stanovuje požadavky na systém, zásady správné praxe, vztahy, řešení a kontrolní procesy a další. Zatím poslední revize byla zveřejněna v roce 2011 [21].

5 Praktická část

Cílem praktické části je demonstrovat, jak lze dostupnými prostředky dostat citlivá data z uživatelských zařízení. Ukázka bude demonstrovaná na telefonech s operačním systémem Android a laptopech s operačním systémem Windows.

Součástí praktické části je také návrh zásad na ochranu dat na těchto zařízeních. Návrh bude vycházet z poznatků teoretické práce a výsledků demonstrace z části praktické.

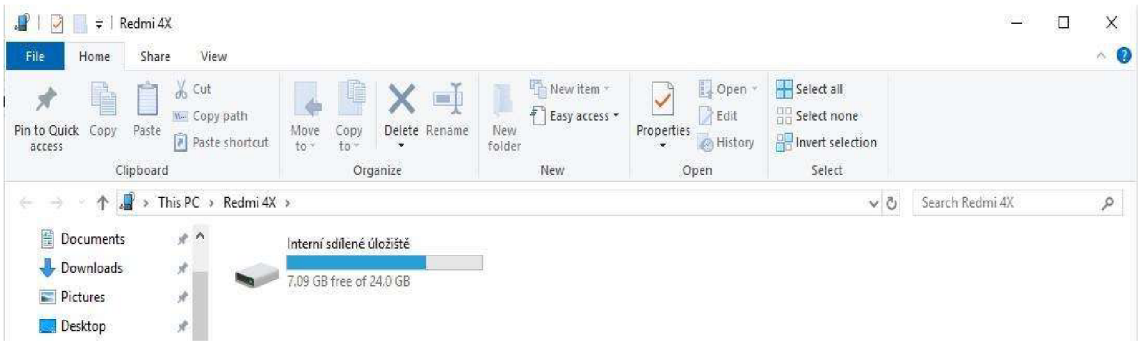
5.1 Šifrování

5.1.1 Nešifrované zařízení Android

První modelový příklad, který bude demonstrován, je situace, kdy se útočník dostane k mobilnímu telefonu se znalostí PIN kódu. Může se jednat o situaci, kdy je PIN kód odpozorován při manipulaci se zařízením ve veřejném prostoru, například v kavárně. Z nestřeženého telefonu je pak možné nepozorovaně vykopírovat data, například na útočníkův laptop.

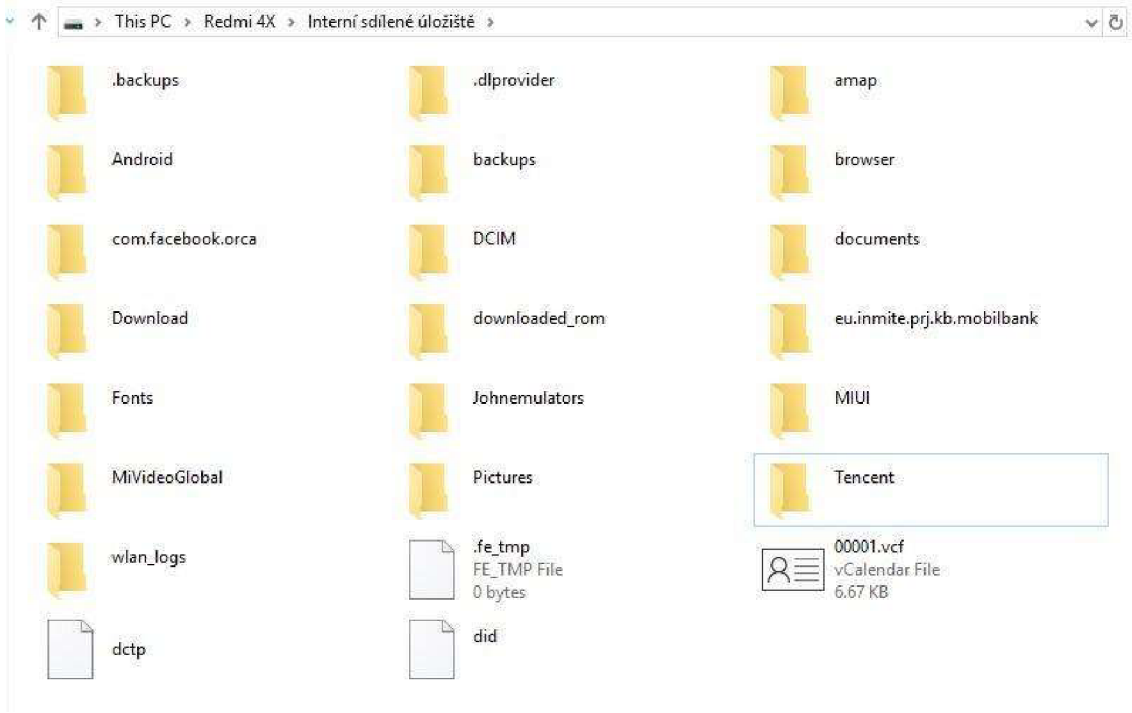
Tento případ bude demonstrován na mobilním telefonu Xiaomi Redmi 4X. Verze operačního systému Andriod je 7.1.2 N2G47H s verzí MIUI 10.0.2. Operační systém je aktualizován na poslední stabilní verzi.

Po připojení zařízení k PC pomocí USB kabelu, se telefon tváří jako velkokapacitní zařízení, na které lze volně přistupovat.



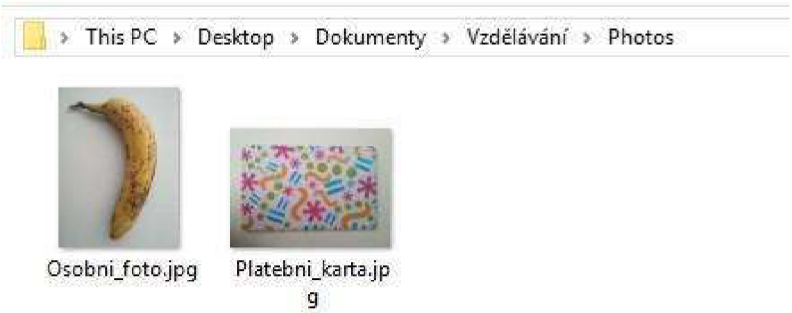
Obrázek 15: Interní úložiště mobilního zařízení

Struktura složek je ve většině zařízeních podobná, lze se v ní tedy velmi snadno zorientovat a dostat se k datům, které útočníka zajímají nejvíce. V modelovém příkladě jsou na telefonu uloženy fotografie osobni_foto.jpg a platebni_karta.jpg. Záměrem útočníka je tyto soubory odcizit tak, aby uživatel o jejich samotném odcizení nevěděl.



Obrázek 16: Struktura složek mobilního zařízení android

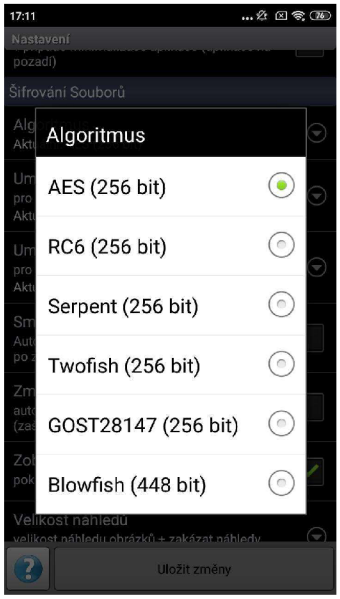
Fotografie jsou uloženy ve složce DCIM. Jelikož složka ani soubory nejsou nijak šifrované, je jejich vykopírování otázkou několika vteřin. V zařízení útočníka jsou pak soubory čitelné a lze s nimi volně manipulovat. Uživatel se o jejich odcizení vůbec nemusí dozvědět.



Obrázek 17: Nešifrované soubory

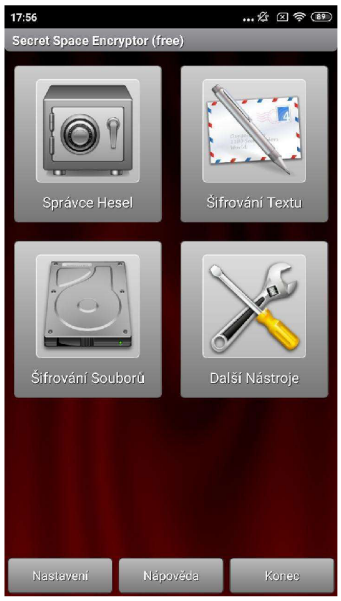
5.1.2 Šifrování souborů na mobilním telefonu Android

Pro šifrování souborů v zařízení s operačním systémem Android lze využít nástroje třetí strany. Pro účel demonstrace byl vybrán software SSE – File/Text Encryption & Password Vault od společnosti Paranoia Works. Tento program je v základní verzi zdarma, lze však koupit další podpůrné moduly. V nastavení lze také vybrat způsob šifrování a program je přeložen do českého jazyka, což usnadní práci uživatelů, kteří neovládají cizí jazyk. Umožňuje také šifrování textu a obsahuje správce hesel.



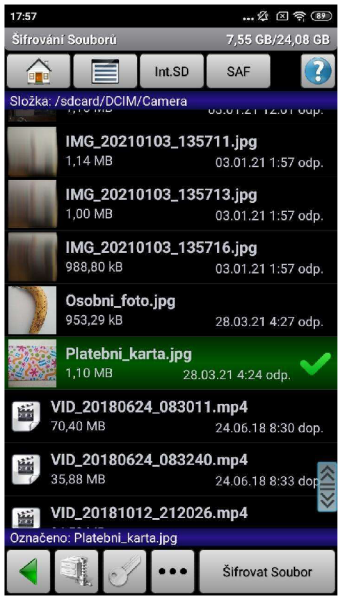
Obrázek 18: Výběr algoritmu pro šifrování v programu SSE

Algoritmus pro šifrování souborů je nastaven na AES (256 bit), což je defaultní hodnota. Je také vhodné nastavit automatické smazání souboru po jeho úspěšném zašifrování. V opačném případě je potřeba zašifrovaný soubor smazat ručně.



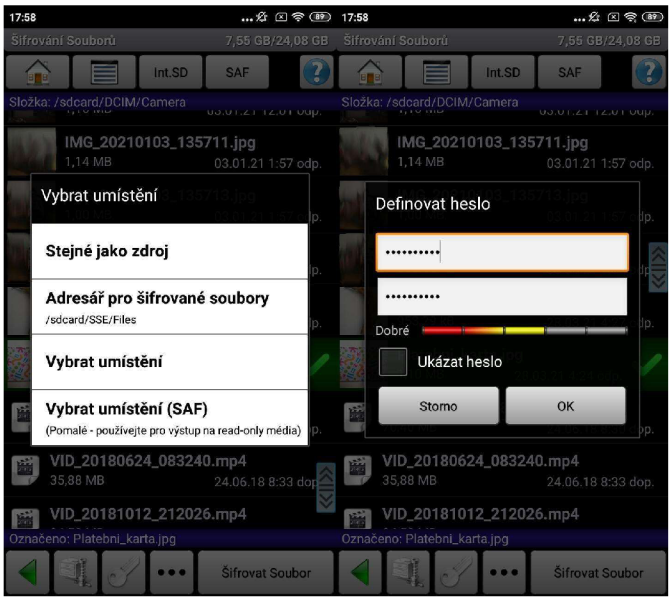
Obrázek 19: Možnosti programu SSE

Z hlavního menu je nutné vybrat možnost šifrování souborů. Tato možnost zobrazí strukturu složek, ve které je potřeba najít soubory, které uživatel potřebuje zašifrovat. V případě potřeby zašifrovat celou složku, je uživateli umožněno ji vybrat dlouhým stiskem.



Obrázek 20: Výběr souborů pro šifrování

Po vybrání souboru nebo složky k zašifrování je uživatel vyzván k zadání hesla a výběru umístění pro šifrovaný soubor.



Obrázek 21: Proces šifrování v programu SSE

Pro zvolení umístění a hesla se soubor zašifruje. Pokud není v nastavení zvolena možnost smazání původního souboru po jeho šifrování, musí uživatel původní soubor smazat. V opačném případě by se útočník mohl dostat k původním datům.

5.1.3 Šifrované zařízení Android

Po zašifrování souborů pomocí softwaru SSE – File/Text Encryption & Password Vault se soubory pro útočníka stávají nečitelnými. Bez znalosti hesla je nemožné soubor otevřít.

