Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Bezpečnost přenosu dat a komunikace v internetu

Marek Zvelebil

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Marek Zvelebil

Informatika

Název práce

Bezpečnost přenosu dat a komunikace v internetu

Název anglicky

Security of data transfer and internet communication

Cíle práce

Hlavním cílem bakalářské práce je analyzovat způsoby ochrany zabezpečení dat v síti internet a navrhnout způsoby ochrany uživatelů.
Ochrana elektronických dat a elektronické komunikace bude řešena ve smyslu anonymizace a šifrování komunikace i dat pro uživatele internetu v ČR.

Metodika

Teoretická část práce bude analyzovat kritická místa v online prostředí u protokolů TCP/IP a DNS, definovat bezpečnostní rizika a potenciální hrozby. Práce bude definovat rizika vznikající při využívání internetu a bude vycházet ze studia odborných publikací.

Na základě zjištěných informací budou v praktické části práce navrženy způsoby, jak efektivně ochránit uživatele a jeho činnost v online prostředí.

Součástí návrhu bude komprace variant řešení pro ochranu uživatele pomocí šifrování, VPN (virtuální privátní síť) a sítě TOR (anonymní síť), případně dalších možností. Na základě zjištěných poznatků budou vyvozeny závěry.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

internet, bezpečnost, šifrování, VPN, TOR

Doporučené zdroje informací

KABELOVÁ, A., DOSTÁLEK, L. Velký průvodce protokoly TCP/IP a systémem DNS. Praha, 2012. 483 s. ISBN 978-80-251-2236-5

LEVICKÝ, D. Kryptografia a bezpečnosť komunikačných sietí. Košice, 2016. Elfa,s.r.o. 352 s. ISBN 9788080862541

LUDVÍK, M., ŠTĚDROŇ, B. Teorie bezpečnosti počítačových sítí. 2008. Computer Media. 98 s. ISBN 8086686353

MOJMÍR, K. Bezpečný internet. Praha, 2015. Grada Publishing,a.s. 184 s. ISBN 978-80-247-5453-6

Předběžný termín obhajoby

2017/18 ZS – PEF (únor 2018)

Vedoucí práce

Ing. Václav Lohr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 21. 10. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 10. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 11. 2017

Čestné prohlášení

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

V Praze dne: 30.11.2017 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Václavu Lohrovi, Ph.D. za vedení a cenné připomínky při zpracování bakalářské práce. Mé poděkování také patří přítelkyni a rodině za podporu během studií.

Bezpečnost přenosu dat a komunikace v internetu

Souhrn

Práce se zabývá problematikou bezpečnosti datového přenosu a komunikace v síti internet. Hlavním cílem je na základě analýzy způsobů zabezpečení dat a internetové komunikace navrhnout metody ochrany uživatelů. Metoda ochrany uživatele je řešena ve smyslu anonymizace, šifrování dat a komunikace uživatele internetu. V úvodu teoretické části jsou popsány základní protokoly a principy nutné pro připojení uživatele do internetu. Následující kapitoly se zaměřují na symetrické, asymetrické šifrování a hašovací algoritmy. Práce průběžně definuje rizika spojená s využíváním dané technologie a soustřeďuje se na varianty ochrany uživatele a protokoly zajišťující bezpečnost.

Praktická část analyzuje vhodné řešení pro specifické druhy uživatele pomocí komparace variant. Varianty jsou vyhodnoceny pomocí vícekriteriální analýzy variant, a nakonec autor výsledky interpretuje.

Klíčová slova: internet, bezpečnost, šifrování, VPN, TOR

Security of data transfer and internet communication

Summary

Concern of the paper is security of data transfer and communication via internet. Main aim is to design a method for user security based on analysis of data security options and internet communication. The user security method is discussed in terms of anonymization, data encryption and internet communication of the user. Basic principles and protocols needed for user internet connection are described in the beginning of the theoretical part. Concerns of following chapters are symmetric and asymmetric encryption and hash algorithms. The paper continually defines risks connected to usage of certain technology. Accent is put on various users' security systems and security protocols.

The practical part analyses suitable solutions for particular types of users by comparing these variations. Options are evaluated by multicriterial analysis. Subsequently the author interprets the results.

Keywords: internet, security, encryption, VPN, TOR

Obsah

1 Úvod **12**

2 Cíl práce a metodika **13**

2.1 Cíl práce 13

2.2 Metodika 13

3 Teoretická východiska **14**

3.1 Počítačové sítě 14

3.1.1 Síťové prvky 14

3.1.2 WIFI 14

3.2 TCP/IP 16

3.2.1 IP protokol a IP datagram 17

3.2.2 TCP a UDP 18

3.2.3 Zapouzdření dat v síti TCP/IP 18

3.3 DNS 19

3.3.1 Útoky na DNS 20

3.3.2 HTTP/HTTPS 20

3.4 Kryptografie 21

3.4.1 DES 21

3.4.2 3DES 22

3.4.3 AES 22

3.4.4 BLOWFISH 23

3.4.5 RC5 23

3.4.6 Bezpečnost šifrovacích algoritmů 23

3.5 Hašovací funkce 24

3.5.1 MD5 24

3.5.2 SHA-1 25

3.5.3 MAC 26

3.6 Symetrické šifrovaní v síťové komunikaci 26

3.6.1 Umístění šifrovacích funkcí 26

3.6.2 Distribuce klíčů 27

3.7 Kryptografie s veřejným klíčem 28

3.7.1 Kategorizace kryptografických systémů s veřejným klíčem 30

3.7.2 RSA 30

3.8 Digitální certifikát 31

3.9 VPN 32

3.9.1 Open VPN 33

3.9.2 PPTP 34

3.9.3 L2TP 34
3.9.4 IPSec 35
3.9.5 SSL/TLS 36
3.10 TOR 37
3.10.1 Princip funkce sítě TOR 38
3.10.2 Hidden Services 39
3.10.3 Bezpečnost TOR 40
3.10.4 Kombinace TOR a VPN/Proxy 41
3.11 Proxy server 42
3.12 Vybrané metody pro zpracování praktické části 42
3.12.1 Vícekriteriální rozhodování 43
3.12.2 Persona 44
4 Praktická část 45
4.1 Varianty 45
4.1.1 Kritéria 45
4.1.2 Stanovení person 46
4.2 Testovací uživatel č. 1 46
4.3 Vyhodnocení uživatele č. 1 49
4.4 Testovací uživatel č. 2 49
4.5 Vyhodnocení uživatele č. 2 51
4.6 Testovací uživatel č.3 52
4.7 Vyhodnocení uživatele č. 3 53
5 Závěr 54
6 Seznam použitých zdrojů 56

Seznam obrázků

Obrázek 1 Srovnání TCP/IP a ISO/OSI 17
Obrázek 2 IP hlavička 18
Obrázek 3 Zapouzdření dat v síti 19
Obrázek 4 Schéma použití veřejného a privátního klíče 29
Obrázek 5 Digitální certifikát 32
Obrázek 6 SoftEther podpora bezpečnosti 33
Obrázek 7 PPTP 34
Obrázek 8 AH hlavička 35
Obrázek 9 ESP hlavička 36
Obrázek 10 Schéma komunikace v TOR 39

Obrázek 11 Vytvoření řetězce TOR 39
Obrázek 12 Matice 43

Seznam tabulek

Tabulka 1Metoda totálních zkoušek 24
Tabulka 2 Srovnání verzí SHA 26
Tabulka 3 Varianty 45
Tabulka 4 Stanovení vah pro uživatele č. 1 47
Tabulka 5 Sestavení matice pro volbu metody zabezpečení 47
Tabulka 6 Sestavení kriteriální matice pro uživatele č. 1 48
Tabulka 7 Výpočet funkce užitku pro uživatele č. 1 48
Tabulka 8 Stanovení vah pro uživatele č. 2 50
Tabulka 9 Sestavení kriteriální matice pro uživatele č. 2 50
Tabulka 10 Výpočet funkce užitku pro uživatele č. 2 51
Tabulka 11 Stanovení vah pro uživatele č.3 52
Tabulka 12 Sestavení kriteriální matice pro uživatele č. 3 52
Tabulka 13 Výpočet funkce užitku pro uživatele č. 3 53

Seznam grafů

Graf 1 Výsledná míra užitku pro uživatele č. 1 49
Graf 2 Výsledná míra užitku pro uživatele č. 2 51
Graf 3 Výsledná míra užitku pro uživatele č. 3 53

1 Úvod

Bakalářská práce se zabývá tématem zabezpečení dat a elektronické komunikace v internetu. Uživatelé tuto celosvětovou síť používají pro komunikaci, nákupy online, výměnu informací a další různorodé činnosti. Při těchto činnostech putuje internetem velké množství osobních a citlivých firemních dat i finančních zdrojů. Většině uživatelů by vadilo, kdyby někdo sledoval jejich denní aktivity, monitoroval místa, jaká navštěvují, jejich názory, popřípadě zjišťoval, jaký mají soukromý majetek. Je tedy nutné řešit i to, že obdobné údaje se nacházejí online. Uživatelé internetu se nemohou spoléhat na to, že by jejich vlastní bezpečnost vyřešil někdo jiný a měli by se aktivně zamýšlet nad tím, zda jsou jejich informace a data přenášená v internetu v bezpečí. Hodnoty těchto informací jsou si dobře vědomi nejen kriminální živly, marketingové společnosti ale i vlády. Vyvíjejí tedy maximální snahu tato data získat. Útočníci se snaží získat přístupové údaje například k internetovému bankovnictví a účtům na sociálních sítích. Marketingové společnosti monitorují aktivitu uživatelů, aby mohli nabízet nejlepší produkt, nebo si vytvářely podklady pro své analýzy. Některé vlády intenzivně narušují soukromí uživatelů pod různými důvody či záminkami. Většina uživatelů jim práci značně zjednodušuje, nedostatečným zabezpečením plynoucím z neinformovanosti o rizicích spojených s využíváním této sítě. Z těchto důvodů je nutné chránit svá osobní data, firemní data a ztížit či minimalizovat možnost sledování uživatelů v síti internet. Tohoto cíle se dá dosáhnout pomocí šifrování a anonymizace. Pro řešení bezpečnostní problematiky je možno využít anonymizační služby TOR, nebo použití VPN a Proxy serverů. Uvedená řešení lze kombinovat pro zvýšení bezpečnosti a anonymity.

Cílem práce je podrobněji porovnat možná dostupná řešení a nalézt jejich nejvýhodnější způsoby použití pro vybrané skupiny uživatelů.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem bakalářské práce je analyzovat způsoby ochrany zabezpečení dat v síti internet a navrhnout způsoby ochrany uživatelů. Ochrana elektronických dat a elektronické komunikace bude řešena ve smyslu anonymizace a šifrování komunikace i dat pro uživatele internetu v ČR.

2.2 Metodika

Teoretická část práce bude analyzovat kritická místa v online prostředí u protokolů TCP/IP a DNS, definovat bezpečnostní rizika a potenciální hrozby. Práce bude definovat rizika vznikající při využívání internetu a bude vycházet ze studia odborných publikací.

Na základě zjištěných informací budou v praktické části práce navrženy způsoby, jak efektivně ochránit uživatele a jeho činnost v online prostředí.

Součástí návrhu bude komparace variant řešení pro ochranu uživatele pomocí šifrování, VPN (virtuální privátní síť) a sítě TOR (anonymní síť), případně dalších možností. Na základě zjištěných poznatků budou vyvozeny závěry.

3 Teoretická východiska

3.1 Počítačové sítě

Pro počítačové sítě existují dva druhy dělení. Nejpoužívanější dělení je dle rozlehlosti.

- LAN (Local Area Networks) - Jedná se o sítě omezené v rámci budov a podniků, slouží k sdílení prostředků, jako jsou data, aplikace, tiskárny.
- MAN (Metropolitan Networks) - Metropolitní sítě jsou svou rozlohou mezi LAN a WAN.
- WAN (Wide Area Networks) - Rozlehlé sítě z více propojených sítí LAN, MAN. Tvoří celosvětovou síť Internet (Horák a kol., 2006, s. 9-10).

3.1.1 Síťové prvky

Jednotlivá zařízení jsou mezi sebou propojena pomocí pasivních a aktivních prvků. Mezi pasivní prvky patří přenosové médium tedy optická vlákna, kroucená dvojlinka a v případě bezdrátového přenosu vzduch. K aktivním prvkům patří switch propojující prvky v síti. Bridge (Most) propojuje vícero sítí typu LAN, na rozdíl od switche je to inteligentní prvek schopný filtrace paketů a propojení sítě rozdílných standardů. Router (směrovač) je také inteligentním aktivním prvkem, který shromažďuje informace o připojených sítích a následně vybírá nejvhodnější cestu pro posílaný paket. Mimo jiné zvládá filtraci paketů a doplňuje ji o inteligentní směrování. Router se běžně používá pro připojení sítí k internetu (Sosinsky, 2010, s.21-23).

3.1.2 WIFI

WI-FI je bezdrátová lokální síť dále WLAN (Wireless Local Area Network). Používá bezlicenční frekvenční pásmo od 2,4GHz do 5,9GHz dle použitého protokolu, technologie nebo regionu (Ferro, 2014). Bezdrátové sítě pro protokoly WLAN jsou definovány Standardem IEEE 802.11 (Institute of Electrical and Electronics Engineers) (Bučina, 2003).

Do roku 1997 se nepoužívalo zabezpečení připojení, ale pouze filtr IP nebo MAC adres a přihlášení heslem k AP (Access point). Komunikace probíhala v otevřeném tvaru (nezašifrována).

WEP (Wired Equivalent Privacy) protokol byl standardizován v roce 1997 a začal se používat jako volitelný doplněk ke standardu IEEE 802.11b. Šifrování přenášených dat

se provádí 64bitovým klíčem, který je složen z uživatelského klíče a dynamického vektoru IV (Initialization Vector) o délce 24 bitů. IV se posílá v otevřené formě a mění se s každým paketem, přičemž výsledná šifra je jedinečná pro každý jednotlivý paket. WEP používá šifrovací algoritmus RC4. V závislosti na výrobci může nabízet silnější zabezpečení ve formě 128 bitového šifrování (sdílený klíč má délku 104 bitů, vektor 24 bitů). Hlavní slabinou je přenos klíče v otevřeném tvaru, a proto je útočník schopen získat klíč a prolomit zabezpečení. V roce 2001 byl protokol WEP oficiálně prohlášen za prolomený.

Wi-Fi aliance roku 2002 definovala zabezpečení WPA (Wi-Fi Protected Access) pro bezdrátové sítě jako součást standartu IEEE 802.11i. Standart je zpětně kompatibilní s WEP, a navíc funguje i na původním hardwaru. Používá stejně jako WEP proudovou šifru RC4. Hlavní důvodem vzniku bylo odstranění slabiny WEP, a to přenosu klíče v otevřeném tvaru. Odstraněním slabiny bylo docíleno vyvinutím protokolu TKIP (Temporal Key Integrity Protocol). TKIP je protokol pro dynamickou správu klíčů. Klíče jsou bezpečně přenášeny na začátku komunikace i v průběhu. WPA používá 128bitový šifrovací klíč a 48 bitový inicializační vektor. Používá algoritmus CRC-32, který provádí kontrolní součty, tudíž v případě modifikace zprávy, nebude souhlasit kontrolní součet a zpráva bude zahozena. Kontrolní součet se nešifruje, je zasílán v otevřeném tvaru spolu s daty zašifrovanými pomocí RC-4. Pro modifikaci zprávy je nutné znát klíč, aby mohl být vytvořen nový kontrolní součet. Dále se používá algoritmus MIC (Message Integrity Code), který obsahuje počítadlo rámců, a to zabraňuje útokům pomocí zopakování předchozí komunikace. Pro prvotní autentizaci se používá PSK (Pre-shared key), tedy předem definovaný klíč nebo autentizace pomocí serveru (Wong, 2003).

Roku 2006 vznikl protokol WPA2 (Wi-Fi Protected Access 2), jakožto modifikace WPA. Protokol TKIP byl vyměněn za CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol), který je založen na principu AES. WPA 2 je zpětně kompatibilní s WPA a popřípadě na jednom AP může fungovat zároveň WPA i WPA2 (Fitzpatrick, 2016).

Protokol WPA2 byl v říjnu 2017 prolomen útokem KRACK (Key Reinstallation Attacks). Útok směřuje na proces vyjednávání klíče (Handshake), kdy je útočník schopen číst i modifikovat komunikaci v závislosti na nastavení WIFI. Po nalezení chyby byli nejdříve informováni výrobci a poté byla informována veřejnost. Někteří výrobci již vydali záplaty (softwarová oprava), nicméně o jejich instalaci se musejí postarat uživatelé. Je tedy velmi pravděpodobné, že po delší dobu bude v provozu velké množství zranitelných

zařízení. Uživatel se může chránit pomocí další vrstvy šifrování, a to použitím HTTPS nebo VPN. (Krčmář, 2017)

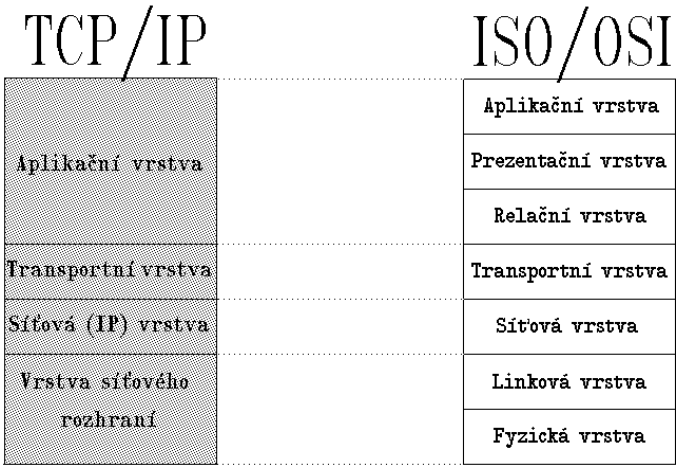
WPS slouží ke zjednodušení přístupu u nastavení bezdrátové sítě. Klient zadá PIN do svého zařízení, a to jej odešle do AP. AP vrátí klíč k zabezpečené síti. WPS je standardně zapnuté od výrobce, čehož si mnozí uživatelé nejsou vědomi. Pro PIN je typické osmimístné číslo, kdy jeho poslední číslo tvoří kontrolní součet předešlých hodnot. Charakteristika protokolu WPS vede k útokům typu „brute force“ na PIN (zkouší se všechny možné kombinace). Při chybném zadání PIN protokol WPS zasílá, jestli byla první nebo druhá polovina chybná, což značně snižuje počet pokusů nutných pro prolomení hesla. Existuje maximálně 11000 možných kombinací. Pokud tedy budeme počítat 3 vteřiny na jeden pokus, tak všechny možné kombinace vyzkoušíme za 9 hodin (Hruška, 2013).

3.2 TCP/IP

Vzhledem k tomu, že model ISO/OSI je považován za zastaralý, není v této v práci popsán. V současné době je základem veškeré komunikace v rámci internetu model TCP/IP a skládá ze čtyř vrstev (ISO/OSI je tvořen sedmi):

- Aplikační vrstva (Application Layer) tvořena aplikačními programy, které komunikují s nižší vrstvou.
- Transportní vrstva (Transport Layer) je nejčastěji realizována pomocí protokolu TCP (Transmission Control Protocol). Zajišťuje přenos dat mezi koncovými body v síti, dále je schopna zajišťovat spolehlivý/nespolehlivý přenos, regulovat tok dat oběma směry a měnit nespojovaný charakter přenosu na spojovaný.
- Sítová (IP) vrstva, která je přiblížena v části IP protokolu.
- Vrstva síťového rozhraní umožňující přístup k fyzickému přenosovému médiu (Peterka, 1992).

Obrázek 1 Srovnání TCP/IP a ISO/OSI



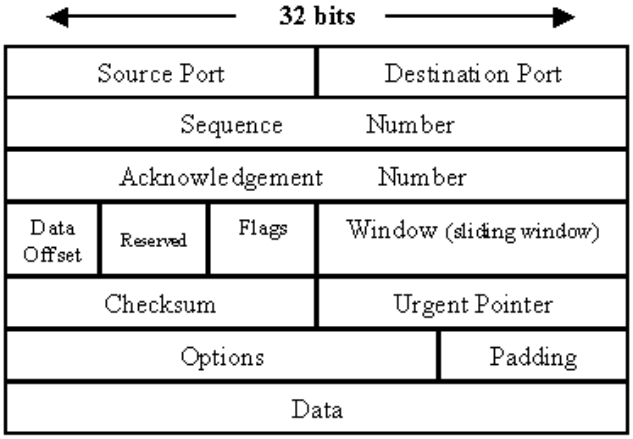
Zdroj: http://www.earchiv.cz/a92/gifs/p231c111.gif

3.2.1 IP protokol a IP datagram

IP (Internet Protocol) definuje tzv. IP datagram, který je základní jednotkou dat přenášených v rámci počítačových sítí. Datagram je tvořen řídící částí a datovou částí. Je vytvořen převzetím dat od transportní vrstvy. Data od transportní vrstvy vloží do své datové části a přidá svou hlavičku. Datagram je následně předán vrstvě síťového rozhraní, které ho vkládá do své datové časti a přidá svou hlavičku, obsahující fyzickou adresu odesílatele, příjemce a údaje o významu přenášených dat. Podstatné je, že každý datagram

obsahuje adresu odesílatele a příjemce. Při zachycení tohoto datagramu třetí osobou, osoba získá informaci o odesílateli a příjemci zprávy (Peterka, 1992).

Obrázek 2 IP hlavička



Zdroj: https://www.techrepublic.com/article/exploring-the-anatomy-of-a-data-packet/

3.2.2 TCP a UDP

Protokol TCP a UDP patří do čtvrté vrstvy TCP/IP modelu, vrstvy transportní (Peterka, 1999).

TCP (Transmission Control Protocol) je definován v dokumentem RFC 793 z roku 1981. Jedná se o protokol zajišťující spolehlivé spojení. Spolehlivé spojení znamená, že každý paket bude doručen v řádném pořadí, což přináší i nevýhody v podobě vyšší režie vzniklé zajišťováním spolehlivého přenosu. Spolehlivý přenos je zabezpečen pomocí číslování paketů, ověření o doručení, znovu zasílání poškozených nebo ztracených paketů (RFC: 793, 1981).

UDP (User Datagram Protocol) definován roku 1980 v dokumentu RFC 768 je protikladem protokolu TCP (RFC: 768, 1980). Zajišťuje nespolehlivý přenos, tedy nekontroluje, zda byl paket doručen, popřípadě dorazil-li duplicitně. Používá se například u VOIP (Voice Over Internet Protocol) a data streamu, kde není vyžadováno spolehlivé připojení (Peterka, 1999).

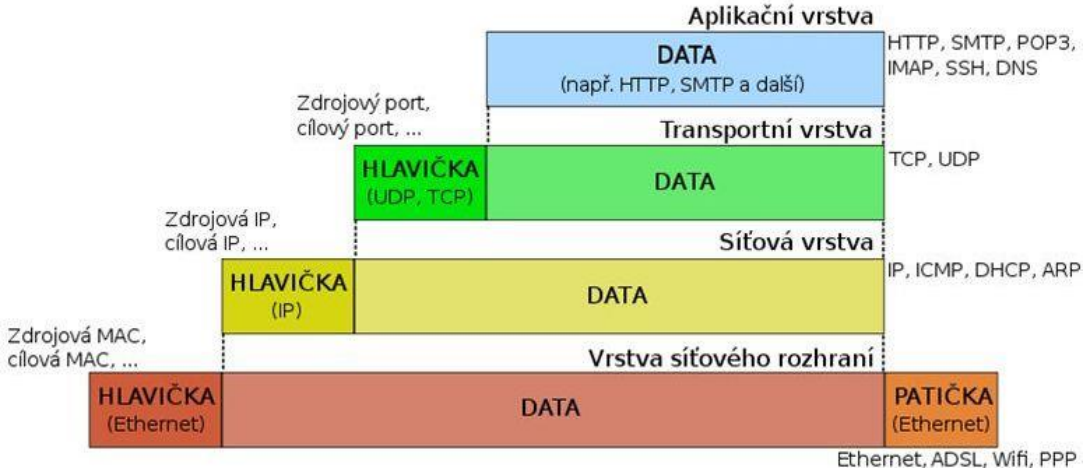
3.2.3 Zapouzdření dat v síti TCP/IP

Zapouzdření dat v síti TCP/IP probíhá v několika krocích. Nejvyšší vrstva, aplikační, předá svá data do nižší vrstvy, a to transportní, síťové, a nakonec vrstvy síťového rozhraní.

V každém kroku přidává vrstva svou hlavičku a následně jej odešle. V případě přijetí proces probíhá reverzně.

V obrázku níže jsou zobrazeny jednotlivé vrstvy, hlavičky a protokoly podle toho, ve které vrstvě operují (Sosinsky, 2010, s. 45-49).

Obrázek 3 Zapouzdření dat v síti



Zdroj: http://vyukasiti.wz.cz/zapouzdreni.jpg

3.3 DNS

DNS (Domain Name System) je tvořen hierarchicky rozdělenou sítí serverů. Protokol DNS se používá pro komunikaci s doménovými servery a k vzájemné komunikaci. Účelem tohoto systému je převod IP adres do lépe zpracovatelného tvaru pro uživatele.

Struktura DNS serverů je rozdělena podle úrovní. Nejvyšší úroveň (TLD – Top Level Domain), druhá úroveň (SLD – Second Level Domain), pod kterou spadá doména.cz a následují domény třetí, čtvrté, páté i dalších úrovní (Peterka, 1992).

DNS funguje následovně: uživatel zadá do webového prohlížeče adresu www.seznam.cz, tím odešle dotaz na lokální DNS server, který adresu zná a zašle jí uživateli. V případě, že adresu lokální DNS server nezná, zašle dotaz jeho nadřazenému serveru. Pokud nadřazený server adresu zná, zašle jí klientovi a pokud ne, tak se buď dotáže nadřazeného serveru, nebo ho odkáže na DNS server obsahující doménu .cz. Tímto způsobem pokračuje dotazování a stoupání v hierarchii, dokud není záznam nalezen. V případě, že DNS server záznam nenašel, zašle informaci o nenalezení záznamu o adrese webového serveru. DNS servery mají cache paměť, tedy dočasnou paměť, kam si ukládají

již nalezené IP adresy a doménová jména, která již byla vyhledávána za účelem zrychlení dotazování. (CZ.NIC, 2007)

3.3.1 **Útoky na DNS**

Mezi rozšířené útoky na DNS patří ARP Cache poisoning. ARP cache poisoning spočívá v zaslání ARP paketu v lokální síti, kde útočník podvrhne adresu reálného DNS serveru za svou vlastní. Následně je útočník schopen podvrhovat adresy webů, které žádá zařízení s napadenou ARP pamětí. Cílem útočníka je podvrhnout adresu typu www.banka.cz s adresou 1.2.3.4 za www.banka.cz s adresou 10.11.12.13 vlastněnou útočníkem. Klient netuší, že se nachází na podvržené stránce a zadává své přihlašovací údaje. Zabránit tomuto útoku je možno více způsoby. Jednou z možností je nepřipustit do lokální sítě žádné neprověřené zařízení, popřípadě nastavit adresy staticky do ARP tabulky. Další možností je použití DNSSEC, zabezpečené verze DNS, pomocí digitálního podpisu. Každý záznam je digitálně podepsán a tím je zamezeno podvržení (Sanders, 2010). Jiný typ útoků zasílá falešné odpovědi klientovi obsahující adresu DNS serveru žádanou klientem, ale s podvrženou adresou webového serveru patřící útočníkovi. Útočník tedy zasílá odpověď DNS serveru a aby uspěl, je potřeba uhodnut ID dotazu. Tento útok se používá v kombinaci s útoky na přetížení DNS serveru, čímž útočník získá více času na uhodnutí ID odpovědi. I před tímto druhem útoku uživatele ochrání DNSSEC (Haller, 2006).

3.3.2 **HTTP/HTTPS**

HTTP (Hypertext Transfer Protocol) je definován pro verze HTTP /1.0 v dokumentu RFC 1945 a pro verzi HTTP/1.1 dokumentem RFC 2616. Protokol pracuje na aplikační vrstvě TCP/IP modelu. Cílem tohoto protokolu je zajistit přenos dat v systému www (World Wide Web) složeného z HTML dokumentů uložených na webových serverech. Pro přenos dat využívá protokol TCP.

V případě komunikace s webovým serverem jsou data pomocí HTTP přenášena v otevřeném stavu a není ověřena důvěryhodnost webového serveru. Data v otevřeném tvaru jsou čitelná pro třetí osoby a zároveň je mohou modifikovat. Tento problém byl odstraněn vytvořením protokolu HTTPS. (RFC 2616, 1999)

HTTP 2.0 je nástupce předešlých verzí. Vznikl za účelem urychlení načítání webových stránek a snižuje dobu načítání webové stránky až o 64 %. (Chronium, 2017). Zrychlení bylo dosaženo změnou způsobu přenosu dat. Ve verzi 1.0 je navázáno jedno TCP

spojení a komunikace probíhá v podobě dotazů a odpovědí. Ve verzi 1.1 je možno použít více TCP spojení. To vedlo ke zvýšení režie na straně serveru i klienta. HTTP 2.0 tento problém řeší pomocí jednoho TCP spojení, na kterém se paralelně přenáší více proudů dat a zároveň nejsou na sobě závislé. Webová stránka se načítá po částech a přenáší se v jednotlivých proudech. Pakety mohou býti promíchány bez vlivu na výsledek. Zabezpečení je zajištěno pomocí protokolu HTTPS stejně jako u verze HTTP 1.0. (Satrapa, 2015)

HTTPS (Hypertext Transfer Protocol Secure) je popsán v dokumentu RFC 7540. Protokol HTTP využívá SSL/TLS pro navázání spojení s webovým serverem. HTTPS zajišťuje šifrování dat a ověření důvěryhodnosti pomocí certifikátu. Pomocí certifikátu se ověřuje pravost webového serveru. Vhledem k použití SSL/TLS a ověření důvěryhodnosti pomocí certifikátu, nemělo by docházet k útokům MITM (Man-in-the-middle). Principem útoku MITM je připojení útočníka do středu komunikace mezi klientem a webovým serverem. Následně je útočník schopen monitorovat a případně modifikovat komunikaci. (Helpton, 2013)

3.4 Kryptografie

Kryptografie má za úkol utajit obsah zprávy před jejím odesláním metodami šifrování. Po zachycení zprávy neoprávněnou osobou by tato osoba neměla získat nezašifrovaný obsah zprávy. (Levický, 2016, s. 4-6)

3.4.1 DES

DES (Data Encryption Standart) byl vyvinut firmou IMB na základě algoritmu LUCIFER. Tento standard byl přijat již roku 1977 a původně byl určen pro finanční sektor. V roce 1999 byla institucí NIST (National Institute of Standard and Technology) přijata nová verze standardu DES a to 3DES. Využívá trojnásobné šifrování DES a používá 2 nebo 3 klíče.

Algoritmus používá 16 rund, tedy 16 opakování šifrování, přičemž v každé rundě se používá jiný klíč, jenž je vygenerován z předešlé operace. DEC je symetrická šifra, která pro šifrování a dešifrování používá stejný klíč. Pracuje s 64 bitovými bloky otevřeného textu. Otevřený text se v první rundě rozdělí na 2 části. Každá část se modifikuje pomocí funkce *f* a klíče, následně se vymění strany a proces se opakuje šestnáctkrát.

Bezpečnost DES se zakládá na délce klíče a vlastnostech algoritmu. Agentura NSA jej prohlásila za bezpečný i ve variantě s 56 bity, ačkoliv se původně počítalo s 112bity. Vzhledem k vlastnostem algoritmu jsou problematické některé klíče tvořené pouze nulami nebo jedničkami, které generují stejné klíče pro všechny rundy nebo klíče generující rozdílné pouze dva nebo čtyři klíče místo šestnácti. Těchto problematických klíčů bylo pouze 64 z možných 2^{56}, to v dané době nepředstavovalo významné riziko. V roce 1998 byl DES prohlášen za nevyhovující z hlediska bezpečnosti, následně byl několikrát modifikován. Neznámějším nástupcem DES je 3DES. (Levický, 2016, s. 74-80)

3.4.2 **3DES**

Vzhledem k pokroku ve výkonu výpočetních technologií byly vytvořeny další verze založené na DES a to:

1. dvojnásobný DES
2. trojnásobný DES se dvěma klíči
3. trojnásobný DES se třemi klíči

Dvojnásobný DES zašifruje otevřený text pomocí DES s klíčem číslo 1 a výsledek se zašifruje znovu s klíčem 2. Možnost kombinací klíče je 2^{112}. V současné době jsou známé útoky ze "středu" (meet-in-the-middle attacks), což značně snižuje kryptografickou bezpečnost dvojnásobného DES.

Trojnásobný DES používá tři kroky označované jako EDE (Encrypt-Decrypt-Encrypt). Šifrování probíhá tak, že se zpráva zašifruje klíčem jedna, poté dešifruje klíčem dvě a zašifruje klíčem tři. Efektivní délka klíče je 168 bitů. (Levický, 2016, s. 99)

3.4.3 **AES**

AES (Advance Encryption Standart) vznikl jako výsledek veřejné soutěže, kterou vyhlásila NIST v roce 1997. Splňoval následující podmínky, a to bezpečnost ve smyslu vynaloženého úsilí na prolomení algoritmu kryptoanalýzou. Dále minimální délka klíče, která byla 128 bitů, a proto použití metody totálních zkoušek s využitím současných a přepokládaných technologií nepřipadala v úvahu. Splnil předpoklad, že algoritmus má vysokou výpočetní efektivnost, bude aplikován v široké oblasti, a i pro vysoké přenosové rychlosti. Poslední podmínkou byla jednoduchost a použitelnost na různém hardwaru a softwaru, tzv. implementace.

Algoritmus Rijndael vytvořen Joanem Daemenem a Vincentem Rijmenem, představuje základ AES s tím rozdílem, že AES používá výhradně 128 bitový blok, zatímco původní algoritmus umožňoval 128, 192 i 256 bitový blok. Principem funkce je rozdělení zprávy do matice 4*4. Tento blok se v procesu šifrování a dešifrování transformuje na blok dat s mezivýsledky, které se modifikují a na konci se zapíšou do dvourozměrného bloku dat, opět ve formě matice s rozměrem 4*4.(Levický, 2016, s. 81-91)

3.4.4 **BLOWFISH**

Blowfish je bloková symetrická šifra, která transformuje 64 bitový blok otevřeného textu na 64 bitový blok zašifrovaného textu. Dosahuje značné rychlosti na 32 bitových procesorech. Má pouze 5 kB paměťově nároky a je snadno implementovatelná. Délka klíče je zde proměnná do maximální délky 448 bitů. Využívá klíč ve tvaru 32 bitových slov a jejich počet je od 1 do 14. Z těchto slov generuje klíče pro 16 rund plus dva dodatečné a v součtu používá 18 klíčů. Algoritmus nejprve rozdělí blok dat na 2 části, kde je každá strana zašifrována dle daného klíče pro aktuální rundu, poté výsledek rundy podrobí operaci XOR se dvěma dodatečnými klíči. To se děje s každou rundou a na konci se obě strany opět prohodí a podrobí operaci XOR s dodatečnými klíči. Délka klíče je od 32 do 448 bitů, a navíc je díky svému charakteru odolná vůči útoku ze středu. (Levický, 2016, s. 100)

3.4.5 **RC5**

RC5 je symetrická bloková šifra vytvořena Ronem Rivestem. Vyznačuje se flexibilitou v parametrech o délce dat 16, 32 a 64 bitů. Dále počtem rund 0, 1 až 255 a délkou klíče 0, 1 až 255 bitů. RC5 používána ke generování subklíčů množinu poměrně složitých operací. V každé rundě generuje dva subklíče, přičemž další dva klíče v části, která není součástí rund, tedy klíč o maximální délce 256 bitů a zároveň s možností až 256 rund. (Baldwin a kol., 1996)

3.4.6 **Bezpečnost šifrovacích algoritmů**

Vzhledem k výše uvedeným vlastnostem algoritmů je jediný způsob, jak dešifrovat data bez znalosti klíče, a to je klíč uhádnout. Tato metoda se nazývá brute force (metoda hrubou silou, metoda totálních zkoušek). Při zkoušení všech kombinací je velká pravděpodobnost, že na správný klíč narazíme již v první polovině hledání kombinací nutných pro vyzkoušení. (Buchanan, 2013)

Tabulka níže znázorňuje časovou náročnost v případě zkoušení všech kombinací. Počítá se s výkonem 1000 procesorů řady i7 (Intel), schopné vyzkoušet 10 000 000 000 kombinací za vteřinu. (Asecuritysite, 2017)

Tabulka 1Metoda totálních zkoušek

Délka klíče	Počet klíčů	Čas potřebný k vyzkoušení všech kombinací v rocích
64	18446744073709551616	29.25 let
128	340282366920938463463374607431768211456	$539,514,153,540,301*10^7$
256	115792089237316195423570985008687907853269984665640564039457584007913129639936	$183,587,153,154,040*10^{32}$

Zdroj: www.asecuritysite.com

3.5 Hašovací funkce

Hašovací funkce představují významný prostředek v oblasti autentizace uživatelů, autorizace dat a digitálních podpisů. Aplikují svůj algoritmus na data a z toho vznikne kontrolní součet. Pokud budou data modifikována nebo poškozena, výsledek znovu aplikované hašovací funkce se nebude rovnat. (Klíma, 2005)

3.5.1 MD5

Algoritmus MD5 (Message-Digest algorithm) zpracovává vstupní data po 512 bitových blocích a generuje hašovací kód o délce 128 bitů. Výsledný kód má vždy 128 bitovou délku bez ohledu na obsah zpracovaného bloku. Zpráva musí být vždy o 64 bitů kratší, než celočíselný násobek 512 (například při délce zprávy 448 bitů je doplněna o 512 bitů a výsledná délka je 960, což je o 64 bitů méně než 2*512 bitů). Doplněné bity začínají hodnotou 1 a zbytek jsou 0. Prvním krokem je přidání informace o délce zprávy. V tomto případě 64 bitů. Zpráva je nyní rozdělena na 512 bitové bloky. Nyní se realizuje inicializace registru hašovacího kódu. Registr je tvořen 4 registry A, B, C, D a ukládá průběžné výsledky výpočtu 128 bitového hašovacího kódu. Inicializace spočívá v naplnění těchto registrů. Posledním krokem je zpracování 512 bitových bloků zprávy ve 4 rundách, kde každá runda

má 16 kroků. Všechny rundy mají stejnou strukturu, ale každá používá jinou logickou funkci. Vstup do každé rundy je složen z bloku dat a hodnotou uloženou v registrech. Dále každá runda používá 16 konstant z tabulky T. Tabulka T obsahuje 64 položek s velikostí 32 bitů. Hodnoty jsou uvedeny od funkce absolutní hodnoty abs(sin(*i*)), kde *i* je hodnota v radiánech. Po zpracování všech 512 bitových bloků poskytuje 128 bitový hašovací kód. (Levický, 2016, s. 188-190)

3.5.2 **SHA-1**

SHA (Secure Hash Algorithm) byl zaveden standardem NIST v roce 1993 a revidován roku 1995 pod standardem FIPS-180-1 a označením SHA-1. Algoritmus SHA-1 umožňuje zpracovat zprávu o délce menší než 2^{64} bitů a představuje výstupní hašovací kód o délce 160 bitů. Stejně jako algoritmus MD5 zpracovává bloky dat o velikosti 512 bitů. Algoritmus SHA-1 probíhá v několika krocích. První krok spočívá v doplnění původní zprávy, aby byla shodná s 448 modulo 512 a zároveň se počet bitů mění v rozsahu od 1 do 512. Skupina doplněných bitů začíná jedničkou a dále pokračuje 0. V druhém kroku se doplní blok o délce 64 bitů obsahující údaj o délce původní zprávy, přičemž je jako první uveden nejvíce významný bajt. Třetím krokem je inicializace 160 bitového registru hašovacího kódu složeného z registrů A, B, C, D, E s délkou 32 bitů. Dále probíhá zpracování zprávy po 512 bitových blocích. Zpracování se realizuje pomocí čtyř rund, kde každá runda má 20 kroků, stejnou strukturu, ale jinou logickou funkci. Navíc každá runda v jednotlivých krocích používá konstantu *k*. Výsledek po zpracování jednoho bloku s délkou 160 bitů je sloučen s výsledky ostatních bloků a získáme konečný hašovací kód. (IETF, 2001)

Existují další varianty algoritmu SHA, které byly inovovány ve standardu FIPS 180-2 o tři nové hašovací algoritmy a to SHA-256, SHA-384, SHA-512, též označovány jako SHA-2. Hlavní rozdíl oproti algoritmu SHA-1 spočívá v délce hašovacího kódu, který určuje odolnost vůči metodě totálních zkoušek. (Lórencz, 2011)

Tabulka 2 Srovnání verzí SHA

	SHA-1	SHA-256	SHA-384	SHA-512
Délka hašovacího kódu	160	256	384	512
Délka zprávy	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
Velikost bloku	512	512	1024	1024
Velikost slova	32	32	64	64
Počet kroků algoritmu	80	80	80	80
Ekvivalence bezpečnosti v bitech	80	128	192	256

Zdroj: https://edux.fit.cvut.cz/oppa/BI-BEZ/prednasky/bez5.pdf

3.5.3 **MAC**

MAC (Message Authentication Code) slouží k autentizaci zprávy, jedná se o hašovací algoritmus využívající společný tajný klíč mezi stranou A i B. Vytváří hašovací kód o konstantní délce, který se přidává k originální zprávě. Při výpočtu MAC se použije původní zpráva a tajný klíč A, vypočte se MAC a připojí se ke zprávě a odešle straně B. Strana B použije zprávu, kterou obdržela od A a pomocí svého tajného klíče aplikuje MAC. V případě, že se MAC rovná hašovacímu kódu uvedeném ve zprávě, tak zpráva nebyla modifikována a byla odeslána vlastníkem stejného klíče, tím je zajištěna autentizace zprávy. (Sosinsky, 2010, s.683)

3.6 **Symetrické šifrovaní v síťové komunikaci**

V dnešní době se pro autentizaci a integritu dat a v digitálních podpisech používá symetrické šifrování. Dříve pro zabezpečení zprávy. Důležité je vhodné umístnění šifrovacích funkcí a vyřešení distribuce klíčů. (Pavlis, 2013)

3.6.1 **Umístění šifrovacích funkcí**

Pro vhodné umístění šifrovacích funkcí je nejprve potřeba podrobit informační systém analýze rizikových míst a následně zvolit optimální řešení. Rizikovým prvkem v sítích LAN jsou mosty, směrovače i rozvodové skříně pro strukturovanou kabeláž. Potencionální útočník v případě, že se fyzicky dostane k daným zařízením, může odposlouchávat komunikaci. V případě metalických vedení (kroucená dvojlinka), může docházet k indukčnímu přístupu založeném na vyzařování elektromagnetického pole.

Rozlišují se aktivní a pasivní útoky. Aktivní znamená fyzický přístup k danému zařízení, přenosovému médiu. Pasivní útok je monitorování aktivity v síti bez fyzického přístupu.

Snadno zranitelné jsou WIFI sítě, plošně vysílají signál a útočník je schopen dané vysílaní zachytit. (Levický, 2016, s. 107)

Obrana vůči těmto útokům se dá rozdělit na dva způsoby. Prvním je link encryption (linkové šifrování), přepokládá se šifrovací zařízení na začátku a na konci linky. Druhým opatřením je end – to – end encryption (šifrování v koncových zařízení). Zařízení zašifruje paket a ten putuje přes síť až k cíli, který ho je schopen dešifrovat. (Ivanov, 2016)

3.6.2 **Distribuce klíčů**

Z principu šifrování symetrickými šiframi vyplývá, že pro zašifrování a dešifrování je potřeba klíč, který musí být utajený. Získání klíče třetí osobou znamená prolomení zabezpečení komunikace. Důležitá je častá změna klíče pro zvýšení odolnosti vůči kryptoanalýze, což vyžaduje vyřešení distribuce klíčů.

Techniky distribuce klíčů se dají rozdělit na čtyři způsoby, tak aby strana A i B získala tajný klíč bez odhalení klíče třetí stranou.

1. strana A vybere klíč a fyzicky ho doručí straně B
2. třetí strana C vybere klíč a fyzicky ho doručí stranám A i B
3. pokud strana A i B již vlastní klíč, mohou si zaslat nový klíč zašifrovaný původním klíčem
4. pokud strana A i B má šifrované spojení s třetí stranou C, strana C může zaslat klíč pomocí šifrovaného spojení straně A i B

První dva způsoby spadají do takzvané manuální distribuce klíčů, ty jsou použitelné pouze pro linkové spojení. U linkového spojení je potřeba klíč pouze na začátku a na konci spojení. V případě rozsáhlejších systémů je použití fyzické cesty k doručení klíče neproveditelné, díky časové i logistické složitosti. Například pro síť o 1000 zařízeních je nutné zajistit různé klíče pro každé možné spojení. Tento příklad se dá vyjádřit vzorcem: počet klíčů = 1000 (1000-1) / 2 tedy 499500 klíčů.

Třetí varianta je vhodná pro šifrování linkových spojení i konečných zařízení. Nevýhodou je, že v případě získání jediného klíče nepovolanou osobou, získá nepovolaná osoba přístup ke všem ostatním klíčům.

Čtvrtá varianta je nejvhodnější pro šifrování koncových zařízení za předpokladu existence CDK (Centrum pro Distribuci Klíčů). Systém je hierarchicky rozdělen na dvě

části, hlavní prvek CDK a *n* podřízených zařízení. Každé podřízené zařízení komunikuje s CDK pomocí šifrovaného spojení s klíčem master key (hlavní klíč). CDK zasílá session key (dočasný klíč) pomocí kterého, mezi sebou komunikují dva podřazené prvky systému. (Levický, 2016, s. 101)

3.7 Kryptografie s veřejným klíčem

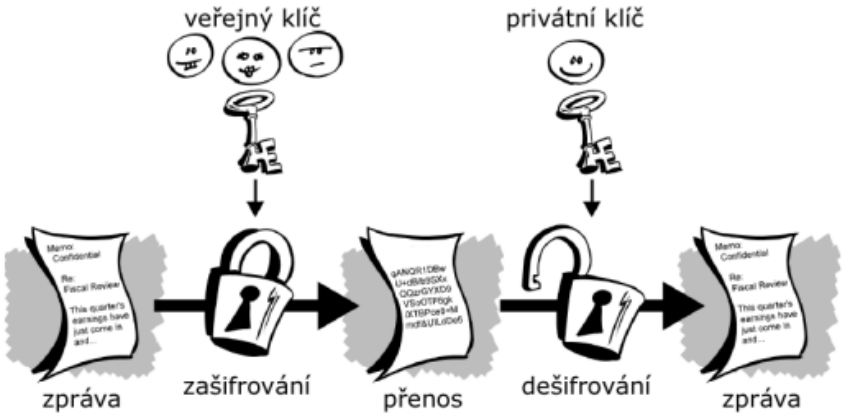
Kryptografie s veřejným klíčem (public-key cryptography) je založena na asymetrickém šifrování. Asymetrické šifrování používá dva rozdílné klíče oproti symetrickému šifrování, které používá jeden klíč na šifrování i dešifrování. Tím odpadá nutnost zajištění distribuce klíče pro koncové zařízení.

První algoritmus využívající koncepci s veřejným a soukromým klíčem je Diffie-Hellman. Diffie-Hellman umožňuje výměnu tajných klíčů přes veřejný přenosový kanál. Tento algoritmus stále vyžaduje interakci mezi účastníky, kteří si vyměňují zašifrovaný text a data. Nicméně Diffie-Hellman stále vyžadoval interakci mezi účastníky komunikace, ale byl průkopníkem v oboru kryptografie s veřejným klíčem.

Každý účastník komunikace je vlastníkem dvou klíčů, veřejného (public key) a soukromého (private key). Veřejný klíč může být zveřejněn, zatímco soukromý klíč se drží v utajení. (MS, 2007)

Kryptografie s veřejným klíčem zabezpečuje šifrování a autentizaci. Obě funkce jsou založeny na principu, kde každý účastník komunikace vlastní svůj soukromý a veřejný klíč tvořící pár. Veřejný klíč je dostupný každému účastníkovi komunikace a soukromý zná pouze vlastník. Kryptografie s veřejným klíčem je tvořena šesti základními složkami: otevřený text, šifrovací algoritmus, soukromý klíč, veřejný klíč, zašifrovaný text a dešifrovací algoritmus. (Redakce PCT, 2005)

Obrázek 4 Schéma použití veřejného a privátního klíče



Zdroj: http://pctuning.tyden.cz/ilustrace2/Matous/sifrovani_asymetricke.GIF

Šifrování v kryptografii s veřejným klíčem probíhá následovně. Účastník A chce zaslat zprávu účastníkovi B, účastník A si zjistí veřejný klíč účastníka B a pomocí veřejného klíče B zašifruje zprávu a odešle jí účastníkovi B. Ten je schopen zprávu dešifrovat pomocí svého soukromého klíče, který tvoří pár s jeho veřejným klíčem. Vzhledem k tomu, že vlastníkem soukromého klíče B je pouze účastník B, tak kdokoliv jiný není schopen dešifrovat zprávu.

Autentizace je řešena reverzně oproti šifrování. Pokud odesílatel zašifruje zprávu svým soukromým klíčem a odešle zprávu příjemci, tak je dešifrovatelná pouze veřejným klíčem odesílatele a tím je zajištěna autentizace.

Bezpečnost je založena na utajení soukromého klíče a obtížnosti získání soukromého klíče nepovolanou osobou, vzhledem k tomu, že útočník má přístup k veřejnému klíči, popřípadě k zašifrovanému obsahu komunikace. Zároveň je nemožné editovat zprávy bez znalosti soukromého klíče, došlo by při dešifrování k zásadní změně zprávy, a tedy i k jejímu znehodnocení. Tak zabezpečuje nejen utajení zprávy, ale zároveň autentizaci zprávy i integritu dat.

Základní podmínky pro realizace kryptografických systémů s veřejným klíčem

1. výpočetně jednoduché generování dvojice veřejného a soukromého klíče
2. výpočetně jednoduchá realizace šifrování
3. výpočetně jednoduchá realizace dešifrování
4. výpočetně složité získání soukromého klíče z veřejného klíče
5. výpočetně složité získání textu ze zašifrované zprávy při známosti veřejného klíče nepovolanou osobou
6. funkce šifrování i dešifrování jsou vzájemně zaměnitelné

Všechny algoritmy pracující s veřejnými klíči používají speciální třídu matematických funkcí nazývané jednocestné funkce (one-way functions) a jednocestné funkce se skrytým vstupem (trap-door one-way function). (Levický, 2016, s. 139-140)

3.7.1 **Kategorizace kryptografických systémů s veřejným klíčem**

Kryptografické systémy s veřejným klíčem se dají na základě určitých algoritmů rozdělit do třech kategorií:

- šifrování a dešifrování
- digitální popisy
- výměna klíčů

Na šifrování se používá veřejný klíč příjemce, pro dešifrování soukromý klíč příjemce.

Digitální podpis zprávy se realizuje pomocí zašifrování zprávy soukromým klíčem odesílatele a dešifrování veřejným klíčem odesílatele. (Kessler, 2017)

3.7.2 **RSA**

Algoritmus RSA (Rivest-Shamir-Adleman) byl vytvořen roku 1978 a je to jeden z prvních kryptografických systémů založených na veřejném klíči. Tento algoritmus stále odolává útokům a díky tomu je široce využíván v kryptografických systémech s veřejným klíčem. Bezpečnost algoritmu je založena na obtížnosti faktorizace velkých čísel. Soukromý a veřejný klíč se odvozuje ze dvou 200 a vícemístných prvočísel. RSA je bloková šifra, kde otevřený i zašifrovaný text je převeden na celá čísla v rozmezí 0 (n-1), kde *n* je zvolené číslo. Typická velikost *n* je 1024 až 2048 bitů. Útok na zašifrovanou zprávu se znalostí veřejného klíče probíhá na základě odhadu faktorizace součinu dvou prvočísel, popřípadě metodou totálních zkoušek. (Wright, 2007)

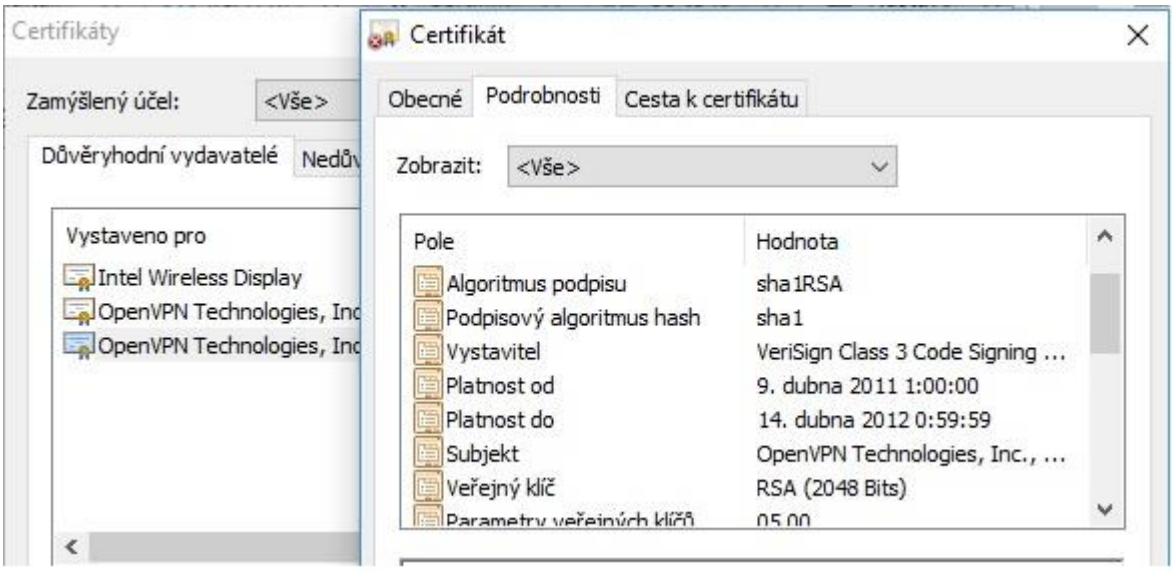
3.8 Digitální certifikát

Digitální certifikát využívá asymetrické kryptografie a certifikační autority (CA) k identifikaci protistrany. Aplikuje se při navazování bezpečného spojení například u HTTPS, VPN nebo ověření odesílatele elektronické pošty. Pro získání digitálního certifikátu se nejprve vygeneruje veřejný klíč a k němu párový soukromý klíč. Takto se dá vytvořit Self-signed certificate (certifikát podepsán sám sebou). Pokud tedy zašifrujeme zprávu svým soukromým klíčem od certifikátu, tak je dešifrovatelná veřejným klíčem od certifikátu. Tím je zaručeno, že odesílatel je vlastníkem certifikátu. Nicméně takto vytvořené certifikáty nejsou důvěryhodné vzhledem k tomu, že je může vytvářet kdokoliv. Použitelné jsou například při připojení do sítě VPN. VPN server vygeneruje certifikát a ten je předán na zařízení, které má být do sítě připojeno. (Doležal, 2003)

Důvěryhodný certifikát je vydán nezávislým subjektem, kterým je poskytovatel certifikačních služeb dle zákona 227/2000 Sb. o elektronickém podpisu, obecně certifikační autorita. Struktura certifikátu se řídí mezinárodní normou X.509. Každý certifikát podepsaný certifikační autoritou obsahuje více údajů, například sériové číslo, které jednoznačně identifikuje daný certifikát a délku platnosti. Dále obsahuje veřejný klíč, typ algoritmu použitý k podepsání a také identifikační údaje certifikační autority. Jeho součástí jsou i identifikační údaje vlastníka. Tyto údaje jsou ověřovány certifikační autoritou pomocí kontroly dokladů totožnosti nebo notářským zápisem. Standardně se certifikáty vydávají na 1 rok z důvodu bezpečnosti, aby nebyl kompromitován soukromý klíč nedbalostí vlastníka nebo metodou totálních zkoušek.

Certifikát je taktéž podepsán soukromým klíčem certifikační autority, aby nemohl být podvrhnut. Platnost certifikátu se ověřuje certifikátem CA, který je dostupný online, případně je obsahem webového prohlížeče. (Brechlerová, 2004)

Obrázek 5 Digitální certifikát



Zdroj: Autor

3.9 VPN

S rozvojem informačních technologií a s dostupností připojení vznikl požadavek na rozdělení privátních a veřejných sítí, ale také ochranu dat a soukromí. Jedním z hlavních způsobů, jak toho docílit je využití technologie VPN (Virtual Private Networks) neboli „virtuální privátní sítě“. Jde o soukromé sítě vytvořené na již existujících, které zajišťují bezpečnou komunikaci mezi subjekty. Výhodou VPN je využití dostupných zdrojů z veřejných sítí a vytvoření vlastní privátní sítě. (Microsoft, 2003)

Vytvoření vlastní privátní sítě lze docílit i pomocí ATM (Asynchronous Transfer Mode) a Frame Relay. Tyto služby jsou schopny garantovat přenosový kanál na rozdíl od VPN, nicméně jsou finančně náročnější. (Greene, 2007)

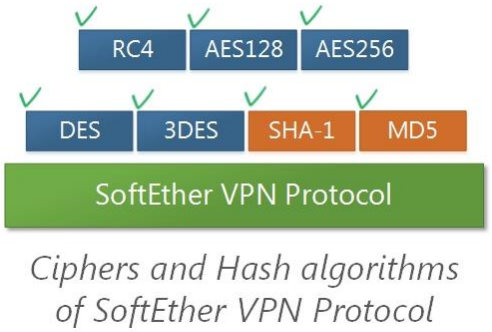
Vzhledem k topologii sítí rozlišujeme více modelů VPN:

- Uzel–Uzel propojení dvou koncových zařízení
- Uzel – Síť propojení jednoho a více zařízení v rámci jednotné sítě LAN
- Síť – Síť Jedná se o model, který vytváří rozsáhlejší homogenní lokální síť vzájemným propojením soukromých sítí. (Luhov, 2003)

Virtuální privátní sítě se používají pro propojení více bodů či uzlů. Zcela zásadní je bezpečnost přenosu, přístupu a integrita dat. Bezpečnost VPN je rozdělena do čtyř kategorií: autentizace, autorizace, důvěrnost a integrita. Autentizace je proces identifikace

uživatele pomocí znalosti nebo vlastnosti, kterou vlastní právě uživatel. K identifikaci uživatele se běžně používá heslo, tajný klíč, certifikát, biometrické údaje nebo kombinace předešlých metod autentizace. Po autentizaci probíhá autorizace, což je proces ověření, zda má daná entita právo přistoupit do sítě. Důvěrnost zajišťuje bezpečnost přenosu dat tak, aby neautorizovaná osoba neměla možnost přečíst obsah přenášených dat. Toho lze docílit pomocí šifrovacích algoritmů DES, 3DES, Blowfish a dalších. Integrita dat je zajištěna pomocí šifrování, hašovacích funkcí a opravnými kódy. Tím je zaručena obrana před chybami vzniklými přenosem, popřípadě daty modifikovanými útočníkem. (Microsoft, 2017)

Obrázek 6 SoftEther podpora bezpečnosti



Zdroj: https://www.softether.org

3.9.1 **Open VPN**

Open VPN je software v licenci GNU GLP (General Public License), kde je volně dostupný zdrojový kód. Aktuálně pro zabezpečení přenášených dat používá SSL. Výměnu klíčů, autentizaci a integritu zajišťuje protokol TLS pomocí HMAC. Pro zabezpečení používá knihovnu OpenSSL. Podporuje kompresi přenášených dat a regulaci šířky přenosového pásma. OpenVPN je multiplatformní, podporuje většinu požívaných operačních systémů i virtuálních serverových řešení. Komunikace může probíhat jako klient-klient nebo klient – server, využívá k tomu TCP nebo UDP. (OpenVPN)

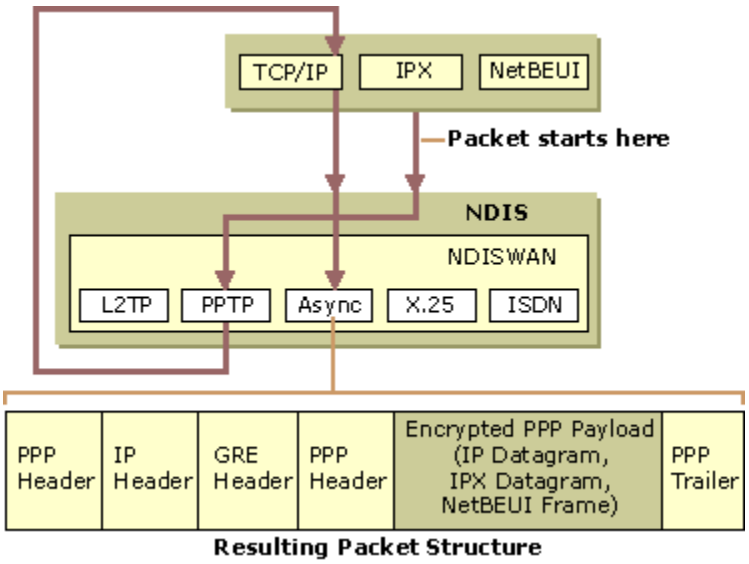
Míra zabezpečení se dá konfigurovat. OpenSSL například nabízí SHA-1, SHA-2 (224 až 512) pro hašování. Pro šifrování využívá AES (128/192/256) v režimech symetrické nebo blokové šifry. Pro digitální podpisy a šifrování s veřejným klíčem RSA a jiné. (Openssl, 2017)

Klient OpenVPN je široce podporován společnostmi poskytujícími VPN jako jsou ExpressVPN, NordVPN, IPvanishVPN, TigerVPN a další. (Top10bestvpn, 2017)

3.9.2 PPTP

PPTP (Point-to-Point Tunneling Protocol) zajišťuje vzdálený přístup mezi dvěma body a vytváří tunel mezi nimi. Funguje na principu původního paketu zabaleného do PPTP v upravené verzi GRE a finálně je předán protokolu IP, který připojí svou hlavičku. V tomto momentu je paket připraven na cestu ke druhému bodu pomocí IP protokolu, ale již obsahuje všechny nutné položky k vytvoření VPN spojení. (Microsoft, 2017)

Obrázek 7 PPTP



Zdroj: https://i-technet.sec.s-msft.com/dynimg/IC212845.gif

3.9.3 L2TP

L2TP (Layer 2 Tunneling Protocol) byl poprvé publikován roku 1999 jako standard RFC 2661. Je nástupcem L2F (Layer 2 Forwarding Protocol) a PPTP od Microsoftu. Novější verze L2TPv3 byla standardizována roku 2005 pod číslem RFC 3931, kde byly přidány bezpečnostní funkce, vylepšené zapouzdření a možnost přenosů dat například pomocí Frame Relay nebo ATM.

Protokol L2TP je postaven na standardech, má tedy vysokou míru podpory od výrobců, a tím je i uživatelsky přívětivý. Je podporován operačními systémy Windows, Android a Mac OS X. L2TP je kompatibilní se směrovacími protokoly například u IP, IPX, AppleTalk a technologiemi v sítích WAN jako jsou Frame Relay, ATM a X.25.

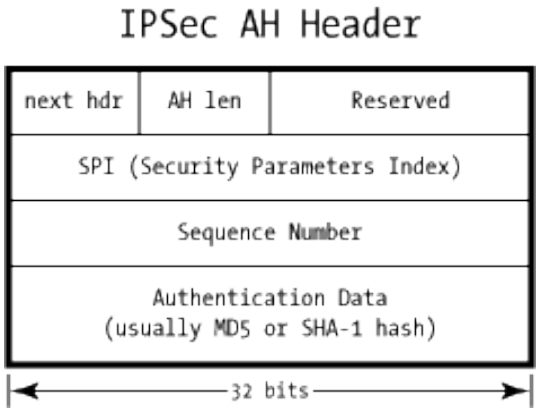
L2TP nativně neobsahuje šifrování a kompresi, ale dá se kombinovat s IPSec. L2TP na rozdíl od PPTP obsahuje navíc autentizaci pomocí certifikátu, autentizace na úrovni uživatele je stejná. Nevýhodou L2TP je nutnost oboustranné podpory NAT (překlad síťových adres), zatímco u PPTP se tento problém nevyskytuje. (Microsoft, 2017)

3.9.4 **IPSec**

IPSec (Internet Security Protocol) se používá již od roku 1995. Je to bezpečností protokol založený na kryptografické bázi. Slouží k rozšíření třetí síťové vrstvy referenčního modelu ISO/OSI. IPSec je množina zahrnující protokoly AH (Authentication Header), ESP (Encapsulating Security Payload), IPcomp (IP Payload Compression Protocol), ISAKMP (Internet Security Association and Key Management Protocol). Podporuje šifrovací algoritmy SHA-1, SHA-2 a hašovací funkce jako MD5.

AH kontroluje hlavičky paketu pomocí kontrolního součtu. Tím zjistí, zda paket nebyl modifikován, poškozen nebo jestli pochází z důvěryhodného zdroje. Dále kontroluje sekvenční čísla, čímž zamezuje duplikaci paketů. Proces probíhá na základně dohody obou komunikujících stran na počátečním čísle paketů a pak jej zvyšují a kontrolují, což zamezuje útoku „replay-attack“. Replay-attack spočívá v zaslání modifikovaného paketu (odchyceného z původní komunikace) útočníkem. (Friedel, 2005)

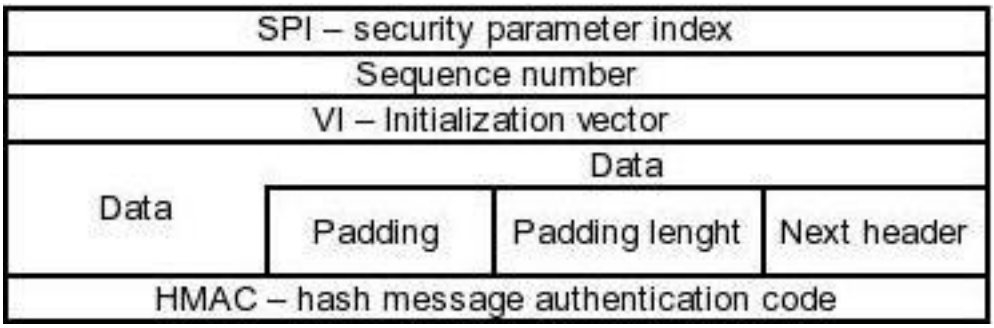
Obrázek 8 AH hlavička



Zdroj: http://www.unixwiz.net/images/IPSec-AH-Header.gif

ESP zajišťuje autentičnost dat pomocí symetrických šifrovacích algoritmů, dříve podporoval pouze NULL a DES, nyní podporuje silnější algoritmy jako 3DES, AES a Blowfish.

Obrázek 9 ESP hlavička



Zdroj: http://www.adeptus-mechanicus.com/codex/contrib/as-ipsec/ipsec8.bmp

Protokol ISAKMP/IKE (Internet Security Association Key Management) (Internet–Key Exchange) slouží pro výměnu klíčů a vyjednání šifrovacího algoritmu. (Pan_R, 2005)

3.9.5 **SSL/TLS**

Protokoly SSL/TLS byly vyvinuty za účelem zabezpečení a ochrany dat pro architekturu klient/server a server/server. Uvedené protokoly realizují šifrování, zabezpečení integrity zprávy a autentizaci serveru vůči klientovi nebo naopak pomocí certifikátů X 509. Vrstva SSL/TLS je vložena mezi aplikačním protokolem a protokolem TCP. Zpráva předána aplikační vrstvou je pomocí SSL/TLS zabezpečena a odevzdána protokolu TCP. Tyto protokoly neanalyzují přijímaná data, ale pouze se starají o jejich zabezpečení. Při navazování spojení se vždy realizuje autentizace serveru a klienta dle potřeby. Komunikace je plně duplexní, nicméně pro každý směr jsou použity různé symetrické šifrovací klíče a tajné parametry na výpočet kontrolního součtu (hašovací funkce). Hlavní výhodou SSL/TLS je implementace přímo v prohlížeči bez použití klienta, čehož se využívá například v zabezpečeném připojení do internetového bankovnictví a procházení webu pomocí HTTPS. (Pornin, 2017)

Architektura SSL je rozdělena do dvou vrstev, každá obsahuje čtyři protokoly. Nejnižší vrstva je tvořena protokolem Record Protocol (RP), nadřazená vrstva je tvořena Alert Protocol (AP), Change Cipher Specification Protocol (CCSP) a Handshake Protocol (HP).

RP přebírá data od aplikační vrstvy, šifruje data a vypočítává kontrolní součet MAC a na straně příjemce kontroluje výsledek MAC.

Handshake Protocol slouží pro komunikaci mezi účastníky. Pomocí tohoto protokolu se účastníci komunikace dohadují o typu šifrování, komprimačního algoritmu a vyměňují

si data pro výpočet tajného údaje master secret. Master secret je hodnota, od které si následně odvodí tajný klíč pro symetrické šifrování a tajný údaj pro výpočet kontrolního součtu MAC.

CCSP potvrzuje, že parametry dohodnuté pomocí HP, byly připsány do seznamu parametrů. K potvrzení využívá jednobajtové zprávy.

Protokol SSL definuje dvě aktivity – spojení a relace, obojí na základě SSL. Protokol SSL je komunikační vztah mezi koncovými zařízeními a každé spojení je vázáno s jednou relací. Relace na bázi SSL je vztah mezi klientem a serverem, zároveň definuje kryptografické parametry, které jsou společné pro obě strany. Mimo jiné odstraňuje nutnost definovat bezpečností parametry pro každé spojení. (Onyszko, 2002)

Protokol TSL 1.0 je definován standardem RFC 2246 a je v podstatě stejný jako SSL popsaný výše, až na malé rozdíly. Používá algoritmus HMAC (Keyed-hash Message Authentication Code) pro tvorbu autentizací zprávy pomocí symetrických blokových šifer, které používají tajný klíč. K autentizaci využívá hašovací funkce MD5, SHA-1, RIPEMD-160. Pro šifrování s veřejným klíčem RSA, Diffie – Hellman a pro symetrické se užívá RC4, DES, 3DES, AES. (IETF, 1999)

TLS 1.1 je vylepšení předešlé verze. Změněn byl Inicializační vektor (IV) z implicitního na explicitní jako ochrana proti Cipher Block Chaining (CBC). Také byla změněna metoda zaslání chyby v případě, že nevyšel kontrolní součet. (Luxsci, 2017)

TLS 1.2 změna oproti původní verzi nastala u hašovacích funkcí MD5/SHA1, byly nahrazeny PRFs (Pseudo Random Function secure). Odebrána byla podpora šifer IDEA, DES a přidána podpora HMAC – SHA256. (IETF, 2008)

Podle zprávy od NIST SP 800-52 R1 je silně doporučeno používat TLS ve verzi 1.2 od roku 2015. (Mimiso, 2014)

3.10 **TOR**

TOR (The Onion Router) je anonymizační služba založena na kaskádových mix serverech. Hlavním cílem je zajistit anonymitu uživatelů sítě TOR (Mojmír, 2015, s. 165).

Síť TOR je skupina dobrovolnických serverů, které umožňují uživatelům vylepšit ochranu jejich soukromí a bezpečnosti na internetu. Uživatelé sítě TOR používají sérii virtuálních tunelů oproti klasickému přímému spojení, což umožňuje organizacím nebo jednotlivcům sdílet informace napříč veřejnými sítěmi, bez ohrožení jejich soukromí. Dále umožňuje obcházet blokace obsahu internetových stránek, v případě že jsou blokace založené na lokaci uživatele. Uživatelé jsou chráněni proti sledování jejich aktivity na webu.

TOR mohou využívat také vývojáři při vytváření komunikačních nástrojů s vestavěnou ochranou soukromí.

Hidden Services (skryté služby) umožňují publikovat webové stránky v rámci sítě TOR bez možnosti lokalizovat reálné umístění stránek. Využití nachází u novinářů, disidentů nebo whistleblowerů. Mohou tak šířit informace anonymně, a tedy se i chránit. Síť TOR doporučují organizace jako Indymedia, tedy sdružení nezávislých zpravodajců. Electronic Frontier Foundation (EFF) doporučuje TOR jakožto nástroj pro zachování občanských svobod. Dokonce i pobočka Amerického námořnictva (US Navy) využívá tohoto nástroje pro sběr dat. (Torproject, 2017)

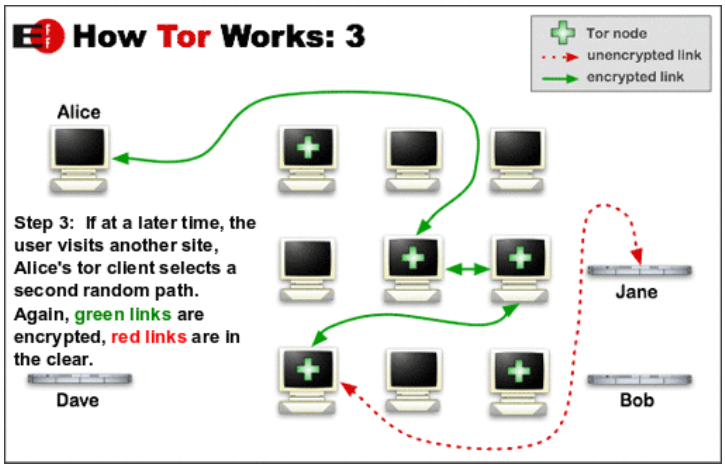
3.10.1 **Princip funkce sítě TOR**

Síť TOR se skládá z uzlů, Exit Node (výstupní bod) a Directory serverů. Uzly jsou tvořeny uživateli, kteří používají TOR. Exit Node je rovněž TOR client, ale nastaven je tak, že umožňuje vystupovat ze sítě TOR ven. Directory servery listují všechny uzly. Každý uzel si pravidelně stahuje seznam uzlů od Directory servers.

Komunikace v síti TOR probíhá následovně:

1. Před započetím komunikace si klient vymění data s Directory serverem, a tím získá informace o ostatních uzlech.
2. Náhodně vybere tři uzly, vytvoří z nich řetězec a přidělí cell ID (identifikátor řetězce). Zároveň dle jejich veřejných klíčů zašifruje zprávu po částech v opačném pořadí. Tedy pokud zprávu odesílal PC1 přes UZEL1, UZEL2. Exit Node bude zpráva vypadat takto zpráva = šifra UZEL 1(šifra UZEL 2 (šifra Exit Node [původní zpráva]).
3. Odešle zprávu na UZEL1 ten pomocí svého soukromého klíče dešifruje první vrstvu a zjistí adresu UZEL2. Zašle mu zprávu, UZEL 2 pomocí svého klíče dešifruje adresu Exit Node a zašle mu zprávu. Výstupní uzel vlastním klíčem dešifruje původní zprávu a odešle jí na adresu, která je uvedena v původní zprávě.
4. Přijatá data v Exit Node se zašifrují soukromým klíčem daného uzlu, výsledkem je šifra Exit Node (přijatá data). Následně zašifruje veřejným klíčem UZEL2 a UZEL1. Šifra tedy vypadá následovně UZEL1(šifra UZEL2[šifra Exit Node {přijatá data}]) a odešle je. Postup je stejný, ale klient data dešifruje pomocí veřejného klíče Exit Node a nodů v opačném pořadí.

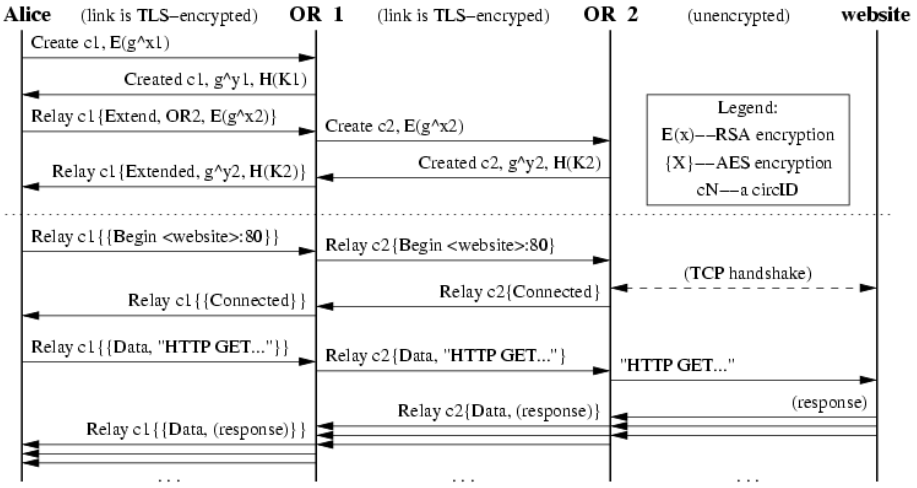
Obrázek 10 Schéma komunikace v TOR



Zdroj: www.torproject.org

Spojení mezi prvky sítě TOR se realizuje pomocí TLS. Každý prvek sítě zná pouze sousedního odesílatele a příjemce – nikoliv celý řetězec. Pro verifikaci odesílatele se používá šifra RSA, což zabraňuje podvržení zprávy. Data jsou šifrována pomocí algoritmu AES se 128 bitovým klíčem v módu proudové šifry. (Torproject, 2017)

Obrázek 11 Vytvoření řetězce TOR



Zdroj: http://www.security-portal.cz/img/clanky/114/ustaveni_tor_retezce.png

3.10.2 Hidden Services

Síť TOR umožňuje i publikaci webových stránek, chat server a další. Zásadní rozdíl oproti běžnému připojení k webovému serveru je neznalost cesty vedoucí k úložišti webových stránek a zároveň server nezná cestu k uživateli. Webové adresy končí příponou .onion a na stránky .onion se není možné navštívit bez připojení do sítě TOR.

Princip funkce:

1. Server nabízející službu kontaktuje několik náhodných klientů za pomoci tunelů a zašle dotaz, zda budou dělat introduction pointy (vstupní body). Zároveň uzlům zašle svůj veřejný klíč (musí být jiný, než server používá, aby nemohl být identifikován).
2. Server zašle seznam vstupních bodů spolu s veřejným klíčem a zároveň tento klíč podepíše svým privátním klíčem a předá jej do distribuované hašovací tabulky. Adresa vypadá následovně XYZ.onion. Kde XYZ je 16místné slovo odvozené z veřejného klíče serveru. Díky odvození adresy z veřejného klíče si mohou vstupní body, distribuovaná tabulka, popřípadě klienti ověřit, že komunikují právě s chtěným serverem.
3. Klient zadá adresu, následuje dotaz na tabulku s adresami vstupních bodů a veřejným klíčem. Nyní klient vytvoří nový tunel v rámci sítě TOR a náhodně vybere jeden prvek sítě a zašle mu dotaz, zda pro něj udělá randevous point (náhodně zvolené místo setkání) a zašle mu náhodně vygenerované číslo.
4. Pokud je randevous point připraven, klient zašle zprávu vstupnímu bodu zašifrovanou veřejným klíčem zveřejněným serverem v tabulce vstupních bodů, předem vygenerované náhodné číslo a adresu místa setkání. Komunikace probíhá stále pomocí TOR tunelů.
5. Server dešifruje klientovu zprávu, pomocí adresy místa setkání a vygenerované hodnoty, vytvoří okruh do místa setkání. Randevous point kontaktuje klienta, že spojení je navázáno a nyní může komunikace začít. Data se přenáší zašifrovaná v rámci komunikace bod-bod. (Torproject, 2017)

3.10.3 **Bezpečnost TOR**

TOR používá velice solidní šifrování a metodu anonymizace, nicméně existují zde určitá rizika, které mohou vést k identifikaci uživatele, popřípadě odcizení osobních údajů. K vyzrazení identity uživatele stačí například plugin Flash. Tento plugin je určený především pro přehrávání video obsahu na webových stránkách. Naneštěstí uchovává informace o uživateli ohledně operačního systému, verze prohlížeče i IP adresu a velice snadno prozradí identitu uživatele. Toto platí taktéž pro Javascript i Javu. (ASHUTOSH, 2017)

Speciální případ jsou takzvané otrávené Exit Node. Výstupní body může provozovat kdokoliv. Mohou je provozovat uživatelé podporující tuto anonymní síť, popřípadě útočníci usilující o osobní údaje uživatelů a monitorování jejich aktivity. Výstupní bod nezná adresu

uživatele, ale zná jeho cíl a přenášená data. Je tedy velice nebezpečné používat HTTP. Taktéž uživatel nesmí používat stejné přezdívky, email atd. v rámci sítě TOR i mimo ní. Nesmí se taktéž přihlašovat ke stejnému účtu s TORem i bez něj. To vše může vést k identifikaci uživatele. Určité riziko vzniká i samostatným používáním, kdy provozovatel internetové připojení vidí, zda uživatel používá TOR. Což je možno považovat za podezřelou aktivitu. (Albaugh, 2016)

Přímo zabezpečení TOR nebylo dle dostupných zdrojů prolomeno, nicméně chyba HeartBleed tykajících se OpenSSL knihoven vedla ke zranitelnosti 12 % klientů TORu (ÇALIŞKAN a spol., 2015). Dle materiálů odtajněných Edvardem Snowdenem obsahujících tajné dokumenty britské a americké bezpečností služby - zejména účinný útok pomocí analýzy přenesených dat, tento postup vyžaduje velké množství zdrojů (monitorují se vstupy a výstupy ze sítě TOR a pomocí statistických metod se deanonymizuje uživatel). Dále z dokumentů vyplývá, že TOR samotný označují za čtvrtý stupeň obtížnosti, zatím co získat přístup k facebookovém účtu za triviální, z čehož vyplývá efektivita TORu. (APPELBAUM a spol., 2014)

Agentura NSA (The National Security Agency) za podpory poskytovatelů internetového připojení je schopna přepojovat uživatele TORu na své speciální servery a následně je identifikovat.

Akademického výzkumu ukázal, že pokud někdo získá kontrolu nad jedním a více autonomními systémy (ASes) a IXPs (Internet Exchange Points) je schopen deanonymizovat běžného uživatele TORu s 50 % pravděpodobnostní za tři měsíce. Pokud by měl šest měsíců, pravděpodobnost stoupá na 80 %, tato metoda se nazývá Traffic Correlation Attack (korelační útok). (ÇALIŞKAN a spol., 2015)

3.10.4 **Kombinace TOR a VPN/Proxy**

Připojení do sítě TOR je možno kombinovat s proxy i VPN. Zaručují vyšší míru zabezpečení, ale přinášejí nová rizika.

První metoda je Klient-TOR-proxy/VPN-Internet, tento způsob zajišťuje maskování připojení do TOR před provozovatelem internetového připojení. Je možné navštěvovat webové stránky v rámci TORu. Problém nastává u provozovatelů proxy/VPN serverů, zda shromažďují data o uživatelích. Tento způsob zvyšuje odolnost vůči analýze přenášených dat. (WHONIX, 2017)

Druhou metodou je klient-proxy/VPN-Tor-Internet, provozovatel internetového připojení má informaci o tom, zda je klient připojen do sítě TOR. Nicméně komunikace je šifrována dle nastavení VPN. Pokud se jedná o placenou službu VPN/PROXY, je nutné zaplatit anonymně. Vzhledem k tomu, že platba například kreditní kartou by mohla vést k identifikaci uživatele. Stejně jako předešlý způsob zvyšuje bezpečnost a opět záleží na provozovateli VPN/PROXY. (SUNNY, 2017)

3.11 **Proxy server**

Jedná se o softwarovou aplikaci vytvářející prostředníka mezi dvěma koncovými body. Důležitou funkcí proxy je schování klientovy adresy, pokud se klient připojí pomocí proxy serveru k webovému serveru, webový server zná pouze adresu proxy serveru. Paket zaslaný proxy serveru obsahuje adresu klienta a adresu cíle. Proxy server nahradí adresu klienta za svou a odešle paket dále, když přijde odpověď proxy serveru, odešle paket zpět klientovi. Proxy servery monitorují veškerou komunikaci procházející skrze ně. Proxy může sloužit jako paketový filtr i filtr obsahu, dokáže číst HTTP zprávy. (Dean, 2010, s. 592)

Operuje na aplikační vrstvě, podporuje protokoly jako HTTP, SMTP (Simple Mail Transfer Protocol) a SOCKS. Protokoly TCP a UDP mohou komunikovat skrze protokol SOCKS. Pro připojení k proxy serveru stačí webový prohlížeč, popřípadě se nastaví adresa proxy serveru v aplikaci. (Mitchell, 2016)

S používání proxy souvisí určitá rizika, a to v podobě důvěry v proxy server. Server si může uchovávat záznamy ohledně aktivity vytvářené uživatelem a poskytnou je třetím osobám.

Dále se dají dělit podle míry anonymity, a to na Transparent, Anonymous a Elite. V případě Transparent není, příliš užitečná, v hlavičce HTTP protokolu ponechává adresu uživatele. Anonymous adresu uživatele již zcela skrývá, ale z hlavičky HTTP je známo použití proxy. Elite maskuje adresu uživatele i použití proxy. (Abclinux, 2015)

3.12 **Vybrané metody pro zpracování praktické části**

K nalezení vhodné metody zabezpečení pro uživatele je nejprve nutné definovat jeho požadavky, k tomu slouží takzvaná persona (Řezníček, 2016). Ke zvolení ideálního způsobu zabezpečení, kdy má uživatel více požadavků, je nejvhodnější metoda vícekriteriální analýzy variant. (Cristoba, 2012)

3.12.1 **Vícekriteriální rozhodování**

Vícekriteriální rozhodování je disciplína operačního výzkumu, která se zabývá analýzou rozhodovacích situací. Posuzují se varianty podle více kritérií, kritéria mohou být navzájem konfliktní.

Vícekriteriální rozhodovací problémy jsou popsány množinou hodnotících kritérií, množinou variant a řadou vazeb mezi variantami a kritérii. Umožňuje definovat hodnotící funkce a metodu výběru. Takto je možné definovat vícekriteriální matematický model.

Vícekriteriální hodnocení variant je množina přípustných variant, která je zadána ve formě konečného seznamu. Formulace úlohy je následující:

Seznam variant $A = \{a_1, a_2, \dots, a_n\}$ a seznam hodnotících kritérií $K = \{k_1, k_2, \dots, k_k\}$

Každá variant $a_i, i = 1, 2, \dots, n$ je podle těchto kritérií popsána vektorem kriteriálních hodnot $(y_{i1}, y_{i2}, \dots, y_{ik})$. Takto vznikne matematický model úlohy vícekriteriálního hodnocení variant. Matice se vyjadřují $Y = (y_{ij})$, $D = \{a_{i1}, a_{i2}, \dots, a_{im}\}$ je pak množina vybraných variant, kde $1 < i_1 < \cdots < i_m$, $1 < ij < n, j = 1, \dots m$. (Soukupová, 2012)

Matici lze zapsat jako

Obrázek 12 Matice

$$\begin{array}{c} \\ a_1 \\ a_2 \\ \vdots \\ a_p \end{array} \begin{array}{c} \begin{array}{cccc} f_1 & f_2 & \dots & f_k \end{array} \\ \begin{bmatrix} y_{11}, & y_{12}, & \dots, & y_{1k} \\ y_{21}, & y_{22}, & \dots, & y_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ y_{p1}, & y_{p2}, & \dots, & y_{pk} \end{bmatrix} \end{array}$$

Zdroj: http://elektro.tzb-info.cz/inteligentni-budovy/7651-vyuziti-multikriterialni-analyzy-mca-pro-hodnoceni-inteligentnich-elektroinstalaci

Pokud není uvedeno jinak, přepokládá se, že všechny kritéria jsou maximalizační. Pokud existují minimalizační kritéria transformují se na maximalizační.

Nedominovaná varianta je taková, ke které neexistuje varianta lepší, v případě že by bylo možné, některá kritéria zlepšit, aniž by došlo ke zhoršení jiných kritérií. Nechť $a_i \approx (y_{i1}, y_{i2}, \dots, y_{ik})$ a $a_i \approx (y_{j1}, y_{j2}, \dots, y_{jk})$ jsou dvě varianty. Jestliže $a_i \geq a_j$, pak variantaa_i dominuje variantu a_j. Pokud v množině rozhodujících variant A neexistuje

varianta, která dominuje a tak se nazývá nedominovaná. Množina A_N označuje všechny nedominované varianty.

Optimální varianta není jednoznačně definována, ale používá se k doporučení pro konečný výběr. Kompromisní varianta nastává v případě, že v množině A je pouze jediná nedominová varianta. Varianta hypotetická nebo skutečná, která má nejnižší hodnoty ve všech kritériích, se nazývá bazální (D). Ideální (H) varianta je taková, která dosáhne nejlepších hodnot ve všech kritériích.

Stanovení vah kritérií probíhá ohodnocením preferované vlastnosti. Čím větší hodnota tím větší preference. Pro srovnatelnost je potřebné, aby součet vah byl roven jedné. Pro potřebu této práce bude použita metoda bodovací. Váhy vypočteme vydělením jednotlivých bodů u daných kritérií součtem všech udělených bodů.

Metoda váženého součtu vychází z principu maximalizace užitku. Nejdříve je vytvořena normalizovaná kriteriální matice $R = (r_{ij})$, hodnoty získáme z $Y = (y_{ij})$, pomocí transformačního vzorce pro maximalizaci.

$$r_{ij} = \frac{H_j - Y_{ij}}{H_j - D_j}$$

Matice nyní představuje hodnoty užitku i-té varianty j-tého kritéria. Následně se aplikuje vzorec pro výpočet užitku.

$$u(a_i) = \sum_{j=1}^{k} v_j \cdot r_{ij}$$

Výsledek je graficky interpretován po seřazení dle variant s maximální hodnotou užitku po variantu nejnižším užitkem. Pro součet užitků použiji vzorec $\sum u(ai)$. (Brožová, 2000)

3.12.2 **Persona**

Persona je model uživatele se zaměřením na cíl za použití artefaktu. Model má specifický účel pro softwarový nebo produktový návrh. Model persony se přibližuje klasickým uživatelům, ale s výraznými rozdíly. Je to archetypální reprezentace reálných nebo potencionálních uživatelů. Není to popis reálného, jediného nebo průměrného uživatele. Persona přestavuje vzorové chování uživatelů, cílů a motivů uživatelů v jedné osobě. Persona také obsahuje osobní údaje, pro lepší představivost vývojového týmu. (Blomkvist, 2002)

4 Praktická část

V teoretické části práce, byly popsány prostředky pro připojení k internetu. Dílčí část se zabývala riziky spojenými s komunikací a přenosem dat v internetu a způsoby jakými se může uživatel chránit. Detailně byly popsány a vysvětleny metody ochrany a jejich výhody a nedostatky. Velká pozornost byla také věnována bezpečnostním algoritmům, které jsou nejvíce rozšířené.

Na základě zjištěných informacích autor porovnává metody zabezpečení užívání internetu z hlediska uživatele (definovaného jako persona v kapitole 3.12.2).

4.1 Varianty

Dostupná odborná literatura uvádí devět nejužívanějších nástrojů pro zabezpečení uživatele internetu. Posuzované varianty jsou uvedeny v následující tabulce, vzhledem k délce názvů byla přiřazena kratší označení v podobě varianta 1 až 9 a u kritérií přiřazeny zkratky A až G.

Tabulka 3 Varianty

HTTP	varianta 1
HTTPS	varianta 2
VPN+HTTPS	varianta 3
PROXY+HTTPS	varianta 4
TOR+HTTPS	varianta 5
PROXY/VPN+TOR+HTTPS	varianta 6
VPN(zpoplatněné)+HTTPS	varianta 7
PROXY(zpoplatněné)+HTTPS	varianta 8
VPN/PROXY(zpoplatněné)+TOR+HTTPS	varianta 9

Zdroj: autor

4.1.1 Kritéria

Na základě poznatků z teoretické části byla sestavena následující kritéria:

Bezpečnost: míra zabezpečení komunikace dle použitých šifrovacích a hašovacích algoritmů. Maximalizační kritérium. Označeno písmenem A.

Důvěryhodnost: kritérium maximalizační hodnotící, zda jsou podporovány digitální certifikáty. Označeno písmenem B.

Rychlost: kritérium maximalizační zachycující vliv používané služby na přenosovou rychlost. Označeno písmenem C.

Zprostředkovaná komunikace: využití prostředníka v průběhu komunikace, respektive je-li známa adresa prostředníka, nikoliv uživatele. Kritérium maximalizační. Označeno písmenem D.

Variabilní prostředník: zda se v průběhu komunikace využívá různých prostředníků, zdali se dynamicky mění IP adresa prostředníka. Kritérium maximalizační. Označeno písmenem E.

Cena: Maximalizační kritérium, zda je daná služba zpoplatněna nebo zdarma. Označeno písmenem F.

Anonymita: míra anonymity dle použité technologie, kritérium maximalizační. Označeno písmenem G.

4.1.2 Stanovení person

Pro výsledné porovnání byly stanoveny tři rozdílné persony s odlišnými požadavky. Tyto persony slouží v případném hledání vhodné metody zabezpečení komunikace a nalezení optimálního řešení pro daný typ uživatele.

4.2 Testovací uživatel č. 1

Uživatel č. 1 používá internet každý den, za účelem procházení webu, používá sociální sítě a služby elektronické pošty, čte online noviny, nakupuje online. Znalosti o počítačích a jejich bezpečnosti jsou minimální, kromě již vyjádřených činností se těžko učí používat nové postupy a technologie. Požadavky uživatele č. 1 je alespoň minimální zabezpečení, bez omezení rychlosti připojení, není ochoten platit další služby. Možnost že činnost uživatele č. 1 je monitorována, nepokládá za důležité. Nejdůležitější jsou tedy kritéria výběru:

1) rychlost
2) cena

Dle nároků uživatele č.1 je sestavena následující tabulka:

Tabulka 4 Stanovení vah pro uživatele č. 1

Kritéria	Bezpečnost	Důvěryhodnost	Rychlost	Zprostředkovaná komunikace	Variabilní prostředník	Cena	Anonymita	∑
Body	3	3	10	1	1	10	0	28
Váhy	0,1071	0,1071	0,3571	0,0357	0,0357	0,3571	0	1

Zdroj: autor

Bodové ohodnocení pro stanovení vah:

V rozsahu hodnot 0 až 10, kdy 10 znamená maximální preferenci a 0 absolutní nezájem o dané kritérium uživatelem.

Po sestavení kritérií a výpočtu bazálních a ideálních hodnot byla vytvořena následující tabulka:

Tabulka 5 Sestavení matice pro volbu metody zabezpečení

kritérium	MAX	MAX	MAX	MAX	MAX	MAX	MAX
Kritéria	A	B	C	D	E	F	G
Váhy	0	0	0	0	0	0	0
varianta 1	0	1	3	1	1	2	1
varianta 2	1	2	3	1	1	2	2
varianta 3	3	2	1	2	1	2	2
varianta 4	2	2	1	2	1	2	2
varianta 5	2	2	1	2	2	2	3
varianta 6	4	2	1	2	2	2	3
varianta 7	3	2	3	2	1	1	2
varianta 8	2	2	3	2	1	1	2
varianta 9	4	2	1	2	2	1	3
Ideální v.H.	4	2	3	2	2	2	3
Bazální v.D.	0	1	1	1	1	1	1
H-D	4	1	2	1	1	1	2

Zdroj: autor

Sestavení kriteriální matice proběhne pomocí vzorce:

$$r_{ij} = \frac{H_j - Y_{ij}}{H_j - D_j}$$

Tabulka 6 Sestavení kriteriální matice pro uživatele č. 1

Kritéria	A	B	C	D	E	F	G
Váhy	0,1071	0,1071	0,3571	0,0357	0,0357	0,3571	0,0000
varianta 1	0	0	1	0	0	1	0
varianta 2	0,25	1	1	0	0	1	0,5
varianta 3	0,75	1	0	1	0	1	0,5
varianta 4	0,5	1	0	1	0	1	0,5
varianta 5	0,5	1	0	1	1	1	1
varianta 6	1	1	0	1	1	1	1
varianta 7	0,75	1	1	1	0	0	0,5
varianta 8	0,5	1	1	1	0	0	0,5
varianta 9	1	1	0	1	1	0	1

Zdroj: autor

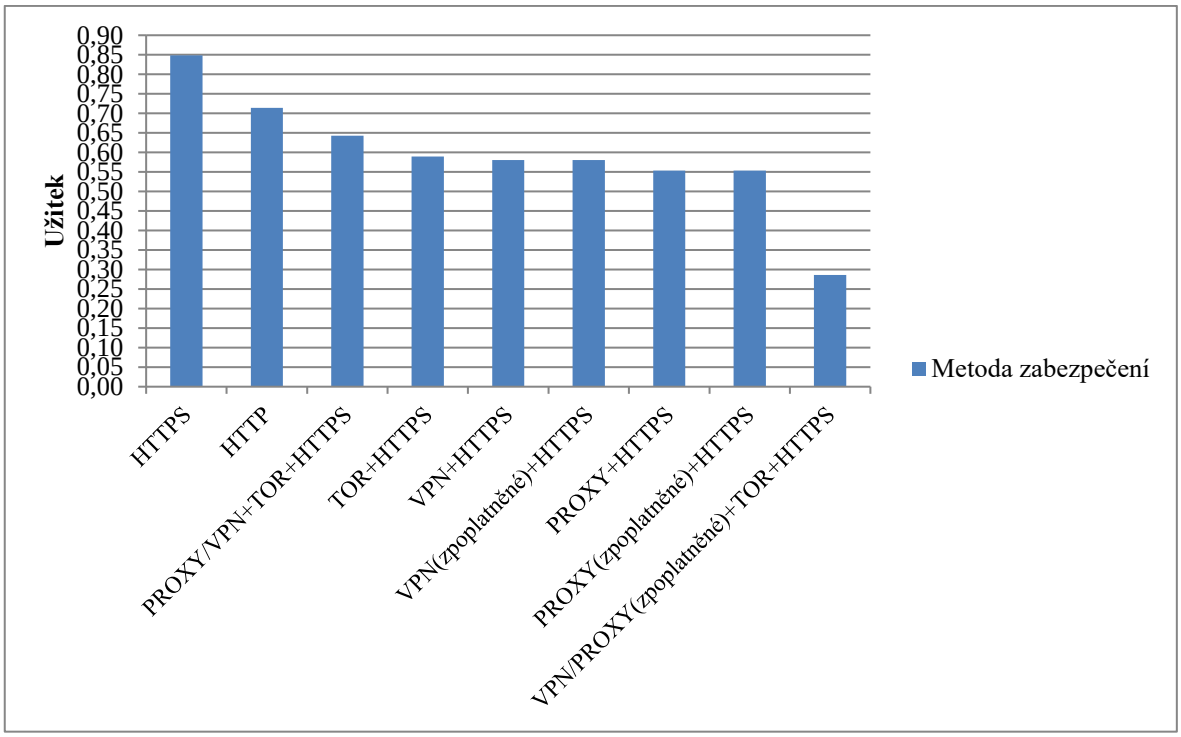
Následně je pomocí vzorce: $u(a_i) = \sum_{j=1}^{k} v_j \cdot r_{ij}$ vypočítán užitek.

Tabulka 7 Výpočet funkce užitku pro uživatele č. 1

Kritéria	A	B	C	D	E	F	G	Užitek
Váhy	0,1071	0,1071	0,3571	0,0357	0,0357	0,3571	0,0000	$\sum u(ai)$
varianta 1	0,0000	0,0000	0,3571	0,0000	0,0000	0,3571	0,0000	0,7142
varianta 2	0,0268	0,1071	0,3571	0,0000	0,0000	0,3571	0,0000	0,8481
varianta 3	0,0803	0,1071	0,0000	0,0357	0,0000	0,3571	0,0000	0,5802
varianta 4	0,0536	0,1071	0,0000	0,0357	0,0000	0,3571	0,0000	0,5535
varianta 5	0,0536	0,1071	0,0000	0,0357	0,0357	0,3571	0,0000	0,5892
varianta 6	0,1071	0,1071	0,0000	0,0357	0,0357	0,3571	0,0000	0,6427
varianta 7	0,0803	0,1071	0,3571	0,0357	0,0000	0,0000	0,0000	0,5802
varianta 8	0,0536	0,1071	0,3571	0,0357	0,0000	0,0000	0,0000	0,5535
varianta 9	0,1071	0,1071	0,0000	0,0357	0,0357	0,0000	0,0000	0,2856

Zdroj: autor

Graf 1 Výsledná míra užitku pro uživatele č. 1



Zdroj: autor

4.3 Vyhodnocení uživatele č. 1

Dle požadavků uživatele č. 1 se umístilo využití protokolu HTTPS na prvním místě s užitkem 0,8481. Nejvíce ovlivnila výsledek kritéria rychlost a cena, ale také nezájem o anonymitu. Pokud by uživatel nevyžadoval alespoň mírné zabezpečení, nejvhodnější by byla varianta HTTP. Téměř třikrát horší užitek získala zpoplatněná varianta VPN/PROXY+TOR+HTTPS vzhledem k pomalosti, zpoplatnění, nadměrné bezpečnosti a zvýšené náročnosti na použití.

4.4 Testovací uživatel č. 2

Uživatel č. 2 představuje firmu aktivně využívající internet pro komunikaci s dodavateli a zákazníky, sběru dat, editace firemních účtů na sociálních sítí. Firma požaduje zabezpečení i za cenu zvýšení nákladů. Má požadavek na skrytí firemních aktivit v rámci internetu, aby nemohla být kontrolována konkurencí. Firma je ochotna přijmout částečně zpomalení komunikace při zvýšené bezpečnosti a ochraně jejich aktiv v rámci internetu. V informačních technologiích je firma zdatná.

Důležitá jsou pro firmu následující kritéria:

1) Bezpečnost
2) Anonymita
3) Důvěryhodnost
4) Rychlost

Dle nároků uživatele č. 2 je sestavena následující tabulka:

Tabulka 8 Stanovení vah pro uživatele č. 2

Kritéria	Bezpečnost	Důvěryhodnost	Rychlost	Zprostředkovaná komunikace	Variabilní prostředník	Cena	Anonymita	∑
Body	6	6	9	5	1	3	5	35
Váhy	0,1714	0,1714	0,2571	0,1429	0,0286	0,0857	0,1429	1

Zdroj: autor

Tabulka 9 Sestavení kriteriální matice pro uživatele č. 2

Kritéria	A	B	C	D	E	F	G
Váhy	0,1714	0,1714	0,2571	0,1429	0,0286	0,0857	0,1429
varianta 1	0	0	1	0	0	1	0
varianta 2	0,2500	1	1	0	0	1	0,5000
varianta 3	0,7500	1	0	1	0	1	0,5000
varianta 4	0,5000	1	0	1	0	1	0,5000
varianta 5	0,5000	1	0	1	1	1	1
varianta 6	1	1	0	1	1	1	1
varianta 7	0,7500	1	1	1	0	0	0,5000
varianta 8	0,5000	1	1	1	0	0	0,5000
varianta 9	1	1,	0	1	1	0	1

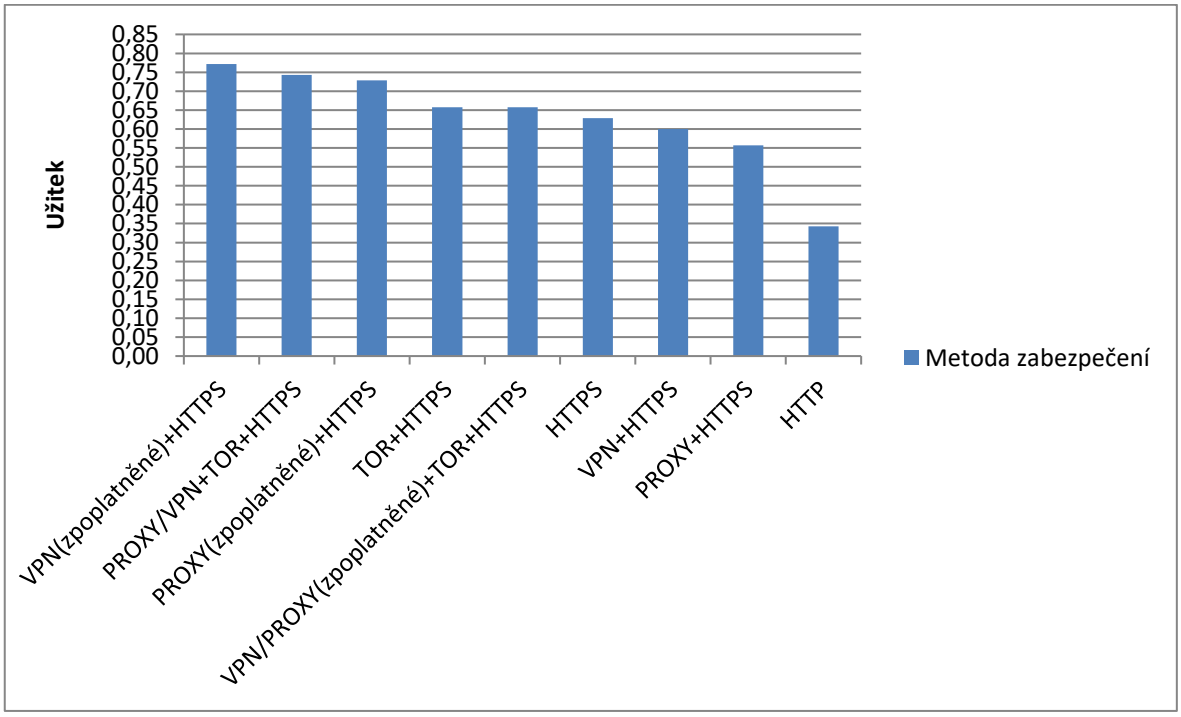
Zdroj: autor

Tabulka 10 Výpočet funkce užitku pro uživatele č. 2

Kritéria	A	B	C	D	E	F	G	Užitek
Váhy	0,1667	0,1667	0,05	0,1667	0,1667	0,1167	0,1667	$\sum u(ai)$
varianta 1	0	0,	0,2571	0	0	0,0857	0	0,3429
varianta 2	0,0429	0,1714	0,2571	0	0	0,0857	0,0714	0,6286
varianta 3	0,1286	0,1714	0	0,1429	0	0,0857	0,0714	0,6000
varianta 4	0,0857	0,1714	0	0,1429	0	0,0857	0,0714	0,5571
varianta 5	0,0857	0,1714	0,	0,1429	0,0286	0,0857	0,1429	0,6571
varianta 6	0,1714	0,1714	0	0,1429	0,0286	0,0857	0,1429	0,7429
varianta 7	0,1286	0,1714	0,2571	0,1429	0	0	0,0714	0,7714
varianta 8	0,0857	0,1714	0,2571	0,1429	0	0	0,0714	0,7286
varianta 9	0,1714	0,1714	0	0,1429	0,0286	0	0,1429	0,6571

Zdroj: autor

Graf 2 Výsledná míra užitku pro uživatele č. 2



Zdroj: autor

4.5 Vyhodnocení uživatele č. 2

Dle vypočítaného užitku 0,7714 lze doporučit zpoplatněnou verzi VPN kombinovanou s HTTPS. Na druhém místě s 0,7429 užitku, se umístila kombinace PROXY/VPN+TOR+HTTPS díky větší míře bezpečnosti, anonymity a není zpoplatněna,

ale zaostává v rychlosti. Absolutně nejhůře dopadlo použití HTTP zásluhou neposkytnutí zabezpečení, ověření certifikátu ani anonymity.

4.6 Testovací uživatel č.3

Uživatel č. 3 je novinář nacházející se v zemi s autoritářským režimem. Publikuje kritické články na webu ohledně aktuálního dění v dané zemi. Jeho požadavky tedy jsou maximální míra zabezpečení a anonymizace. Rychlost připojení, vzhledem k jeho aktivitě na internetu není důležitým kritériem. Hlavní kritéria jsou:

1) Anonymita
2) Bezpečnost
3) Variabilní prostředník
4) Důvěryhodnost

Dle nároků uživatele č.3 je sestavena následující tabulka:

Tabulka 11 Stanovení vah pro uživatele č.3

Kritéria	Bezpečnost	Důvěryhodnost	Rychlost	Zprostředkovaná komunikace	Variabilní prostředník	Cena	Anonymita	∑
Body	10	10	3	10	10	7	10	60
Váhy	0,1667	0,1667	0,0500	0,1667	0,1667	0,1167	0,1667	1

Zdroj: autor

Tabulka 12 Sestavení kriteriální matice pro uživatele č. 3

Kritéria	A	B	C	D	E	F	G
Váhy	0,1667	0,1667	0,0500	0,1667	0,1667	0,1167	0,1667
varianta 1	0	0	0,6667	0	0	0,5000	0
varianta 2	0,2500	0,5000	0,6667	0	0	0,5000	0,3333
varianta 3	0,7500	0,5000	0	0,5000	0	0,5000	0,3333
varianta 4	0,5000	0,5000	0	0,5000	0	0,5000	0,3333
varianta 5	0,5000	0,5000	0	0,5000	0,5000	0,5000	0,6667
varianta 6	1	0,5000	0	0,5000	0,5000	0,5000	0,6667
varianta 7	0,7500	0,5000	0,6667	0,5000	0	0,	0,3333
varianta 8	0,5000	0,5000	0,6667	0,5000	0	0	0,3333
varianta 9	1	0,5000	0	0,5000	0,5000	0	0,6667

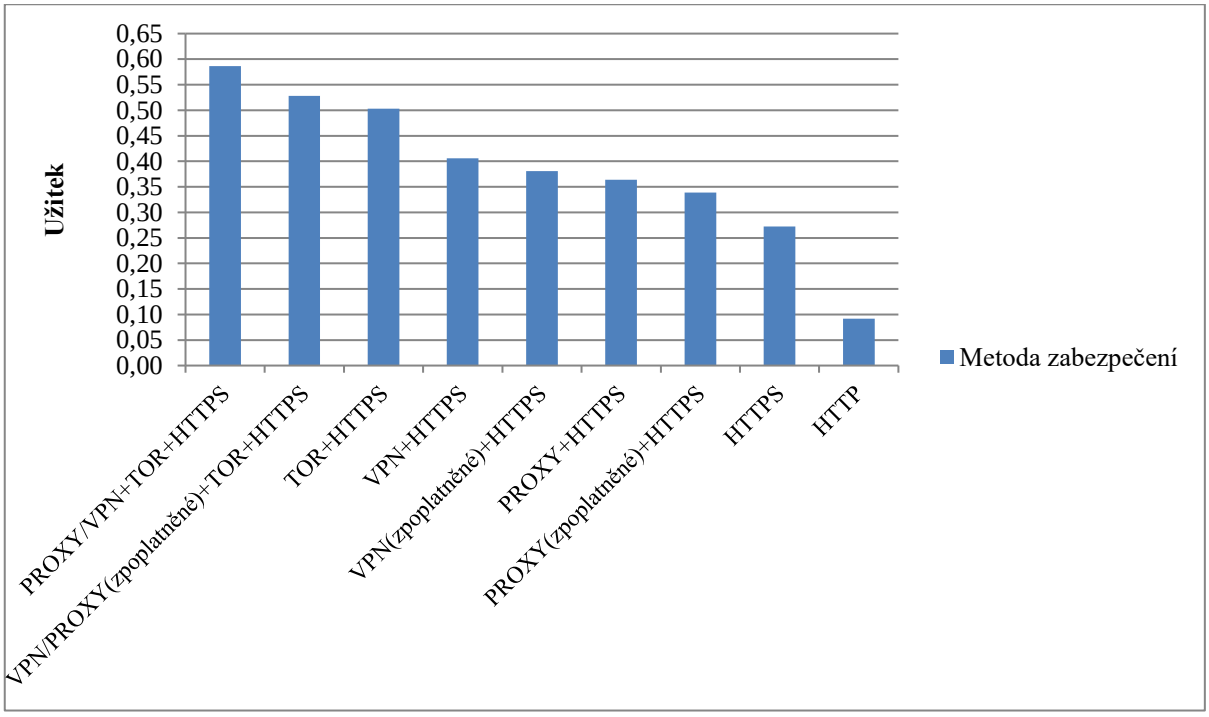
Zdroj: autor

Tabulka 13 Výpočet funkce užitku pro uživatele č. 3

Kritéria	A	B	C	D	E	F	G	Užitek
Váhy	0,1667	0,1667	0,0500	0,1667	0,1667	0,1167	0,1667	$\sum u(ai)$
varianta 1	0,0000	0,0000	0,0333	0,0000	0,0000	0,0583	0,0000	0,0917
varianta 2	0,0417	0,0833	0,0333	0,0000	0,0000	0,0583	0,0556	0,2722
varianta 3	0,1250	0,0833	0,0000	0,0833	0,0000	0,0583	0,0556	0,4056
varianta 4	0,0833	0,0833	0,0000	0,0833	0,0000	0,0583	0,0556	0,3639
varianta 5	0,0833	0,0833	0,0000	0,0833	0,0833	0,0583	0,1111	0,5028
varianta 6	0,1667	0,0833	0,0000	0,0833	0,0833	0,0583	0,1111	0,5861
varianta 7	0,1250	0,0833	0,0333	0,0833	0,0000	0,0000	0,0556	0,3806
varianta 8	0,0833	0,0833	0,0333	0,0833	0,0000	0,0000	0,0556	0,3389
varianta 9	0,1667	0,0833	0,0000	0,0833	0,0833	0,0000	0,1111	0,5278

Zdroj: autor

Graf 3 Výsledná míra užitku pro uživatele č. 3



Zdroj: autor

4.7 Vyhodnocení uživatele č. 3

Pro uživatele č. 3 nejlépe dopadla metoda PROXY/VPN+TOR+HTTPS s užitkem 0,5861. S malým rozdílem se přibližuje stejná metoda, ale s využitím zpoplatněné služby. Pro uživatel č. 3 dále dle výsledků nemohu doporučit metodu HTTP i HTTPS se zřetelem k neposkytnutí anonymity.

5 Závěr

V práci byly charakterizovány způsoby pro bezpečné a anonymní připojení do sítě internet. Vzhledem k rozvoji technologií roste i množství přenášených citlivých dat – ať se jedná přihlašovací údaje, osobní údaje, aktivitu uživatele v síti, popřípadě citlivá firemní data. Vzniká nutnost chránit tato data, zabezpečení se taktéž vyvíjí, nicméně je důležité se vyhnout zastaralým, již prolomeným způsobům ochrany. Práce nabízí přehled protokolů a zařízení potřebných pro připojení do internetu. Zároveň průběžně informuje o rizicích a protiopatřeních u daných technologií.

U bezdrátových sítí je vždy nutné vyžadovat nejvyšší možnost zabezpečení tedy WPA2 v kombinaci s AES. Nicméně i tento ochranný prvek byl prolomen útokem KRACK. Tento problém lze odstranit pomocí VPN.

Virtuální privátní sítě nejen maskují uživatele, ale vytváří i zabezpečení spojení mezi klientem a VPN serverem. Zaručují tedy bezpečné spojení bez ohledu na to, jak je daná cesta zabezpečena. Slabinou je samotná důvěra ve VPN server. Server si může ponechávat záznamy o aktivitách uživatele. V některých zemích je to dokonce nařízeno zákonem, tedy zajišťuje anonymitu pouze do určité míry.

V případě proxy serverů je nutné správně zvolit typ proxy, jelikož rozdíly mezi jednotlivými typy jsou přímo úměrné míře anonymity. Opět si servery mohou ponechávat záznamy o aktivitě uživatele a existuje zde totožný problém jako u VPN.

Sítě TOR poskytují maximální anonymitu a zabezpečení přenosu dat. Bohužel přenosová rychlost je velice pomalá ve srovnání s VPN či Proxy. Klíčové je používat síť TOR v kombinaci s VPN, popřípadě s proxy. Jedním z důvodů je ochrana před korelačními útoky a faktem, že používání TORu samotného upozorňuje na podezřelou aktivitu.

V praktické části byly vytvořeny tři odlišné persony pokrývající spektrum potřeb uživatelů ohledně zabezpečení a anonymity. Uživatel č.1 požaduje maximální rychlost a není ochoten využít placené služby, nepovažuje anonymitu za potřebnou. Vhodným doporučením je používat využívat HTTPS (viz vyhodnocení uživatele č.1). Uživatel č.2 požaduje zabezpečení, anonymitu, rychlost a je ochoten využít placené služby. Dle výsledků je nejvhodnější využít VPN a HTTPS (viz vyhodnocení uživatele č.2). Uživatel č.3 požaduje maximální anonymitu, bezpečnost a použití variabilního prostředníka. Vyhovujícím výsledkem je použití VPN/PROXY v kombinaci s TOR a HTTPS (viz

vyhodnocení uživatele č.3). Tyto persony slouží k porovnání požadavků a nalezení vhodného řešení.

6 Seznam použitých zdrojů

Tištěné zdroje:

DEAN, Tamara. *Network guide to networks*. 5th ed. Boston, Mass.: Course Technology Cengage Learning, c2010, ISBN 978-1-423-90245-4.

LEVICKÝ, Dušan. *Kryptografia a bezpečnosť komunikačných sietí*. 2016. Košice: elfa, 2016. ISBN 978-80-8086-254-1.

HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 3., aktualiz. vyd. Brno: ComputerPress, 2006. Bestseller (ComputerPress). ISBN 8025108929.

KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

Elektronické zdroje:

APPELBAUM, Jacob, Aaron GIBSON, Christian GROTHOFF, Andy MÜLLER-MAGUHN, Laura POITRAS, Michael SONTHEIMER a Christian STÖCKER. Inside the NSA'sWar on Internet Security. Www.spiegel.de[online]. 2014 [cit. 2017-10-15]. Dostupné z: http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html

ASHUTOSH, KS. 11 Do’s and Don’ts of Tor Network. Www.hongkiat.com [online]. Culture, 2017 [cit. 2017-10-15]. Dostupné z: https://www.hongkiat.com/blog/do-donts-tor-network/

BALDWIN, Robert W. a Ronald L. RIVEST. RFC 2616: The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms. Internet Engineering Task Force [online]. MIT, RSA Data Security, 1996 [cit. 2017-7-27]. Dostupné z: https://tools.ietf.org/html/rfc2040

BLOMKVIST, Stefan. Persona – an overview. Uu [online]. Uppsala Universitet, 2002 [cit. 2017-10-3]. Dostupné z: https://it.uu.se/edu/course/homepage/hcidist/vt05/Persona-overview.pdf

Bolest proxy. Abclinuxu [online]. 2015 [cit. 2017-9-18]. Dostupné z: http://www.abclinuxu.cz/blog/bystroushaak/2015/2/bolest-proxy

BRECHLEROVÁ, Dagmar. Certifikáty jako základ e-podpisu, autentizace i šifrování. Systemonline [online]. 2004 [cit. 2017-4-19]. Dostupné z: https://www.systemonline.cz/clanky/certifikaty-jako-zaklad-e-podpisu-autentizace-i-sifrovani.htm

BROŽOVÁ, Helena. Vícekriteriální model teorie rozhodování. Agris [online]. 2000 [cit. 2017-10-19]. Dostupné z: http://www.agris.cz/clanek/101667

BUČINA, Tomáš. Bezdrátové sítě WiFi - 2. Díl Principy a pravidla Wireless LAN. PCworld [online]. TestCentrum IDG, 2003 [cit. 2016-9-6]. Dostupné z: http://pcworld.cz/internet/bezdratove-site-wifi-2-dil-principy-a-pravidla-wireless-lan-13405

BUCHANAN, Bill. For the Love of Cryptography. BILLATNAPIER [online]. 2013 [cit. 2016-10-8]. Dostupné z: https://billatnapier.wordpress.com/2013/05/15/for-the-love-of-cryptography/

ÇALIŞKAN, Emin, Tomáš MINÁRIK a Anna-Maria OSULA. Technical and Legal Overview of the Tor Anonymity Network [online]. Tallinn, 2015 [cit. 2017-11-29]. Dostupné z: https://ccdcoe.org/sites/default/files/multimedia/pdf/TOR_Anonymity_Network.pdf

CompareFeatures of the Top 5 VPN Services. Top10bestvpn [online]. [cit. 2017-8-18]. Dostupné z: http://www.top10bestvpn.com/compare

CRISTOBAL, Sab. Multi-Criteria Analysis: Chapter 2. Eprints.lse.ac.uk [online]. Hardcover, 2012 [cit. 2017-11-29]. Dostupné z: www.eprints.lse.ac.uk/12761/1/Multi-criteria_Analysis.pdf

DOLEŽAL, Dušan. Co to je digitální certifikát. Interval.cz [online]. 2003 [cit. 2017-10-08]. Dostupné z: https://www.interval.cz/clanky/co-to-je-digitalni-certifikat/

Encryption Keys. Asecuritysite [online]. [cit. 2017-10-10]. Dostupné z: https://asecuritysite.com/encryption/key

FERRO, Derek a Bill RINK. Understanding Technology OptionsforDeploying Wi-Fi. Ubeeinteractive [online]. 2014 [cit. 2016-10-25]. Dostupné z: http://www.ubeeinteractive.com/sites/default/files/Understanding%20Technology%20Options%20%20for%20Deploying%20Wi-Fi%20White%20Paper.pdf

FITZPATRICK, Jason. The DifferenceBetween WEP, WPA, and WPA2 Wi-Fi Passwords. Howtogeek [online]. 2016 [cit. 2017-9-19]. Dostupné z: https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

FRIEDEL, Steve. An IllustratedGuide to IPsec. Unixwiz.net [online]. 2005 [cit. 2016-11-08]. Dostupné z: http://www.unixwiz.net/techtips/iguide-ipsec.html

HALLER, Martin. Odposloucháváme data na přepínaném Ethernetu (5.). Lupa [online]. 2006 [cit. 2016-10-18]. Dostupné z: https://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-5/?ic=serial-box&icc=text-title

HELPTON, Shane. How to get HTTPS: Setting up SSL on yourwebsite. Howto-expert [online]. 2013 [cit. 2017-8-19]. Dostupné z: http://www.howto-expert.com/how-to-get-https-setting-up-ssl-on-your-website/

HRUŠKA, Pavel. Prolomení WPA/WPA2-PSK přes WPS snadno a rychle (praxe). Mrpear [online]. 2013 [cit. 2017-9-19]. Dostupné z: http://www.mrpear.net/cz/blog/435/prolomeni-wpa-wpa2-psk-pres-wps-snadno-a-rychle-praxe

IVANOV, Tihomir. END-TO-END ENCRYPTION VS LINK ENCRYPTION. Securegroup [online]. 2016 [cit. 2017-5-16]. Dostupné z: http://blog.securegroup.com/end-to-end-encryption-vs-link-encryption

KESSLER, Gary C. An Overview of Cryptography. Garykessler [online]. 2017 [cit. 2017-6-13]. Dostupné z: http://www.garykessler.net/library/crypto.html

KLÍMA, Vlastimil. Hašovací funkce, principy, příklady a kolize. Crypto-world [online]. 2005 [cit. 2016-11-11]. Dostupné z: http://crypto-world.info/klima/2005/cryptofest_2005.htm#_Toc98987052

KRČMÁŘ, Petr. Šifrování WPA2 prolomeno, Wi-Fi sítě je možné odposlouchávat. Root.cz [online]. 2017 [cit. 2017-2-20]. Dostupné z: https://www.root.cz/clanky/sifrovani-wpa2-bylo-prolomeno-wi-fi-site-je-mozne-odposlouchavat/

LÓRENCZ, Róbert Lórencz. Bezpečnost: 5. Hašovací funkce, MD5, SHA-x, HMAC. Edux.fit.cvut.cz [online]. Praha, 2011 [cit. 2017-9-15]. Dostupné z: https://edux.fit.cvut.cz/oppa/BI-BEZ/prednasky/bez5.pdf

LUHOV, Karel. VPN (3) – typologie virtuálních privátních sítí. Svetsiti [online]. 2003 [cit. 2017-10-18]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=VPN-3--typologie-virtualnich-privatnich-siti-1312003

MICROSOFT, WhatIs VPN? Www.technet.microsoft.com [online]. 2003 [cit. 2017-11-08]. Dostupné z: https://technet.microsoft.com/en-us/library/cc739294(v=ws.10).aspx

MIMOSO, Michael. Federal AgenciesTold to Support TLS 1.2 by 2015. Threatpost [online]. 2014 [cit. 2017-9-18]. Dostupné z: https://threatpost.com/federal-agencies-told-to-support-tls-1-2-by-2015/105906/

MITCHELL, Bradley. Introduction to Proxy Servers in Computer Networking. Lifewire [online]. 2016 [cit. 2017-9-18]. Dostupné z: https://www.lifewire.com/introduction-to-proxy-servers-computer-networking-816448

MS, Anoop. Public Key Cryptography: ApplicationsAlgorithms and Mathematical Explanations. Infosecwriters [online]. India, 2007 [cit. 2017-3-19]. Dostupné z: http://www.infosecwriters.com/text_resources/pdf/Public_Key_Cryptography_AMS.pdf

O DOMÉNÁCH A DNS. Dnssec [online]. CZ.NIC, 2017 [cit. 2017-2-18]. Dostupné z: https://www.dnssec.cz/page/312/o-domenach-a-dns/

ONYSZKO, Tomasz. Secure Socket Layer. Techgenix [online]. 2002 [cit. 2017-5-1]. Dostupné z: http://techgenix.com/secure_socket_layer/

OpenSSL FIPS Object Module SE: OpenSSL FIPS 140-2 Security Policy. Openssl [online]. 2016 [cit. 2017-10-18]. Dostupné z: https://www.openssl.org/docs/fips/SecurityPolicy-2.0.13.pdf

OpenVPN. OpenVPN [online]. [cit. 2017-10-18]. Dostupné z: https://openvpn.net/

Overview of virtual private networks (VPN). Technet.microsoft.com [online]. 2017 [cit. 2017-9-08]. Dostupné z: https://technet.microsoft.com/en-us/library/cc995148.aspx

PAN_R. Jak funguje IPSEC? Security-portal [online]. 2005 [cit. 2016-7-18]. Dostupné z: http://www.security-portal.cz/clanky/jak-funguje-ipsec

PAVLIS, Jakub. Bezpečnost na sítích II. – šifrování. Notebook [online]. 2013 [cit. 2017-10-08]. Dostupné z: https://notebook.cz/clanky/technologie/2013/bezpecnost-na-sitich-ii-sifrovani

PETERKA, Jiří. Jména v TCP/IP sítích - I. Earchiv [online]. 1992 [cit. 2016-9-1]. Dostupné z: http://www.earchiv.cz/a92/a244c110.php3

PETERKA, Jiří. Referenční model ISO/OSI – sedm vrstev. Www.earchiv.cz [online]. 1992 [cit. 2016-10-15]. Dostupné z: http://www.earchiv.cz/a92/a213c110.php3

PETERKA, Jiří. Síťový model TCP/IP. Http://www.earchiv.cz/ [online]. 1992 [cit. 2016-9-1]. Dostupné z: http://www.earchiv.cz/a92/a231c110.php3

PETERKA, Jiří. TCP a UDP. Earchiv [online]. 1999 [cit. 2016-9-2]. Dostupné z: http://www.earchiv.cz/anovinky/ai1864.php3

Point-to-Point Tunneling Protocol. Technet.microsoft [online]. Microsoft [cit. 2017-9-18]. Dostupné z: https://technet.microsoft.com/en-us/library/cc958045.aspx

PORNIN, Thomas. Howdoes SSL/TLS work? Informationsecurity [online]. [cit. 2017-4-25]. Dostupné z: https://security.stackexchange.com/questions/20803/how-does-ssl-tls-work

POSTEL, J. User Datagram Protocol. Internet Engineering Task Force [online]. 1980 [cit. 2017-1-11]. Dostupné z: https://www.ietf.org/rfc/rfc768.txt

REDAKCE PCT. Moderní metody šifrování. Pctuning [online]. 2005 [cit. 2017-6-13]. Dostupné z: http://pctuning.tyden.cz/software/ochrana-soukromi/4711-moderni_metody_sifrovani

RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1. Internet Engineering Task Force [online]. California, 1999 [cit. 2017-1-15]. Dostupné z: https://tools.ietf.org/html/rfc2616

RFC: 793: Transmission Control Protocol. Internet Engineering Task Force [online]. California, 1981 [cit. 2017-2-12]. Dostupné z: https://www.ietf.org/rfc/rfc793.txt

ŘEZNÍČEK, Josef. Tvoříme persony pro obsahový marketing. Vceliste.cz [online]. 2016 [cit. 2017-11-29]. Dostupné z: https://vceliste.cz/blog/tvorime-persony-pro-obsahovy-marketing/

SANDERS, Chris. Understanding Man-In-The-Middle Attacks: Part2: DNS Spoofing. TechGenix [online]. 2010 [cit. 2016-10-18]. Dostupné z: http://techgenix.com/Understanding-Man-in-the-Middle-Attacks-ARP-Part2/

SATRAPA, Pavel. Jak funguje nový protokol HTTP/2. ROOT [online]. 2015 [cit. 2017-1-18]. Dostupné z: https://www.root.cz/clanky/jak-funguje-novy-protokol-http-2/

SOUKOPOVÁ, Jana. Vícekriteriální metody hodnocení. Muni [online]. 2012 [cit. 2017-10-19]. Dostupné z: https://is.muni.cz/el/1456/jaro2013/MKV_VZVP/um/33149329/33203827/

SPDY: An experimental protocol for a faster web. Chromium [online]. [cit. 2017-8-19]. Dostupné z: https://www.chromium.org/spdy/spdy-whitepaper

SSL versus TLS – What's the difference? Luxsci [online]. 2017 [cit. 2017-8-18]. Dostupné z: https://luxsci.com/blog/ssl-versus-tls-whats-the-difference.html

SUNNY, Hoi. WhichIsBetter: TOR over VPN Or VPN over TOR? Www.sunnyhoi.com [online]. 2017 [cit. 2017-10-22]. Dostupné z: https://www.sunnyhoi.com/which-is-better-tor-over-vpn-or-vpn-over-tor/

The TLS Protocol Version 1.0. Internet Engineering Task Force [online]. The Internet Society, 1999 [cit. 2017-4-15]. Dostupné z: https://tools.ietf.org/html/rfc2246

The Transport Layer Security (TLS) Protocol Version 1.2. Internet Engineering Task Force [online]. The Internet Society, 2008 [cit. 2017-8-17]. Dostupné z: https://www.ietf.org/rfc/rfc5246.txt

Tor: HiddenService Protocol. Torproject [online]. [cit. 2017-7-15]. Dostupné z: https://www.torproject.org/docs/hidden-services.html.en

Tor: Overview. Torproject [online]. [cit. 2017-7-15]. Dostupné z: https://www.torproject.org/about/overview.html.en

US Secure Hash Algorithm 1 (SHA1). Internet Engineering Task Force [online]. 2001 [cit. 2016-10-23]. Dostupné z: https://tools.ietf.org/html/rfc3174

WHONIX. Combining Tunnels with Tor. Www.whonix.org [online]. 2017 [cit. 2017-10-22]. Dostupné z: https://www.whonix.org/wiki/Tunnels/Introduction#Introduction

WONG, Stanley. The evolution of Wireless security in 802.11 networks: WEP, WPA and 802.11 standards [online]. 2003 [cit. 2017-9-19]. Dostupné z: https://www.sans.org/reading-room/whitepapers/wireless/evolution-wireless-security-80211-networks-wep-wpa-80211-standards-1109

WRIGHT, Dan. The RSA Algorithm. Mcmaster [online]. 2007 [cit. 2016-11-10]. Dostupné z: http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/wrighd/rsa_alg.html