Bezpečnost Protokolů Elektronické Komunikace

Radek Kudela

BAKALÁŘSKÁ PRÁCE
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Radek Kudela**
Osobní číslo:	**A13043**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost protokolů elektronické komunikace**
Téma anglicky:	**The Security of Electronic Communication Protocols**

Zásady pro vypracování:

1. **Seznamte se s problematikou bezpečnosti elektronické komunikace.**
2. **Definujte základní pojmy a popište možnosti bezpečné komunikace pomocí e-mailu a dalších komunikačních nástrojů.**
3. **Specifikujte nejčastější bezpečnostní hrozby.**
4. **Vyhodnoťte bezpečnost jednotlivých způsobů komunikace.**
5. **Navrhněte doporučení pro bezpečnou komunikaci.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MALANÍK D., Bezpečnostní Politiky v Kontextu Bezpečnosti Informačních Systémů. In Bezpečnostní technologie, systémy a management 2013. Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2013, s. 1-4. ISBN 978-80-7454-289-3.**
2. **KOPECKÝ, Kamil, KREJČÍ, Veronika. RIZIKA VIRTUÁLNÍ KOMUNIKACE, 1.vyd. NET UNIVERSITY, s.r.o., 2010. 36 s. ISBN 978-80-254-7866-O.3.**
3. **SORIANO, Miguel. Zabezpečení informací a sítí. Vyd. 1. V Praze: České vysoké učení technické. ISBN 978-80-01-05296-9.**
4. **Data Security Management. DSM - data security management. 2, Praha : TATE International, s.r.o., 2012, Sv. XVI. ISSN1211-8737.**
5. **SATRAPA, Pavel. IPv6: internetový protokol verze 6. 3., aktualiz. a dopl. vyd. Praha:CZ.NIC, 2011, 407 s. CZ.NIC. ISBN 978-80-904248-4-5.**

Vedoucí bakalářské práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **23. února 2016**

Termín odevzdání bakalářské práce: **30. května 2016**

Ve Zlíně dne 16. února 2016

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 23.5.2016

.....
podpis diplomanta

ABSTRAKT

Práce se zabývá analýzou bezpečnosti elektronické komunikace. Jsou rozebrány možnosti bezpečné komunikace pomocí e-mailu a dalších komunikačních nástrojů. Práce obsahuje testy zabezpečení jednotlivých způsobů komunikace a návrh doporučení pro bezpečnou komunikaci. Hlavní částí práce je návrh zabezpečení vůči odposlechu. Dále práce specifikuje nejčastější hrozby a zranitelnosti protokolů, kde se soustředí převážně na odposlech sítě, sociotechniky a následně na možnosti jak se proti nim bránit.

Klíčová slova: bezpečnost, komunikace, odposlech, Wireshark, sociální inženýrství, HTTP, FTP, POP, IMAP, SMTP

ABSTRACT

This thesis deals with security analysis of electronic communication. It explores and analyses various options for safe and secure communication via email and other electronic tools. Part of this thesis also includes a security evaluation of each particular method of communication and a recommendation for more secure communication. The main part of the thesis is a security proposal against sniffing. This thesis further specifies the most common risks and vulnerabilities of protocols, where it focuses mainly on network sniffing, sociotechnics and then proposes various defense options.

Keywords: security, communication, sniffing, Wireshark, social engineering, HTTP, FTP, POP, IMAP, SMTP

Můj velký dík patří panu Ing. Davidovi Malaníkovi Ph.D. za předání zkušeností, cenné rady a za odborné vedení při vypracování bakalářské práce.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V dnešní době bychom asi těžko hledali domácnosti, firmy nebo úřady, které nepoužívají ke svým potřebám zařízení připojené k síti. Zde se však vyskytuje problém bezpečnosti přenášených informací. Uniklé informace z firmy, mohou obsahovat know-how nebo utajené dokumenty a mohou mít pro danou instituci nedozírné následky. Firmy vydávají nemalé prostředky na zabezpečení svých sítí, ale jednu věc většinou opomíjejí, a tou je chyba lidského faktoru, pokud útočník využije některou ze sociotechnik, způsobí to, že i nejlepší zabezpečení přijde vniveč.

Pojem informace je využíván jako všeobecný pojem, představuje všechna aktiva, které mají pro instituci nějakou hodnotu. Bezpečnost protokolů je základním kamenem pro zajištění informační bezpečnosti. Ta má za cíl zajistit bezpečný chod systémů, které organizace nebo uživatelé potřebují pro své činnosti. Hlavním cílem je zajistit, aby byla zajištěna ochrana před selháním dostupnosti, důvěrnosti nebo integrity dat.

K dosažení co nejlepšího zabezpečení musí instituce dbát kromě softwarových, hardwarových, komunikačních opatření také na personální opatření. Možnosti, jak předcházet útokům založených na sociálním inženýrství, jsou školení personálu nebo udržování kvality lidských vztahů ve firmě. Tímto krokem se vyhneme útokům, které konají nespokojení zaměstnanci.

Zabezpečení protokolů je nedílnou součástí bezpečné komunikace. Množství protokolů bylo vyvinuto v začátcích Internetu a nesplňují dnešní požadavky na bezpečnost. Odchozí komunikace přes tyto protokoly je nešifrovaná a pro útočníka, který má přístup k síti, je jednoduché komunikaci zachytit a nakládat s ní podle jeho potřeb. Z tohoto důvodu je potřeba veškerou komunikaci šifrovat. Pro útočníky jsou zajímavé jen takové informace, které může zpeněžit nebo takové kterými se může dostat do systému a překonat jeho zabezpečení.

Pomocí elektronické pošty komunikuje snad každý z nás, ale většina uživatelů používající tuto službu si neuvědomuje rizika, která tento způsob komunikace přináší. Existuje několik možností, jak získat obsah zprávy, proto by tato komunikace neměla být využívána pro přenos důležitých zpráv. Pokud se chceme získat data obsažená ve zprávě, kterou uživatel napsal, můžeme k tomu využít odposlech komunikace nebo kombinaci sociálního inženýrství a malwaru, kde malware poslouží k nainstalování keyloggeeru, který následně získá data uložená v zařízení a útočník se může přihlásit ke službě a zde si obsah zprávy přečíst.

I. TEORETICKÁ ČÁST

1 ODPOSLECH DAT NA SÍTI

Tato kapitola se zabývá útoky na počítače a počítačovou síť. Jsou zde uvedeny jednotlivé typy a jejich popis.

Zařízení, která jsou připojena do nezabezpečené sítě, jsou jednoduchou kořistí pro hackera. Osobní počítače byly ještě v minulém století využívány hlavně hackery pro jejich výpočetní výkon. V dnešní době se napadená zařízení využívají pro sofistikovanější úkony. Hacker používá své zařízení k rozesílání nežádoucí pošty, tzv. spamu nebo také k DoS útokům. Dalším důvodem proč hacker útočí na cizí zařízení je získání přístupových údajů, k důležitým informacím.

1.1 Odposlech sítě

Tento pojem se někdy označuje jako „packet capturing“, ale není zcela přesný, protože se při tomto ději zachytávají rámce z 2. síťové vrstvy OSI modelu. Pakety, které jsou ve 3. síťové vrstvě, jsou zachytávány taktéž, a to kvůli tomu, že se nachází uvnitř těchto rámců. Ty ale tvoří jenom část síťových dat, které jsou zachyceny.

Odposlech sítě je možný, pokud má hacker fyzický přístup k dané síti, jelikož musí své zařízení propojit s datovým kabelem. Další možností, jak provést odposlech sítě, je dostat se k zařízení, které není zabezpečené. Pro tento typ útoku si můžeme vybrat z několika programů. Mezi ty nejvíc populární patří open source program Wireshark.

Programy nepoužívají pouze hackeři, ale jsou používány i administrátory, kteří jimi sledují síťový provoz. [1].

1.2 Odposlech hesel

Program určený pro odposlech hesel, tzv. „password sniffer“, je podle definice software, který odposlouchává příchozí a odchozí komunikaci a třídí pakety podle toho, jestli obsahují heslo. Tento software může být aplikován na většinu protokolů, jakými jsou HTTP, IMAP, FTP, POP3 a příbuzné protokoly, které nesou v nějakém formátu heslo. Jiný typ password snifferu je instalován na bránu nebo na proxy server, ten potom získává hesla v rámci sítě. Tyto programy jsou primárně používány jako nástroj pro zabezpečení sítě. Jsou také používány hackery i crackery pro nelegální a nekalé účely.

Získat hesla jde několika dalšími způsoby. Asi nejjednodušším je heslo od někoho odkoukat. Vzhledem k tomu, že si stále mnoho uživatelů píše heslo na papír a nechává si ho v blízkosti svého

zařízení, není problém, aby se útočník tohoto hesla zmocnil a nemusí být ani fyzicky přítomen. Může k tomu použít webovou kameru, se kterou má rozhled na uživatelovu pracovní plochu.

Útok hrubou silou je jedna z dalších možností jak získat heslo. Hacker k tomu používá všechny kombinace znaků, a pokud heslo není dostatečně dlouhé, tomuto útoku neodolá. Bránit se proti takovému útoku je možné několika způsoby. Nejčastějším způsobem je, že pokud útočník zadá 10x heslo, tak se zařízení zablokuje. To je pak možné odemknout až po uplynutí určitého času. Další možností, jak se bránit, je mít dostatečně dlouhé heslo. Doporučení je, aby mělo minimálně 12 písmem a byly zde použity malá a velká písmena a znaky z ASCII abecedy.

Pokud máme hesla uložena na disku v nešifrované podobě a útočník získá přístup buď k zařízení, nebo přímo k disku, je pro něho snadné z tohoto disku data nebo hesla získat. Pokud jsou tato hesla v zašifrované podobě, může útočník použít metodu, kterou jsme uvedli výše, tedy útok hrubou silou. Může také použít program slovníkového typu, který získává hesla z .pdf a .rar souborů. Bránit se proti takovým útokům je jednoduché. Šifrovat disk a zamezit fyzický přístup nežádaným osobám k zařízení a používat dostatečně dlouhá hesla, to nám zajistí obranu proti tomuto útoku.

Můžeme se setkat i se softwarem, který umožňuje monitorovat vstupní zařízení, útočník díky tomuto softwaru pozná, co jsme na klávesnici právě napsali. Tento software se může dostat do zařízení několika způsoby. Nejčastěji je to součást instalace programu z neoficiálního zdroje nebo nám ho někdo při fyzickém přístupu k zařízení může nainstalovat. Můžeme si vybrat z nepřeberného množství takových softwarů, mezi nejpopulárnější však patří Homekey Logger. Tento software není primárně určený pro běžné uživatele, kteří by ho mohli zneužít, ale je hlavně určen pro testovaní bezpečnosti sítě.

Všechna doporučení na bezpečná hesla nám zbytečná, pokud jsou ukládána v prohlížeči . Spustíme-li si v prohlížeči plugin pro vývojáře, můžeme jednoduše pole, které je ve formátu „password“, přepsat na formát „text“ a heslo, které je skryto pod tečkami nebo hvězdičkami, se zobrazí nezašifrované v otevřeném textu. Jsou zde například i programy jako je PassView, které útočníkovi pomůžou tyto uložená hesla získat.

1.3 Chyby v programech

Chyby dělíme na syntaktické a běhové, ty syntaktické chyby detekuje kompilátor během překladu. Tyto chyby se také nejlépe vyhledávají a opravují. Kompilátor programátorovi ukáže, v jaké části programu se chyba nachází, a vypíše upozornění, které ukazuje, co je v kódu špatně. Hackeři dělají chyby ve svých škodlivých softwarech kvůli tomu, aby je nemohl využít úplně každý. Běhové

chyby jsou vyhledávány složitěji. Při kompilaci kompilátor chyby nedetekuje, ty se pak můžou, ale nemusí projevit při chodu programu. Při výskytu chyb může v lepších případech program spadnout, v horších případech může být bránou pro útočníka do zařízení a získat tak administrátorská práva.

Pro předcházení běhovým chyb slouží testování. To ověřuje správné pracování programu a zjišťuje, jestli program má nějaké vedlejší efekty. Testování by mělo být prováděno jinou osobou, než tou která program vytváří. Důvod je prostý. Ten, kdo vytváří program, nevidí nebo ani neví o chybách, které udělal. Některé programy se vypouští na trh hned po odstranění syntaktických chyb a očekává se, že běhové chyby budou odhaleny po dobu provozu [1][2][3].

2 ŠPIONÁŽNÍ TECHNIKY

Nejznámějšími špionážními technikami jsou ty, které jsou založeny na sociálním inženýrstvím. Tato sociální věda se zabývá tím, jak útočník získá za podvodného jednání přístup k důležitým informacím.

2.1 Sociální inženýrství

Metoda využívá nejslabší článek systému, člověka. Cílem metody je získat si důvěru lidí, aby konali tak, jak útočník zamýšlí. Můžeme se setkat se dvěma typy sociotechnických útoků, které jsou fyzické a psychologické.

Bránit se takovým útokům je složité, u firem se dodržují přísná opatření pro předcházení takovým útokům. Jedním z opatření může být školení zaměstnanců napříč všemi pozicemi.

Nejlepší nástroj pro aplikaci sociálního inženýrství je Internet. Jedna z nejčastějších technik je získávání hesel z webových stránek, kde útočník vytvoří naprosto totožnou stránku s originální a vyzve např. emailem uživatele, aby se na této stránce přihlásil. Tímto způsobem získá údaje pro autentizaci na příslušnou stránku. Statistiky uvádí, že každý pátý uživatel internetu naletět tzv. phishingu.

Administrátoři při závadách vyhledávají pomoc na internetových diskuzích, jelikož neví všechno a na těchto diskuzích získájí informace bez toho, aniž by se museli zabývat problémem dopodrobna. Toto je využito útočníky, kteří záměrně způsobují chyby v systémech, a potom nabízí řešení v již zmiňovaných diskuzích. To pak vede k tomu, že administrátor udělá přesně to, co po něm útočník chce. Tato metoda se nazývá reverzní sociální inženýrství [5].

Reverzní sociální inženýrství má 3 fáze:

- Sabotáž – útočník způsobí závadu v systému
- Inzerci – nabídne řešení závady
- Asistenci – závadu vyřeší, ale po čas opravy se naboural do systému

Do sociálního inženýrství spadá několik metod. Těmi neznámějšími jsou:

2.1.1 Pretexting

Metoda, která využívá smyšlený příběh na to, aby vylákala z lidí různé informace. Využívá pravdivé informace, aby ujistila oběť, že se jedná o důvěryhodnou věc. Většinou se z obětí snaží vytáhnout informace jako je rodné číslo, jméno otce, jméno matky za svobodna, místo narození a další. Je především využívaná soukromými detektivy a také útočníky, kteří potřebují tyto údaje

pro překonání služby, kterou oběť používá. Metoda je stále využívaná, jelikož pořád mnoho služeb a uživatelů používá tyto údaje jako bezpečnostní otázky při zapomenutí hesla. Mimo síť se tato metoda vyznačuje tím, že se někdo vydává za druhou osobu.

2.1.2 Phishing

Phishing se označuje jako podvodná zpráva, která na první pohled vypadá důvěryhodně, ta potom přesměruje oběť na webovou stránku, jenž vypadá úplně stejně jako stránka originální. Tato stránka vyzve oběť, aby se přihlásila a provedla akci, kterou útočník požaduje. Útočníci se soustředí z velké části na bankovní účty a na služby, které byly zhotoveny za účelem placení, např. PayU, PayPal.

Phishingovou zprávu poznáme podle několika znaků. Všechny tyto zprávy obsahují odkaz na webovou stránku. Hned na první pohled můžeme poznat, že adresa nesouhlasí s originální, navíc tato stránka neobsahuje žádné zabezpečení. Dalším znakem může být žádost o aktualizaci bezpečnostních údajů nebo vyplnění údajů, které bychom nikomu nesdělili, např. PIN ke kartě, číslo karty, číslo účtu, autentizační údaje pro internetové bankovnictví apod. Všechny tyto zmíněné údaje jsou zákonem po uživatelích zakázané požadovat. Existuje několik doporučení, jak se proti phishingu bránit. Nejdůležitější je samozřejmě vůbec takové zprávy nečíst a ignorovat je. Pokud chceme jít na stránku, která poskytuje bankovní služby, měli bychom napsat adresu ručně a nevyhledávat ji přes prohlížeče. Při zadávání adresy dbát na to, abychom neudělali chybu, protože tato metoda využívá i překlepů. Jako další musíme dbát na nejnovější verzi OS, používat zabezpečení zařízení jako jsou antivirové a antispywarové programy, neinstalovat programy z neověřených zdrojů a k službám poskytující internetové bankovnictví se přihlašovat pouze ze svých zařízení [5][23].

2.1.3 IVR

Metoda je také označována jako telefonní phishing. Používá stejnou metodu jako zmíněný phishing s tím rozdílem, že žádá oběť o zavolání na číslo za účelem ověření informace. Pokud oběť zavolá na toto číslo, tak se tváří jako bankovní automat, ten potom požaduje pin nebo heslo k nějaké službě. Existují i více sofistikovanější automaty. Ty využívají přesměrování na operátora, který je v tomto případě útočník. Ten pak může vylákat z oběti více informací.

2.1.4 Baiting

Baiting je v několika ohledech stejný jako phishingové útoky. To, co odlišuje tuto metodu od phishingu, je, že hacker nabízí oběti zdarma filmy, hry, programy a další. Za to, že se uživatel vzdá svých přihlašovacích údajů na jim vybrané služby. Baiting není omezen pouze na poli

internetu. Hackeři se mohou také zaměřit na využití lidské zvídavosti a k tomu využivají fyzické nosiče dat. Útok se provede tak, že infikované USB klíče se rozmístí na místa, kde bude jasné, že oběť tento klíč najde. USB klíč se popíše tak, aby oběť donutil tento klíč zapojit do svých zařízení. Po zapojení do zařízení se aktivuje obsah USB klíče. Většinou jsou zde umístěny keylogery, které umožňují přístup k řadě přihlašovacích údajů.

2.1.5 Quid pro quo

V překladu tento výraz znamená něco za něco. Metoda má několik podob. Např. získávání důležitých informací od nespokojeného zaměstnance nebo využívání zpráv, které upozorňují oběť na to, že má bezpečnostní chybu ve svém zařízení. Útočník chybu nabídne opravit a při opravování chyby vypnou zabezpečení zařízení a nainstalují zde špehovací software. Metoda názorně ukazuje, že všechna zabezpečení jsou k ničemu, protože jak ukázaly příklady z reálného světa, zaměstnanci byli ochotni se vzdát svých hesel již za tabulku čokolády. Je důležité si uvědomit, že útočnici mohou používat mnohem méně sofistikované metody pro získání klíčových informací, proto by firmy měli pečlivě vybírat své zaměstnance.

2.1.6 Tailgating

Další metodou sociálního inženýrství je tailgating. Tato metoda vyžaduje někoho, kdo má již přístup do dané instituce. Funguje tak, že zaměstnanec pustí do objektu útočníka se svými autentizačními údaji. Tento způsob však moc nefunguje ve velkých institucích, protože využívají propracovanější přístupové systémy, které neumožňují přístup více osobám na jeden autentizační prvek. Hackeři, kteří se zabývají právě sociálním inženýrstvím využívají lidské psychologie a zvědavosti. Tyto útoky mohou být odraženy pouze, pokud je uživatel dobře poučen o těchto útocích [6].

2.2 DoS

Denial of Service, což v překladu znamená odmítnutí služby. Tento útok patří mezi nejčastější . Běžný uživatel pozná tento útok tak, že když zadá URL adresu a odešle požadavek na server nedojde k zobrazení stránky. Je to dáno tím, že server může zpracovat jen určitý počet žádostí. Útok spočívá v tom, že napadnuté zařízení může odmítat poskytovat řádné plnění služeb. Jednou z možností, proč k tomuto dochází, je zahlcení zprávami elektronické pošty, ftp přenosy, požadavky na www server a další. Útok se projevuje tím, že je nemožné spustit software z toho důvodu, že je využita interní paměť nebo není možné uložit data z důvodu využití externí paměti.

DoS útoky můžou být používány jako odpoutání pozornosti od dalších útoků, které mohou cílit např. na firewally. Je to také velmi populární zbraň, jenž využívají Internetoví vandalové, hacktivisté nebo Internetoví vyděrači. Tyto útoky mohou trvat dny, týdny, v některých případech i měsíce. Proti těmto útokům se nelze zabránit, ale lze se na nich připravit. Jedna z nejlepších možností je otestovat infrastrukturu třetí stranou, která provede simulovaný útok. Pokud chceme úplně minimalizovat ztráty, musíme mít někoho, kdo nám nepřetržitě bude sledovat síťový provoz. [4]

2.3 Programy pro odposlech sítě

Tyto programy můžeme najít pod různými označeními jako jsou packet analyzer, network analyzer nebo sniffer. Jsou rozděleny podle toho, jakou daná síť používá technologii. Buď to můžou být ethernetové sniffery, nebo bezdrátové sniffery. Zachytávají každý datový paket a ty jsou schopné pomocí filtrů třídit dle potřeby.

2.3.1 Wireshark

Je to asi nejznámější open source pro odposlech sítě. Funguje na většině operačních systémů, kterými jsou Linux, OS X a Windows. Jedna z největších výhod tohoto softwaru je přehledné grafické uživatelské rozhraní, díky kterému je velmi snadné ho používat. K jeho dalším výhodám patří velká oblíbenost mezi uživateli, díky které můžeme najít spoustu tutoriálů a diskuzí k tomuto programu.

Wireshark je schopen zachytit pakety v reálném čase a pomocí filtrů je roztřídit a dešifrovat na základě jejich protokolu. Je dokonce schopný rozpoznat a zachytit VOIP hovory a v některých případech může tyto zachycené média přehrávat. Program je stále vyvíjen a aktivně ho podporují obrovské komunity uživatelů a vývojářů, proto je často aktualizován a přináší nové funkce.

2.3.2 SniffPass Password Sniffer

SniffPass je velmi specifickým nástrojem pro odposlech komunikace, zaměřený na zachytávání hesel z datové komunikace. Když zapneme password sniffer začne sledovat datovou komunikaci, a pokud zachytí paket, ve kterém je obsaženo heslo, tak ho hned vypíše. Tímto způsobem můžeme najít zapomenutá hesla k účtům. Program je poměrně snadné používat, protože poskytuje velmi jednoduché a srozumitelné grafické prostředí a také zachytává hesla na většině protokolů, mezi ty nejznámější protokoly ze kterých může získat heslo patří POP, IMAP ,FTP a HTTP.

2.3.3 Microsoft Network Monitor

Microsoft Network Monitor je zdarma ke stažení na oficiálních stránkách Microsoftu. Kompatibilní je pouze ze systémem Microsoft Windows. Poskytuje rozšířené možnosti při sledování komunikace v reálném čase. Software je stále podporován a aktualizován společností Microsoft. Má také velice intuitivní grafické prostředí, takže je vhodný pro začátečníky, jenž s ním mohou sledovat domácí datovou komunikaci. Převážně je určený pro administrátory. Jeho výhodou je, že podporuje více než 300 veřejných protokolů a protokolů vlastněných společností Microsoft, mimo to podporuje i zachytávání paketů na bezdrátové síti.

2.3.4 Tcpdump

Tcpdump je jedním z nejstarších nástrojů na odposlech sítě. Byl vytvořen v roce 1987 Lawrence Berkley Laboratory. Pracuje na platformě UNIX, takže je možné ho spustit na systémech, které jsou na této platformě založeny. Těmi jsou Linux, Solaris, OS X, AIX a další. Nemá grafické prostředí, a pracuje v příkazovém řádku, z toho důvodu je určen pro pokročilejší uživatele. Nástroj analyzuje chování sítě a sleduje aplikace, které generují provoz v síti [7].

2.4 Zákon

Sledování sítě jako takové není trestnou činností. O trestnou činnost se jedná tehdy, pokud zaměstnavatel odposlouchává své zaměstnance. Pokud by toto zaměstnanec nahlásil na policii, může být zaměstnavatel potrestán peněžní pokutou nebo dokonce i odnětím svobody až na jeden rok. Nelegální odposlech je trestná činnost. Zákon říká, že: *„dle § 239 trestního zákona (porušování tajemství dopravovaných zpráv), případně podle § 240 trestního zákona č. 151/2000 Sb. O telekomunikacích definuje v § 84 dílu 12 telekomunikační tajemství a zprostředkovacích dat. Předmětem telekomunikačního tajemství je obsah zpráv přepravovaných nebo zprostředkovaných telekomunikačními zařízeními a sítěmi s výjimkou zpráv určených veřejnosti, provozní popisující obsah přepravovaných zpráv a data související s poskytováním telekomunikačních složek, zejména údaje o účastnících telekomunikačního spojení. Podobně zákon č. 29/2000 Sb. o poštovních službách definuje v § 16 hlavy III. poštovní tajemství a podmínky mlčenlivosti nositelů poštovního tajemství. Porušování uvedených tajemství podléhá trestnímu zákonu*" [8].

2.5 Zranitelné protokoly vůči odposlechu

V současnosti je stále používáno množství protokolů, které nejsou šifrované a je jich možné odposlouchávat. Ty nejpoužívanější jsou popsané níže.

2.5.1 HTTP

HTTP protokol dokáže přenášet text, zvukovou stopu, videa a další multimediální soubory pomocí World Wide Web. Komunikační protokol slouží pro připojení k webovým serverům. Jeho primární funkcí je navázat spojení se serverem a poslat HTML stránky zpět do prohlížeče uživatele. Spojení se udržuje mezi klientem a serverem pouze do okamžiku, kdy dojde k požadavku a poté se spojení uzavře. HTTP pracuje na nejvyšší vrstvě protokolu TCP/IP, ta se nazývá aplikační vrstva. Text, který se přenáší tímto protokolem je nešifrovaný, takže je snadné odposlouchávat. Pro zabezpečení tohoto protokolu se používá šifrovaná verze HTTPS [9].

2.5.2 SMTP

SMTP protokol poskytuje možnost odesílat elektronickou poštu. Pracuje na aplikační vrstvě TCP/IP. Byl vytvořen a je spravován institucí Internet Engineering Task Force. Je také známý pod označením RFC 821 a RFC 2821. Je nejpoužívanější protokol pro odesílání e-mailových zpráv. Složen je ze 4 částí: uživatelský agent (MUA), agent pro předání (MSA), agent pro spojení (MTA), agent pro doručení (MDA). Funguje tak, že je zahájena relace mezi MUA a MSA, zatímco MTA a MDA vyhledává domény a místní poštovní služby. SMTP na portu 25 umožňuje odposlech komunikace, jelikož komunikace probíhá v nezašifrované podobě[10].

2.5.3 POP

Nejnovější protokol z této řady je POP3, jedná se o třetí verzi. Ta byla vypuštěna roku 2012. POP běží na aplikační vrstvě TCP/IP protokolu. Slouží pro přijímání pošty a také ji filtruje do příslušných uživatelských složek. Pro získání pošty se uživatel musí připojit k síti a jeho pošta se uloží na disk. Potom si ji uživatel může prohlížet i bez připojení k síti. Stejně jako u SMTP protokolu jsou data na portu 110 nešifrována a můžeme si je při zachycení komunikace přečíst. Je zde možnost i odposlechu hesel [11].

2.5.4 IMAP

IMAP je další z řady emailových protokolů. Ukládá elektronickou poštu na poštovní server a umožňuje koncovému uživateli zobrazit, upravovat zprávy a zařazovat je do složek. Podporuje připojení několika zařízení, takže můžeme být připojení současně na PC i na mobilním zařízení. I přesto, že má IMAP ověřovací mechanismus, proces ověřování lze obejít, pokud je protokol v nezašifrované podobě a máme přístup k síti, můžeme použít password sniffery, které získají

z datové komunikace uživatelské jméno a heslo, to je však možné jenom na nešifrovém portu 143. V současné době se pro zabezpečení tohoto protokolu používá šifrovací protokol SSL [12].

2.5.5 FTP

FTP je protokol určený pro přenos souborů přes Internet. K souborům, které jsou uložené na FTP serveru, lze přistupovat pomocí FTP klienta. FTP server může být nakonfigurován tak, že může mít několik režimů. Anonymní režim umožňuje se připojit k serveru komukoliv, ale v tomto režimu uživatel nemusí mít přístup ke všem souborům a složkám. Je-li tento režim vypnut, uživatelé se musí přihlásit k serveru přihlašovacími údaji, aby mohli prohlížet, stahovat nebo upravovat soubory. Standartní FTP není šifrován, což znamená, že lze odposlouchávat. Proto byly vyvinuty protokoly FTPS a SFTP, které zajišťují, že veškerá komunikace je šifrována [13].

3 ŠIFROVÁNÍ KOMUNIKACE

Protokoly, přes které odesíláme elektronickou poštu nejsou z velké části šifrovány, proto musíme tyto zprávy zašifrovat, abychom se nám nestalo, že někdo odchytí komunikaci a přečte si zprávu v otevřeném textu. Pro šifrování zpráv máme několik možností, které tuto bezpečnostní chybu řeší.

3.1.1 Bitmessage

Bitmessage je převážně využíván pro odesílání šifrované elektronické pošty. Aplikuje některé myšlenky z Bitconu. Jedna z největších výhod těchto produktů je decentralizovanost. Firma BitTorrent, která tento protokol provozuje odmítá spolupráci s NSA. Vzhledem k tlaku na technologické firmy, aby spolupracovali s vládami, je tento protokol pro uživatele, kteří chtějí bezpečnou komunikaci velice zajímavý. Je odolný vůči odposlechu i spoofingu, což představuje pozměnění elektronické pošty. Bitmessage je open source a je dostupný na platformách Windows, OS X a Linux [15].

3.1.2 OpenPGP

OpenPGP slouží pro šifrování elektronické pošty za využitím asymetrické kryptografie. Je založen na původním PGP, které vyvinul Phil Zimmermann. Definuje standardní formáty pro šifrované zprávy, podpisy a certifikáty pro výměnu veřejných klíčů. Tento standard může být používán jakoukoliv institucí bez licenčních poplatků. Metoda šifrování je používána i samotným Edwardem Snowdenem [16].

3.1.3 S/MIME

S/MIME je standard pro šifrovaní s veřejným klíčem, který byl vyvinutý společností RSA Data Security. Je používán většinou moderních e-mailových klientů. Poskytuje mnoho kryptografických služeb, kterými jsou autentizace, integrita zpráv, digitální podpis a pomocí šifrování zajišťuje soukromí a zabezpečení dat. Ne každý emailový klient, ale podporuje S/MIME digitální podpis, pokud je taková zpráva doručena a klient ji nepodporuje, výsledkem je to, že dostaneme přílohu s názvem smime.p7s [21].

3.1.4 SSL

SSL je protokol, jenž slouží pro šifrování komunikace. Princip protokolu je založen na asymetrickém šifrování. Je to standartní bezpečnostní protokol pro vytvoření šifrovaného spojení mezi serverem a klientem, nejčastěji mezi webovým serverem a prohlížečem. Právě označení HTTPS upozorňuje na to, že HTTP je zabezpečený šifrovacím protokolem SSL/TLS. SSL by mělo být využíváno na každé webové stránce, která v nějaké podobě shromažďuje data o uživatelích.

3.1.5 TLS

TLS je novější verzí SSL, mezi verzemi SSL 3.0 a TLS 1.0 jsou rozdíly minimální [21].

3.1.6 SSH

SSH je síťový protokol, který administrátorům poskytuje bezpečný způsob, jak se přihlásit ke vzdálenému zařízení. Secure shell nebo-li SSH funguje jako plugin na prohlížeči i jako plnohodnotný klient na různých platformách. Poskytuje silné ověřování a bezpečně šifrovanou datovou komunikaci mezi dvěma zařízeními, které komunikují po nezabezpečené síti. SSH je nejvíce používaný administrátory sítí pro správu systémů a aplikací na dálku, což umožňuje spouštět příkazy a přesouvat soubory z jednoho zařízení do druhého [17].

3.1.7 IPsec

IPsec je používán pro realizace virtuálních privátních sítí a pro vzdálený přístup. Velkou výhodou je, že IPsec opatření mohou být řešeny bez nutnosti větších změn v jednotlivých zařízeních. Tato technologie je implementována společností Cisco do svých směrovačů. IPsec umožňuje dvě bezpečnostní opatření jednou z nich je „Authentication Header“, která umožňuje autentizaci odesílatele a druhá „Encapsulating Security Payload“, která podporuje jak autentizaci odesílatele, tak i šifrování odeslaných dat [21].

4 NÁVRH NA ZABEZPEČENÍ KOMUNIKACE

Emailová komunikace patří bez debat mezi nejvíce využívané služby, proto je také velmi často zneužívána. Existuje několik způsobů, jak zneužít elektronickou poštu. Mezi nejčastější patří zfalšování uživatele, který poštu odesílá, nebo odeslání zfalšovaného obsahu zprávy jménem napadeného uživatele. Zpráva od odesílatele putuje ze zařízení celou sítí až k příjemci zprávy a právě tady je zranitelná, proto zpráva musí být zabezpečená již na zařízení uživatele.

4.1 Návrh na zabezpečení elektronické pošty

Protokoly pro přenos elektronické pošty jsou v základním tvaru nezabezpečené. Je-li SMTP nastaveno tak, že nepožaduje autentizaci, je velmi lehce zranitelné. Útočník může z této emailové adresy odesílat email komukoli pod jeho jménem. V nejzazších případech se přes tuto napadenou službu mohou rozesílat viry nebo makro viry. POP3 a IMAP protokoly již požadují autentizaci uživatele, ale je zde možnost odposlechu hesel, jelikož protokoly nejsou v základním stavu šifrované.

4.1.1 Zabezpečení pomocí protokolů

Protokoly, které jsou šifrované chrání komunikaci mezi odesílatelem a příjemcem a jsou imunní vůči odposlechu. Tyto protokoly řeší chyby, jenž mají základní protokoly pro odeslání a příjem pošty. Těmito chybami jsou nedostatečná autentizace a komunikace, která probíhá v otevřeném textu. Nové protokoly pro zabezpečení elektronické pošty používají jiné porty. Možnost velmi silného zabezpečení závisí na opatřeních, která je schopna instituce nebo uživatel dodržovat. Jednou z možností je umístění zařízení v lokální síti, kde je možnost využití IP adresy. Tento krok zajistí, že právě jenom z této IP adresy bude možnost odesílat elektronickou poštu bez vyžádání autentizace.

Chybou autentizace, kterou trpí SMTP protokol řeší jeho rozšířená verze ESMTP, ta vyžaduje autentizaci, která má označení SASL. Tato metoda však má nedostatky týkající se šifrování komunikace. Pro bezpečnější komunikaci je tedy nutno využít protokolů, které poskytují autentizaci a šifrování komunikace. Nejpoužívanějšími protokoly pro tuto činnost jsou TLS/SSL, které běží na portu 443. Pro zabezpečení příchozí pošty je nutno použít nové POP3 a IMAP4, které umožňují šifrovat komunikaci. Tyto protokoly běží na jiných, než dosavadních portech. Těmi jsou u POP3 port 995 a u IMAP4 port 993. Pro webové klienty se požívá zabezpečeného HTTP protokolu, tedy verze HTTPS, která také využívá jiného portu, než standartní HTTP a tím je port 443.

4.1.2 Digitální podpis

Digitální podpis je jedním z nejzákladnějších zabezpečení pro elektronickou komunikaci. Může být použit s jakýmkoliv druhem zprávy, je jedno jestli je šifrovaná nebo ne. Ruční podpis lze zfalšovat, ale ten digitální zfalšovat nelze [21] [25] [37] [39].

5 BEZPEČNOST DAT

Bezpečnost dat je bez diskuzí jedním z největších problémů dnešní doby, jelikož jsme v době, kdy drtivá většina institucí a uživatelů má svá důvěrná data v elektronické podobě a většina ani nezjistí, že jsou napadeni. Je to z toho důvodu, že na trhu je nedostatek lidí, kteří se specializují na tuto problematiku. Čím větší je množství dat uložených na zařízeních, tím větší je motivace pro útočníka získat tato data, a proto je potřeba mít data zabezpečená. Nejedná se tady jenom o data, ale i o identitu uživatele. Pokud se útočník zmocní identity, může způsobit velké množství škody.

Dnešní doba přináší operační systémy, které jsou zabezpečené již v továrním nastavení, jde o automatizaci zabezpečení. Je to z toho důvodu, aby se eliminovaly možné chyby způsobené uživatelem. Operační systém může být jakkoliv zabezpečen, pokud uživatel není seznámen se základními bezpečnostními praktikami, hrozí, že provede operaci, kterou tento operační systém systém může oslabit. . Nejčastějšími chybami jsou administrátorská práva na zařízení, ponechání zaznamenaného hesla poblíž počítačového nebo mobilního zařízení nebo nezašifrovaná data na úložišti.

Bránit se proti nežádoucímu přístupu k důležitým datům je důležité hlavně tam, kde je zařízení využíváno více uživateli. Zařízení, respektive operační systém, by měl být schopný bránit před nežádoucím přístupem, změnou nastavení nebo odcizení důležitých dat.

Pro ochranu zařízení je důležité jak zabezpečení fyzické, tak i systémové. Když dojde k odcizení úložiště, neměl by být útočník schopný se dostat k datům, která jsou zde uložena. Ochrana dat před fyzickým přístupem v malých a středních podnicích je velmi složitá, protože proti technikám, které jsou popsány v sociálním inženýrstvím, je velmi těžké se bránit. Z tohoto důvodu by měla být data na úložišti chráněná bezpečným šifrováním.

Oblast bezpečnosti rozděluje 3 aspekty:

- Důvěrnost - přístup ke službám je možný jenom po zadání přístupových údajů
- Integrita – službu může editovat jenom oprávněný uživatel
- Dostupnost – služba je dostupná tehdy, když to uživatel s oprávněním vyžaduje

Dojde-li k narušení jednoho z uvedených bodů, naruší se tím bezpečnost služby. Při napadení zařízení jsou tyto aspekty zastoupeny pokaždé v jiné míře, např. když útočník ukradne zařízení, dojde k narušení dostupnosti nebo může také dojít k narušení důvěrnosti služby, podle toho jak jsou data na zařízení zabezpečena. Dalším příkladem je škodlivý software, který může narušit všechny 3 aspekty. Pokud modifikuje systém, dojde k narušení integrity, pokud prolomí autentizaci, dojde

k narušení důvěrnosti a pokud zahltí systém nesmyslnými požadavky, dojde k narušení dostupnosti služby.

Dále dělíme bezpečnost, podle toho, na co je útok namířen:

- Bezpečnost hardwarová – zde řadíme bezpečnost zaměřenou na neoprávněný fyzický přístup k zařízení,
- Bezpečnost operačního systému – zahrnuje systémová opatření vůči napadení OS
- Bezpečnost síťová – řeší zneužitelný přístup ke službě vně i mimo organizaci
- Bezpečnost aplikační – zabezpečuje službu, před neoprávněnou editací
- Bezpečnost personální – řeší problematiku nespokojeného zaměstnance
- Bezpečnost organizační – má na starosti problematiku týkající se přístupu k informacím, kteří mají jednotlivý zaměstnanci
- Bezpečnost databázová – řeší bezpečnost v rámci důvěrnosti

Při zabezpečení systému by mělo být dbáno na to, aby byl dodržen každý z uvedených bodů. Také by zabezpečení mělo být navrhováno více osobami z toho důvodu, že specialisté na SW a HW většinou opomíjí bezpečnost personální a organizační. Tyto rámce bezpečnosti jsou velmi důležité, protože zabezpečení SW a HW může být stoprocentní, ale vůči sociotechnikám se neubrání.

5.1 Kvantifikace bezpečnosti

Kvantifikovat přesně úrovně bezpečnosti na všechny OS je velmi složité z toho důvodu, že nabídka na trhu obsahuje velké množství OS, které jsou postaveny na jiném jádru a komparace bezpečnosti mezi nimi je proto složitá. Jsou metody, které tyto úrovně určují přesněji a které méně. Náklady na co nejpřesnější stanovení úrovní jsou o poznání vyšší, jelikož se na nich podílí více specialistů a zaberou více času.

Právě obsah vložených prostředků do zabezpečení OS je důležitou indicií pro stanovení úrovně bezpečnosti. Peněžní částka, která je do zabezpečení vložena by měla souhlasit s náklady, které by musel vynaložit útočník pro překonání tohoto zabezpečení. Tato indicie pro stanovení bezpečnosti však není objektivní z důvodu relativní hodnoty peněz. Zakoupením hodnotného komponentu, který je s ostatními nekompatibilní, znamená vysoké náklady a minimální zabezpečení.

Pro movitější organizace je tady možnost stanovit úroveň bezpečnosti specializovanou společností. Problémem je, že každá firma posuzuje podle svého uvážení, a pokud se posudek dá zpracovat více společnostem, může být výsledek odlišný.

V dnešní době můžeme najít několik standardů pro určení bezpečnosti, tím nejstarším je TCSEC. Tento standard však není tak všestranný jako Common Criteria, mimo jiné je používán i Českou republikou. Standardy představují předběžnou úroveň zabezpečení, ale jsou obecné a méně přesné, než posouzení od specializované firmy. Avšak posouzení bezpečnosti těmito standardy je méně nákladně a umožňuje jednoduché porovnání.

5.1.1 Trusted Computer System Evalution Criteria

Standard TCSEC, byl vytvořen v roce 1981 NCSC, což představuje dnešní NSA a v roce 1983 byl schválen jako oficiální standard pro určení bezpečnosti OS, síťových prvků a aplikací.

TCSEC je určený pro přibližné určení bezpečnosti celého systému. Pokud je systém ohodnocen jednou z úrovní, tak musí splňovat minimálně i všechny nejnižší úrovně zabezpečení ostatních prvků. Minimální ochrana je označena tímto standardem jako D, to znamená, že splňuje všechny základní úrovně, ale nebyla splněna žádná lepší úroveň. Tento standart má 7 úrovní, z čehož D představuje nejnižší bezpečnost a A1 nejvyšší. TCSEC dnes může použít pouze pro ohodnocení starých systémů, pro nové systémy je tento standard zastaralý. Je však možnost bezpečnost systému odhadnout a udělat komparaci s novými. To pomůže k pochopení možnosti zabezpečení.

Dnešní doba stále nepřináší OS s úrovní hodnocení A1. Pro bezpečné užívání OS je doporučena minimálně úroveň C2. Firma Microsoft tuto certifikaci získala se svým systémem Windows NT 3.5 se Service Pack 3. Byl to první systém, který splňovala tato firma, předchozí systémy MSDOS a Windows 3.1 tento standard nesplňovali. Systémy založené na OS UNIX byly hodnoceny od úrovně C1 až po B3, dle toho jaký zásah byl do struktury [18].

Úrovně hodnocení jsou určeny následovně:

- D - Minimální ochrana
- C1 – Volitelná ochrana přístupu
- C2 – Kontrolovaná ochrana přístupu
- B1 – Povinné řízení přístupu
- B2 – Strukturovaná ochrana
- B3 – Bezpečnostní domény
- A1 – Verifikovaný návrh

5.1.2 Common Criteria

Common Criteria je standard, který je v dnešní době nejvíce používaným a uznávaným ve všech vyspělých zemích. Je označován jako ISO/IEC 15408 a je jím ohodnocena většina operačních,

přístupových a biometrických systémů, dále jím mohou být ohodnocena víceúčelová zařízení a další.

Licencované laboratoře pro určení tohoto standardu jsou v Austrálii, Kanadě, Francii, Německu, Itálii, Japonsku, Malajsii, Nizozemsku, Norsku, Jižní Koreji, Španělsku, Švédsku, Turecku, Velké Británii a Spojených státech.

Pro porozumění tomuto standardu, je potřeba znát několik pojmů, které jsou uvedeny při ohodnocení jednotlivých systémů a zařízení.

TOE (Target Of Evaluation) znamená cíl hodnocení, jak již vyplývá z názvu, soustředí se na cíl, který je hodnocen. Cíle jsou určovány podle předem daných dokumentů.

PP (Protection Profile) znamená ochranný profil. Tento dokument je postupně doplňován uživateli a je přidáván k závěrečné certifikaci. Definuje bezpečnostní problémy pro systémy a výrobky.

ST (Security Target) znamená bezpečnostní cíl. Tento dokument je obsažen v PP a je poskytnutý výrobcem produktu. Ukazuje na to, jak produkt řeší požadavky na zabezpečení. Obsahuje informace, které jsou nezbytné pro určení úrovně bezpečnosti.

Výstupem standardu je dokument označený jako EAL. Dokument obsahuje úroveň bezpečnosti daného systému nebo zařízení.

Moderní OS poskytují bezpečnost EAL4, což znamená v přepočtu na stupnici TCSEC úroveň C2. Například Windows 10 je ohodnocen na bezpečnostní úrovni EAL4+. Nejlépe hodnocené systémy na portálu CommonCriteriaPortal.org jsou od firmy IBM. Ty mají bezpečnostní úrovně na EAL5+ [18] [19].

Common Criteria má 7 úrovní hodnocení:

EAL1 – Funkčně testováno

EAL2 – Strukturálně testováno

EAL3 – Metodicky testováno a kontrolováno

EAL4 - Metodicky testováno a kontrolováno

EAL5 – Semiformálně navrženo a testováno

EAL6 – Semiformálně ověřený a testovaný návrh

EAL7 – Formálně ověřený a testovaný návrh

II. PRAKTICKÁ ČÁST

6 BEZPEČNOST JEDNOTLIVÝCH ZPŮSOBŮ KOMUNIKACE

Pro testování bezpečnosti jednotlivých způsobů komunikace byl vybrán operační systém Mac OSX El Capitan 10.11 a pro zachytávání paketů program Wireshark. Testování ukazuje, které způsoby komunikace jsou bezpečné a které pro komunikaci nejsou doporučené. Pro jednotlivé nezabezpečené druhy komunikace jsou vyhodnoceny návrhy na zabezpečení.

6.1 Instalace wireshark

Software je nainstalován na zařízení MacBook Pro model A1398 s operačním systémem Mac OSX 10.11 El Capitan. Program byl stažen s oficiální webové stránky Wireshark.org, vybrána byla verze 64-bit. Pro správné fungování Wiresharku je potřeba nainstalovat balíček XQuartz, který obsahuje knihovny potřebné pro spuštění programu. Program se po instalaci nachází v **/Applications/Wireshark.app/Contents/MacOS/Wireshark**. Pokud uživatel spustí terminál a napíše zde tuto cestu, program se spustí [27].

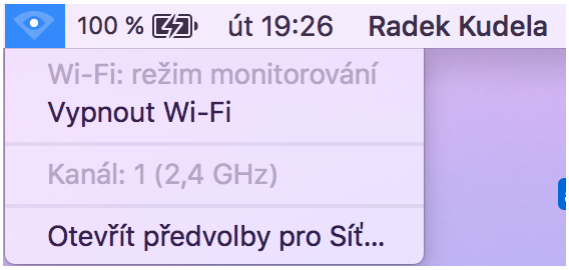
6.2 Nastavení

Pro odchycení komunikace musí být správně nastavena síťová karta. Pro zachytávání všech paketů musí být v módu, který je označován jako „monitor mód“. Mód se vyznačuje tím, že síťová karta se chová skoro stejně jako kdyby byla v promiskuitním režimu. O tento režim se však nejedná. V monitor módu karta může přijímat veškerou komunikaci standardu IEEE 802.11, kterou má ve svém dosahu, zatímco v promiskuitním módu musí být přímo připojena k dané síti a nemůže zachytávat všechny pakety [22].

Zvolené zařízení pro odposlech obsahuje kartu, která nese označení Airport Wireless Card 607-8356 661-6534. Samotná karta má možnost režimu monitorování, tudíž je vhodná pro účely této práce.

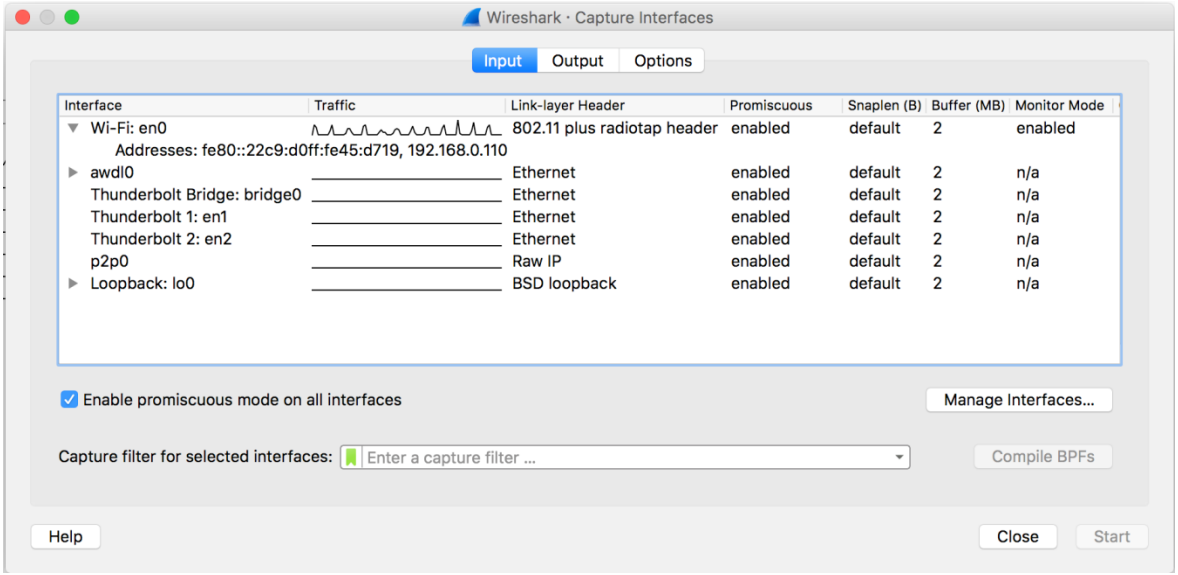
Režim monitorování lze aktivovat několika způsoby:

- Příkazem **- sudo ln -s /System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport /usr/local/bin/airport**, tento způsob zapnutí režimu monitorování je určen spíše pro odposlech komunikace v Terminálu.



Obr. 1: Režim monitorování, Zdroj: autor

- Manuálně – v programu Wireshark, v záložce **Capture** zvolíme možnost **Option** a otevře se okno **Capture Interfaces**. V tomto okně se nachází sloupec **Monitor mode**, zde vybereme rozhraní, na kterém probíhá komunikace a povolíme možnost **Enabled** [28].



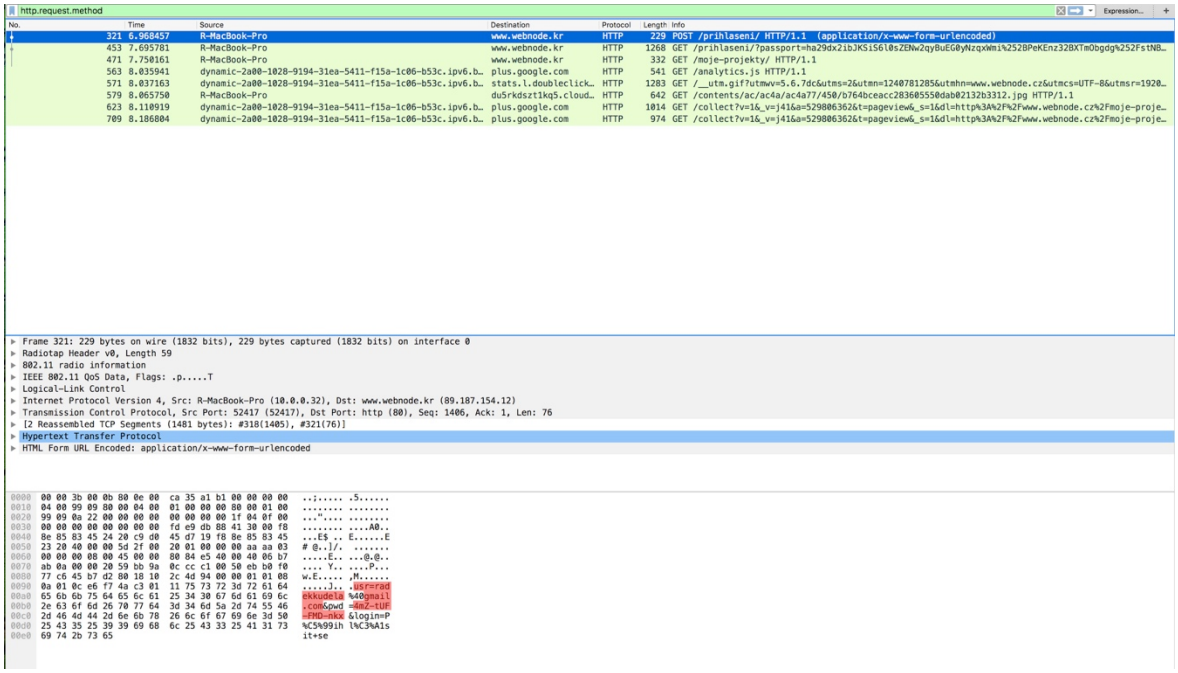
Obr. 2 : Režim monitorování, Zdroj: autor

Pro dešifrování komunikace se musí nastavit dešifrování 802.11 standardu, který se provede v předvolbách Wiresharku, kde se zvolí key type **wpa:pwd** z toho důvodu, že připojení je šifrované pomocí WPA2-PSK. Pole vyžaduje vyplnění hesla k síti a její SSID ve tvaru **SSID:HESLO**.

6.3 HTTP

Je-li zachycen protokol HTTP v základní formě bez jakéhokoliv šifrování, je snadné z něho získat data. Pomocí HTTP mohou být přenášena veškerá data, proto se v dnešní době přechází na HTTPS, který šifruje datovou komunikaci, a je tedy ve většině případech nemožné takto přenášená data dešifrovat. V případě, že jakýmkoliv způsobem přesvědčíme uživatele, že nemá používat certifikát na dané stránce, je zde opět možnost snadného odposlechu.

Pomocí Wiresharku je názorně ukázáno jak je snadné zachytit komunikaci a následně z paketů data číst v otevřeném textu.



Obr. 3 : Odchycený paket s heslem, Zdroj: autor

Obrázek č.3 znázorňuje HTTP paket, který v sobě nese heslo. Zde je vidět jak je snadné zachycený paket vyhledat a přečíst. Pomocí filtru **http.request.method** se zobrazí jen ty pakety, které potřebujeme pro získání hesla z HTTP protokolu. Ten v sobě nese přihlašovací jméno uživatele a heslo, které je v obrázku znázorněno červeně. Může být použito jakékoliv bezpečné heslo, ale pokud uživatel použije pro autentizaci HTTP protokol, vystavuje se nebezpečí odposlechu hesel. Pro demonstraci bylo heslo automaticky vygenerováno generátorem bezpečných hesel.

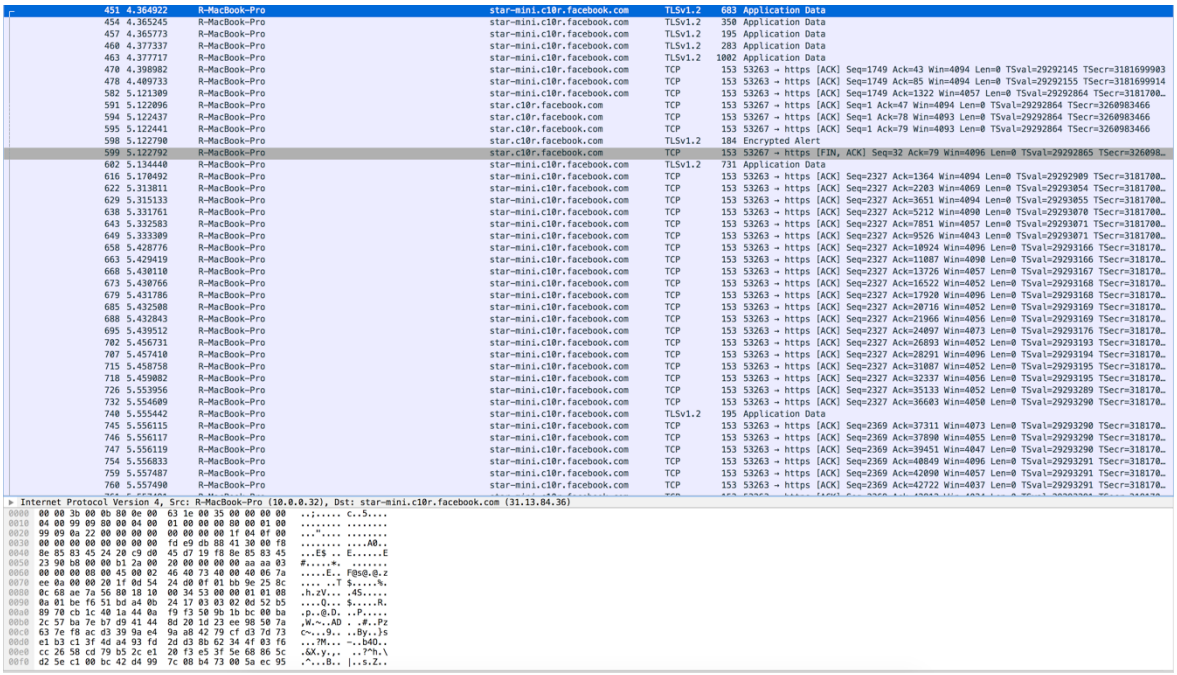
Přes protokol HTTP je možnost odposlouchávat veškerou datovou komunikaci, která momentálně probíhá na síti. Pokud uživatel navštíví webovou stránku, útočník hned ví, co si právě prohlíží.

6.3.1 Návrh na zabezpečení

HTTP protokol je pro bezpečné využívání komunikace nepřípustný, proto by na to měl uživatel brát zřetel. Pro bezpečnou komunikaci musí bezpodmínečně být tento protokol šifrován. Současné protokoly, které jsou využívány pro šifrování komunikace, jsou bezpečné za určitých předpokladů. Aplikace musí být správně nastavené a musí podporovat nejnovější verzi šifrovacího protokolu. Staré verze v sobě obsahují bezpečnostní chyby, které mohou být zneužitelné.

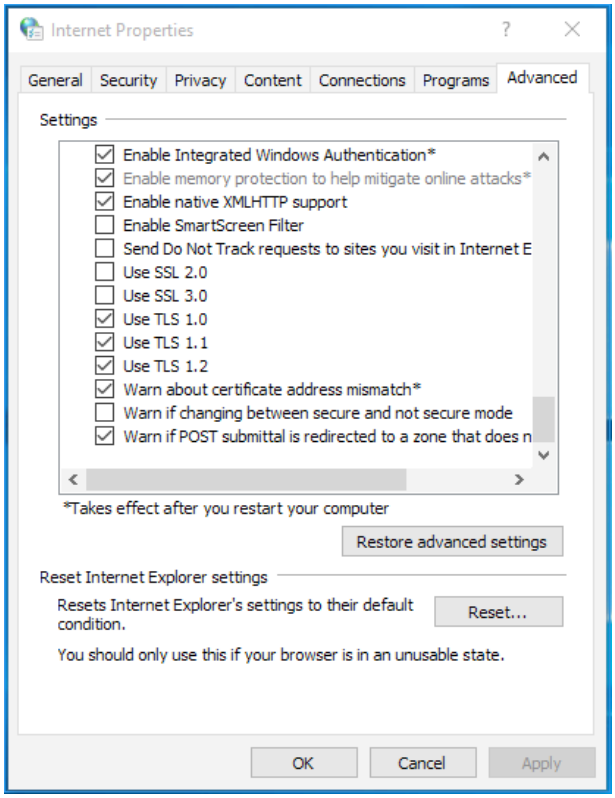
V dnešní době se nedoporučuje používat starší verze SSL protokolu. Pro ověření bezpečnosti protokolu na serveru slouží webová stránka ssllabs.com, kde si uživatel zadá url nebo

ip webové stránky a algoritmus mu vygeneruje podporu certifikátů a oznámkuje stupněm zabezpečením daný server. Pro zajímavost server google.com má známku B a seznam.cz známku A a nejlépe ohodnocený server může získat známku A+. Tato známka byla udělena serveru zoho.com. Server ssllabs.com, testuje SSL/TLS a jejich bezpečnost pak ohodnotí známkou. Výsledek testu zobrazí všechny informace o certifikátu, jeho případné zranitelnosti a použité šifry.



Obr. 4 : Šifrovaná komunikace, Zdroj: autor

Jak je vidět z obrázku č.4 server facebook.com využívá pro svou datovou komunikaci protokol TLSv1.2. Tento protokol je považován za bezpečný a doposud neprolomený. Zachycené pakety jsou zašifrovány, takže z nich nelze nic vyčíst. Obsah takového paketu můžeme vidět na spodní straně obrázku č.4.



Obr. 5: Nastavení šifrovacích protokolů,
Zdroj: autor

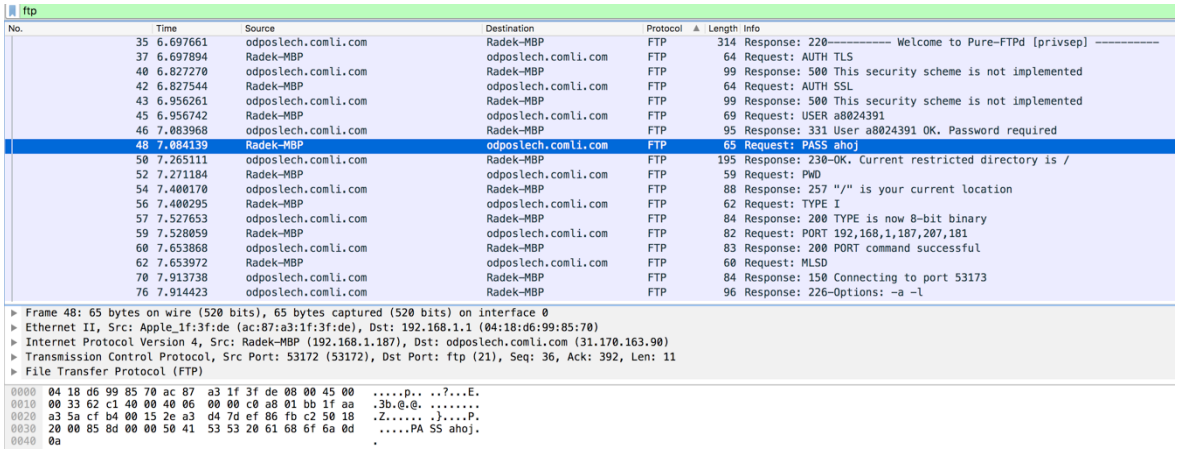
Obrázek č.5 ukazuje, které protokoly jsou pro datovou komunikaci bezpečné. Protokol SSL 3.0 je stále hojně využíván, ale není již doporučen [46].

Doporučení pro zabezpečení HTTP protokolu je používat nejnovější verzi šifrovacích protokolů. Pokud zařízení nebo software nepodporuje nejnovější verze certifikátu, měl by si uživatel rozmyslet, za jakým účelem tento protokol využívá. Uživatel by měl mít nějaký všeobecný přehled, jaký šifrovací protokol je stále aktuální a doporučován, protože to, co platí dnes, nemusí platit i zítra. Využití HTTPS nemá jen výhody šifrované komunikace, ale je i rychlejší oproti běžnému HTTP. Pro provozovatele webových stránek je tak výhodnější využívat protokol HTTPS, kvůli rychlejšímu provozu stránky. Dnešní doba přináší certifikáty pro takové webové stránky zdarma. Nabízí je služba Let`s Encrypt. Nevýhodou však pro některé uživatele může být, že má kratší dobu platnosti, než ostatní služby. Pro šifrování komunikace je to však výhoda, jelikož při objevení chyby v technologii pro vygenerování protokolu, je tato chyba odstraněna za kratší dobu, než u konkurence [32] [31] [30] [29] [25] [24] .

6.4 FTP

FTP je protokol, který byl vyvinut již v 80. letech minulého století. Byl to první protokol sestrojený na bázi klient a server. Nepočítal tedy při vzniku se zabezpečením datové komunikace a nese v sobě několik zásadních chyb. Stále se můžeme setkat s nezabezpečenou verzí FTP protokolu, kterou využívají někteří poskytovatelé webových hostingů. Využíván je především pro sdílení dat a administraci webových stránek. Protokol nešifruje v základním nastavení odchozí komunikaci, a tak je velmi snadné zachytit paket nesoucí heslo.

Port, na kterém běží FTP protokol většina zdrojů označuje jako port 21, to však není zcela přesné. Přes port 21 probíhá řízení a k přenosu příkazů a port 20 zajišťuje přenos souborů.



Obr. 6 : Odposlech FTP, Zdroj: autor

Odposlech hesla z FTP z datové komunikace je možný pouze s připojením kabelu RJ-45 do zařízení. Jelikož zařízení, které bylo zvoleno k této práci byl Macbook Pro Retina 15, bylo zapotřebí pořídit redukci. Byla zvolena redukce Thunderbolt to Ethernet, která může být připojena k síti 10/100/1000BASE-T, takže může zvládnout připojení 1 Gbit/s.

Na obrázku č.6 vidíme všechny potřebné údaje, které útočník potřebuje, je to přihlašovací jméno, heslo a jméno hostitele. Pokud se tyto údaje k útočníkovi dostanou, může napáchat v našem případě na webové stránce nevyčíslitelné škody.

Co se praxe týče, tato metoda není pro získání přístupových údajů (na FTP server) útočníky nejpoužívanější. Nejčastěji jsou údaje získávány z automatického uložení hesel a opět zde největší roli hraje lidský faktor, pokud by uživatel neukládal hesla do zařízení, nedocházelo by k tomu. Může zde dojít k několika scénářům, jak se útočník dostane k těmto uloženým údajům. Může to být nevyžádaný fyzický přístup k PC, nebo škodlivý software, který se může dostat do zařízení skrz nežá-

doucí elektronickou poštu nebo instalací programu z neověřeného zdroje. Po získání přístupových údajů je na útočníkovi, jestli webovou stránku modifikuje pro své účely nebo ji znepřístupní.

6.4.1 Návrh na zabezpečení

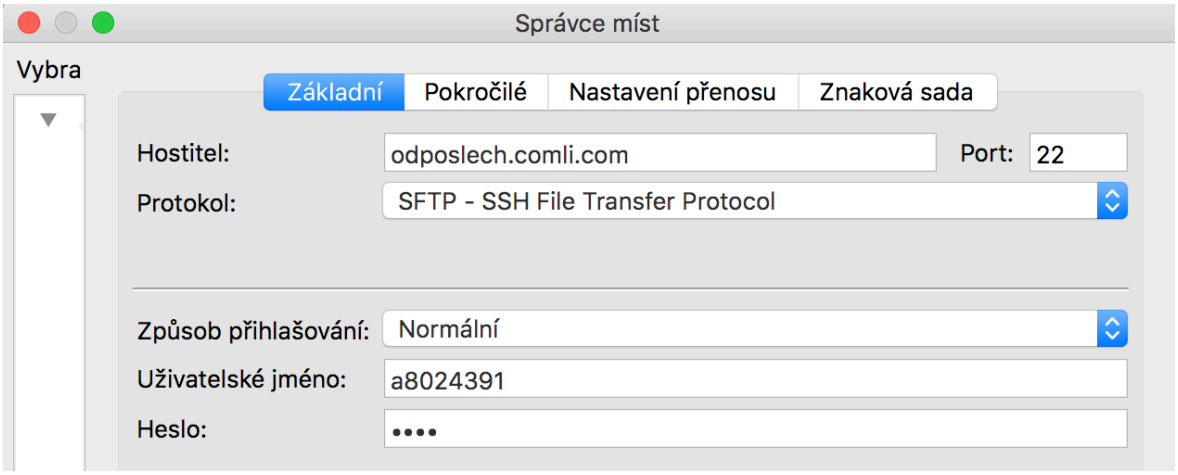
Zabezpečení FTP lze provést dvěma způsoby. Buď pomocí SSH, nebo pomocí SSL/TLS. Pro ukázku byla vybrána metoda s SFTP, tedy metoda s SSH. Pro demonstraci zabezpečení byl použit FTP klient Filezilla, který je zdarma ke stažení na oficiálních stránkách.

Pro ověření přihlášení pomocí veřejných klíčů potřebuje program Filezilla znát veřejné klíče, které má použít. Klíč je možné vygenerovat pomocí příkazů v Terminálu operačního systému OS X. Pro vygenerování veřejného klíče použijeme příkaz **ssh-keygen –t rsa**. Po zadání tohoto příkazu nás Terminál vyzve k cestě uložení tohoto klíče a po potvrzení je třeba zadat heslo uživatele.

```
Last login: Wed May  4 15:11:53 on console
Radek-MBP:~ radekkudela$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/radekkudela/.ssh/id_rsa):
Created directory '/Users/radekkudela/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/radekkudela/.ssh/id_rsa.
Your public key has been saved in /Users/radekkudela/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:LxVguEBzzV8N3q3o4RK8jt8pF9yajxniZ9BPqlReXOM radekkudela@Radek-MBP
The key's randomart image is:
+---[RSA 2048]----+
|    .o .+o   .o  |
|     .o..o. ..... |
|      . . .... ..o|
|       .  ... o.o.|
|        S +o+.+E  |
|         o.B+oo   |
|        . *.=B    |
|         *.+B=.   |
|        ..=*=..   |
+----[SHA256]-----+
```

Obr. 7 : Generování veřejného klíče, Zdroj: autor

Jakmile je vygenerovaný klíč k dispozici, je potřeba ho vložit do programu Filezilla. Pro tento krok musíme jít do nastavení programu a v záložce SFTP zvolíme přidat soubor s klíčem a vybereme námi vygenerovaný klíč. Poté vyskočí upozornění, že tento klíč není podporován aplikací Filezilla, a program vyzve pro převedení na podporovaný formát. Zvolíme pole ano a potvrdíme heslem zařízení.



Obr. 8 : Nastavení SFTP, Zdroj: autor

Pro nastavení SFTP v programu Filezilla bylo použito nastavení, které je zobrazeno na obrázku č. 8. Byl použit port 22, který je pro určen pro SSH. Uživatelské jméno a jméno hostitele bylo zvoleno podle přidělených údajů od poskytovatele služby.

```
00 00 19 00 6f 08 00 00  66 42 57 90 00 00 00 00   ....o... fBW.....
12 6c 99 09 80 04 cc a6  00 08 02 2c 00 20 c9 d0   .l...... ...,. ..
45 d7 19 00 4f 62 00 38  20 04 18 d6 99 85 70 f0   E...Ob.8  .....p.
e9 aa aa 03 00 00 00 08  00 45 10 00 7c 7c 39 40   ........ .E..||9@
00 39 06 2d 49 55 76 80  0e c0 a8 01 bd 00 15 c4   .9.-IUv. ........
86 8e 23 ff 62 43 82 2d  f2 80 18 00 82 67 e2 00   ..#.bC.- .....g..
00 01 01 08 0a 85 f2 85  c6 1f e3 e9 c6 17 03 03   ........ ........
00 43 46 a6 55 f1 69 84  92 2e 46 a2 09 f8 46 10   .CF.U.i. ..F...F.
96 ef 5c b2 81 da 32 53  72 c4 31 56 80 ee 46 f0   ..\...2S r.1V..F.
d4 bb fb 74 d6 cd bc c7  09 b3 4b 09 64 47 70 36   ...t.... ..K.dGp6
79 f0 d4 3e 87 10 e3 76  3c c6 e6 93 22 c1 af cf   y..>...v <..."...
29 29 93 b5 e7 15 89 13  ae                        )).....  .
```

Obr. 9 : Zachycená komunikace po nastavení šifrování, Zdroj: autor

Jak můžeme vidět na obrázku č.9 ze šifrované komunikace nemůže útočník vyčíst údaje potřebné pro získání přístupu ke službě.

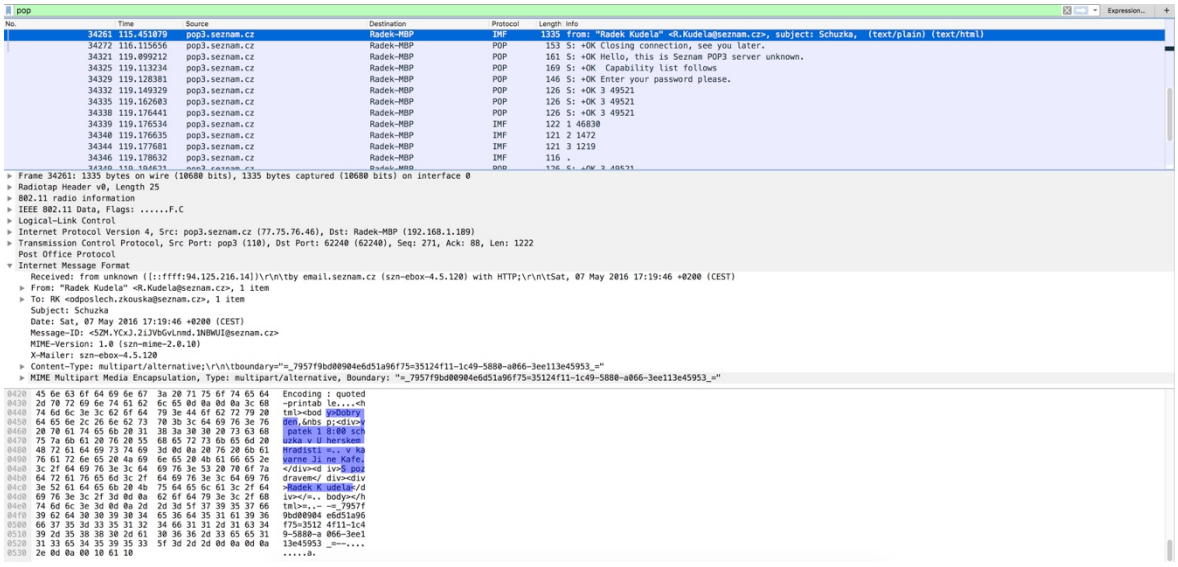
FTP protokol je v dnešní době stále hojně využíván a někteří poskytovatelé, kteří provozují webhosting neumožňují šifrované spojení. Proto pokud uživatel přistupuje ke serveru FTP, měl by být obezřetný a zkontrolovat si zabezpečení služby před přihlášením. Když není služba zabezpečená, mělo by být použito šifrování pomocí SSL/TLS protokolů nebo pomocí SSH. Šifrování dá uživateli jistotu, že bude mít zabezpečenou službu a bude imunní vůči odposlechu, a tak udrží své data v bezpečí. Uživatel dále musí dbát na základní bezpečnostní doporučení, kterými jsou neukládat si svá hesla v zařízení, nepoužívat administrátorský účet a neinstalovat

aplikace z neověřených zdrojů. Všechna základní doporučení jsou popsána v kapitole bezpečnostní doporučení [24] [25] [33] [34] [35] .

6.5 POP

POP neboli Post Office Protocol je využíván pro příjem pošty. Je využívaný uživateli zvláště v emailových klientech, kde si mohou vybrat mezi IMAP a POP protokolem pro příjem pošty. V pořadí je to 3. verze protokolu, využívá port 110, který není zabezpečený žádným způsobem šifrování. Tedy pokud poskytovatel nepoužívá pro zabezpečení tohoto portu TLS šifrování. Většina poskytovatelů na portu 110 poskytuje alespoň šifrovanou autentizaci, ale obsah samotné zprávy je při odchycení komunikace možno přečíst, stejně jako by člověk neměl posílat poštou důležité zprávy nebo je říkat na veřejnosti, neměl by je ani zasílat emailem pokud si není jistý, že má zabezpečenou komunikaci. Jedním z bezpečných způsobů, jak používat email, je používat pro komunikaci službu PGP, tu mimo jiné používá i Edward Snowden, který se proslavil vynesením informací z americké NSA.

Pro demonstraci bezpečnosti protokolu POP byla vybrána služba od nejznámějšího českého poskytovatele seznam.cz. Jako emailový klient, byl zvolen program Thunderbird od firmy Mozilla Corporation. Program je ke stažení zdarma na oficiálních stránkách mozilla.org. Nastavení adres pro příjem pošty bylo nastaveno pomocí údajů, které jsou zveřejněny na oficiálních stránkách podpory poskytovatele. Adresa serveru pro příchozí poštu je pop3.seznam.cz a port námi použitý byl 110.

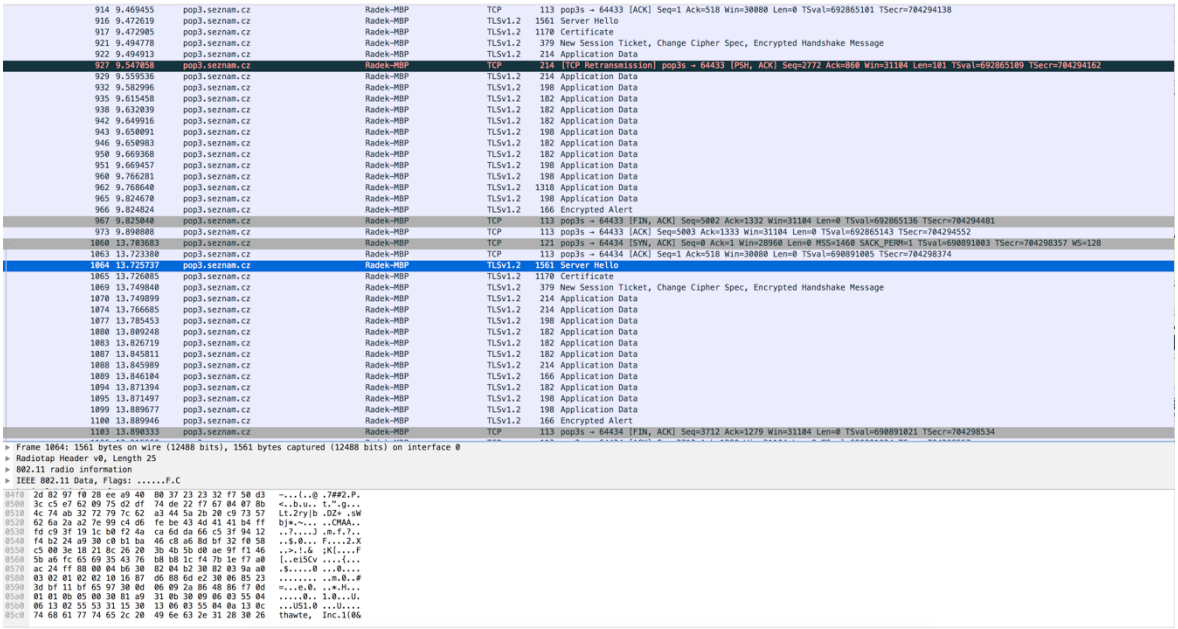


Obr. 10: Zachycená komunikace POP, Zdroj: autor

Na obrázku č.10 je vidět zachycený paket s příchozí zprávou. Text, který je poslaný ve zprávě, je ve formátu HTML. Pokud útočník zachytí paket s příchozí poštou, může si přečíst obsah zprávy. Pro běžného uživatele se tady vyskytuje nebezpečí, pokud přenáší ve své zprávě důležité informace, ty pak mohou být zneužity. V prostředí firmy však může tento únik informací znamenat nevyčíslitelné škody.

6.5.1 Návrh na zabezpečení

Zabezpečení Post Ofiice Protocol je možné pomocí šifrovacích protokolů. První, co uživatel musí udělat pro zabezpečení POP, je změnit port z původního 110 na 995. Tento port je určený pro POP3S, SSL. Po změně na tento port je veškerá příchozí komunikace POP šifrována a uživatel tak může bezpečně stahovat poštu i na nezabezpečené síti. Pro ochránění soukromí je tento krok nezbytně nutný.



Obr.11: Zachycená šifrovaná komunikace POP3S, Zdroj: autor

Jak můžeme názorně vidět na obrázku č.11 veškerá komunikace s pop3.seznam.cz probíhá v šifrované podobě. Poskytovatel služby používá na portu 995 TLSv1.2. Jde o nejnovější verzi protokolu, kde dosud nejsou známy žádné útoky. Považuje se za bezpečný.

Port 995 je nezbytný pro bezpečnou komunikaci mezi serverem poskytovatele a poštovním klientem. Proto by měl uživatel při používání emailové služby přes klienta zkontrolovat port, na kterém POP běží. Jak je vidět ze zachycené komunikace POP na portu 110, je sice zabezpečen od poskytovatele seznam.cz proti odposlechu hesel, ale ne proti odposlechu zpráv, které v sobě nesou zprávu, která je ve formátu HTML. Důležité zprávy, které mají nějakou hodnotu, by neměli

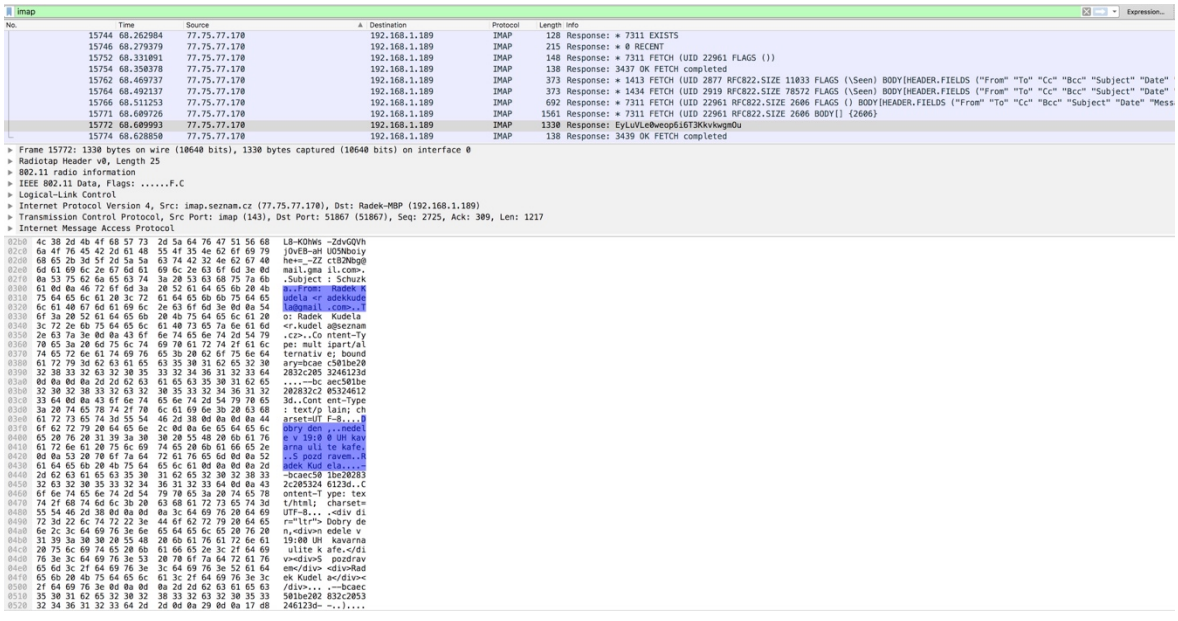
být pomocí elektronické pošty vůbec přenášeny. Bezpečnost šifrování může být dočasná a chyby v protokolu nejsou opraveny ze dne na den. Dalším důvodem, proč přijímat nebo posílat zprávy, je, že jsou fyzicky uloženy v zařízení, a pokud se útočník zmocní zařízení, tak uživateli šifrování pomocí TLS/SSL nepomůže [24] [25] [36] [37] [38].

6.6 IMAP

IMAP slouží stejně jako POP pro příjem pošty. Výhodou IMAP je, že umožňuje připojení více zařízení současně. Pro někoho může mít tu nevýhodu, že vyžaduje trvalé připojení, o čemž můžeme v současné době silně spekulovat. Zprávy a složky jsou uloženy na serveru a do zařízení se stahují jen nezbytná data. Pokud otevřeme poštovního klienta a aktualizujeme zprávy, stáhne se do zařízení pouze hlavička a teprve až po rozkliknuti zprávy se stáhne do zařízení celá zpráva.

Stejně jako u POP poskytuje většina providerů IMAP na portu 143 alespoň zabezpečenou autentizaci. Ostatní komunikace již probíhá v nešifrované podobě. Útočník zde může číst obsah zprávy bez jakéhokoli úsilí. Další výhodou pro útočníka je, že může snadno získat databázi emailových adres a posílat na ně nevyžádanou poštu.

Pro demonstraci bezpečnosti IMAP protokolu byl vybrán port 143. Emailová schránka je zaregistrovaná u poskytovatele seznam.cz a jako emailový klient byl stejně jako u POP použit emailový klient Mozilla Thunderbird. Adresa IMAP pro propojení se serverem je imap.seznam.cz. Na portu 143 je implementováno zabezpečení autentizace a ostatní komunikace je nešifrovaná.

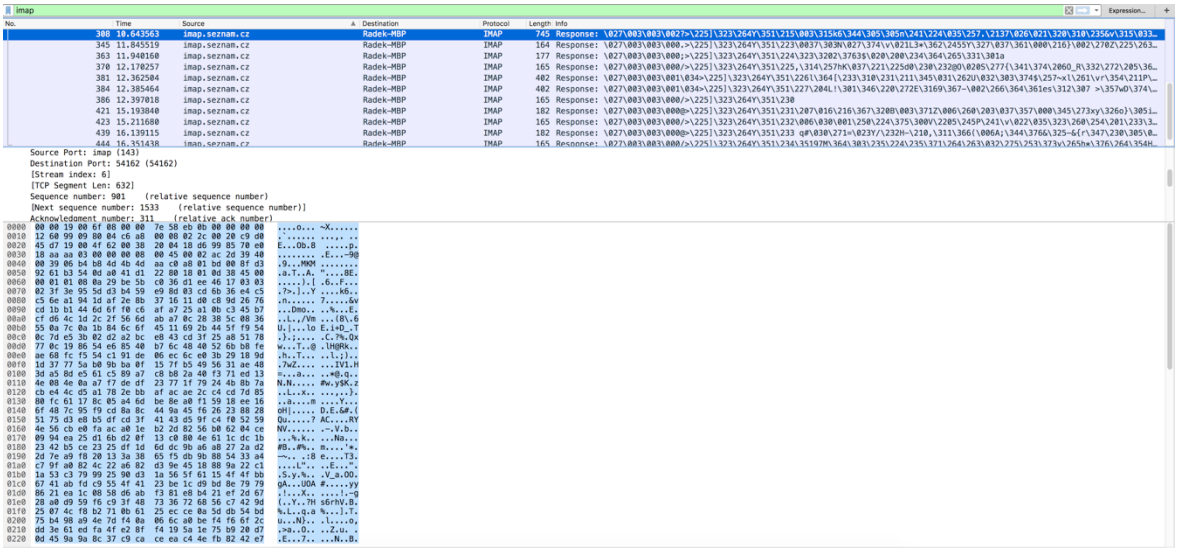


Obr. 12: Zachycená komunikace IMAP, Zdroj: autor

Obrázek č.12 ukazuje zachycenou komunikaci IMAP protokolu a v dolní části zobrazuje obsah zachyceného paketu s celým obsahem zprávy. Text je opět ve formátu HTML a je tak snadné ho přečíst. Port 143 je pro bezpečnou komunikaci nepřípustný a uživatel by měl zvážit jeho využití, zvláště pokud používá pro svou potřebu veřejné Wi-Fi sítě.

6.6.1 Návrh na zabezpečení

Zabezpečení IMAP je stejné jako u POP, a to je používat jiný port, na kterém poskytovatel garantuje šifrovanou komunikaci pomocí STARTTLS nebo TLS/SSL. Uživatel má na výběr port 993 nebo port 143. Oba tyto porty mohou být šifrované, ale pouze za správného nastavení emailového klienta. Poskytovatel služby seznam.cz umožňuje šifrování STARTTLS na portu 143 a na portu 993 šifrování pomocí SSL/TLS.



Obr. 13: Zachycená komunikace IMAP port 143, STARTSSL, Zdroj: autor

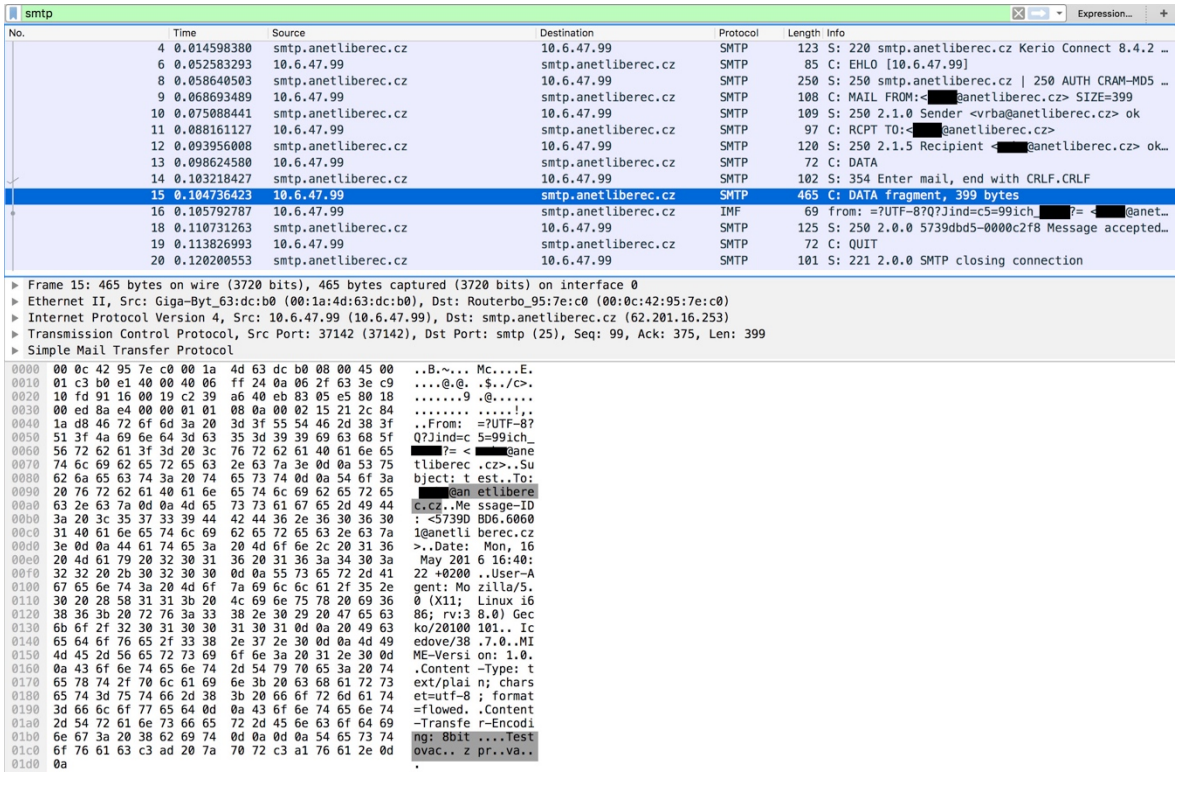
Z obrázku č.13 je vidět, že po nastavení šifrování na portu 143 je nečitelné, proto by uživatel měl dbát při natavování emailového klienta na to, aby v poli šifrování při nastavování portu 143 neměl zadané šifrování „žádné“. Pokud není tato možnost k dispozici, musí nastavit port 993, kde je nastavené automaticky šifrování pomocí TLS/SSL [37] [39] [40] [41].

6.7 SMTP

SMTP protokol je určen k odesílání elektronické pošty. Je využíván především v emailových klientech, bez jejichž použití by nebylo možné odesílat poštu. Protokol může pracovat na několika portech. Těmi jsou port 25, port 465 nebo 587, které podporuje většina poskytovatelů elektronické pošty. Port 25 je všemi velkými poskytovateli zablokován kvůli spamu. Ani firewall systému nedovoluje tento port využívat pro odesílání pošty, a pokud ho uživatel chce požívat, musí ho povolit v nastavení firewallu.

Protokol na portu 25 není využíván z toho důvodu, že nemá šifrovanou odchozí komunikaci, a tak je možné tento protokol odposlouchávat. Pokud útočník získá přístup k síti, zachycené pakety si může přečíst ve formátu HTML, a to představuje obrovské riziko pro únik informací. Port 25 je stále využíván firmami v rámci vnitřních sítí. Většina firem si myslí, že bezpečnost komunikace v rámci vnitřní sítě si ohlídají, ale ať někdo ze zaměstnanců nebo z útočníků, kteří získají přístup k síti, mohou získat přístup také k citlivým datům.

Ke zkoumání bezpečnosti SMTP protokolu bylo nutné najít prostředí, kde by bylo možné uskutečnit tuto demonstraci, proto bylo osloveno několik firem, které mají vnitřní síť a běží zde SMTP na portu 25. Tímto bych chtěl poděkovat firmě A-net Liberec s.r.o za umožnění přístupu k jejich síti.

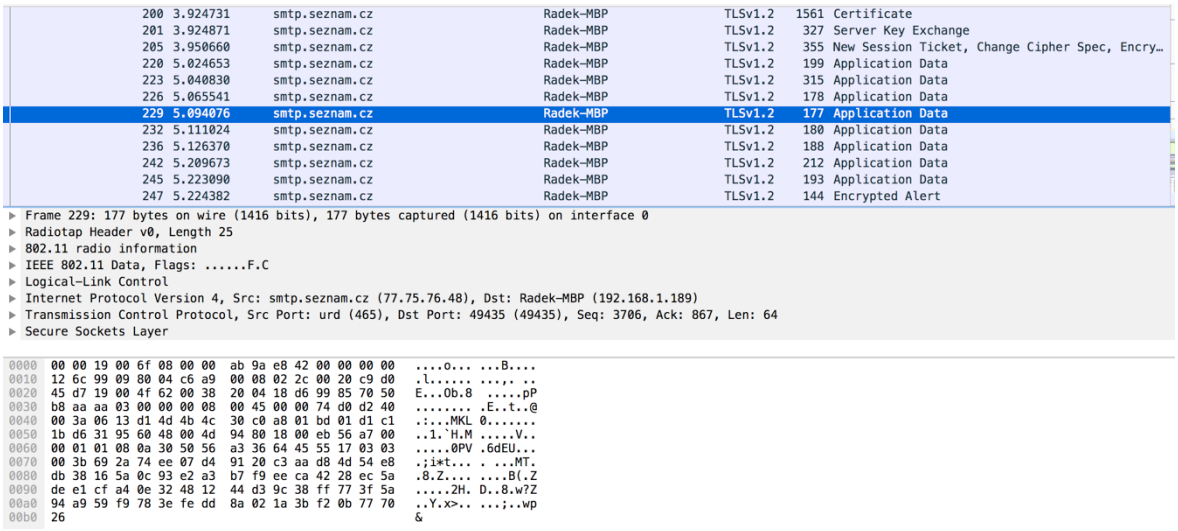


Obr. 14: Zachycená komunikace SMTP port 25, Zdroj: autor

Obrázek č. 15 nám jasně ukazuje odchycenou komunikaci v nezašifrované podobě. Ze zachycené komunikace je možno zjistit obsah zprávy, komu a od koho byla poslána, a také obsah samotné zprávy. Pro útočníka, který získá přístup k vnitřní síti, může tato nezabezpečená komunikace představovat bohatý zdroj informací.

6.7.1 Návrh na zabezpečení

SMTP je možné zabezpečit pomocí šifrovacích protokolů, které zajistí to, že veškerá odchozí komunikace bude šifrovaná a útočníkovi minimálně ztíží přístup k informacím. Využít lze port 465, který podporuje drtivá většina poskytovatelů této služby. Port 465 na kterém běží SMTPS již v sobě nese zabezpečení ve formě TLS/SSL.



Obr. 15: Zachycená komunikace SMTP port 465, Zdroj: autor

Jelikož nebyl umožněn jakýkoliv zásah do sítě firmy A-net Liberec s.r.o z pochopitelných důvodů, bylo simulováno zabezpečení SMTP na elektronické poště od poskytovatele seznam.cz. Byl využit port 465, kde nám poskytovatel nabízí šifrování komunikace pomocí TLS, v tomto případě v doposud nejnovější verzi TLSv1.2. Všechna odchozí komunikace je šifrována. Samotné šifrování odchozí komunikace data nezabezpečí. Jedna z možností je, když se útočník dostane do uživatelova zařízení, provést přesměrování SMTP na útočníkův server [37] [41] [42] [43].

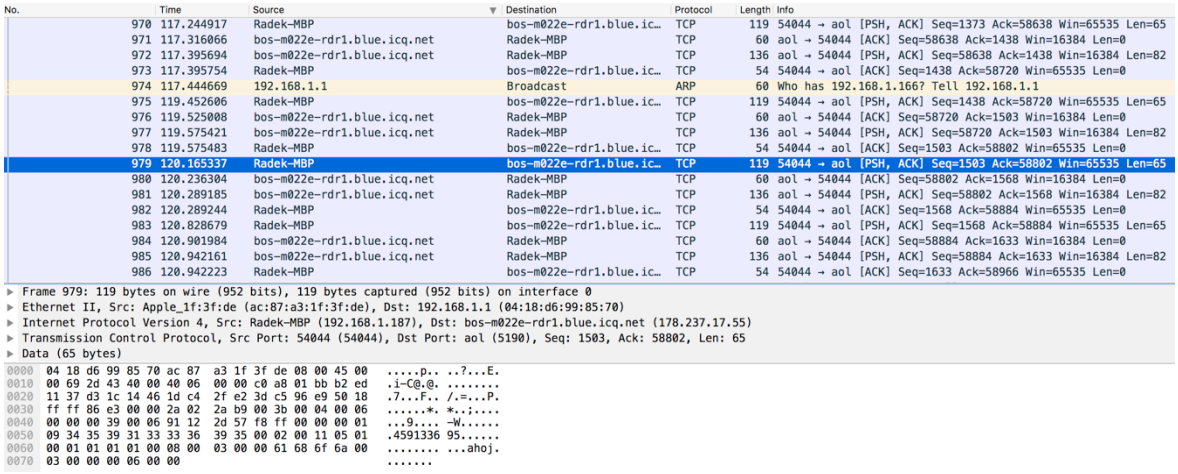
6.8 ICQ

ICQ je komunikační nástroj nebo stejnojmenný protokol, který je stále využíván. Podle serveru bloomberg.com má 11 milionů aktivních uživatelů, kteří minimálně jednou týdně použijí tento

protokol a má více než 100 milionů registrovaných uživatelů. Protokol byl vyvinut v roce 1996 a rychle si získal svou oblibu a stal se nejpoužívanějším protokolem pro tzv. „instant messaging“.

Existuje několik komunikačních nástrojů, které umožňují propojení s ICQ účtem, neznámějšími jsou ICQ klient, Miranda IM a QIP. Co se týče bezpečnosti, každý z klientů ji pojímá jinak. Zatímco ICQ nedovoluje spustit starší verze a nejnovější verze podporují šifrování protokolu, Miranda IM a QIP se vůbec nesnaží mít komunikaci zašifrovanou.

Pro demonstraci bezpečnosti protokolu byl vybrán komunikační nástroj Miranda Instant Messenger verze 0.8.27. Oproti ICQ klientu má tento nástroj výhodu tu, že nijak nezatěžuje zařízení a zabírá minimum paměti, neobsahuje žádné reklamy, je přehledná a podporuje mimo ICQ protokolu ještě IRC, AIM, MSN, Skype, Jabber, Yahoo!, Messenger aj.

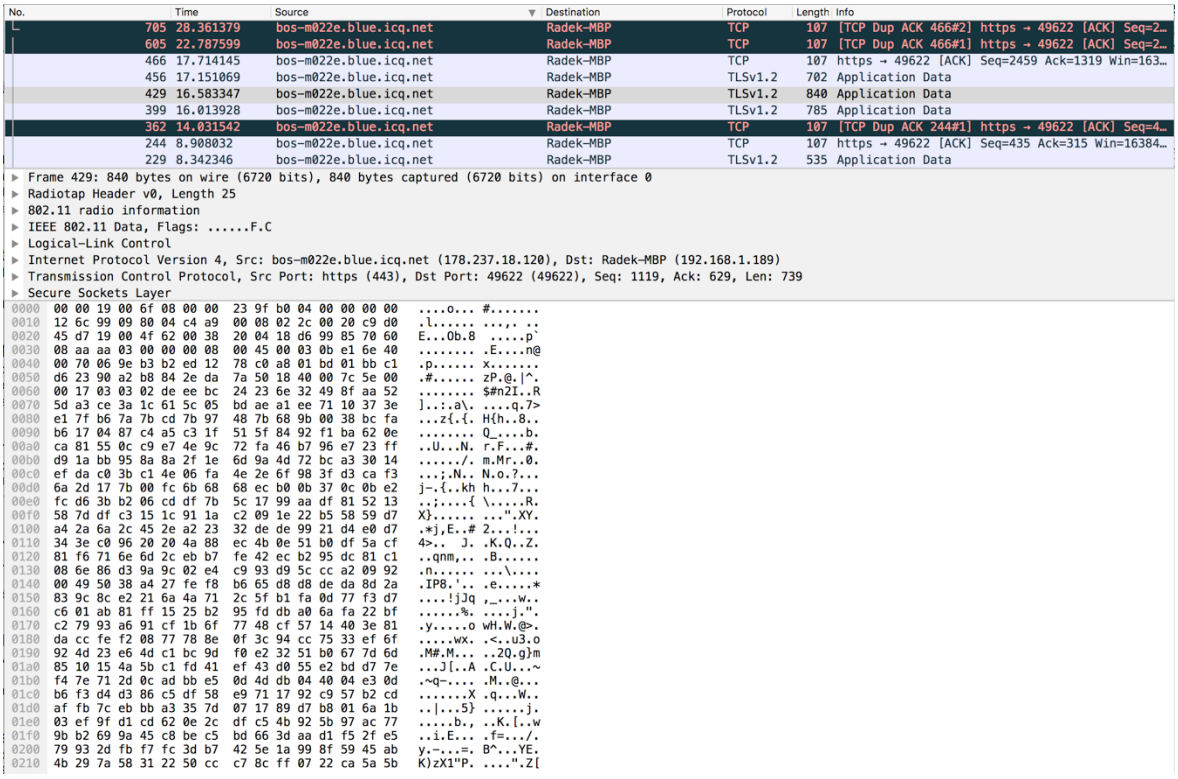


Obr. 16: Zachycená komunikace ICQ protokol, Zdroj: autor

Ze zachyceného paketu na obrázku č.15 je vidět, s jakým účtem uživatel komunikuje a jakou zprávu mu zasílá. Účet uživatele představuje devítimístné číslo. V našem případě je to číslo 459133695.

6.8.1 Návrh na zabezpečení

Stejné jako u všech protokolů, je možné i u tohoto zabezpečit odchozí komunikaci pomocí šifrovacích protokolů TLS/SSL. Starší verze programu ICQ a Miranda IM tuto funkci podporují, ale musí být ručně nastavena, jelikož při prvotním instalaci tato funkce povolena není. Novější verze mají tuto funkci již povolenou v základní verzi, a proto se uživatel nemusí bát o to, že by jeho odchozí komunikace nebyla šifrována. Proto je velmi důležité, abychom používali nejnovější verze programu, jelikož staré verze podporují pouze zabezpečení v podobě již nedoporučovaných SSL a MD5.



Obr. 17 Odchycená šifrovaná komunikace ICQ, Zdroj: autor

Pro zabezpečení byla použita nejnovější verze ICQ 10.0 10242. Je také třeba zmínit, že firma Digital Sky Technologies, která je vlastníkem této aplikace, nedovoluje použití starých verzí tohoto programu. Tímto krokem zamezí tomu, aby se útočník dostal přes známé chyby v programu do uživatelova zařízení, a také zajistí to, že odchozí komunikace je šifrována [44] [45].

6.9 Shrnutí

V následující tabulce je shrnutí všech používaných portů pro POP, IMAP, SMTP, HTTP a FTP. Zabezpečení komunikace a autentizace taky záleží ve velké míře na poskytovateli služby, proto jsou v tabulce u některých protokolů uvedeny dva rozdílné pojmy.

Protokol	Port	Zabezpečení
POP3	110	Žádné nebo TLS
POP3S	995	TLS
IMAP	143	žádné nebo TLS
IMAPS	993	TLS
SMTP	25 nebo 625	žádné nebo TLS
SMTP	587	TLS
SMTPS	465	SSL
HTTP	80	Žádné
HTTPS	443	SSL/TLS
FTP	20	Žádné
SFTP	115	SSH
FTPS	21 nebo 990	TLS/SSL

Tab. 1: Přehled portů a zabezpečení, Zdroj: autor

Chce-li uživatel využívat bezpečnou komunikaci, měl by používat jen zabezpečené protokoly. Samotné šifrování nezabrání úniku dat. Získá-li útočník přístup k síti, může např. na zabezpečené SMTP útočit pomocí kombinace sociálního inženýrství a malwaru, který může do zařízení nainstalovat keylogger. Ten je konstruován na to, aby získal ze zařízení hesla. Dále je možné přesměrovat oběť na vlastní SMTP a díky tomu získá útočník přístupové údaje ke službě.

Je důležité poznamenat, že protokoly, které jsou imunní vůči odposlechu nejsou imunní vůči sociotechnikám [26].

Celá praktická část bakalářské práce se zabývá pouze zabezpečením vůči odposlechu, nikoli proti ostatním druhům útoků, jelikož rozsah práce by musel být několikanásobně větší. Popsány zde byli jen ty nejpoužívanější protokoly, aby bylo demonstrováno, za jakých podmínek jsou protokoly zabezpečené vůči odposlechu [24] [25] [37].

7 BEZPEČNOSTNÍ DOPORUČENÍ

Pro zachování bezpečnosti komunikace se musí dodržovat bezpečnostní doporučení, a uživatel by měl být také seznámen se základními typy útoků, které jsou založeny na sociotechnikách. Těchto pravidel je velká řada, nelze je zde všechny vyjmenovat, proto byla vybrána jen ty základní.

7.1 Aktualizace

Aktualizace jsou jedním z nejzákladnějších zabezpečeních, předchází se tak napadnutí zařízení přes chyby v programech. Čím častěji je tedy systém aktualizován, tím větší je odolnější proti zranitelnosti z venčí. Aktualizace jsou zbytečné, pokud stáhneme nelegální distribuci SW. Ty mohou nést škodlivý software, který si stáhne svá data a ty se tváří jako aktualizace. Doba, za kterou se aktualizace od objevení chyby v systému dostanou k uživateli, se uvádí v řádech dnů, záleží na výrobci. V průměru se však jedná o dobu 6 dnů. Pokud nám tedy výrobce umožňuje automatické aktualizace, měl by uživatel využít tuto možnost. Pokud tedy uživatel chce mít zabezpečenou komunikaci na základní úrovni, měl by udržovat své komunikační nástroje aktualizované.

7.2 Antivirový program

Antivirový program odráží útoky nevyžádaného a škodlivého softwaru. Dennodenně se na síti objevuje nějaký nový škodlivý software, a proto by uživatel měl používat kvalitní antivirovou ochranu, která je aktualizovaná, protože denní aktualizace jsou základem bezpečného zařízení. Antivirový program, by neměl být vypnutý z toho důvodu, že pokud je nainstalovaný a neběží na pozadí, nechrání zařízení. Při přístupu ke službám by mělo být dbáno na to, aby antivirový program měl nejnovější aktualizaci a běžel na pozadí.

7.3 Firewall

Firewall řeší základní zabezpečení datové komunikace. Firewally s vyšším stupněm zabezpečením monitorují veškerou odchozí a příchozí komunikaci, proto by měl být na zařízení nainstalován firewall, který tuto funkci podporuje. Obousměrné firewally tak zvyšují zabezpečení a chrání uživatelská data. Tyto firewally si nastavují svá pravidla, a tak si je uživatel nemusí nastavovat sám, když firewall pracuje špatně nebo nereaguje. Pokud by tato funkce nebyla, musel by uživatel vymazat všechna pravidla a postupně si nastavit nová [20].

7.4 Administrátorský účet

Administrátorský účet by měl být pro běžné uživatele, kteří používají své zařízení pro běžnou práci, nepřístupný. Nepovolí provádět akce, které jsou pro šíření škodlivého softwaru potřebné. Další výhodou je, že minimálně ztíží nevyžádané osobě změnit nastavení zařízení. Doporučení tedy je, přihlašovat se pod běžným účtem a využít administrátorský účet pouze pro změnu nastavení nebo instalaci nového softwaru. Zvláště nezkušeným uživatelům je tento krok silně doporučen.

7.5 Záloha dat

Záloha dat na zařízení by měla být samozřejmostí. Pokud používáme důležitá data, měla by být zálohována minimálně na dvou místech. Vyhneme se zbytečným komplikacím při ztrátě nebo poškození zařízení. Data, která jsou uložená na jakémkoliv, nosiči by měla být šifrována, aby k nim útočník nezískal lehce přístup.

7.6 Zdroje

Na zařízení by měl být instalován software jenom z oficiálních zdrojů, a pokud uživatel hledá software jemu potřebný, měl by ověřit, jestli se jedná o důvěrný software k tomu určený. Po nainstalování softwaru z neoficiálních zdrojů, může dojít k nainstalování nežádoucího softwaru, který může uživateli narušit znatelně soukromí. Toto doporučení je jedním ze základních opatření proti nežádoucímu softwaru a uživatel by měl používat pouze legální a ověřený software.

.

7.7 Bezpečnostní doporučení na síti

Existuje několik doporučení pro bezpečnost na síti. V této kapitole jsou popsány ty nejdůležitější.

7.7.1 Ověření pravosti

Přistupujeme-li k webové stránce, neměli bychom na tuto stránku vstupovat pomocí klinutí na link umístěný na nedůvěryhodné stránce nebo kliknutím na logo v pochybném emailu a neznámé webové stránce. Uživatel by měl zadávat adresu ručně a zkontrolovat, jestli je adresa napsaná správně, protože podvodné techniky využívají právě překlepů. Dalším doporučením je používat šifrovanou verzi HTTP v případě, když uživatel přistupuje k nezabezpečené verzi tohoto protokolu vystavuje se zranitelnosti vůči odposlechu.

Pokud se uživatel nachází na webové stránce, má zabezpečení pomocí šifrovacího protokolu SSL/TLS, je adresní řádek označen zeleně. V případě červeného adresového pole by měl uživatel

informovat provozovatele a v žádném případě se nepřihlašovat. Zabezpečení stránky se může ověřit také pomocí kliknutí na ikonku uzamčeného zámku, která je obsažena v adresním řádku.

7.7.2 Přihlašování ke službě

Přihlašování ke službě můžeme provést pomocí několika způsobů. Tím nejméně bezpečným způsobem je přihlašování pomocí přihlašovacího jména a hesla, přesto je stále nejvíce používaným. Pokud uživatel používá tento způsob přihlašování, měl by dbát na základní pravidla pro bezpečnou autentizaci. Základním pravidlem je nikomu své přihlašovací jméno a heslo neposkytovat, pamatovat si je a hlavně je nikde neukládat. Je zde možnost ukládat hesla do programů pro uchování hesel tzv. „manažerů hesel“, tento způsob uložení hesel není doporučován. Samozřejmostí je mít silné heslo, které v sobě obsahuje malá a velká písmena, číslice a speciální znaky. Naopak by heslo v sobě nemělo mít uživatelské jméno, po sobě se opakující znaky nebo po sobě jdoucí znaky na klávesnici. Tato hesla jsou snadnou překážkou pro slovníkové útoky. Slabší hesla by měla být obměňována jednou za 3 měsíce.

Dalšími způsoby pro autentizaci jsou přístupové certifikáty, náhodně generovaná hesla přes SMS nebo jednorázové bezpečnostní kódy. Při zachování základních pravidel, jsou tyto způsoby autentizace bezpečnější než pomocí přihlašovacích údajů.

Uživatel by se neměl ke službě přihlašovat, pokud ho k tomu někdo vyzve pomocí emailu, vyskakovacího okna v prohlížeči nebo telefonu.

7.7.3 Cizí zařízení

Při přihlašování nebo komunikaci z cizího zařízení se uživatel vystavuje možnosti odposlechu hesel, komunikace a následným problémům s tím spjatými. Pokud se uživatel rozhodne připojit ke službě přes cizí zařízení, měl by ho restartovat a zkontrolovat aplikace běžící na pozadí. Ukončeny by měly být všechny programy, které komunikují s vnějšími servery. Také by mělo být zkontrolováno, jestli běží na zařízení základní ochrana, antivirový program nebo firewall popř. jejich správné nastavení. Při používání internetového prohlížeče vybrat ten nejaktuálnější, pokud systém obsahuje více než jeden. Nejlépe odstranit všechna prohlížeč a všechna jeho data a nainstalovat ho znovu. Upravuje-li uživatel dokument na zařízení, měl by použít vlastní datový nosič. Nečekané ukončení programu během používání může způsobit, že práce, kterou jsme prováděli, se může ukládat, proto by měl uživatel znovu spustit program a ujistit se, že nezůstal přihlášený nebo jeho práce nebyla uložena v úložišti zařízení [20].

7.7.4 Veřejné sítě

Užívání veřejných sítí v sobě skýtá několik nebezpečí. Pokud je uživatel připojený na veřejnou síť a posílá zprávy druhé osobě, měl by si být vědom toho, že je to bezpečné asi jako vést rozhovor uprostřed skupiny lidí. Na bezpečnost bezdrátových sítí se nemůže spolehnout ani tehdy, když jde o zabezpečenou síť pomocí hesla. Útočníci využívají několik sofistikovaných způsobů, jak se dostat do uživatelova zařízení nebo donutit uživatele, aby s ním spolupracoval. Využívají i soukromých hotspotů, které vytvoří pomocí mobilního zařízení a nazvou ho podle místa, kde se nachází. Po připojení na síť se uživateli objeví úvodní stránka, která vyzve uživatele např. pro vypnutí antivirové ochrany, firewallu nebo zadání kreditní karty za slib zvýšení rychlosti připojení. Po vypnutí uživatelovy ochrany může útočník do jeho zařízení umístit škodlivý software. Např. to může být škodlivý software, který umožňuje sledovat uživatelovu klávesnici a získat z ní přihlašovací údaje. Proti tomuto kroku je možná ochrana pomocí grafické klávesnice na obrazovce, kde je heslo zadáváno pomocí kliků na dané písmeno. Další možností je zneužití programu pro sdílení souborů. Tyto programy jsou rozšířené ve velkém množství a nejsou továrně zabezpečené nebo obsahují chyby, proto útočník v některých případech může na zařízení umístit i pokročilejší škodlivý software.