Obrázek 22: Reprezentace šifrovaných souborů v prostředí programu SSE

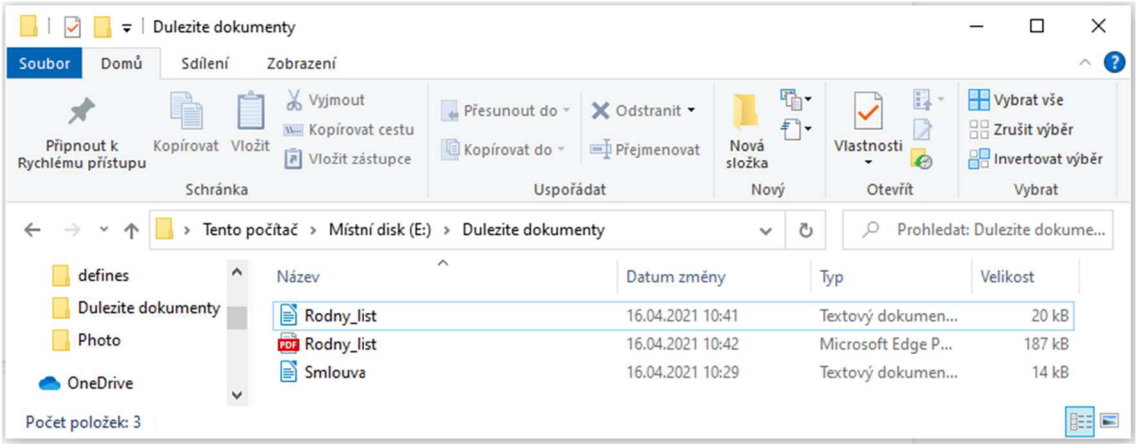
Citlivé soubory jsou zašifrovány ve formátu ENC. Tento formát souborů je použit pro šifrované soubory, které se dají pouze programem, ve kterém byly zašifrovány. I když jsou ale zašifrovány, stále může dojít k jejich ztrátě, jelikož jsou stále uloženy na úložišti mobilního zařízení. Pokud uživatel nechce o takto zašifrovaná data přijít, měl by zvážit jejich zálohování. Ideální úložiště je například Google Drive, z mobilního zařízení je nahrání souboru pohodlné a rychlé, nevýhoda spočívá v nutnosti mít zařízení připojené k internetu.

5.2 Bezpečné mazání dat

5.2.1 Neskartované soubory a jejich obnova

Většina uživatelů považuje přesunutí souboru do koše a jeho následné vysypání jako dostatečnou metodu odstranění dat. Ve skutečnosti ale operační systém označí místo na disku jako prázdné, a až do přepsání tohoto místa jinými daty lze soubor obnovit.

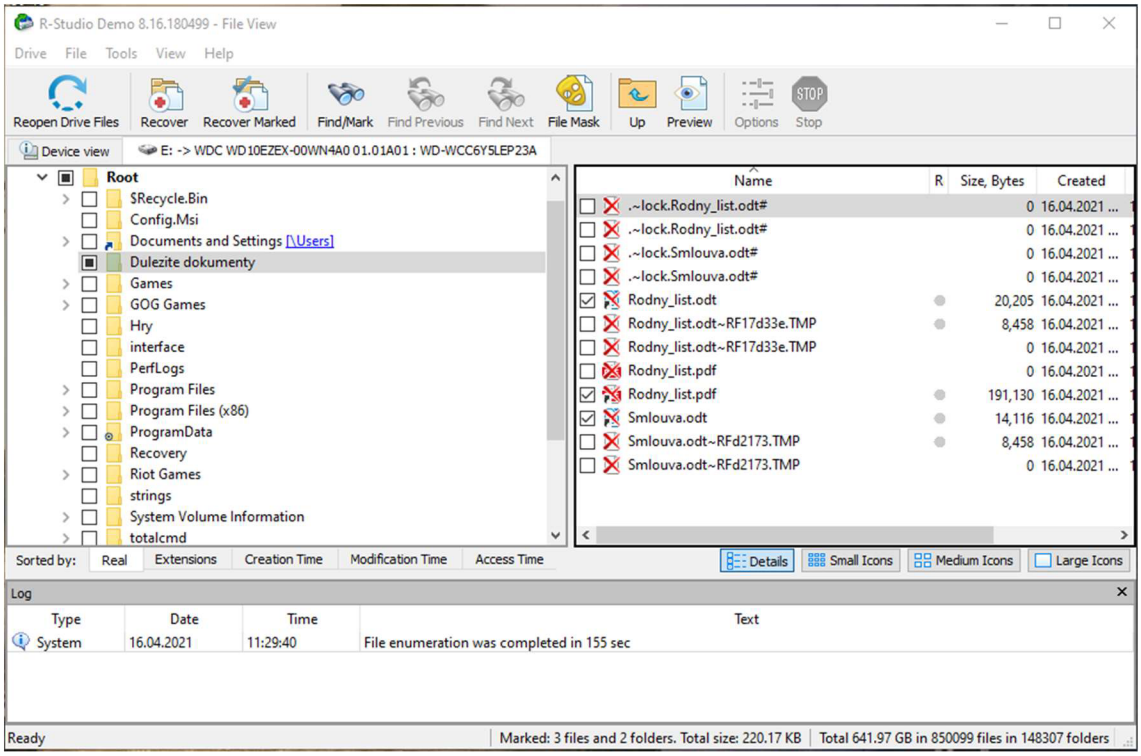
Pro ukázku jsou na harddisku vytvořeny testovací soubory, které budou nesprávně smazány a následně obnoveny. Pevný disk je připojen ke stolnímu PC přes rozhraní SATA a namapován jako sekundární disk. Na primárním SSD disku je nainstalován operační systém Windows 10 Pro a software pro obnovu dat R-Studio (verze 8.16). Pro účel demonstrace bude využita pouze demo verze.



Obrázek 23: Testovaci soubory

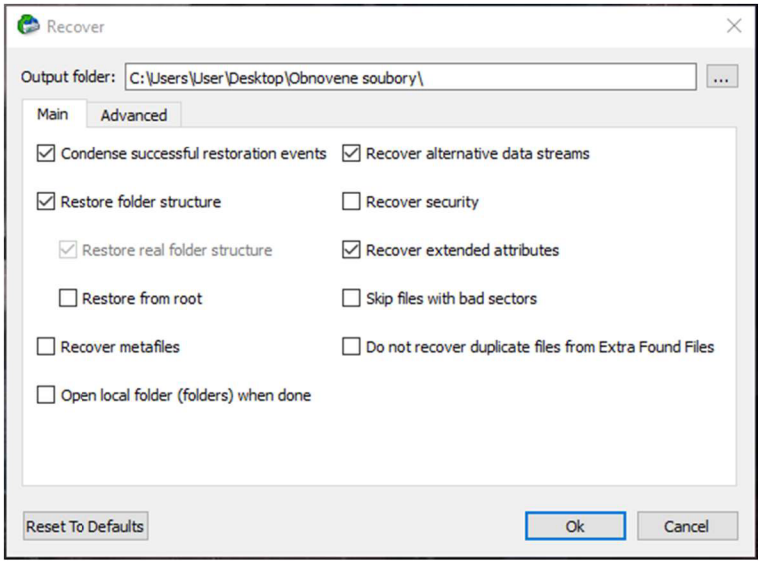
Testovací soubory byly smazány standardním způsobem, tedy přesunem do koše a následném odstranění z koše. Operační systém tedy reprezentuje tyto soubory

jako smazané. Pomocí softwaru R-Studio byl proveden sken celého HDD disku. Sken odhalil i soubory, které byly smazány a operační systém je dále nevidí.



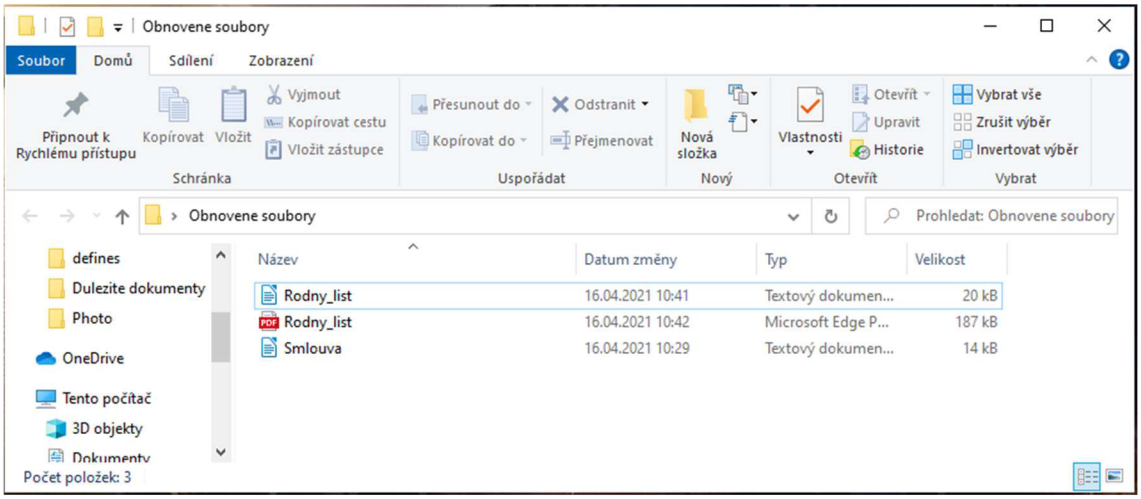
Obrázek 24: Smazané soubory reprezentované v prostředí softwaru R-Studio

Po naskenování souborů program umožňuje buď obnovit vše, nebo vybrat, které soubory budou obnoveny. Vzhledem k tomu, že smazané soubory jsou známé, včetně umístění, byla vybrána možnost obnovení konkrétních souborů.



Obrázek 25: Možnosti obnovení

Pro obnovu je nutné nastavit parametry obnovení. Na obrázku 25 je vidět defaultní nastavení, které bylo ponecháno i pro účely demonstrace. Je nutné vybrat umístění, do kterého budou soubory obnoveny. Zde je důležité si uvědomit, že uložení souborů na disk, ze kterého je obnovujeme není ideální. Mohlo by dojít k přepsání místa, kde se původní data nacházela, a to by mohlo vést k poškození původních souborů.

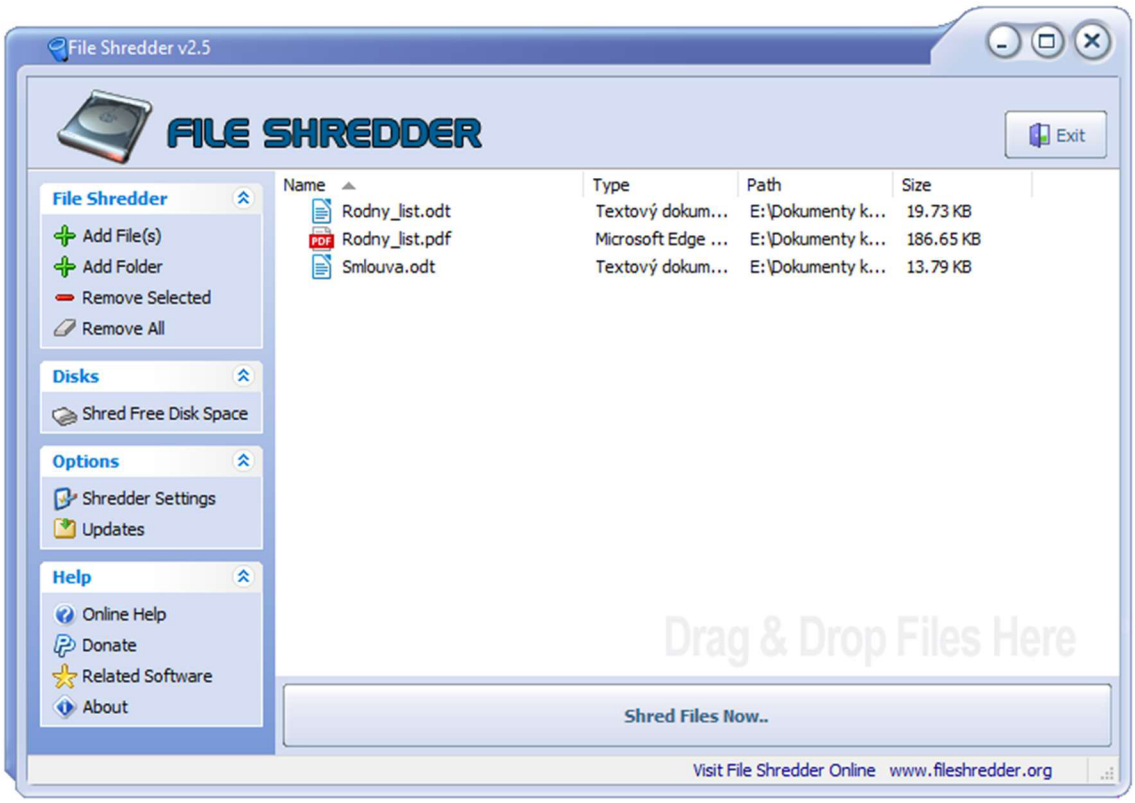


Obrázek 26: Obnovené soubory

5.2.2 Skartované soubory a jejich obnova

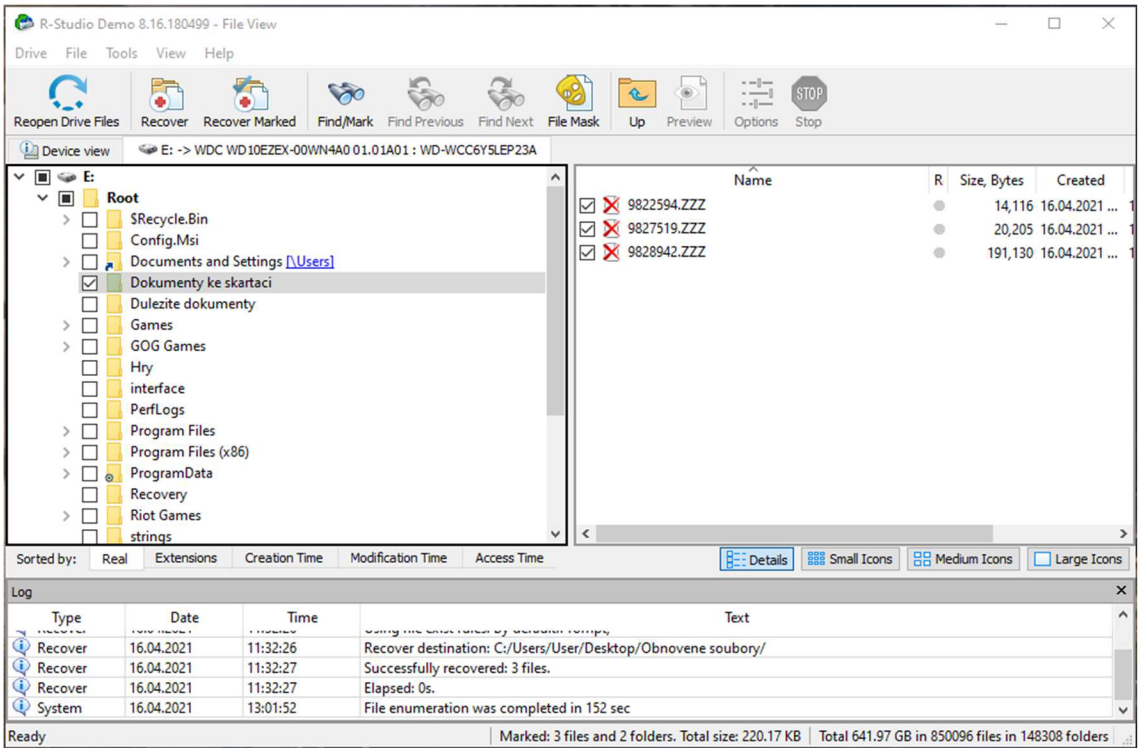
Pro bezpečné smazání dat je potřeba využít specializovaného softwaru. Pokud by uživatel potřeboval bezpečně smazat celý disk, například při prodeji svého notebooku, je vhodné využít Hiren's BootCD. Tento software umožňuje vytvořit flash disk nebo CD s prostředím, do kterého je možné se nabootovat při startu zařízení. V tomto prostředí je k dispozici několik utilit, například pro diagnostiku hardwaru a také pro bezpečné smazání celého disku.

Pokud chce uživatel smazat pouze konkrétní soubory, může využít několik programů, které umožní vybrat konkrétní data pro skartaci. Jedním z těchto programů je například File Shredder, který je k dispozici zdarma s možností dobrovolného příspěvku pro autora.



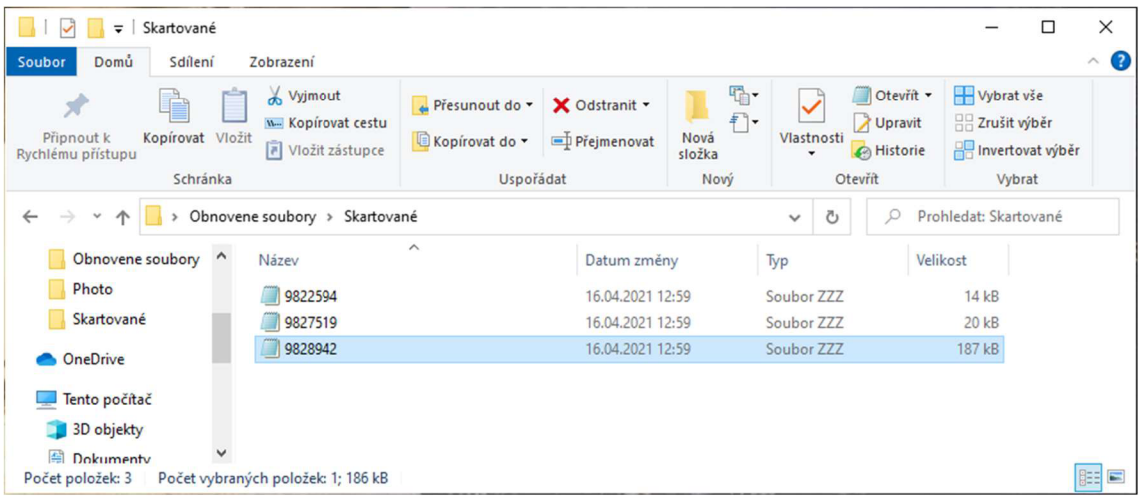
Obrázek 27: Soubory ke skartaci

V prostředí programu File Shredder je možnost vybrat ke skartaci konkrétní soubory nebo celé složky. Pro demonstraci byly vybrány pouze konkrétní soubory, které je vhodné vzhledem k jejich obsahu bezpečně smazat.



Obrázek 28: Reprezentace skartovaných souborů v prostředí programu R-Studio

Při pokusu o obnovu je patrné, že naskenování disku sice našlo smazaná data, ale už není možné je spolehlivě přečíst. Při pokusu o obnovu se soubory obnoví, ale jsou již nečitelné.



Obrázek 29: Obnovené soubory po skartaci

5.3 Návrh zásad ochrany dat na mobilních zařízeních

5.3.1 Fyzická ochrana

Fyzická ochrana je jeden z nejjednodušších a nejlevnějších opatření, jakým může uživatel svoje data ochránit. Jelikož jsou mobilní zařízení ze své podstaty malé a lehké přístroje, je pro útočníka velmi jednoduché se k nim dostat anebo je odcizit. Uživatelé by proto měli dbát na to, aby mobilní telefony nebo laptopy nenechávali volně přístupné a bez dozoru na veřejných místech, jakou jsou kavárny, bary nebo restaurace. I malá chvilka může útočníkovi stačit, aby se zařízení zmocnil, nebo se pokusil o přístup k systému, s cílem zcizit důležité informace nebo nainstalovat škodlivý software.

Pokud není možné vzít si mobilní telefon nebo notebook s sebou a tato zařízení pak zůstávají například v kanceláři, kde se pohybuje víc lidí, je vhodné využít uzamykatelný box nebo šuplík. Pro notebooky lze také využít zámky, které sice útočníkovi nezabrání dostat se fyzicky k přístroji, ale zamezí mu v jeho odcizení. Pokud by se tedy snažil o přístup nebo instalaci škodlivého softwaru, byl by nucen tuto činnost provádět na veřejném místě, což zvyšuje pravděpodobnost, že si někdo neoprávněného zacházení s hardwarem všimne. Toto nebezpečí může útočníka znejistit anebo ho zcela odradit.

Důležité zásady fyzické ochrany

- Nenechávejte svoje zařízení bez dozoru na veřejných místech.
- Pokud není možné si zařízení odnést, zamkněte ho.

5.3.2 Bezpečné heslo

Tvorba silného hesla je jedno ze základních opatření, kterým uživatelé mohou chránit svá data. Pro heslo platí několik zásad, kterými by se měli při jeho tvorbě řídit.

Délka hesla by měla být minimálně 8 znaků, obecně lze ale doporučit alespoň 14 znaků. Mělo by se jednat o kombinaci čísel a znaků, malých a velkých písmen. Uživatelé by také neměli volit běžná, často používaná hesla. Například heslo “Password.123” kombinuje všechna zmíněná doporučení, obsahuje ale velmi často

používané slovo a sérii čísel. Automatizovanému programu, který má k dispozici slovník, by prolomení trvalo maximálně několik vteřin.
Jako heslo by se také neměli používat informace, které jsou snadno dohledatelné. V době, kdy je na sociálních sítích snadné dohledat podrobnosti, je důležité se při tvorbě hesla zabývat otázkou, jestli útočník dokáže heslo odhadnou z údajů, které uživatel vyplní na svém veřejném profilu. Nevhodná je například kombinace jména a data narození, jméno domácího mazlíčka nebo členů rodiny.

Důležité zásady pro bezpečné heslo

- Délku hesla zvolte minimálně 8 znaků
- Kombinujte číslice, znaky, velká a malá písmena
- Nepoužívejte častá a známá hesla
- Nepoužívejte hesla, která se dají uhodnout jen díky znalosti veřejných informací, jako je třeba datum narození nebo jméno dcery

5.3.3 Nakládání s heslem

Nakládání s heslem je pro bezpečnost stejně důležité, jako jeho tvorba. Heslo do systému by měl znát pouze uživatel, který je oprávněn do toho systému přistupovat a pracovat v něm. Nikdo, ani administrátor systému, není oprávněn požadovat po uživateli heslo.
Uživatelé by neměli používat stejné heslo do všech zařízení a služeb, které používají. Heslo do emailu by nemělo být stejné jako heslo pro přihlášení do zařízení. tato zásada však může přinášet i řadu nevýhod. Vzhledem k velkému počtu hesel je pro uživatele složité si je všechny zapamatovat, a to může vést k tomu, že s nimi uživatelé nevhodně nakládají.
Přilepení papírku s heslem na notebook je typický příklad nevhodného zacházení s heslem. Pokud by se útočník k takovému zařízení dostal, dokáže se i přes složitost hesla bez problému autentizovat.
Pro ukládání hesel je proto vhodné použít správce hesel, jako je například KeePass, což je speciální program, která všechna hesla ukládá do šifrované databáze, která je chráněna hlavním heslem.

Důležité zásady pro nakládání s hesly:

- Nikdy nikomu neříkejte své heslo.
- Heslo nepište na papírek, který je volně přístupný.
- Do každého systému používejte jiná hesla.
- Pokud si hesla potřebujete zapsat, používejte speciální software pro ukládání hesel, například KeePass.

5.3.4 Aktualizace

Dalším důležitým aspektem je pravidelná aktualizace systému a všech nainstalovaných aplikací. Útočníci často využívají bezpečnostních děr, pomocí kterých mohou infiltrovat systém.

Vydavatelé softwaru a operačních systémů tyto díry pravidelně opravují formou aktualizací, a tím podstatně snižují riziko infiltrace systému.

Aktualizace antivirových programů také doplňuje jejich databázi známých virů, díky kterým pak mohou lépe chránit zařízení.

Důležité zásady aktualizací:

- Pravidelně kontrolujte, jestli je váš systém aktuální.
- Pokud vám systém nebo aplikace nabídne aktualizaci, proveďte jí.

5.3.5 Antivirové programy

Antivirový program je software, který slouží k identifikaci a eliminaci počítačových virů, jako je například malware a spyware, a škodlivého softwaru.

Správné nastavení a pravidelné kontroly zařízení, prováděné pomocí antiviru, chrání uživatelská data před jejich zneužitím. Po instalaci navíc antivir sám provede scan zařízení a odhalí případné hrozby.

V současné době je možné využít širokou nabídku antivirových programů, které nabízejí základní ochranu zcela zdarma. Vydavatelé těchto programů navíc velmi často podporují více operačních systémů, lze tak stejným antivirem chránit jak laptop, tak mobilní telefon, ať už s iOS nebo Andriod.

Z antivirů, dostupných na trhu, lze doporučit Avast, který je nabízen v základní verzi zdarma, nebo v rozšířené verzi za roční poplatek. Stejný obchodní model má také antivirus Kaspersky nebo AVG.
V následující tabulce je srovnání základní verze zdarma a placené verze programu Avast.

	Free antivirus	Premium security
V reálném čase odhalí viry, ransomware a jiné hrozby	✔	✔
Odhalí nepovolané uživatele a bezpečnostní nedostatky v síti	✔	✔
Uloží hesla do zabezpečeného souboru a umožní přihlašovat se k webovým stránkám jedním kliknutím	✔	✔
Ochrání osobní fotografie a soubory před zašifrováním ransomwarem	✔	✔
Ochrání hesla a údaje o platebních kartách před zneužitím	×	✔
Umožní testovat bezpečnost aplikací v Sandboxu – dříve, než jsou spuštěny v počítači	×	✔
Ochrání váš počítač před hackery pokročilým firewallem	×	✔
Ochrání poštu před obtěžujícími nevyžádanými e-maily	×	✔

Ochrání před špehováním přes webovou kameru	×	✔
Vymaže soubory tak, že už je nikdo nedokáže obnovit	×	✔
Omezí bezpečnostní rizika tím, že programy udržuje neustále aktuální	×	✔

Tabulka 3: Porovnání funkcí antiviru Avast v placené a free verzi

Ze srovnání je patrné, že i verze, které jsou zdarma, dokáží odvrátit největší hrozby. Pro kompletní ochranu je ale třeba zvážit investici do placené verze. Škody, které může útočník napáchat, jsou často mnohem finančně náročnější než roční poplatek za antivirový program.

Důležité zásady ochrany pomocí antivirových programů:

- Používejte alespoň základní edici antivirového systému.
- Pokud jsou vaše data cenná, zvažte upgrade na placenou verzi.
- Udržujte svůj antivirový program vždy aktualizovaný.
- Provádějte pravidelné kontroly vašeho zařízení pomocí antivirového programu.

5.3.6 Zálohování

Zálohování je jeden ze způsobu, jak ochránit svá data. V případě ztráty nebo zničení zařízení, což je například v případě mobilního telefonu velmi běžné, se společně se zařízením ztratí nebo poškodí také data. Zatímco hardware lze nahradit snadno, získat zpět ztracená data je v některých případech takřka nemožné.

Tomu může uživatel zabránit, pokud pravidelně zálohuje obsah svého zařízení. Fotky, videa, ale i soubory nebo celé složky z telefonu používající systém Android, je možné zálohovat do Google účtu. V případě ztráty nebo poškození pak lze soubory jednoduše obnovit na novém telefonu.

Podobnou funkci nabízí i systém iOS, kde je možné zálohovat do iCloudu. Pro zálohu dat na laptopech používající systém MS Windows je vhodné využít Google cloud.

Výhoda cloudu je, že se ke svým souborů uživatel dostane z jakéhokoliv jiného zařízení.
Nevýhoda zálohování do online úložiště je, že aby byla data přístupná, je potřeba připojení k internetu. Kapacity také nejsou neomezené, pro zvětšení prostoru pro data poskytovatel požaduje platbu, často ve formě měsíčního, čtvrtletního nebo ročního předplatného.
Pokud je potřeba mít přístup k datům i za předpokladu, že je uživatel offline, je možné provádět zálohu na flash disk, nebo využít velkokapacitní externí disky. V operačním systému Windows lze nastavit pravidelné plány, které automaticky vytváří zálohy vybraných složek a souborů do požadovaného umístění.
Nevýhoda externích disků je, že při větší velikosti zálohovaných dat je potřeba investovat do větších úložišť. Může také dojít k hardwarové závadě, která může vést i ke ztrátě zálohovaných dat. Tomu se dá zabránit pomocí jednotek NAS. jedná se o chytrá uložiště, která kombinují více disků a obsahují technologii RAID, která dokáže data ochránit i při poruše disku. tato zařízení jsou však velmi nákladná a jejich pořizovací hodnota často bývá násobně vyšší než koupená kapacita online cloudu.
Důležité zásady zálohování:

- Zálohujte data, o které nemůžete přijít.
- Nastavte si automatické zálohování v operačním systému.
- Pokud zálohujete na externí disk, použijte systém NAS s technologií RAID.

5.3.7 Šifrování

Pokud dojde ke ztrátě nebo odcizení přístroje, jako je laptop nebo telefon, může se útočník k datům dostat i bez znalosti hesla či PIN kódu. Data, která nejsou šifrovaná, lze ze zařízení přečíst bez větších potíží.
Aby se takovým situacím zabránilo a data byla chráněná, je vhodné provést jejich šifrování. Šifrování je proces, který pomocí kryptologie převádí nešifrovaná data na šifrovaná. Takto zabezpečená data pak lze přečíst pouze pomocí dešifrovacího klíče.

U mobilních zařízení je šifrovací mechanismus součástí operačního systému. Android i iOS nabízí možnost šifrování přímo v nastavení, pro zašifrování je nutné si zvolit PIN, heslo nebo gesto pro dešifrování.
V operačním systému Windows lze využít nástroj BitLocker, který je vyvíjený společností Microsoft. Tento nástroj však není k dispozici v edici Windows 10 Home. Pro šifrování lze využít i software třetích stran. Nástroj TrueCrypt je open source software, který je podporován na platformách Windows, Linux a Mac OS X. TrueCrypt umožňuje uložení dat následujícími způsoby:

- Je vytvořena virtuální disková jednotka v podobě souboru. Tato metoda není ideální, v případě, že na fyzickém mistu není dostatečná kapacita, může dojít k poškození dat.
- TrueCrypt zašifruje celý diskový oddíl.
- Šifrovaný systémový oddíl, v tomto případě je při spuštění požadované heslo a operační systém je spuštěný až po jeho zadání. Šifrované jsou také všechny soubory na dané oddílu.

Další způsob, jak může uživatel chránit svá data, je využít pro jejich uložení speciální flash disky s šifrováním. Jedná se o speciální USB zařízení, které je hardwarově zabezpečeno. Nejčastěji jsou používané k přenosu citlivých informací.
Zásady k šifrování:

- Pro citlivá data využívejte šifrování.
- Pokud není šifrovací nástroj součástí operačního systému, použijte specializovaný software, například TrueCrypt .

5.3.8 Bezpečná likvidace dat

Mobilní zařízení jsou častou komoditou na trhu s použitou elektronikou. Pokud chce uživatel svoje zařízení prodat nebo vyhodit, měl by se zamyslet nad tím, jak naložil s daty.
Pro bezpečná nakládání s citlivými daty je důležitá také jejich bezpečná likvidace. Smazání souboru a vysypání koše není dostatečné a takto smazaný soubor se dá

pomocí běžných nástrojů obnovit. Je proto nutné zvolit vhodnější metodu pro likvidaci dat.

Jako nejúčinnější způsob je fyzická skartace média. Existuje mnoho firem, který se zabývají fyzickou likvidací dat. K tomu může dojít pomocí demagnetizace média, nebo jeho rozstříhání pomocí speciálních přístrojů. Tyto firmy se řídí platnými zákony a dodržují stanovené normy, po likvidaci vám také vystaví certifikát s potvrzením o bezpečné likvidaci.

Často však není pro uživatele vhodné hardware fyzicky zničit, například při prodeji. Pro mobilní zařízení je v tomto případě nutné použít specializovaný software, jako je například iShradder, Shreddit nebo Data Eraser. Tyto programy přepíší místo, kde byl soubor uložen náhodnými znaky. Uživatel si může vybrat, v kolika cyklech přepsání proběhne.

Pro zařízení s operačním systémem Windows je také potřeba využít programů jako je Eraser, který umožňuje jednotlivé soubory bezpečně mazat. Pro celkové smazání disku, včetně systému, je nutné použít specializované nástroje. Ty nabízí například balíček Hiren's boot, který kromě diagnostických nástrojů nabízí i ty na bezpečné mazání dat.

Zásady pro bezpečné mazání dat:

- Pokud se zbavujete zařízení, zvažte, jestli není vhodná fyzická likvidace.
- Pro bezpečné mazání dat používejte specializované nástroje.

6 Shrnutí výsledků

Výsledek práce ukazuje, že nezabezpečená uživatelská data jsou pro útočníka snadným cílem. Pro jejich odcizení a zneužití dnes nemusí útočník disponovat velkými znalostmi a lze je realizovat pomocí volně dostupných prostředků.

Uživatel ale může svoje data zabezpečit pomocí nástrojů a programů, které jsou v mnoha případech v základní verzi zdarma. Tato ochrana útočníkovi značně ztíží zneužití nebo krádež dat a v mnohých případech ho může i úplně odradit.

7 Závěry a doporučení

V současné době, kdy jsou mobilní zařízení masivně rozšířena, by měli být uživatelé seznámeni se základními pravidly ochrany dat. Uživatelé by měli vědět, jaká rizika jim hrozí a jak se jim bránit.

Teoretická část je věnována historii a vymezení pojmu bezpečnost dat. Dále je zde popsáno dělení fyzické bezpečnosti a autentizace a řízení přístupu. Je zde také podrobně popsána kryptologie.

V teoretické části je také podrobně popsán škodlivý software a ochrana pomocí antivirových programů. Je zde také kladen důraz na útočníky, jejich motivaci a druhy prováděných útoků.

Poslední oblast, které se teoretická část věnuje jsou bezpečnostní standardy a normy s konkrétními ukázkami nejdůležitějších norem v oblasti počítačové bezpečnosti.

V praktické části jsou demonstrovány ukázky šifrování souborů na mobilních zařízeních s operačním systémem Android. Tyto ukázky jsou zaměřeny na porovnání získání nešifrovaných dat, jejich následné zabezpečení a demonstrace získání šifrovaných dat.

Praktická část dále obsahuje ukázku bezpečného smazání dat, kde je demonstrováno obnovení souborů, které nejsou nevratně smazány. Dále je zde ukázán způsob bezpečného mazání pomocí softwaru třetí strany a pokus o obnovení takto odstraněných souborů.

Dalším cílem bylo navrhnout soubor zásad a doporučení pro bezpečné nakládání s citlivými daty, které vychází z informací teoretické části a praktických ukázek.

Bakalářská práce tedy přináší přehled možností, kterými se mohou uživatelé řídit a zabezpečit tak svoje data. Všechna doporučení jsou podložena teoretickým výzkumem a demonstrací praktických ukázek.

- # Seznam tabulek

- # Seznam obrázků

8 Seznam použité literatury

[1] ŽILKA, Radek. Bezpečnost informací. Dostupné z: http://www.vtpup.cz/cs/download/vavpropraxi/vav-prezentace/15-bezpecnost-informaci.pdf

[2] (PDF) Computer Security and Mobile Security Challenges. ResearchGate | Find and share research [online]. Copyright © 2008 [cit. 3.04.2021]. Dostupné z: https://www.researchgate.net/publication/298807979_Computer_Security_and_Mobile_Security_Challenges

[3] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

[4] DOBDA, Luboš. Ochrana dat v informačních systémech. 1. vyd. Praha: Grada Publishing, 1998, 286 s. ISBN 80-716-9479-7.

[5] ŠENOVSKÝ, Pavel. Počítačové sítě a ochrana dat [online]. VŠB – Technická univerzita Ostrava: Ostrava 2015, 88 str., dostupné z https://fbiweb.vsb.cz/~sen76/data/uploads/skripta/poitaove-sit-a-ochrana-dat.pdf

[6] LOBKOVSKY MEITIV, Alexander. Are Android unlock patterns as secure as numeric PINs? [online]. 2020 [cit. 2021-03-1]. Dostupné z: https://playingwithmodels.wordpress.com/?s=android

[7] RSA SecurID | IPTP Networks. [online]. Copyright © 2021 [cit. 14.03.2021]. Dostupné z: https://www.iptp.net/en_US/business-solutions/security/rsa-securid/

[8] Samsung Will Make the Galaxy S10's Fingerprint Sensor Even Better | Digital Trends. [online]. Copyright ©2021 Designtechnica Corporation. All rights reserved. [cit. 14.03.2021]. Dostupné z: https://www.digitaltrends.com/mobile/samsung-galaxy-s10-fingerprint-sensor-improvements-news/

[9] FAR and FRR: security level versus user convenience. Gebruikersvriendelijke biometrische beveiliging van hoge kwaliteit [online]. Dostupné z: https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience

[10] Replay Attack – GeeksforGeeks. GeeksforGeeks | A computer science portal for geeks [online]. Dostupné z: https://www.geeksforgeeks.org/replay-attack/

[11] SORIANO, Miguel. Zabezpečení informací a sítí. Vydání: 1. České vysoké učení technické v Praze. ISBN 978-80-01-05296-9

[12] BITTO, Ondřej. HISTORIE KRYPTOLOGIE. Faculty of Informatics Masaryk University [online]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm

[13] AMMIROVÁ, Kamilla. Úvod do kryptografie [online]. 2007 [cit. 2021-03-1]. Dostupné z: https://sifrovani.fd.cvut.cz/asym_algo.html

[14] Proč a jak na šifrování disků v Linuxu? [online]. 2008 [cit. 2021-01-31]. Dostupné z: https://www.root.cz/clanky/proc-a-jak-na-sifrovani-disku-v-linuxu/

[15] How Can You Prevent DDOS Attacks With Log Analysis. Tek-Tools: IT Management Software Reviews [online]. Copyright © 2021 SolarWinds Worldwide, LLC. All rights reserved. [cit. 14.03.2021]. Dostupné z: https://www.tek-tools.com/apm/detect-ddos-attack-with-log-analysis

[16] HEJDA, Daniel. Techniky sociálního inženýrství [online]. 2020 [cit. 2021-03-1]. Dostupné z: https://www.kpcs.cz/cs/novinky/blog/techniky-socialniho-inzenyrstvi

[17] KOHOUT, Roman a Radek KARCHŇÁK. Bezpečnost v online prostředí. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.

[18] Co je počítačový virus? | Nástroj na nalezení a odstranění virů | Avast. [online]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus

[19] Co je ransomware a jak se ho zbavit | Avast. [online]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware

[20] ISO/IEC 27001 Bezpečnost informací | BSI Česká republika. Standards, Training, Testing, Assessment and Certification | BSI [online].

Copyright © The British Standards Institution [cit. 14.03.2021]. Dostupné z: https://www.bsigroup.com/cs-CZ/ISO-IEC-27001-Bezpecnost-informaci/

[21] Jaké standardy se vztahují na odvětví informačních technologií?. [online]. Dostupné z: https://www.nqa.com/cs-cz/certification/sectors/information-technology

[22] Jak vymazat data nebo pevné disky bezpečně a nenávratně ITIGIC. Technical How-to's, Tips, and Tricks | ITIGIC [online]. Copyright © 2021 ITIGIC [cit. 14.03.2021]. Dostupné z: https://itigic.com/cs/erase-data-or-hard-drives-safely-and-irretrievably/

[23] Bezpečné mazání dat: žádný problém | Chip.cz - recenze a testy. Informace, testy a novinky o hardware, software a internetu – CHIP.cz [online]. Copyright © 2003 [cit. 14.03.2021]. Dostupné z: https://www.chip.cz/casopis-chip/earchiv/rubriky/technika/bezpecne-mazani/

[24] Jak vymazat disk a zničit uložená data na HDD navždy? Rady odborníků. inSmart.cz | Držíme krok s dobou chytrých technologií [online]. Copyright © 2021. [cit. 14.03.2021]. Dostupné z: https://insmart.cz/jak-trvale-smazat-data/

[25] STALLINGS, William. Cryptography and network security: principles and practice. Seventh edition. Boston: Pearson, [2017]. Global edition. ISBN 978-1-292-1585

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2019/2020

Studijní program: Aplikovaná informatika
Forma studia: Kombinovaná
Obor/kombinace: Aplikovaná informatika (ai3-k)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení: **Jiří Klouda**
Osobní číslo: **I1800494**
Adresa: Budyňská 24, Praha – Suchdol, 16500 Praha 620, Česká republika

Téma práce: Ochrana uživatelských dat na mobilních zařízeních
Téma práce anglicky: Protection of user data on mobile devices

Vedoucí práce: Ing. Hana Švecová
Katedra informačních technologií

Zásady pro vypracování:

Cíl závěrečné práce:
Cílem práce je seznámit čtenáře s možnostmi ochrany dat na mobilních zařízeních (laptopech, mobilních telefonech, tabletech a USB discích) včetně komparace variant pro bezpečné smazání uložených dat.
Součástí práce je i demonstrace získání dat z chráněného, správně smazaného uložiště, a nechráněného, nesprávně smazaného uložiště.

Seznam doporučené literatury:

Tomáš Doseděl. Počítačová bezpečnost a ochrana dat.
ISBN: 9788025101063, 8025101061
Luboš Dobda. Ochrana dat v informačních systémech.
Josef Zelenka. Ochrana dat : informační bezpečnost : výkladový slovník
ISBN: 80-7041-197-X

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: