Mendelova univerzita v Brně
Provozně ekonomická fakulta

Bezpečnost a ochrana soukromí v informační době

Diplomová práce práce

Vedoucí práce:
Ing. Jan Přichystal, Ph.D.

Bc. Jiří Suda

Brno 2015

Na tomto místě bych chtěl poděkovat vedoucímu své diplomové práce, Ing. Janu Přichystalovi, Ph.D., za poskytnuté rady a jeho trpělivost.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Bezpečnost a ochrana soukromí v informační době**
vypracoval samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*
Jsem si vědom, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.
Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 22. května 2015 .....

Abstract

Suda, J. Security and privacy in the information age. Diploma thesis. Brno: Mendel University, 2015.

The thesis is focused on personal computer security from the perspective of an ordinary user. This text in the theoretical part mainly introduces the reader to the most common risks associated with the use of a personal computer connected to the Internet. In the practical part based on the collected knowledge was created application used to configure and secure operating system Ubuntu.

Abstrakt

Suda, J. Bezpečnost a ochrana soukromí v informační době. Diplomová práce. Brno: Mendelova univerzita v Brně, 2015.

Diplomová práce je zaměřena na zabezpečení osobního počítače z pohledu běžného uživatele. Práce v teoretické části především seznamuje čtenáře s nejčastějšími riziky spojenými s užitím osobního počítače připojeného k Internetu. V praktické části byla na základě shromážděných poznatků vytvořena aplikace sloužící k nakonfigurování a zabezpečení operačního systému Ubuntu.

Obsah

1 Úvod

Informační technologie a jejich bezpečnost nejsou jenom trendy dnešní doby, ale čím dál více nutnost pro každého, kdo s nimi přichází do styku. Určitý základ v této oblasti by měl patřit mezi základní dovednosti každého moderního člověka.

S tím, jak se moderní technologie stávají zcela běžné a rozšiřují se do všech odvětví lidské činnosti, budou ruku v ruce také vzrůstat nároky na znalosti, jak je bezpečně používat. Jinými slovy jsou to dobří sluhové, ale zlí páni. Samozřejmě zdaleka ne vše může být ochráněno pouze znalostmi a chováním uživatele, ale tyto aspekty se podílí na zabezpečení významným dílem.

V současné době si správu vlastních počítačů zajišťují obvykle uživatelé sami, ať už jde o systém Windows, Linux nebo Mac. To je nebezpečné, neboť většina běžných uživatelů toho ví o informační bezpečnosti příliš málo a praktikují ji reálně ještě méně.

Za běžného uživatele je považována počítačově gramotná osoba, která používá počítač k soukromým účelům bez firemní politiky. Typickým příkladem užití je např. internetové bankovnictví, komunikace, vyhledávání informací na Internetu a podobně. Je zde také předpoklad, že bude uživatel vlastnit notebook, se kterým se bude pohybovat a připojovat k různým sítím.

Obecně se dá říci, že o počítačové bezpečnosti je nutné uvažovat jako o procesu, který se musí neustále zdokonalovat. Toto tvrzení platí také pro koncového uživatele a jeho znalosti této problematiky. Pokud se uživatel nebude vyvíjet v oblasti zabezpečení zároveň s nově vznikajícími hrozbami, může v souvislosti s neustále narůstajícím významem počítačů utrpět citelné škody. Nestačí tedy dosáhnout určité úrovně a dále se už o toto téma nezajímat.

Aktuálnost a závažnost situace dokazují prakticky každodenní zprávy, které informují o nových zranitelnostech a elektronických útocích. Nejedná se však pouze o bezpečnostní zpravodajství vydávané pouze pro odborníky z dané oblasti, ale přímo o informační zprávy určené běžným uživatelům.

1.1 Cíl práce

Hlavním cílem této práce je pomoci čtenáři zorientovat se ve složitém světě bezpečnostních hrozeb spojených s užíváním osobního počítače a jeho programového vybavení. Pro správné pochopení problematiky je potřeba zabývat se těmito otázkami:

- Co vše se může stát v případě zanedbání bezpečnostních opatření?
- Kdo a proč by mohl chtít narušit bezpečnost uživatele?
- Jaké možnosti jsou k dispozici pro provedení různých útoků, zneužití zranitelností, využití uživatelských chyb a neznalosti?
- Jakým způsobem je možné se bránit?

V této práci budou popsány hrozby, kterými mohou být osobní počítače v současné době reálně vystaveny. Přesto není cílem vytvořit sadu přesných návodů, jak provést jednotlivé útoky, ale spíše jim teoreticky porozumět a umět se jim bránit. S bezpečností je do určité míry spjatá i anonymita. Proto budou popsány i základní problémy a nutné znalosti v této oblasti.

Jako praktická část bude uživatelům sloužit pomocná aplikace, která usnadní a zrychlí proces zabezpečení vybraného operačního systému. Po nastudování této práce a využití pomocné aplikace by mělo být možné zabezpečit osobní počítače tak, aby došlo k výraznému snížení hrozby úspěšného útoku.

2 Metodika

Na základě rešerše budou identifikovány hlavní aktuální bezpečnostní hrozby v oblasti uživatelské práce s osobním počítačem. Pomocí prohloubení znalostí dané problematiky se v jednotlivých částech vyhodnotí možné riziko. V souvislosti s tím budou analyzovány jednotlivé vztahy mezi hrozbami. V potaz se budou brát pouze aktuální bezpečnostní problémy.

Dále se provede průzkum možných řešení bezpečnostních problémů, postupů a protiopatření. Jednotlivé návrhy se budou srovnávat a vybírat s ohledem na komplexní řešení tak, aby zapadaly do celkového konceptu a navrhované metodiky užití informačních systémů. Zároveň je potřeba brát ohled na uživatelské pohodlí a zvolit určitý kompromis. Pokud by opatření byla až moc svazující a obtěžující mohla by působit kontraproduktivně a odrazovat uživatele od jejich používání a dodržování.

Na vybraném operačním systému se vhodná bezpečnostní opatření (v podobě změn konfigurace systému či instalací vhodných doplňkových softwarů) zautomatizují naprogramováním pomocné aplikace s grafickým prostředím. Před samotnou prací na aplikaci bude nutné prozkoumat operační systém a jeho základní nastavení v souvislostech se zranitelnostmi a proveditelnými útoky. Jako zdroj informací poslouží doporučená literatura, volně dostupné odborné práce a články na specializovaných serverech zabývající se bezpečností.

3 Hrozby

Slovo hrozba v bezpečnosti informačních systémů znamená určitou skutečnost, událost nebo osoby, jejíchž působení může způsobit poškození, zničení, ztrátu důvěry nebo určité hodnoty. Útok je pak faktickou realizací hrozby. (Požár, 2011)

Charakteristikou hrozby je její zdroj, např. vnější nebo vnitřní, motivace potencionálního útočníka (např. finanční zisk), frekvence a kritičnost uplatnění hrozby. Hrozby lze rozdělit na následující kategorie:

- Objektivní
  - Přírodní nebo fyzické hrozby, mezi které patří požár, povodeň, výpadek napětí, poruchy. Prevence u těchto hrozeb je obtížná a řeší se u nich spíše minimalizace dopadů.
  - Technické nebo logické hrozby jako jsou porucha paměti, špatné propojení jinak bezpečných komponent, krádež, zničení paměťového média nebo dokonalé zrušení informace na něm.
  - Fyzikální hrozby, například elektromagnetické vyzařování.
- Subjektivní, tj. hrozby plynoucí z lidského faktoru
  - Neúmyslné, například při nesprávném a neodborném zacházení s informační technikou.
  - Úmyslné, tj. představované potencionální existencí vnějších útočníků jako kriminální živly, konkurenti, hackeři, a vnitřních útočníků, např. zaměstnanci. (Hanáček, 2000)

Typické hrozby podle Hanáčka (2000):

- Neautorizovaná modifikace informací, informačních zdrojů a služeb (tj. odchytávání a modifikace zpráv)
- Neautorizované zpřístupnění informace odposlechem po přenosovém médiu
- Neoprávněné kopírování
- Agregace citlivých informací z méně citlivých dílčích informací
- Dedukce ze znalosti (uložená informace v databázi)
- Dedukce z informací neoprávněně dostupných na veřejných zdrojích
- Odposlech pomocí zařízení pro práci se zvukem
- Neautorizované používání informačních systémů a služeb jimi poskytovaných
- Neoprávněné využívání HW (krádež strojového času)
- Krádež dat (prodej, zneužití, špionáž)

- Úmyslné poškození zařízení
- Znepřístupnění služeb (akce a události bránící využívání systému)

Jedna z nepříjemných hrozeb pro uživatele jsou ohrožená data. Pro uživatele mohou mít uchovávaná data totiž větší hodnotu než zařízení samotné. Může se jednat o různé tabulkové záznamy, fotografie, videozáznamy, uloženou práci na projektech a podobně. Často si uživatel uvědomí, jak jsou pro něj tato data cenná až v okamžiku, kdy nastane problém. Rozlišujeme tyto tři druhy hrozeb:

- Kompromitace – pokud se k datům dostane neoprávněná osoba, mohou pro uživatele nastat problémy. Útočník, který získá důležité informace, s nimi může pokračovat v dalších trestných činnostech, především pokud jsou uchovávána data, ke kterým by se nikdo neměl dostat, např. informace použitelné pro další průnik do jiného systému.
- Modifikace – změněná data, většinou pro cizí prospěch, nebo také odepření přístupu, například za účelem vylákání finančních prostředků.
- Zničení – může jít o úmyslné zničení dat útočníkem či nějakým škodlivým kódem, ale také i neúmyslné zničení při nějaké chybě či selhání. (Doseděl, 2004)

Hrozba, že přestane být z nějakého důvodu operační systém v dobré kondici nebo dokonce zcela nefunkční, je také určitý druh problému, který uživateli hrozí. Je třeba provést reinstalaci systému nebo jiný servisní zásah. Tato situace nastává, pokud je počítač neudržován a například napaden virem.

I kdyby bylo pomyslné zdraví vlastního počítače uživateli lhostejné (často při tvrzení, že na počítači není nic důležitého), měl by na něj dbát alespoň kvůli okolním počítačům. V podstatě je to srovnatelné s tím, že by se nemocný člověk neměl zdržovat v okolí zdravých lidí, aby je nenakazil.

Pokud se na konkrétním zanedbaném počítači opravdu neprovádí nic kritického, neznamená to, že na ostatních počítačích ve stejné síti je tomu stejně. Nezabezpečený počítač se tak může nevědomky stát otevřenou bránou k ostatním systémům na síti.

Další citelnou hrozbou v souvislosti s rychlým rozvojem elektronických platebních služeb a jejich obsluhováním z osobních počítačů, jsou pokusy o jejich zneužití, ke kterým dochází i v České republice. Česká národní banka proto varuje, že bezpečnost každého vzdáleně ovládaného účtu nezávisí pouze na zabezpečení informačních systémů jednotlivých bank, ale také na péči a pozornosti, kterou věnuje bezpečnosti samotný klient. (ČNB, 2014)

Pro uživatele je také nebezpečnou hrozbou krádež identity, která je známa od nepaměti. V současné době se změnila především její podoba. Osobní údaje totiž nejsou pouze čísla dokladů nebo rodné čísla, ale jsou to všechny údaje, na základě kterých by mohl někdo jiný přímo či nepřímo určit konkrétní osobu. Pokud někdo zkopíruje či odpozoruje osobní údaje v elektronické formě, není to na rozdíl od krádeže dokladů snadno zjistitelné. Následně se tedy může útočník na Internetu vydávat

za jinou osobu. Čím více informací má k dispozici, tím může být záměna identity přesvědčivější a nebezpečnější. Ve světě Internetu vzrůstá počet podvodů, jejichž cílem je zcizit citlivé osobní informace (zejména pro finanční prospěch). Útoky jsou prováděny kombinací technických prostředků a sociálního inženýrství. (Nykodýmová, 2006)

Pro uživatele samotného můžou předcházející hrozby vést k důsledkům jako:

- narušení soukromí
- ztráta osobní prestiže, dobrého jména a financí
- problémy v rodině a partnerském životě
- problémy v zaměstnání a následně jeho ztrátě
- vyloučení ze školy a podobně.

4 Právní předpisy o počítačové bezpečnosti

V souvislosti s informačními systémy a útočníky je nutné zmínit zákony vztahující se k této problematice na území České republiky. Upravuje ji trestní zákoník č. 40/2009 Sb. Zjednodušeně řečeno je trestný jakýkoliv čin neoprávněně zasahující do cizího systému nebo sítě. Testování je možné pouze na vlastním majetku či po přechozí domluvě s vlastníkem zařízení.

Od 1. 1. 2015 začíná platit v České republice nový zákon 181/2014 Sb. o kybernetické bezpečnosti. Nový zákon je primárně zaměřen na zvýšení bezpečnosti kritické infrastruktury státu a významných informačních systémů, spravujících osobní údaje velkého množství lidí.

4.1 Porušení tajemství dopravovaných zpráv

Podle § 182 trestního zákoníku bude potrestán až dvěma lety odnětím svobody nebo zákazem činnosti ten, kdo úmyslně poruší tajemství datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací, a to včetně elektromagnetického vyzařování z počítačového systému.

Stejně tak bude trestán ten, kdo má v úmyslu způsobit jinému škodu nebo opatřit sobě neoprávněný prospěch v podobě prozrazeného tajemství, které mu nebylo určeno. Nebo takového tajemství využije.

4.2 Neoprávněný přístup k počítačovému systému a nosiči informací

Podle § 230 trestního zákoníku bude potrestán až jedním rokem odnětím svobody ten, kdo překoná bezpečnostní opatření a získá neoprávněně přístup k počítačovému systému nebo jeho části. Pokud neoprávněně zpřístupněná data změní, podvrhne nebo zničí, potom mu hrozí až dva roky odnětí svobody.

Pokud je počítačová síť jakýmkoliv i slabým způsobem zabezpečena, je patrný projev vůle zabezpečit ji. Jakékoliv pronikání do této sítě je považováno za trestné. Příkladem může být malá domácí bezdrátová síť zabezpečená slabým WEP klíčem na domácím routeru.

4.3 Přechovávání přístupového zařízení a hesla

Podle § 231 Zákona č. 40/2009 Sb. trestního zákoníku bude potrestán až pěti lety odnětím svobody ten, kdo vytvoří a zprostředkuje zařízení nebo jeho součást, postup, nástroj nebo jakýkoliv jiný prostředek, včetně počítačového programu, vytvořeného nebo přizpůsobeného k neoprávněnému přístupu do sítě elektronických komunikací nebo počítačového systému.

5 Druhy útočníků a jejich poloha

V této kapitole budou specifikováni počítačoví útočníci. Člověk útočící na počítačový systém je obecně označován jako útočník. Je vhodné vědět, komu uživatel čelí a na jaké útočníky se připravit. Dále se určitě hodí znát jejich motivaci a teoretické možnosti, kterých jsou schopni. Významnou veličinou ovlivňující možnosti útočníka je pak jeho poloha. Čím blíže je útočník (z hlediska logické polohy) k uživateli, tím více možností má k provedení útoku.

Je třeba mít na paměti, že existují programy pro uskutečnění různých počítačových útoků. Tyto programy jsou uživatelsky jednoduché a zároveň umožňují napáchat relativně velké škody. Útočné nástroje jsou určeny teoreticky pouze pro testování zabezpečení, ale to neznamená, že nemohou být použity ke skutečnému útoku. A protože jsou tyto nástroje dostupné volně ke stažení z Internetu, může se stát útočníkem prakticky kdokoliv.

5.1 Druhy útočníků

V reálném světě je možné narazit na různé druhy útočníků, kteří se liší především schopnostmi a prostředky, které mají k útokům k dispozici. Motivace jejich útočných činů bývá také značně odlišná. Tato práce je zaměřená na první tři druhy (boti, amatéři a hackeři). Jejich techniky a způsoby jsou obecně známé, také existují prostředky, jak se proti nim bránit. Běžný uživatel se s nimi může relativně snadno a často dostat do kontaktu.

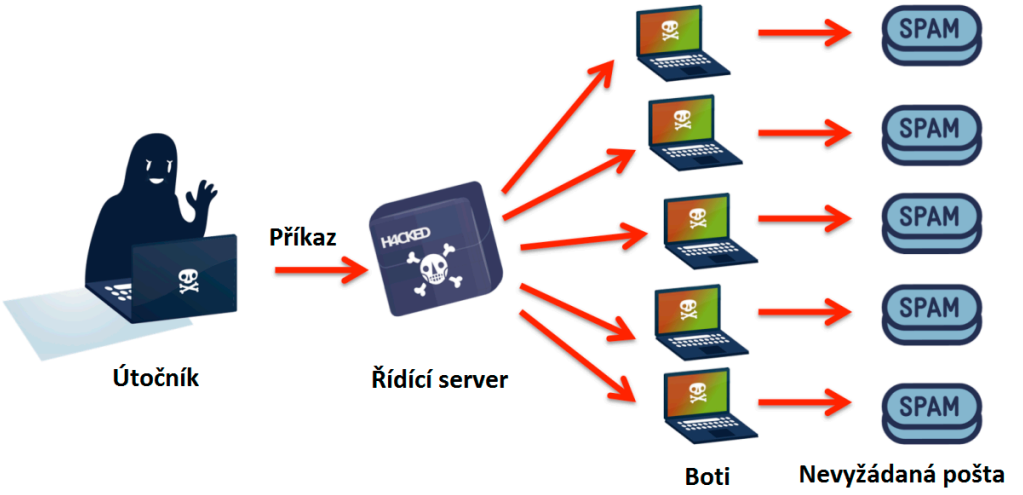
5.1.1 Boti a jiní zcela automatizovaní útočníci

Botnet je síť napadených počítačů, která je řízena vzdáleně útočníkem. K vytvoření botnetové sítě je použit škodlivý kód na určitou konkrétní slabinu. Mezi hlavní dvě metody šíření patří:

- Umístění škodlivého kódu na různé populární webové stránky, které obsahují neošetřené zranitelnosti. Odkud se šíří dále na uživatelské stanice prostřednictvím prohlížečů, které obsahují různé slabiny využitelné tvůrcem botnetu.
- Zaslání velkého množství podvodných a nevyžádaných emailů obsahujících jako přílohy například nakažené soubory typu PDF nebo dokumenty programu Microsoft Word.

Velikost takové sítě skládající se z ovládnutých počítačů, kterým se říká boti se pohybuje od malých čísel v řádech desítek a stovek až po největší sítě, které čítají miliony botů. Nejznámější pojmenované sítě, o kterých je možné slyšet v médiích, jsou například Conficker, Zeus, Waledac. (Fisher, 2013)

Zasaženy bývají především stanice se systémem Windows a servery, na kterých běží Linux. Zatímco uživatelské stanice Linuxu jsou relativně bezpečné, protože obyčejně na nich neběží žádná veřejná služba, či nejsou konfigurované pro vzdálený



Obrázek 1: Příklad základního konceptu fungování sítě botnet.
Zdroj: SWITCH Security Blog, 2013.

přístup. V neposlední řadě také kvůli odlišné filozofii zabezpečení oproti stanicím se systémem Windows.

V roce 2014 pokračuje trend v narůstajícím počtu nakažených počítačů. Novinkou v této oblasti je implementace několika nových způsobů nahlášení bota svému majiteli a vylepšené maskovací techniky využívající skrytých sítí jako je Tor. Obě tyto nové vlastnosti zvyšují odolnost a robustnost celé sítě. Taktéž jsou tvůrci schopni daleko rychleji reagovat na protiopatření antivirových firem.

Tvůrce botnetu se především snaží, aby z této nelegální sítě měl jakýkoliv možný osobní profit převážně finančního charakteru. Jedná se hlavně o tyto způsoby využití:

- Škodlivý kód orientovaný na bankovní služby, který krade přihlašovací údaje. Například botnet Carberp orientovaný na bankovní služby zcizil zákazníkům od svého vzniku v roce 2013 za jediný rok přes 250 milionů dolarů.
- Provádění DDoS útoků. Cílem bývá vyřadit službu běžící na konkrétním serveru. Samotný útok probíhá jednoduše. Botnetová síť vytvoří obrovský datový provoz směřující na vybraný cíl. Jelikož všichni boti posílají různé požadavky zároveň, tak se při dostatečném počtu zapojených botů cílový server zahltí. Obvykle se používá této praktiky k nekalým konkurenčním bojům. Nebo třeba také k odvrácení pozornosti od jiného skutečného útoku. Zisk plyne tvůrci botnetu od firmy či jedince, která si ho najme.
- Rozesílaní hromadných emailů. Tento způsob využití může mít mnoho účelů. Například inzerent zaplatí tvůrci botnetu, aby distribuoval reklamu na nějaký povětšinou pochybný výrobek či službu.
- Využití celkové výpočetní síly pro složité matematické operace. Pokud například útočník potřebuje prolomit zabezpečení pomocí hesla a vyzkoušet velké

množství kombinací pomocí paralelního brute-force distribuovaného útoku.

- Zapojení do těžení kryptoměn. Především v roce 2013 vynášelo těžení virtuální měny velké finanční zisky. Zjednodušeně řečeno je k vytváření virtuálních měn potřeba řešit složité matematické problémy. K tomu je třeba velký výpočetní výkon, kterým sítě botnet disponují. Takto vytvořená měna může být poté anonymně vyměněna za jinou nevirtuální měnu. V současné době se již tato takzvaná těžba tolik nevyplácí, proto je prozatím na ústupu.

Pro běžného uživatele tyto sítě představují problém především v tom, že počítač se bez jeho vědomí zapojuje do nelegální a trestné aktivity a stopy zanechané na Internetu ukazují na fyzického vlastníka bota. Dalším problémem je, že kompromitovaný počítač může vyzradit (k nelibosti jeho majitele) úplně vše, co je mu svěřeno.

Pokud je počítač v botnetu zapojen dlouhodoběji, při výpočetně náročném úkolu, může se to také projevit na vyšším účtě za spotřebu elektřiny. Samozřejmě nikdo z běžných uživatelů takto napadených počítačů neví, co se děje za jejich zády. (Sophos, Security Threat Report 2014)

Botnety představují opravdu seriózní hrozbu. Přestože se každoročně FBI povede vyřadit z provozu mnoho velkých botnetových sítí, tak FBI odhaduje, že zločinci každoročně infikují dalších 500 milionů počítačů (18 počítačů za vteřinu) a způsobí škody za více než 110 miliard dolarů. (Demarest, 2014)

5.1.2 Amatéři

Amatéři jsou považováni za nejméně nebezpečné útočníky, nicméně jsou početně velmi rozšíření. V současné době už jimi může být prakticky kdokoliv s určitým zájmem o danou problematiku. Patří sem především studenti středních technických škol. S rozvojem útočných nástrojů, které se stávají stále více uživatelsky přívětivé a snadno na Internetu dostupné, se však nebezpečí amatérů stále zvyšuje. K dispozici je také mnoho textových návodů nebo video tutoriálů, které jim práci usnadňují.

Amatéři většinou jen zkouší, zda dokáží využít útočných nástrojů a bezpečnostních chyb, o kterých se dočetli na Internetu. Nabyté zkušenosti mohou později využít v jejich prospěch při vhodné příležitosti. Například zkopírování učitelem připravené školní písemky. Často si ani nemusí uvědomovat závažnost svého chování a jeho trestní postihnutelnost. Jejich technické zázemí bývá velmi omezené. Nemají dostatek znalostí ani vybavení k provedení sofistikovaného útoku.

Obrana bývá obyčejně relativně jednoduchá a levná. Spočívá v dodržování základních bezpečnostních pouček, zajištění fyzické bezpečnosti, záplatování a užívání bezpečnostního softwaru. (Doseděl, 2004)

5.1.3 Hackeři

Hackeři jsou v útocích mnohem nebezpečnější než předchozí skupina. Mají dobré znalosti principů výpočetní techniky. Typicky se může jednat o vysokoškolské stu-

denty informačních technologií. Rozumí přesně tomu, co dělají. Dokážou přizpůsobovat svoje útoky prostředí a aktuálním potřebám. Jejich útoky mohou být velmi nepříjemné. (Doseděl, 2004)

Stále jsou však limitováni prostředky a výpočetním výkonem, ale v současné době není již problém toto omezení zmírnit. Už v roce 2010 špičkové grafické procesory nabízely paralelní výpočetní výkon až 2 teraflops. Tento výkon se vyrovnal výkonu největších superpočítačů v roce 2000. V době psaní této diplomové práce je nejvýkonnější grafická karta AMD Radeon 295X2 výkonnostně okolo 12 teraflops. (Houser, 2010)

Obrana proti tomuto typu útočníků je středně náročná. Je třeba dodržovat relativně přísná pravidla. Používat specializovanější softwarové a hardwarové prostředky.

5.1.4 Profesionálové

Do této skupiny patří pouze počítačoví profesionálové s velkými praktickými zkušenostmi. Mohou pracovat samostatně nebo ještě hůře ve skupinách a různých organizacích. Jejich postupy jsou originální a nápadité. Jejich motivace bývá různá. Spadají sem nájemní zločinci, vládní organizace i tajné služby ze všech států světa.

Technické omezení nemají téměř žádné. K dispozici mají nejnovější a nejpokročilejší technologie. Prakticky jediný jejich nepřítel je v podobě matematických a fyzikálních zákonů, které se obejít nedají.

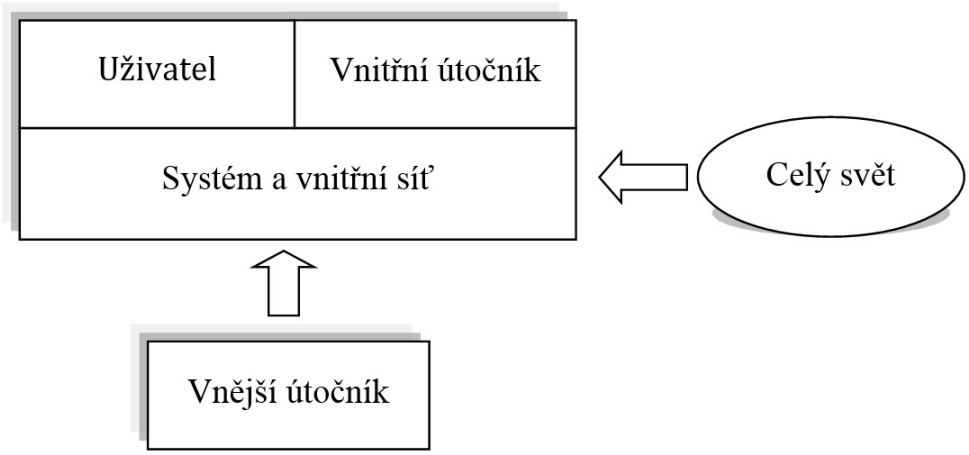
Ovšem šance, že na profesionály narazí běžný uživatel je velmi malá. Z jejich pohledu je totiž zcela nezajímavý. Zaměřují se pouze na skutečně hodnotné cíle. Obrana proti tomuto typu je velmi složitá, nákladná a zcela mimo rámec této práce. Jsou zde zmíněni hlavně proto, aby i uživatel, který se aktivně zabývá svojí bezpečností, nenabyl dojmu absolutního bezpečí. (Doseděl, 2004)

5.2 Poloha útočníka

Rozdílná logická a fyzická poloha útočníka vůči uživateli z pohledu přístupu ke sdíleným prostředkům hraje podstatnou roli v bezpečnosti. Proto je důležité přemýšlet o tom, kdo a kde má jaký přístup k počítačové síti a informačním systémům. Od toho se odvíjejí teoretické možnosti útoku a jejich složitost.

5.2.1 Vnitřní útočník

Pokud se někdo z uživatelova okolí rozhodne zaútočit ze společné vnitřní sítě nebo prostředí, jedná se o nepříjemnou a nejvíce nebezpečnou polohu. Může jít o kolegu z firmy, spolužáka ve škole či někoho komu byl například za úplatu přístup umožněn. Velké nebezpečí hrozí v případě, že uživatel přistupuje k otevřeným veřejným sítím, kterými jsou rozšířené free Wi-Fi hotspoty (například kavárny, restaurace a podobně), kde je umožněno se komukoliv anonymně připojit k Internetu. Může se tak



Obrázek 2: Pozice útočníků vzhledem k uživatelskému systému a síti.

snadno dostat zároveň do stejné lokální sítě s útočníkem, který má pak k dispozici mnoho relativně snadných možností, jak zaútočit.

Co se týče zkušeností útočníků a vnitřní pozice, je to nejjednodušší varianta. Pro amatéry často také jediná. Odpadá jim tak krok nabourat se nejdříve do místní sítě nebo překonat další bezpečnostní překážky, přes které by se nemusel povést realizovat průchod. (Doseděl, 2004)

5.2.2 Vnější útočník

Osoba nemá přístup k systému ani k vnitřní síti. Hlavní skupina pro tuto polohu jsou obecně šikovnější hackeři. Pro vnějšího hackera je třeba kombinací několika různých útoků. Protože počet prvků zabezpečení bývá obyčejně větší z vnější polohy. V cestě mu stojí například firewall a jiné síťové zabezpečení. Nevýhoda je také neznalost infrastruktury a zavedených bezpečnostních opatření.

Výhodou je naopak pro vnějšího útočníka daleko obtížnější vystopování, pokud nepřistupuje k prostředkům, na které útočí napřímo. Ať již z hlediska vlastní osoby nebo svého počítače. (Doseděl, 2004)

5.2.3 Celý svět

Do této kategorie spadají různé distribuované útoky botnetů, které byly popsány výše. Jeden člověk může ovládat různé množství nakažených botů, serverů či komunikačních uzlů zkoušejících napadat všechno, co jim přijde pod pomyslnou ruku.

Z hlediska uživatele se nejedná o cílený útok, ale je na něj útočeno hlavně proto, že se prostě připletl do cesty a může z toho být nějaký prospěch. Úspěšně ovládnutý stroj může například pasivně sbírat informace nebo jinak aktivně zasahovat do komunikace především za účelem zisku, například podstrkáváním reklamy. Internet je prakticky jedna velká celosvětová síť, proto se může skutečný útočník nacházet

úplně kdekoliv. Postihnutelnost či vypátratelnost je velmi omezená téměř nemožná. (Doseděl, 2004)

6 Útoky a zranitelnosti

Slabina informačního systému, která může být využitelná pro způsobení škod, se nazývá zranitelné místo. Je to důsledek chyb, selhání v analýze, v návrhu či implementaci informačního systému. Obvykle kvůli vysoké hustotě uložených informací, složitosti softwaru a existenci skrytých kanálů pro přenos informace jinou než zamýšlenou cestou apod. (Požár, 2011)

Útokem, kterým nazýváme rovněž bezpečnostní incident, rozumíme úmyslné zneužití zranitelného místa (tj. využití zranitelného místa ke způsobení škody). Informační bezpečnost znamená především komplexní pohled, který pomáhá poznat a chránit cenná data a také vede praktickými opatřeními k výraznému snížení dopadů v případě bezpečnostního incidentu. (Požár, 2011)

6.1 Útoky s fyzickým přístupem k zařízení a datům

Útokům tohoto typu se lze účinně bránit pouze zajištěním fyzické bezpečnosti. Bez zamezení fyzického přístupu k zařízení a chráněným datům nelze dosáhnout dobré informační bezpečnosti. Pokud se útočník vůbec k chráněnému počítači nedostane, může ho jen velmi složitě napadnout v porovnání s fyzickým přístupem k systému. V opačném případě existuje tolik možností útoků, že zamezit všem, je téměř nemožné. Z hlediska běžného uživatele je zajištění fyzické ochrany problematické. Každopádně je dobré mít na paměti tuto skutečnost a připravit se i na tuto možnost.

6.1.1 Obnova nedokonale vymazaných dat

Po odstranění souborů z odpadkového koše v běžných operačních systémech nejsou soubory skutečně smazány. Systém pouze označil takovéto soubory jako dostupné pro přepsání. Pokud nebudou skutečně fyzicky přepsány a nahrazeny jinými soubory, existuje možnost obnovy za pomocí speciálního volně dostupného software na obnovu dat, jakým je například software Recuva[1].

Problém pro uživatele tedy může být to, že se spoléhá na skutečné vymazání dat, která se ovšem můžou opět objevit. Typickým příkladem může být prodej počítače s pevným diskem nebo ohrožení v podobě útočníka, který získal fyzický přístup k danému počítači. (Rubens, 2012)

Běžné operační systémy ve své základní konfiguraci neumožňují neobnovitelné odstranění dat. Je potřeba použít programy třetích stran, které přidají možnost bezpečného smazání. Odstranění se poté provádí v kontextové nabídce vyvolané pravým tlačítkem myši na konkrétním souboru. Dále je obvykle k dispozici také důkladné dodatečné odstranění všech již dříve smazaných souborů.

[1] Dostupné na http://www.piriform.com/recuva

6.1.2 Nedostatečná slabá hesla

Zaheslovaný soubor nebo hesla uložená v zahashovaném (tj. zpětně nečitelném) formátu mohou být s narůstajícím výpočetním výkonem v ohrožení. Pokud se jedná o samotná hesla, typicky jsou zabezpečena jednocestnou kryptografickou hashovací funkcí. Ochrana spočívá ve vygenerování (podle určitých pravidel) úplně jiného unikátního řetězce znaků (otisk), který se pak ukládá do systému nebo databází.

Pokud je potřeba ověřit shodu tohoto hesla, tak se jednoduše provede opětovné vygenerování otisku z předloženého hesla. Následně se již pouze porovná, jestli sedí nový otisk s uloženým otiskem.

Jak již bylo řečeno, k hashovací funkci neexistuje funkce inverzní. Jediným způsobem jak zpětně určit předlohu je postupně vyzkoušet (za použití stejné kryptografické funkce) všechny možné kombinace (útok hrubou silou neboli brute-force) nebo vyzkoušet často používaná známá hesla (slovníkový útok).

V posledních letech dochází z různých webových služeb k sériím úniků skutečných hesel uživatelů. Jenom v posledních pár letech bylo ukradeno přes 100 milionů hesel. Získaná hesla jsou ukládána do databází, které útočníci dále používají při slovníkovém útoku. Takové množství dat poskytuje významnou pomoc k prolomení použitého hesla na jiných místech zabezpečených heslem[2].

Například v roce 2012 došlo k 7 milionovém úniku hesel z profesní sociální sítě LinkedIn. Úspěšně bylo převedeno 90 % do otevřené formy za použití jediného počítače se čtyřmi grafickými kartami AMD Radeon HD6990. (Goodin, 2012)

Výše zmíněná grafická karta vyzkouší zašifrovaný soubor programem WinRAR rychlostí reálně kolem 25 tisíc kombinací za vteřinu[3]. Při použití 4 grafických karet ověří okolo 100 000 kombinací za vteřinu. Celkový počet kombinací nejčastěji používaného 8 místného hesla za použití malých písmen, velkých písmen a číslic je $62^8 = 218\ 340$ miliard. Prolomení by tedy trvalo okolo 70 let.

Pokud se zohlední v čase rostoucí výkon superpočítačů, který je dobře viditelný na grafu, viz obrázek č. 3, nemusí toto heslo za pár let stačit. Současné osobní počítače kopírují výkonnostní vývoj superpočítačů přibližně se zpožděním 15 let. (Houser, 2010)

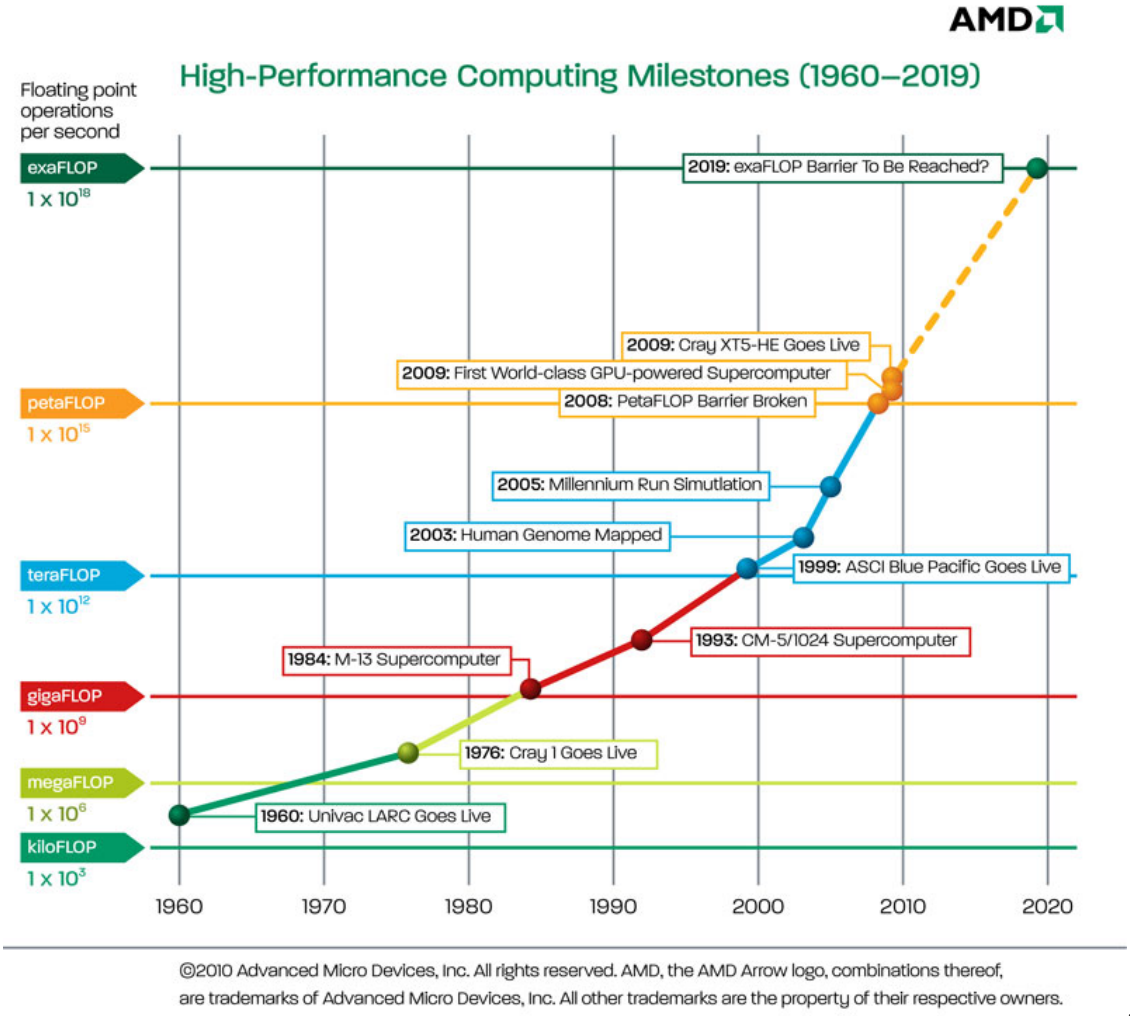
Moorův zákon říká, že se každých 18 měsíců zdvojnásobí výpočetní výkon. Prozatím se výkon superpočítačů každých 11 let znásobil přibližně 1000 krát. Jak je vidět na obrázku č. 3. (Mims, 2012)

Uživatel, který si není vědom razantního výkonnostního posunu výpočetní techniky v nadcházejících letech, může zaznamenat s nejčastěji používaným a doporučovaným 8 místným heslem bezpečnostní problém v řádu jednotek let[4].

[2]Například z úniku 130 milionů uživatelských hesel společnosti Adobe je k nahlédnutí 100 nejpoužívanějších hesel dostupných na http://stricture-group.com/files/adobe-top100.txt. Pro představu na 54. místě bylo použito 20961 krát heslo asdasd.

[3]Při použití výpočetně náročného algoritmu AES.

[4]Pro zjištění počtu kombinací a přibližného odhadu obtížnosti prolomení hesla je jednoduché použít formulář na stránkách www.howsecureismypassword.net. Není ovšem vhodné zadávat skutečná použitá hesla.



Obrázek 3: Růst výkonu nejvýkonnějších superpočítačů v operacích za vteřinu s plavoucí čárkou.
Zdroj: AMD, 2010.

Pro účinnou ochranu je třeba volit nejlépe 16 místná hesla složená alespoň z písmen a číslic. Takové heslo nesmí být srozumitelné a odvozené ze znalosti konkrétního uživatele. Počet kombinací je pak dostačující. Pro každou kritickou aplikaci hesla je nutné mít heslo jiné (bankovní účet, emailový účet).

Důležitá je také správa samotných hesel. V některých programech a na většině internetových stránek je možné hesla uložit přímo do počítače, aby je uživatel nemusel zadávat při každém přístupu znovu. Hesla bývají zobrazována v podobě zástupných hvězdiček maskující skutečné znaky. Takto uchovávat uložená hesla v počítači je nebezpečné, protože je možné je snadno zobrazit v jejich skutečné podobě. Například v internetových prohlížečích Google Chrome a Mozilla Firefox je možné takovéto heslo zobrazit do několika vteřin následujícím postupem:

- Otevřít webovou stránku uchovávající uložené heslo.
- Pravým tlačítkem kliknou do boxu s heslem skrytým za hvězdičkami.
- Vybrat možnost Zkontrolovat prvek (Inspect element).
- Ve spodní části prohlížeče se otevře nástroj se zdrojovým kódem webové stránky. Poté stačí vyhledat řetězec type="password" a zaměnit ho za type="text".
- Po stisknutí klávesy Enter se již objeví v boxu čitelné heslo. (Voo, 2013)

Na obnovu uložených hesel z různých programů jsou pak k dispozici jim odpovídající volně dostupné obnovovací nástroje, zaměřující se na obnovu konkrétních programů. Pokud nebude heslo v počítači uloženo, odpadá možnost jeho obnovy.

6.1.3 Nechráněná operační paměť

Obsah operační paměti spuštěného systému je uložen v otevřené formě a chráněn operačním systémem. Problém může nastat, pokud bude operační paměť za provozu vyjmuta a vložena do systému útočníka (nebo může být použit jiný způsob získání přístupu k obsahu paměti). Následně bude možné modifikovat obsah operační paměti, získat šifrovací klíče anebo informace v ní uložené (bez přítomnosti všech bezpečnostních opatření hostitelského operačního systému).

Za předpokladu, že je uživatelský počítač regulérně ukončen, může se každý software postarat o smazání svých citlivých dat z operační paměti. Ovšem při náhlém přerušení napájení, nestačí systém ani programy zareagovat a ukončí se nekorektně. Útočníkovi pak stačí vyjmout[5] z napadeného PC operační paměť, následně ji vložit do svého počítače a všechna data z ní zkopírovat a zanalyzovat. Tento útok nazývaný Cold boot attack je možný, protože se zjistilo, že navzdory všeobecnému očekávání si operační paměť udrží (bez napájení) dočasně svůj obsah v řádu minut, a to v závislosti na její teplotě. (Pepak, 2012)

Součástí počítače je DMA řadič využívaný k urychlení přesunu dat z úložného zařízení do paměti a opačně. Pokud nějaké zařízení požádá o přenos dat, tak ho bez obtěžování procesoru řadič DMA provede. Tím je snížena výpočetní zátěž procesoru, který se může věnovat jiným procesům. Problém nastává, pokud dojde k ustanovení přenosu mezi řadičem a zařízením bez povolení procesoru a operačního systému.

DMA je součástí všech běžně používaných rozhraní (FireWire, PCI, USB a další). Komplexní obrana proti útoku prostřednictvím DMA je problematická, protože je DMA téměř všudypřítomné. Existující návody se soustředí alespoň na zablokování snadno zneužitelného FireWire. Pro uživatele je nejlepší způsob ochrany úplné vypínání počítače v jeho nepřítomnosti. (Pepak, 2012)

Pokud není rozhraní FireWire k dispozici na základní desce napadeného počítače, může být emulováno pomocí rozhraní Thunderbolt. U notebooků existuje

[5]Jednodušší alternativou může být nabootování vlastního operačního systému.

možnost připojení dalších různých emulujících adaptérů například přes PCMCIA rozhraní. (Maartmann-Moe, 2012)

U otevřeného zašifrovaného diskového oddílu musí být šifrovací klíč uchovaný v operační paměti v otevřené formě. Tento klíč se odstraní až po uzavření diskového oddílu. Stejně tak musí být v operační paměti programová sekvence, která ověřuje heslo při odemykání obrazovky operačního systému. K uzamknutí dochází automaticky po určité časové nepřítomnosti uživatele či po opětovném zapnutí počítače po hibernaci. Tato programová sekvence ověřuje správně vložené heslo. Je uložena v operační paměti, kde může být zaměněna za sekvenci akceptující jakékoliv heslo.

Volně dostupný nástroj Inception je schopný přepsat kontrolu přístupového hesla v operačním systému zapnutého a uzamknutého počítače u přihlášeného uživatele. Stačí pouze propojit útočníkův počítač s počítačem uživatele pomocí FireWire kabelu a nechat program pracovat. Při zadání libovolného hesla se pak útočník přihlásí jako běžný uživatel. Vše je zautomatizováno na stisknutí jediného tlačítka. Nástroj Inception dokáže projít skrz kontrolu operačních systémů Windows a Linux. Po restartování počítače se do paměti obnoví původní programová sekvence kontroly hesla. Tato technika je tedy prakticky nezjistitelná z pohledu uživatele. (Maartmann-Moe, 2011)

6.1.4 Snadno prolomitelné ochrany operačního systému

Někteří uživatelé spoléhají na zabezpečení svého počítače na úrovni operačního systému nebo BIOSu[6]. Ve skutečnosti jsou to pouze symbolické formy zabezpečení. Tyto ochrany se nechají snadno obejít různými způsoby. Vstupní heslo do operačního systému může být útočníkem zjištěno nebo odstraněno použitím vlastního připojeného systému. Takovým liveCD[7] systémem je například volně dostupný Ophcrack[8]. Náhled tohoto programu je zobrazen v příloze č. 12. (Thompson, 2013)

Pokud je systém uzamčen pomocí BIOSu, je kontrolní součet (hash) hesla uložen v FlashROM paměti na základní desce. U většiny výrobců desek dojde po třech chybných zadáních vstupního hesla k zobrazení kontrolního součtu. Způsoby výpočtu různých výrobců jsou veřejně známé. Proto stačí zadat toto číslo například do veřejně dostupného webového formuláře[9], který veškerou práci provede za útočníka. Pro vymazání hesla postačí také prosté vyjmutí baterie ze základní desky. Baterie totiž udržuje informace o hesle uloženém v paměti základní desky. (Dogbert, 2009)

Vysokou ochranu počítače a jeho dat je možné zajistit zašifrováním nejlépe celého operačního systému i se všemi daty. To umožňují některé operační systémy již rovnou při instalaci nebo je možné doinstalovat program třetí strany podle druhu

[6]Základní program uložený přímo v základní desce. Slouží pro inicializaci a konfiguraci hardwaru.

[7]Systém uložený na CD, který nemusí být instalován do pevné paměti počítače. Může fungovat dokonce zcela bez HDD.

[8]http://ophcrack.sourceforge.net/

[9]Jednoduchý formulář dostupný na www.bios-pw.org.

operačního systému. Při spuštění počítače je pak nutné vždy zadat heslo. Bez znalosti hesla se není možné dostat do systému a ani k datům žádným rozumným způsobem. V případě použití slabého hesla je tento způsob zabezpečení nejvíce náchylný právě na útok hrubou silou.

Obecně je použití hrubé síly tím nejméně elegantním útokem, ale také zároveň tím prvním, který se bere v úvahu. Nevyužívá totiž žádnou nalezenou slabinu, chybu či útočníkův důvtip. Jde pouze o prosté vyzkoušení všech možných variant, které připadají v úvahu. Zabezpečení proti útoku hrubou silou spočívá hlavně na co největším množství teoretických variant. Nejlépe by jich mělo být tolik, aby ani s nejlepším počítačem na světě a neomezeným časem nebylo možné, aby byl útočník schopný se úspěšně propracovat ke správné variantě. To v praxi ovšem není často splněno, proto při dostatečném výpočetním výkonu a času bývá tento druh útoku efektivní.

6.1.5 Útok zlé uklízečky

Jedná se o útok zaměřený na dobře zabezpečené počítače s plným šifrováním, které jsou v nepřítomnosti uživatele vypnuté. Prolomit takto dobře zabezpečený systém je obtížný úkol i pro profesionály, natož pro uklízečky, po kterých je tento útok pojmenován.

Jediné, co je potřeba k vykonání úspěšného útoku a získání hesla, je krátký fyzický přístup k počítači. To může právě umožnit například instruovaná uklízečka v hotelovém pokoji, zatímco uživatel například obědvá v jídelně. Postup útoku:

- Zavedení útočníkova operačního systému a záměna zavaděče se škodlivým kódem v napadeném počítači.
- Uživatel nevědomě zadá škodlivému zavaděči své vstupní heslo do systému, které se zaznamená na pevný disk v otevřené formě. Následně se předá řízení regulérnímu zavaděči systému, který spustí počítač jako obvykle.
- Stejná uklízečka druhý den vyzvedne heslo i data uložená v počítači a smaže po sobě všechny stopy.

Způsob ochrany proti tomuto útoku je velmi obtížný, protože pokročilejší škodlivý kód může eliminovat (po zadání odchyceného uživatelského hesla) všechny zavedené softwarové ochrany. Obrana spočívá především na fyzické bezpečnosti. Další možností je nosit zavaděč[10] operačního systému na přenosném USB flash disku neustále s sebou a zapínat počítač pomocí něho. (Schneier, 2009)

[10]Zavaděč jediný nemůže být zašifrovaný, protože by pak nemohl být použit k zavedení systému a zadání hesla.

6.2 Útoky z místní sítě

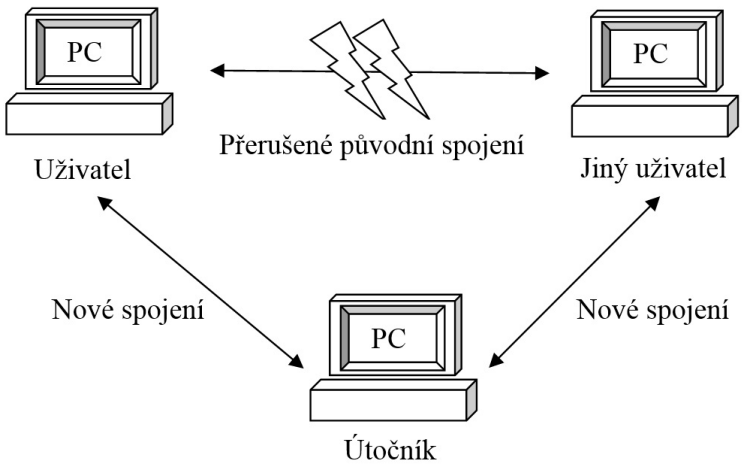
Počítače jsou často zapojovány do různých místních počítačových sítí kvůli možnosti komunikace s ostatními počítači a sdílení informací. Takové sítě nemusí být vždy důvěryhodné a může se k nim oprávněně či neoprávněně připojit i potencionální útočník.

Útoky vedené z této pozice jsou pro útočníka z hlediska jeho osoby relativně bezpečné, protože často není třeba překonávat žádné fyzické překážky k připojení k místní síti. Zároveň existuje velké množství zranitelností a k nim odpovídající útoky, které lze s volně dostupnými aplikacemi snadno uskutečnit.

6.2.1 Přesměrování síťového provozu

Balík protokolů TCP, přes který je dodnes směrován veškerý síťový provoz, používá stejné principy od roku 1983. V té době na něj byly kladeny zcela jiné požadavky, než je tomu dnes. Jeho primární vlastností měla být schopnost přežít jaderný útok v případě válečného konfliktu. Pokud by byla určitá část sítě poškozena, automaticky by se přesměroval provoz přes jiné dostupné komunikační uzly. Pokud by přes zničenou část zrovna probíhala komunikace, nesměla být data ztracena, ale opětovně přeposlána v co nejkratším čase. Z tohoto důvodu existuje řada technik jak přesměrovat datový tok, což patří mezi určitý základ k úspěšnému útoku. (Toxen, 2003)

Pro odposlech na počítačové síti nebo podvrhnutí internetové stránky útočníkovou variantou je potřeba přesměrovat (neboli unést) regulérní datový tok skrz útočníka (nebo na jím ovládaný stroj). Tomuto postupu se obecně říká útok s mužem uprostřed, protože je nutné se dostat, jak název napovídá, mezi dvě komunikující strany. Obě strany ovšem musí věřit, že komunikují pouze spolu. Muž uprostřed se tedy stane takovým neviditelným prostředníkem. (Schneier, 2008)



Obrázek 4: Útok s mužem uprostřed.

Na lokální síti zajišťuje distribuci dat mezi jednotlivé počítače síťové zařízení typu switch[11] (přepínač). Za běžné situace posílá síťové pakety pouze těm účastníkům komunikace, které se jí opravdu zúčastňují, především kvůli tomu, aby se zbytečně nepřetěžovala místní síť.

Mezi různými počítačovými sítěmi se přeposílají pakety pomocí zařízení typu router (směrovač) na základě IP[12] adres. Jakmile paket dorazí do cílové lokální sítě, předá router přijatý paket přepínači, který pracuje s MAC[13] adresami. Přepínač vyšle požadavek (ARP protokolem) všem počítačům na síti a zjišťuje, kdo má konkrétní cílovou IP adresu. Pokud je dotyčný počítač přítomen (nebyl například vypnut), ozve se a přepínač si poznamená (do své ARP tabulky) jeho MAC adresu a také port na jakém se nachází. Dále se již bez opakovaného dotazování přeposílají pakety rovnou k němu. Dojde tedy k přiřazení určité IP adresy k určité MAC adrese.

Problém nastává, jakmile se do této situace vloží útočník, protože v protokolu ARP není implementována žádná ochrana proti falšování. Plně zautomatizovaný útok zvládne například volně dostupný program Ettercap (ukázka je přiložena v příloze č. 14). Útočník tedy snadno pošle pomocí ARP paketu přepínači falešnou informaci, že on vlastní cílovou IP adresu. Přepínač tuto informaci přijme, i když nezaslal žádný požadavek pro její zjištění. Aby měl útočník zároveň přehled i o komunikaci ze směru od uživatele k přepínači, pošle další falešnou informaci počítači uživatele, že jeho zařízení je výstupní brána ze sítě (nebo cílový počítač, pokud se nachází na stejné síti). Takto je teoreticky uskutečněn útok s mužem uprostřed. Pokud není z pohledu správce sítě realizováno nějaké bezpečnostní opatření oddělující jednotlivé lokální počítače od útočníkova stroje, tak přes útočníka prochází veškerá komunikace. Změny MAC adres přiřazené k IP adresám vyvolané tímto útokem, je možné monitorovat speciálním softwarem (například volně dostupným XArp), který uživatele varuje v případě nestandardního chování. (Harris, 2008)

Další způsob přesměrování datového toku v rámci místní sítě umožňuje ICMP[14] protokol. Ten obsahuje potenciálně nebezpečný druh paketu ICMP redirect, který provádí dynamické změny ve směrovací tabulce[15]. Legitimně by tuto zprávu (informující uživatelský počítač o existující lepší cestě) měly posílat pouze routery. Přesto může útočník označit svůj útočný počítač jako rychlejší cestu při směrování paketů. Pokud napadený počítač přijímá tento druh zpráv, přesměruje veškerou komunikaci. Tímto útočník docílí útoku s mužem uprostřed. Plně zautomatizovaný útok opět zvládne volně dostupný program Ettercap. Doporučená obrana je vypnout v operačním systému příjem zpráv o přesměrování pomocí ICMP protokolu. (Dostálek, 2008)

[11] Běžné domácí routery obsahují funkcionalitu přepínače.

[12] Je zde uvažována nejrozšířenější a zdaleka nejpoužívanější verze síťového protokolu IPv4.

[13] Jedinečný identifikátor síťového rozhraní. Softwarově je možné měnit MAC adresu na jinou hodnotu.

[14] Protokol ICMP slouží routovacím zařízením k zasílání chybových a provozních zpráv o stavu počítačové sítě.

[15] Obsahuje zjednodušený obraz topologie sítě, podle kterého systém rozhoduje, jak naložit s přijatým nebo odesílaným síťovým paketem.

6.2.2 Podvrhnutí DNS

Před načtením konkrétní webové stránky v internetovém prohlížeči probíhá nejprve překlad adresy URL na konkrétní číselnou IP adresu[16]. Je potřeba poslat žádost DNS serveru, který tento překlad zajistí. Pokud útočník úspěšně provedl nějakou variantu útoku muže uprostřed, vidí tyto procházející žádosti o překlad a je též schopen je modifikovat. Tímto podvrhnutím DNS záznamů je tak schopný přesměrovat uživatele na své potencionálně škodlivé stránky (jako překlad se vrátí podvrhnutá IP adresa na škodlivé stránky). Tyto stránky mohou vypadat úplně identicky jako ty skutečné, kam se chtěl uživatel dostat. Zde již obyčejně čeká formulář na přihlášení s údaji, které obdrží útočník, jakmile je uživatel zadá. (Hatch, 2008)

V lokální síti je obvykle přidělován DNS server (stejně tak jako ostatní konfigurační údaje pro připojení k počítačové síti) místním routerem (obsahující DHCP server). V případě jeho napadení může router rozesílat adresu útočníkovo záškodnického DNS serveru umístěného v Internetu. Následně bude možné nepozorovaně zaměnit požadovanou URL adresu na libovolnou IP adresu. Uživatelská kontrola v podobě ověření URL adresy v prohlížeči je v tomto případě zbytečná, protože se kvůli útoku shodují s požadovanou podvrhnutou URL adresou. (Hatch, 2008)

Dobrým způsobem obrany je nenechávat DNS server přidělovat automaticky, ale uživatelsky ho pevně nastavit konkrétní IP adresou nějakého dobře zabezpečeného DNS serveru. Vhodným doplňkem zabezpečení ve webovém prohlížeči je pak využívání rozšíření DNSSEC pro ověření (elektronickým podpisem) správného přeložení URL adresy na IP adresu.

6.2.3 Zranitelné domácí Wi-Fi routery

Většina běžných uživatelů nevěnuje dostatečnou pozornost svému domácímu zařízení, které spravuje celou lokální síť. Tudíž je to ideální místo, které by rád potencionální útočník ovládl, aby tak získal kontrolu nad celou sítí. Signál Wi-Fi technologie se šíří všemi směry a skrze hmotné překážky. Proto je možné, aby byl její signál zachycen z fyzicky nechráněného místa. Pokud router nebývá pravidelně aktualizován, nepoužívá dostatečně silné šifrování (WPA2) a současně také heslo, razantně to zvyšuje jeho zranitelnost.

WPA2 je považován za nejvíce zabezpečený bezpečnostní protokol pro komunikaci po bezdrátové síti Wi-Fi. Uživatelé využívající tento protokol tedy spoléhají na zašifrovanou komunikaci mezi nimi a bezdrátovým routerem. WPA2 k tomu používá dva druhy symetrických šifrovacích klíčů:

- PTK – privátní klíč stanovený mezi jednotlivým uživatelem a komunikujícím routerem. Každý připojený uživatel má jiný klíč a nemůže tak dešifrovat komunikaci ostatních uživatelů.

[16]Například URL adresa www.seznam.cz se přeloží na IP adresu 77.75.76.3.

- GTK – skupinový privátní klíč (náhodně generovaný) rozeslaný všem uživatelům připojeným ke stejnému bezdrátovému routeru.

GTK symetrický klíč je používán routerem jako šifrovací klíč a počítač uživatele jej používá pro následné dešifrování. Nejedná se ale o asymetrické šifrování, proto je použit jeden společný klíč. Klienti v normálním provozu nikdy nepoužívají tento klíč jako šifrovací a neposílají pomocí něj data.

Útočník může ovšem tento klíč vzít a zašifrovat s ním zprávu otravující ARP cache a odeslat, jako by jí poslal samotný router. Tato zpráva tak přiřadí IP adresu výchozí brány (adresa bezdrátového routeru) k MAC adrese útočníka. Počítač napadeného uživatele pak posílá všechna jeho data sice na správnou IP adresu, ale špatně přiřazenou k MAC adrese útočníka. Proto router přijme zprávu, kterou konkrétním PTK klíčem uživatele dešifruje a přepošle[17] ji útočníkovi zašifrovanou pouze jeho vlastním PTK. On ji pak může modifikovat nebo odposlechnout a poslat do Internetu. Jedná se o útok s mužem uprostřed. Tento útok je možný pouze z vnitřní pozice vzhledem k routeru. Nepřipojený útočník, který nezná přístupové heslo, nemůže tento útok využít. (Rosenblatt, 2013)

K získání přístupu k domácímu routeru se zabezpečením typu WPA/WPA2 bez znalosti hesla je možné využít zranitelnosti standardu WPS[18]. Konkrétně se jedná o chybu způsobu ověřování 8 místného PIN kódu, který je pevně svázaný s daným zařízením[19]. Při bezdrátovém ověřování se totiž kontroluje zvlášť první čtveřice PIN kódu a poté následující trojice. Poslední znak je z hlediska zabezpečení nadbytečný, slouží pouze jako kontrolní součet. Pokud je zadána alespoň jedna část kódu správně, je klientovi sděleno, která to byla. Poté už stačí stejným způsobem zjistit druhou část. Celkově je tedy třeba vyzkoušet pouhých 11 tisíc možností. Implicitně bývá funkce WPS aktivována na většině zařízení. (Viehböck, 2011)

Volně dostupný nástroj Reaver[20] je takto schopen odhalit nejprve PIN kód a posléze přístupové heslo na širokém spektru zařízení během 10 hodin. Tento nástroj je schopen se přizpůsobovat změně vysílacího kanálu i dočasnému zablokování přístupu v případě jeho detekce. Jako obrana se doporučuje deaktivovat podporu WPS. Ovšem bylo zjištěno, že mnohá zařízení i po deaktivaci funkce WPS ji dále umožňují využívat. Nejlépe je tedy nahrát do zařízení nejnovější firmware, pokud ho výrobce aktualizoval, případně pořídit zařízení nové. (Pash, 2012)

V případě, že je router dobře zabezpečen a nastaven, existuje ještě možnost rozsáhlého slovníkového útoku. Jednoduše se porovná soubor se zachycenými pakety autentizace (authentication handshake)[21] s předem spočítanou tabulkou kontrolních

[17]Na základě špatně přiřazené MAC adresy výchozí brány přepošle router zprávu útočníkovi. Správně by měl router odeslat zprávu směrem do Internetu bez průchodu skrz útočníka.

[18]Standard v počítačových sítích umožňující snadno nakonfigurovat domácí síť. Je povinně přítomný u zařízení využívající zabezpečení WPA/WPA2.

[19]PIN kód k danému zařízení bývá napsán vespod zařízení.

[20]https://code.google.com/p/reaver-wps/

[21]Může poskytnout například volně dostupný program Wireshark zachycující síťovou komunikaci.

součtů hesel (rainbow table) dostupných na Internetu. Takovou zpoplatněnou službu nabízí například web CloudCracker.com, který má k dispozici 5 miliard kontrolních součtů hesel pro prolomení zabezpečení typu WPA/WPA2. Tato operace porovnávání kontrolních součtů hesel zabere serveru CloudCracker maximálně 2 hodiny. V případě, že není vybráno dostatečně silné a unikátní heslo, získá tímto způsobem útočník přístupové heslo pro připojení k zabezpečené Wi-Fi síti. (DeLeeuw, 2012)

I pokud je s routerem uživatelsky správně zacházeno, obsahují současné domácí routovací zařízení řadu jiných zranitelností, těžko ovlivnitelných z jiné pozice než ze strany výrobce. Uživateli tedy zbývá pouze důkladný výběr zařízení nebo nahrání jiného firmwaru od třetí strany.

6.2.4 Útok zlého dvojčete

Zlým dvojčetem je myšlen útočníkův podvodný bezdrátový přístupový bod (AP), který předstírá, že je legitimní zařízení ve veřejné infrastruktuře. Pokud se uživatel omylem připojí k takovému nedůvěryhodnému zařízení, může útočník provést řadu útoků, a to i v případě, když se používá SSL[22], jak bude popsáno v dalším bodě. Pokud je uživatel připojen, je útočník v pozici muže uprostřed. Pozice dosažená útokem zlého dvojčete nevyžaduje v dnešní době žádné speciální technické schopnosti.

Podvrhnuté AP potřebuje pouze změnit SSID a MAC adresu (BSSID) na stejné hodnoty jako má legitimní router. V případě použití zabezpečení WPA-Personal/WPA2-Personal je potřeba znát i přístupové heslo, které je například u veřejných AP přístupné. U zabezpečení typu WPA (na rozdíl od zastaralého WEP) by bez zadání správného hesla neproběhla korektně vzájemná autorizace.

K útoku zlého dvojčete poslouží volně dostupný program airbase-ng. Útok je proveditelný, i pokud je uživatel již připojený ke správnému zařízení. K tomu slouží speciální rámec (disassociate packet) pro odpojení libovolné stanice, zaslaný útočníkem pomocí programu airbase-ng. Útočník může dále záměrně zvýšit výkon svého přístupového bodu tak, aby docílil přepojení klienta od původního přístupového bodu k jeho podvrhnutému. Uživatelův počítač se pak automaticky připojí (v případě existence dvou parametrově přesně stejných AP) k přístupovému bodu s nejsilnějším signálem. (How to Hack Wi-Fi, 2013)

Pokud potřebuje útočník zjistit heslo WPA2, může použít volně dostupný program Linset[23], který vytvoří parametrově identické AP bez hesla. Tento program bude automaticky blokovat (neustálým odpojováním) připojení k původnímu AP. Následně bude Linset spoléhat, že se uživatel sám připojí k falešnému přístupovému bodu. Pokud se připojí, budou všechny požadavky ve webovém prohlížeči přesměrovány (díky přidělení vlastního DNS) na podstrčenou stránku[24] požadující (formou

[22]Protokol SSL se nejčastěji používá pro bezpečnou komunikaci s webovými servery pomocí HTTPS.

[23]https://github.com/vk496/linset

[24]Heslo může být požadováno i z jiných smyšlených důvodů. Například jako potvrzení důležité bezpečnostní aktualizace k danému zařízení.

webového formuláře) ověření hesla k AP. Zadané heslo program samozřejmě uloží a předá ho útočníkovi. Útok se pak automaticky ukončí.

Pro uživatele je problematické si všimnout nebo zjistit, zda je připojen ke správnému přístupovému bodu. Doporučuje se používat zašifrovanou komunikaci, VPN[25] připojení a kontrolovat, zda jsou tato opatření aktivní. (Rapp, 2013)

6.2.5 Útok na zašifrovanou komunikaci

Kryptograficky chráněná komunikace představuje pro útočníka významně stěžující faktor. Přesto existují metody, které především při uživatelské nepozornosti dokáží tuto ochranu snadno vyřadit z provozu.

Zašifrovaná komunikace pomocí SSL, která prochází skrz útočníka, může být jeho zásahem převedena do otevřené formy pomocí volně dostupného programu SSLstrip[26]. Tento nástroj, chovající se jako proxy server[27], využívá skutečnosti, že protokol HTTP žádným způsobem neověřuje informace, které přes něj obdrží internetový prohlížeč. Jednoduše je pak nástrojem SSLstrip modifikován požadavek připojení k dané službě ze zabezpečeného protokolu HTTPS na nezabezpečený HTTP protokol. Této na první pohled nenápadné změny si může všimnout pouze pozorný uživatel, který kontroluje po načtení webové stránky použitý protokol (zobrazený v adresním řádku internetového prohlížeče). (Shaver, 2014)

Této zranitelnosti se snaží zabránit nový webový bezpečnostní mechanismus HTTP Strict Transport Security (HSTS). Je určen pro weby, které chtějí být dostupné pouze přes zabezpečené připojení. Ve všech případech, kdy je vyžadováno HSTS se z daného webu předá informace prohlížeči, aby využíval striktně protokol HTTPS. Všechna ostatní spojení mají být odmítána. Před prvním spojením ještě není tato informace k dispozici, proto ji může útočník ovládající datový tok k uživateli zablokovat. Některé prohlížeče jako je Google Chrome a Mozilla Firefox nově obsahují seznamy populárních webů se zapnutým HSTS ještě před první návštěvou. (Zap, 2012)

HSTS protokol se v prohlížeči váže na konkrétní DNS názvy webů. Proto je možné vylepšeným nástrojem SSLstrip+[28] zaměnit název stránky v adresním řádku prohlížeče za název implicitně nechráněný HSTS protokolem. Tato změna může být například přidaná subdoména tematicky sladěná s konkrétní stránkou[29]. Jako obrana je uživatelům především doporučena kontrola adresního řádku a aktivního HTTPS. Vhodné je také využívání technologie DNSSEC, která garantuje správnost DNS

[25]Pomocí digitálních certifikátů zabezpečená virtuální počítačová síť, která se používá při připojení k nedůvěryhodným počítačovým sítím.

[26]http://www.thoughtcrime.org/software/sslstrip

[27]Funguje jako prostředník mezi klientem a cílovým serverem, překládá klientské požadavky a vůči cílovému počítači vystupuje sám jako klient.

[28]https://github.com/LeonardoNve/dns2proxy

[29]Například přihlášení k webovým službám společnosti Google www.accounts.google.com zaměnit za neexistující, ale podobné www.account.google.com.

záznamů a jejich integritu při cestě k uživateli. V České republice podporuje tuto technologii přibližně 40 % ze všech zaregistrovaných domén[30]. (Nve, 2014)

Pokud je potřeba se připojit do Internetu z nedůvěryhodného prostředí, je často použita VPN síť. Nicméně ochrana, kterou poskytuje, není zcela vyhovující. Pokud má útočník přístup k datovému toku, může ukončit VPN spojení (například zahozením řídících paketů), které vrátí spojení do otevřené formy, typicky bez varování uživatele. (Lance, 2014)

Výše zmíněné útoky mají za cíl nenápadně deaktivovat ochranu, která je řešena pomocí certifikátů. Dalším způsobem je tyto certifikáty podvrhnout. Podvrhnutí je více nápadné než deaktivace, protože prohlížeč na nesprávný certifikát upozorní. Nepozorný uživatel přesto, jak píše (Lanze, 2014), většinou odklikne elektronicky špatně podepsaný SSL certifikát. Tímto přestává být jeho komunikace zabezpečena a je útočníkovi k dispozici v otevřené formě.

HTTP proxy server Mitmproxy[31] je schopen za letu generovat falešné certifikáty, které jsou přesně vyplněné jako certifikáty pravé. Na takto vytvořených certifikátech nesouhlasí pouze podvržený podpis. Proto je z hlediska bezpečnosti důležité nepřijímat v prohlížeči certifikáty, které nemají správný elektronický podpis. (Celetka, 2015)

6.3 Útoky na Internetu

Informační technologie nabízejí svým uživatelům stále lepší možnosti efektivní a rychlé výměny dat. Zároveň ale poskytují výhody těm, kteří chtějí prostředí Internetu zneužít k nekalým záměrům. Anonymita a také prostorová neuchopitelnost Internetu způsobuje značný přesun kriminálních aktivit do kyberprostoru, který útočníkům poskytuje různé možnosti s minimálním rizikem případného postihu.

Z prostředí Internetu je možné provádět i většinu výše popsaných útoků, ovšem provedení již není zdaleka tak jednoduché, protože je potřeba překonat vnější ochrany (např. firewall[32]) a dostat se do místní sítě. Přesto existuje řada jiných rozšířených hrozeb spojených především s přístupem na webové stránky.

6.3.1 Nedůvěryhodný webový prohlížeč

Muž uprostřed se nemusí nutně vyskytovat pouze na síti, ale také například ve webovém prohlížeči napadeného systému (Man in the Bowser). Zde teoreticky může kompletně měnit přijaté a na monitoru zobrazované informace za svoje vlastní. Prohlížeč se může navenek chovat naprosto normálně, ale když přijde určitá specifická akce (jako posílání elektronické platby z uživatelského bankovního účtu), provede něco úplně jiného (například změnu částky a čísla účtu příjemce na útočníkovy údaje), než zobrazuje.

[30] Aktuální statistiky jsou dostupné na https://stats.nic.cz/stats/domains_by_dnssec/

[31] http://mitmproxy.org/

[32] Zařízení sloužící k zabezpečení síťového provozu. Typicky mezi místní sítí a Internetem.

Muž v prohlížeči se může objevit po úspěšném napadení škodlivým kódem (kliknutím na odkaz, navštívení nakažených webových stránek, stáhnutím souboru, atd.). Škodlivý kód následně na napadeném počítači provozuje proxy server, který provádí za letu požadované modifikace. Kromě finančně zaměřených cílů jsou často zneužívány také sociální sítě.

Zákeřný a nebezpečný útok je hlavně v tom, že prakticky není možné zjistit, že je něco v nepořádku (adresa URL, platnost certifikátu i vyplněné údaje jsou totiž zobrazeny správně). Účinná obrana v elektronickém bankovnictví spočívá hlavně ve dvoufaktorové kontrole (ověření údajů v přijaté SMS zprávě, především cílového účtu a částky). Mnoho bezpečnostních expertů doporučuje používat oddělený operační systém striktně pouze pro účely bankovnictví. Je důležité také udržovat aktualizovaný prohlížeč a operační systém v dobrém stavu. V případě užití systému Windows je vhodné používat antivirový software. (ZoneAlarm, 2014)

Obvykle uživatelé také nevěnují pozornost nainstalovaným doplňkům webového prohlížeče a často neověřují, zda jsou důvěryhodné. Tyto pluginy ovšem mohou vést k infekci škodlivým kódem (malwarem), pokud nejsou stahovány až po pečlivém uvážení. Nejlepší řešení je nepotřebné a nedůvěryhodné pluginy zakázat. To může vést k zvýšení výkonu prohlížeče, pokud jich bylo aktivováno hodně. (Rao, 2014)

6.3.2 Cross-Site Scripting

Jedním z nejrozšířenějších způsobů jakým se objevuje škodlivý skript na seriózních webových stránkách je Cross-Site Scripting (XSS). Jedná se o využití zranitelnosti špatně zabezpečených webových stránek, kde je prostřednictvím bezpečnostní chyby (většinou neošetřených vstupů) podstrčen útočníkův skript. I když je XSS umožněn špatným ošetřením vstupů na straně webového serveru, tak XSS není útokem proti webovému serveru, ale proti webovému prohlížeči uživatele, který útočný kód vykonává.

Obecně řečeno může být nebezpečný prakticky jakýkoliv neošetřený vstup, který má šanci být někdy použit a zobrazen návštěvníkovi ve výstupu webových stránek. Například útočníkem vložený diskuzní příspěvek, který obsahuje vložený JavaScriptový kód je typickým příkladem použití XSS na webové stránce. Příspěvek se uloží do databáze a následně se zobrazuje (včetně spuštění daného skriptu) všem dalším návštěvníkům webu. (Brady, 2014)

Kromě trvale uloženého škodlivého skriptu na webovém serveru, je možné být vystaven skriptu uloženém v odkazu na webové stránky. Zjednodušeně řečeno se v odkazu předá skript webové stránce, která ho obratem vrátí uživateli zpět ve svém výstupu (za předpokladu, že nedochází ke kontrole vstupů na straně serveru).

Do podvědomí většiny uživatelů se dostal XSS hlavně jako zranitelnost, která umožní útočníkovi vyvolat na zranitelné webové stránce pouze výstražné okno se zprávou. Tato představa je mylná, protože útočník může skrz zranitelný web získat (s využitím skriptování) plnou kontrolu nad webovým prohlížečem. (Kümmel, 2011)

Ze strany webové aplikace je uživatel často identifikován pouze prostřednictvím souborů cookie. Ke krádežím těchto souborů dochází nejčastěji právě pomocí XSS. Útočník může následně (s využitím ukradených souborů cookie) na daných webových stránkách vystupovat pod identitou své oběti po dobu trvání relace. (Brady, 2014)

Útoky XSS nemusí být pouze statické. Útočník může dokonce s napadenou obětí navázat spojení a vyměňovat si s ní data nebo jí zadávat příkazy. Realizace v takovém případě probíhá tak, že se útočný skript zacyklí a v pravidelných intervalech se zasílají požadavky na útočníkův server. (Kümmel, 2011)

Dalším způsobem jak vložit skript je například technikou SQL injection, která dokáže vložit přes neošetřený vstup pozměněný SQL dotaz přímo do databáze. (Brady, 2014)

Útočník může využít pro nalezení webových zranitelností nějaký volně dostupný a zautomatizovaný bezpečnostní skener. Například skener obsahující různé exploitační nástroje (SQL injection, XSS a další) se jmenuje w3af[33]. Slouží především jako testovací nástroj zabezpečení webových stránek.

6.3.3 Falešný webový certifikát

HTTPS je zabezpečený webový protokol HTTP odolný proti odposlechu. Využívá asymetrického šifrování založeného na certifikátech ověřujících identitu protistrany. Pokud se uživatel připojí na stránky podporující protokol HTTPS, webový server odešle prohlížeči digitálně podepsaný certifikát ověřující jeho identitu. Prohlížeč má k dispozici předinstalované kořenové certifikáty významných institucí vydávajících certifikáty. Pomocí nich matematicky zkontroluje, zda podpis souhlasí s identitou stránek.

Pokud má útočník pod kontrolou datový tok mezi uživatelem a serverem, může podvrhnout tento certifikát za svůj vlastní falešný. Prohlížeč bude varovat uživatele, že je útočníkův certifikát nedůvěryhodný, ale uživatelé často tomuto varování nevěnují pozornost. Falešný certifikát může být vyplněn stejnými údaji (název společnosti, datum platnosti a další), přesně jako ten pravý. Jediné v čem se liší, je samotný neověřený elektronický podpis. (Clark, 2013)

Poté co uživatel vyplní formulář s přihlašovacím jménem a heslem (které si útočník zaznamená), může být komunikace dále vedena skrz něj na regulérní stránky. Bude tedy vystupovat v roli tichého prostředníka. Kromě zabezpečení je zachována veškerá funkcionalita. (Hatch, 2008)

6.3.4 Kontrolní otázka u webových služeb

K mnohým internetovým službám bývá uživateli dána volitelná či povinná možnost zadat odpověď na jednu kontrolní otázku v případě zapomenutí hesla. Až po správném zodpovězení je umožněn opětovně přístup k dané službě. Služby samotné

[33] http://w3af.org/

nabádají, aby byl na vybranou otázku uživatel schopen odpovědět i po několika letech. Například emailová služba na stránkách seznam.cz nabízí tyto otázky:

- Můj nejoblíbenější film/seriál?
- Nejoblíbenější herec/herečka?
- Rodné příjmení matky?
- Vysněná destinace pro dovolenou?
- Příjmení vaší první lásky?
- Nejoblíbenější kniha/spisovatel?

S trochou štěstí, úsilí a základních znalostí o uživateli služby je správně schopen odpovědět na tyto otázky v podstatě každý, pokud byly pravdivě zadány. V případě emailové služby bývá situace o to vážnější, že je na ní navázána řada dalších služeb, které obnovu hesla umožňují na základě přístupu k emailové službě, ze kterých byly zřizovány. Proto je vhodné tyto otázky nevyplňovat korektně a raději myslet dopředu v podobě bezpečného uložení skutečná hesla.

6.3.5 Nebezpečné reklamy na webových stránkách

Na důvěryhodných webových stránkách, které obsahují reklamy třetích stran, není zaručeno, že v reklamě nemůže být nějaký druh škodlivého skriptu. Samotné webové stránky nejsou tímto způsobem nakažené. Škodlivý kód přichází ze vzdálených serverů, které umísťují reklamu. Napadená stránka nemá žádnou kontrolu nad konkrétně umístěnou reklamou. Důvěryhodné weby je zobrazují, protože jsou často financovány pouze z příjmů za tyto reklamy, které zobrazují na svých stránkách. Tyto reklamy tam zprostředkovaně umístí reklamní společnost, která na základě návštěvnosti proplatí provozovateli stránek honorář. Ovšem takto může reklamní společnost nasadit nějaký druh závadné reklamy využívající neopravenou zranitelnost, která se může spustit a škodit i bez uživatelského zásahu.

Napadení počítače touto metodou probíhá většinou až po kliknutí na danou reklamu. Ta může mít například formu vyskakovacího okna. Ovšem stále častěji se objevuje napadení počítačů prostým načtením webové stránky bez dalšího uživatelského zásahu. Vše se navíc děje nepozorovaně v pozadí, tudíž uživatel si neuvědomí, co se stalo. Typicky je k tomu využita chyba v prohlížeči nebo jednom z jeho pluginů (Adobe Flash Player, Java nebo Microsoft Silverlight). Po úspěšném vstupu do prohlížeče jsou nainstalovány další druhy škodlivých kódů na počítač uživatele.

Pro zabránění nakažení se doporučuje mít aktualizovaný prohlížeč a blokovat tyto reklamy v automatickém spuštění. V případě systému Windows by měl aktualizovaný antivirový program rozpoznat a zabránit nakažení škodlivým kódem. Jako nejúčinnější řešení může být nainstalován plugin blokující skripty (např. NoScript pro Firefox) do prohlížeče. Tento plugin spolehlivě zablokuje samovolné spouštění všech skriptů. (Scharr, 2014)

6.3.6 Podvržený odesílatel emailu

U klasické neelektronické pošty není možné spoléhat na odesílatele uvedeného na dopise, protože ho mohl poslat kdokoliv a pouze se vydávat za odesílatele. Naprosto stejně je tomu tak u běžné elektronické pošty, pokud obě strany nevyužívají služeb elektronického podpisu[34]. (Toxen, 2003)

Email obecně nemá žádnou jinou obecně používanou ochranu před falšováním adresy odesílatele. Proto je možné místo odesílatele vyplnit zcela libovolnou adresu. Webové stránky sendanonymousemail.net veřejně umožňují poslat takto upravený email. Samotní autoři zmíněných stránek uvádějí například tyto legální možnosti využití:

- Informování policie o nelegálních aktivitách
- Emailový vtip na uživatelovy přátele
- Zjištění, zda přítel je opravdový přítel
- Další mnohé důvody.

Příklad takového snadného emailového vtipu je uveden na obrázku č. 12, snadno by se ale nechal vymyslet jiný nebezpečný text. Proto je namístě uživatelská obezřetnost a opatrnost. V případě podezření je vhodné si u odesílatele ověřit pravost emailu.

6.4 Chyby software a škodlivý kód

Software je obecně velice složitá věc. Čím více funkcí je v něm implementováno, tím přímo úměrně narůstá jeho složitost. Při narůstající složitosti nastává problém prozkoumání všech možný variant jeho chování ve všech možných podmínkách, do jakých se může software dostat. To představuje velkou zátěž na správné otestování funkcionality programu, ale samozřejmě taktéž na jeho zabezpečení. (Harris, 2008)

Rozmezí času mezi objevením nové zranitelnosti v softwaru a její opravou ze strany vývojáře se nazývá zranitelnost nultého dne. Pokud ji první objeví útočník a využije ji, tak je to útok nultého dne. Jakmile se útok veřejně někým objeví a nahlásí, měli by vývojáři začít pracovat na opravné záplatě. Mezi útočníky je nalezená a zatím neopravená chyba velmi cenná a dá se dobře prodat různým organizacím. (Zetter, 2014)

Existují i nezávislí bezpečnostní experti, kteří tyto chyby vyhledávají, často pro zábavu nebo kvůli vlastní reputaci. Na zveřejňování těchto prozatím neopravených chyb existují mezi experty dva rozdílné názory:

- Chybu zveřejnit – objevenou chybu nahlásit vývojáři i široké veřejnosti. Výhoda této strategie nahlašování chyb je, že pokud existuje útočník, který chybu již

[34]Obdoba klasického podpisu. Pro konkrétní elektronicky podepsaná data existuje možnost ověřit, zda byla vytvořena deklarovanou osobou.

využívá, můžou se proti ní uživatelé začít bránit svépomocí. Například pozastavením využívání softwaru.

- Chybu pouze nahlásit vývojáři – při této variantě se veřejnost nedozví o existenci nově nalezené chyby. Vývojář má tedy čas pracovat na opravě, a poté chybu oznámit až při vydání aktualizace. Nevýhodou tohoto způsobu je, že uživatelův software je do té doby proti nalezené chybě nechráněn. Dokonce ani samotný uživatel nemá jak se dozvědět o této hrozbě.

Přesto po vydání opravné aktualizace mnoho uživatelů a administrátorů zanedbává ochranu pomocí aktualizací. Proto prakticky vždy zůstává řada systémů potencionálně zranitelných.

Jedním z nejčastějších způsobů útoků na různý software je pomocí programátorem neošetřených vstupů. Technika přetečení vyrovnávací paměti (bufferu) využívá chyb programátorů při tvorbě softwaru. Při zapsání většího množství dat, než má daná paměť k dispozici, dojde k přepsání původního obsahu (pokud není přesně specifikované množství dat, které se do paměti může zapsat). Jakmile spuštěný program potřebuje z konkrétního místa opět číst, nacházejí se zde již změněné instrukce. (Toxen, 2003)

Z pohledu uživatele se jedná spíše o záležitost programátora. Přesto je možné ovlivnit tyto zranitelnosti výběrem kvalitního software. Vhodné je sledovat četnost aktualizací a předchozí známé bezpečnostní incidenty.

Pokud je již uživatelský stroj zasažen škodlivým kódem (malwarem), útočník má možnost prakticky plné kontroly. Počítač zkompromitovaný škodlivým kódem, již nevykonává pouze uživatelské příkazy, ale zároveň v utajení ty záškodnické. Přirovnat by se nechal k zlému dvojitému agentovi s pravou loajalitou k útočníkovi. (Skoudis, 2004)

Je důležité zmínit, že úroveň práv, které má uživatel přiděleny pro práci se systémem, ovlivňuje velikost potencionálních škod a možností při napadení škodlivým kódem. Ve velkém množství případů je činnost omezena právy daného uživatele. A čím menší oprávnění uživatel má, tím menší oprávnění má i škodlivý kód.

Snížení práv, pod kterými uživatel běžně pracuje, ale nepomůže proti zvláště pokročilým útokům. Přesto je dobré toto opatření zavést jako část strategie zabezpečení. Na konkrétní nutné změny či administraci systému si uživatel krátkodobě zvýší své oprávnění na administrátorské. (Tubin, 2013)

Uživatelé si často pletou jednotlivé druhy škodlivého kódu. Problémem je především, pokud dobře nerozumí rozdílům mezi jednotlivými kategoriemi. Nejsou pak schopni se rozhodnout, která určitá ochrana jim může pomoci v jejich konkrétních podmínkách. Určitě je dobré užívat správnou terminologii, ale rovněž je potřeba poznamenat možnost různého křížení mezi těmito druhy. Například nějaké viry můžou být rovněž červi. Podobně červi mohou obsahovat zadní vrátka, rootkity a podobně. (Skoudis, 2004)

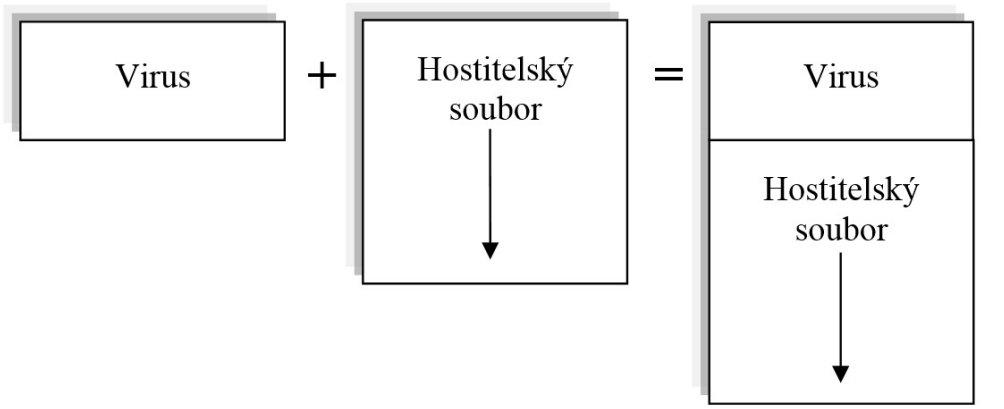
Účinná ochrana před škodlivým kódem je užití programů specializujících se na identifikaci, odstraňování a eliminaci škodlivého software a jeho nežádoucího chování. Různý bezpečnostní software může zastávat zároveň více funkcí z následujících:

- Firewall – odděluje provoz mezi počítačem a zbytkem sítě. Povoluje pouze předem definovaná pravidla a brání tak zejména neoprávněnému odesílání dat a přístupu k systému z počítačové sítě bez vědomí uživatele.
- Antivirový program – slouží k ochraně počítače před viry a dalšími různými druhy škodlivého kódu. Kromě předem naplánovaných kontrol obsahuje antivirus většinou i rezidentní ochranu, která nepřetržitě kontroluje a vyhodnocuje provoz počítače v reálném čase. Je potřeba zmínit, že žádný antivirový program[35] není naprosto spolehlivý.
- Kontrola integrity – nástroj pro kontrolu jakýchkoliv změn v kritických souborech systému na základě kontrolního součtu. Porovnává se předchozí výpočet s aktuálně provedeným. V případě změny bude uživatel informován, protože změna určitých částí systému může být příznakem nakažení škodlivým kódem nebo provedené neoprávněné změny.
- Antispyware – antivirové programy většinu spywaru nenajdou, proto je nutné použít speciální software. Antispyware se zaměřuje na důkladné vyhledávání a smazání nežádoucího spyware. Může chránit počítač v reálném čase podobně jako antivirus. Nejčastější příznaky, při kterých je vhodné použít antispyware jsou problémy s nežádoucí změnou domovské stránky, pomalý start počítače, časté vyskakování reklam při surfování na Internetu a podobně.
- Rootkit skenery – nástroje zaměřené na vyhledávání rootkitů a backdoorů.
- Sandbox – odděluje procesy ze spuštěného programu od ostatních procesů. Přístup programů spuštěných v sandboxu je omezen na vybrané adresáře a přísně kontrolovanou množinu zdrojů. Typicky jsou po ukončení tohoto programu smazány všechny jeho data a navráceny změny, které provedl. Bývá používán kromě ladění kódu také k otestování nedůvěryhodných programů, které by mohly poškodit systém nebo data. Kvůli poskytování vysoce kontrolovaného prostředí může být sandbox považován za příklad virtualizovaného prostředí.
- Jednoúčelové nástroje pro odstranění infiltrací – slouží pouze pro odstranění konkrétního škodlivého kódu na již infikovaném systému, protože některé infiltrace vyžadují speciální postup k jejich vyléčení.

[35] Webové stránky www.av-comparatives.org pravidelně zveřejňují testy mnoha antivirových programů v různých kategoriích (falešný poplach, výkonnost, úspěšnost v léčení, úspěšnost detekce a další) s hodnocením.

6.4.1 Počítačový virus

Jako virus se v počítačové terminologii označuje program, který se dokáže sám šířit bez vědomí uživatele, ale za jeho určité pomoci. Primárně se viry rozšiřují přeposíláním emailů s přílohami, stažením závadného souboru z webových stránek nebo pomocí přenosu z USB disku. Aby se vir rozmnožil, vkládá se do jiných spustitelných souborů či dokumentů. Chování počítačového viru je obdobné jako u viru biologického, který se šíří vkládáním svého škodlivého kódu do živých buněk.



Obrázek 5: Základní principiální schéma infekce souboru virem.

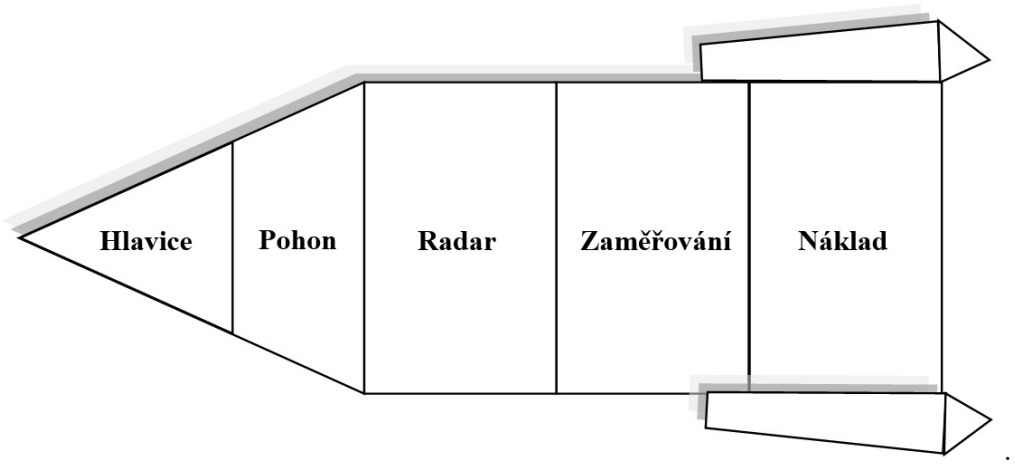
Existuje několik způsobů přidání viru k hostitelskému souboru. Nejzákladnější možnost je přidat virus před nebo za hostitelský soubor, takže se vykoná nejprve virus, který poté předá řízení právoplatnému programu nebo obráceně. Jak je vidět na obrázku 5. Dalším způsobem je přepsání části původního souboru virem, což ovšem může způsobit nefunkčnost původního souboru a uživatel může nabýt podezření, že není něco v pořádku. Co se týče velikosti souboru, je zachována přesná velikost jako před nakažením. (Skoudis, 2004)

S příchodem složitých programových balíků, které ukládají soubory různě na disku, se šíření virů podstatně omezilo. Málokdo tyto soubory přenáší na jiný počítač. Proto se tvůrci virů zaměřují na soubory, které se často přenáší. To jsou především dokumenty, které tuto podmínku splňují.

Firma Microsoft v rámci zdokonalování svého kancelářského balíku Microsoft Office zavedla možnost přidávat do svých dokumentů makra (posloupnost akcí, funkcí nebo příkazů). Jedná se o programovatelnou část dokumentu, která usnadňuje a automatizuje často se opakující činnosti. Tato makra se přenášejí v jednom souboru zároveň s dokumentem. Pro aktivaci viru v dokumentu stačí například nastavit infikované makro jako automaticky se spouštějící po otevření dokumentu. Základním stavebním kamenem makro virů je nevědomost uživatele. Neočekávají totiž v textovém nebo tabulkovém dokumentu výskyt viru. (Dočekal, 2004)

6.4.2 Počítačový červ

Počítačový červ je samoreplikující se kus škodlivého kódu, který se šíří skrze počítačové sítě. Ve většině případů nepotřebuje faktor lidského přičinění, na rozdíl od počítačového viru. Rychlost šíření může být díky plně automatizovaným útokům v porovnání proti počítačovým virům opravdu závratná. Červ zaútočí na všechny počítače ve svém okolí. Počítače, proti kterým proběhl útok úspěšně, převezmou kontrolu nad hostitelem a opět pokračují ve svém rozmnožování.



Obrázek 6: Komponenty počítačového červa zobrazeného jako řízená raketa.

Typický počítačový červ se nechá rozložit na několik základních částí. Jak je ilustrováno na obrázku výše. Pro lepší představu je možné metaforicky přirovnat červa k řízené raketě. Stejně jako řízená raketa je červ uzpůsoben a používán pro proniknutí k cíli.

Pokud se chce červ nebo raketa probít k cílovému systému musí obsahovat hlavici. Nejprve je potřeba prorazit zabezpečovací opatření. V hlavici je uložen kousek škodlivého kódu využívající odhalené zranitelnosti v zaměřeném systému. Tyto takzvané exploity mohou proniknout do systému využitím rozličného počtu zranitelností cíle. Mezi nejpoužívanější techniky proniknutí patří:

- Přetečení zásobníku – mnoho softwarových vývojářů často dělá chybu, když nekontrolují velikost dat, které poté různě přenášejí v paměti. Červ proto posílá větší množství dat, než původně programátor ve svém programu očekával. Takto neošetřená chyba poté vede k jeho přetečení a ovládnutí hostitelského stroje.
- Útok na sdílené soubory – například peer–to–peer sítě, kterými se sdílejí soubory mezi uživateli, mohou být použity pro přenos červa. Pokud červ převezme kontrolu nad procesem sdílení souborů, může se šířit tímto způsobem do dalších systémů.
- Využití špatné konfigurace – červ může v situaci, kdy je po něm požadováno heslo (potřebné pro další šíření), vyzkoušet nativní přístupová hesla nebo jiná

běžně používaná. Dále umí zneužít i jiné způsoby při zanedbané konfiguraci bezpečnostního systému.

- Pomocí emailu – základní metoda šíření je prostřednictvím hojně využívané elektronické pošty. Nejznámější emailový červ se nazývá I Love You. Počítačový červ zvládne napadnout a ovládnout (úplně bez uživatelské pomoci) třeba samotný poštovní server, který obsahuje mnoho cenných emailových adres.

Po získání přístupu k cílovému systému skrz kód hlavice, musí červ přesunout zbytek jeho těla do infikovaného systému pomocí pohonu. Hlavice mu totiž umožňuje pouze vykonání instrukcí na nakaženém systému. V nějakých případech jako je přenos pomocí emailu, může být část pomyslného pohonu a celého červa součástí hlavice. Pro přenos se používají tyto základní mechanizmy:

- FTP – protokol určený pro přenos souborů po síti
- HTTP – HyperText Transfer protokol běžně používaný k přístupu na webové stránky. Taktéž, ale muže být využit k přenosu dat
- SMB – protokol ke sdílení souborů pro operační systém Windows, podpora ostatních systému je také možná.

Radarový mechanizmus vyhledává oběti. Tvůrce radarového algoritmu a celého červa má k dispozici množství použitelných způsobů kam expandovat. Tyto mechanizmy nebývají vůbec složité:

- Emailové adresy – červ prohledá počítač, jestli nenajde uživatelův adresář s jeho elektronickými kontakty
- Síťoví sousedé – prohledá své okolí. Využije například protokolu SMB pro nalezení sdíleného úložiště nebo programu ping
- DNS dotaz – červ se připojí na místní DNS server překládající URL adresy na IP adresy, které jsou zpracovatelné počítačem. Takto červ zneužije DNS server jako výborný repozitář s cílovými adresami
- Náhodně vybraná síťová adresa – náhodné zkoušení cílových adres.

Předposlední částí je zaměřování. Červ se snaží odhalit zranitelná místa, kde by mohl zaútočit. Stejně tak jako řízená raketa musí zasáhnout obranu na nejslabším místě. Červ zkouší jestli exploit obsažený v hlavici bude proti různým zranitelnostem fungovat.

Poslední část běžného červa je náklad. Je to hlavní důvod, proč vůbec červ existuje. Náklad představuje kus škodlivého kódu červa, který přidá útočníkem požadované chování na napadený systém:

- Otevření zadních vrátek do systému – po průniku do systému otevře nový vchod pro případ, kdyby byla zranitelnost, kterou původně vnikl do systému opravena.

Díky zadním vrátkům je pro útočníka napadený stroj vzdáleně snadno ovladatelný a přístupný.

- Využití napadeného počítače v síti botnet.

Kromě základních výše popsaných částí červa, může obsahovat i další přídavné pokročilé moduly rozšiřující funkčnost. Například modul na zamaskování nebo modul polymorfní změny vlastní struktury.

Z velké části závisí úspěšné šíření červů na prostředí systémů, které jsou v pozici oběti. Jakákoliv komponenta totiž může být odkázaná na přítomnost specifických programů, knihoven nebo konfiguračního nastavení. (Skoudis, 2004)

6.4.3 Zadní vrátka

Zadní vrátka (anglicky backdoors) jsou programy, které dovolují útočníkovi, který je tam nasadil, obejít normální bezpečnostní kontrolu systému a umožnit mu do něj přímý přístup. Samy o sobě zadní vrátka nejsou nebezpečná ani neškodí. Pouze dávají útočníkovi přístup do systému. Až později začne útočník v systému neoprávněně škodit.

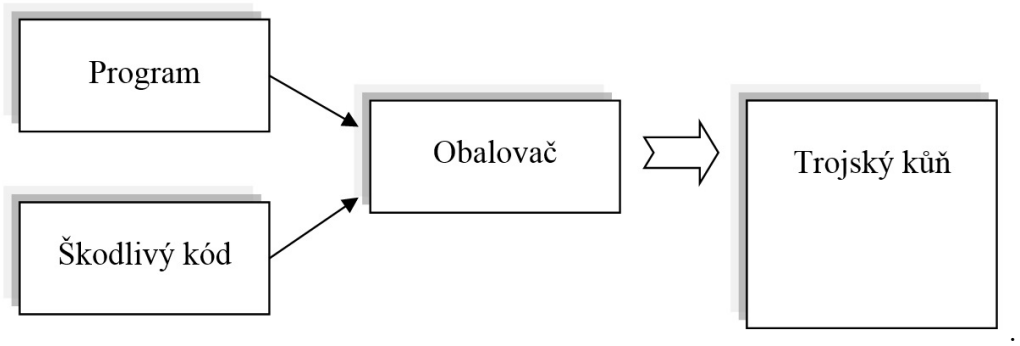
Kvalitní zadní vrátka jsou těžko zjistitelná, zvláště pokud nejsou často využívána. Komunikace s napadeným počítačem se uskutečňuje pomocí spuštěné služby na nějakém číselně vysoko umístěném portu UDP nebo TCP. Maskovat se dá také jako standardní služba běžící na svých vyhrazených číselných portech. Firewally komunikaci skrz taková maskovaná zadní vrátka obyčejně nefiltrují. Modernější programy backdoors používají například komunikační protokol ICQ. (Jirovský, 2007)

ICMP protokol, sloužící pro zpravování ostatních počítačů v síti o chybových hlášeních, může být také použit jako utajený komunikační kanál. Jelikož se nejedná o UDP nebo TCP komunikaci, tak uniká různým skenovacím programů pro detekci otevřených portů. Protože funguje na odlišném principu. (Skoudis, 2004)

6.4.4 Trojský kůň

Název je převzatý z řecké historie. Původní trojský kůň byl zákeřný dar, který dovolil útočníkům projít skrze velmi dobře střežené hradby města Trója. Úplně na stejném principu funguje i počítačový trojský kůň. Je to normálně vypadající a většinou funkční software s přidanou nežádoucí funkcí. Nereprodukuje se sám jako vir nebo červ. Obvykle je umístěn na pochybné webové stránce, kde si ho uživatel stáhne sám. A to například v podobě nelegálního software nebo aktivačních klíčů. Hlavní cíl je přesvědčit uživatele, že je vše v pořádku a žádaný program[36] je přesně tím programem, kterým se zdá být.

[36]Nemusí jít vždy pouze o programy. Trojský kůň se může stylizovat do podoby souboru s muzikou nebo jakýkoliv jiných souborů. Na první pohled tento dojem podpoří změnou ikony, změnou názvu a také přidáním odpovídající koncové přípony souboru (pokud systém skrývá koncovku souboru, může uživatel například soubor muzika.mp3.exe vidět jako muzika.mp3).



Obrázek 7: Dva programy zkombinované do jednoho trojského koně.

Mezi běžné triky patří, že si uživatel stáhne v dobré víře trojského koně vydávajícího se za antivirový program, který pro odstranění fiktivní nákazy požaduje zakoupení své plné verze. Zapojena je tedy určitá forma sociálního inženýrství.

Jakmile se podaří trojskému koni nastěhovat do hostitelského počítače, tak u zdařilejších verzí bývá jeho první starost vyřazení bezpečnostního software jako antivirový program a firewall. (What Is The Difference Between A Virus, Worm, Trojan, And A Rootkit, 2014)

Pro vytvoření trojského koně používají útočníci obalovač neboli wrapper. Nejprve se vezme nějaký legitimní dobře fungující program a škodlivý kód k němu přibalí pomocí nástroje typu wrapper. Například obalovací nástroj eLiTeWrap[37] spojí kód trojského koně a nosného programu. Přibaleno je k němu také nezbytné řízení pro rozbalování. Jak píše (Jirovský, 2007).

Takto jsou oba dva sloučené programy v jednom sdíleném výstupním souboru jako je vidět na obrázku 7. Pokud je program společně s trojským koněm spuštěn, stanou se z nich dva oddělené procesy. Z pokročilejších technik může být implementováno například vlastní maskování, aby trojský kůň zmátl antivirové programy. Bývá používáno šifrování nebo polymorfní chování měnící svůj vlastní kód. (Skoudis, 2004)

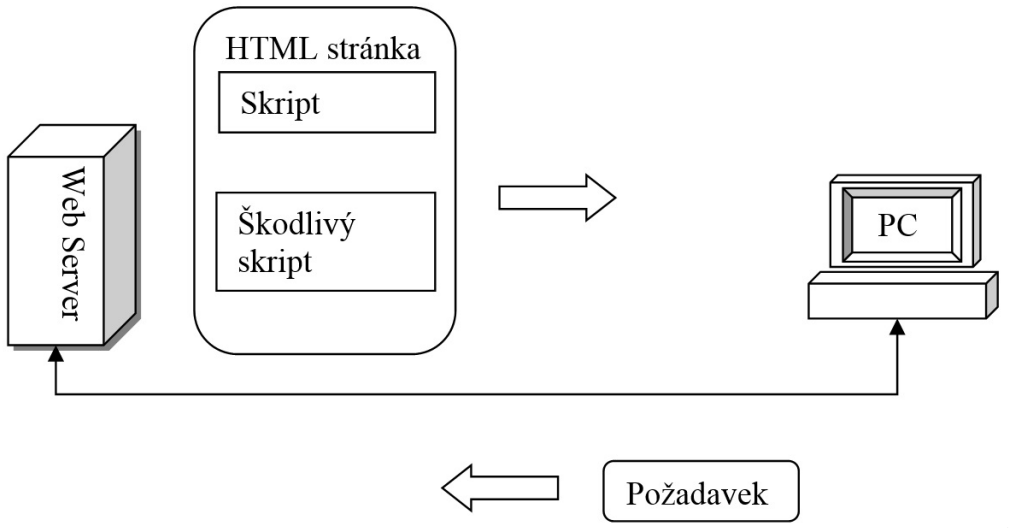
6.4.5 Škodlivé webové skripty

Webový skript je druh odlehčeného mobilního programu, který se stahuje na lokální počítač z navštíveného webového serveru společně s webovou stránkou. Je vykonáván s minimálním nebo žádným uživatelským zásahem. Primárně dělá z webového obsahu, který je statického rázu, obsah dynamický. Rozpohybuje stránky, reaguje na uživatelské akce a přizpůsobuje se chování uživatele. Vzhledem k malému a jednoduchému kódu je ideální k přenosu po internetových sítích. (Skoudis, 2004)

Skriptovací jazyky jsou vlastně jazyky interpretovanými. Skripty tak ke svému běhu potřebují interpret jazyka, který bude vykonávat jednotlivé příkazy. V případě

[37]Na Internetu není tento program již běžně dostupný ani podobné jiné nástroje jako YAB.

skriptů na straně webových browserů, jsou interprety právě webové prohlížeče, které interpret jazyka obsahují. (Kümmel, 2011)



Obrázek 8: Znázornění přenosu škodlivého skriptu ve webové stránce.

To ovšem také otevírá různé možnosti, jak těchto vlastností zákeřně využít a dostat útočníkův kód na uživatelský počítač. Pro představu následuje několik konkrétních základních případů využití:

- Monitorování uživatelských aktivit na webových stránkách
- Přesměrování na webové stránky, kam se uživatel dostat rozhodně nechtěl
- Podstrčení trojského koně a podobně.

Škodlivé skripty se dobře šíří přes webové prohlížeče, které díky své složitosti obsahují spoustu využitelných chyb. Přidáváním další funkcionality prohlížečů se objevují chyby nové, které je nutné pomocí záplat ošetřovat.

Skripty jsou připraveny k použití okamžitě po jejich natažení společně s webovou stránkou. V paměti zůstávají až do chvíle, kdy uživatel přejde na jinou stránku nebo kdy stránku se skriptem zavře. V tom případě budou skripty z paměti smazány a nebude je již možné využívat. (Kümmel, 2011)

Schopnost vykonávat stažené skripty mají rovněž moderní emailoví klienti. Podporují totiž funkcionalitu webových stránek zobrazením HTML kódu v elektronické zprávě. Zde se může následně vyskytnout nějaký druh škodlivého skriptu. Nejpoužívanější skriptovací jazyky na webových stránkách:

- JavaScript – obvykle jsou jím interaktivně ovládány a měněny grafické prvky stránek. JavaScript nemůže pracovat se soubory na pevném disku. Jedná se o úmyslné bezpečnostní omezení. Je tak zabráněno tomu, aby útočník mohl na

disk ukládat nebezpečné soubory nebo číst z pevného disku soukromé informace. Tato skutečnost je asi největším omezením skriptovacích jazyků.

- Flash – obsahuje programovací jazyk, který se používá pro tvorbu animací na webových stránkách reagujících na chování uživatele. Často je pomocí tohoto jazyka zobrazována reklama. (Skoudis, 2004)

6.4.6 Rootkit

Škodlivý kód s názvem rootkit je ve své podstatě druh trojského koně s funkcionalitou zadních vrátek, který přímo mění operační systém. Žádný kód z předtím popsaných nenapadá přímo hostující operační systém a jeho základní funkce. Pokud úspěšně převezme kontrolu, zamaskuje sebe a své chování v systému tak, aby nebyl uživatelem snadno zjistitelný. Často tedy rootkit musí upravit programy nacházející se v napadeném systému, které by ho mohly uživateli odhalit a jeho přítomnost zobrazit. Existují různé stupně nebezpečí a stupně závažnosti ze strany rootkitů. Především je důležité jaké má rootkit oprávnění nakládat se systémem. Nejnebezpečnější varianta je s přístupem k jádru operačního systému. (Kassner, 2008)

Speciální poddruh rootkitu je bootkit. Liší se v tom, že je zaváděn před operačním systémem. Bootkit totiž přepisuje zavaděč v MBR tabulce, odkud se začíná nahrávat sám a až poté předá řízení napadenému systému. Díky tomu je těžko zjistitelný, protože ze své pozice má možnost se vyhnout všem ochranám operačního systému. (Golovanov, 2008)

6.4.7 Keylogger

Hlavní náplní práce keyloggeru je skrytě monitorovat stisknuté klávesy na klávesnici. Je to speciální druh slídícího škodlivého programu, který vše co zachytí, posílá útočníkovi (nejčastěji například uživatelská hesla). Existují i varianty zaměřené na nahrávání zvuku (snímaný mikrofonem), pořizování snímků obrazovky (Print Screen) nebo videozáznamu z připojené webkamery (bez indikace LED diodou).

Za zmínku určitě stojí i existence keyloggerů v hardwarové formě. Hardwarový keylogger je malé zařízení o velikosti několika málo centimetrů zapojující se mezi klávesnici a počítač. Pokud útočník získá na chvilku fyzický přístup k zařízení, představuje tato metoda nejsnadnější způsob získání uživatelských hesel na počítačích. Současné HW keyloggery jsou vybavené i bezdrátovým modulem, který může v pravidelných intervalech odesílat zachycená data prostřednictvím emailu. Tímto tedy odpadá útočníkovi nutnost opětovného vyzvednutí dat a snižuje se riziko odhalení. Jelikož zařízení odchytává přímo elektrické signály z klávesnice, není zde možnost softwarové detekce ze strany uživatele. Proti takovému zařízení existuje obrana pouze ve formě vizuální kontroly počítače. (Kümmel, 2015)

6.4.8 Spyware

Jedná se o špionážní software sledující různé druhy informací o uživateli, které následně shromažďuje, aniž by o tom informoval. Obyčejně bývá uživatelem nevědomky nainstalován současně s nějakým volně dostupným programem. Jeho účelem není poškodit počítač, ale uživatele. Hlavním důvodem pro znepokojení je především narušení soukromí uživatele.

Spyware může také měnit nastavení počítače a způsobit tím například jeho zpomalení nebo zaseknutí. Spyware je obyčejně vytvořen za účelem zisku. Proto zobrazuje například reklamy, mění domovskou stránku v prohlížeči, přidává pluginy a toolbary do webového prohlížeče, krade osobní informace (emailovou adresu, cookies, číslo kreditní karty a další), které následně prodává k marketingovým účelů.

Například v druhé čtvrtině roku 2014 došlo podle záznamů k 175 milionům úniků uživatelských dat (emailové adresy, uživatelská jména, čísla kreditních karet a podobně). To je přibližně 2 miliony denně. (Goldman, 2014)

Pokud byl uživatel předem informován o přidání spyware, pak se zjednodušeně řečeno nazývá Adware. Jedná se o legitimní způsob nasazení, zejména pro uživatele, kteří nechtějí platit za software. (Beal, 2013)

6.4.9 Ransomware

Druh vyděračského škodlivého kódu (ransomware) znemožňuje uživateli přístup k počítači nebo datům. Obyčejně se snaží u napadeného uživatele lživým tvrzením vyvolat paniku (například z možného trestu za porušení zákona) a následně vyžaduje peněžní platbu[38], aby se situace vyřešila. Tvůrci se také často stylizují do role záchranářů. Kdy vyvolají nějaký druh zdánlivého problému (vir, poškození dokumentů) a za úplatu nabízejí nástroj pro jeho opravu.

Při variantě zablokování systému nebývá situace tak vážná. Po spuštění operačního systému je co nejdříve zaveden škodlivý kód odepírající přístup, který obyčejně vypadá zdařile a věrohodně. Nedovolí spustit správce úloh ani jinak pracovat se systémem. Zobrazena je falešná výzva (policie, výrobce operačního systému a jiných) často doplněná o záznam z přítomné webkamery (pokud jde o notebook) zobrazující uživatele na monitoru. V příloze je jedna z mnoha možných variant vzhledu výzvy. Tyto případy jsou řešitelné reinstalací, obnovou systému nebo zásahem z jiného systému. (Erben, 2014)

Při útoku na data je situace daleko vážnější, protože dojde k zašifrování všech uživatelských dat uložených na pevných discích a připojených USB flash zařízeních. V případě že jsou k systému připojené cloudové disky (například služby Disk Google a Dropbox) dojde k zašifrování i těchto dat umístěných na Internetu, které obvykle slouží jako záloha. Pokud uživatel nemá provedenou zálohu, tak se s velkou prav-

[38]Novinku v oblasti platby představují kryptoměny (elektronické měny jako Bitcoin), kdy převody mezi jednotlivými účty k majiteli jsou prakticky nedohledatelné. Používány jsou, ale také jiné metody jako prémiové SMS zprávy a převod na účet.

děpodobností k datům již nedostane. I po zaplacení slíbená pomoc často nepřijde. (Myers, 2013)

Například v roce 2014 ransomware TorrentLocker zablokoval počítače 40 tisícům uživatelů. Z tohoto počtu 3500 infikovaných počítačů pocházelo z České republiky. Výkupné (v průměru okolo 22 tisíc korun) se rozhodlo zaplatit 28 Čechů. (Čížek, 2014)

6.5 Sociální inženýrství

Překvapivě jednoduchou cestu průniku zabezpečením představuje sociální inženýrství. Tato metoda nepřekonává technické prostředky, ale samotného uživatele. Nezkušení a neinformovaní uživatelé se tak nechávají od útočníka[39] různými způsoby uvést v omyl, který pak vede k bezpečnostnímu incidentu. Lidské oči a uši jsou v podstatě také takové vstupy, do kterých jde vložit škodlivá informace zneužívající přirozené důvěřivosti člověka. Bezpečnost informačních technologií je tedy do velké míry spojena s uživatelem a jeho chováním v různých situacích. Proto je třeba věnovat se kromě zabezpečení osobního počítače také samotnému uživateli.

Útočník využívající sociálního inženýrství se nazývá sociotechnik. Může kombinovat všechny možné způsoby[40] a cesty, jak se dostat k uživateli. Tato práce se omezuje pouze na nejběžnější metody prováděné elektronicky. Teoretický základ je, ale u všech útoků směřující na člověka stejný. Nezáleží tak na tom, jaká metoda se použije, vždy se cílí na konkrétní zranitelné lidské vlastnosti. Narazí-li uživatel na některou z následujících situací, měl by zbystřit a promyslet své další kroky:

- Důvěra – sociotechnik se snaží navázat přátelský vztah a proto nenápadně předhazuje informace podporující dojem důvěryhodné a legitimní osoby. Přitom pouze předstírá a vydává se za někoho jiného (například za skutečnou osobu či člena organizace). Informace potřebné pro úspěšný útok skládá a shromažďuje z různých veřejných zdrojů. Používá například oficiální loga společností, nechráněné interní informace, dokumenty nalezené v odpadu, napodobuje způsob a styl komunikace, využívá znalosti o konkrétních lidech a další metody.
- Pocit viny – snaží se nabudit v uživateli pocit viny, kterým sociotechnik navede oběť na řešení dané situace způsobem pro něj výhodným.
- Zvědavost – sociotechnik může připravit pro oběť neodolatelnou informaci týkající se její osoby nebo někoho z okruhu známých lidí.
- Touha být užitečný – vrozený altruismus u většiny lidí vede k dobrému pocitu z vykonaného dobra. Proto mohou být různé okolnosti zanedbány. Obzvláště zranitelní pak mohou být muži pomáhající ženám.

[39] Nejznámějším sociotechnikem na světě je Kevin Mitnick. Ve své knize Umění klamu odhaluje důmyslné techniky ovlivňování lidí, kterými se dokázal dostat do počítačových systémů různých podniků a institucí.

[40] Telefon, osobní kontakt, prohledávání odpadků, sběr informací na Internetu a další.

- Strach – oběti je vyhrožováno postihem, pokud nebude splněná určitá podmínka. Oběť začne často neuváženě jednat podle přání sociotechnika, aby nenastal zmiňovaný problém.
- Vidina osobního zisku – sociotechnik může učinit oběti falešnou lákavou nabídku, například z pozice výše postavené osoby. Oběť pak může pozapomenout na správné zásady bezpečnosti a vykonat oč se po ní žádá.
- Zmatení – pokud není dostatek času na promyšlení situace a oběť je pod určitým tlakem, může snáze udělat chybu.
- Ostražitost – sociotechnik zprvu podniká neškodné kroky, které po určitém čase, až opadne ostražitost, proloží svým skutečným zájmem.

Sociální inženýrství je účinná a moderní metoda jak manipulovat s lidmi a získávat informace důvěrného charakteru. Nevyžaduje téměř žádné speciální technické znalosti a technologické prostředky. Vychází především z dobré znalosti psychologie člověka a jeho chování. I přes velké nebezpečí se o tomto tématu moc nemluví a neplatí na něj žádný program. Uživatel se může bránit především vnímáním detailů, podezřelého chování, kritickým myšlením[41] a důsledným ověřováním informací. (Jirovský, 2007)

6.5.1 Phishing

Podvodná metoda phishing znamená rozesílání falešných emailů žádajících uživatele o citlivé údaje[42]. Na první pohled se snaží přesvědčit, že jde o legitimní zprávu zaslanou uvedeným odesílatelem. Po kliknutí na přiložený odkaz se otevře stránka s formulářem pro přihlášení k dané službě. V emailu i na stránkách bývají pravá loga společnosti a uvedeni jsou také skuteční zaměstnanci. Emailová adresa je také často pravá. (Co je to phishing?, 2014)

Často mají zaslané phishingové zprávy za cíl uživatele donutit otevřít přiloženou přílohu emailu, která obsahuje nebezpečný škodlivý kód. Uživatel tak například obdrží zprávu z banky o jeho fiktivním dluhu, kde jsou podrobnosti a platební pokyny uvedeny v příloze. Po otevření přiloženého souboru je místo avizovaných podrobností spuštěn škodlivý kód.

Metody tvůrců phishingových zpráv jsou opravdu různorodé a často i nečekané. Podvést se tak může nechat i zkušenější uživatel. Běžné důvody, které útočníci používají:

- Konec platnosti služeb – podvodná informace sdělující vypršení platnosti uživatelského účtu. Pro prodloužení je třeba vyplnit formulář s uživatelským heslem.
- Neprovedená bankovní transakce – údajně zamítnutá transakce z různých důvodů (překročen limit, nedostatek prostředků, chybně zadané bankovní kódy

[41] Schopnost nepodléhat prvnímu dojmu, obecnému mínění nebo naléhavosti nějakého sdělení.
[42] Přístupová hesla, čísla kreditních karet a další důvěrné informace.

a další). V emailu je vyžadován zásah uživatele. Je zde také připraven odkaz na falešné webové stránky dotyčné banky.

- Odměna za vyplnění dotazníku – po vyplnění falešného dotazníku a vyplnění bankovních údajů má být zaslána odměna.
- Nová zpráva – doručení informace o nové údajné zprávě nebo oznámení s připraveným odkazem k falešným webovým stránkám.
- Internetová objednávka – potvrzení fiktivní objednávky z internetového obchodu.
- Oznámení o neobvyklé aktivitě – správce systému provozující poštovní schránku pozastaví její užití na základě zaznamenané neobvyklé aktivity. Pro obnovení účtu je údajně třeba kliknout na přiložený odkaz.
- Varování o podvodných zprávách – falešná zpráva informuje o předešlých falešných zprávách. Využívá k tomu oficiálního varovného textu na stránkách bankovní instituce. Zároveň žádá o verifikaci emailového účtu na připraveném falešném odkazu.

Z hlediska uživatele je zásadní si uvědomit, že provozovatelé důvěryhodných služeb nikdy nežádají o důvěrné informace. A zdaleka ne prostřednictvím emailu.

6.5.2 Pharming

Hlavní princip pharmingu spočívá ve vytvoření falešné iluze reálné webové stránky. Uživatel je za pomoci různých technických prostředků přesměrován na podvrženou webovou stránku, která se jeví přesně jako pravá stránka, na kterou se chtěl dostat. Ve skutečnosti jde pouze o její napodobeninu, ale o tom uživatel obyčejně neví. Účelem je vylákat z oběti pod nejrůznějšími záminkami soukromé údaje (především ty přihlašovací). Určitou indicií pharmingu je jakékoliv nestandardní chování. Například požadování údajů, které nejsou běžně k přihlášení potřeba.

6.5.3 Baiting

Baiting je útok pomocí fyzického nosiče jako je CD, DVD nebo USB disk místo obvyklého emailu. Na tyto nosiče je nahrán škodlivý software, který nakazí počítač. Tímto získá útočník přístup k nakaženému počítači nebo jeho prostřednictvím rovnou k celé místní počítačové síti.

Poté tyto nosiče umístí podle potřeby tak, aby se k nim uživatel mohl dostat. Například v chodbách a veřejných prostorech pohodí tato CD s inteligentně vybraným popiskem, který zbudí zvědavost. Jakmile uživatel nalezne nastražený disk a vloží ho ze zvědavosti do svého PC, nevědomky ho nakazí malwarem. Nedoporučuje se tedy připojovat nalezené neznámé disky k počítači. (Rao, 2014)

6.5.4 Poplašné zprávy

Poplašné zprávy (neboli hoax) mají za cíl své příjemce úmyslně mystifikovat. Jsou rozesílány elektronickou formou (email, IM zprávy, sociální sítě) v podobě různých falešných poplachů, zpráv, proseb, petic a výzev. Obvykle bývá součástí těchto zpráv část nabádající uživatele, aby zprávu přeposlali dále svým známým. Škodlivost tak spočívá pro příjemce pošty především v poskytovaných nebezpečných radách a nepravdivých informacích. Uživatelé mohou dále rozesíláním zpráv nevědomě napomáhat v dezinformování ostatních uživatelů. Obranou proti poplašným zprávám je v první řadě zdravý úsudek. S ním pak souvisí ověřování informací pomocí různých specializovaných informačních databází[43]. (Kysela, 2012)

[43]Například www.hoax.cz nabízí vyhledávání v pravidelně aktualizované databázi s nejrozšířenějšími hoax zprávami.

7 Anonymita

Internet nebyl navrhnut jako anonymní prostředí. IP adresy slouží počítačům jako virtuální adresy na základě, kterých komunikují. To znamená, že je možné zpětně dohledat a přiřadit IP adresu k určitému místu. Například pokud se uživatel připojuje pod IP adresou určitého poskytovatele Internetového připojení, je tento provozovatel schopný říct, komu byla tato adresa poskytnuta.

Pro běžného uživatele je důležité rozumět rozdílům mezi zabezpečením a anonymitou. A v případě potřeby s ní umět pracovat a vyvarovat se běžných uživatelských chyb, které by mohly stát prozrazení a narušení soukromí.

7.1 Otisk prohlížeče

Pokud je uživatelem používán standardní prohlížeč, tak je možné i pouhým porovnáváním záznamů v databázi dřívějších přístupů odhalit unikátnost prohlížeče. Takzvaný otisk prstu webového prohlížeče umožňuje velmi přesně určit konkrétní identitu prohlížeče pomocí zdánlivě neškodných informací jako:

- Časové pásmo
- Verze použitých pluginů
- Rozlišení obrazovky
- Dostupné systémové písmo
- Cookies a další.

Tyto drobné informace dohromady vytvoří téměř jedinečnou informační stopu, podle které je možné rozlišit jednotlivé uživatele, a to i pokud používají Tor.

Organizace EFF[44] vytvořila testovací stránky Panopticlick[45], kde je možné zkušebně ověřit informace, které jsou daným prohlížečem poskytovány. Zároveň z vlastní databáze předchozích pokusů vypočítá unikátnost takového přístupu.

7.2 Záznam IP adresy

Při běžné komunikaci na Internetu je na komunikačních uzlech (router) vidět odkud a kam komunikace probíhá. Většinou se používá co nejkratší a nejrychlejší cesta, která se nemění, pokud to není nutné. To velmi usnadňuje odposlech. Pokud je tedy znám zdroj a cíl internetového datového toku, pak je umožněno vystopování uživatelovo zájmů a úmyslů. Tyto informace se ukládají na komunikačních uzlech pro případnou budoucí potřebu.

[44]Electronic Frontier Foundation (EFF) je mezinárodní nezisková organizace, která obhajuje právo na občanskou svobodu v digitálním světě.

[45]Dostupné na webových stránkách www. panopticlick.eff.org.

V krajním případě může toto odhalení ohrozit uživatelovu práci nebo fyzickou bezpečnost. Například pokud je uživatel v zahraničí a připojí se na server svého zaměstnavatele. Odhalí tím národnostní původ a profesní příslušnost komukoliv, kdo sleduje síť. Pokud není použito nějakého šifrování, tak je dokonce viditelný celý obsah protékajících dat.

7.3 Informační stopa

Aktivní uživatelé Internetu za sebou zanechávají velmi silnou informační stopu. Kromě již zmíněných záznamů IP adres jsou to především fotografie, komentáře, dokumenty a jiná uživatelem nahraná data. S trochou nadsázky by se dalo říci, že co se na Internet jednou nahraje, už nezmizí. Data jsou různě zrcadlena, zálohována a kopírována. Je třeba počítat, že i neveřejná data nahraná na Internet se mohou za nějaký čas dostat na veřejnost. Proto je vždy užitečné vzít tuto skutečnost v úvahu.

Mnoho společností poskytující různé služby na Internetu má dlouhé licenční ujednání, které často obsahuje zmínku o tom, že uživatelská data se mohou používat k reklamním účelům a výzkumu dat. (Bašta, 2013)

7.4 Cookies

Uživatelé zajímající se o své soukromí by měli vědět o cookies[46]. Jedná se o určitý druh textové značky zanechávaný webovými servery v uživatelských počítačích. Tyto samotné značky nemají žádnou možnost, jak uživatele sledovat. Sledují je až webové služby využívajících těchto značek na rozpoznání uživatelů, kteří již službu navštívili dříve. Pokud se nashromáždí dostatek údajů i z jiných stránek, vytvoří to o dané osobně určitý vypovídající obraz (zájmy, vyhledávané informace, četnost návštěvností webů a dalších). Ten nejčastěji bývá použit k reklamním účelům šitým dané osobě na míru. Například hledá-li osoba vážnou hudbu, reklama nabídne vážnou hudbu.

Cookies mohou být z počítače vymazány, nebo webový prohlížeč lze nastavit tak, aby je neukládal. (Brain, 2014)

7.5 Uživatelské chyby při užití programu Tor

Zjednodušeně řečeno má Tor[47] pomoci uživateli zůstat v anonymitě při využívání služeb Internetu (webové stránky, komunikace či obcházení blokovaných služeb poskytovatelem Internetu).

To je možné pouze za předpokladu správného zacházení se službou Tor. Pracuje tím způsobem, že uživatelův Tor klient vybere náhodně několik uzlů ze sítě Tor

[46] Slouží především vývojářům webových stránek. Na základě identifikace uživatele může pak být webová stránka modifikována podle jeho potřeb. Například zobrazení košíku s předměty v elektronickém obchodě, které si uživatel navolil by bez cookies nebo podobné technologie nebylo možné.

[47] Domovská stránka projektu Tor je www.torproject.org.

a vytvoří z nich komunikační obvod, přes který anonymně posílá všechna data. Po určitém čase nebo množství přenesených dat se komunikační obvod změní, aby byl uživatel prakticky nevystopovatelný.

Při sestavování komunikačního obvodu se používá vrstvené asymetrické šifrování vzdáleně připomínající strukturu cibule[48]. Jednotlivé uzly na cestě postupně dešifrují paket. Sloupnou jednu pomyslnou slupku cibulového paketu a přečtou následující adresu, na kterou mají paket předat. Trasa je klientem na uživatelském stroji dopředu naplánovaná. Instrukce o následujícím skoku paketu zná pouze uzel, kterého se přeposlání týká. (Winter, 2013)

Počítače zapojené do sítě projektu Tor se dělí na tři druhy serverů. Jsou to vlastně virtuální nody (onion routery) sdílející mezi sebou veřejné asymetrické šifrovací klíče[49] všech ostatních nodů v síti:

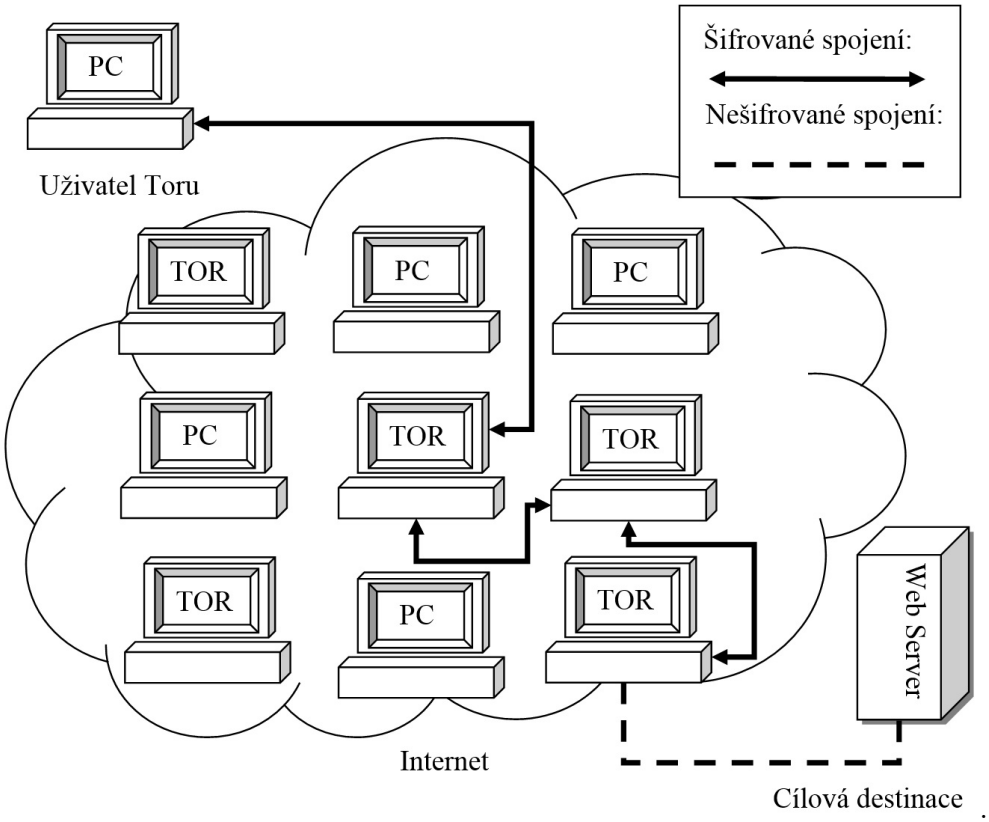
- Prostředník (middle relay) – data putují skrze klientský software Tor náhodně vybranými prostředníky. Odchozí komunikace ze sítě Tor skrz prostředníka je zcela zakázaná. Prostředník je de facto uzel, který neakceptuje odchozí požadavky. Každý z nich zná pouze svého předchůdce a následníka.
- Výstupní uzel (exit relay) – je naopak na hranici sítě Tor s Internetem a zprostředkovává výstupní komunikaci, která již není v rámci sítě Tor šifrována. Výstupní uzel totiž může být v útočníkovo držení a zároveň zaznamenávat každý bit procházející informace. Tento fakt je velmi důležité si uvědomit, jedná se zřejmě o největší zranitelnost celého procesu komunikace v této anonymní síti. Počítač cílového uživatele (nebo internetové služby) předpokládá, že je v přímém spojení s uživatelem Toru. Ve skutečnosti je v přímém spojení s výstupním uzlem, který se vydává za původce komunikace a dále ji jenom zprostředkovává. Jelikož výstupní uzel může být použit kýmkoliv na libovolnou činnost, dokonce i nezákonnou, tak se vystavuje jeho provozovatel možným problémům se zákonem.
- Most (bridge relay) – po spuštění jednoho ze dvou předchozích variant Tor serverů se přidá jejich adresa do veřejného seznamu serverů. Proto je k dispozici i neveřejná varianta serveru most, která v těchto seznamech zařazená není. To umožní použití v místech, kde je Tor blokován. Například místní vládou nebo někým jiným.

Celá struktura je pak složena ze všech klientských software na straně uživatelů poskytujících dobrovolně svoji konektivitu. Tato volitelná možnost umožňuje celému konceptu fungovat, protože přes tyto dobrovolníky prochází šifrovaně komunikace. Zabraňuje se tím vystopování původní IP adresy uživatele.

I když se zdá být koncept Toru slušně promyšlen a zabezpečen, existuje velké množství útoků, které ho mohou ohrozit. Ať už je to například z pohledu konstrukč-

[48]Odtud také vznikl název The Onion Routing neboli cibulové směrování.

[49]Podrobné informace o principu certifikátů, asymetrického a symetrického šifrování lze nastudovat z (Dostálek, 2006).



Obrázek 9: Schématické znázornění komunikace uživatele využívající síť Toru.

ního návrhu nebo vyžití neznalosti jeho uživatelů. Přesto na provedení úspěšného útoku je potřeba profesionálních znalostí a značného technického zázemí. Tyto útoky jsou nad rámec běžného uživatele a nebudou v této práci zmiňovány na rozdíl od využití chyb uživatele:

- Otevírání dokumentů online – tvůrci Tor varují před automatickým otevřením stažených dokumentů, které jsou zpracovávány externí aplikací. Speciálně je upozorňováno na typy souborů DOC a PDF. Dokumenty obsahují zdroje, které by se mohly stáhnout mimo síť Tor a odhalit tak pravou IP adresu uživatele. Doporučuje se tyto dokumenty prohlížet na odpojeném počítači.
- Tor Browser Bundle – internetová komunikace je chráněna pouze pokud je klientská aplikace správně nastavená. V opačném případě může komunikovat mimo zabezpečenou síť, která by pak tímto ztratila úplně smysl. Zároveň také může sama vyzradit citlivé údaje, které by mohly vést k odhalení totožnosti. Proto je doporučeno používat oficiální předkonfigurovaný prohlížeč Tor Browser Bundle, kde téměř nehrozí, že by byl uživatel odhalen například aktivovaným pluginem jako je Flash, RealPlayer, Quicktime a dalšími. Samozřejmostí je používat tento prohlížeč pouze v síti Tor.

- Chování uživatele – sám uživatel se může dopustit očividných primitivních chyb jako třeba podepsání svého příspěvku nebo specifický styl psaní, který je možné porovnat s dřívějšími příspěvky a zjistit IP adresu z dob kdy nebyl ještě Tor uživatelem používán.
- Kombinace účtů – používání nových anonymních účtů různých služeb a zároveň kombinované využívání uživatelských běžných neanonymních účtů. (Miller, 2014)

Tor zajistí anonymitu na Internetu, ale nikoliv na lokální síti. Administrátor lokální sítě (nebo poskytovatel Internetu) nedokáže zjistit, která místa na Internetu uživatel navštěvuje, ale ví, že je na počítači použit Tor. Nejvhodnější opatření je používat Tor na veřejných přístupových bodech k Internetu (free Wi-Fi sítě, internetové kavárny a další).

Je důležité zmínit, že Tor se zaměřuje především na poskytnutí anonymity, ale příliš neřeší bezpečnost. Uživatel je vystaven hrozbám spojeným s výstupními uzly. Ty totiž mají kontrolu nad výstupní komunikací. Mohou tedy uživatele šmírovat a realizovat různé útoky s mužem uprostřed.

7.6 Neanonymní vyhledávače

Současné nejrozšířenější internetové vyhledávače (Google, Bing a Yahoo) zaznamenávají historii vyhledávání uživatele. Následně tyto záznamy používají kromě vylepšování vyhledávače samotného k vytvoření určitého profilu uživatele a jeho zájmů. Pokud uživatel přistupuje na internetové stránky skrz vyhledávače, tak je zároveň poskytnut dané stránce i výraz, kterým uživatel stránku vyhledal. (Wawro, 2013)

Data, která shromažďuje o uživatelích společnost Google se sloučí i s ostatními používanými službami, jako například vyhledávání v mapových podkladech Google Maps, nebo informacemi získanými z emailového klienta Gmail. Tím může vzniknout této společnosti slušný obraz o osobnosti uživatele, se kterým může dále pracovat například v oblasti cílení reklamy. (Schenker, 2015)

Alternativa zohledňující soukromí uživatele je vyhledávač DuckDuckGo, který neuchovává o uživateli žádné informace a rovněž je neposkytuje žádné třetí straně. (Wawro, 2013)

8 Tvorba bezpečnostní aplikace

Hlavním cílem praktické části této práce je navrhnout a implementovat aplikaci, která uživateli umožní snadným způsobem nakonfigurovat vybraný operační systém a dosáhnout tak značného posílení v zabezpečení systému. Aplikace bude vytvořena především s důrazem na uživatelsky jednoduché a přívětivé grafické rozhraní. Jednotlivá bezpečnostní opatření budou vybrána v závislosti na dostupných možnostech a potřebách konkrétního operačního systému. Jako základ poslouží provedená analýza v teoretické části této práce, ve které byly popsány hlavní aktuální bezpečnostní problémy spojené s užitím osobního počítače.

Spuštění samotné aplikace probíhá jednoduše pomocí terminálu přímo z prostředí složky UbuntuS, ve které se použije příkaz **sudo bash startUbuntuS**. Systém požádá uživatele o vložení administrátorského hesla, které se potvrdí klávesou Enter. Následně se spustí samotná aplikace s grafickým prostředím. Není tedy třeba ze strany uživatele nic instalovat ani nastavovat.

Jediným předpokladem této aplikace je vytvořený uživatelský profil[50] v internetovém prohlížeči Firefox. V opačném případě budou všechny instalace týkající se tohoto prohlížeče přeskakovány, dokud nebude profil vytvořen. Výslednou aplikaci bylo nutné také otestovat pro ujištění, zda všechny její komponenty pracují správně.

8.1 Použité nástroje a technologie

8.1.1 Operační systém Linux

Na základě konzultace s vedoucím této práce byl vybrán operační systém Linux. Jelikož se tato práce zaměřuje především na uživatele, kteří mají aktivní zájem o informační bezpečnost, je zde předpoklad, že budou ochotni použít tento méně rozšířený systém, mezi jehož přednosti patří především bezpečnost.

Linux zvládá prakticky všechny činnosti, které by mohl běžný uživatel od operačního systému vyžadovat. Významným omezením je pouze podpora počítačových her. V této oblasti dominuje dlouhodobě systém Microsoft Windows.

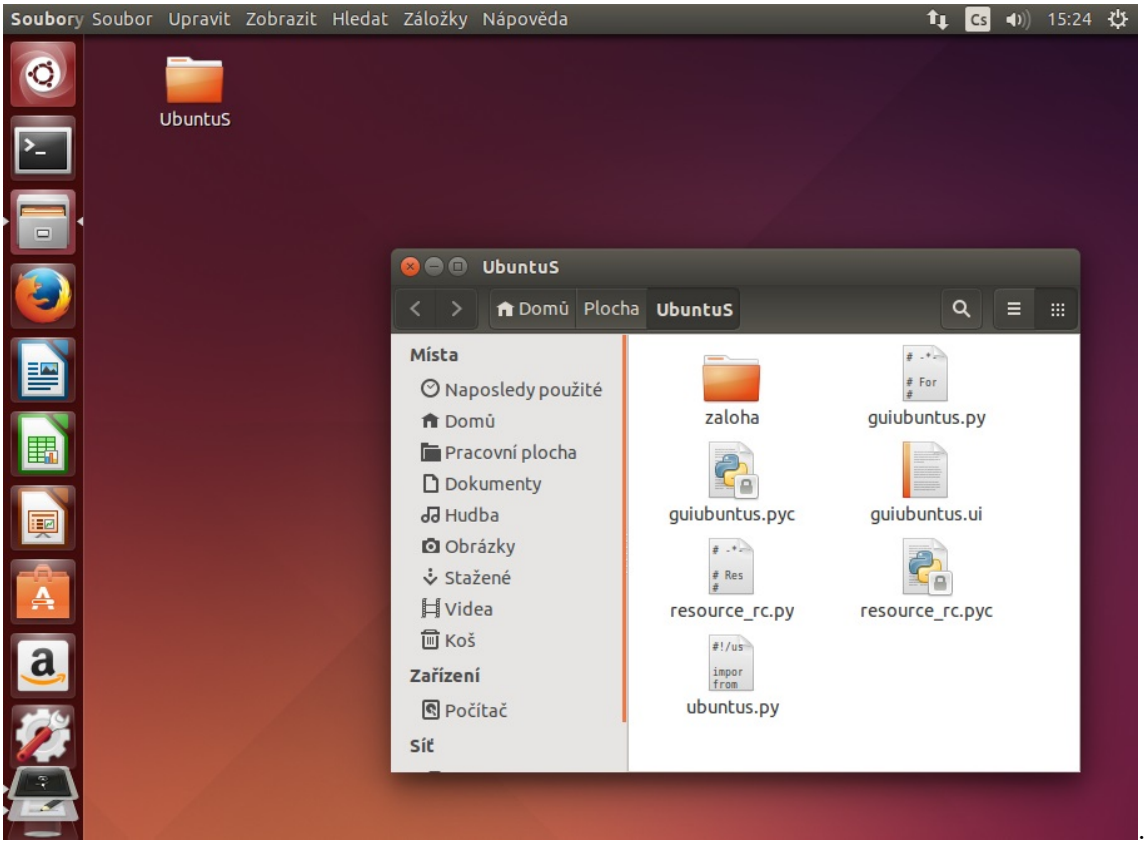
Pro současné počítače není problém mít nainstalováno zároveň několik operačních systémů. Proto je možné tento systém používat například jako doplněk v případě specifických bezpečnostních požadavků (prohlížení rizikových internetových stránek, internetové bankovnictví, otevírání emailových příloh a podobně).

Linux jako takový představuje pouze jádro operačního systému. Proto, aby bylo možné používat počítač s Linuxem je potřeba doplnit jádro o další programy. Soubor různě předpřipravených programů zakomponovaných a odladěných do jednoho celku se nazývá Linuxová distribuce.

[50] Uživatelský profil se automaticky vytvoří při prvním spuštění prohlížeče Mozilla Firefox.

8.1.2 Linuxová distribuce Ubuntu

V souladu se zamýšlenou filozofií bezpečnostní aplikace byla vybrána moderní linuxová distribuce Ubuntu 14.04 LTS (vydaná v dubnu 2014) s grafickým rozhraním. Jedná se o oblíbenou verzi s dlouhodobou podporou 5 let (Long Term Support) přeloženou do 25 jazyků, včetně češtiny. Je k dispozici ke stažení zdarma na internetových stránkách www.unbuntu.cz, bez nutnosti platit licenční poplatky. Standardní instalace probíhá pomocí přehledného grafické průvodce a neměla by trvat déle než 25 minut.



Obrázek 10: Prostředí linuxové distribuce Ubuntu 14.04 LTS.

Od základu je systém Ubuntu navržen s ohledem na bezpečnost, díky čemuž se minimalizuje riziko zavirování nebo jiného narušení počítače. Zároveň je systém svižný, jednoduchý a má k dispozici vše, co je k běžné práci potřeba. Proto je také tato distribuce doporučována jako vhodný kandidát při přechodu z jiných operačních systémů. Pokud by nastal nějaký problém s Ubuntu, jeho velkým kladem je početná uživatelská základna ochotná pomoci[51]. Na obrázku číslo 10 je k nahlédnutí grafické prostředí tohoto operačního systému, které je k uživateli přívětivé a přehledné.

[51]Například české fórum zabývající se systémem Ubuntu dostupné na http://forum.ubuntu.cz/.

Ubuntu je koncipováno tak, aby bylo co nejsnadněji použitelné a atraktivní pro běžného uživatele. Bezpečnostní aplikace se tedy velmi hodí do tohoto prostředí, protože se podobným způsobem snaží uživateli pomoci v otázce zabezpečení.

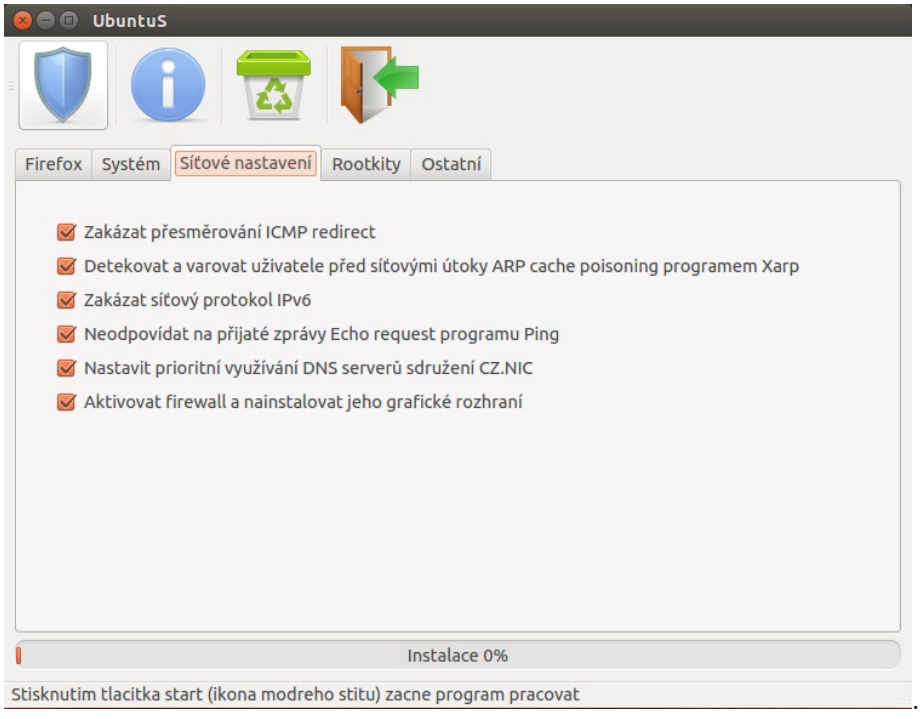
8.1.3 Programovací jazyk Python

K naprogramování vlastní aplikace byl použit programovací jazyk Python (verze 2.7), který je přítomen v základní instalaci linuxové distribuce Ubuntu a je okamžitě připraven k použití. Python je interpretovaný, objektově orientovaný jazyk s podporou mnoha modulů, který lze použít na celé řadě platforem. Základním rysem Pythonu je snadná čitelnost programového kódu a jeho kratší a rychlejší zápis v porovnání s ostatními jazyky (C++ nebo Java).

Součástí jazyka Python je balíček subprocess, který umožňuje komunikovat s příkazovým řádkem Linuxu a spouštět požadované příkazy z prostředí tohoto jazyka.

Programování aplikace probíhalo přímo v Ubuntu s využitím vývojového prostředí Komodo Edit, které je volně stažitelné[52]. Prostředí je přehledné a programování ulehčuje inteligentním zvýrazňováním a našeptáváním syntaxe.

8.1.4 Grafické rozhraní PyQt4



Obrázek 11: Grafické rozhraní, které bylo vytvořené pro bezpečnostní aplikaci UbuntuS.

[52]Například přímo ze stránek vývojářů www.komodoide.com.

Z důvodů minimalizace uživatelských kroků nutných pro spuštění bezpečnostní aplikace, bylo zvoleno grafické rozhraní knihovny PyQt4, které se již nachází v základní instalaci linuxové distribuce Ubuntu a není tak třeba ji doinstalovávat.

Pro vytvoření grafického návrhu byla použita aplikace Qt designer, která je volně k dispozici v repozitářích Ubuntu. Samotná bezpečnostní aplikace UbuntuS je vzhledově přizpůsobená danému prostředí a vypadá jako nativní aplikace operačního systému. Grafická podoba spuštěné aplikace UbuntuS je vidět na obrázku 11.

8.2 Vlastnosti aplikace

- Záloha nastavení – aplikace v případě všech zásahů do konfigurace systému provádí zálohu celých konfiguračních souborů, pro případ, že by došlo k problému. Záložní soubory jsou tedy připraveny pro případ obnovy.
- Jednoduché ovládání – ovládání aplikace bylo zjednodušeno pouze na výběr požadovaných možností zabezpečení a stisknutí jediného tlačítka start s ikonou štítu (kdy dojde k plně automatické instalaci). K dispozici je také možnost odinstalace (ikona odpadkového koše) jednotlivých částí pro uvedení systému do původního stavu. Během instalace není třeba žádný zásah uživatele. Průběh instalace je graficky zobrazován ve spodní části aplikace a vše je plně zautomatizováno. Nápověda pro jednotlivé položky z různých kategorií je zobrazena po stisknutí informační ikony.
- Signalizace nainstalovaných částí – pokud byly některé položky (nebo všechny) již nainstalovány, zobrazí se vedle jednotlivých zaškrtávacích boxů zelená ikona ve tvaru fajfky při každém spuštění aplikace. Po provedené odinstalaci se zobrazí červený křížek. Aplikace také umožňuje opětovnou reinstalaci podle potřeby uživatele.
- Aktualizace – bezpečnostní aplikace řeší aktualizace nastavením jednotlivých vybraných možností tak, aby je v závislosti na konkrétním případě dále spravoval operační systém, webový prohlížeč či přímo nainstalovaný program.
- Protokol instalace – zaznamenávány jsou všechny informace zobrazené v terminálu včetně chybových hlášení. Konkrétně se jedná o textový soubor (log.txt), který je uchováván pro pozdější možné nahlédnutí. Nachází se ve složce spolu s bezpečnostní aplikací.
- Automatické spuštění – jednotlivé kontroly nainstalovaných bezpečnostních nástrojů jsou automaticky spouštěné v pravidelných intervalech po několika startech operačního systému. Uživatel nemusí sám plánovat jednotlivé kontroly a ani ho nebudou vyrušovat v průběhu jeho práce. Úmyslně jsou proto všechny kontroly spouštěny po startu systému. V případě, že se daná kontrola zrovna z nějakého důvodu nehodí, jednoduše ji uživatel ukončí zavřením konkrétního

okna. Monitorovací nástroje se úmyslně spouští v minimalizovaném stavu, tak aby nebyl uživatel zbytečně vyrušován.

8.3 Implementované možnosti bezpečnostní aplikace

Uživatel má v aplikaci na výběr z pěti tematicky rozdělených kategorií zabezpečení, mezi kterými je možné přepínat pomocí záložek zobrazených v horní části aplikace.

V Linuxu je realizována konfigurace systému a jednotlivých programů ve formě konfiguračních souborů. Jako základ bylo potřeba naprogramovat metodu, která se o tyto změny v souborech postará. Tato metoda musí nejprve ověřit, zda již není požadovaná konfigurace v souboru nastavena. Pokud ano, tak ji přepíše na požadovanou hodnotu. V opačném případě připíše záznam na konec souboru. Zároveň je potřeba rozlišit více příkazů na jedné řádce a v případě potřeby je od sebe oddělit.

8.3.1 Kategorie Firefox

V Ubuntu je nativně přítomen moderní webový prohlížeč Mozilla Firefox, který je již v základu připraven na každodenní použití. Je možné ho rozšiřovat o další funkcionalitu přidáním doplňků.

Aby mohla bezpečnostní aplikace automaticky přidávat různé doplňky pomocí skriptu, bylo nutné vytvořit metodu installFirefoxPlugin, která zajistí správné vložení konkrétního doplňku do prohlížeče. Nejprve se zjistí přesný název profilu uživatele[53] prohledáním souboru profiles.ini v adresáři Mozilly. Následuje stažení samotného doplňku z URL odkazu, který se předává jako vstupní parametr metodě installFirefoxPlugin. Aby prohlížeč začal doplněk používat, musí být uložen ve složce pojmenované přesně podle konkrétního identifikačního názvu doplňku, který se nachází v doprovodném instalačním souboru install.rdf (uvozený tagem a ukončený). Pro jeho nalezení byl vytvořen následující příkaz (obsahující regulární výrazy zadané programu sed):

```
unzip -p 'temp/addon.xpi' 'install.rdf' | grep '' | head -n '1'
    | sed -e   's/.*//' | sed -e 's/<\/em:id>.*//'
```

Poté je již možné rozbalit doplněk a přesně ho umístit do složky extensions, podle názvu uživatelského profilu. Prohlížeč bude daný doplněk při každém spuštění sám aktualizovat na nejnovější verzi. Aplikace umožňuje přidat tyto doplňky:

- DNSSEC Validátor – kontroluje zabezpečení doménového jména v adresním řádku DNSSEC protokolem. Uživatelé tak snadno poznají, zda byla stránka zobrazena z autentického zdroje, nebo zda stránka mohla být podvržena.
- Adblock Plus – automaticky nastavuje blokování reklam a známých domén se škodlivým software.

[53] Zjistit název profilu uživatele je nutné vždy, protože se může lišit v jednotlivých instalacích.

- WOT (Web of Trust) – služba zobrazuje hodnocení webových stránek v podobě ikony semaforu, vedle výsledků vyhledávání napomáhá při rozhodnutí, zda stránku navštívit či ne. Kliknutím na ikonu semaforu lze zobrazit detaily o hodnocení dané stránky včetně názorů ostatních uživatelů. Hodnocení a recenze na WOT pocházejí z globální komunity, která se skládá z milionů uživatelů hodnotících na základě svých osobních zkušeností.
- NoScript Security Suite – doplněk dovoluje spouštět skripty pouze na webových stránkách, které uživatel explicitně povolil.

Kromě přidání výše zmíněných doplňků umožňuje aplikace také přidat některé užitečné odkazy do lišty záložek, která snadno zpřístupňuje webové stránky. Záznam vytvářející záložky bylo nutné přidat přímo do lokální SQL databáze Mozilly prostřednictvím SQLite knihovny, která umožňuje s touto databází pracovat.

Soubor lokální databáze places.sqlite se nachází v adresáři s profilovými daty uživatele. Aby mohla být přidána nová záložka, musí nejprve existovat záznam o návštěvě této stránky. Ten je možné uměle přidat na konec tabulky s historií navštívených stránek nacházejícího se v souboru places.sqlite. Maximální identifikační číslo jednotlivých záznamů je vždy jiné, ale je možné ho zjistit pomocí metody fetchone(). Poté co je přidán záznam (prostřednictvím metody execute() a SQL příkazu INSERT INTO) o návštěvě konkrétní webové stránky, je možné na něj odkázat webovou záložku. Záložka se vytvoří formou záznamu v tabulce spravující záložky (s referencí na základě ID záznamu). Bezpečnostní aplikace umožňuje přidat odkazy na tyto webové stránky:

- Virusscan.jotti.org – online služba umožňující otestování jednotlivých souborů na přítomnost škodlivého software. Kontrolu provádí zároveň více jak 20 antivirových programů od různých firem. Výsledky kontroly jsou poté zhodnoceny každým antivirovým řešením individuálně.
- Hoax.cz – online databáze nejrozšířenějších podvodných emailů a poplašných zpráv v České republice.
- DuckDuckGo.com – alternativní internetový vyhledávač, který neshromažďuje a dále nevyužívá údaje o uživatelích. Taktéž žádným způsobem neupravuje výsledky vyhledávání v závislosti na konkrétním uživateli.

8.3.2 Kategorie Systém

Obecně je systém Ubuntu dobře nakonfigurován v oblasti zabezpečení. Přesto aplikace nabízí možnosti pro vylepšení tohoto stavu. A to zejména v oblasti konfigurace a přidání monitorovacího software.

První možnost dostupná v kategorii Systém je vypnutí rozhraní FireWire. Toho je možné docílit zakázáním nahrání ovladačů pro rozhraní FireWire. Aplikace tedy nastaví v konfiguračním souboru (/etc/modprobe.d/blacklist-firewire.conf)

programu modprobe (spravuje přidávání ovladačů do systému) tento zákaz odkomentováním předpřipravených příkazů pro zablokování FireWire.

Druhá položka aplikace zamezuje spouštění programového kódu ve sdílené paměti. Provádí se editací konfiguračního souboru (/etc/fstab), spravujícího připojené souborové systémy. Záznam o připojené sdílené paměti (run/shm) poté stačí obohatit o parametr noexec, který zamezí spouštění programového kódu z této oblasti:

```
none     /run/shm     tmpfs     rw,noexec,nosuid,nodev
```

Třetí položka upravuje správce přihlášení LightDM. Ten umožňuje ve výchozím nastavení komukoliv se přihlásit k počítači pod uživatelským účtem Guest. Tento účet je možné vypnout v konfiguračním souboru správce přihlášení (/etc/lightdm/lightdm.conf) nastavením parametru allow-guest na hodnotu false.

Čtvrtá položka řeší aktualizace systému. Standardně se totiž stará o aktualizace systému Ubuntu sám uživatel. Pro zjednodušení práce je tuto důležitou a opomíjenou povinnost možné přenechat na starosti systému. Automatické stažení bezpečnostních záplat systému a jejich následná instalace se aktivuje provedením příslušných editací v konfiguračním souboru /etc/apt/apt.conf.d/10periodic na následující:

```
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::Unattended-Upgrade "1";
```

Aktualizace se kontrolují každý den. Pokud bude dostupná nějaká nová, tak se okamžitě o všechno postará systém sám a bez vyrušení uživatele. Tímto je udržován systém zabezpečený podle současných maximálních možností.

Poslední možností v kategorii Systém je instalace a nastavení monitorovacího software indicator-multiload, který uživateli dovoluje kontrolovat aktuální vytížení systémových zdrojů (CPU - vytížení, síť - komunikace, HDD - zápis). Tento software zobrazuje na hlavním panelu (vedle hodin) malé přehledné grafy s aktuálním vytížením jednotlivých zdrojů. Uživatel je pomocí těchto grafů schopen vizuálně rozpoznat podezřelou situaci v podobě nekorespondujících zátěží jednotlivých zdrojů s aktuální činností uživatele.

Program indicator-multiload byl nakonfigurován prostřednictvím programu gsettings[54], přes který je možné pomocí příkazů v skriptu editovat program indicator-multiload:

```
gsettings set de.mh21.indicator-multiload.general width 180;
gsettings set de.mh21.indicator-multiload.graphs.disk enabled true;
gsettings set de.mh21.indicator-multiload.graphs.net enabled true;
gsettings set de.mh21.indicator-multiload.general speed 1500;
gsettings set de.mh21.indicator-multiload.general
```

[54]Nástroj pro editaci databáze, která uchovává centrálně nastavení jednotlivých aplikací v systému Ubuntu. Zdaleka ne všechny aplikace si ukládají svá nastavení do této databáze, ale využívají i jiných způsobů.

```
    background-color traditional:background;
gsettings set de.mh21.indicator-multiload.traces.net1
    color traditional:load1;
gsettings set de.mh21.indicator-multiload.traces.net2
    color traditional:load1;
```

Kromě již v základu se zobrazujícího grafu CPU, byly přidány i grafy vytížení sítě a HDD. Dále byla upravena jejich velikost, barevné podání a rychlost obnovování grafů. Nakonec bezpečnostní aplikace nastaví automatické spouštění programu indicator-multiload po startu systému.

8.3.3 Kategorie Síťové nastavení

V kategorii Síťového nastavení je možné posílit ochranu počítače proti síťovým útokům. Opatření v této kategorii jsou užitečným doplňkem z pohledu koncového počítače a přispívají k ostatním bezpečnostním opatřením celé sítě.

První možností je vypnutí přesměrování pomocí paketu ICMP redirect. To se provede v konfiguračním souboru /etc/sysctl.conf změnou nastavení následujících proměnných na nulu:

```
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
```

Po nastavení změn a spuštění programu sysctl (načte a modifikuje jádro Linuxu podle aktuálního nastavení), nebude již daný systém reagovat na výzvy o přesměrování paketů prostřednictvím protokolu ICMP.

Aplikace dále nabízí ochranu před útoky na bázi ARP protokolu. A to konkrétně nainstalováním, konfigurací a následným automatickým spouštěním volně dostupného programu XArp, který běží neustále v pozadí. Tento program v případě detekce útoku okamžitě upozorní uživatele zobrazením varující hlášky (podobně jako Antivirus při detekci škodlivého software).

Protože se XArp nenachází v základním repozitáři Ubuntu je stáhnut z webových stránek (www.xarp.net) vývojáře. K dispozici jsou 32 a 64 bitové verze. Pro určení konkrétní architektury, na které je bezpečnostní aplikace spuštěna, byl použit modul Pythonu platform. Tento modul získává různé informace a parametry hostitelského systému. Mezi nimi jsou i podrobnosti o architektuře, na základě kterých se vybere verze programu XArp odpovídající hostitelskému systému.

Následujícím příkazem se ještě před samotnou instalací stáhnou programové balíčky nutné ke spuštění programu XArp:

```
sudo apt-get install libwxgtk2.8-0 libxerces-c3.1 libpcap0.8
    libc6 menu arptables
```

Po instalaci těchto závislostí následuje již samotná instalace programu XArp a to instalačním programem dpkg, který provádí nízkoúrovňové operace nad celým balíkovacím systémem.

Program XArp vyžaduje ke své práci administrátorské oprávnění. Aby bylo možné program samovolně spouštět po startu systému (bez nutnosti zadávání hesla), byl vytvořen soubor /etc/sudoers.d/xarp. Do tohoto souboru se vloží následující záznam, který povolí spouštět (prostřednictvím příkazu sudo) program XArp bez zadávání hesla:

```
ALL ALL = (root) NOPASSWD: /usr/bin/xarp
```

Při startu systému je pak nastaveno automatické spuštění XArp s parametrem hide, který provede minimalizovaný start programu (kvůli komfortu uživatele).

V kategorii Síťové nastavení si uživatel může dále navolit, zda mít aktivní podporu protokolu IPv6. Aplikace ji umožňuje vypnout konfigurací souboru /etc/sysctl.conf a přidáním následujících záznamů:

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

Po nastavení změn a následném spuštění programu sysctl, nebude operační systém tento protokol využívat.

Aplikace také umožňuje vypnout odpovídání na požadavky potvrzení dostupnosti, přijaté z jiného počítače prostřednictvím počítačové sítě (například zaslané programem ping). To se provede v konfiguračním souboru /etc/sysctl.conf změnou nastavení následující proměnné na jedničku:

```
net.ipv4.icmp_echo_ignore_all = 1
```

Předposlední nabízenou možností je, že uživatel nemusí spoléhat na DNS server místního poskytovatele připojení a může místo něj prioritně využívat zabezpečený a spolehlivý DNS server bezpečnostního týmu CSIRT.CZ[55]. Nastavení IP adres DNS serverů, které obyčejně přiděluje DHCP server se upravuje v souboru /etc/dhcp/dhclient.conf následující změnou:

```
prepend domain-name-servers 217.31.204.130;
```

Dále je potřeba vědět, že ve výchozím nastavení Ubuntu je vypnutý firewall a není pro něj nainstalované grafické rozhraní. Protože je firewall důležitým prvkem počítačové bezpečnosti (dohlíží a reguluje tok dat oběma směry komunikace), tak

[55]Na základě dohody mezi Ministerstvem vnitra České republiky a sdružením CZ.NIC provozuje správce domény .CZ bezpečnostní tým CSIRT.CZ. Ten se jako národní tým podílí na řešení incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice.

je zde implementovaná možnost ho aktivovat. S aktivací bude i následně doinstalována jednoduchá a přehledná grafická nadstavba k firewallu gufw a to následujícími příkazy:

```
sudo apt-get install -y gufw
sudo ufw enable
```

Jakmile bude firewall aktivovaný, bude se již nadále spouštět automaticky. Uživatel bude moci v případě potřeby jednoduše přidávat (prostřednictvím nastavení systému Ubuntu) vlastní pravidla.

8.3.4 Kategorie Rootkity

Tato kategorie obsahuje nástroje pro detekci rootkitů a jiných nežádoucích nástrojů. K dispozici na instalaci jsou programy rkhunter a chkrootkit, které se vzájemně doplňují. Oba programy při svém spuštění analyzují a porovnávají své databáze jim známých rootkitů se spuštěnými procesy, systémovými programy a skrytými soubory na daném systému. Zde pak hledají nesrovnalosti a podezřelé chování. Nutno podotknout, že tyto programy provádí pouze detekci. Následná akce je pak na uživateli. Před každou kontrolou je nastaveno stáhnutí nejnovější databáze s informacemi o rootkitech. Dále je možné doinstalovat program unhide, který rozšiřuje rozsah detekce o skryté otevřené síťové porty, přes které by mohla vést neoprávněně komunikace.

Protože je nutné spouštět tyto programy pravidelně, bylo nastaveno automatické spouštění kontroly po startu systému. Obyčejně je nastavené hlášení problému zasláním emailu, které se spíše hodí pro server. Aplikace proto po startu nastaví spuštění interpretu příkazového řádku, ve kterém je dobře viditelná aktuální činnost těchto programů. Výsledky jsou přehledně sumarizovány do výsledného reportu, kde uživatel okamžitě uvidí, zda programy našly nějaký problém.

8.3.5 Kategorie Ostatní

Jednou z dalších možných vrstev zabezpečení (které je vhodné aplikovat v systému Ubuntu) je software monitorující změnu integrity souborů. Hlavní účel takového monitoringu je ujištění, zda nebyly provedeny neautorizované změny systémových binárních souborů a konfigurace. Tato aplikace umožňuje nainstalovat program AIDE, který je volně dostupnou náhradou za známý nástroj Tripwire.

Po provedení instalace AIDE je potřeba tento program nakonfigurovat tak, aby byl uživatelsky více příjemný. V konfiguraci programu AIDE (/etc/default/aide) bylo proto vypnuto plánované spouštění programem cron[56], který pracuje pouze na pozadí systému. Bezpečnostní aplikace ji nahradí viditelnou kontrolou probíhající v terminálu po každém spuštění systému. Uživatel tak okamžitě uvidí přehledné výsledky.

[56]Nástroj pro administraci systému, který v operačních systémech automatizovaně spouští v určitý čas příkazy. V systému slouží jako plánovač úloh.

V základním nastavení AIDE se při kontrole na každém souboru aplikuje postupně řada hashovacích algoritmů (md5, sha1, rmd160, tiger, haval a další). To několikanásobně prodlužuje čas nutný k prozkoumání celého systému v porovnání při užití pouze jednoho algoritmu. Aplikace tedy nastaví v této situaci dostatečný algoritmus sha256, se kterým proběhne kontrola podstatně rychleji.

Aby program AIDE mohl při dalším spuštění systému ihned pracovat, bylo potřeba vytvořit jeho počáteční databázi až úplně nakonec, po provedení všech ostatních úprav této aplikace. V opačném případě by program AIDE rovnou hlásil všechny provedené změny.

Z důvodu pohodlí uživatele byl vyjmut z oblasti kontroly uživatelský adresář. Program AIDE by hlásil mnoho změn, což by mohlo v konečném důsledku uživatele od kontroly odradit.

Poslední možností v této kategorii je instalace programu Wipe, který umožňuje důkladně smazat soubory. Lze tak učinit jednoduše z kontextové nabídky, vyvolané pravým tlačítkem myši.

9 Zhodnocení a diskuse

9.1 Zhodnocení implementace

Konfigurační změny a instalace, které provádí aplikace UbuntuS, se rozdělují do pěti hlavních skupin (Firefox, Systém, Síťové nastavení, Rootkity, Ostatní), z nichž je možné uživatelsky navolit konkrétní požadovaná opatření. Tato opatření vhodně posilují základní přednastavenou úroveň zabezpečení systému v potencionálně slabších místech. Veškeré ovládání je prováděno prostřednictvím vytvořeného grafického rozhraní.

Předinstalovaný prohlížeč Firefox může být rozšířen různými doplňky (kontrola DNS, zakázání skriptů, zobrazení hodnocení stránek atd.), které navyšují bezpečnost při surfování po webových stránkách. Také je umožněno přidat několik záložek s odkazy na vybrané webové stránky (kontrola škodlivých souborů, falešných zpráv a podobně). Dále jsou instalovány a konfigurovány nástroje pro detekci nakažení systému (kontroly integrity, vyhledávání rootkitů a skrytých otevřených portů) nebo síťovým útokům. Přidány byly také nástroje pro důkladné mazání souborů a monitoring systémových prostředků (CPU, HDD, síťové rozhraní). V neposlední řadě je možné provádět změny konfigurace samotného systému Ubuntu. Například je k dispozici zakázání Guest účtu, vypnutí přesměrovávání paketů pomocí ICMP protokolu, neodpovídání na požadavky ping, zákaz rozhraní Firewire a podobně.

Mnoho konfiguračních změn, které provádí aplikace UbuntuS, je primárně uzpůsobeno na ovládání přes grafické prostředí jednotlivých programů. Proto i většina autorů různých dokumentací a návodů počítá s tím, že uživatel veškeré změny provede sám (prostřednictvím myši a grafického rozhraní daného programu). To představovalo komplikaci v implementaci této aplikace, protože bylo potřeba zasahovat do různých nízkoúrovňových databází a jiných podrobných nastavení. Taktéž spolupráce Pythonu a interpretu příkazového řádku nebyla zcela bezproblémová.

Přesto se povedlo naprogramovat užitečnou aplikaci, která výrazně zkrátí uživateli nutný čas pro dodatečné zabezpečení daného systému. Mnohá detailní nastavení by jinak bylo nutné podrobně nastudovat v příslušných anglicky psaných manuálech. Zároveň by bylo třeba k nim vyhledávat odpovídající konfigurační soubory, protože ne všechna nastavení je umožněno spravovat prostřednictvím grafického rozhraní (podobně jako je tomu například u systému Windows a jejich systémových registrů).

9.2 Srovnání s existujícími řešeními

Nejvíce podobný nástroj k porovnání s aplikací této práce je zřejmě Bastille[57]. Nástroj pokládá otázky, na které uživatel odpovídá stylem ano/ne. Na základě odpovědí je pak přistoupeno k opatřením založených na těchto otázkách. Mezi výhody patří:

[57] http://bastille-linux.sourceforge.net/index.html

- Bastille je dostupná pro většinu významných linuxových distribucí. Aplikace UbuntuS z této práce je přesně přizpůsobená a zaměřená na jediný operační systém.
- Bastille se určitým způsobem snaží uživatele zasvětit do problematiky.

Nevýhody Bastille pro běžného uživatele spočívají hlavně v odlišném zaměření:

- Většina nabízených bezpečnostních opatření je vhodná spíše pro servery a stanice na, kterých pracuje více uživatelů.
- K dispozici není čeština.
- Pracuje pouze s konfigurací operačního systému. Nepomáhá s instalací dalších podpůrných software.

9.3 Diskuse

Snahou autora této diplomové práce bylo přinést běžným uživatelům počítačů užitečné a aktuální informace o bezpečnosti, protože mnoho knih věnovaných bezpečnosti se spíše zabývá pohledem z hlediska firem a vytváření jejich bezpečnostní politiky. Informace dostupné na Internetu pro běžné uživatele jsou často v podobě rozkouskovaných článků, zaměřující se vždy pouze na určitou část problematiky.

Bylo potřeba prostudovat velké množství témat a zhodnotit jestli jsou z dnešního pohledu stále aktuální nebo zda skutečně představují určitou hrozbu, která by měla být zmíněna.

Protože informační bezpečnost je rozsáhlé a komplexní téma, tak struktura práce není vždy ideální. Jednotlivé části práce občas spadaly zároveň do více kategorií a to v závislosti na úhlu pohledu.

Jistou odměnou pro autora bylo zjištění, že v průběhu psaní této práce se našli lidé, kteří sami od sebe požádali o zaslání kopie tohoto textu, protože měli o avizované informace zájem.

Alternativou k vytvořené aplikaci UbuntuS, by mohla být naprogramována obdobná aplikace zaměřující se na operační systém Windows, kterou by také jistě ocenilo mnoho uživatelů.

10 Závěr

Cílem diplomové práce bylo podat přehled o aktuální problematice počítačové bezpečnosti a ochraně soukromí. Téma počítačové bezpečnosti patří určitě mezi nejdůležitější témata naší doby. Zatímco před dvaceti až třiceti lety považovala většina lidí počítač maximálně za dobrou hračku či lepší psací stroj, tak v současné době to jsou již nenahraditelní pomocníci zastoupení téměř ve všech oblastech života. S tímto faktem je třeba počítat, protože při podcenění zabezpečení počítačů hrozí velmi reálné a nezanedbatelné škody.

Tato práce se soustředila na zabezpečení počítače z pohledu běžného uživatele jakožto administrátora svého vlastního operačního systému. Byly v ní popsány zásadní bezpečnostní problémy, které souvisí s osobním počítačem a používáním jeho programového vybavení. Jednotlivé problémy byly vysvětleny včetně teoretických principů důležitých pro jejich správné pochopení. Zároveň byl čtenář seznámen s existencí celé řady volně dostupných útočných nástrojů a jejich praktických možností, které jsou uzpůsobené pro snadné provedení různých útoků.

Zdaleka ne všechny problémy, ale leží pouze v oblasti nastavení systému a jeho zabezpečení, proto je v práci také věnována pozornost uživatelským chybám, které je možné nějakým způsobem využít. Znalosti nejrůznějších podvodů, zranitelností a útoků totiž často společně s trochou obezřetnosti rozhodnou o výsledku úrovně zabezpečení.

Praktická část práce se věnovala vývoji aplikace, která umožní uživateli jednoduchým způsobem nakonfigurovat počítač, aby vyhovoval zvýšeným bezpečnostním nárokům. Důraz byl kladen především na jednoduchost a výběr vhodných bezpečnostních opatření, která uživatele příliš neobtěžují. V opačném případě by mohla být tato snaha kontraproduktivní a uživatele odradit.

Závěrem lze říci, že bylo dosaženo požadovaného výsledku v podobě praktické a funkční aplikace, která po stisknutí jediného tlačítka automaticky nakonfiguruje a nainstaluje uživatelem vybraná bezpečnostní opatření. Další velkou výhodou je, že veškerá opatření, použité nástroje a dokonce i samotný operační systém jsou dostupné zdarma a nic tak nebrání k jejich vyzkoušení.

11 Literatura

Bašta, P. *Role uživatelů při boji s kybernetickými útoky.* [online]. 2013 [cit. 2014-12-17]. Dostupné z: http://www.root.cz/clanky/role-uzivatelu-pri-boji-s-kybernetickymi-utoky/.

Brady, P. *Cross-Site Scripting (XSS).* [online]. 2014 [cit. 2015-04-26]. Dostupné z: http://phpsecurity.readthedocs.org/en/latest/Cross-Site-Scripting-(XSS).html/.

Brain, M. *How Internet Cookies Work.* In: [online]. 2014 [cit. 2014-12-21]. Dostupné z: http://computer.howstuffworks.com/cookie3.htm.

Beal, V. *The Difference Between Adware Spyware.* [online]. 2013. vyd. [cit. 2015-03-21]. Dostupné z: http://www.webopedia.com/DidYouKnow/Internet/spyware.asp/.

Celetka, O. *Mitmproxy: útok na šifrované spojení snadno a rychle.* [online]. 2015 [cit. 2015-02-14]. Dostupné z: http://www.root.cz/clanky/mitmproxy-utok-na-sifrovane-spojeni-snadno-a-rychle/.

Clark, J. *Admins warned: Drill SSL knowledge into your Chrome users.* [online]. 2013 [cit. 2014-12-20]. Dostupné z: http://www.theregister.co.uk/2013/08/10/chrome_ssl_clickthrough_report.

Česká republika *Zákon trestní zákoník.* In: http://www.psp.cz/sqw/sbirka.sqw?o=5&t=410. 2009/.

Čížek, J. *Eset: Zákeřný TorrentLocker útočil i na Česko. Mnozí zaplatili výkupné.* [online]. 2014 [cit. 2015-04-26]. Dostupné z:http://www.zive.cz/bleskovky/eset-zakerny-torrentlocker-utocil-i-na-cesko-mnozi-zaplatili-vykupne/sc-4-a-176532/default.aspx/.

Co je to phishing?. *Hoax.cz* In: [online]. Hoax.cz, 2014 [cit. 2014-12-20]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing/.

DeLeeuw, S. *How To Crack WPA / WPA2.* [online]. 2012 [cit. 2015-03-18]. Dostupné z:http://www.smallnetbuilder.com/wireless/wireless-howto/31914-how-to-crack-wpa-wpa2-2012?start=2/.

Demarest, J. *FBI's Cyber Criminal Strategy.* [online]. 2014 [cit. 2015-04-26]. Dostupné z:http://www.fbi.gov/news/testimony/taking-down-botnets.

Doseděl, T. *Počítačová bezpečnost a ochrana dat.* 1. vyd. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

Dostálek, L., Kabelová, A. *Velký průvodce protokoly TCP/IP a systémem DNS.* 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.

Dostálek, L., Vohnoutová, M., Knotek, M. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu.* 2., aktualiz. vyd. Brno: Computer Press, 2009, 542 s. ISBN 978-80-251-2619-6.

Dougbert *BIOS Password Backdoors in Laptops.* [online]. 2009 [cit. 2014-12-15]. Dostupné z: http://dogber1.blogspot.cz/2009/05/table-of-reverse-engineered-bios.html/.

Erben, L. *Příchod hackerů: ransomware.* In: [online]. 2014 [cit. 2014-12-21]. Dostupné z: http://www.root.cz/clanky/prichod-hackeru-ransomware/.

Fisher, D. *What is a Botnet?* Kaspersky, 2013 [cit. 2014-12-08]. Dostupné z: http://blog.kaspersky.com/botnet/.

Golovanov, S. *Bootkit: the challenge of 2008.* [online]. 2008 [cit. 2014-12-14]. Dostupné z: http://securelist.com/analysis/publications/36235/bootkit-the-challenge-of-2008/.

Goldman, J. *Hackers Stole 2 Million Customer Records Per Day in Q2 2014.* [online]. 2014 [cit. 2014-12-20]. Dostupné z: http://www.esecurityplanet.com/hackers/hackers-stole-2-million-customer-records-per-day-in-q2-2014.html/.

Goodin, D. *25-GPU cluster cracks every standard Windows password in <6 hours.* [online]. 2012 [cit. 2014-12-14]. Dostupné z: http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/.

Hanáček, P., Staudek, J. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií.* Praha: Úřad pro státní informační systém, 2000, 127 s. ISBN 80-238-5400-3.

Harris, S., Harper, A., Eagle, Ch. *Hacking: manuál hackera.* 1. vyd. Praha: Grada, 2008, 399 s. ISBN 978-80-247-1346-5.

Hatch, B. *Hacking exposed Linux: Linux security secrets.* 3rd ed. New York: McGraw-Hill, c2008, xxxiii, 613 p. ISBN 00-722-6257-5.

Houser, P. *Hesla lze účinně lámat pomocí grafické karty.* [online]. 2010 [cit. 2014-12-09]. Dostupné z: http://computerworld.cz/securityworld/hesla-lze-ucinne-lamat-pomoci-graficke-karty-47666.

How to Hack Wi-Fi *Creating an Evil Twin Wireless Access Point to Eavesdrop on Data.* [online]. 2013 [cit. 2014-12-20]. Dostupné z: http://null-byte.wonderhowto.com/how-to/hack-wi-fi-creating-evil-twin-wireless-access-point-eavesdrop-data-0147919/.

Jirovský, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských ko-ních bez tajemství.* 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-

247-1561-2.

Kassner, M. *10+ things you should know about rootkits.* [online]. 2008 [cit. 2014-12-14]. Dostupné z: http://www.techrepublic.com/blog/10-things/10-plus-things-you-should-know-about-rootkits/.

Kümmel, R. *HW Keylogger: nejsnadnější způsob získání hesla.* [online]. 2015 [cit. 2015-03-18]. Dostupné z:http://www.soom.cz/clanky/1166–HW-Keylogger-nejsnadnejsi-zpusob-ziskani-hesla/.

Kümmel, R. *XSS: Cross-Site Scripting v praxi : o reálných zranitelnostech ve virtuálním světě.* Náchod: Nakladatelství Manuál, 1994.
ISBN 8090182402.

Kysela, J. *Malware a jeho současné podoby.* [online]. 2012 [cit. 2015-03-21]. Dostupné z: http://www.internetprovsechny.cz/malware-a-jeho-soucasne-podoby/.

Lanze, F., Panchenko, A., Ponce-Alcaide, I. *Undesired Relatives: Protection Mechanisms Against The Evil Twin Attack in IEEE 802.11.* [online]. 2014 [cit. 2015-02-14]. Dostupné z: http://lorre.uni.lu/ andriy/papers/Evil-Twin-Survey-Soft-AP-Q2SWinet2014.pdf/.

Maartmann-Moe, C. *Inception.* [online]. 2011 [cit. 2014-12-17]. Dostupné z: http://www.breaknenter.org/projects/inception/.

Maartmann-Moe, C. *Adventures with Daisy in Thunderbolt-DMA-land: Hacking Macs through the Thunderbolt interface.* [online]. 2012 [cit. 2014-12-17]. Dostupné z: http://www.breaknenter.org/2012/02/adventures-with-daisy-in-thunderbolt-dma-land-hacking-macs-through-the-thunderbolt-interface/.

Miller, T. *How Can I Stay Anonymous with Tor?* [online]. 2014 [cit. 2014-12-17]. Dostupné z: http://lifehacker.com/how-can-i-stay-anonymous-with-tor-1498876762.

Mims, Ch. *Moore's Law Over, Supercomputing In Triage.* [online]. 2012 [cit. 2014-12-14]. Dostupné z: http://www.technologyreview.com/view/427891/moores-law-over-supercomputing-in-triage-says-expert/.

Myers, L. *11 things you can do to protect against ransomware, including Cryptolocker.* [online]. 2013 [cit. 2015-04-26]. Dostupné z: http://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker/.

Nykodýmová, H. *Bojíte se krádeže své identity?* [online]. 2006 [cit. 2015-03-07]. Dostupné z: http://www.lupa.cz/clanky/bojite-se-kradeze-sve-identity/.

Nve, L. *New SSLstrip2 Version to Defeat HSTS.* [online]. 2014 [cit. 2015-02-14]. Dostupné z: http://www.n1tr0g3n.com/?p=6026/.

Pash, A. *How to Crack a Wi-Fi Network's WPA Password with Reaver.* [online]. 2012 [cit. 2015-02-18]. Dostupné z: http://lifehacker.com/5873407/how-to-crack-a-wi-fi-networks-wpa-password-with-reaver/.

Pepak, *Útoky na operační paměť.* [online]. 2012 [cit. 2014-12-17]. Dostupné z: http://www.pepak.net/bezpecnost/utoky-na-operacni-pamet/.

Požár, J. *Kybernetická bezpečnost: sborník příspěvků z bezpečnostního semináře Policejní akademie a evropského vedení AFCEA konaného dne 12. dubna 2011 na Policejní akademii České republiky v Praze.* Vyd. 1. Praha: Policejní akademie České republiky, 2011. ISBN 978-80-7251-347-5. Dostupné z: http://www.cybersecurity.cz/data/Pozar2.pdf/.

Rao, U., Nayak, U. *The InfoSec Handbook.* New York: Apress, 2014. ISBN 978-1-4302-6382-1. Dostupné z: http://www.apress.com/9781430263821?gtmf=f/.

Rapp, D. *Evil Twin Access Point Attack Explained.* [online]. 2013 [cit. 2015-02-14]. Dostupné z: https://dalewifisec.wordpress.com/2013/05/16/evil-twin-access-point-attack-explained/.

Rosenblatt, S. *Top Wi-Fi routers easy to hack, says study.* [online]. ZoneAlarm, 2013 [cit. 2014-12-17]. Dostupné z: http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/.

Rubens, P. *How to Securely Delete Data from Hard Drives.* [online]. 2012 [cit. 2014-12-13]. Dostupné z: http://www.esecurityplanet.com/windows-security/how-to-securely-delete-data-from-hard-drives.html.

Security Threat Report 2014 *Sophos.* 2014 [cit. 2014-12-08]. Dostupné z: https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf/.

Shaver, J. *4+ Years Later, What Did We Learn From Firesheep and SSLStrip?* [online]. 2014 [cit. 2015-02-14]. Dostupné z: https://jimshaver.net/2015/01/10/4-years-later-what-did-we-learn-from-firesheep-and-sslstrip/.

Schenker, M. *Google Now Takes a Bite Out Of Your Privacy.* [online]. 2015 [cit. 2015-03-18]. Dostupné z: http://www.webdesignerdepot.com/2015/02/google-now-takes-a-bite-out-of-your-privacy/.

Schneier, B. *Man-in-the-Middle Attacks.* [online]. 2008 [cit. 2014-12-15]. Dostupné z: https://www.schneier.com/blog/archives/2008/07/maninthemiddle_1.html.

Schneier, B. *"Evil Maid"Attacks on Encrypted Hard Drives.* [online]. 2009 [cit. 2014-12-17]. Dostupné z: https://www.schneier.com/blog/archives/2009/10/evil_maid_attac.html.

Scharr, J. *Malvertising Is Here: How to Protect Yourself.* [online]. 2014 [cit. 2014-12-20]. Dostupné z: http://www.tomsguide.com/us/malvertising-what-it-is,news-19877.html.

Skoudis, E. *Malware: fighting malicious code.* Upper Saddle River: Prentice Hall, c2004, xxii, 647 s. Prentice Hall series in computer networking and distributed systems. ISBN 01-310-1405-6.

The Man-In-The-Browser: It Hungers For Your Online Credentials *ZoneAlarm.* [online]. 2014 [cit. 2014-12-17]. Dostupné z: http://www.zonealarm.com/blog/2014/05/the-man-in-the-browser-it-hungers-for-your-online-credentials/.

Thompson, J. *Lost PC password? here's how to recover it.* [online]. 2013 [cit. 2014-12-15]. Dostupné z: http://www.techradar.com/news/software/operating-systems/lost-pc-password-here-s-how-to-recover-it-1151893.

Toxen, B. *Bezpečnost v Linuxu: prevence a odvracení napadení systému.* Vyd. 1. Brno: Computer Press, 2003, 849 s. ISBN 80-722-6716-7.

Tubin, G. *Endpoint Security: No Admin Rights, No Malware? Yeah, Right!* [online]. 2013 [cit. 2014-12-14]. Dostupné z: http://securityintelligence.com/endpoint-security-admin-rights-malware-yeah-right/.

Tubin, G. *Malvertising Campaigns Get a Boost From Unpatched Java Zero-Day Exploits.* [online]. 2013 [cit. 2014-12-20]. Dostupné z: http://securityintelligence.com/malvertising-campaigns-get-boost-unpatched-java-zero-day-exploits/.

Viehbock, S. *Brute forcing Wi-Fi Protected Setup.* [online]. 2011 [cit. 2015-02-18]. Dostupné z: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf/.

Voo, B. *How To Reveal Hidden Passwords (Asterisks) In Web Browsers.* [online]. 2013 [cit. 2015-04-23]. Dostupné z:http://www.hongkiat.com/blog/reveal-hidden-passwords-in-browsers/.

Wawro, A. *Get your privacy ducks in a row with DuckDuckGo.* [online]. 2013 [cit. 2015-03-18]. Dostupné z:http://www.pcworld.com/article/2035703/get-your-privacy-ducks-in-a-row-with-duckduckgo.html/.

What Is The Difference Between A Virus, Worm, Trojan, And A Rootkit *Global Tech Consulting Group.* 2014 [cit. 2014-12-13]. Dostupné z: http://globaltechconsultants.org/?q=content/what-difference-between-virus-worm-trojan-and-rootkit.

Winter, P., Lindskog, S. *Spoiled Onions: Exposing Malicious Tor Exit Relays.* [online]. 2013 [cit. 2014-12-17]. Dostupné z: http://www.cs.kau.se/philwint/spoiled_onions/techreport.pdf.

Zap, *HSTS se stává novým internetovým standardem.* [online]. 2012 [cit. 2015-02-14]. Dostupné z: http://computerworld.cz/internet-a-komunikace/hsts-se-stava-novym-internetovym-standardem-49145/.

Zetter, K. *Hacker Lexicon: What Is a Zero Day?* [online]. 2014 [cit. 2014-12-15]. Dostupné z: http://www.wired.com/2014/11/what-is-a-zero-day/.

Přílohy

A Ukázky programů

Běžný uživatel často není seznámen (protože to ani nemá zapotřebí) s podobou současných útočných nástrojů. Může tak snadno předpokládat, že provedení informatických útoků je velmi obtížné a jsou toho schopni pouze malé okruhy technicky nadaných jedinců. Následující ukázky jsou určeny pro utvoření lepší představy o současných programových nástrojích, které jsou volně k dispozici.

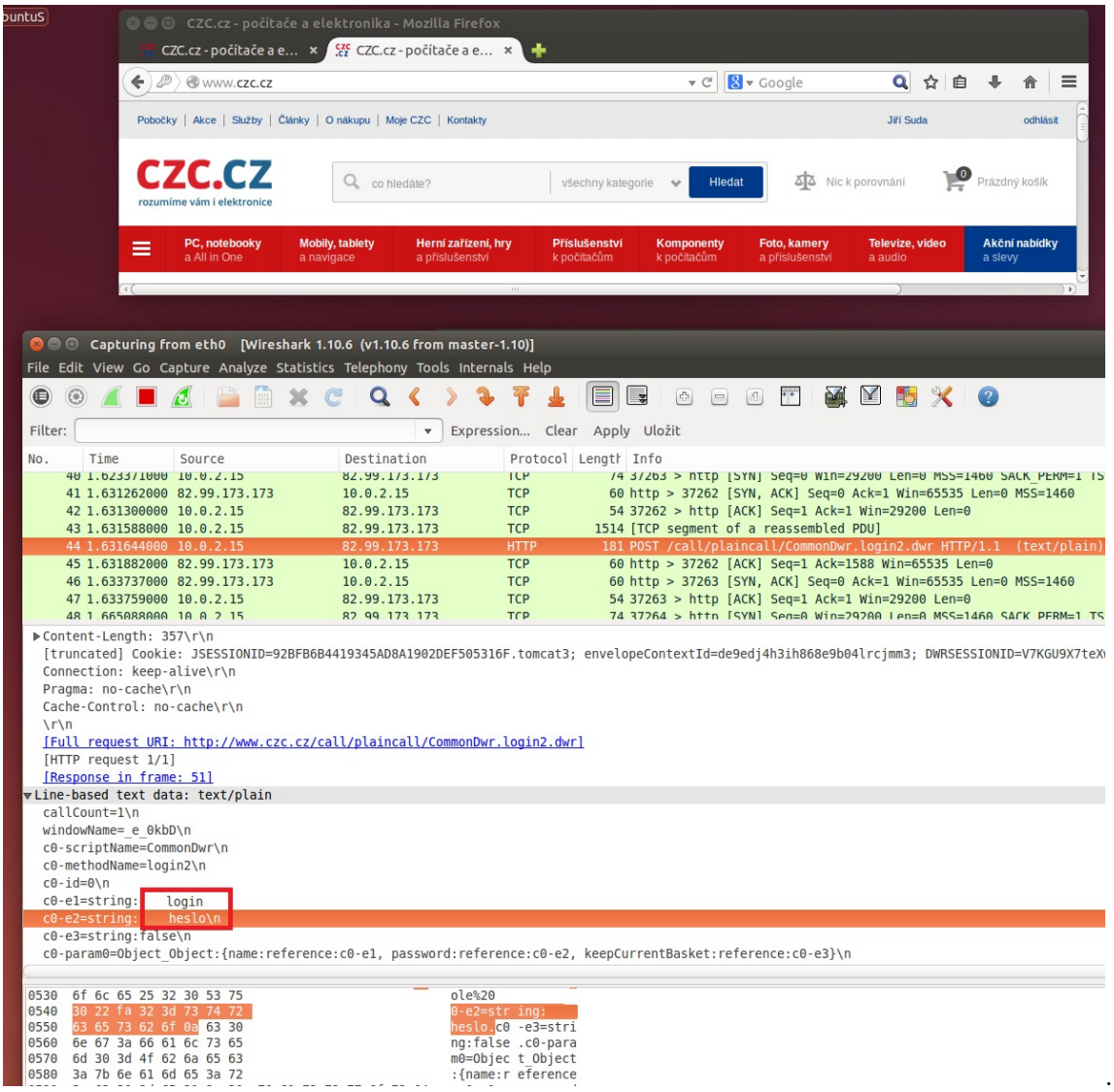
A.1 Odeslání falešného emailu

Takto jednoduše může vypadat formulář na webových stránkách sloužící k odeslání falešného emailu. Vylekaný a nezkušený uživatel může snadno uvěřit, že je zpráva pravá. Pravý útočník si ovšem může naformulovat svůj vlastní text i odesílatele dle vlastní libosti.

Obrázek 12: Příklad odeslání falešného emailu ze stránek www.sendanonymousemail.net.

A.2 Ukázka zachycení hesla programem Wireshark

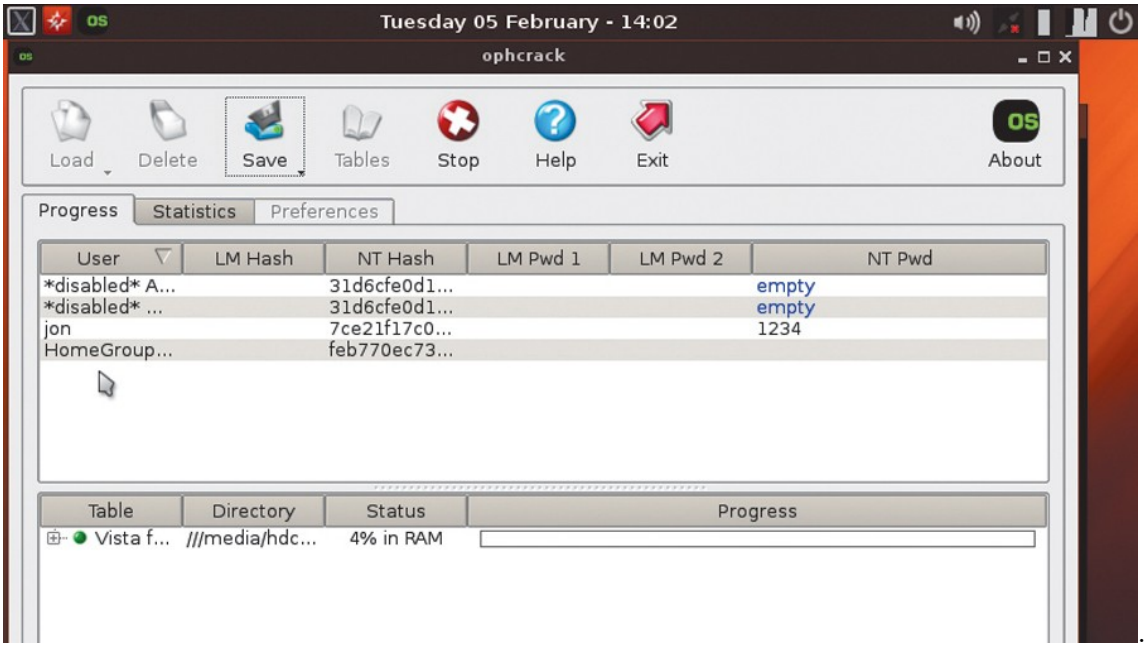
Pro lepší představu, jak snadné je pro útočníka odposlechnout nechráněné heslo je na obrázku níže znázorněna ukázka jeho zachycení pomocí volně dostupného programu Wireshark. K tomuto typu jsou potřeba již nějaké znalosti síťových technologií. Oranžově je vyznačen konkrétní protokol HTTP, kde se heslo nachází. Samotný řetězec s heslem je zvýrazněn červeným rámečkem v inspekčním okně.



Obrázek 13: Zachycení hesla do webového obchodu Czc.cz programem Wireshark.

A.3 Ukázka obnovy hesla operačního systému programem Ophcrack

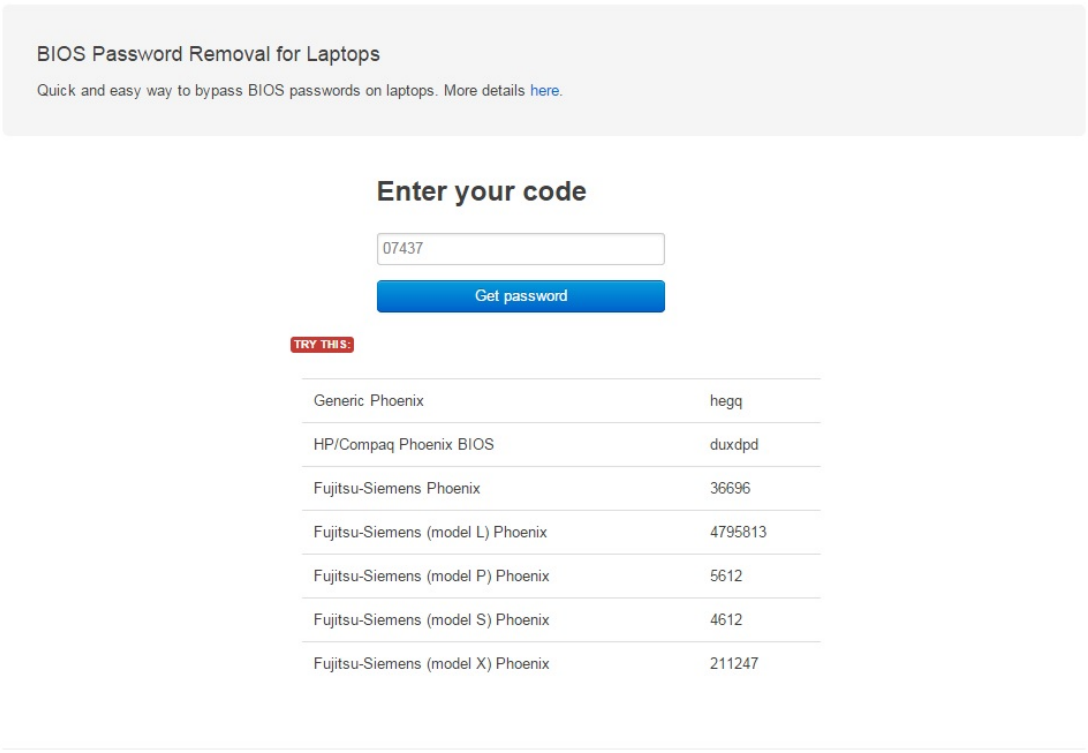
Program prohledá celý systém a najde všechny dostupné uživatele. Na obrázku je vidět obnova hesla jediného uživatele jon. Heslo má 1234. Heslo může být také snadno odstraněné tlačítkem Delete.



Obrázek 14: Program Ophcrack při obnově hesla.
Zdroj: Lost PC password? here's how to recover it, 2013.

A.4 Ukázka obnovy hesla v BIOSu

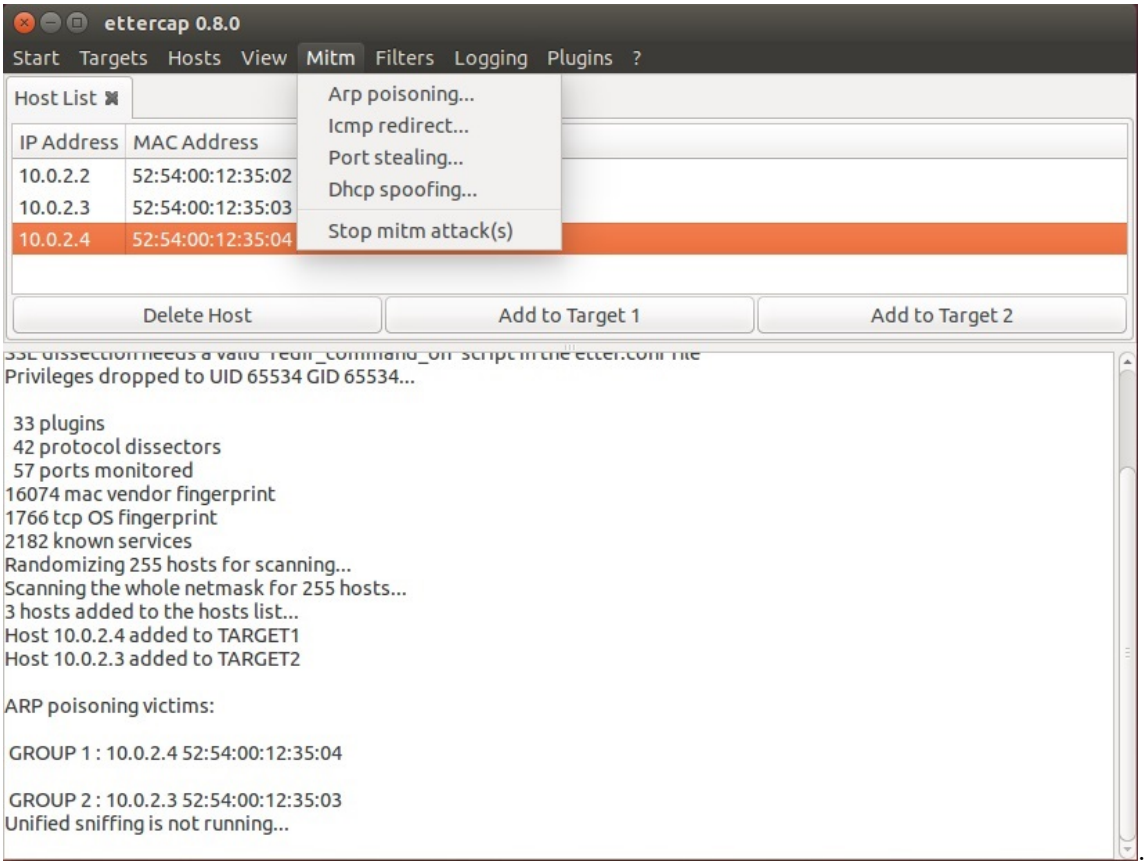
Kontrolní součet zobrazený po třech chybně zadaných pokusech, stačí vložit do této webové stránky (pro ukázku číslo 07437), která obsahuje většinu algoritmů implementovaných výrobci základních desek.



Obrázek 15: Webové stránky www.bios-pw.org pro překonání hesla v BIOSu.

A.5 Ukázka programu Ettercap

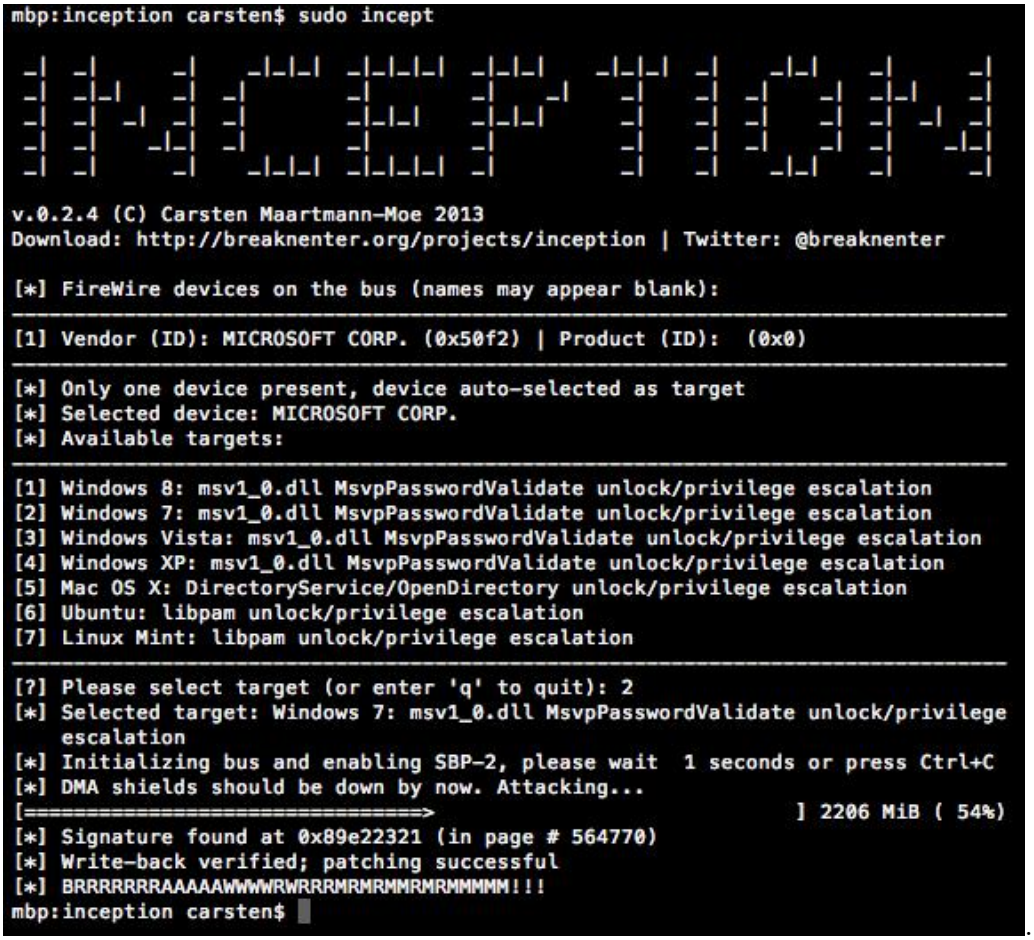
Program Ettercap je schopný provést plně zautomatizované útoky na lokální síti. Stačí pouze vybrat cílové stroje a zvolit typ útoku.



Obrázek 16: Program Ettercap při útoku.

A.6 Program Inception

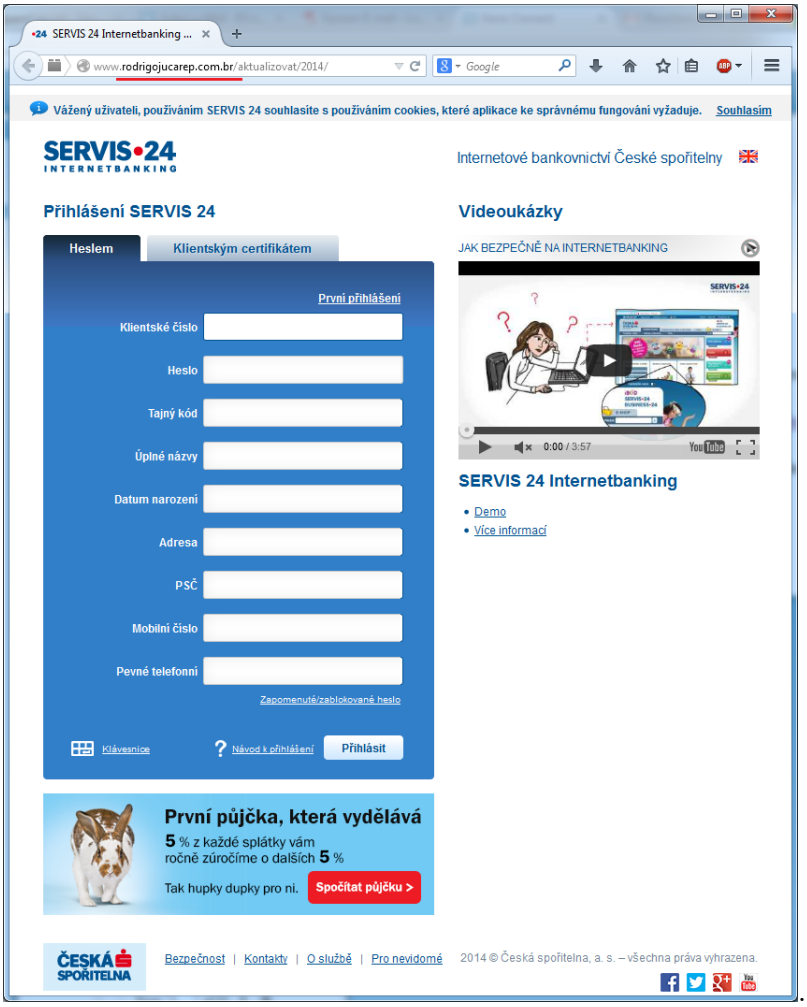
Jak je vidět na obrázku, po spuštění programu Inception vybereme číselně pouze operační systém, do kterého má být umožněn přístup a stiskneme Enter. Program sám automaticky přepíše operační paměť na připojeném počítači skrz kabel Firewire.



Obrázek 17: Program Inception přepisující operační paměť napadeného počítače. Zdroj: ToolsWatch.org.

A.7 Ukázka podvodného webu

Jak je vidět na obrázku podvodná webová stránka se běžnému uživateli jeví na první pohled jako pravá. Obsahuje loga společnosti, reklamy na vlastní produkty. Ovšem nesedí webová adresa a není použito protokolu HTTPS.



Obrázek 18: Podvodná webová stránka, lákající po uživateli citlivé údaje s heslem. Zdroj: Hoax.cz

A.8 Uzamknutí počítače

Jedna z možností jak může vypadat uzamknutí uživatelského počítače. Kvůli věrohodnosti jsou programem zjištěny z Internetu údaje IP adresy, města, poskytovatele připojení. Jsou vyjmenovány zákony, které údajně uživatel měl porušit. V šedém okénku vedle obrázku webkamery se zobrazuje údajně zachycený uživatel.

Obrázek 19: Česká výzva zablokovaného počítače k zaplacení.
Zdroj: CSIRT-MU.

B Obsah přiloženého CD

- Diplomová práce ve formátu PDF
- Bezpečnostní aplikace UbuntuS se zdrojovými kódy