Doporučení, jak se tomuto útoku vyhnout, je vypnout program pro sdílení souborů a zakázat komunikaci ve firewallu. Pokud je uživatel vyzván pro změny certifikátu nebo pro zadání údajů, které by při určitých situacích nikomu nesdělil, měl by se takovým sítím vyhnout.

Využití veřejné sítě pro připojení pomocí VPN je bezpečnou variantou., Při dodržování základních pravidel pro bezpečné užívání sítě se vyhneme všem výše uvedeným útokům.

Po ukončení připojení na veřejné síti je dobré si zkontrolovat zařízení. Uživatel by měl provést restart systému, zvláště pokud je zařízení pouze uspáváno. Ujistit se, že jsou nainstalovány nejnovější aktualizace, které řeší záplatu chyb v zařízení. Zkontrolovat zařízení pomocí antivirového programu a pravidla nastavené ve firewallu. Otevřít v prohlížeči seznam rozšíření a odstranit ty, které nebyly přidány uživatelem a vymazat cache [20].

ZÁVĚR

Bezpečnost elektronické komunikace se v dnešní době stává stále více diskutovaným tématem. Vlády po celém světě by chtěli mít zadní vrátka a získat tak přístup k jimi požadovaným informacím, na druhé straně stojí uživatelé, kteří si přejí, aby jejich informace neshromažďoval někdo z třetích stran. Někteří uživatelé si ale neuvědomují, že to, co zveřejní na sociálních sítích, většinou zveřejní pro všechny a zabezpečení elektronické komunikace je před tímto nijak neochrání.

Práce má demonstrovat bezpečnost protokolů elektronické komunikace a ukázat za jakých podmínek je komunikace opravdu bezpečná. Z toho důvodu, že téma je poměrně obsáhlé a nebylo možné v práci ukázat všechny nebezpečí pro protokoly elektronické komunikace, jsou v této práci popsány, alespoň ty nejčastější bezpečnostní hrozby.

Teoretická část se zabývá hlavně způsoby, jakými je možné získat přístup k datům v zařízeních. Jsou zde popsány techniky, které jsou založené na sociálním inženýrství z toho důvodu, že útočník nemusí mít detailní vědomosti o informačních technologiích, aby získal přístup k citlivým datům. Tyto metody představují pro instituce největší nebezpečí. Dále jsou v této časti práce popsány protokoly, které patří mezi nejpoužívanější a jejich nedostatky vůči zabezpečení.

Praktická část názorně ukazuje odchycenou komunikaci, kde byly použity různé nástroje pro elektronickou komunikaci a dále bylo navrhnuto patřičné opatření na danou bezpečnostní hrozbu. Jak se ukazuje, systémy mohou být zabezpečeny sebelíp, ale proti pečlivě promyšleným sociotechnikám není odolné žádné zabezpečení.

Osobní pohled na tuto problematiku je pozitivní, ale pouze z hlediska pokročilejšího uživatele. Ten může ochránit svou odchozí komunikaci a může tak ochránit svá data před zneužitím. Stačí dodržovat několik pravidel pro bezpečnou komunikaci. Mezi nejdůležitější opatření patří rozhodně nevyužívání veřejných sítí, používání bezpečnostních prvků operačního systému a hlavní je mít zdravý úsudek nad tím, co může představovat riziko pro uživatele.

Nezkušený uživatel může mít na tomto poli obrovské problémy. Tito uživatelé mají v podvědomí nebezpečí, která hrozí, ale nedokáží se proti těmto útokům bránit. Jedním s mála příkladů je phishing. Ten názorně ukazuje chybu lidského faktoru. Neinformovanost při takových útocích hraje velkou roli.

ZÁVĚR V ANGLIČTINĚ

Nowadays, online communication security is becoming more and more of a discussed topic. On one hand, governments all around the world want to gain backdoor access to classified information, and on the other there are users who don't want to see their personal information gathered or shared by any third party. Some of those users, though, don't fully realize that what they share on social media is being shared with everyone and that because of that very reason, the security of electronic communication is unable to protect them.

This thesis demonstrates the security of electronic protocols and shows which criteria need to be met in order for communication to be considered secure. Because of the breadth and wide range of this topic, it wasn't possible for me to describe every single security threat - I stay focused on the most common ones instead.

The theoretical part deals mainly with the ways in which it's possible to gain access to device data. I describe techniques based on social engineering mainly because an attacker doesn't necessarily have to possess deep IT knowledge in order to gain access to sensitive data. These methods pose the biggest danger to institutions. Furthermore, I describe the most widely-used protocols and the errors in their security.

The practical part presents intercepted information obtained using different communication tools. For each of these I also proposed a solution or a precautionary measure. From what we see, though, no matter how secure the system is, they're usually vulnerable to carefully thought-through sociotechniques.

Personal outlook at this issue is positive, but only from an experienced user's perspective- one who can secure outgoing communication and one who is able to secure data from malfeasance or abuse. All it takes is to stick to a few simple rules. Some of the most important ones being: not using public networks, using your OS's security features and the most reliable one of course is to employ sound judgement when it comes to all the things that could become a threat.

An inexperienced used could struggle a lot in this field. These users all subconsciously know about all these threats, but are never able to defend themselves. One of few examples

being phishing, which clearly points to the human error. Lack of information plays a big part in all these attacks.

SEZNAM POUŽITÉ LITERATURY

[1] HARPER. Hacking - manuál hackera. Grada Publishing a.s., 2008. ISBN 8024713462.

[2] WHAT IS PASSWORD SNIFFING? Wisegeek [online]. Conjecture Corporation, 2016 [cit. 2016-04-10]. Dostupné z: http://www.wisegeek.org/what-is-password-sniffing.htm

[3] Password sniffing. Technopedia [online]. Conjecture Corporation, 2016 [cit. 2016-04-10]. Dostupné z: https://www.techopedia.com/definition/8798/password-sniffer

[4] Understanding Denial-of-Service Attacks. US-CERT [online]. Conjecture Corporation, 2016 [cit. 2016-04-10]. Dostupné z: https://www.us-cert.gov/ncas/tips/ST04-015

[5] Co je to phishing. Hoax [online]. Hoax, 2016 [cit. 2016-04-10]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[6] 5 Social Engineering Attacks to Watch Out For. Tripwire [online]. Tripwire, 2016 [cit. 2016-04-10]. Dostupné z: http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

[7] 5 BEST FREE NETWORK PACKET SNIFFER. Ilovefreesoftware [online]. Love Free Software, 2016 [cit. 2016-04-10]. Dostupné z: http://www.ilovefreesoftware.com/16/featured/5-best-free-network-packet-sniffer.html

[8] Sniffing: Odposlech datové komunikace. Itbiz [online]. Nintemedia, 2016 [cit. 2016-04-10]. Dostupné z: http://www.itbiz.cz/sniffing-odposlech-datove-komunikace

[9] HTTP. Pcmag [online]. The Computer Language Company, 2016 [cit. 2016-04-10]. Dostupné z: http://www.pcmag.com/encyclopedia/term/44501/http

[10] Simple Mail Transfer Protocol (SMTP). Technopedia [online]. technopedia, 2016 [cit. 2016-04-10]. Dostupné z: https://www.techopedia.com/definition/1710/simple-mail-transfer-protocol-smtp

[11] POP3. Techterms [online]. sharpened production, 2016 [cit. 2016-04-10]. Dostupné z: http://techterms.com/definition/pop3

[12] IMAP (Internet Message Access Protocol). Techtarget [online]. TechTarget, 2016 [cit. 2016-04-10]. Dostupné z: http://searchexchange.techtarget.com/definition/IMAP

[13] FTP. Techterms [online]. Sharpened production, 2016 [cit. 2016-04-10]. Dostupné z: http://techterms.com/definition/ftp

[14] NNTP. Techtarget [online]. TechTarget, 2016 [cit. 2016-04-10]. Dostupné z: http://searchnetworking.techtarget.com/definition/NNTP

[15] Bitmessage. Bitmessage [online]. BitTorrent, 2014 [cit. 2016-04-25]. Dostupné z: https://bitmessage.org/wiki/Main_Page

[16] About OpenPGP. OpenPGP [online]. OpenPGP Alliance, 2013 [cit. 2016-04-25]. Dostupné z: http://www.openpgp.org/about_openpgp/

[17] Secure Shell. TechTarget [online]. TechTarget, 2015 [cit. 2016-04-25]. Dostupné z: http://searchsecurity.techtarget.com/definition/Secure-Shell

[18] FIŠER, Jiří. Principy operačních systémů II [online]. Univerzita Jana Evangelisty Purkyně. 2007 [cit. 2016-04-18]. Dostupné z: http://ithil.ujep.cz/workspace/OS-2.pdf

[19] Certified Products. Common Criteria [online]. 2015 [cit. 2016-04-18]. Dostupné z: http://www.commoncriteriaportal.org/products/

[20] Bezpečnostní doporučení podrobně. Datové schránky [online]. Praha: Ministerstvo vnitra, 2015 [cit. 2016-04-25]. Dostupné z: https://www.datoveschranky.info/dulezite-informace/bezpecnostni-doporuceni-podrobne

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

[22] KALEEM, Zaib . *RFMON at WLAN* [online]. c2008 [cit. 2016-04-26]. Dostupný z WWW: <http://www.wlanbook.com/rfmon-monitor-mode/>.

[23] KOPECKÝ, Kamil, KREJČÍ, Veronika. RIZIKA VIRTUÁLNÍ KOMUNIKACE, 1.vyd. NET UNIVERSITY, s.r.o., 2010. 36 s. ISBN 978-80-254-7866-O.3.

[24] Data Security Management. DSM - data security management. 2, Praha : TATE International, s.r.o., 2012, Sv. XVI. ISSN1211-8737.

[25] SATRAPA, Pavel. IPv6: internetový protokol verze 6. 3., aktualiz. a dopl. vyd. Praha:CZ.NIC, c2011, 407 s. CZ.NIC. ISBN 978-80-904248-4-5.

[26] MALANÍK D., Bezpečnostní Politiky v Kontextu Bezpečnosti Informačních Systémů. In Bezpečnostní technologie, systémy a management 2013. Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2013, s. 1-4. ISBN 978-80-7454-289-3.

[27] How to get Wireshark running in Mac OS X. Fixed by vonnie [online]. fixed by vonnie, 2015 [cit. 2016-05-22]. Dostupné z: http://www.fixedbyvonnie.com/2015/04/how-to-get-wireshark-running-in-mac-os-x-yosemite/#.V0GfmmPyQ4M

[28] Sniffing in Monitor Mode with Airport. Diogo Monica [online]. Diogo Monica, 2015 [cit. 2016-05-22]. Dostupné z: https://diogomonica.com/sniffing-in-monitor-mode-with-airport/

[29] HTTP VS HTTPS. Instant ssl [online]. Comodo CA Limited, 2016 [cit. 2016-05-22]. Dostupné z: https://www.instantssl.com/ssl-certificate-products/https.html

[30] Zabezpečení webu protokolem HTTPS. Google [online]. San Francisco: Google, 2016 [cit. 2016-05-22]. Dostupné z: https://support.google.com/webmasters/answer/6073543?hl=cs

[31] SSL Server Test. Ssllabs [online]. Qualys, Inc, 2016 [cit. 2016-05-22]. Dostupné z: https://www.ssllabs.com/ssltest/

[32] Otestujte šifrovací schopnosti svého prohlížeče a systému. Magazín o bezpečnosti [online]. ZONER software, a.s., 2016 [cit. 2016-05-22]. Dostupné z: https://blog.sslmarket.cz/ssl/otestujte-sifrovaci-schopnosti-sveho-prohlizece-a-systemu/

[33] Security Risks of FTP. The hacker news [online]. thehackernews, 2016 [cit. 2016-05-22]. Dostupné z: http://thehackernews.com/2013/12/security-risks-of-ftp-and-benefits-of.html

[34] How To Use Filezilla to Transfer and Manage Files Securely. Digitalocean [online]. DigitalOcean™ Inc., 2016 [cit. 2016-05-22]. Dostupné z: https://www.digitalocean.com/community/tutorials/how-to-use-filezilla-to-transfer-and-manage-files-securely-on-your-vps

[35] Jak zabezpečit přístup k hostingu. Flops [online]. Flops, 2013 [cit. 2016-05-22]. Dostupné z: http://www.flops.cz/jak-zabezpecit-pristup-k-hostingu-ftps-sftp-ssh

[36] Here's how to send super-secure messages like Edward Snowden. Business insider [online]. Business Insider Inc., 2015 [cit. 2016-05-22]. Dostupné z: http://www.businessinsider.com/how-to-send-encrypted-messages-using-pgp-like-edward-snowden-2015-6

[37] Nastavení poštovního klienta. Cesky hosting [online]. THINline s.r.o., 2015 [cit. 2016-05-22]. Dostupné z: http://www.cesky-hosting.cz/pro-zakazniky/napoveda/nastaveni-postovniho-klienta.html

[38] Is the POP3 email protocol insecure? Metafilter [online]. MetaFilter, 2015 [cit. 2016-05-22]. Dostupné z: http://ask.metafilter.com/217775/Is-the-POP3-email-protocol-insecure-even-with-TLS

[39] SSL vs TLS vs STARTTLS. Fastmail [online]. FastMail Pty Ltd., 2015 [cit. 2016-05-22]. Dostupné z: https://www.fastmail.com/help/technical/ssltlsstarttls.html

[40] Jaký je rozdíl mezi POP3 a IMAP? Onehelp [online]. ONEsolution s.r.o., 2016 [cit. 2016-05-22]. Dostupné z: https://www.onehelp.cz/onebit/kb/jaky-je-rozdil-mezi-pop3-a-imap

[41] Email Protocols - POP3, SMTP and IMAP. Site ground [online]. SiteGround, 2016 [cit. 2016-05-22]. Dostupné z: https://www.siteground.com/tutorials/email/pop3-imap-smtp-ports.htm

[42] E-mail klient - odchozí pošta a různá místa. Živě [online]. Serafico investment s.r.o., 2013 [cit. 2016-05-22]. Dostupné z: http://www.zive.cz/poradna/e-mail-klient---odchozi-posta-a-ruzna-mista/sc-20-cq-474208/?consultanswers=1

[43] How to configure an SMTP server. Server smtp [online]. Delivery Tech, 2014 [cit. 2016-05-22]. Dostupné z: http://www.serversmtp.com/en/smtp-configuration

[44] Yahoo, ICQ chats still vulnerable. Cnet [online]. CBS Interactive Inc., 2014 [cit. 2016-05-22]. Dostupné z: http://www.cnet.com/news/yahoo-icq-chats-still-vulnerable-to-government-snoops/

[45] Nastavení ICQ. Mirandakex [online]. mirandakex, 2006 [cit. 2016-05-22]. Dostupné z: http://mirandakex.cz/nastavujeme/icq-plugin-icqoscarj/

[46] Protokol SSL/TLS - slabé šifry, zranitelnosti a jejich testování. Samuraj [online]. Samuraj, 2014 [cit. 2016-05-25]. Dostupné z: http://www.samuraj-cz.com/clanek/protokol-ssl-tls-slabe-sifry-zranitelnosti-a-jejich-testovani/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

OS	Operační systém.
Tzv.	Takzvaný.
FTP	FILE TRANSFER PROTOCOL.
HTTP	HYPERTEXT TRANSFER PROTOCOL.
SMTP	SIMPLE MAIL TRANSFER PROTOCOL.
POP	POST OFFICE PROTOCOL.
TLS	TRANSPORT LAYER SECURITY.
SSL	SECURE SOCKETS LAYER.
ICQ	I SEEK YOU.
SSH	SECURE SHELL.
IMAP	INTERNET MESSAGE ACCESS PROTOCOL.
SW	Software.
PGP	Pretty Good Privacy.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK