

**Technická univerzita v Košiciach  
Fakulta elektrotechniky a informatiky**

# **Ľahká kryptografia vo VPN sieťach**

**Diplomová práca**

**2023**

**Bc. Marek Roháč**

**Technická univerzita v Košiciach  
Fakulta elektrotechniky a informatiky**

# **Ľahká kryptografia vo VPN sieťach**

**Diplomová práca**

Študijný program: Počítačové siete  
Študijný odbor: Informatika  
Školiace pracovisko: Katedra elektroniky a multimediálnych telekomunikácií (KEMT)  
Školiteľ: prof. Ing. Miloš Drutarovský, CSc.  
Konzultant:

**Košice 2023**

**Bc. Marek Roháč**

## **Abstrakt v SJ**

slovak

## **Kľúčové slová v SJ**

DSVPN, Ľahká kryptografia, Linux, VPN, Windows, XOODOO

## **Abstrakt v AJ**

english

## **Kľúčové slová v AJ**

DSVPN, Lightweight Cryptography, Linux, VPN, Windows, XOODOO

## **Bibliografická citácia**

ROHAČ, Bc. Marek. *Ľahká kryptografia vo VPN sieťach*. Košice: Technická univerzita v Košiciach, Fakulta elektrotechniky a informatiky, 2023. 84s. Vedúci práce: prof. Ing. Miloš Drutarovský, CSc.

**TECHNICKÁ UNIVERZITA V KOŠICIACH**  
**FAKULTA ELEKTROTECHNIKY A INFORMATIKY**  
Katedra elektroniky a multimediálnych telekomunikácií

# **ZADANIE DIPLOMOVEJ PRÁCE**

Študijný odbor: **Informatika**  
Študijný program: **Počítačové siete**

Názov práce:

**L'ahká kryptografia vo VPN sieťach**  
Lightweight Cryptography in VPN Networks

Študent: **Bc. Marek Rohač**  
Školiteľ: **prof. Ing. Miloš Drutarovský, CSc.**  
Školiace pracovisko: **Katedra elektroniky a multimediálnych telekomunikácií**  
Konzultant práce:  
Pracovisko konzultanta:

Pokyny na vypracovanie diplomovej práce:

Na základe dostupných informácií naštudujte a opište kryptografickú permutáciu XOODOO využívanú v ľahkej kryptografii. Analyzujte a opište dostupné implementácie, ktoré využívajú XOODOO permutáciu v zabezpečení VPN siete. V jazyku C vytvorte demonštračné aplikácie jednoduchej VPN siete využívajúce XOODOO permutáciu na platformách Linux alebo Windows a experimentálne overte ich funkčnosť. Analyzujte aké výpočtové nároky má vytvorená implementácia. Dokumentáciu k diplomovej práci vytvorte tak, aby ju bolo možné využiť aj v špecializovaných predmetoch zameraných na bezpečnosť informačných a komunikačných systémov.

Jazyk, v ktorom sa práca vypracuje: **slovenský**  
Termín pre odovzdanie práce: **21.04.2023**  
Dátum zadania diplomovej práce: **31.10.2022**



prof. Ing. Liberios Vokorokos, PhD.  
dekan fakulty

## **Čestné vyhlásenie**

Vyhlasujem, že som záverečnú prácu vypracoval samostatne s použitím uvedenej odbornej literatúry.

Košice, 28. 5. 2023

.....

*Vlastnoručný podpis*

## **Podakovanie**

Na tomto mieste by som rád poďakoval svojmu vedúcemu práce *prof. Ing. Milošovi Drutarovskému, CSc.* za jeho čas a odborné vedenie počas celého riešenia záverečnej práce.

# Obsah

---

<b>Zoznam skratiek</b>	<b>xiii</b>
<b>Úvod</b>	<b>1</b>
<b>1 Virtual Private Network – VPN</b>	<b>2</b>
1.1 Výhody a nevýhody VPN sieti . . . . .	3
1.2 Charakteristika a definovanie pojmov . . . . .	3
1.2.1 Tunel a tunelovacie rozhrania . . . . .	3
1.2.2 Charakteristika referenčných modelov . . . . .	5
1.2.3 IKEv2 Internet Key Exchange version 2 . . . . .	10
1.2.4 Transport Layer Security – TLS . . . . .	10
1.2.5 Point-to-Point Protocol (PPP) . . . . .	11
1.2.6 Multiprotocol Label Switching (MPLS) . . . . .	11
1.3 Klasifikácia VPN sietí . . . . .	12
1.3.1 Rozdelenie VPN sieti podľa logickej topológie . . . . .	12
1.3.2 Rozdelenie VPN sieti podľa vrstiev referenčného modelu . .	15
1.4 Protokoly vo VPN sieťach . . . . .	16
1.4.1 Point-to-Point Tunneling Protocol (PPTP) . . . . .	17
1.4.2 Layer 2 Tunneling Protocol (L2TP) . . . . .	19
1.4.3 Internet Protocol Security (IPSec) . . . . .	21
1.4.4 Secure Socket Tunneling Protocol (SSTP) . . . . .	23
1.4.5 Ostatné populárne VPN protokoly . . . . .	25
1.5 Zhrnutie VPN sieti . . . . .	28
<b>2 Ľahká kryptografia</b>	<b>29</b>
2.1 Kryptografická permutácia XOODOO a jej variácie . . . . .	31
2.1.1 XOODOO permutácia . . . . .	32
2.1.2 Kryptografický balíček Xoodyak . . . . .	34
2.1.3 Možnosti použitia Xoodyak algoritmu . . . . .	37

---

<b>3</b>	<b>Konfigurácia prostredia, metodika testovania a merania</b>	<b>43</b>
3.1	Prostredie virtuálnych strojov pomocou VirtualBox . . . . .	43
3.1.1	Zmena sieťových adaptérov . . . . .	44
3.2	Nástroje použité v obrazoch a v práci . . . . .	45
<b>4</b>	<b>Implementácia jednoduchej VPN siete</b>	<b>46</b>
4.1	Dead Simple VPN . . . . .	46
4.2	Kryptografia použitá v DSVPN . . . . .	48
4.3	Experimentálne overenie VPN . . . . .	48
4.4	Princíp fungovania programu . . . . .	50
4.5	Analýza zdrojového kódu DSVPN . . . . .	52
4.5.1	Súbor charm.h a charm.c . . . . .	54
4.5.2	Súbor os.h a os.c . . . . .	54
4.5.3	Súbor vpn.h a vpn.c . . . . .	55
4.6	Analýza výpočtových nárokov DSVPN . . . . .	71
4.7	Windows kompatibilita . . . . .	74
<b>5</b>	<b>Vyhodnotenie dosiahnutých výsledkov</b>	<b>75</b>
<b>6</b>	<b>Záver</b>	<b>76</b>
	<b>Literatúra</b>	<b>77</b>
	<b>Zoznam príloh</b>	<b>85</b>
<b>A</b>	<b>Obsah CD Média</b>	<b>86</b>



# Zoznam obrázkov

---

1.1	Ukážka typického VPN pripojenia . . . . .	2
1.2	vpn fancy obrazok . . . . .	3
1.3	<a href="https://www.comptia.org/blog/open-systems-interconnection-reference-model">https://www.comptia.org/blog/open-systems-interconnection-reference-model</a> - dobry zdroj na rozsirenje . . . . .	6
1.4	Schéma TCP/IP modelu s niektorými protokolmi . . . . .	7
1.5	spoj tento obrazok s nasledujucim do jedneho . . . . .	8
1.6	spoj tento obrazok s predchadzajucim do jedneho, plus 1.3 . . . . .	9
1.7	Prehľad operácií v SSL protokole . . . . .	11
1.8	. . . . .	12
1.9	potrebne prerobenie nech sa to nepodoba na 1.1 alebo vyhodit/upravit 1.1 . . . . .	13
1.10	rearanzovat . . . . .	14
1.11	zacomponovat k osi vysvetleniu . . . . .	15
1.12	potreba upravy iba na spoemnute vrstvy . . . . .	16
1.13	Architektura PPTP siete - PPTP je az od nas do PS . . . . .	17
1.14	lepsi obrazok . . . . .	17
1.15	sede sifrovane biele nie . . . . .	18
1.16	. . . . .	20
1.17	IPSec transportný režim . . . . .	22
1.18	IPSec tunelovací režim . . . . .	22
1.19	Proces enkapsulácie PPP rámcov pomocou protokolov naprieč SSTP protokolom . . . . .	24
1.20	. . . . .	26
2.1	Grafické znázornenie terminológie využitej v kryptografickej permutácii XOODOO [60] . . . . .	32
2.2	Grafické znázornenie operácie $\chi$ [60] . . . . .	33
2.3	Grafické znázornenie operácie $\rho$ [60] . . . . .	34
2.4	Ilustrácia miešania vrstiev $\rho_{west}$ (vľavo) a $\rho_{east}$ (vpravo)[60] . . . . .	34

---

2.5	Charakteristika operácií v algoritmickom zápise kryptografickej permutácie XOODOO [60] . . . . .	34
2.6	Algoritmický zápis kryptografickej permutácie XOODOO [60] . . .	35
2.7	Súbor rundových konštánt kryptografického algoritmu XOODOO [60] . . . . .	35
3.1	Konektivita jednotlivých sieťových adaptérov . . . . .	45
4.1	Schéma jednoduchej VPN . . . . .	47
4.2	Zistenie IP adres VPN Servera na VM OSS . . . . .	50
4.3	Zistenie IP adres VPN Klienta na VM OSC . . . . .	51
4.4	Overenie funkcionality DSVPN pomocou traceroute . . . . .	51
4.5	Ukážka prenosu paketu naprieč DSVPN . . . . .	53
4.6	Beh DSVPN . . . . .	60
4.7	Princíp fungovania funkcie doit() . . . . .	61
4.8	Proces šifrovania v funkcii uc_encrypt() . . . . .	64
4.9	Prenos zašifrovaných dát z VPN klienta na VPN server . . . . .	70
4.10	Obsah pôvodného paketu s ICMP žiadosťou . . . . .	70
4.11	Zašifrovaný pôvodný ICMP paket v novom TCP package . . . . .	71

# Zoznam tabuliek

---

4.1	Výsledky získaných meraní . . . . .	73
-----	-------------------------------------	----

# Zoznam zdrojových kódov

---

4.1	Obsah charm.h . . . . .	54
4.2	Obsah ZK os.h . . . . .	55
4.3	Obsah ZK vpn.h . . . . .	56
4.4	Štruktúra Context . . . . .	57
4.5	Načítanie zdieľaného kľúča . . . . .	58
4.6	Premenné funkcie event loop . . . . .	61
4.7	Spôsob zápisu šifrovaných dát . . . . .	63
4.8	Príprava dát na ďalšie čítanie . . . . .	63
4.9	Šifrovanie správy pomocou uc_encrypt . . . . .	65
4.10	Funkcia xor128 . . . . .	66
4.11	Funkcia Permute + makrá . . . . .	67
4.12	Funkcia Permute + makrá . . . . .	69
4.13	Ukážka spôsobu merania pri (de)šifrovaní XOODOO . . . . .	72
4.14	Meranie času vykonávania na OS Windows . . . . .	72

# Zoznam skratiek

---

**AES** Advanced Encryption Standard.

**AH** Authentication Header.

**CHAP** Challenge Handshake Authentication Protocol.

**ECC** Elliptic Curve Cryptography.

**ECDH** Elliptic-Curve Diffie–Hellman.

**ECDSA** Elliptic Curve Digital Signature Algorithm.

**ESP** Encapsulating Security Payloads.

**FSKD** Full-State Keyed Duplex.

**FTP** File Transfer Protocol.

**FW** FireWall.

**GRE** Generic Routing Encapsulation.

**GW** GateWay.

**HTTP** HyperText Transfer Protocol.

**HTTPS** HyperText Transfer Protocol Secure.

**IOT** Internet Of Things.

**IP** Internet Protocol.

**IPSec** Internet Protocol Security.

**ISAKMP** Internet Security Association and Key Management Protocol.

**KP** Cryptographical Primitive.

**L** Layer.

**L2F** Layer 2 Forwarding protocol.

**L2TP** Layer 2 Tunneling Protocol.

**LAC** L2TP Access Concentrator.

**LNS** L2TP Network Server.

**LTS** Long Term Support.

**LWC** LightWeight Cryptography.

**LWCA** LightWeight Cryptography Algorithm.

**MPLS** Multiprotocol Label Switching.

**MS-CHAP** MicroSoft Challenge Handshake Authentication Protocol.

**NAS** Network Access Server.

**NAT** Network Address Translation.

**NIST** National Institute of Standards and Technology.

**OS** Operating System.

**OSI** Open Systems Interconnection reference model.

**PAP** Password Authentication Protocol.

**PDV** Packet Delay Variation.

**PPP** Point-to-Point Protocol.

**PPPoE** PPP over Ethernet.

**PPTP** Point-to-Point Tunneling Protocol.

**RFC** Request For Comments.

**RSA** Rivest–Shamir–Adleman.

**SA** Security Associations.

**SMTP** Simple Mail Transfer Protocol.

**SSL** Secure Socket Layers.

**SSTP** Secure Socket Tunneling Protocol.

**TCP** Transmission Control Protocol.

**TCP/IP** Transmission Control Protocol/Internet Protocol reference model.

**TLS** Transport Layer Security.

**UDP** User Datagram Protocol.

**VB** Virtual Box.

**VM** Virtual Machine.

**VPN** Virtual Private Network.

**XOF** eXtendable-Output Function.

# Úvod

---

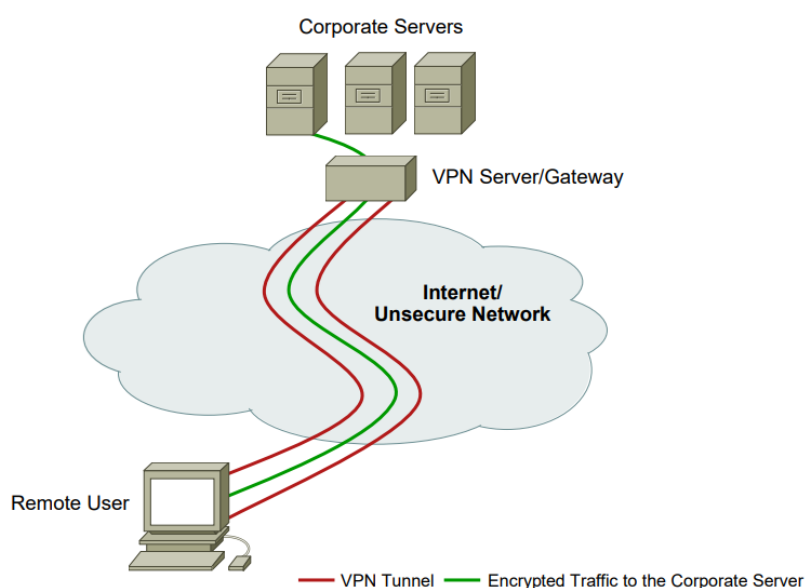
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilissem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi necante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero utmetus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amecante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.VPN [**book**]



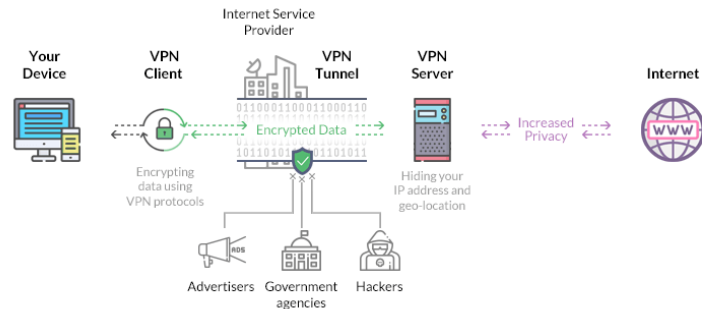
# 1 Virtual Private Network – VPN

---

Virtuálna privátna sieť (ďalej **VPN**) je jeden zo spôsobov prepojenia zariadení, tak že internetová komunikácia medzi nimi je privátna, resp. zabezpečená aj v prípade používania nezabezpečenej, verejnej siete. Bezpečnosť spojenia je docieľaná pomocou kryptografických protokolov v tuneli, ktorý VPN vytvára. Pod pojmom tunel sa v skutočnosti myslí virtuálna zašifrovaná linka, ktorou je dátový paket prenášaný po sieti medzi koncovými zariadeniami. V skutočnosti tunel vzniká pomocou procesu zapuzdrenia dát. V závislosti od toho na akej úrovni OSI referenčného modelu sa pohybujeme. Táto technológia patrí aktuálne k najpoužívanejším spôsobom pripojenia sa medzi 2 rôznymi internetovými doménami. Najčastejší výskyt je možné sledovať v korporačnom prostredí, pričom cieľom je rozšírenie možností bezpečného pripojenia sa k firemnej sieti. Vzhľadom na firemné tajomstvá je nutné aby bolo takéto spojenie bezpečné a zamestnanci sa mohli pripojiť z rôznych miest. Vďaka uvedeným vlastnostiam je následne možná aj práca z domu (z ang. *Home office*), ktorá môže byť benefitom pre obe strany. Ukážka použitia VPN je znázornená pomocou 1.1 a 1.2.



Obr. 1.1: Ukážka typického VPN pripojenia



Obr. 1.2: vpn fancy obrazok

<https://www.webhostingsecretrevealed.net/blog/security/how-vpn-works/>

## 1.1 Výhody a nevýhody VPN sieti

neviem ci to bude rozsahovo treba na samostatnu podkapitolu mozno len doplnit informacie do textu zaciatku.

V prípade nestabilného spojenia, je možný vysoký výskyt straty paketov. Dôvodom je použitie TCP protokolu. Takýto problém je vhodné riešiť, tak sa odporúča prejsť na protokol

## 1.2 Charakteristika a definovanie pojmov

Obsahom tejto podkapitoly je zavedenie a následne stručná charakteristika pojmov, potrebných na pochopenie problematiky VPN sieti.

### 1.2.1 Tunel a tunelovacie rozhrania

**Tunel** v počítačových sieťach predstavuje virtuálne spojenie medzi jedným alebo viacerými zariadeniami. Jeho obsahom sa prenášajú enkapsulované, resp. zapuzdrené dáta. Proces pridávania dát k pôvodným sa v tejto súvislosti zvykne taktiež označovať ako **tunelovanie**. V počítačových sieťach je týmto spôsobom možné zmeniť, resp. zameniť použitý protokol za iný. Príkladom by mohlo byť tunelovanie z IPv4 do IPv6. V uvedenom prípade sa z pôvodného paketu použijú dáta a k nim sa pridajú údaje potrebné na smerovanie v IPv6 sieti. Výhodou je, že týmto spôsobom vieme sprostredkovať kompatibilitu naprieč viacerými sieťami s rôznymi protokolmi. Obdobne vieme do procesu tunelovania začleniť aj bezpečnostné prvky v podobe šifrovania a autentizácie pôvodných dát. V súvislosti s

tunelmi sa používateľ môže stretnúť s pojmami tunelovací protokol a tunelovacie rozhranie.

**Tunelovací protokol** predstavuje súbor činností, ktoré sú v procese tunelovania vykonávajú. V súčasnosti existuje veľa protokolov, ktoré sú štandardne špecifikované a bežne používané v sieťovej komunikácii. Najčastejšie sa používateľ stretne s tunelovaním pri VPN sieťach. Niektoré VPN v sebe nesú názov použitého tunelovacieho protokolu. Za spomenutie stojí protokol *Generic Routing Encapsulation* (ďalej GRE). GRE je tunelovací protokol vyvinutý spoločnosťou Cisco v roku 1994. Ponúka širokú paletu možností tunelovania viacerých sieťových protokolov vo virtuálnych spojeniach medzi zariadeniami, tzv. z ang. *point-to-(multi)point*. Niektoré variácie sa používajú aj pri vytváraní VPN. Viac informácií o GRE je dostupné na [1] a [2].

**Tunelovacie rozhranie**, resp. adaptér je virtuálne zariadenie, ktoré je možné vytvárať v jadre daného operačného systému. Jedná sa o kompletne softvérové riešenie. Dôležité je, že nie každý OS má natívnu podporu pre vytváranie virtuálnych tunelovacích rozhraní. Je preto potrebné používať ovládače tretích strán, ktoré danú funkcionality implementujú. Od roku 2000 podporujú tieto rozhrania Solaris, Linux a BSD operačné systémy. Poznáme dva typy tunelovacích rozhraní. Konkrétne TAP a TUN rozhranie. Nedajú sa použiť spolu, pretože pracujú na rôznych vrstvách. TUN simuluje správanie zariadenia na sieťovej vrstve (L3) a teda spracúva pakety a používa sa pri smerovaní. Na druhej strane TAP rozhranie pracuje o úroveň nižšie s ethernetovými rámcami (L2). Používa sa na premostenie sieťovej premávky. TUN/TAP rozhrania je možné použiť na odosielanie a prijímanie dát. Dáta odoslané OS do TUN/TAP sú dodávané do programu, ktorý rozhrania vytvoril. Na druhej strane používateľ môže v programe taktiež odoslať dáta do rozhraní. V tomto prípade TUN/TAP vloží dáta do sieťového zásobníka OS. Tým emuluje ich príjem z externého zdroja.

Technológia TUN/TAP je pomerne známa a zaužívaná. Svoje uplatnenie zohráva pri softvérovej implementácii VPN. Okrem toho sa bežne používa aj vo sfére virtuálnych strojov. Napríklad aj vo voľne dostupný nástroji na virtualizáciu – VirtualBox. Pri vytvorení a následnom používaní obrazu, dochádza k vytváraniu tunelovacích rozhraní. Prostredníctvom zvolenej konfigurácie stroja sa rozhrania nakonfigurujú. Týmto spôsobom sa pre používateľa sprístupní možnosť komunikácie virtuálneho stroja s inými zariadeniami. Viac informácií o problematike je možné nájsť na [3], [4] a [5], odkiaľ bol obsah tejto kapitoly čerpaný.

## 1.2.2 Charakteristika referenčných modelov

Pred podkapitolou 1.3.2 je potrebné pred samotnou klasifikáciou vysvetliť pojmy Referenčný model prepojenia otvorených systémov<sup>1</sup> (ďalej OSI) a Model opisujúci balíky internetových protokolov, známy ako, TCP/IP referenčný model.

Úlohou uvedených referenčných modelov je vizualizácia postupu spracovania dát od používateľa až k ich odoslaniu zo zariadenia<sup>2</sup>. Pojem spracovanie dát znamená opísanie toho ako dochádza v jednotlivých abstraktných vrstvách k pretransformovaniu používateľských dát na súbor jednotiek a núl, ktoré sú následne odoslané do iného zariadenia.

OSI Model vznikol v skorších fázach evolúcie počítačových sietí. Vychádza skôr z teoretického než praktického prístupu. Pozostáva zo 7 abstraktných vrstiev<sup>3</sup>:

1. **fyzická vrstva** – z ang. *Physical Layer* (ďalej L1),
2. **spojová vrstva** – z ang. *Data Link Layer* (ďalej L2),
3. **sieťová vrstva** – z ang. *Network Layer* (ďalej L3),
4. **transportná vrstva** – z ang. *Transport Layer* (ďalej L4),
5. **relačná vrstva** – z ang. *Session Layer* (ďalej L5),
6. **prezenčná vrstva** – z ang. *Presentation Layer* (ďalej L6),
7. **aplikačná vrstva** – z ang. *Application Layer* (ďalej L7).

V schéme 1.3 sa nachádzajú stručne opísané jednotlivé činnosti vrstiev.

Čím je väčšie číslo vrstvy tým bližšie sa dáta nachádzajú pri používateli. Vďaka uvedeným vlastnostiam je tento model vhodnejší pri začiatku štúdia spracovania sieťových dát v počítači. Z rovnakého dôvodu sa taktiež viac stretávame s jeho použitím pri opise funkcionality riešenia ako s TCP/IP novším modelom. Viac informácií o problematike nájde čitateľ v [osi].

Na druhej strane TCP/IP model vznikol z praktického prístupu. Hlavný rozdiel je v počte abstraktných vrstiev, ktorý je v prípade TCP/IP zmenšený na 4 vrstvy [tcpip]. TCP/IP model je zobrazený pomocou schémy 1.4. V uvedenej schéme sú znázornené aj niektoré z protokolov, ktoré sa na jednotlivých vrstvách používajú.

<sup>1</sup> z ang. *Open Systems Interconnection reference model*

<sup>2</sup> z ang. *end-to-end data communication*

<sup>3</sup> z ang. *layer*

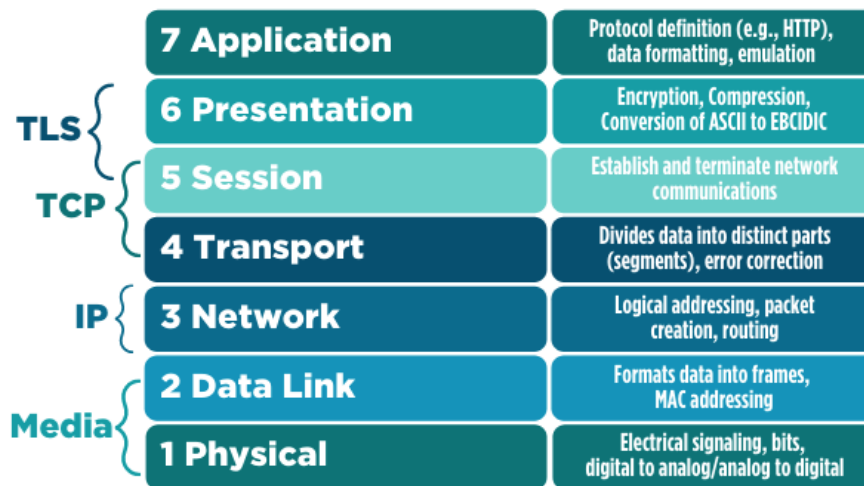


Figure 2: Mapping protocols and procedures to the OSI/RM

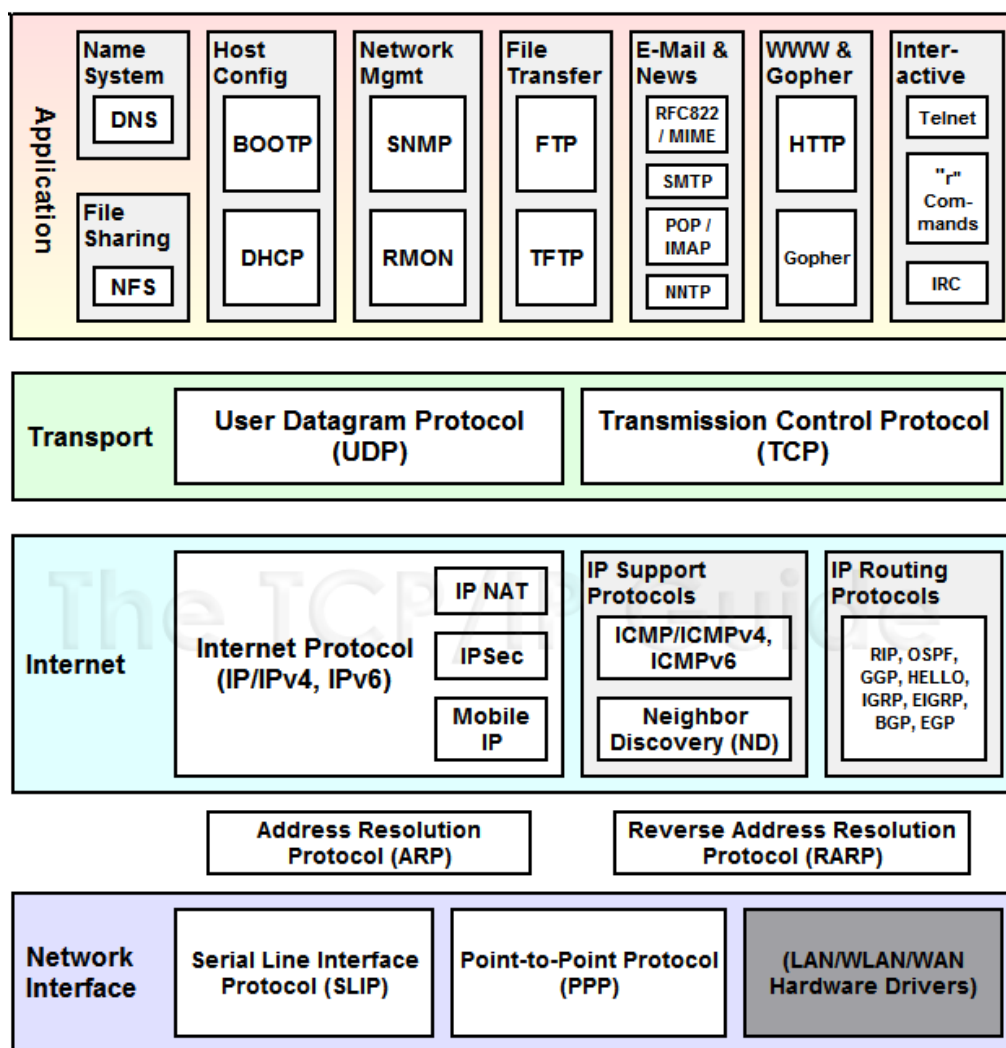
Obr. 1.3: <https://www.comptia.org/blog/open-systems-interconnection-reference-model> - dobrý zdroj na rozšírenie

**Aplikačná vrstva (L5-7)** zahŕňa protokoly používané väčšinou aplikácií na poskytovanie užívateľských služieb alebo výmenu aplikačných dát cez sieťové pripojenia, ktoré je vytvorené protokolmi na nižšej úrovni. Spája vrstvy L5 až L7 OSI modelu. Príklady známych protokolov aplikačnej vrstvy sú HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) a iné. Údaje, resp. dáta sú pri spracovaní kódované podľa L4 protokolov. Sú zapuzdrené do protokolových jednotiek transportnej vrstvy, tzv. **segmentov**.

**Transportná vrstva (L4)** vytvára základné dátové kanály, ktoré aplikácie používajú na výmenu dát. Vrstva vytvára konektivitu medzi hostiteľmi, ktorá je nezávislá od siete, štruktúry užívateľských dát a smerovacích informácií. Konektivita na transportnej vrstve môže byť kategorizovaná ako orientovaná na spojenie, implementovaná v protokole TCP, alebo UDP bez orientácie na spojenie. Uvedené protokoly sú stručne charakterizované nižšie, v tejto podkapitole.

Protokoly v tejto vrstve zabezpečujú:

- riadenie chýb – z ang. *error control* [**ec**],
- segmentáciu dát – z ang. *segmentation* [**sd**],
- riadenie toku dát – z ang. *flow control* [**fc**],
- riadenie preťaženia – z ang. *congestion control* [**cc**],
- adresovanie aplikácií – z ang. *application addressing* [**aa**].



Obr. 1.4: Schéma TCP/IP modelu s niektorými protokolmi

Výstupom transportnej vrstvy sú segmenty, ktoré sú spracované v ďalšej vrstve referenčného modelu.

**Internetová, resp. Sieťová vrstva (L3)** je zodpovedná za odosielanie paketov cez jednu alebo viac sietí. S touto funkcionalitou internetová vrstva umožňuje sieťovanie, prepojenie rôznych IP sietí a v podstate vytvára internet. Z L4 segmentov tvorí pakety, tak že pridá informácie potrebné na ďalšie smerovanie.

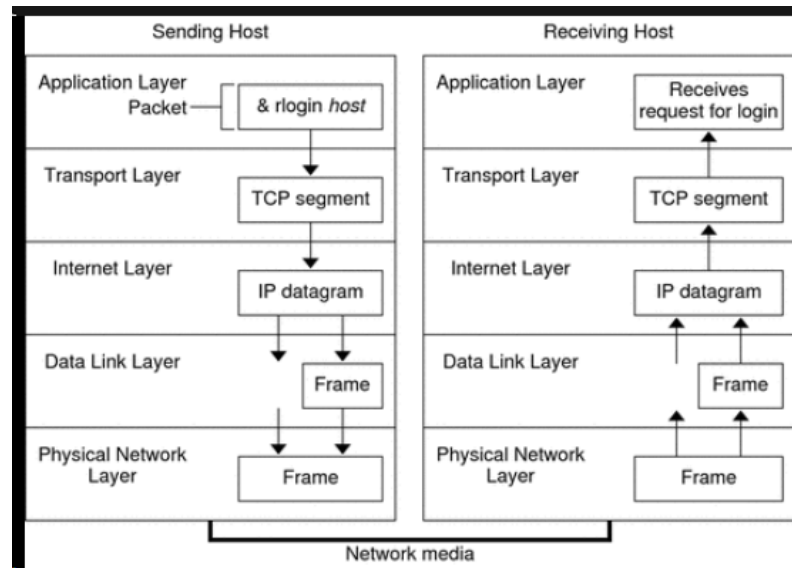
**Linková vrstva (L2)** sa používa na presun paketov medzi rozhraniami internetovej vrstvy dvoch rôznych hostiteľov na rovnakom linku. Procesy vysielania a prijímania paketov na linke je možné konfigurovať. Zariadenia nazývané prepínače<sup>4</sup>, vykonávajú rámcovania<sup>5</sup>. Pripravujú pakety z L3 vrstvy na prenos prídáním ďalších informácií. Týmto úkonom vzniknú rámce. Tie sa prenášajú do fyzickej vrstvy a cez prenosové médium až k hostiteľovi. Fyzická vrstva predstavuje

<sup>4</sup>z ang. *switch*

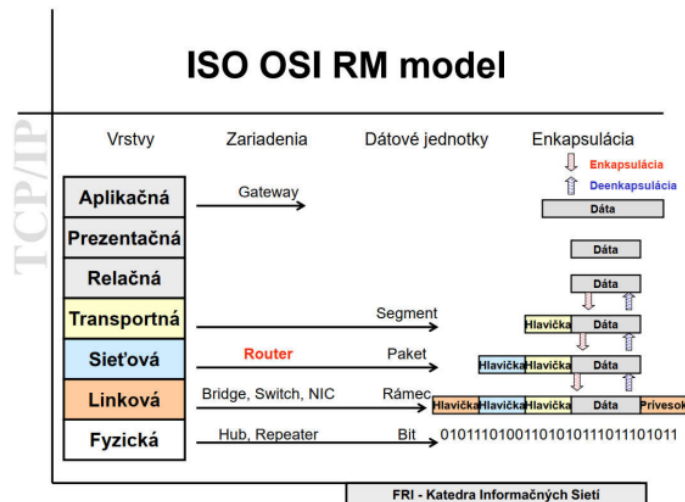
<sup>5</sup>z ang. *frame*

prvok, cez ktoré sú dáta prenášané. Napríklad optický a ethernetový kábel.

Vyššie uvedené procesy prípravy dát sú znázornené pomocou schémy 1.5 a 1.6.



Obr. 1.5: spoj tento obrazok s nasledujucim do jedneho



Obr. 1.6: spoj tento obrazok s predchadzajucim do jedneho, plus 1.3

**Protokol riadenia prenosu** (z ang. *Transmission Control Protocol*, ďalej TCP) je komunikačný protokol orientovaný na nadviazanie a udržanie sieťového spojenia medzi zariadeniami. Môže byť použitý pri úlohe prijímateľa aj odosielateľa (z ang. *full-duplex*). Úlohou je spoľahlivý prenos dát medzi komunikantmi. Odoslanie a príjem dát je v rovnakom poradí. Protokol zároveň obsahuje mechanizmy na kontrolu výskytu chýb. Svoj názov má podľa dvoch najdôležitejších protokolov:

- Protokol riadenia prenosu – z ang. *Transmission Control Protocol*,
- Internet protokol – z ang. *Internet Protocol*.

Na začiatku 21. storočia je 95% paketov používaných na internete TCP. Bežné aplikácie používajúce TCP sú webové (HTTP/HTTPS protokoly), slúžiace na e-mailovú komunikáciu (SMTP/POP3/IMAP) a prenos súborov (z ang. *File Transfer Protocol – FTP*). Minimálna dĺžka hlavičky TCP je 20 bajtov a maximálna dĺžka 60 bajtov. Po pridaní údajov TCP hlavičky k prenášaným dátam, vzniká tzv. *segment*.

V súčasnosti je možné TCP protokol implementovať softvérovo aj hardvérovo. Pri prvom z uvedených je problémom závislosť na OS a následne aj vysoká vyťaženosť procesora pri príprave a spracovaní dát. Pri hardvérovom riešení je výhodou optimalizácia a implementácia bez potreby dodatočnej úpravy OS. Hardvérové implementácie sa realizujú pomocou koprocessorov umiestnených vo vnútri procesora. Následkom toho môžeme dnes bežne pozorovať umiestnenie spomenutých zariadení na našich zariadeniach.

Podrobnejšie informácie o TCP protokole je možné nájsť na [11]. V uvedenej publikácii sa nachádza opis TCP hlavičky, metódy nadviazania a ukončenia spo-



jenia. Obdobne je spomenuté ako dochádza k prenosu dát pomocou sekvenčných čísel. Ak má používateľ nejasnosti v fungovaní TCP protokolu, odporúča sa danú publikáciu prečítať.

**Používateľský datagramový protokol** (z ang. *User Datagram Protocol*, ďalej UDP) je jedným zo základných komunikačných IP protokolov. Používa sa na odosielanie správ iným hostiteľom v sieti. Správy sú prenášané ako datagramy v paketoch. UDP nevyžaduje predchádzajúcu komunikáciu na nastavenie komunikačných kanálov alebo dátových ciest. Používa jednoduchý komunikačný model bez spojenia s minimom protokolových mechanizmov. Poskytuje kontrolné súčty pre integritu údajov a čísla portov na adresovanie rôznych funkcií v zdroji a ciele datagramu.

Narozdiel od TCP) neposkytuje žiadnu záruku doručenia správy alebo duplicitnej ochrany. UDP) je vhodný na účely, kde kontrola a oprava chýb buď nie sú potrebné, alebo sa vykonávajú v aplikácii. Aplikácie citlivé na čas často používajú UDP, pretože zahadzovanie paketov je vhodnejšie ako čakanie na pakety oneskorené v dôsledku opätovného prenosu. Príklad použitia môžu byť streamovacie služby. Podrobnejšie informácie o UDP) protokole nájde čitateľ v [**udp**].

### 1.2.3 IKEv2 Internet Key Exchange version 2

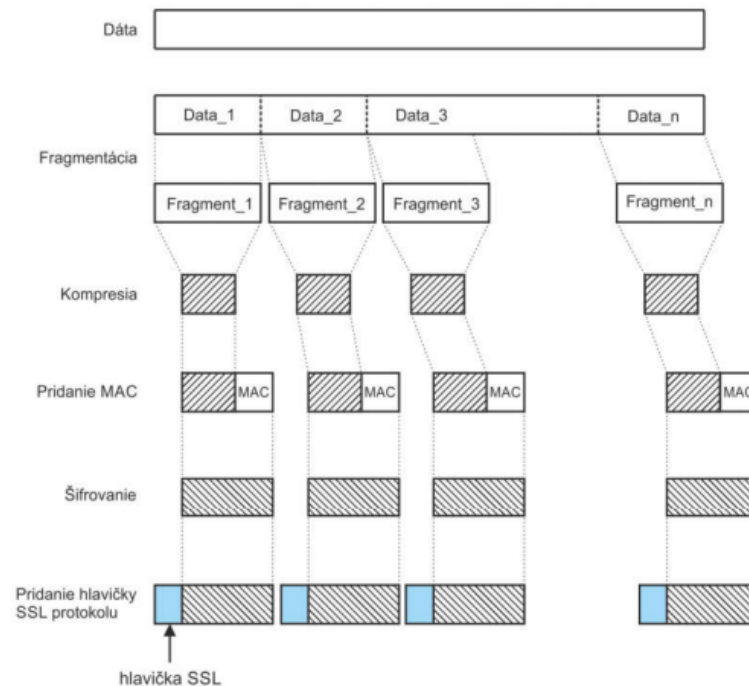
[https://en.wikipedia.org/wiki/Internet\\_Key\\_Exchange](https://en.wikipedia.org/wiki/Internet_Key_Exchange)

### 1.2.4 Transport Layer Security – TLS

TCP protokol sam o sebe nezabezpečí dáta, ku ktorým sa pridáva TCP hlavička. Dôsledkom toho vznikli viacere protokoly slúžiace na autentizované šifrovanie dát. Najznámejší je protokol zabezpečenia prenosu – TLS a IPSec.

Zabezpečenie dát bolo prvotne vykonávané pomocou protokolu *Secure Sockets Layer* – SSL. Tento spôsob používa certifikáty na odšifrovanie dát. SSL malo od svojho vytvorenia dlhý vývoj, ktorý smeroval až k doteraz najpoužívanejšiemu TLS vo verzii 1.3. Inými slovami, TLS protokol je nástupca SSL pričom obsahuje rôzne úpravy a vylepšenia najmä z hľadiska rýchlosti. Zároveň sa v dnešnej dobe neodporúča používanie SSL protokolu. Dôsledkom optimalizácií je, že klienta komunikujúci so serverom cez HTTPS protokol s TLS 1.3 je rýchlejší ako v prípade použitia nešifrovaného HTTP variantu.

TLS pracuje niekde na pomedzi aplikačnej a transportnej vrstvy. Spôsob spracovania dát je zobrazený pomocou schémy 1.7 s SSL operáciami, prebratej z [6].



Obr. 1.7: Prehľad operácií v SSL protokole

Viac informácií o TLS protokole, jednotlivých verziách a optimalizáciách je možné nájsť na [7].

### 1.2.5 Point-to-Point Protocol (PPP)

[https://en.wikipedia.org/wiki/Point-to-Point\\_Protocol](https://en.wikipedia.org/wiki/Point-to-Point_Protocol)

### 1.2.6 Multiprotocol Label Switching (MPLS)

MPLS by sme do slovenčiny mohli preložiť ako Multi-protokolové prepínanie štítkov. Samotný protokol pridáva k paketom tzv. MPLS hlavičku. Jej obsahom sú štítky<sup>6</sup>, na základe ktorých dochádza k smerovaniu a preposielaniu paketov. Týmto spôsobom nie je nutná ďalšia analýza paketov. Štítky neidentifikujú koncové body, ale virtuálne spojenia medzi viacerými uzlami. Označenie multi-protokolový má, pretože dokáže zapuzdrovať viacero sieťových protokolov. MPLS pracuje na pomedzi L2 a L3 vrstvy. Často sa zvykne označovať ako L2.5 protokol. Viac o tomto protokole je možné si prečítať na [8], [9] a [10].

<sup>6</sup>z ang. *labels*

## 1.3 Klasifikácia VPN sietí

V súčasnosti má čitateľ k dispozícii veľa rôznych internetových zdrojov o problematike VPN. Uvedené sú rôzne možnosti klasifikácie VPN siete. V rámci tejto práce klasifikujeme VPN siete podľa logickej topológie, použitých protokolov a vrstiev, na ktorých sú postupy aplikované. Obsahom tejto podkapitoly je rozdelenie a opis jednotlivých typov VPN sietí. V závere kapitoly čitateľ nájde sumárne rozdelenie VPN sietí v tejto práci, znázornené pomocou schémy.

### 1.3.1 Rozdelenie VPN sietí podľa logickej topológie

Podľa topológie, v ktorej VPN spojenie prebieha rozdeľujeme VPN do 3 kategórií:

- **VPN rovný s rovným** – z ang. *Peer to Peer VPN*,
- **VPN klient a server** – z ang. *Client to Server VPN*,
- **VPN sieť so sieťou** – z ang. *Site to Site VPN*.

#### VPN rovný s rovným

Uvedený spôsob vytvára zabezpečený tunel medzi dvoma rovnocennými uzlami, resp. zariadeniami<sup>7</sup>, ktorý spoločne komunikujú cez verejnú sieť. Medzi zariadeniami je vytvorený tunel. Každý koniec má priradenú svoju IP adresu. Z uvedeného modelu vyplýva aj následná limitácia. VPN tunel vznikne iba medzi dvoma komunikujúcimi zariadeniami. Z toho dôvodu nie je toto použitie časté. Na obrázku 1.8 je znázornený uvedený typ VPN spojenia.



Figure 1: Peer to Peer VPN

Obr. 1.8

<sup>7</sup>z ang. *peers*

## VPN Klient a Server

Tento typ spojenia pozostáva z pripojenia medzi nerovnocennými dvoma alebo viacerými zariadeniami. Najjednoduchší model musí pozostávať z jedného VPN servera a VPN klienta. Princíp spočíva vo vytvorení zabezpečeného tunela, ktorý je použitý na prenos dát medzi uvedenými zariadeniami. Zároveň je však možné vytvoriť  $1 : N$  takýchto spojení.  $N$  reprezentuje počet VPN klientov, resp. prepojení, ktorý VPN Server dokáže nadviazať. Tento parameter je závislý najmä od hardvérových prostriedkov daného servera.

Úloha Klienta spočíva v presmerovaní všetkej svojej sieťovej komunikácie cez zabezpečený tunel, ktorý vznikol medzi ním a Serverom. Tento úkon je najčastejšie realizovaný presmerovaním trafiky cez sieťovú bránu<sup>8</sup> (ďalej GW). V danom OS, na ktorom VPN klient beží, je teda potrebné zmeniť IP adresu GW na adresu VPN servera. Vďaka tomu nastane presmerovania komunikácie. Tento úkon je väčšinou realizovaný programovo pomocou aplikácií. Typicky nastolia spojenie medzi Klientom a Serverom. Následne upravujú sieťové nastavenia systému. Spomenuté úkony sú vysoko závislé od OS a daného programovacieho jazyka, prostredníctvom ktorého sú úpravy realizované. Úloha Servera na druhej strane spočíva vo vytvorení možnosti pripojenia pre jedného alebo viacerých klientov. Následne Server zastupuje klientovu prítomnosť v danej sieti. Teda spracúva požiadavky Klienta a komunikuje s ostatnými zariadeniami. Komunikácia ďalej však už nie je zabezpečená pomocou šifrovania alebo tunelu. Tento fakt je znázornený na obrázku 1.9.

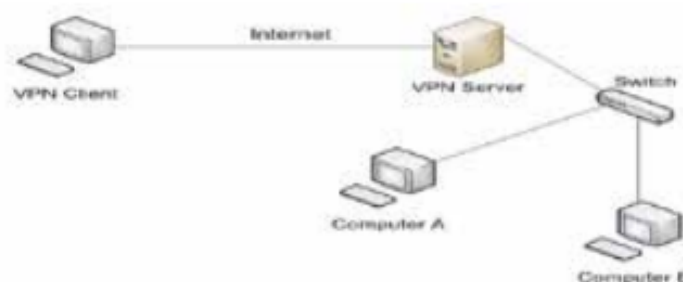


Figure 2: Client to server VPN

Obr. 1.9: potrebné prerobenie nech sa to nepodoba na 1.1 alebo vyhodit/upraviť 1.1

V súčasnosti je tento spôsob považovaný za najviac používaný v oblasti korporátneho sveta. VPN server slúži ako vstupná brána do internej siete. Vďaka tomu

<sup>8</sup>z ang. *GateWay*

je možné sprístupniť zdroje pre používateľov z rôznych oblastí sveta. Používateľ sa taktiež môže stretnúť s pomenovaním model **uzol k sieti**, resp. z ang *point-to-site*. Obidva pojmy sú správne a predstavujú rovnakú myšlienku zapojenia VPN.

### Sieť so Sieťou VPN

VPN model Sieť so Sieťou vytvára zabezpečený tunel medzi dvoma rôznymi sieťami naprieč verejnou sieťou. Model pozostáva z 2 zariadení – VPN servera a VPN Koncentrátora<sup>9</sup>.

VPN Koncentrátor je typ sieťového zariadenia, ktoré poskytuje zabezpečené VPN spojenie a doručenie dát. Zvyčajne je to špecializovaný smerovač<sup>10</sup>. Dokáže vytvárať veľké množstvo VPN tunelov. Používa sa na nastolenie VPN modelu sieť so sieťou. Funkcionalita koncentrátora pozostáva z:

- nastolenie a konfiguráciu VPN tunela – z ang. *Establish and Configure tunnels*,
- autentizáciu používateľa – z ang. *Authenticate users*,
- priradenie IP adries používateľov k tunelom – z ang. *Assign tunnel/IP addresses to users*,
- šifrovanie a dešifrovanie dát – z ang. *Encrypt and Decrypt data*,
- zabezpečiť integritu doručenia – z ang. *Ensure end-to-end delivery of data*.

Model Sieť so sieťou je používaný najmä pri spojení vedľajšej pobočky s hlavnou, ktoré sa nachádzajú na rozdielnych geografických lokalitách. Pomocou schémy 1.10 je znázornený tento model.

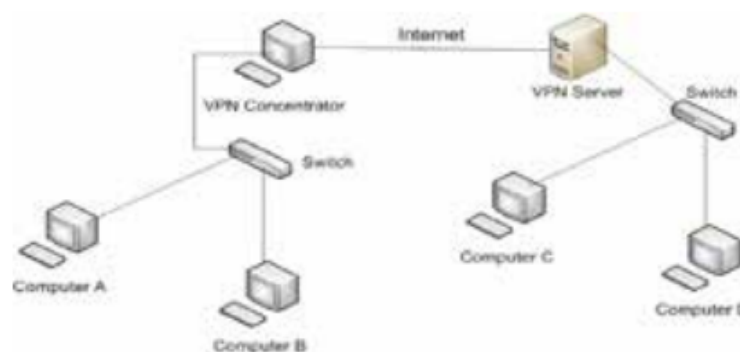


Figure 3: site to site VPN

Obr. 1.10: rearanzovat

Informácia z tejto podkapitoly boli čerpané z [12].

<sup>9</sup>z ang. *VPN Concentrator*

<sup>10</sup>z ang. *router*

### 1.3.2 Rozdelenie VPN sietí podľa vrstiev referenčného modelu

VPN siete môžeme klasifikovať podľa vrstvy (ďalej L) referenčného modelu, na ktorej dochádza k šifrovaniu dát. Stručná charakteristika referenčných modelov je obsahom podkapitoly 1.2.2.

Klasifikácia VPN sietí podľa OSI modelu:

- **L2 VPN** – VPN na spojovej vrstve,
- **L3 VPN** – VPN na sieťovej vrstve,
- **L4 VPN** – VPN na transportnej vrstve.

Pri implementácii VPN komunikácie medzi zariadeniami je pre pochopenie dôležité určiť aké dáta vstupujú do šifrovacieho algoritmu. Pomocou tejto informácie a klasifikácie vyššie následne dokážeme zaradiť do určitej kategórie. Na schéme 1.11 je možné si všimnúť aké dáta sú výstupom jednotlivých vrstiev. (spoj dva obrázky do jedného netreba zbytočne dva)

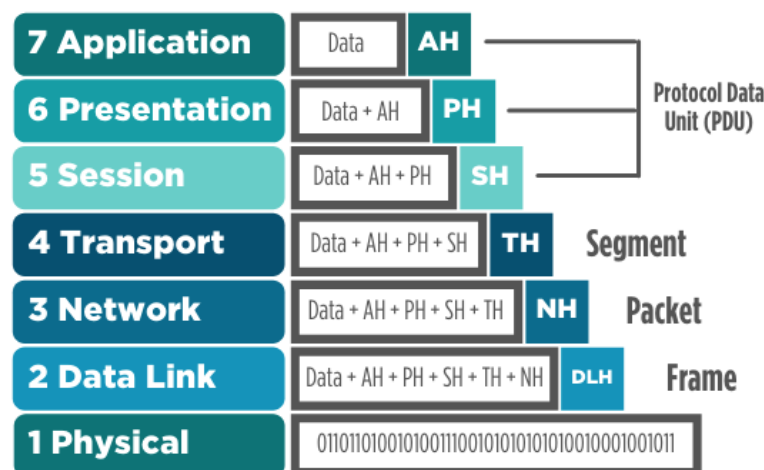
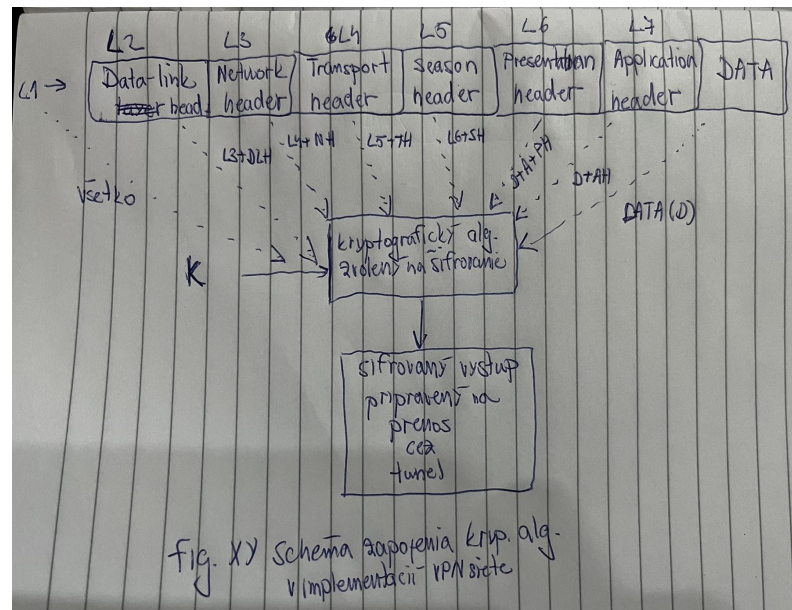


Figure 3: How the OSI/RM is used to model the creation of network packets

Obr. 1.11: zakomponovať k osi vysvetleniu

Princíp použitia bloku na šifrovanie je znázornený pomocou schémy 1.12.

Zo schémy je viditeľné, že spracovaním nižšej vrstvy dochádza k zväčšeniu bloku dát, ktoré je potrebné šifrovať. To môže negatívne ovplyvniť výslednú rýchlosť celého systému. Okrem uvedenej vlastnosti je ďalším problémom prenos vrámci rôznych sietí. Každé zariadenie, ktoré smeruje dáta by muselo repetitívne šifrovať a dešifrovať čím by v danej implementácii vzniklo viac rizikových miest pre potenciálny útok. Z uvedených dôvodov je preto najrozšírenejší spôsob zapojenia



Obr. 1.12: potreba upravy iba na spoemnute vrstvy

šifrovacieho bloku na pomedzi L3 až L4 vrstvy. Smerovanie ostáva bez zásahu a k dešifrovaniu dochádza až na konečnom zariadení, prípadne v aplikácii na samotných dátach.

Typický sa s L2 a L3 VPN sieťami môže používateľ stretnúť na špecializovaných sieťových zariadeniach. Konkrétne na routroch a switchoch. Prvé z uvedených je využívané najmä pri smerovaní, respektíve určení cesty smerom von z lokálnej siete až k cieľovej destinácii. Tento úkon je vykonaný za pomoci aplikácie smerovacích protokolov. Router je možné použiť aj na smerovanie v rámci lokálnej siete. V porovnaní so switchom však nedosahuje porovnateľný výkon. Na druhej strane klasický switch je možné použiť len v rámci lokálnej siete. V súčasnosti sa používajú aj tzv. L3 switchy. V porovnaní s routrom je ich prednosťou vyššia rýchlosť spracovania prichádzajúcich paketov pri väčšom počte pripojených zariadení.

## 1.4 Protokoly vo VPN sieťach

V predchádzajúcej podkapitole sme klasifikovali VPN siete na základe zapojenia kryptografického bloku do OSI referenčného modelu. V tejto podkapitole pomocou uvedeného rozdelenia, zaradíme a charakterizujeme zopár protokolov, ktoré sa typicky používajú vo VPN sieťach. Pred začiatkom by som rád čitateľa upozornil, že aktuálne neexistuje svetový štandard na vytváranie VPN spojení. Dôsledkom toho existuje veľké množstvo rôznych protokolov. V rámci tejto pod-

kapitoly si predstavíme niektoré z nich.

### 1.4.1 Point-to-Point Tunneling Protocol (PPTP)

?nerozumiem?PPTP enables on-demand, virtual private networks over the Internet or other public TCP/IP-based data networks ??

TCP/IP sieťový protokol PPTP poskytuje zabezpečuje bezpečný prenos dát z klienta do privátneho servera vo VPN sieti. Jedná sa o starší Microsoft L2 protokol, ktorý bol definovaný v roku 1996. Je rozšírením L2 PPP protokolu. PPTP zapuzdruje PPP pakety do IP datagramov. Následne ich prenáša cez sieť. Typicky pozostáva spojenie z 3 zariadení, ktoré sú znázornené na schéme 1.13 a 1.14.

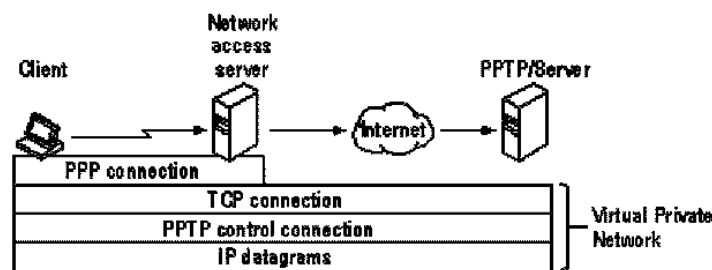
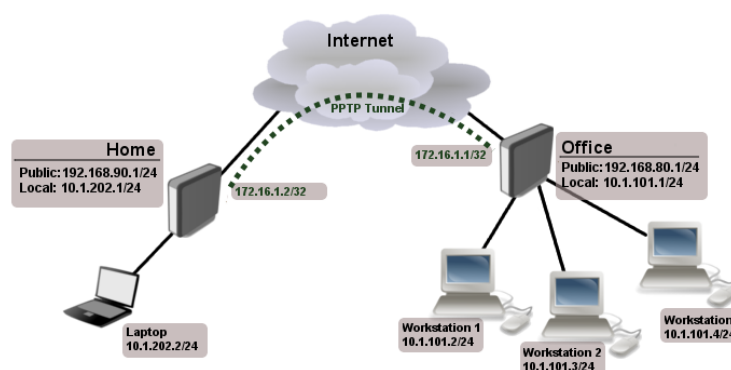


Figure 1. The PPTP tunnel

Obr. 1.13: Architektura PPTP siete - PPTP je az od nas do PS



Obr. 1.14: lepsi obrazok

Zabezpečenie prenosu pomocou PPTP pozostáva typicky z 3 po sebe nasledujúcich procesov:

1. PPP pripojenie a komunikácia – z ang. *PPP Connection and Communication*,



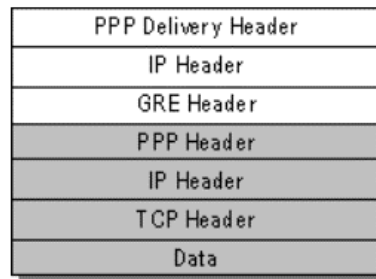


Figure 7. IP datagram containing encrypted PPP packet as created by PPTP

Obr. 1.15: sede sifrovane biele nie

2. riadenie spojenia pomocou PPTP protokolu – z ang. *PPTP Control Connection*,
3. prenos dát PPTP tunelom – z ang. *PPTP Data Tunneling*.

Prechod medzi procesmi je možný len ak došlo k úspešnému dokončeniu predchádzajúceho kroku. V prvom procese sa PPTP klient pripája k serveru s prístupom na internet<sup>11</sup> (ďalej NAS). Používa sa pri tom PPP protokol, ktorý nastolí spojenie a zašifruje pakety. V druhom kroku následne vznikne TCP pripojenie medzi NAT a PPTP serverom. Použitý je port 1723. Uvedeným postupom nám vznikne medzi zariadeniami PPTP Tunel. Po úspešnom vytvorení konektivity dochádza k zapuzdrovaniu prichádzajúcich zašifrovaných PPP dát do PPTP protokolu a ich prenosu cez tunel. PPTP zapuzdruje dáta do tzv. IP datagramov, ktoré už obsahujú zašifrovaný PPP paket. Datagramy su vytvorené pomocou GRE protokolu, ktorý bol opísaný v ?? Na schéme 1.15 je znázornená schém PPTP Paketu.

PPTP Server po prijatí dáta rozbalí, dešifruje PPP paket a následne ho smeruje v rámci lokálnej siete.

Je dôležité poznamenať, že PPTP klient môže mať priamy prístup na internet. V uvedenom prípade sa nevytvára prvotné PPP spojenie až k internetovému poskytovateľovi. Viac informácií o protokole PPTP nájde čitateľ na [13] a [14], ktoré boli zdrojom pri tvorbe tejto podkapitoly.

## Bezpečnosť a použitie protokolu

Protokol vznikol v júny 1996. Implementácia poskytuje používateľovi:

- **Autentizáciu** – z ang. *Authentication*, overenie totožnosti používateľa pomocou mena a hesla. Na výber boli autentizačné protokoly *Challenge Handshake*

<sup>11</sup>z ang. *Network Access Server*

*Authentication Protocol* (CHAP) [15], *MicroSoft Challenge Handshake Authentication Protocol* (MS-CHAP) [16] a *Password Authentication Protocol* (PAP) [17].

- **Kontrolu prístupu** – z ang. *Access Control*, po úspešnej autentizácii je následne prístup používateľa riadený na základe pravidiel a politiky prístupu daného OS.
- **Šifrovanie dát** – z ang. *Data Encryption*, je vykonané pomocou vopred zdieľaného kľúča, ktorý sa získa odvodením z hašovanej hodnoty uloženého hesla používateľa. Haš je vstupom do prúdovej šifry RC4 [18] a výstupom je 40-bitový kľúč relácie.
- **Filtrovanie PPTP paketov** – z ang. *PPTP Packet Filtering*, možnosť zapnutia filtrovania paketov len autentizovaných PPTP klientov.
- **Preddefinované Firewall pravidla pre PPTP** – z ang. *PPTP with Firewalls and Routers*, PPTP má štandardne definovaný TCP port 1723 a ID 47 v IP protokole. Vďaka tomu je možné jednoducho presmerovať tok dát.

Protokol je aktuálne štandardne zahrnutý v každej distribúcii OS Windows aj Linux. Pri vytváraní VPN siete teda používateľ môže zvoliť uvedený protokol na zabezpečený prenos dát v lokálnej, ale aj naprieč verejnou sieťou. Výhodou protokolu je vysoká kompatibilita naprieč rôznymi platformami. Nevýhodou je veľké množstvo zraniteľných miest, možností zneužitia a použitie starších kryptografických algoritmov. Aktuálne existujú protokoly poskytujúce lepšiu bezpečnosť ako uvedená implementácia. Z uvedených dôvodov sa tento protokol neodporúča používať.

### 1.4.2 Layer 2 Tunneling Protocol (L2TP)

Ďalším z VPN tunelovacích protokolov je L2TP. Špecifikovaný bol v roku 2000 v dokumente RFC<sup>12</sup> 2661 [19]. Inšpirovaný dvoma staršími protokolmi L2F<sup>13</sup> [20] a PPTP.

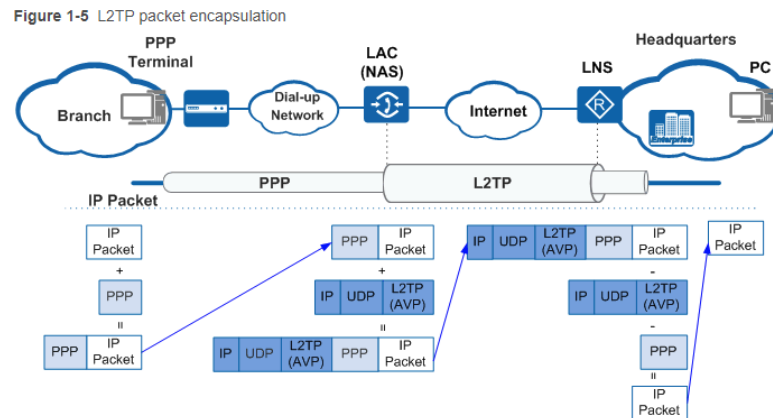
L2TP sieť pozostáva primárne z 3 zariadení:

1. **PPP terminál** – ľubovoľné zariadenie na vykonanie PPP enkapsulácie na dáta a pripojenie k LAC<sup>14</sup>. Môže to byť aj samotné zariadenie, ktoré sa pripája.

<sup>12</sup>z ang. *Request For Comments*

<sup>13</sup>z ang. *Cisco Layer 2 Forwarding Protocol*

<sup>14</sup>z ang. *L2TP access concentrator*



Obr. 1.16

2. **L2TP prístupového servera** – LNS<sup>15</sup>, jeden z koncov tunela, ktorý deenkapsuluje dáta a poskytuje prístup do lokálnej siete. Na zariadení prebieha autentizácia používateľa, nastolenie PPP relácie<sup>16</sup> a L2TP tunela s LAC. Nasadzuje sa na hranici medzi privátnou a verejnou sieťou, zvyčajne ako sieťová brána na opustenie danej súkromnej siete<sup>17</sup>. Obdobne poskytuje funkcionality prekladu adres z privátnych do verejných a opačne. Uvedená funkcionality sa nazývajú Network Address Translation (NAT). Viac o tomto protokole je dostupné na [21].
3. **L2TP koncentrátora** – LAC, zariadenie umiestnené medzi LNS a klientom. Služí na preposielanie paketov oboma smermi. V smere k LNS vytvára L2TP tunel. LAC server môže byť nasadený aj na PPP termináli a pracovať ako PPPoE<sup>18</sup> server. Zvyčajne je koncentrátor nasadený na NAS, ale je možné ho nasadiť na ľubovoľné sieťové zariadenie.

V schéme 1.16 je znázornené ako sú spomenuté zariadenia zapojené v logickej topológii. Na schéme je znázornený aj proces enkapsulácie PPP paketov, prenosu dát naprieč tunelom a následnej deenkapsulácie.

L2TP používa namiesto TCP protokolu UDP, ktorého výhodou je rýchlejší prenos bez kontroly prijatia na druhej strane spojenia. Pri vzniku tunela používa UDP port 1701. Iniciátor tohto procesu následne vyberá náhodne z nečinných portov a smeruje ním pakety s portom 1701. Prijímač po prijatí paketu taktiež náhodne určí nečinný port a preposiela ním pakety prijaté iniciátorom. Takto zvolené portové čísla sa používajú až kým nie je komunikácia cez tunel ukončená.

<sup>15</sup> z ang. *L2TP Network Server*

<sup>16</sup> z ang. *session*

<sup>17</sup> z ang. *gateway*

<sup>18</sup> z ang. *PPP Over Ethernet*

L2TP vytvára 2 druhy spojenia počas vytvárania konektivity medzi LAC a LNS.

- **tunelové spojenie** – z ang. *tunnel connection*, napomáha k nastoleniu viacerých tunelov medzi zariadeniami. Pozostáva z jedného alebo viacerých relačných spojení. Žiadosť o vytvorenie vytvára LAC server po prijatí PPP žiadosť od vzdialeného používateľa. LAC a LNS si vymenia informácie potrebné na vznik spojenia ako sú napríklad autentizačné informácie tunela a ID. Po úspešnom vyjednávaní<sup>19</sup> vznikne tunel, ktorý je identifikovateľný pomocou dohodnutého ID.
- **relačné spojenie** – z ang. *session connection*, reprezentuje PPP spojenie naprieč tunelom. Môže vzniknúť až keď je tunel úspešne vytvorený.

Po vytvorení oboch spojení následne odchádza k prenosu zapuzdrených PPP paketov naprieč týmto tunelom.

L2TP ponúka kompatibilitu pre mnohé platformy a jednoduchú konfiguráciu. OS Windows, Linux a Mac majú tento protokol zabudovaný v sebe. Výhodou je použitie UDP, vďaka tomu je možné protokol používať aj v nestabilnom sieťovom prostredí. Nevýhodou je zníženie prenosovej rýchlosti. L2TP používa tiež vopred zdieľané kľúče a v prípade ak sa nezhodujú, tak dochádza k zastaveniu chodu. L2TP podporuje iba limitovaný počet portových čísel. Samotná implementácia L2TP neposkytuje, respektíve nezabezpečuje žiadne šifrovanie alebo autentizáciu paketa. Na zabezpečenie sa používa v kombinácii s iným protokolom. Veľmi známa je implementácia L2TP/IPSec.

V roku 2005 vznikla 3. verzia protokolu, ktorá priniesla zväčšenie dĺžky ID v L2TP hlavičke, zo 16 na 32 bitov. Rozšírenie tunelového autentizačného mechanizmu a oddelenie L2TP dát súvisiacich s PPP protokolom. Viac o tomto upravenom protokole je možné nájsť na [22].

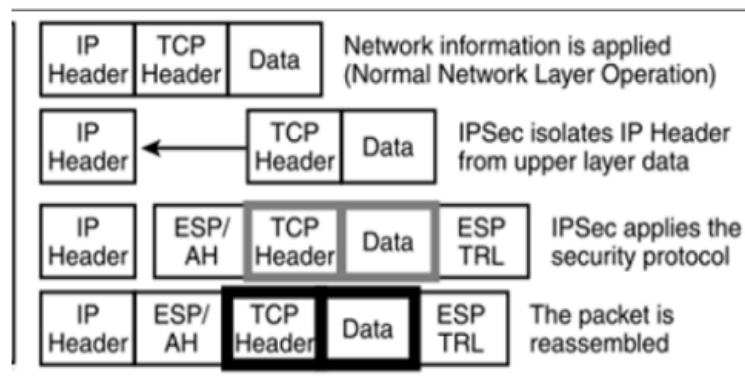
Viac informácií o L2TP problematike je možné nájsť v [23], [19], [24], odkiaľ boli informácie z tejto podkapitole čerpané.

### 1.4.3 Internet Protocol Security (IPSec)

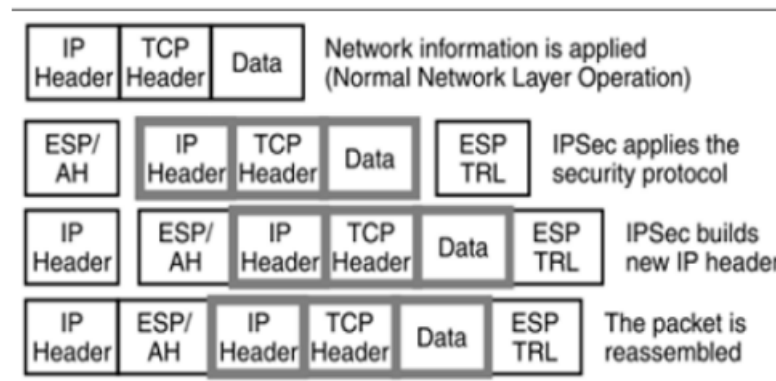
IPSec je otvorený štandard. Vďaka tomu vďačí za veľkú popularitu a pravidelné aktualizácie kryptografických algoritmov. Protokol sa využíva na zabezpečenie bezpečnosti v sieti. IPSec môžeme klasifikujeme ako L3 protokol nakoľko pracuje s dátami zo sieťovej vrstvy. Má dva režimy:

<sup>19</sup>z ang. *negotiation*

- **transportný režim** – po prijatí paketu z vyššej vrstvy sú smerovacie dáta zachované a na základe nich sú dáta odosielané ďalej. K zvyšným dátam je pridaná hlavička použitého IPSec protokolu. Princíp pridania dát k paketu je znázornený na 1.17
- **tunelovací režim** – zapuzdruje paket z vyššej vrstvy. Pridáva novú IP hlavičku a hlavičku IPSec protokolu k pôvodnému nezapuzdrenému paketu. Uvedená skutočnosť je zobrazená na obrázku 1.18



Obr. 1.17: IPSec transportný režim



Obr. 1.18: IPSec tunelovací režim

Za účelom poskytnutia zabezpečeného spojenia, protokol vykonáva autentizáciu, šifrovanie a vyjednávanie, resp. výmenu potrebných kľúčov. Jednotlivé činnosti sú realizované pomocou týchto IPSec protokolov:

- **Autentizačná hlavička** – z ang. *Authentication Header*, pridáva k prepravovanému paketu dáta na zabezpečenie dátovej integrity a pôvodu. Chráni proti z ang. *Replay attack* [25]. Dáta v tomto režime nie sú šifrované. AH

hlavička je vygenerovaná v závislosti od toho v akom IPSec režime je protokol použitý.

- **Bezpečnostné zapuzdrenie nákladu** – z ang. *Encapsulating Security Payloads*, narozdiel od AH, ESP aj šifruje dáta z vyššej vrstvy. Vďaka tomu dochádza k zabezpečeniu dôvernosti, datovej integrity a autentizácie pôvodu. Výsledná hlavička závisí od dát zo sieťovej vrstvy a konfigurácie IPSec.
- **Internet Security Association and Key Management Protocol** – ďalej ISAKMP, protokol na autentizáciu a výmenu kľúčov. Slúži taktiež na vytvorenie parametra SA, ktorý sa používa v hlavičke AH/ESP.

IPSec je možné nakonfigurovať, tak aby používal AH a ESP selektívne alebo aj súčasne. V závislosti od konfigurácie následne dochádza k zapuzdrovaniu prichádzajúceho paketu. Používateľ má na výber viacero štandardných kryptografických algoritmov. Príkladmi sú AES [26], RSA [27], Diffie-Hellman [28] a eliptické krivky (ECDSA [29] aj ECDH [30]).

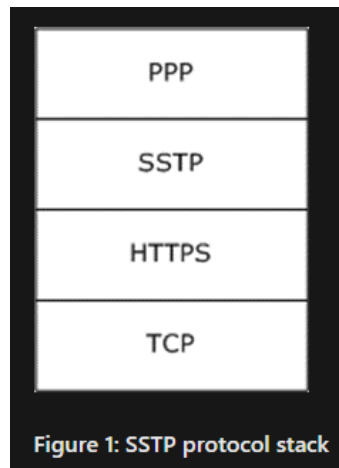
Nabudúce sa opýtať či biki predmet môže byť zdroj alebo nie. [6]

#### 1.4.4 Secure Socket Tunneling Protocol (SSTP)

SSTP je bežný L2 VPN protokol, ktorý zapuzdruje PPP rámce cez HTTPS protokol [31]. Spolieha sa na SSL, resp. TLS, ktoré sú opísané v úvode práce. Vďaka tomu umožňuje ľahší prechod cez väčšinu firewallov a proxy brán. Teda blokovanie takto vytvoreného VPN spojenia je pre poskytovateľov internetu a správcov siete zložitejšie.

SSTP bol vytvorený v roku 2007 spoločnosťou Microsoft. Primárne pre platformu Windows. Cieľom bolo poskytnúť bezpečnejšiu náhradu za PPTP a L2TP. V súčasnosti sa považuje za jeden zo štandardných protokolov. Je dostupný vo viacerých operačných systémoch vrátane Linuxu a BSD. Pravidelne udržiavaný o čom svedčia aj priebežná aktualizácia dokumentácie na Microsoft dokumentačných stránkach. Informácie k tejto podkapitole boli čerpané z [32]. V uvedenom zdroji je možné nájsť podrobnejšie informácie o protokole.

Proces enkapsulácie s využitím protokolov je znázornený pomocou schémy 1.19. Pri vytváraní SSTP segmentu dochádza k zapuzdreniu PPP rámcov pomocou HTTPS s využitím TCP protokolu s portovým číslom 443. Po úspešnom nadviazaní TCP a overení SSL/TLS spojenia dochádza k spracovaniu SSTP hlavičky. Po úspešnom odstránení sa následne získa prístup k pôvodnému PPP rámcu.



Obr. 1.19: Proces enkapsulácie PPP rámcov pomocou protokolov naprieč SSTP protokolom

Podobne ako tomu bolo v prípade L2TP protokolu, opísaného vyššie, tak z hľadiska premávky putujú naprieč tunelom dva druhy paketov. Vytvára a odosiela ich klient aj server. Majú špecifický formát a musia byť prenášané po bajtoch a v sieťovom poradí bajtov<sup>20</sup>, z ľava do prava, teda od najvýznamnejšieho bitu po najmenej významný<sup>21</sup>. Prvé 4 parametre v oboch hlavičkách sú rovnaké:

1. **Verzia** – z ang. *Version*, má veľkosť 8-bitov, používa sa pri komunikácii a vyjednávanií SSTP verzie, ktorá sa má použiť. Prvé 4 bity signalizujú majoritnú verziu a zvyšné minoritnú verziu.
2. **Rezervované** – z ang. *Reserved*, 7 bitov nastavených na 0, rezervované pre budúce použitie, pri spracovaní sa ignorujú.
3. **C** – 1 bit, indikátor pre dátový (0) a kontrolný SSTP paket (1).
4. **Dĺžka paketu** – z ang. *LengthPacket*, 16-bitový parameter, pozostáva z:
  - **R** – 4 bity, pripravené na budúce použitie, nastavené na 0 a ignorované,
  - **Dĺžka** – z ang. *Length*, 12 bitov, špecifikuje bajtovú veľkosť celého SSTP paketu

Rozdielnosť medzi hlavičkami vzniká v:

- **Dátové SSTP pakety** – z ang. *SSTP Data Packets* [33], obsahujú 5. parameter
  - **5. Dáta** – pole variabilnej dĺžky. Obsahuje zapuzdrený náklad z vyššej vrstvy.

<sup>20</sup>z ang. *network byte order*

<sup>21</sup>sieťové spracovanie dát známe aj ako z ang. *Big Endian*

- **Kontrolné SSTP pakety** – z ang. *SSTP Control Packets* [34], obsahuje 3 datočné parametre:
  - **5. Typ správy** – z ang. *Message Type*, 16-bitové pole s SSTP správou o stave spojenia. Celkovo 9 možných správ [34].
  - **6. Číselné atribúty** – z ang. *Num Attributes*, 16-bitové pole, ktoré špecifikuje počet parametrov v správe
  - **7. Atribúty** – z ang. *Attributes*, zoznam parametrov s variabilnou veľkosťou.

Protokol vo všeobecnosti nepodporuje spojenie typu sieť k sieti. Primárne je orientovaný na pripojenie klienta k sieti, za účelom získania vzdialeného prístupu. To isté platí pri autentizácii. Je možné autentizovať iba používateľa, iné možnosti nie sú podporované (zariadenie, smart card, počítač,...). V prípade nestabilného spojenia, je možný vysoký výskyt straty paketov. Dôvodom je použitie TCP protokolu.

Bezpečnosť SSTP je sprostredkovaná za pomoci HTTPS protokolu, ktorý používa SSL/TLS. Aplikované kryptografické algoritmy závisia od verzie SSL/TLS, ktorá je použitá v implementácii. TLS bol predmetom opisu v úvode práce. SSTP sa považuje za veľmi bezpečný protokol. Na druhej strane použitie robustných šifrovacích a autentizačných algoritmov, dosť spomaľuje výsledné SSTP VPN pripojenie.

Viac informácií o protokole môže čitateľ nájsť v [32], odkiaľ boli aj informácie pre túto podkapitolu čerpané.

### 1.4.5 Ostatné populárne VPN protokoly

Vrámcí tejto práce si predstavíme ešte dvojicu veľmi populárnych VPN riešení. Koncepcne sú riešenia pri vytváraní tunelu a prenose správ podobné vyššie opísaným protokolom. Z uvedeného dôvodu protokoly len stručne charakterizujeme.

#### OpenVPN

OpenVPN je jeden z najznámejších voľne dostupných VPN tunelovacích protokolov. Vznikol v roku 2001. Dostupné ako firmvérové riešenie pre výrobcov sieťových zariadení. Pre používateľa je dostupná vo forme softvéru, ktorý je potrebné nainštalovať na cieľovú platformu. Ponúka aj grafické rozhranie. Zabezpečené spojenie naprieč internetom je sprostredkované prostredníctvom SSL/TLS



protokolu. Dokáže pracovať s dátami na L2 aj L3 vrstve v závislosti od konfigurácie. Vďaka voľnému prístupu do zdrojového kódu poskytuje jednoduché možnosti na skúmanie výsledných riešení, validáciu a prípadnú úpravu podľa potrieb konkrétného používateľa. Protokol je napísaný v jazyku C. Bezpečnostné prvky su implementované pomocou OpenSSL knižnice. Knižnica v sebe zahŕňa funkcie potrebné na šifrovanie, autentizáciu, výmenu kľúčov a mnoho ďalšieho. Na obrázku 1.20 je znázornená výstupná štruktúra paketu po zapuzdrení.

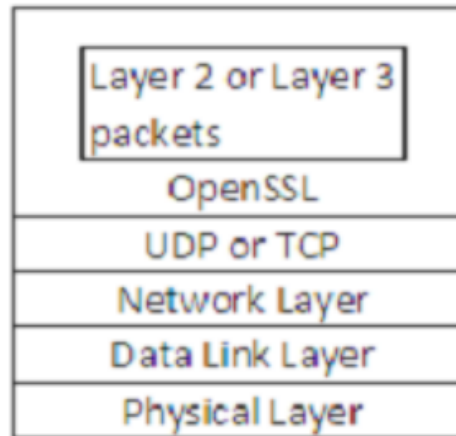


Figure 5 : Packet Structure of OpenVPN

Obr. 1.20

Aktuálne používa na šifrovanie AES s 256-bitovou veľkosťou kľúča. V súčasnosti sa OpenVPN považuje za najbezpečnejšiu implementáciu VPN dostupnú pre viacero platforiem. Používateľ má možnosti vo voľbe protokolu TCP alebo UDP. Podporuje aj prácu s IPv6. OpenVPN nie je kompatibilná s ostatnými protokolmi. Je preto potrebné mať implementáciu na serveri aj klientovi. Nevýhodou je pomerne veľké, energeticky a výpočtovo náročné prevedenie.

Viac informácií o tomto komplexnom programe je možné nájsť v [12], [35] a priamo na stránke OpenVPN<sup>22</sup>. Z uvedených zdrojov boli aj informácie čerpané. Zdrojový kód je dostupný napríklad na Githube<sup>23</sup>.

## WireGuard

WireGuard je najnovší protokol z vyššie uvedených. Pracuje iba na L3 vrstve. Jedná sa o implementáciu s voľne dostupným zdrojovým kódom. Vznikol v roku 2015. Cieľom projektu bolo vytvoriť jednoduchý protokol, ktorý sa ľahko používa,

<sup>22</sup><https://openvpn.net/faq/what-is-openvpn/>

<sup>23</sup><https://github.com/OpenVPN/openvpn/>

dosahuje vysoké prenosové rýchlosti a poskytuje kvalitnú bezpečnosť pre používateľa. Vo výsledku sa to vývojárom podarilo. Od roku 2020 sa stal súčasťou Linuxového jadra, konkrétne verzie Linux 5.6 kernel. Aktuálne podporuje veľké množstvo OS vrátane Androidu, Windowsu, MacOS, OS založené na BSD [36] a ďalšie. Za úspešne prevedenie vďaka WireGuard implementovaniu svojich funkcionalít do samotných jadier OS, čo značne zrýchľuje spracovanie dát. Samozrejmosťou ostáva aj využitie moderných, extrémne rýchlych kryptografických algoritmov a podpora pre IPv4 a IPv6.

Protokoly použité vo WireGuarde sú:

- **X25519** [37] – zabezpečuje výmenu kľúčov vďaka kryptografii s eliptickým krivkami [38] (ďalej ECC), ponúka 128-bitovú bezpečnosť s veľkosťou kľúča 256-bitov. Považuje sa za jednu z najrýchlejších kriviek v ECC.
- **ChaCha20** [39] – zabezpečuje symetrické šifrovanie.
- **Poly1305** [40] – vytvára autentifikačný kód správy<sup>24</sup>. Veľmi častá je kombinácia ChaCha20-Poly1305 za účelom autentizovaného šifrovania s pridruženými dátami<sup>25</sup>.
- **SipHash** [41] – algoritmus sa používa na vytvorenie a mapovanie kľúčov k hodnotám v hashovacej tabuľke. Hashovacie tabuľky sú známy pojem v oblasti dátových štruktúr. Ich hlavnou výhodou je vysoká rýchlosť v porovnaní s ostatnými možnosťami.
- **BLAKE2s** [42] – hashovacia funkcia, rýchlejšia než aktuálne štandardy z rodiny SHA.
- **UDP** – protokol na prepravu zapuzdrených dát.

WireGuard podporuje aj použitie vopred zdieľaného kľúča za účelom symetrického šifrovania. Dôvodom je pokrok v oblasti kvantových počítačov, ktoré predstavujú riziko pre algoritmy založené na asymetrickom šifrovaní.

Viac informácií o tomto protokole je k dispozícii na [43] a [44], odkiaľ boli informácie aj čerpané. Zdrojový kód je rozdelený do viacerých repozitárov. Zoznam je dostupný na stránkach Wireguardu<sup>26</sup>.

<sup>24</sup>z ang. [Message Authentication codes]

<sup>25</sup>z ang. *Authenticated encryption with associated data*

<sup>26</sup><https://www.wireguard.com/repositories/>

## 1.5 Zhrnutie VPN sieti

Jednoduchá schema so všetkým v jednom obraze

[45], [46] <https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/> <https://www.top10vpn.com/what-is-a-vpn/vpn-types/> <https://www.auvik.com/types/> <https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/?ref=rp> <https://www.geeksforgeeks.org/difference-between-site-to-site-vpn-and-remote-access-vpn/?ref=rp>

V súčasnosti je trend, využívanie VPN na súkromné účely. Dôvodov môže byť viacero. Napríklad prístup k lokálne blokoványm doménam, anonymita v internetovom prostredí, zabezpečenie pripojenia a iné. V tomto prípade vstupujú do popredia tzv. VPN poskytovatelia (z ang. *VPN Providers*). Ktorý za poplatok poskytujú výhody pripojenia cez VPN k verejnej sieti. – stojí za zmienku <https://github.com/vpnhood/VpnHood> a plus v iných jazykoch

## 2 Ľahká kryptografia

---

V počítačovej sfére sa do popredia dostávajú zariadenia, ktorých hardvérové prostriedky a ponúkaný výkon sú podstatne nižšie ako v prípade bežne dostupných zariadení na domáce, resp. komerčné použitie. Príkladom môžu byť IOT zariadenia, senzorové uzly, mikro-ovládače a podobné. Dôležitou vlastnosťou je aj komunikácia medzi sebou alebo inými zariadeniami. V dôsledku toho je nutné riešiť aj otázku zabezpečenia, resp. bezpečnosti takého prenosu dát.

Kryptografia je oblasť počítačovej vedy, ktorá sa zaoberá práve spomenutou problematikou. Hlavným cieľom je utajiť správu pri jej ceste z bodu A do B. Teda od odosielateľa (tvorcu) správy, až k jej prijímateľovi. Dôsledkom tohto úkonu dochádza k zabezpečeniu 3 hlavných úloh kryptografie:

- **ochrana osobných údajov** (dôvernosť) – z ang. *Data Privacy*,
- **autenticita údajov** (prišla z miesta, kde sa uvádza) – z ang. *Data Authenticity*,
- **integrita údajov** (nebolia upravená počas prenosu) – z ang. *Data Integrity*.

Pojem kryptografia vznikol už pomerne dávno a bol už viackrát charakterizovaný. Z toho dôvodu sa tejto problematike ďalej nebudeme venovať. Ak by však bol čitateľ v tejto oblasti nový, odporúčame najprv načerpať viac informácií. Kvalitné spracovanie problematiky je možné nájsť v [47].

V súčasnosti má používateľ možnosť vybrať si zo širokej ponuky kryptografických algoritmov. Výber je volený na základe potrebnej funkcionality, ktorú sa snažíme implementovať. Napríklad za účelom symetrického šifrovania by sme mohli použiť AES [26], ktorý je aktuálne používaný ako štandardný kryptografický algoritmus. Detailný opis jednotlivých blokov a postupov použitých v AES-e, je obsahom rôznych vydání. Viac informácií o problematike nájde čitateľ v [47].

V prípade zariadení spomenutých v úvode kapitoly, však môže nastať problém s výpočtovým výkonom pri realizácii algoritmov. Vo výsledku trvá vykonávanie funkcionality omnoho dlhšie ako v prípade normálnych zariadení. V roku

2005 bol prvýkrát definovaný pojem, z ang. *Lightweight Cryptography*. Konkrétne v práci [48]. V rámci tejto práce voľne preložíme tento pojem ako **Ľahká kryptografia** (ďalej LWC).

LWC algoritmy sú mnoho násobne efektívnejšie ako súčasne používané konvenčné kryptografické štandardy. Dôvodom je ich vysoká rýchlosť a nízky počet potrebných procesorových inštrukcií na vykonanie cielenej funkcionality. V súčasnosti je častým javom použitie označenia *lightweight* pre ľubovoľný kryptografický algoritmus. Jedná sa o implementácie, ktoré svojimi vlastnosťami splňajú základné požiadavky LWC. Tie boli definované samotnými autormi už v diele [48]. Sú nimi:

- **minimalizácia spotreby zdrojov zariadenia** – veľkosť kódu, používaných dát a spotreby energie,
- **poskytnutie vysokého stupňa bezpečnosti,**
- **odolnosť voči útoku cez postranné kanály** – z ang. *side-channel attack*, napríklad útokom na analýzu výkonu a na časovanie,
- **jednoduchá implementácia a efektívnosť,**
- **nízka pamäťová stopa** – z ang. *low memory footprint*.

V práci budeme tieto algoritmy označovať ako *Lightweight Cryptographic Algorithm* (ďalej LWCA). LWCA tvoria kryptografické algoritmy, ktoré splňajú vyššie stanovené vlastnosti a teda je možné ich aj nasadiť do tzv. *low resource* zariadení. V závislosti od výslednej implementácie sa sledujú požiadavky na daný algoritmus. V prípade hardvérovej implementácie najväčšiu rolu pri tvorbe optimálneho algoritmu zohráva energetická spotreba a potrebná veľkosť čipu (chip size iba v zdroji – In hardware implementations, chip size and/or energy consumption are the important measures to evaluate the lightweight properties.). Na druhej strane, pri softvérovej implementácii je dôležitým aspektom veľkosť algoritmu a/alebo jeho využitie RAM pamäte. Čím sú uvedené parametre nižšie, tým výhodnejší je nasadenie daného algoritmu pre cieľové zariadenie. V prípade slabých zariadení sa pri výslednej implementácii LWCA môžeme stretnúť aj s kompromisom medzi ponúknutou bezpečnosťou a efektívnosťou.

V rámci tejto kapitoly si predstavíme jeden z novších LWCA algoritmov. Konkrétne balíček Xoodoo s kryptografickou permutáciou XOODOO [49] a jeho použitie. Xoodoo sa stal jedným z 10 finalistov v LWC štandardizačnom procese Národného inštitútu pre štandardy a technológie (ďalej NIST) [50]. Aktuálne ešte stále prebieha výber štandardu.

Viac podrobností nájde čitateľ v [48], [51] a [50], odkiaľ boli aj informácie z tejto kapitoly čerpané.

## 2.1 Kryptografická permutácia XOODOO a jej variácie

Permutácia je operácia, ktorá mení pozíciu vstupných prvkov, tak aby vo výsledku vzniklo nová usporiadaná množina. Kryptografické permutácie sú špeciálne navrhnuté matematické algoritmy, tak aby bolo možné využiť ich za účelom šifrovania a dešifrovania. Operácie vykonané v takýchto permutáciách musia byť invertibilné. Kryptografické permutácie tvoria základný stavebný blok pri následnej tvorbe ďalších kryptografických blokov. Množina základných stavebných blokov sa v kryptografii spoločne označuje ako kryptografické primitíva (ďalej KP). Príkladom môžu byť hašovacie funkcie, generátory náhodných čísel a podobne. Viac informácií nájde čitateľ v [52].

XOODOO je sada 384-bitových kryptografických permutácií parametrizovaných počtom kôl. Funkcia kola/rundy<sup>1</sup> funguje na 12 slovách<sup>2</sup> po 32 bitoch. Vďaka tomu je efektívna aj na menej výkonných procesoroch nižšej triedy. Vytvoril ju tím Keccak, ktorý stojí za viacerými úspešnými kryptografickými algoritmami. Napríklad hashovacie funkcie z rodiny SHA-3 a iné – [53]. XOODOO algoritmus vznikol po vytvorení tzv. Kravatte autentizačno-šifrovacieho algoritmu [54], založené na Keccak-p permutácií [55]. Ten sa ukázal ako dostatočne rýchly na širokom spektre platforiem. Avšak nezapadá do kategórie LWCA.

Tím Keccak vypracoval nové riešenie. Ním bol port medzi ich prvotným Keccak-p dizajnom a Gimli-ho [56] permutačným algoritmom. Vo výsledku autori zlúčili lepšie realizované prvky z oboch algoritmov do jedného celku. Primárny problém samotnej Gimli permutácie bol v slabom prejave zmeny výstupu po malých zmenách vo vstupnej správe. Táto vlastnosť sa v kryptografii označuje pomocou anglického pojmu, tzv. *propagation properties*<sup>3</sup>. Novo-vzniknuté riešenie autori pomenovali XOODOO. Na základe rôznych variácií tohto kryptografického primitíva sa im následne podarilo vytvoriť sadu vysoko efektívnych kryptografických funkcií. Medzi sady, ktorých jadro tvorí XOODOO, patrí Xoodyak a Xoofff. Xoofff pozostáva zo zlúčenia Farfalle konštrukcie [57] so XOODOO permutáciou.

<sup>1</sup>z ang. *round*

<sup>2</sup>z ang. *words*

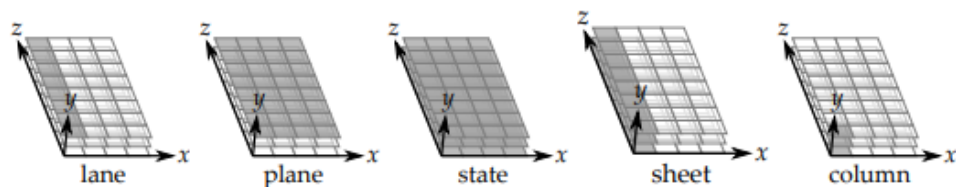
<sup>3</sup>Cieľom je aby aj zmena jedného bitu na vstupe, ovplyvnila čo najviac bitov vo výstupe – tzv. *Lavínový efekt*

Xoodyak ma narozdiel od Xoofff duplexovú konštrukciu [58]. Vo výsledku máme ľahko prenosnú, všestrannú, kryptografickú knižnicu. Je vhodná do výkonovo obmedzených prostredí. Môže sa použiť pre väčšinu kryptografických funkcií, ktoré používajú symetrický kľúč. Napríklad hashovanie, šifrovanie, výpočet MAC alebo autentizované šifrovanie. O kvalite riešenia napovedá aj fakt, že sada Xoodyak je jedným z 10 finalistov v oblasti ľahkej kryptografie NIST štandardizačného procesu. V rámci tejto kapitoly opíšeme kryptografické primitívum XOODOO a následne balík Xoodyak. Informácie o téme boli čerpané z týchto zdrojov: [49], [59], [60], [61], [62], [63].

### 2.1.1 XOODOO permutácia

XOODOO je permutácia, definovaná počtom rúnd. Má klasickú iteračnú štruktúru. Teda opakovane sa vola rundová funkcia s aktuálnym stavom. Pre pochopenie operácií je nutné pochopiť určité označenie použité v algoritme.

Stav – **state**, pozostáva z 3 rovnako veľkých horizontálnych rovín – **planes**<sup>4</sup>. Každá z týchto rovín obsahuje štyri paralelne 32-bitové pruhy – **lanes**<sup>5</sup>. Okrem tejto charakteristiky je možné opísať stav ako množinu zloženú zo stĺpcov – **columns**<sup>6</sup>, pričom jeden stĺpec obsahuje 4 bity v jednej rovine. Stav je teda tvorený zo stĺpcov usporiadaných v poli o rozmere  $4 \times 3 \times 32 = 384$  bitov. Posledná položka na opis stavu sú tzv. listy – **sheets**<sup>7</sup>. List sa skladá z 3 na sebe uložených pruhov. Uvedené pojmy sú znázornené pomocou schémy 2.1, ktorá bola prebraná z [60].



Obr. 2.1: Grafické znázornenie terminológie využitej v kryptografickej permutácii XOODOO [60]

Roviny majú index  $y$ . Index  $y = 0$  zodpovedá spodnej rovine a vrchná rovina má index  $y = 2$ . Bit je označený s indexom  $z$  vrámci množiny pruhov. List označujeme pomocou indexu  $x$ . Pozícia pruhu v stave je definovaná pomocou dvoch súradníc  $(x, y)$ . Konkrétny bit je možné reprezentovať v stave pomocou trojice sú-

<sup>4</sup>V jednej rovine je 128 bitov

<sup>5</sup>V jednom pruhu je 32 bitov

<sup>6</sup>V jednom stĺpci je 12 bitov

<sup>7</sup>V jednom liste je 96 bitov

radníc  $(x, y, z)$ . Pri určení stĺpca sú potrebné 2 súradnice  $(x, z)$ . Pred spustením samotného algoritmu musí používateľ vykonať mapovanie 384-bitovej správy voči horizontálnym rovinám. Tento úkon sa realizuje pomocou vzorca 2.1.

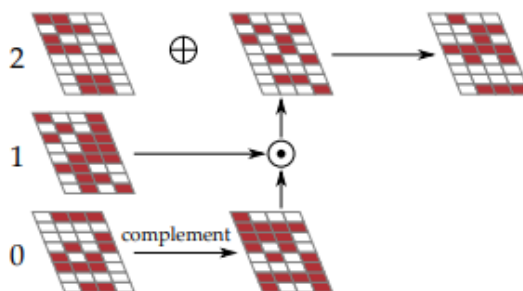
$$i = z + 32(x + 4y) \quad (2.1)$$

Výhodou XOODOO je, že celý stav, 384 bitov, dokáže byť uložený v 12 registroch po 32 bitov. Vďaka tomu ideálne vyhovuje nízko výkonným 32-bitovým zariadeniam.

Rundová funkcia pozostáva z 5 krokov:

1. miešanie vrstvy – z ang. *a mixing layer*  $\theta$ ,
2. posun rovín – z ang. *a plane shifting*  $\rho_{west}$ ,
3. pridanie rundových konštánt – z ang. *the addition of round constants*  $\iota$ ,
4. nelineárna vrstva – z ang. *a non-linear layer*  $\chi$ ,
5. posun rovín – z ang. *an another plane shifting*  $\rho_{east}$ .

Opis jednotlivých krokov je znázornený pomocou schémy 2.2, 2.3, 2.4 ktoré sú prebraté z [60].

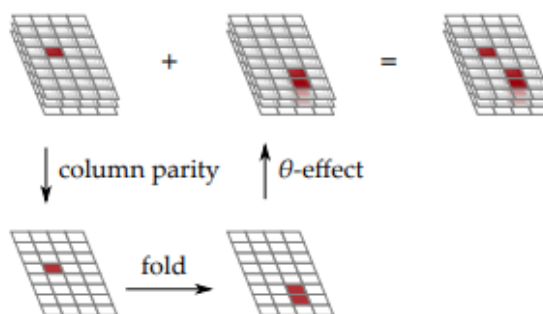
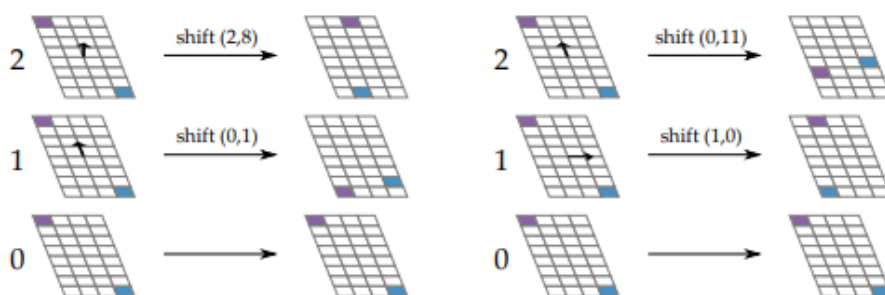


Obr. 2.2: Grafické znázornenie operácie  $\chi$  [60]

K spomenutej schéme 2.4, by sme rád doplnili, že posun je realizovaný na každom bite. Na schéme sú ilustrované len posuny 2 bitov.

Tabuľka 2.5 vysvetľuje jednotlivé operácie, ktoré sa v algoritme používajú. Algoritmus permutácie je následne znázornený pomocou 2.6. Súčasťou implementácie sú aj tak zvané rundové konštanty. Tie je možné vidieť v 2.7. Uvedené ilustrácie boli prebrané z dokumentu [60].



Obr. 2.3: Grafické znázornenie operácie  $\rho$  [60]Obr. 2.4: Ilustrácia miešania vrstiev  $\rho_{west}$  (vľavo) a  $\rho_{east}$  (vpravo) [60]

$A_y$	Plane $y$ of state $A$
$A_y \lll (t, v)$	Cyclic shift of $A_y$ moving bit in $(x, z)$ to position $(x + t, z + v)$
$\overline{A_y}$	Bitwise complement of plane $A_y$
$A_y + A_{y'}$	Bitwise sum (XOR) of planes $A_y$ and $A_{y'}$
$A_y \cdot A_{y'}$	Bitwise product (AND) of planes $A_y$ and $A_{y'}$

Obr. 2.5: Charakteristika operácií v algoritmickej zápise kryptografickej permutácie XOODOO [60]

### 2.1.2 Kryptografický balíček Xoodyak

Xoodyak možno považovať za všestranný kryptografický nástroj. Je vhodný pre väčšinu operácií využívajúcich symetrický kľúč. Napríklad generovanie pseudonáhodných bitov, autentizáciu, šifrovanie a iné. Tím Keccak použil pri návrhu duplexnú konštrukciu. Konkrétne variant s plným stavom a využitím kľúča. Tento dizajn označujeme ako Full-State Keyed Duplex (FSKD). Viac o tejto konštrukcii si čitateľ môže prečítať v [58]. Operačný režim, v ktorom Xoodyak pracuje sa nazýva Cyklista – z ang. *Cyclist*. Tento názov získal ako opozitum k pomenovaniu režimu Motorista, ktorý je možné nájsť v Keyak schéme [64]. Narozdiel od uvedeného balíka Keyak, nie je Xoodyak limitovaný len na autentizované šifrovanie. Je jednoduchší hlavne kvôli tomu že neobsahuje paralelné varianty.

---

**Algorithm 1** Definition of XOODOO $[n_r]$  with  $n_r$  the number of rounds
 

---

**Parameters:** Number of rounds  $n_r$   
**for** Round index  $i$  from  $1 - n_r$  to 0 **do**  
      $A = R_i(A)$

Here  $R_i$  is specified by the following sequence of steps:

$\theta :$   
      $P \leftarrow A_0 + A_1 + A_2$   
      $E \leftarrow P \lll (1, 5) + P \lll (1, 14)$   
      $A_y \leftarrow A_y + E$  for  $y \in \{0, 1, 2\}$   
 $\rho_{\text{west}} :$   
      $A_1 \leftarrow A_1 \lll (1, 0)$   
      $A_2 \leftarrow A_2 \lll (0, 11)$   
 $\iota :$   
      $A_0 \leftarrow A_0 + C_i$   
 $\chi :$   
      $B_0 \leftarrow \overline{A_1} \cdot A_2$   
      $B_1 \leftarrow \overline{A_2} \cdot A_0$   
      $B_2 \leftarrow \overline{A_0} \cdot A_1$   
      $A_y \leftarrow A_y + B_y$  for  $y \in \{0, 1, 2\}$   
 $\rho_{\text{east}} :$   
      $A_1 \leftarrow A_1 \lll (0, 1)$   
      $A_2 \leftarrow A_2 \lll (2, 8)$

---

Obr. 2.6: Algoritmický zápis kryptografickej permutácie XOODOO [60]

$i$	$c_i$	$i$	$c_i$	$i$	$c_i$	$i$	$c_i$
-11	0x00000058	-8	0x000000D0	-5	0x00000060	-2	0x000000F0
-10	0x00000038	-7	0x00000120	-4	0x0000002C	-1	0x000001A0
-9	0x000003C0	-6	0x00000014	-3	0x00000380	0	0x00000012

Obr. 2.7: Súbor rundových konštánt kryptografického algoritmu XOODOO [60]

## Režim Cyklista

Režim Cyklista funguje na princípe kryptografických permutácií  $f$ , teda zmeny usporiadania bitov za pomoci tajného kľúča a matematických operácií. Parametrami sú veľkosti blokov  $R_{\text{hash}}$ ,  $R_{\text{kin}}$ ,  $R_{\text{kout}}$  a veľkosť račety, resp. západky<sup>8</sup> [65]  $\ell_{\text{ratchet}}$ . Uvedený pojem sa v kryptografii používa vo forme obrazného pomenovania. Cieľom je poukázať na jednoduchý pohyb vpred, ale s ťažkým, resp. zložitejším pohybom naspäť. Dôležité je, že uvedený scenár je vyvolaný zámerným dizajnom. Šírka permutácie  $b'$  je definovaná pomocou vzorca 2.2. Všetky uvedené

---

<sup>8</sup>z ang. *the ratchet size*

parametre sú v bajtoch. Pre označenie prázdneho slova budeme používať  $E$ .

$$\max(R_{hash}, R_{kin}, R_{kout}) + 2 \leq b' \quad (2.2)$$

Cyklista operuje v dvoch režimoch – **hašovací a kľúčový**<sup>9</sup>. Inicializácia prebieha pomocou príkazu `CYCLIST(K, id, counter)`. Ak sa parameter  $K$  rovná prázd-  
nemu slovu  $E$ , tak potom nastane spustenie v hašovacom režime. Aktuálne nie je  
do implementácie zakomponovaná možnosť zmeny režimu po inicializácii. Vý-  
vojári však túto vlastnosť nevylúčili pre prípadné aktualizácie balíka.

Dostupné funkcie závisia od režimu, v ktorom sa Cyklista spúšťa. Medzi ne  
patria `ABSORB()` a `SQUEEZE()`. Možno ich volať v oboch režimoch, zatiaľ čo funkcie  
`ENCRYPT()`, `DECRYPT()`, `SQUEEZEKEY()` a `RATCHET()` sú dostupné len pre kľúčový  
režim. Účel každej funkcie je nasledujúci:

- `ABSORB(X)` absorbuje vstupný reťazec  $X$ ,
- $C \leftarrow \text{ENCRYPT}(P)$  zašifruje  $P$  do  $C$  a absorbuje  $P$ ,
- $P \leftarrow \text{DECRYPT}(C)$  dešifruje  $C$  do  $P$  a absorbuje  $P$ ,
- $Y \leftarrow \text{SQUEEZE}(L)$  vytvára  $L$ -bajtový výstup, ktorý závisí od doteraz absor-  
bovaných dát,
- $Y \leftarrow \text{SQUEEZEKEY}(L)$  funguje ako `SQUEEZE(L)`, ale používa sa za účelom ge-  
nerovania odvodeného kľúča,
- `RATCHET()` transformuje stav na nevratný tak, aby sa zabezpečila dopredná  
bezpečnosť<sup>10</sup> [66].

Stav bude závisieť od postupnosti volaní funkcií a od jeho vstupných reťaz-  
cov. Presnejšie povedané, zámerom je, že akýkoľvek výstup závisí od postup-  
nosti všetkých vstupných reťazcov a volaní, tak že akékoľvek dva nasledujúce  
výstupné reťazce budú výstupom rôznych domén. Napríklad volanie `ABSORB(X)`  
znamená, že výstup bude závisieť od reťazca  $X$ . Na druhej strane `ABSORB()` vo  
funkcii `ENCRYPT(P)` vytvorí výstup závislý aj od  $P$  z funkcie šifrovania. Okrem  
uvedených závislostí ovplyvňujú výstup aj iné dizajnové riešenia. Príkladom je  
minimalizácia pamätevej stopy. Vo výsledku teda výstup závisí od počtu pred-  
chádzajúcich volaní funkcie `SQUEEZE()` a predtým spracovaných textov pomocou  
funkcií `ENCRYPT()` a `DECRYPT()`. Viac informácií o režime je dostupných v kapi-  
tole 7.2, publikácie [60]. Algoritmický zápis jednotlivých funkcií a doplňujúce  
informácie o režime Cyklista je možné nájsť v [67], konkrétne v kapitole 2.2.

<sup>9</sup>z ang. *hash and keyed mode*.

<sup>10</sup>z ang. *Forward secrecy*

## Definícia a bezpečnosť

Xoodyak je definovaný pomocou operatívneho režimu Cyklista nasledovne:

$$CYCLIST[f, R_{hash}, R_{kin}, R_{kout}, L_{ratchet}] \quad (2.3)$$

Kde jednotlivé parametre majú veľkosti:

1.  $f$  – permutácia XOODOO so šírkou 48 bajtov (384 bitov),
2.  $R_{hash}$  – 16 bajtov,
3.  $R_{kin}$  – 44 bajtov,
4.  $R_{kout}$  – 24 bajtov,
5.  $L_{ratchet}$  – 16 bajtov.

Takto definované parametre algoritmu dokážu poskytnúť 128-bitovú bezpečnosť v oboch režimoch Cyklistu. Samozrejmosťou je, že v prípade kľúčového režimu, musí byť veľkosť kľúča rovná alebo väčšia ako 128 bitov. Viac informácií o kryptografickej bezpečnosti algoritmov je možné nájsť v [68].

Viac informácií o bezpečnosti Xoodyak-a je možné nájsť v [7.3, 60] a [67], odkiaľ boli informácie čerpané.

### 2.1.3 Možnosti použitia Xoodyak algoritmu

Obsahom tejto podkapitoly sú uvedené postupy ako a za akých okolností je daný balík možné použiť.

#### Použitie hašovacieho režimu

Xoodyak sa dá aplikovať ako hašovacia funkcia. Konkrétne je možné ju použiť ako funkciu na rozšírenie výstupu<sup>11</sup> (ďalej XOF). Nominálne, resp. nie bežné použitie by v tomto prípade bolo nasledujúce:

```

CYCLIST(E, E, E) //spustenie v hašovacom režime,
ABSORB(X)       //absorpcia vstupného reťazca X,
SQUEEZE(L)      //vytvára L-bajtový výstup,
                //závislý od doteraz absorbovaných dát.

```

V tomto prípade by sa kryptografická bezpečnosť algoritmu pohybovala v závislosti od veľkosti výstupu L. Konkrétne v intervaloch:

<sup>11</sup>z ang. *eXtendable-Output Function*

- **odolnosť voči kolíziám** – z ang. *collision resistance* [69],  $\min(8L/2, 128)$  bitov,
- **odolnosť voči** – z ang. *preimage and second preimage resistance* [70],  $\min(8L, 128)$  bitov,
- **odolnosť voči** – z ang. *m-target preimage resistance* [70],  $\min(8L - \log m, 128)$  bitov.

Bežná je však absorpcia sekvencie viacerých reťazcov.

### Použitie kľúčového režimu

Inicializácia režimu začína použitím príkazu `CYCLIST(K, id, counter)`. Autori uviedli celkovo 6 spôsobov použitia. V nich sa opisuje význam parametrov *id*, *counter* *nounce* a podobne aj možnosti použitia funkcií, spomenutých na začiatku podkapitole.

- **Použitie na zabránenie viac-cieľového útoku** – z ang. *Two ways to counteract multi-target attacks*,
- **Tri spôsoby spracovania jednorázového kľúča** – z ang. *Three ways to handle the nonce*,
- **Autentizované šifrovanie** – z ang. *Authenticated encryption*,
- **Autentizované relačné šifrovanie** – z ang. *Session authenticated encryption*,
- **Použitie funkcie RATCHET()** – z ang. *Ratchet*,
- **Pohyblivé subkľúče** – z ang. *Rolling subkeys*,

**Použitie na zabránenie viac-cieľového útoku** – *id* parameter je voliteľný identifikátor kľúča *K*. Pre každý tajný kľúč by mal byť jedinečný. Ponúka možnosť zabránenia viac-cieľovým útokom. Jedná sa o útok na viacero používateľov daného kryptografického systému, resp. viacero kľúčov používateľa. Viac o tomto útoku je možné nájsť v [71]. V prípade použitia *id* parametra algoritmus rozšíri veľkosť kľúča. Následne pri vyhľadávaní kľúčov nedochádza k degradácii bezpečnosti a veľkosť tajného kľúča môže ostať 128 bitov. Týmto spôsobom bude zachovaná aj rovnaká bezpečnosť systému pred útokom. Príklad za účelom šifrovania správy *P* za pomoci tajného kľúča *K* s *id*, je na nasledujúci:

```

CYCLIST(K, id, E)
ABSORB(nonce)
C ← ENCRYPT(P).

```

**Tri spôsoby spracovania jednorázového kľúča** – 3. parameter pri inicializácii režimu cyklista je *counter*, resp. počítadlo. Jedná sa o dátový prvok vo forme bajtového reťazca, ktorý môže byť inkrementovaný. Spracúva sa po jednej číslici. Vďaka tomu sa obmedzuje počet informácií, ktoré vie útočník využiť pre rôzne vstupy. Pri inicializácii používateľ zvolí veľkosť počítadla v intervale  $2 \leq B \leq 256$ . Predpokladá sa, že počítadlo je reťazec z množiny  $\mathbb{Z}_B^*$ . Potom ak je počítadlo inicializované ako prázdny reťazec, tak množina všetkých možných hodnôt po inkrementácii je  $\mathbb{Z}_B^*$ . Pri každom ďalšom navýšení sa zvýši hodnota za \*. Spracovanie prebieha od najvýznamnejšieho bitu. Čím menšia je hodnota  $B$ , tým menší je počet možných vstupov pri každej iterácii permutácie. Vďaka tomu je zabezpečená lepšia ochrana pred tzv. z ang *Power analysis* [72] útokmi a jeho variantami. Za účelom zamedzenia týchto útokov sa používa `ABSORB(nonce)` v prípade ak si počítadlo pri inicializácii zvolíme prázdny reťazec  $E$ .

**Autentizované šifrovanie** – za účelom autentizovaného šifrovania je Xoodyak možné použiť nasledovne:

```

CYCLIST( $K$ , nonce,  $E$ )
ABSORB( $A$ )
 $C \leftarrow \text{ENCRYPT}(P)$ 
 $T \leftarrow \text{SQUEEZE}(t)$ 
return ( $C, T$ )

```

Pričom  $K$  je tajný kľúč s pridruženým jednorázovým heslo a dátami  $A$  k heslu. Z týchto údajov sa získa autentizačný tag  $t$ . Jeho veľkosť je rovná 16-bajtom. V prípade dešifrovania by postupnosť volaní vyzerala nasledovne:

```

CYCLIST( $K$ , nonce,  $E$ )
ABSORB( $A$ )
 $C \leftarrow \text{ENCRYPT}(P)$ 
 $T \leftarrow \text{SQUEEZE}(t)$ 
if  $T = T'$  then
    return  $P$ ,
else
    return  $\perp$  //vyjadrenia hodnoty false

```

Kryptografická bezpečnosť takto implementovaného šifrovania je minimom z uvedených hodnôt  $\min(184, K, 8t)$ .

**Autentizované relačné šifrovanie** – pracuje so sekvenciou správ a autentizačných tagov. V princípe sa opakuje viacero blokov z predchádzajúcej možnosti použitia. Prvé volanie je rovnaké ako v predchádzajúcom príklade. Implemen-

tácia však zahŕňa aj možnosť vytvoriť tag bez toho aby bolo nutné použiť funkcie `ABSORB()`, `ENCRYPT()` alebo obe súčasne pred volaním `SQUEEZE()`. Aj napriek tomu bude možné vytvoriť nový tag na základe predchádzajúcich dát, uložených v pamäti.

**Použitie funkcie `RATCHET()`** – používateľ môže v režime kľúča kedykoľvek volať funkciu `RATCHET()`. Volanie spôsobí prepísanie časti stavu s nulami. Vďaka tomu je nemožné vypočítať stav pred volaním funkcie `RATCHET()`. Týmto spôsobom je možné zťažiť snahu pri pokuse obnoviť vnútorný stav, napríklad pri útoku postrannými kanálmi. `RATCHET()` je možné použiť obdobne aj pri autentizovanom šifrovaní. Konkrétne pred alebo za funkciou vytvárania tagu `SQUEEZE()`.

```

CYCLIST(K, nonce, E)
ABSORB(A)
C ← ENCRYPT(P)
RATCHET() //príklad volania pred
T ← SQUEEZE(t)
RATCHET() //príklad volania za

```

Obidva spôsoby majú svoje výhody. Volanie pred vytváraním tagu je najefektívnejšie. Dôvodom je, že vďaka tomu je potrebné len jedno extra volanie permutácie. V prípade volania funkcie `RATCHET()` za `SQUEEZE()` sa šifrovaný text prenáša, funkcionality `RATCHET()` je vykonaná asynchrónne a algoritmus môže spracovať ďalšiu správu, určenú na šifrovanie.

**Pohyblivé subkľúče** – je alternatíva k použitiu dlhodobého tajného kľúča *K* s inkrementovanými pridruženým jednorázovým kľúčom *nonce* alebo identifikátorom kľúča *id*. Subkľúč/e sa vytvára/jú pomocou funkcie `SQUEEZEKEY()`. Pri šifrovaní je teda možné nahradiť procesy inkrementácie a ukladania jednorázových hesiel pri každom použití *K*, pomocou použitia pohyblivých subkľúčov.

```

 $K_1 \leftarrow K$  and  $i \leftarrow 1$  //inicializacia tajneho kluca
while condition do
  CYCLIST( $K, E, E$ ) //inicializacia novej Xoodyak inštancie
   $K_{i+1} \leftarrow \text{SQUEEZEKEY}(\ell_{sub})$ 
  RATCHET() //volitelne
  ABSORB( $A_i$ )
   $C_i \leftarrow \text{ENCRYPT}(P_i)$  //sifrovanie
   $T_i \leftarrow \text{SQUEEZE}(t)$  //vypocet tagu
   $\Rightarrow$  output( $C_i, T_i$ ) //caka na dalsiu spravu
   $i \leftarrow i + 1$ 

```

Parameter  $\ell_{sub}$  je vo veľkosti 32 bajtov (256 bitov). Táto veľkosť by mala byť dostatočná aby sa zabránilo kolíziám za predpokladu, že v subkľúčoch nevznikla kolízia. Použitie týmto spôsobom ponúka odolnosť voči útokom cez postranné kanály. Tajný kľúč nie je po dodávke prvého subľúča používaný. Vďaka tomu nie je ani vystavený možnému útoku. Každým ďalším šifrovaním sa mení aj použitý kľúč na šifrovanie, čo veľmi sťažuje možnosti ďalšej analýzy.

### Použitie za účelom autentizovaného šifrovania s bežným heslom

Protokoly na výmenu kľúčov, ako napríklad Diffie-Hellman, poskytujú vo výsledku bežný tajný kľúč. Pred symetrickým šifrovaním je však potrebná jeho úprava. Za týmto účelom je možné použiť Cyklistu v hašovacom režime. Následne po spracovaní bežného kľúča použijeme odvodený kľúč na spustenie režimu kľúča. Funkcionalita je jednotlivých volaní je znázornená nižšie.

```

CYCLIST( $E, E, E$ ) //hasovací režim
ABSORB( $ID$ ) //ID použiteho protokolu
ABSORB( $K_A$ ) //verejny kluc A
ABSORB( $K_B$ ) //verejny kluc B
ABSORB( $K_{AB}$ ) //tajny kluc
 $K_D \leftarrow \text{SQUEEZE}(\ell)$ 

CYCLIST( $K_D, nonce, E$ ) //režim kluca
ABSORB( $A$ )
 $C \leftarrow \text{ENCRYPT}(P)$ 
 $T \leftarrow \text{SQUEEZE}(t)$ 
return ( $C, T$ )

```

Ak platí  $\ell \leq R_{hash}$ , tak implementácia dokáže efektívne zreťaziť tajný kľúč  $K_D$



a reinicializovať cyklistu  $CYCLIST(\$K\_D$, \$E$, \$E$)$ . Dôvodom je, že tajný kľúč je už súčasťou stavu permutácie. Je len potrebné nastaviť zvyšné parametre. Note also that if at least one of the public key pairs is ephemeral, the common secret K<sub>AB</sub> is used only once and no nonce is needed. ??[3.3, 67]

## 3 Konfigurácia prostredia, metodika testovania a merania

---

### 3.1 Prostredie virtuálnych strojov pomocou Virtual-Box

Pri testovaní funkcionality VPN sme použili virtualizačný nástroj (ďalej VM) Virtual Box (ďalej VB), spoločnosti Oracle, vo verzii 6.1.38. VB je voľne dostupný. Inštalácia je jednoduchá a rýchla. Viac informácií o nástroji je možné dohľadať v [73].

Pre použitie je potrebné aby mal používateľ k dispozícii obraz operačného systému (ďalej OS). Tie nie je problém získať ani pre OS Windows a podobne, avšak pri našej práci sme zvolili využitie voľno dostupného OS – **Linux Ubuntu** vo verziách 22.04.3(LTS<sup>1</sup>)– OSC a následne vytvorili klon – OSS. Pri opise práce použijeme označenia OSS pre VPN server a OSC pre klienta.

Pri jednoduchej inštalácii VM sme použili konfiguráciu s 2048 MB RAM a 2 jadrami. (Minimálna inštalácia). V prípade potreby dávame do popredia návod na prípravu Windows OS v VM – [74], avšak postup je triviálny. Po inštalácii sme OS aktualizovali pomocou príkazov:

```
sudo apt-get update  
sudo apt-get upgrade
```

Následne sme doinštalovali potrebné súčasti k VM OS vo verzii ako je VB, teda 6.1.30. Dôvodom bolo zväčšenie rozlíšenia a využívanie možnosti zdieľaného priečinka s OS, na ktorom daný VB beží. Za účelom správneho fungovania priečinka bolo nutné v termináli použiť príkaz:

```
sudo usermod -aG vboxsf $(whoami)
```

a následne reštartovať OS.

---

<sup>1</sup>z ang. Long Term Support

Posledné úpravy prostredia sú spojené s jazykom C a balíčkom Make. Inštalácia je opäť jednoduchá. Použili sme príkazy:

```
sudo apt install gcc
sudo apt install make
```

Uvedené úpravy boli vykonané na oboch OS.

V prípade použitia OS Windows je postup inštalácie jazyka C a balička Make zložitejší. Používateľovi odporúčam použitie knižníc Winlibs<sup>2</sup>. Po stiahnutí balíčkov musí používateľ importovať uvedený balíček, resp. cestu k nemu, do premenných prostredia OS Windows. Jeden zo spôsobov je uvedený aj na Winlibs stránke.

### 3.1.1 Zmena sieťových adaptérov

VB ponúka rôzne možnosti nastavenia sieťových adaptérov. Aktuálne su dostupné tieto:

- Not attached
- Network Address Translation (ďalej NAT)
- NAT Network
- Bridge adapter
- Internal
- Host-Only
- Generic driver
- Cloud-Based – experimentálne

Konektivita jednotlivých možností je znázornená pomocou obrázku 3.1. Viac informácií o jednotlivých režimoch je dostupných na [75].

Vzhľadom k našim potrebám, teda obojsmerná komunikácia medzi 2 VM, sú pre nás relevantné režimy bridge a NAT network. Ako si môžeme všimnúť, NAT vyžaduje dodatočnú konfiguráciu portov v prípadoch kedy chceme aby nastala komunikácia medzi dvoma VM. Z tohto dôvodu je pre čo najjednoduchší prístup zvoliť práve režim bridge. Ten priradí VM vlastnú IP adresu, pomocou, ktorej stroj komunikuje.

Viac o jednotlivých režimoch je taktiež možné nájsť v [76]. Autor sa venuje postupu konfigurácie jednotlivých režimov spoločne s ich opisom.

---

<sup>2</sup>dostupne na <https://winlibs.com/>

Mode	VM→Host	VM←Host	VM1↔VM2	VM→Net/LAN	VM←Net/LAN
Host-only	+	+	+	–	–
Internal	–	–	+	–	–
Bridged	+	+	+	+	+
NAT	+	<a href="#">Port forward</a>	–	+	<a href="#">Port forward</a>
NATservice	+	<a href="#">Port forward</a>	+	+	<a href="#">Port forward</a>

Obr. 3.1: Konektivita jednotlivých sieťových adaptérov

## 3.2 Nástroje použité v obrazoch a v práci

Winlibs balík

Visual studio Code

GCC prekladač a balík Make

Tunelovacie rozhranie Wintun

Zdrojový kód na meranie počtu cyklov a času

Umelá inteligencia založená na GPT3/4

## 4 Implementacia jednoduchaj VPN siete

---

Za účelom demonštrácie jednoduchaj VPN siete sme zvolili voľne dostupnú implementáciu v jazyku C. V tejto kapitole postupne rozoberieme funkcionality a správanie vzniknutej VPN siete.

### 4.1 Dead Simple VPN

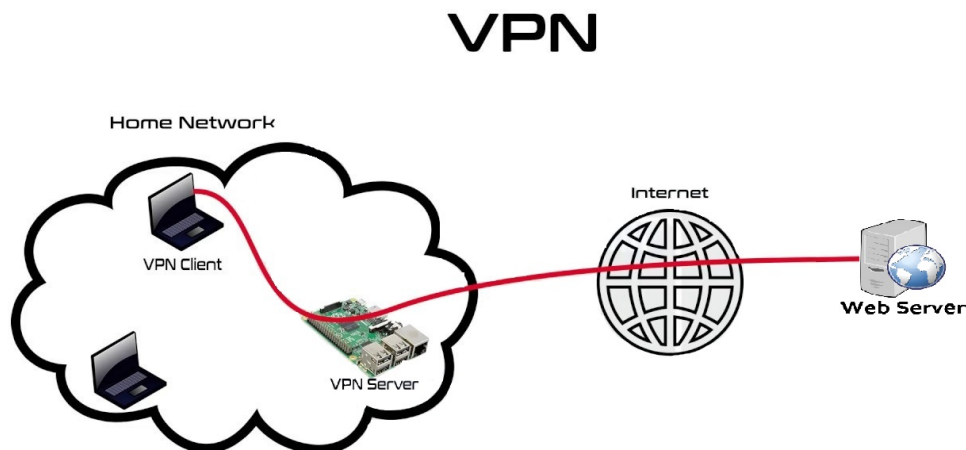
Dead Simple VPN je voľne dostupný<sup>1</sup> program, napísaný v jazyku C. Určený je pre operačný systém Linux. Autorom je Frank Denis. DSVPN rieši najbežnejší prípad použitia VPN, teda pripojenie klienta k VPN serveru cez nezabezpečenú sieť. Následne sa klient dostane na internet prostredníctvom servera. Uvedenú skutočnosť je možné vidieť na schéme 4.1.

DSVPN používa protokol riadenia prenosu – TCP [77]. Medzi ďalšie pozitíva patrí:

- Používa iba modernú kryptografiu s formálne overenými implementáciami.
- Malá a konštantná pamäťová stopa. Nevykonáva žiadne dynamické alokovanie pamäte (z ang. *heap memory*).
- Malý (25 KB) a čitateľný kód. Žiadne vonkajšie závislosti (z ang. *Dependencies*).
- Funguje po preklade GCC prekladačom. Bez dlhej dokumentácie, žiadene konfiguračného súboru, dodatočnej konfigurácie. DSVPN je spustiteľná jednoriadkovým príkazom na serveri, obdobne na klientovi. Bez potreby konfigurácie brány firewall a pravidiel smerovania.
- Funguje na Linuxe (kernel  $\geq 3.17$ ), macOS a OpenBSD, DragonFly BSD, FreeBSD a NetBSD v klientských a point-to-point režimoch. Pridanie podpory pre iné operačné systémy je triviálne.

---

<sup>1</sup><https://github.com/jedisct1/dsvpn>



Obr. 4.1: Schéma jednoduchkej VPN

- Nedochádza k úniku IP medzi pripojeniami, ak sa sieť nezmení. Blokuje IPv6 na klientovi, aby sa zabránilo úniku IPv6 adresy.

V uvedenej VPN autor zakomponoval aj možnosť pokročilejších nastavení. Celkový súhrn vstupných parametrov pri štarte programu je takýto:

```
./dsvpn server
<key file>
<vpn server ip or name>|"auto"
<vpn server port>|"auto"
<tun interface>|"auto"
<local tunnel ip>|"auto"
<remote tunnel ip>"auto"
<external ip>|"auto"
```

```
./dsvpn client
<key file>
<vpn server ip or name>
<vpn server port>|"auto"
<tun interface>|"auto"
<local tunnel ip>|"auto"
<remote tunnel ip>|"auto"
<gateway ip>|"auto"
```

Väčšina parametrov je v zdrojovom kóde prednastavených na automatické hodnoty. Príkladom je port 443, vytvorenie rozhrania tun0, prevzatie externej IP ad-

resy zo siete a ďalšie. Používateľ teda môže spúšťať DSVPN pomocou príkazu s najmenej 2 parametrami v prípade servera a tromi pre prípad klienta. Dôvodom je, že klient potrebuje mať určenú IP adresu servera, na ktorý sa má pripojiť (3. parameter). Druhý parameter v poradí je už spomenutá cesta k zdieľanému 256-bitovému kľúču.

## 4.2 Kryptografia použitá v DSVPN

DSVPN používa v svojej implementácii malú sebestačnú kryptografickú knižnicu – *Charm*<sup>2</sup>. Jej autorom je tvorca DSVPN. Implementácia umožňuje autentizované šifrovanie (z ang. *authenticated encryption*) a hašovanie kľúčov (z ang. *keyed hashing*). Správnosť implementácie algoritmu v knižnici programátor overil pomocou nástroja **Cryptol**<sup>3</sup>. Uvedený nástroj slúži na zápis algoritmu do matematickej špecifikácií. Tým poskytne možnosť jednoduchšej a hlavne korektnej implementácie zvoleného kryptografického algoritmu. Zároveň je možné program využiť aj na verifikáciu vytvoreného riešenia. Obdobne sú v repozitári knižnice ponechané overovacie skripty pre jednoduché spustenie.

Kryptografický algoritmus použitý v DSVPN je Xoodoo permutácia v duplex móde, pričom môže byť jednoducho nahradená napríklad Gimli-im<sup>4</sup> [78] alebo Simpira384<sup>5</sup> [79]. Pri zmene musí používateľ zasiahnuť do zdrojového kódu v súbore **charm.c**, ktorého obsahom sú kryptografické primitíva.

## 4.3 Experimentálne overenie VPN

DSVPN sme prakticky overili pomocou dvojice virtuálnych strojov OSS a OSC, ktorých opis je obsahom 3.1. Na zariadení OSS sme pomocou balička make a GCC prekladača vykonali inštaláciu DSVPN. Obdobný postup je aplikovaný aj vo VM OSC. Na OSS spúšťame VPN Server, ktorý nám poskytne IP adresu, prostredníctvom ktorej budeme komunikovať s vonkajším svetom. Na spustenie a vytvorenie spojenie vykonáme nasledujúce úkony:

1. Vygenerovanie zdieľaného kľúča:

```
dd if=/dev/urandom of=vpn.key count=1 bs=32
```

<sup>2</sup><https://github.com/jedisct1/charm>

<sup>3</sup><https://cryptol.net/index.html>

<sup>4</sup><https://github.com/jedisct1/gimli>

<sup>5</sup><https://github.com/jedisct1/simpira384>

– zdieľaný kľúč, ktorý sme vygenerovali, sa nám uložil do súboru *vpn.key*. Jeho veľkosť je 32 bajtov, teda 256 bitov. Kľúč je potrebné vložiť do priečinka s programom *dsvpn* v oboch zariadeniach – OSS aj OSC alebo zadať cestu ako parameter, kde sa kľúč nachádza.

## 2. OSS zariadenie:

```
sudo ./dsvpn server vpn.key auto
2340 auto 10.8.0.254 10.8.0.2
```

– tento príkaz zabezpečí spustenie VPN servera na prostredí OSS s IP adresou. Príkaz *sudo* nám spustí program s administrátorskými právami. Piaty parameter nastavuje IP adresu servera. V našom prípade **auto**, použije aktuálne používanú IP na komunikáciu s vonkajším prostredím. Príkazom ďalej definujeme portové číslo 2340, ktoré sa použije pri nastolení TCP spojenie medzi klientom a serverom. Poslednou konfiguráciou je priradenie mena a IP adresy tunelov, ktoré bude využívať naše zariadenie – 10.8.0.254 a druhý koniec tunela – 10.8.0.2. Používateľ má ešte možnosť nastaviť tzv. External IP. Tú by sme využili ak by sme spúšťali DSVPN na routri poskytovateľa internetu. Obdobne na klientovi vieme nastaviť gateway IP, ktorá slúži na presmerovanie komunikácie k serveru. Po spustení príkazu si vieme overiť našu konfiguráciu<sup>6</sup>.

## 3. OSC zariadenie:

```
sudo ./dsvpn client vpn.key 192.168.88.62
2340 auto 10.8.0.2 10.8.0.254
```

– uvedený príkaz zabezpečí, že sa pripojíme na VPN Server, ktorý má IP adresu 192.168.88.62 s portom 2340. Následne vzniká TCP spojenie. Dôležité je si všimnúť poradie adries tunelov. Je opačné ako v prípade servera.

## 4. V prípade úspešnej konektivity sa operácia podarila a pre okolitý svet sme viditeľný pomocou IP adresy, ktorú sme zvolili.

Na overenie správnosti funkcionality nám postačí jednoduchý sieťový príkaz *tracert*. Napríklad *tracert google.sk*<sup>7</sup>. Prvá z uvedených adries je práve tá, ktorú dané zariadenie používa.

<sup>6</sup>Pomocou *ip address show tun0* overíme IPv4 adresu VPN tunela.

<sup>7</sup>vo Windows CMD prostredí: *tracert google.sk*



```

ubuntu21@ubuntu21-VirtualBox: ~/Plocha/dsvpn-master
ubuntu21@ubuntu21-VirtualBox: ~/Plocha/dsvpn-master$ ip address show
: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:42:5a:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.88.60/24 brd 192.168.88.255 scope global dynamic noprefixroute enp0s3
        valid_lft 362sec preferred_lft 362sec
    inet6 fe80::da75:ade1:9470:f56a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 9000 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.8.0.254 peer 10.8.0.2/32 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 64:ff9b::a08:fe peer 64:ff9b::a08:2/96 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::698a:bcc9:aaad:fb43/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
ubuntu21@ubuntu21-VirtualBox: ~/Plocha/dsvpn-master$

```

Obr. 4.2: Zistenie IP adresy VPN Servera na VM OSS

V našom prípade bolo nutné použiť lokálne adresy vzhľadom na to, že obe VM bežia na jednom hosťovskom počítači. Obidva zariadenia sú tým pádom pripojené k jednému internetovému poskytovateľovi, čo má za následok takmer rovnaké smerovanie k vzdialenej doméne.

Proces zistenia IP adresy VPN servera, po spustení, a overenie funkčnosti je následne znázornené pomocou 4.2, 4.3, 4.4. V 4.2 sme žltou farbou znázornili IP adresu, na ktorej je VPN server dostupný. Oranžová farba znázorňuje IP adresy tunelu medzi serverom a klientom v tomto poradí. Následne v 4.3 môžeme vidieť to isté pre klienta.

Nakoniec, v 4.4 môžeme vidieť ako klient pri internetovej komunikácii používa namiesto svojej vlastnej, adresu poskytnutú VPN Serverom na zariadení OSS – žltou zvýraznená IP. Červenou je zaškrnutá farba poskytovateľa internetu.

## 4.4 Princíp fungovania programu

DSVPN vytvára VPN sieť medzi VPN klientom a VPN serverom. Na oboch zariadeniach je potrebné spustiť program pomocou korešpondujúcich príkazov.

Princíp vysvetlíme na praktickom príklade. Klienta umiestnime na lokálnu sieť bez prístupu na internet. Následne vymažeme všetky smerovacie pravidlá v zariadení. Klient po tomto kroku nedokáže komunikovať so žiadnym zariadením nakoľko nemá žiadne prednastavené pravidlá kam by smeroval internetový ko-

```

ubuntu20@ubuntu20-VirtualBox: ~/Desktop/dsvpn-master
ubuntu20@ubuntu20-VirtualBox: ~/Desk... x ubuntu20@ubuntu20-VirtualBox: ~/Desk... x
18 prg03s13-in-f3.1e100.net (142.251.37.99) 21.788 ms 63.739 ms 63.745 ms
ubuntu20@ubuntu20-VirtualBox:~/Desktop/dsvpn-master$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
  1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group de
  fault qlen 1000
    link/ether 08:00:27:3f:3c:49 brd ff:ff:ff:ff:ff:ff
    inet 192.168.88.62/24 brd 192.168.88.255 scope global dynamic noprefixroute enp0s3
        valid_lft 444sec preferred_lft 444sec
    inet6 fe80::b281:ce29:9ef4:aefa/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP> mtu 9000 qdisc noop state DOWN group default ql
  en 500
    link/none
4: tun1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 9000 qdisc fq_codel state UNKNO
  WN group default qlen 500
    link/none
    inet 10.8.0.2 peer 10.8.0.254/32 scope global tun1
        valid_lft forever preferred_lft forever
    inet6 64:ff9b::a08:2 peer 64:ff9b::a08:fe/96 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::90cf:ae1b:e16:7a93/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
ubuntu20@ubuntu20-VirtualBox:~/Desktop/dsvpn-master$ S

```

Obr. 4.3: Zistenie IP adresy VPN Klienta na VM OSC

```

ubuntu20@ubuntu20-VirtualBox: ~/Desktop/dsvpn-master
ubuntu20@ubuntu20-VirtualBox: ~/Desk... x ubuntu20@ubuntu20-VirtualBox: ~/Desk... x
ubuntu20@ubuntu20-VirtualBox:~/Desktop/dsvpn-master$ traceroute google.sk
traceroute to google.sk (142.251.36.131), 30 hops max, 60 byte packets
 1 10.8.0.254 (10.8.0.254) 0.963 ms 1.439 ms 1.589 ms
 2 router.lan (192.168.88.1) 2.045 ms 2.205 ms 2.261 ms
 3 192.168.2.222 (192.168.2.222) 2.262 ms 2.686 ms 2.591 ms
 4 192.168.100.1 (192.168.100.1) 8.927 ms 7.779 ms 9.113 ms
 5 172.22.2.33 (172.22.2.33) 9.782 ms 12.546 ms 12.446 ms
 6 172.22.2.1 (172.22.2.1) 18.061 ms 13.177 ms 11.143 ms
 7 172.22.21.1 (172.22.21.1) 9.578 ms 22.255 ms 22.927 ms
 8 23.712 ms 24.022 ms 22.927 ms
 9 * * *
10 185.171.141.148 (185.171.141.148) 26.491 ms 29.919 ms 29.955 ms
11 185.171.140.8 (185.171.140.8) 29.954 ms 28.328 ms 27.494 ms
12 185.171.140.6 (185.171.140.6) 22.624 ms 22.746 ms 26.569 ms
13 185.171.140.12 (185.171.140.12) 26.734 ms 26.762 ms 26.715 ms
14 185.171.140.254 (185.171.140.254) 27.144 ms 26.904 ms 27.156 ms
15 87.244.236.49 (87.244.236.49) 26.686 ms 26.159 ms 26.180 ms
16 87.244.238.221 (87.244.238.221) 26.132 ms 36.561 ms 29.559 ms
17 87.244.238.78 (87.244.238.78) 24.069 ms 23.925 ms 24.922 ms
18 prg03s12-in-f3.1e100.net (142.251.36.131) 72.807 ms 72.852 ms 72.798 ms
ubuntu20@ubuntu20-VirtualBox:~/Desktop/dsvpn-master$

```

Obr. 4.4: Overenie funkcionality DSVPN pomocou traceroute

munikáciu. V uvedenej lokálnej sieti bude prítomný taktiež VPN server, ktorý ako jediný dokáže komunikovať s okolitým svetom. Po spustení DSVPN na obidvoch zariadeniach, dochádza k spojeniu. Jedná sa o TCP spojenie vytvorené soketmi. Úlohou soketového TCP spojenia je preposielanie už zašifrovaných dát v novom L3 pakete. Následne DSVPN overuje stav soketov a tunelovacieho rozhrania. Ak je tun rozhranie pripravené na čítanie (obsahuje pakety), tak dochádza k ich spracovaniu (šifrovaniu) a preposlaní cez soket. Po prijatí sa dáta dešifrujú a smerujú na základe dát z L3 IP hlavičky.

Toto je celý princíp zabezpečenej komunikácie medzi Klientom a Serverom vo VPN sieti na L3 vrstve. Aby sme docielili plnohodnotnú funkcionálnu VPN, tak potrebujeme do tohto riešenia zakomponovať smerovanie. Tým, že dáta smerujeme von z tejto siete, tak je ešte potrebné upraviť niektoré systémové smerovacie pravidla.

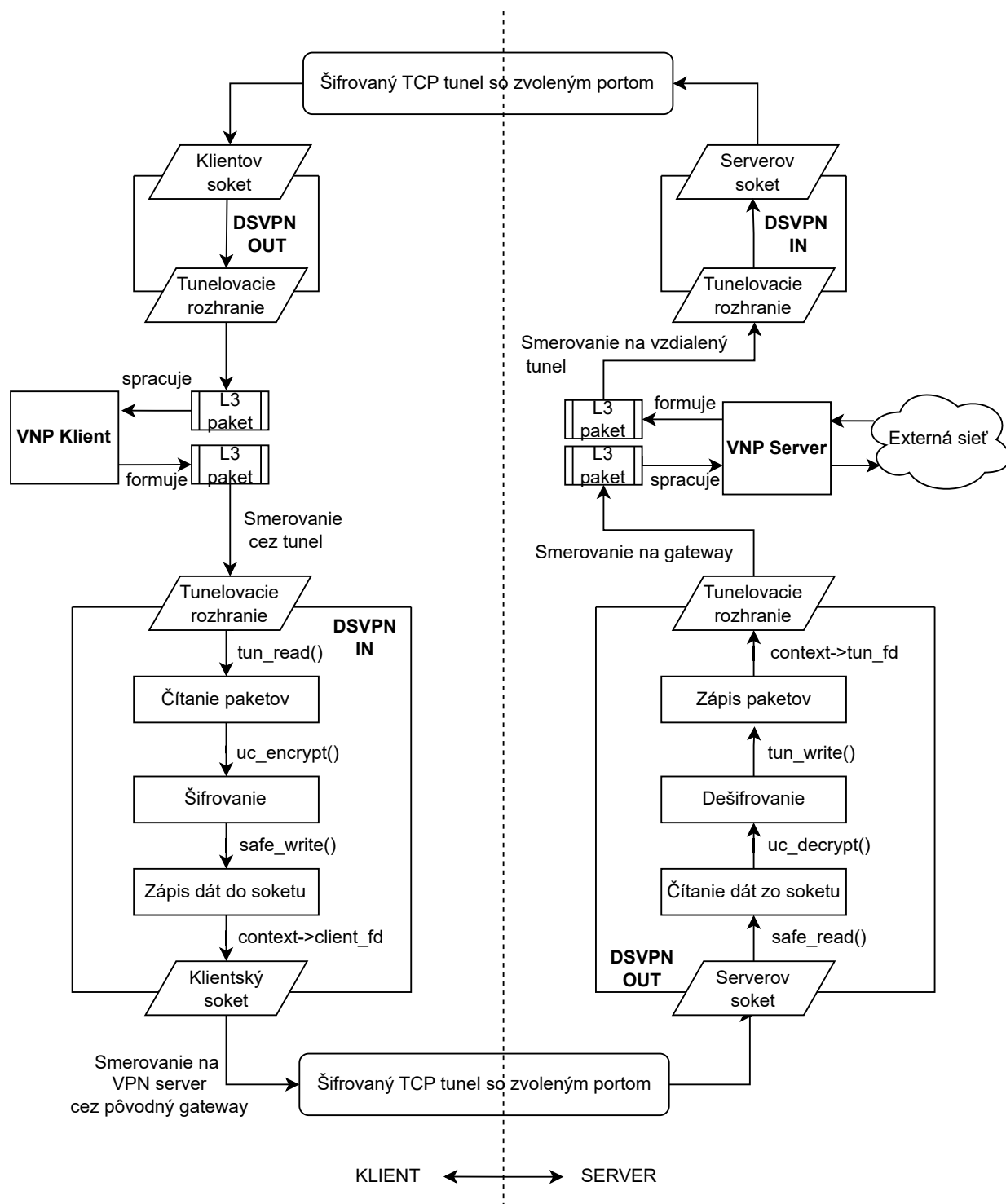
Okrem načrtnutého príkladu s prístupom na internet, dokáže klient takto získať konektivitu k jemu nedostupným segmentom siete. Samozrejme za predpokladu, že sú dostupné pre server. Ako príklad môže byť diskové úložisko. Prípadne prístup na internetové domény. V angličtine sa takýto termín označuje ako *remote access*, teda vzdialený prístup. Je to tiež veľmi obľúbený a používaný typ VPN siete.

Funkcionalita DSVPN je znázornená pomocou schémy 4.5. V nej môžeme na ľavej strane vidieť čo sa deje s paketom pri požiadavke smerom od VPN klienta k VPN serveru. OS na základe požiadavky formuje L3 pakety. Po presmerovaní paketu na tunel DSVPN zašifruje tieto dáta. Následne ich zapíše na soket, ktorý tvorí so serverom TCP spojenie. Server tieto dáta spracuje a vykoná potrebné náležitosti. Po získaní odpovede zasa Server odpovedá klientovi rovnakým mechanizmom. Čitateľovi by som rád doplnil, že v schéme sme pre DSVPN vytvorili 2 bloky. **DSVPN IN** a **DSVPN OUT**. Funkcionalita je znázornená iba v spodnej časti schémy. Jedná sa však o identické bloky.

## 4.5 Analýza zdrojového kódu DSVPN

Pri analýze sa zameriame výhradne na dôležité časti kódu DSVPN pre programovací jazyk C. Repozitár pozostáva z jedného make-file balíčka[80]. 3 hlavičkových (.h) a k nim korešpondujúcimi zdrojovými kódmi (.c), s pomenovaním:

1. **charm.h** – kryptografická knižnica so 6 funkciami,
2. **os.h** – funkcie čítania a zápisu paketov, vytvorenia, používania a zrušenia



Obr. 4.5: Ukážka prenosu paketu naprieč DSVPN

tunelovacieho rozhrania,

### 3. **vpn.h** – deklarácia konštánt, endianness[81] a niektorých závislostí OS.

V spomenutých hlavičkových súboroch sa nachádzajú deklarácie funkcií, ktoré VPN používa. Definície sú obsahom .c súborov, ako je v jazyku C zaužívaným

zvykom. Obsahom tejto podkapitoly je analýza týchto kódov.

### 4.5.1 Súbor charm.h a charm.c

Obsahom sú prevažne funkcie slúžiace pri behu kryptografického algoritmu XOODOO. Charm.h pozostáva z 6 funkcií. Ich implementácia nie je až tak rozsiahla. Zaberá celkovo 337 riadkov. Princípy použité v algoritme boli opísané v kapitole 2.

Zdrojový kód 4.1: Obsah charm.h

```
1 void uc_state_init(uint32_t st[12], const unsigned char key[32],  
2                     const unsigned char iv[16]);  
3 void uc_encrypt(uint32_t st[12], unsigned char *msg,  
4                 size_t msg_len, unsigned char tag[16]);  
5 int uc_decrypt(uint32_t st[12], unsigned char *msg,  
6                size_t msg_len,  
7                const unsigned char *expected_tag,  
8                size_t expected_tag_len);  
9 void uc_hash(uint32_t st[12], unsigned char h[32],  
10              const unsigned char *msg, size_t len);  
11 void uc_memzero(void *buf, size_t len);  
12 void uc_randombytes_buf(void *buf, size_t len);
```

Z názvov funkcií je pomerne jasné čo sa v jednotlivých volaniach deje.

### 4.5.2 Súbor os.h a os.c

Obsahom sú funkcie, ktorých úlohami sú čítanie alebo pridanie GW, vytvorenie a nastavenie tunelu v danom OS. Následne je aplikovaná úprava firewall pravidiel, tak aby všetka komunikácia bola presmerovaná na VPN server. Úprava firewall pravidiel je závislá od role, pod ktorou je VPN spustená. Teda či sa jedná o server alebo klienta. Celkovo je obsahom 12 funkcií, ktoré riešia uvedené úlohy. Detail je možné vidieť v 4.2.

Zdrojový kód 4.2: Obsah ZK os.h

```

1  ssize_t safe_read(const int fd, void *const buf_, size_t count,
2                      const int timeout);
3  ssize_t safe_write(const int fd, const void *const buf_,
4                      size_t count,
5                      const int timeout);
6  ssize_t safe_read_partial(const int fd, void *const buf_,
7                          const size_t max_count);
8  ssize_t safe_write_partial(const int fd, void *const buf_,
9                          const size_t max_count);
10
11 typedef struct Cnds {
12     const char *const *set;
13     const char *const *unset;
14 } Cnds;
15
16 Cnds firewall_rules_cmds(int is_server);
17 int shell_cmd(const char *substs[][2], const char *args_str,
18              int silent);
19 const char *get_default_gw_ip(void);
20 const char *get_default_ext_if_name(void);
21 int tcp_opts(int fd);
22 int tun_create(char if_name[IFNAMSIZ], const char *wanted_name);
23 int tun_set_mtu(const char *if_name, int mtu);
24 ssize_t tun_read(int fd, void *data, size_t size);
25 ssize_t tun_write(int fd, const void *data, size_t size);

```

Samozrejmosťou je implementácie čítania a zápisu dát z TUN tunelu, soketu a príkazového riadku.

### 4.5.3 Súbor vpn.h a vpn.c

Hlavičkový súbor obsahuje prevažne definovanie niektorých parametrov potrebných na správnu funkcionality VPN, spoločne s korekciou pre niektoré OS. Vid'. 4.3. Ostatné parametre, ktoré boli opísané pre spustenie, su definované práve v tomto súbore (porty, IP adresy, MTU atď.).

Zdrojový kód 4.3: Obsah ZK vpn.h

```

1  /*UNIX-like OS Dependent Libraries*/
2  #include <sys/ioctl.h>
3  #include <sys/socket.h>
4  #include <sys/types.h>
5  #include <sys/uio.h>
6  #include <sys/wait.h>
7  #include <net/if.h>
8  #include <netinet/in.h>
9  #include <netinet/tcp.h>
10 /*End UNIX-like OS Dependent Libraries*/
11 /*OS setup dependencies*/
12 #ifdef __linux__
13 #include <linux/if_tun.h>
14 #endif
15
16 #ifdef __APPLE__
17 #include <net/if_utun.h>
18 #include <sys/kern_control.h>
19 #include <sys/sys_domain.h>
20 #endif
21
22 #ifdef __NetBSD__
23 #define DEFAULT_MTU 1500
24 #else
25 #define DEFAULT_MTU 9000
26 #endif
27 /*End of OS setup dependencies*/

```

### Main() – Beh programu

Pred samotným opisom by som rád upozornil na jeden fakt. Autor DSVPN používa vo veľkej miere zápis pomocou tzv. ternárnych operátorov. Viac informácií o tejto problematike je možné nájsť v [82]. V skratke, používa sa podmienený zápis hodnoty do premennej.

Vpn.c je hlavným zdrojovým kódom DSVPN. V jeho vnútri nájdeme hlavnú, štartovaciu, funkciu main. Zároveň má prilinkované aj vyššie uvedené knižnice. Ako prvé dochádza k inicializácii premennej štruktúry Context4.4. Štruktúra v

sebe nesie všetky premenné, potrebné na správne fungovanie programu.

Zdrojový kód 4.4: Štruktúra Context

```

1 typedef struct Context_ {
2     const char * wanted_if_name;
3     const char * local_tun_ip;
4     const char * remote_tun_ip;
5     const char * local_tun_ip6;
6     const char * remote_tun_ip6;
7     const char * server_ip_or_name;
8     const char * server_port;
9     const char * ext_if_name;
10    const char * wanted_ext_gw_ip;
11    char        client_ip[NI_MAXHOST];
12    char        ext_gw_ip[64];
13    char        server_ip[64];
14    char        if_name[IFNAMSIZ];
15    int         is_server;
16    int         tun_fd;
17    int         client_fd;
18    int         listen_fd;
19    int         congestion;
20    int         firewall_rules_set;
21    Buf         client_buf;
22    struct pollfd fds[3];
23    uint32_t     uc_kx_st[12];
24    uint32_t     uc_st[2][12];
25 } Context;

```

Následne dochádza k načítaniu vopred zdieľaného kľúča pomocou pomocnej funkcie

`load_key_file()` 4.5. Úlohou je prečítanie kľúča, pričom sa používa funkcia z `os.c` – `safe_read()`. Realizuje sa znakové spočítanie, v ktorom je zakomponovaná funkcia `poll()` [83]. Dôvodom je, že `safe_read()` sa používa aj pri čítaní zo soketu a tunelu. V linuxe je čítanie z týchto typov rovnaké. Tato časť kódu je však podmienená špecifickou chybou, ktorú je možné dostať len pri čítaní soketu, respektíve tunelu. V prípade, ak sa prečítalo 32 bajtov, `safe_read()` vracia 0. Následne sa inicializuje stav v `XOODOO`.



Zdrojový kód 4.5: Načítanie zdieľaného kľúča

```

1  static int load_key_file(Context *context, const char *file)
2  {
3      unsigned char key[32];
4      int          fd;
5
6      if ((fd = open(file, O_RDONLY)) == -1) {
7          return -1;
8      }
9      if (safe_read(fd, key, sizeof key, -1) != sizeof key) {
10         (void) close(fd);
11         return -1;
12     }
13     uc_state_init(context->uc_kx_st, key,
14                  (const unsigned char *) "VPN_Key_Exchange");
15     uc_memzero(key, sizeof key);
16
17     return close(fd);
18 }

```

Ako môžeme vidieť v implementácii sú bežne použité smerníky. Vo výsledku tak dokážeme preniesť zmenu hodnôt na viaceré premenné.

V prípade, ak používateľ pri štarte nezmenil parameter pre IP adresu sieťovej brány<sup>8</sup> (ďalej GW), tak sa používa pôvodná. Tá sa získa pomocou funkcie `get_default_gw_ip()`, ktorá je deklarovaná v 4.2. Prostredníctvom shell príkazu `ip route` a `read_from_shell_command()` funkcie, dochádza k extrakcii informácií priamo z príkazového riadka. Tento krok je teda závislý od OS, v ktorom používateľ pracuje. Nasleduje overenie návratových hodnôt z funkcií iba v prípade ak je DSVPN spustené ako Klient.

Program v prípade servera pokračuje s `get_default_ext_if_name()`. Obdobne ako v predchádzajúcom odstavci je realizácia funkcionality, vykonaná pomocou terminálu. Podstata spočíva v zistení mena tunelovacieho rozhrania.

Po nastavení parametrov sa dostávame k vytvoreniu tunelovacieho rozhrania. V tomto kroku autor používa funkciu `tun_create`. Úloha je vysoko závislá od OS. Dôsledkom toho je možné vidieť vetvenie funkcionality vzhľadom k bežiacemu OS. DSVPN poskytuje kompatibilitu pre 6 OS, medzi, ktoré patrí Linux, FreeBSD, NetBSD, OpenBSD, MacOS, DragonFly. Následne na základe systému dochádza

<sup>8</sup>z ang. *GateWay*

k vytváraniu tunelu s prednastaveným, resp. zvoleným menom. Program ďalej nastaví maximálnu veľkosť prepravovaného paketu<sup>9</sup> (ďalej MTU) na 1500/9000 bajtov.

Po príprave tunelu dochádza k overeniu dostupnosti VPN servera. Tento krok vykonáva funkcia `resolve_ip`. Tá ma v sebe vnorené 2 funkcie, ktoré su meným ekvivalentom aj vo Windows knižniciach. Jedná sa o funkcie `getaddrinfo` a `getnameinfo`.

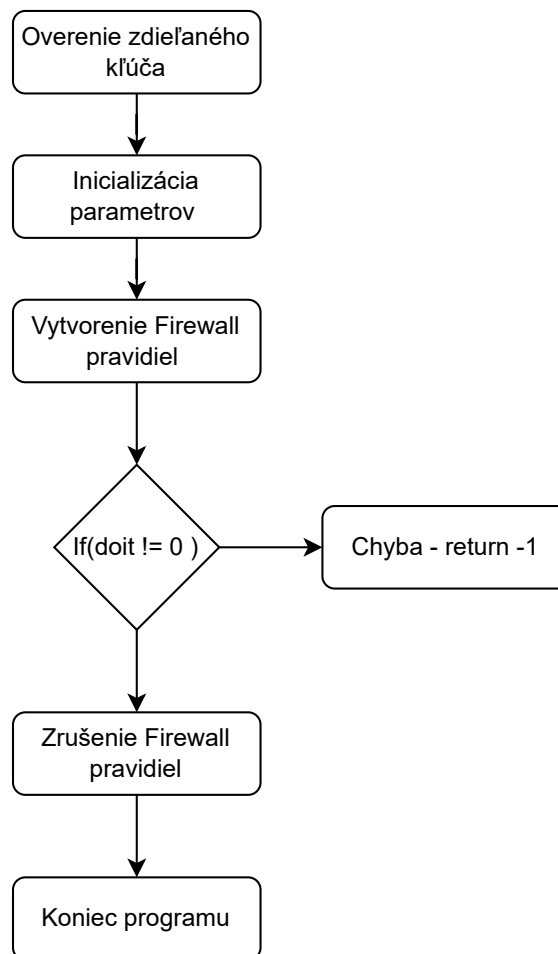
Posledným krokom súvisiacim s konfiguráciou prostredia je vytvorenie pravidla pre branu FireWall (ďalej FW). Tento úkon realizuje `firewall_rules()`. Tento proces je opäť systémovo závislý. Jeho realizácia je vykonaná pomocou globálne definovanej funkcie `Cmds firewall_rules_cmds()`. Tá obsahuje súbor prednastavených príkazov. Ich úlohou je presmerovanie celej premávky cez vzniknutý tunel.

Posledným úkonom je samotný beh VPN. Ten spúšťa funkcia `doit()`. Doterajší beh programu je jednoducho znázornený pomocou flow diagramu 4.6.

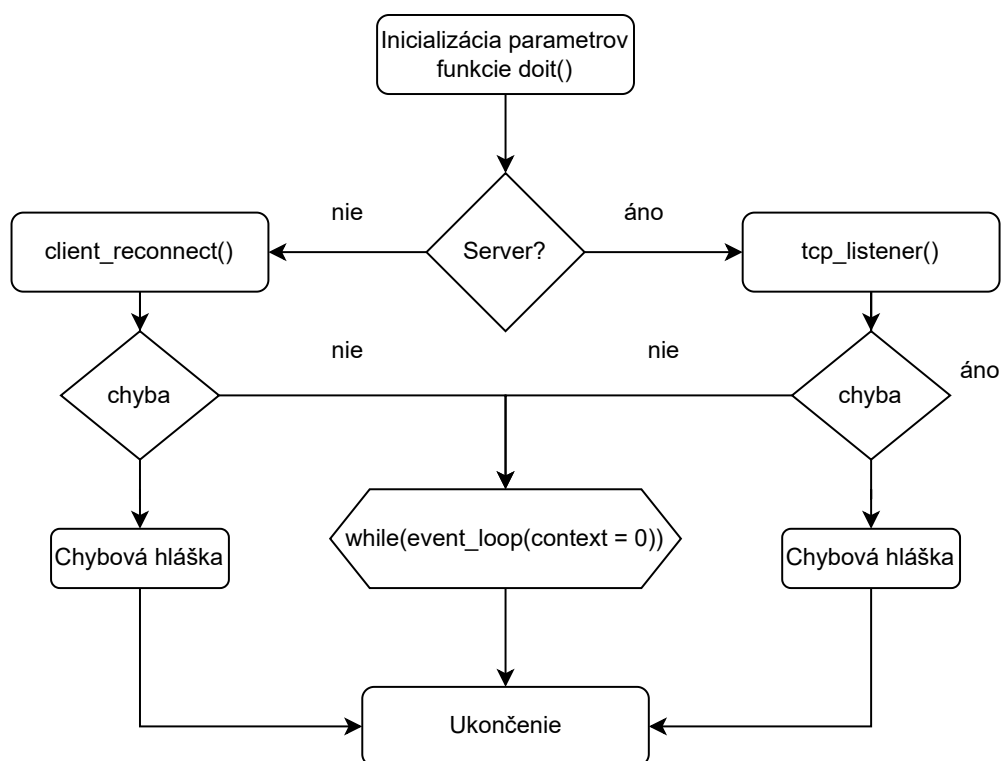
Od tohto momentu sa presúvame k postupnému vnáraníu do procesu spojenia a spracovania dát. Hlavnou úlohou funkcie `doit()` je nadviazanie soketového TCP spojenia medzi klientom a serverom. Vo vnútri `doit()` preto dochádza k vetveniu programu. V prípade, že je DSVPN spustená ako server spustí sa funkcia `tcp_listener()`. V opačnom prípade `client_reconnect()`. Listener vytvára socket a následne pomocou systemovej funkcie `bind()` sa napojí na zvolený port. Potom čaká na spojenie od klienta pomocou funkcie `listen()`. Smerník na socket je uložený do smerníka na štruktúru `Context`. Klient používa vetvu s `Client_reconnect()`. V nej sa snaží opakovane nadviazať spojenie so serverom. Za týmto účelom `client_connect()`. Pred týmto úkonom samozrejme dochádza k overeniu či už nedošlo k nadviazaniu spojenia. O to sa stará `client_disconnect()`, ktorý ruší aktívne spojenie.

`Client_connect()` slúži na pripojenie klienta k serveru. Vykonáva aj úpravu pravidiel v FW. Následne sa pokúša o nadviazania spojenia pomocou funkcie `tcp_client()`. Po tejto sérii úloh sa vraciame opäť do `doit()`. V cykle **while** sa vykonávaná funkcia `event_loop()`, v ktorej dochádza k použitiu kryptografickej knižnice `charm`. Jej obsahom je inicializácia pomocných premenných. viď. zdrojový kód 4.6. Schéma 4.7 znázorňuje doteraz opísané skutočnosti.

<sup>9</sup>z ang. *Maximum Transmission Unit*



Obr. 4.6: Beh DSVPN



Obr. 4.7: Princíp fungovania funkcie doit()

Zdrojový kód 4.6: Premenné funkcie event loop

```

1  struct pollfd *const fds = context->fds;
2  Buf          tun_buf;
3  Buf *        client_buf = &context->client_buf;
4  ssize_t      len;
5  int          found_fds;
6  int          new_client_fd;

```

### Funckia event\_loop()

Event\_loop() je 111 riadkov dlhá funkcia. Jej obsah môžeme rozdeliť na overovací a výkonový. Úlohou niekoľkých **if**-ov vo funkcii je preverovanie signálov, spätných hodnôt a podobných premenných, ktoré by signalizovali chybu, používateľov záujem o ukončenie programu alebo signál pre čítanie dát zo soketov, respektíve tunelov.

Zaujímavé je taktiež predom definované makro **BUFFERBLOAT\_CONTROL**. Jeho úlohou je zamedzenie problému zvaného **Bufferbloat**. V skratke, je to nechcený jav, ktorý je zapríčinený nadmerným ukladaním paketov do vyrovnávacej pamäte, tzv. zahltenie. To ma za následok vysokú latenciu a tzv. z ang. *Packet Delay*

*Variation* (ďalej PDV/Jitter), v paketovo-orientovaných sieťach. Viac o tejto problematike je možné si prečítať na [84].

Na druhej strane výkonové funkcie, ako hovorí ich názov, niečo vykonávajú. Do tejto kategórie sme zaradili funkcie:

- `tcp_accept()` – slúži na nastolenie nového soketového TCP spojenia s klientom,
- `tun_read()` – v prípade linuxového OS, volá `safe_read_partial()` na zapísanie dát do nami vytvoreného tunelovacieho rozhrania,
- `uc_encrypt()` – kryptografické šifrovanie paketov z tunelovacieho rozhrania,
- `safe_write_partial()` – používa štandardizovanú funkciu `write()` vo while cykle, zapíše zašifrované dáta do buffera určeného pre odoslanie klientovi, vracia počet zapísaných dát,
- `safe_write()` – používa sa v prípade ak došlo k zahlteniu paketmi,
- `client_reconnect()` – slúži na obnovu spojenia v prípade chyby,
- `safe_read_partial()` – obdobne ako pri `write()`, používa `read()` funkciu,
- `uc_decrypt()` – kryptografické dešifrovanie správy a následne odoslanie na tunelovacie rozhranie,
- `tun_write()` – volá `safe_write` pri OS Linux, teda klasický zápis dešifrovaných dát.

Metóda použitá pri zápise zašifrovaných dát vo funkcii `event_loop()` je znázornená v 4.7.

Zdrojový kód 4.7: Spôsob zápisu šifrovaných dát

```

1
2  writenb = safe_write_partial(context->client_fd, tun_buf.len,
3                               2U + TAG_LEN + len);
4  if (writenb < (ssize_t) 0) {// kontrola zahltenia -- bufferbloat
5      context->congestion = 1;
6      writenb              = (ssize_t) 0;
7  }
8  // ak doslo k zahlteniu
9  if (writenb != (ssize_t)(2U + TAG_LEN + len)) {
10     writenb = safe_write(context->client_fd, tun_buf.len + writenb,
11                          2U + TAG_LEN + len - writenb, TIMEOUT);
12 }

```

V princípe celá logika tejto VPN pozostáva z kontroly obsahu tunelovacieho rozhrania a aktívnych soketov. Následne ak sa na vstupoch nachádzajú dáta dochádza k ich čítaniu, dešifrovaniu a následnému odoslaniu dát aplikácií, ktorej prislúchajú.

Na konci funkcie `event_loop()` sa nachádza ešte overenie pre prípad keď buffer s dátami nie je úplne plný. V tomto prípade funkcia vykonáva posun uložených bajtov na začiatok bufferu. Inými slovami pripravuje dáta na ďalšie čítanie. Vyššie uvedené výroky sú znázornené v zdrojovom kóde 4.8.

Zdrojový kód 4.8: Príprava dát na ďalšie čítanie

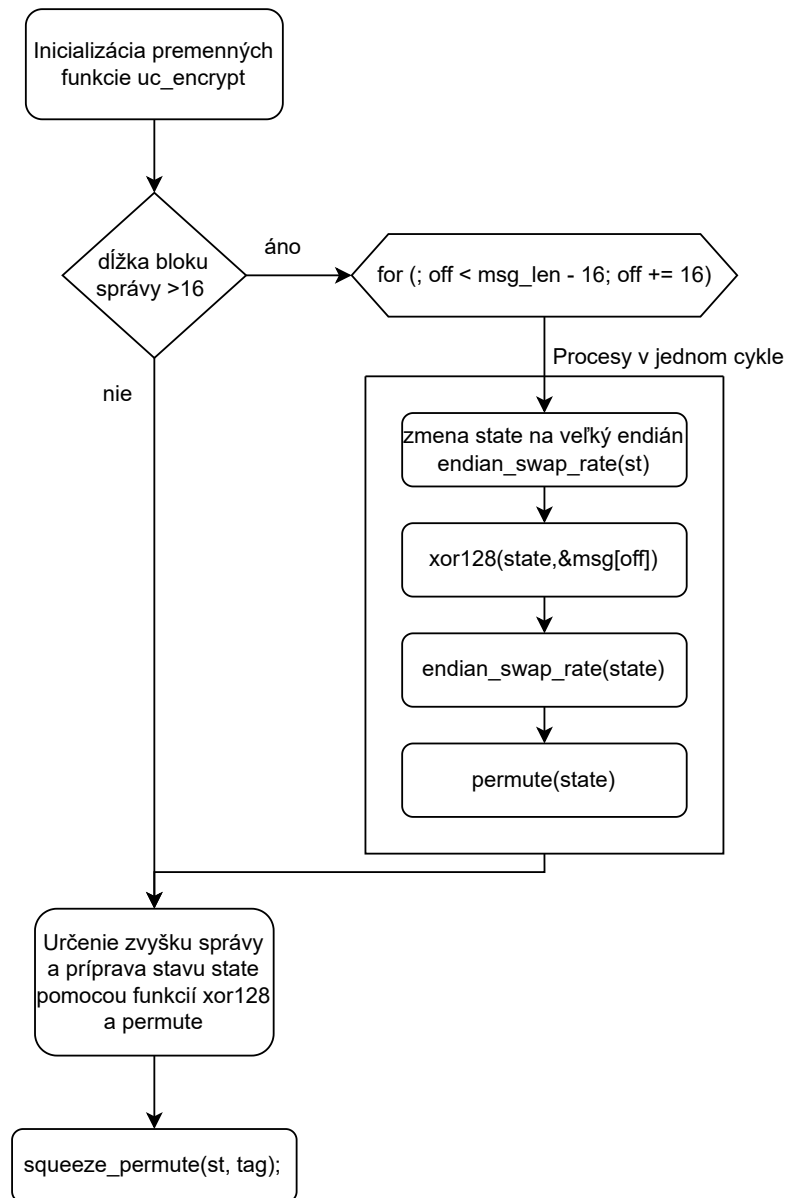
```

1
2  if (2 + TAG_LEN + MAX_PACKET_LEN != len_with_header) {
3      unsigned char *rbuf      = client_buf->len;
4      size_t          remaining = client_buf->pos - len_with_header;
5      memmove(rbuf, rbuf + len_with_header, remaining);
6  }
7  client_buf->pos -= len_with_header;

```

## Šifrovanie a dešifrovanie

Proces šifrovania resp. dešifrovania správy nastáva na oboch stranách spojenia, teda pri klientovi aj serveri. Zdrojový kód 4.9 demonštruje šifrovanie implementované v funkcii `uc_encrypt()`. Tento proces sme sa pokúsili opísať v grafe 4.8.



Obr. 4.8: Proces šifrovania v funkcii `uc_encrypt()`

Zdrojový kód 4.9: Šifrovanie správy pomocou uc\_encrypt

```

1
2 void uc_encrypt(uint32_t st[12], unsigned char *msg,
3               size_t msg_len, unsigned char tag[16])
4 { //spracovanie po 16 znakov
5   unsigned char squeezed[16];
6   unsigned char padded[16 + 1];
7   size_t      off = 0;
8   size_t      leftover;
9
10  if (msg_len > 16) {
11    for (; off < msg_len - 16; off += 16) {
12      endian_swap_rate(st);
13      memcpy(squeezed, st, 16);
14      xor128(st, &msg[off]);
15      endian_swap_rate(st);
16      xor128(&msg[off], squeezed);
17      permute(st);
18    }
19  }
20  leftover = msg_len - off;
21  memset(padded, 0, 16);
22  mem_cpy(padded, &msg[off], leftover);
23  padded[leftover] = 0x80;
24  endian_swap_rate(st);
25  memcpy(squeezed, st, 16);
26  xor128(st, padded);
27  endian_swap_rate(st);
28  st[11] ^= (1UL << 24 | (uint32_t) leftover >> 4 << 25
29           | 1UL << 26);
30  xor128(padded, squeezed);
31  mem_cpy(&msg[off], padded, leftover);
32  permute(st);
33  squeeze_permute(st, tag); //vytvorenie tagu
34 }

```

Ako je viditeľné v kóde dochádza k častému použitiu 2 funkcií. Nimi sú `xor128()` a `permute()`. Jedná sa o pomerne dôležité bloky pre správne fungovanie šifrovacieho algoritmu. Obsah prvej z uvedených je preto znázornený v zdrojovom kóde



## 4.10.

Zdrojový kód 4.10: Funkcia xor128

```

1 static inline void xor128(void *out, const void *in)
2 {
3     #ifdef __SSSE3__
4         _mm_storeu_si128((__m128i *) out,
5         _mm_xor_si128(_mm_loadu_si128((const __m128i *) out),
6         _mm_loadu_si128((const __m128i *) in)));
7     #else
8         unsigned char * out_ = (unsigned char *) out;
9         const unsigned char *in_ = (const unsigned char *) in;
10        size_t i;
11
12        for (i = 0; i < 16; i++) { //xorovanie jednotlivych znakov
13            out_[i] ^= in_[i]; //v 16 bitovom bloku spravy
14        }
15    #endif
16 }

```

Funkcia `permute()` je pomerne rozsiahla. Jej obsah sa rozprestiera na 100 riadkoch. Jedná sa o implementáciu XOODOO permutácie, ktorá bola opísaná v kapitole číslo 2. Funkcionalita závisí od prostredia a procesorových inštrukcií. Samozrejmosťou je softvérová implementácia, ktorá je aj použitá pri behu. Dôvodom je, že naše zariadenie nemá k dispozícii uvedené procesorové inštrukcie. Blok, ktorý je použitý pri volaní sa nachádza v 4.11.

Zdrojový kód 4.11: Funkcia Permute + makrá

```

1  #define ROTR32(x, b) (uint32_t)((((x) >> (b)) |
2      ((x) << (32 - (b)))))
3  #define SWAP32(s, u, v) \
4  do { \
5      t = (s)[u]; \
6      (s)[u] = (s)[v], (s)[v] = t; \
7  } while (0)
8
9  static void permute(uint32_t st[12])
10 {
11     uint32_t e[4], a, b, c, t, r, i;
12     for (r = 0; r < XOODOO_ROUNDS; r++) {
13         for (i = 0; i < 4; i++) {
14             e[i] = ROTR32(st[i] ^ st[i + 4] ^ st[i + 8], 18);
15             e[i] ^= ROTR32(e[i], 9);
16         }
17         for (i = 0; i < 12; i++) {
18             st[i] ^= e[(i - 1) & 3];
19         }
20         SWAP32(st, 7, 4);
21         SWAP32(st, 7, 5);
22         SWAP32(st, 7, 6);
23         st[0] ^= RK[r];
24         for (i = 0; i < 4; i++) {
25             a = st[i];
26             b = st[i + 4];
27             c = ROTR32(st[i + 8], 21);
28             st[i + 8] = ROTR32((b & ~a) ^ c, 24);
29             st[i + 4] = ROTR32((a & ~c) ^ b, 31);
30             st[i] ^= c & ~b;
31         }
32         SWAP32(st, 8, 10);
33         SWAP32(st, 9, 11);
34     }
35 }

```

Na druhej strane k **dešifrovaniu** dochádza v momente ak sa v klientskom sockete nachádzajú dáta. Program overuje či sú v premennej `fds[POLLFD_CLIENT]`

dáta určené na spracovanie. `fds[POLLFD_CLIENT]` predstavuje smerník na pamäťový blok, kde je uložený soket na druhú stranu spojenia, teda akceptovaného klienta. V momente keď sa tam nachádzajú dáta dôjde k ich čítaniu pomocou funkcie `safe_read_partial()`. Následne program realizuje dešifrovanie funkciou `uc_decrypt()`, ktorá je inverznou k `uc_encrypt()`. V ukážke zdrojového kódu 4.12, si používateľ môže prezrieť obsah funkcie `uc_decrypt()`. Po odšifrovaní dát ich program zapisuje do tunelovacieho rozhrania prostredníctvom funkcie `tun_write()`. Následne TUN rozhranie dotvára paket a vloží ho do sieťového zásobníka<sup>10</sup>. OS následne vykonáva ďalšie spracovanie paketu do nižších vrstiev sieťového modelu.

---

<sup>10</sup>z ang. *network stack*

Zdrojový kód 4.12: Funkcia Permute + makrá

```

1  int uc_decrypt(uint32_t st[12], unsigned char *msg,
2              size_t msg_len,
3              const unsigned char *expected_tag,
4              size_t expected_tag_len)
5  {
6      unsigned char tag[16];
7      unsigned char squeezed[16];
8      unsigned char padded[16 + 1];
9      size_t      off = 0;
10     size_t      leftover;
11
12     if (msg_len > 16) {
13         for (; off < msg_len - 16; off += 16) {
14             endian_swap_rate(st);
15             memcpy(squeezed, st, 16);
16             xor128(&msg[off], squeezed);
17             xor128(st, &msg[off]);
18             endian_swap_rate(st);
19             permute(st);
20         }
21     }
22     leftover = msg_len - off;
23     memset(padded, 0, 16);
24     mem_cpy(padded, &msg[off], leftover);
25     endian_swap_rate(st);
26     memset(squeezed, 0, 16);
27     mem_cpy(squeezed,
28             (const unsigned char *) (const void *) st,
29             leftover
30             );
31     xor128(&padded, squeezed);
32     padded[leftover] = 0x80;
33     xor128(st, padded);
34     endian_swap_rate(st);
35     st[11] ^= (1UL << 24 | (uint32_t) leftover >> 4
36             << 25 | 1UL << 26);
37     mem_cpy(&msg[off], padded, leftover);
38     permute(st);
39     squeeze_permute(st, tag);
40     \\
41     if (equals(expected_tag, tag, expected_tag_len) == 0) {
42         memset(msg, 0, msg_len);

```

Pre čitateľa sme si pripravili aj názornú ukážku šifrovania a prenosu týchto dát cez soket. Za účelom ukážky použijeme už spomínaný nástroj Wireshark na zachytávanie premávky v sieťových rozhraniach. Prechod dát z pohľadu klienta medzi zariadeniami je znázornený na obrázku ???. Na VPN klientovi sme spustili

25	3.043615224	10.8.2.1	10.8.1.1	ICMP	100 Echo (ping) request
26	3.043662924	192.168.88.25	192.168.88.36	TCP	160 33000 → 2340 [PSH,
27	3.059505089	192.168.88.36	192.168.88.25	TCP	160 2340 → 33000 [PSH,
28	3.059535035	192.168.88.25	192.168.88.36	TCP	68 33000 → 2340 [ACK]
29	3.066620423	10.8.1.1	10.8.2.1	ICMP	100 Echo (ping) reply

Obr. 4.9: Prenos zašifrovaných dát z VPN klienta na VPN server

v príkazovom riadku jednoduchý príkaz `ping 10.8.1.1`. Ten nám vytvára veľmi známy ICMP paket so žiadosťou o odpoveď<sup>11</sup>. Obsah tohto paketu je možné si pozrieť v obrázku 4.10. Tento paket je vo VPN klientovi po spracovaní vo DSVPN

00 04 ff fe 00 00 00 00	00 00 00 00 00 00 08 00	.....
45 00 00 54 4f 13 40 00	40 01 d4 84 0a 08 02 01	E..TO..@..@.....
0a 08 01 01 08 00 0c 19	00 01 00 06 c0 92 35 64	.....5d
00 00 00 00 30 16 07 00	00 00 00 00 10 11 12 13	....0.....
14 15 16 17 18 19 1a 1b	1c 1d 1e 1f 20 21 22 23	.....!"#
24 25 26 27 28 29 2a 2b	2c 2d 2e 2f 30 31 32 33	\$%&'()*+,-./0123
34 35 36 37		4567

Obr. 4.10: Obsah pôvodného paketu s ICMP žiadosťou

zašifrovaný pomocou XOODOO permutácie a odoslaný cez soketové TCP spojenie<sup>12</sup>. Obsah zašifrovaného paketu je znázornený v 4.11. Označená časť paketu v obrázku je už spomenutý zašifrovaný ICMP paket z obrázku 4.10. VPN server ho po prijatí dešifruje a posíla na vlastné tunelovacie rozhranie. Oďiaľ prevezme paket OS a vygeneruje odpoveď na pôvodnú požiadavku vo forme nového paketu. Ten je prenesený na klienta opäť cez soketové TCP spojenie<sup>13</sup>. Paket číslo 28 je odpoveď na úspešne prijatie. DSVPN spracuje tento paket a zapíše pôvodný na tunelovacie rozhranie.. Z hľadiska klienta už vidíme dešifrovanú odpoveď v pakete číslo 29, ktorú spracuje OS.

<sup>11</sup>paket číslo 25<sup>12</sup>paket číslo 26<sup>13</sup>paket číslo 27

24	3.022035206	127.0.0.1	224.0.0.251	MDNS	84 Standard query 0x0
25	3.043615224	10.8.2.1	10.8.1.1	ICMP	100 Echo (ping) request
26	3.043662924	192.168.88.25	192.168.88.36	TCP	160 33000 → 2340 [PSH, ACK]
27	3.059505089	192.168.88.36	192.168.88.25	TCP	160 2340 → 33000 [PSH, ACK]
28	3.059535035	192.168.88.25	192.168.88.36	TCP	68 33000 → 2340 [ACK]
29	3.066620423	10.8.1.1	10.8.2.1	ICMP	100 Echo (ping) reply
30	3.209940911	192.168.88.28	224.0.0.251	MDNS	141 Standard query 0x0
31	3.209941241	fe80::14f2:2b7a:876...	ff02::fb	MDNS	161 Standard query 0x0

Frame 26: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface any, id 0					
Linux cooked capture v1					
Internet Protocol Version 4, Src: 192.168.88.25, Dst: 192.168.88.36					
Transmission Control Protocol, Src Port: 33000, Dst Port: 2340, Seq: 333, Ack: 277, Len: 92					
Data (92 bytes)					
Data: 5400115444c27255fd4e5ab2d8c351ab5a2b4e320332d6a9c29e4b426d74d56811d1d57c...					
[Length: 92]					

0000	00 04 00 01 00 06 08 00	27 9a 1b 31 00 00 08 00	.....'..1....
0010	45 00 00 90 47 ab 40 00	40 06 c1 2e c0 a8 58 19	E...G..@..X.
0020	c0 a8 58 24 80 e8 09 24	5b e7 b5 3b d9 c6 c3 b6	..X\$. \$ [..;....
0030	80 18 01 f5 32 11 00 00	01 01 08 0a 50 d5 7d 95	...2....P..
0040	c7 48 6f 33 54 00 11 54	44 c2 72 55 fd 4e 5a b2	..Ho3T...T D.rU.NZ.
0050	d8 c3 51 ab 5a 2b 4e 32	03 32 d6 a9 c2 9e 4b 42	..Q.Z+N2 .2....KB
0060	6d 74 d5 68 11 d1 d5 7c	f8 3b 26 e9 3e 4e 49 08	mt.h...  .;>NI.
0070	5a 35 0f 07 6a f4 7a 81	c0 81 6e 3d 63 b5 7f b5	Z5..j.z..n=C...
0080	e9 db 07 d1 57 4a 41 6f	f6 0b 61 4d ab 51 bd 32	...WJAo ..aM.Q.2
0090	66 52 83 6d 59 06 28 5a	a1 09 9e 29 53 16 c8 b7	fR.mY.(Z ...)S...

Obr. 4.11: Zašifrovaný pôvodný ICMP paket v novom TCP pakete

## Ukončenie činnosti programu

Používateľ má možnosť ukončiť vzniknuté VPN spojenie medzi klientom a serverom pomocou jednoduchej príkazu `crtl + c`. Program zaznamená tento vstup a ukončí cyklus. Po návrate až do hlavnej funkcie `main()` sa z OS vymažú aplikované FW pravidlá a používateľ môže používať počítač ako pred spustením DSVPN.

## 4.6 Analýza výpočtových nárokov DSVPN

Za účelom analýzy výpočtových nárokov sme sa v práci zamerali na meranie potrebného počtu cyklov a zároveň aj času, potrebného na vykonanie šifrovania a dešifrovania permutácie XOODOO. Pre linuxovú platformu sme použili niektoré zabudované funkcie ako je `clock()`. Pomocou nej sme zmerali čas vykonávania. Ukážka ako bol kód na meranie implementovaný do DSVPN je možné vidieť v ukážke zdrojového kódu

Zdrojový kód 4.13: Ukážka spôsobu merania pri (de)šifrovaní XODOO

```

1  uint64_t time,tick; //inicializacia premennych
2  clock_t t = clock();
3
4  tick = cpucyclesS();
5  codeToMeasure(); //funkcia urcena na meranie
6  time = cpucyclesE()-tick;
7
8  t = clock() - t; //vyhodnotenie
9  double time_taken = ((double)t)/CLOCKS_PER_SEC;
10 printf(Size(%ld B): "%llu_cycles_in_%f_s\n", msg_length,
11         time, time_taken);

```

V prípade, ak by používateľ potreboval vykonať podobné meranie času v prostredí OS Windows, tak dávame do pozornosti tento variant. Viď zdrojový kód 4.14. Viac o použití a limitáciách je možné nájsť v práci [bc].

Zdrojový kód 4.14: Meranie času vykonávania na OS Windows

```

1  #include <windows.h>
2
3  #define TIMER_INIT \ //inicializacia makra
4  LARGE_INTEGER frequency; \
5  LARGE_INTEGER t1,t2; \
6  double elapsedTime; \
7  QueryPerformanceFrequency(&frequency);
8
9  #define TIMER_START QueryPerformanceCounter(&t1);
10 #define TIMER_STOP \
11 QueryPerformanceCounter(&t2); \
12 elapsedTime=(double)(t2.QuadPart-t1.QuadPart)
13         /frequency.QuadPart;
14
15 TIMER_INIT    \\pouzitie
16 {
17     TIMER_START
18     codeToMeasure()
19     TIMER_STOP
20 }

```

Spojenie medzi klientom a serverom je spustené na VM. Šifrovanie bolo me-

rané na strane Klienta. Dešifrovanie sme merali v OS servera. Počas spojenia sme sa snažili naviesť stav väčšieho sieťového zataženia. Tento úkon sme zrealizovali otvorením viacerých rôznych kariet vo webovom prehliadači. Týmto spôsobom sme odsimuloval potrebu prenosu väčšieho množstva dát naprieč sieťou. Najčastejšie však do šifrovania vstupovali TCP pakety, ktoré majú za úlohu udržať sokeťové TCP spojenie. Ich veľkosť je 52 bajtov. Z výpisu sme ešte na základe pozorovania sledovali aké veľkosti sa najčastejšie vyskytujú. Na základe takto získaných dát sme vypracovali tabuľku 4.1. Hodnoty pre jednotlivé stĺpce boli získane ako aritmetický priemer z meraní. Pakety, ktoré vstupovali do šifrovania, resp. dešifrovania menej ako 20-krát sme z meraní vypustili. Dôvodom je snaha o získanie lepších štatistických údajov. Obdobne sme pri výpočte aritmetického priemeru nebrali do úvahy príliš veľké výchylky pri meraní počtu cyklov. Uvedené chyby merania spôsobil samotný OS, kvôli prerušovania činnosti programu DSVPN.

Veľkosť dát[B]	Názov meranej funkcie			
X	uc_encrypt()		uc_decrypt()	
Počet meraní	Počet cyklov	Čas vykonávania [s]	Počet cyklov	Čas vykonávania [s]
52 X 1376	1 648	0.000 076	2 377	0.000 062
60 X 79	2 527	0.000 049	2 769	0.000 044
64 X 47	1 799	0.000 048	2 341	0.000 043
80 X 145	2 853	0.000 053	3 343	0.000 057
91 X 128	2 944	0.000 046	2 965	0.000 042
116 X 35	4 083	0.000 049	2 878	0.000 049
222 X 23	4 220	0.000 345	3 976	0.000 040
569 X 51	10 245	0.000 950	8 574	0.000 043
1 385 X 147	21 232	0.000 165	19 046	0.000 045
1 452 X 14	22 599	0.000 077	20 083	0.000 532
Celkom [B]	-	-	-	-
364 656	74 150	0.001 858	68 352	0.000 957

Tabuľka 4.1: Výsledky získaných meraní

Ako môžeme vidieť z experimentálnych meraní, tak implementácia XOODOO algoritmu je na bežnom počítači extrémne rýchla. Faktom ostáva že do meraní nám vo veľkej miere zasahuje OS. Okrem tohto faktu bežal klient aj server vo virtuálnom prostredí nad iným natívnym OS, so značne obmedzeným výkonom. Z výsledkov však môžeme zhodnotiť, že šifrovanie a dešifrovanie dokáže držať na úrovni 40-70 mikrosekúnd v závislosti od veľkosti vstupujúcich dát a prostredia, na ktorom aplikácia beží.

Súčasťou príloh sú súbory s logmi, z ktorých bola tabuľka vytvorená. Zároveň



prikladáme aj zdrojový kód programu, ktorý bol použitý na spracovanie výsledkov. Vid' priečinok Measurements.

## **4.7 Windows kompatibilita**

## 5 Vyhodnotenie dosiahnutých výsledkov

---

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam lobortis facilissem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis fringilla tristique neque. Sed interdum libero utmetus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

## 6 Záver

---

# Literatúra

---

1. Generic Routing Encapsulation. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Generic\\_Routing\\_Encapsulation](https://en.wikipedia.org/wiki/Generic_Routing_Encapsulation). [Online; Citované: 31.3.2023].
2. Generic Routing Encapsulation (GRE). [B.r.]. Dostupné tiež z: <https://www.rfc-editor.org/info/rfc1701>. [Online; Citované: 31.3.2023].
3. Tunneling protocol. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Tunneling\\_protocol](https://en.wikipedia.org/wiki/Tunneling_protocol). [Online; Citované: 31.3.2023].
4. TUN/TAP. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/TUN/TAP>. [Online; Citované: 31.3.2023].
5. Universal TUN/TAP device driver. [B.r.]. Dostupné tiež z: <https://www.kernel.org/doc/Documentation/networking/tuntap.txt>. [Online; Citované: 31.3.2023].
6. DRUTAROVSKÝ, Miloš. Bezpečnosť v architektúre TCP/IP II (BIKS pr7). [B.r.]. [Online; Citované: 6.2.2022].
7. Transport Layer Security. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Transport\\_Layer\\_Security#TLS\\_1.3](https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_1.3). [Online; Citované: 21.5.2021].
8. Multiprotocol Label Switching. [B.r.]. Dostupné tiež z: [https://cs.wikipedia.org/wiki/Multiprotocol\\_Label\\_Switching](https://cs.wikipedia.org/wiki/Multiprotocol_Label_Switching). [Online; Citované: 4.2.2023].
9. Princípy technológie MPLS VPN. [B.r.]. Dostupné tiež z: <https://magazin.kpi.fei.tuke.sk/2020/06/principy-technologie-mpls-vpn/>. [Online; Citované: 4.2.2023].
10. VISWANATHAN, Arun; ROSEN, Eric C.; CALLON, Ross. *Multiprotocol Label Switching Architecture* [RFC 3031]. RFC Editor, 2001. Request for Comments, č. 3031. Dostupné z DOI: 10.17487/RFC3031.

11. COMPUTER SCIENCE UPJS, Institute of. 5. Prednáška - Transportná vrstva: Protokol TCP. [B.r.]. Dostupné tiež z: <https://siete.ics.upjs.sk/prednaska-5/>. [Online; Citované:6.2.2022].
12. S., Sridevi; D.H, Dr.Manjaiah. Technical Overview of Virtual Private Networks (VPNs). *International Journal of Scientific Research*. 2013, roč. 2, č. 7, s. 93–96. Dostupné tiež z: [https://www.worldwidejournals.com/international-journal-of-scientific-research-\(IJSR\)/file.php?val=July\\_2013\\_1372777193\\_d5c86\\_32.pdf](https://www.worldwidejournals.com/international-journal-of-scientific-research-(IJSR)/file.php?val=July_2013_1372777193_d5c86_32.pdf). [Online; Citované: 2.2.2023].
13. ZORN, Glen; PALL, Gurdeep-Singh; HAMZEH, Kory. *Point-to-Point Tunneling Protocol (PPTP)* [RFC 2637]. RFC Editor, 1999. Request for Comments, č. 2637. Dostupné z doi: 10.17487/RFC2637. [Online; Citované: 2.2.2023].
14. Understanding Point-to-Point Tunneling Protocol (PPTP). 1997. Dostupné tiež z: [https://wwwdisc.chimica.unipd.it/luigino.feltre/pubblica/unix/winnt\\_doc/pppt/understanding\\_pptp.html](https://wwwdisc.chimica.unipd.it/luigino.feltre/pubblica/unix/winnt_doc/pppt/understanding_pptp.html). [Online; Citované: 2.2.2023].
15. Challenge-handshake authentication protocol. [B.r.]. Dostupné tiež z: [https://cs.wikipedia.org/wiki/Challenge-handshake\\_authentication\\_protocol](https://cs.wikipedia.org/wiki/Challenge-handshake_authentication_protocol). [Online; Citované: 2.2.2023].
16. MS-CHAP. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/MS-CHAP>. [Online; Citované: 2.2.2023].
17. Password Authentication Protocol. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Password\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Password_Authentication_Protocol). [Online; Citované: 2.2.2023].
18. RC4. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/RC4>. [Online; Citované: 2.2.2023].
19. TOWNSLEY W. Valencia A., Rubens A.; G., Pall; G., Zorn; PALTER, B. *Layer Two Tunneling Protocol "L2TP"* [RFC 2661]. RFC Editor, [b.r.]. Request for Comments, č. 2661. Dostupné z doi: 10.17487/RFC2661. [Online; Citované: 2.2.2023].
20. VALENCIA A., Littlewood M.; KOLAR, T. *Cisco Layer Two Forwarding (Protocol) "L2F"* [RFC 2341]. RFC Editor, [b.r.]. Request for Comments, č. 2341. Dostupné z doi: 10.17487/RFC2341. [Online; Citované: 2.2.2023].
21. Network address translation. [B.r.]. Dostupné tiež z: [https://sk.wikipedia.org/wiki/Network\\_address\\_translation](https://sk.wikipedia.org/wiki/Network_address_translation). [Online; Citované: 4.2.2023].

22. TOWNSLEY, Mark; GOYRET, Ignacio; LAU, Jed. *Layer Two Tunneling Protocol - Version 3 (L2TPv3)* [RFC 3931]. RFC Editor, 2005. Request for Comments, č. 3931. Dostupné z DOI: 10.17487/RFC3931.
23. Layer 2 Tunneling Protocol. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Layer\\_2\\_Tunneling\\_Protocol](https://en.wikipedia.org/wiki/Layer_2_Tunneling_Protocol). [Online; Citované: 4.2.2023].
24. AR500, AR510, AR531, AR550, and AR2500 V200R008 CLI-based Configuration Guide - VPN. [B.r.]. Dostupné tiež z: <https://support.huawei.com/enterprise/en/doc/EDOC1000154777/83e5177f/overview>. [Online; Citované: 4.2.2023].
25. Replay attack. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Replay\\_attack](https://en.wikipedia.org/wiki/Replay_attack). [Online; Citované: 20.2.2023].
26. Advanced Encryption Standard. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard). [Online; Citované: 8.5.2021].
27. RSA (cryptosystem). [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/RSA\\_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem)). [Online; Citované: 20.2.2023].
28. Diffie–Hellman key exchange. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman\\_key\\_exchange](https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange). [Online; Citované: 20.2.2023].
29. Elliptic Curve Digital Signature Algorithm. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Elliptic\\_Curve\\_Digital\\_Signature\\_Algorithm](https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm). [Online; Citované: 20.2.2023].
30. Elliptic-curve Diffie–Hellman. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Elliptic-curve\\_Diffie%E2%80%93Hellman](https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman). [Online; Citované: 20.2.2023].
31. HTTPS. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/HTTPS>. [Online; Citované: 20.2.2023].
32. [MS-SSTP]: Secure Socket Tunneling Protocol (SSTP). [B.r.]. Dostupné tiež z: [https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-sstp/c50ed240-56f3-4309-8e0c-1644898f0ea8](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/c50ed240-56f3-4309-8e0c-1644898f0ea8). [Online; Citované: 20.2.2023].
33. 2.2.3 SSTP Data Packet. [B.r.]. Dostupné tiež z: [https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-sstp/1e71add9-7243-490a-b816-2174d5b3c179](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/1e71add9-7243-490a-b816-2174d5b3c179). [Online; Citované: 20.2.2023].

34. 2.2.2 SSTP Control Packet. [B.r.]. Dostupné tiež z: [https://learn.microsoft.com/en-us/openspecs/windows\\_protocols/ms-sstp/a961ef2b-daeb-4d1e-bf28-45f10c8ba565](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/a961ef2b-daeb-4d1e-bf28-45f10c8ba565). [Online; Citované: 20.2.2023].
35. OpenVPN. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/OpenVPN>. [Online; Citované: 20.2.2023].
36. List of BSD operating systems. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/List\\_of\\_BSD\\_operating\\_systems](https://en.wikipedia.org/wiki/List_of_BSD_operating_systems). [Online; Citované: 20.2.2023].
37. Curve25519. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/Curve25519>. [Online; Citované: 7.3.2023].
38. Elliptic curve cryptography. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Elliptic\\_curve\\_cryptography](https://en.wikipedia.org/wiki/Elliptic_curve_cryptography). [Online; Citované: 7.3.2023].
39. ChaCha Variant. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Salsa20#ChaCha\\_variant](https://en.wikipedia.org/wiki/Salsa20#ChaCha_variant). [Online; Citované: 7.3.2023].
40. Poly1305. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/Poly1305>. [Online; Citované: 7.3.2023].
41. SipHash. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/SipHash>. [Online; Citované: 7.3.2023].
42. BLAKE2. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/BLAKE\\_\(hash\\_function\)#BLAKE2](https://en.wikipedia.org/wiki/BLAKE_(hash_function)#BLAKE2). [Online; Citované: 7.3.2023].
43. WireGuard. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/WireGuard>. [Online; Citované: 20.2.2023].
44. WireGuard. [B.r.]. Dostupné tiež z: <https://www.wireguard.com/papers/wireguard.pdf>. [Online; Citované: 20.2.2023].
45. SRIDEVI, Sridevi; D H, Manjaiah. Technical Overview of Virtual Private Networks(VPNs). *International Journal of Scientific Research*. 2012, roč. 2, s. 93–96. Dostupné z doi: 10.15373/22778179/JULY2013/32. [Online; Citované: 22.1.2022].
46. Virtual Private Networks Simplified. [B.r.]. Dostupné tiež z: [https://www.cisco.com/c/dam/en\\_us/training-events/le21/le34/downloads/689/academy/2008/sessions/BRK-134T\\_VPNs\\_Simplified.pdf](https://www.cisco.com/c/dam/en_us/training-events/le21/le34/downloads/689/academy/2008/sessions/BRK-134T_VPNs_Simplified.pdf). [Online; Citované: 26.1.2022].
47. LEVICKÝ, Dušan. *Kryptografia v informačnej bezpečnosti*. Elfa, 2005.

48. PAAR, Christof; POSCHMANN, Axel; SCHMIDT, Markus D. Efficient hardware implementation of the advanced encryption standard (AES). 2005, s. 319–333.
49. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *Xoodyak*. Team Keccak, 2020. Dostupné tiež z: <https://keccak.team/xoodyak.html>. [Online; Citované:6.2.2022].
50. BASSHAM, Lawrence; ÇALIK, Çağdaş; MCKAY, Kerry; TURAN, Meltem Sönmez. Submission requirements and evaluation criteria for the lightweight cryptography standardization process. *US National Institute of Standards and Technology*. 2018. Dostupné tiež z: <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/final-lwc-submission-requirements-august2018.pdf>. [Online; Citované: 20.2.2023].
51. KATAGI, Masanobu; MORIAI, Shiho et al. Lightweight cryptography for the internet of things. *sony corporation*. 2008, roč. 2008, s. 7–10. Dostupné tiež z: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9595b5b8db9777d5795625886418d38864f78bb3>. [Online; Citované: 20.2.2023].
52. Cryptographic primitive. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Cryptographic\\_primitive](https://en.wikipedia.org/wiki/Cryptographic_primitive). [Online; Citované: 20.3.2023].
53. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *The Keccak-p Permutations*. Team Keccak, 2020. Dostupné tiež z: <https://keccak.team/specifications.html>. [Online; Citované:6.2.2022].
54. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *Kravatte*. Team Keccak, 2020. Dostupné tiež z: <https://keccak.team/kravatte.html>. [Online; Citované:6.2.2022].
55. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *The Keccak-p Permutations*. Team Keccak, 2020. Dostupné tiež z: <https://keccak.team/keccakp.html>. [Online; Citované:6.2.2022].
56. BERNSTEIN, Daniel J; KÖLBL, Stefan; LUCKS, Stefan; MASSOLINO, Pedro Maat Costa; MENDEL, Florian; NAWAZ, Kashif; SCHNEIDER, Tobias; SCHWABE, Peter; STANDAERT, François-Xavier; TODO, Yosuke et al. Gimli: a cross-platform permutation. In: *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2017, s. 299–320.



57. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *Farfalle: parallel permutation-based cryptography*. Team Keccak, 2020. Dostupné tiež z: <https://keccak.team/farfalle.html>. [Online; Citované:6.2.2022].
58. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *The sponge and duplex constructions*. Team Keccak, 2020. Dostupné tiež z: [https://keccak.team/sponge\\_duplex.html](https://keccak.team/sponge_duplex.html). [Online; Citované:6.2.2022].
59. JOAN DAEMEN Seth Hoffert, Gilles Van Assche; KEER, Ronny Van. The design of Xoodoo and Xoofff. 2018, roč. 2018. Dostupné z doi: 10.13154/tosc.v2018.i4.1-38. [Online; Citované:6.2.2022].
60. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *Xoodoo cookbook*. Team Keccak, 2020. Dostupné tiež z: <https://eprint.iacr.org/2018/767.pdf>. [Online; Citované:6.2.2022].
61. DAEMEN, Joan; HOFFERT, Seth; PEETERS, Michaël; ASSCHE, Gilles Van; KEER, Ronny Van. *Xoodoo cookbook (2.revision)* [Cryptology ePrint Archive, Report 2018/767]. 2019. Dostupné tiež z: <https://eprint.iacr.org/2018/767.pdf>. [Online; Citované:6.2.2022].
62. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *Xoodyak, an update*. Publication to NIST Lightweight Cryptography Standardization Process (round ..., 2020. Dostupné tiež z: <https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/status-update-sep2020/Xoodyak-update.pdf>. [Online; Citované:6.2.2022].
63. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *Xoodyak*. Publication to NIST Lightweight Cryptography Standardization Process, 2020. Dostupné tiež z: <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Xoodyak-spec.pdf>. [Online; Citované:6.2.2022].
64. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *The Keyak authenticated encryption scheme*. Team Keccak, 2020. Dostupné tiež z: <https://keccak.team/keyak.html>. [Online; Citované:6.2.2022].

65. What is a ratchet? [B.r.]. Dostupné tiež z: <https://crypto.stackexchange.com/questions/39762/what-is-a-ratchet>. [Online; Citované: 1.1.2023].
66. Forward secrecy. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Forward\\_secrecy](https://en.wikipedia.org/wiki/Forward_secrecy). [Online; Citované: 1.1.2023].
67. DAEMEN, Joan; HOFFERT, Seth; MELLA, Silvia; PEETERS, Michaël; VAN ASSCHE, Gilles; VAN KEER, Ronny. *Xoodyak, a lightweight cryptographic scheme*. Publication to NIST Lightweight Cryptography Standardization Process, 2022. Dostupné tiež z: <https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/xoodyak-spec-final.pdf>. [Online; Citované: 19.3.2023].
68. Security level. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Security\\_level](https://en.wikipedia.org/wiki/Security_level). [Online; Citované: 1.1.2023].
69. Collision resistance. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Collision\\_resistance](https://en.wikipedia.org/wiki/Collision_resistance). [Online; Citované: 20.3.2023].
70. Preimage attack. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Preimage\\_attack](https://en.wikipedia.org/wiki/Preimage_attack). [Online; Citované: 20.3.2023].
71. What is a multi-target attack? [B.r.]. Dostupné tiež z: <https://crypto.stackexchange.com/questions/75880/what-is-a-multi-target-attack>. [Online; Citované: 20.3.2023].
72. Power analysis. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Power\\_analysis](https://en.wikipedia.org/wiki/Power_analysis). [Online; Citované: 20.3.2023].
73. Oracle VM Virtual Box. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/VirtualBox>. [Online; Citované: 20.1.2022].
74. MIKETHETECH. Installing Windows 10 on Virtualbox 6.1.12 – FULL PROCESS, 2020 – video tutorial. 2020. Dostupné tiež z: [https://www.youtube.com/watch?v=gKQvaPejxpc&ab\\_channel=MikeTheTech](https://www.youtube.com/watch?v=gKQvaPejxpc&ab_channel=MikeTheTech). [Online; Citované: 17.5.2021].
75. ORACLE. 6.2. Introduction to Networking Modes. [B.r.]. Dostupné tiež z: <https://www.virtualbox.org/manual/ch06.html>. [Online; Citované: 26.1.2022].
76. BOSE, Michael. VirtualBox Network Settings: Complete Guide. 2019. Dostupné tiež z: <https://www.nakivo.com/blog/virtualbox-network-setting-guide/>. [Online; Citované: 26.1.2022].
77. WIKIPEDIA. Transmission Control Protocol. [B.r.]. Dostupné tiež z: [https://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol). [Online; Citované: 26.1.2022].

- 
78. NIST LIGHTWEIGHT CRYPTOGRAPHY STANDARDIZATION PROCESS, Publication to. Gimli 2019-03-29. [B.r.]. Dostupné tiež z: <https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/gimli-spec.pdf>. [Online; Citované:6.2.2022].
  79. SHAY GUERON, Nicky Mouha. Simpira v2: A Family of Efficient Permutations Using the AES Round Function. [B.r.]. Dostupné tiež z: <https://hal.inria.fr/hal-01403414/document>. [Online; Citované:6.2.2022].
  80. ORG., GNU. GNU Make Manual. [B.r.]. Dostupné tiež z: [https://www.gnu.org/software/make/manual/html\\_node/index.html](https://www.gnu.org/software/make/manual/html_node/index.html). [Online; Citované:20.2.2022].
  81. WIKIPEDIA. Endianita. [B.r.]. Dostupné tiež z: <https://sk.wikipedia.org/wiki/Endianita>. [Online; Citované:20.2.2022].
  82. FREECODECAMP.ORG. Ternary Operator in C Explained. [B.r.]. Dostupné tiež z: <https://www.freecodecamp.org/news/c-ternary-operator/>. [Online; Citované:20.2.2022].
  83. MAN7ORG. Poll. [B.r.]. Dostupné tiež z: <https://man7.org/linux/man-pages/man2/poll.2.html>. [Online; Citované:20.2.2022].
  84. Bufferbloat. [B.r.]. Dostupné tiež z: <https://en.wikipedia.org/wiki/Bufferbloat>. [Online; Citované: 1.3.2021].

# Zoznam príloh

---

**Príloha A** CD médium – vid'. obsah CD média

# A Obsah CD Média

---

Obsah tohto média je dostupný na gite:

- <https://github.com/mr171hg/DiplomaProject>

Použite obrazy, zdrojové kody...