Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Šifrování komunikace v IP sítích

Bakalářská práce

Autor: Daniel Ildža
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Ondřej Hornig

Hradec Králové Duben 2016

Prohlášení:

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

V Hradci Králové dne 25.4.2016 Daniel Ildža

Poděkování:
Chtěl bych vřele poděkovat Ing. Ondřeji Hornigovi za podnětné rady, odborné vedení práce a čas který mi věnoval.

Anotace

Cílem této bakalářské práce je obeznámit s možnostmi zabezpečení komunikace pomocí šifrování v IP sítích a navržení řešení pro zabezpečení datové komunikace v sítích energetické přenosové soustavy Smart Grid.

Práce představuje referenční ISO/OSI model, Smart Grid, různé typy VPN a šifrovací algoritmy. V praktické části je popsán výběr vhodné VPN a určení požadavků na kryptografické metody pro použití k zabezpečení komunikace ve Smart Gridu na základě zákona o kybernetické bezpečnosti. Vzhledem ke zjištěným požadavkům je pak provedeno porovnání šifrovacích metod a je popsán jejich dopad na síťovou komunikaci.

Annotation

Title: Encrypting communication in IP networks

The aim of this bachelor thesis is to present the possibilities of secure communication by encryption in IP networks and design the solution for secure data communication in the networks of power transmission system Smart Grid.

This thesis explains the reference ISO/OSI model, Smart Grid, different types of VPNs and encryption algorithms. Practical part of this thesis describes the selection of the appropriate VPN and requirements for cryptographic methods which can be used to secure communication in Smart Grid under the act on cyber security. On the basis of identified requirements there is a comparison of the encryption methods and is described their impact on network communication.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Síťová komunikace je dnes nejvíce používaným typem komunikace, a to jak v soukromém, tak i firemním prostředí. Je tedy od věci důkladně se zabývat možnostmi zabezpečení takovéto komunikace. Zabezpečení síťové komunikace jako takové patří k jedné z nejdůležitějších oblastí světa informačních technologií. S velkým technologickým rozvojem v tomto odvětví stoupají stále více nároky na bezpečnost. Jednou z nejrozšířenějších možností zabezpečení síťové komunikace jsou virtuální privátní sítě (VPN), které mají širokou škálu využití.

K dnešním velkým fenoménům patří Inteligentní sítě (anglicky Smart Grid), které umožňují vzájemnou komunikaci mezi spotřebiči a distribuční sítí, pomocí které lze regulovat výrobu a spotřebu dle daných potřeb. I zde je na místě řešit otázky bezpečnosti komunikace mezi distributorem a jednotlivými spotřebními jednotkami připojenými do rozvodné sítě.

Těmito oblastmi se v následujících kapitolách tato práce zabývá. Kapitola 2. shrnuje potřebné teoretické znalosti. Nejprve přibližuje ISO/OSI model a na něm ukazuje způsob komunikace v dnešních IP sítích. Poté je představen Smart Grid, jeho principy a prvky společně s důvody pro nutnost řešení jeho bezpečnosti. Zmíněn je též zákon o kybernetické bezpečnosti. Dále jsou popsány VPN a jejich typy společně s jejich vlastnostmi a způsoby řešení bezpečnosti komunikace. Jako poslední jsou uvedeny typy šifrování, principy šifrování a též jednotlivé šifrovací algoritmy nejběžněji používané ve VPN. V kapitole 3. je v první části povedeno určení ideální VPN pro zabezpečení komunikace ve Smart Gridu. S ohledem na zákon o kybernetické bezpečnosti jsou určeny požadavky na kryptografické metody, které budou použity v rámci VPN pro zajištění důvěrnosti, integrity a autentizace. V druhé části této kapitoly je popsán postup konfigurace samotné VPN následovaný porovnáním šifrovacích algoritmů a též to, jak se nasazení VPN projeví na odezvě a propustnosti linky. V kapitole 4. jsou pak zhodnoceny výsledky.

2 Teoretická část

2.1 Komunikace – ISO/OSI model

ISO/OSI model (Open Systems Interconnection Basic Reference Model) byl vytvořen organizací ISO a poté byl v roce 1984 přijat jako mezinárodní norma ISO 7498. ISO/OSI model je abstraktní popis komunikace v počítačových sítích a protokolů použitých pro komunikaci mezi počítači. Model je rozdělen na 7 vrstev. Každá vrstva zpracovává a operuje nad daty svým určitým způsobem, který je odlišný od ostatních vrstev. [1]

Datová jednotka, s kterou jednotlivé vrstvy operují, se nazývá PDU (protokol data unit) a je pro každou vrstvu odlišná. Uplatňuje a používá se zde tzv. princip zapouzdření (encapsulation), pomocí něhož se PDU vyšší vrstvy „zabalí“ do PDU vrstvy nižší, která k ní přidá další informace v hlavičce popř. patičce, v závislosti na dané vrstvě. Hlavičky se mohou lišit v závislosti na použitém protokolu. Tento postup se uplatňuje na straně odesílatele, zde se data zapouzdřují a analogicky se na straně příjemce data „rozbalují“, tedy od vrstvy nejnižší až po vrstvu nejvyšší. [2]

Cílem vytvoření tohoto modelu byla standardizace komunikace hardwaru i softwaru různých výrobců tak, aby byla umožněna vzájemná komunikace. Popis ISO/OSI modelu vznikl před dlouhou dobou a i přesto, že je považován za základ síťových technologií, tak nebyl nikdy zcela přesně realizován.

Obdobou ISO/OSI modelu je TCP/IP model, který vychází z ISO/OSI modelu, ale upravuje jej tak, že je více flexibilní. Podle ISO/OSI modelu je vždy možná komunikace mezi sousedícími vrstvami, a zároveň všechny vrstvy musí být v komunikaci obsaženy, což nám v řadě praktických úloh přináší zbytečnou zátěž (časovou i datovou), např. na routeru je potřeba operovat se třemi nejnižšími vrstvami, jelikož participace vyšších vrstev zde nemá smysl. Přesto je ISO/OSI model dobrý nástroj k vysvětlení a popisu komunikace v sítích. [1]

Obr. 1 ISO/OSI model [1]

2.1.1 Fyzická vrstva

Je tvořena převážně hardwarem. PDU této vrstvy je bit. Jejím úkolem je zakódování jednotlivých bitů tvořící rámce do signálu (elektrického, optického nebo mikrovlnného), a následně je odeslat přes médium, nebo naopak signál přijmout. Kromě samotných dat, která jsou přenášena přes médium, je potřeba také posílat řídící informace. Existují zde dva způsoby jak řídící informace poslat. První způsob je ten, že jsou řídící informace zasílány přes stejný kanál jako ostatní data, tomu se říká in-line signaling, nebo je možno řídící informace posílat přes oddělený kanál, což je označováno jako off-line signaling nebo out-of-line signaling. Použité protokoly fyzické vrstvy závisejí na typu použitého média a způsobu signálování. Fyzická vrstva je tedy určována přenosovým médiem, konektory, způsobem reprezentace bitů na daném médiu a způsobem kódování. [2] Hlavní funkce fyzické vrstvy:

- aktivace a deaktivace spojení, které se provádí, pokud přijde žádost od linkové vrstvy
- přenos bitů ze zdroje k cíli přes médium
- sequencing (pořadí bitů) - zajištění že bity dorazí ve stejném pořadí, v jakém byly odeslány

- management fyzické vrstvy – závislé na protokolu a fyzickém médiu, např. detekce chyb, správa přenosu [2]

2.1.2 Linková vrstva

PDU této vrstvy je rámec (frame). Zajišťuje spojení mezi dvěma uzly a nezávislost na typu média. Komunikace v rámci jednoho subnetu. Skládá se ze dvou podvrstev. První je MAC (Media Access Control), která je implementována hardwarově. Jejím úkolem je řízení příjmu a vysílání signálů médiem, uspořádání přijímaných dat od fyzické vrstvy do rámců, fyzické adresování a kontrola příjemce pomocí MAC adresy (48 bitů). Druhá podvrstva je LLC (Logical Link Control), která identifikuje protokol a zapouzdřuje pakety síťové vrstvy do rámců.
Je implementována softwarově. Funkcemi linkové vrstvy jsou: řízení toku, detekce chyb, zabraňování resp. řešení kolizí (CSMA/CD nebo CSMA/CA), potvrzování rámců a multiplexování. Komunikace může probíhat buď half-duplex, nebo full-duplex. Rámce na linkové vrstvě se mohou mírně lišit podle protokolu. [3]
Zde příklad ethernetového rámce:

7	1	6	6	2	46-1500	4
Preamble	SOF	Destination address	Souce address	Type	Data	FCS

Obr. 2 Ethernet Frame [4]

Vysvětlení jednotlivých polí:

- **Preamble** – synchronizace
- **Destination** – cílová MAC adresa
- **Source** – zdrojová MAC adresa
- **Type** – určuje typ protokolu vyšší vrstvy
- **Data** – samotná přenášená data
- **FCS** – kontrolní součet, správnost dat [4]

Protokoly této vrstvy jsou např. PPP, L2TP, PPTP.

2.1.3 Síťová vrstva

PDU síťové vrstvy je paket. Má na starosti směrování a zprostředkovává komunikaci koncových zařízení (end-to-end komunikaci), k tomu využívá IP adresy hostů (32 bitů nebo 128 bitů), které jsou jedinečné v rámci jedné sítě. Na základě IP adres tak jednoznačně určuje hosta a směruje pakety skrz síť. Od transportní vrstvy přijímá datagram/segment a přidává k němu svou hlavičku, jejíž formát se liší v závislosti na použitém protokolu. [2]
Funkce síťové vrstvy:

- směrování – nalezení nejlepší cesty skrz síť od zdroje k cíli
- segmentace (fragmentace) – důležitá funkce v případě, že data procházejí přes sítě s rozdílnými standardy na linkové vrstvě, z čehož by vyplývaly různé max. velikosti paketů a následná nekompatibilita, nebo pokud je paket prostě moc velký
- detekce chyb – síťová vrstva používá oznamování chyb od linkové vrstvy a může tak zažádat o znovu zaslání
- sekvencování a kontrola toku – zajištění správného pořadí paketů a zajištění nezahlcení cíle
- mapování síťové adresy na linkovou adresu
- zapouzdření – přidání hlavičky [2]

Důležitým pojmem zde je také QoS (Quality of Service). Jde o jakýsi soubor technologií, který řeší problémy okolo traffic managementu. Účelem QoSu je nastavení kvality přenosu při posílání dat přes síť. Je možno rozlišovat mezi jednotlivými typy přenosů, a každému typu pak nastavit jiné hodnoty kvality přenosu. Je možno upřednostnit důležitější síťový provoz před méně důležitým a zajistit tak jeho včasné a správné doručení. [1]
Je možno upravovat následující oblasti:

- zpoždění
- jitter - variace zpoždění
- ztrátovost

- doručení mimo pořadí
- šířka pásma [1]

Nejpoužívanějšími protokoly jsou IPv4 resp. IPv6, ARP, ICMP, atd. [1]

2.1.3.1 IPv4 protokol

IP protokol verze 4 byl standardizován roku 1981. Jeho kompletní popis je v dokumentu RFC 791. Poskytuje základní komunikační mechanizmus v Internetu a používá 32bitové IP adresy. Je nespolehlivý a nespojový tudíž nedokáže garantovat doručení, ovšem má velmi nízkou režii. Řízení přenosu a potvrzování je ponecháno na protokolu TCP. Tento protokol postrádá jakýkoliv mechanizmus zabezpečení a odchycení paketů je velmi jednoduché, proto existují rozšíření či doplňky tohoto protokolu, který tento problém řeší. [5]
Protokol implementuje tři základní funkce:

- adresování
- směrování
- fragmentaci [5]

IPv4 hlavička:

<table>
<tr><th>bity</th><th>0-3</th><th>4-7</th><th>8-15</th><th>16-18</th><th>19-31</th></tr>
<tr><td>0</td><td>Version</td><td>IHL</td><td>Type of Service</td><td colspan="2">Total lenght</td></tr>
<tr><td>32</td><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td>64</td><td colspan="2">Time to live</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td>96</td><td colspan="5">Source address</td></tr>
<tr><td>128</td><td colspan="5">Destination address</td></tr>
<tr><td>160</td><td colspan="4">Options</td><td>Padding</td></tr>
</table>

Obr. 3 IPv4 header [4]

Vysvětlení jednotlivých polí IPv4 hlavičky:

- **Version** – verze protokolu
- **IHL** – délka hlavičky
- **Type of Service** – priorita paketu
- **Total lenght** – celková velikost paketu
- **Identification** – pro identifikaci při fragmentaci
- **Flags** – pole využívané při fragmentaci, obsahuje bity 0, DF,MF DF – nastaven na 1 -> fragmentace zakázána MF – nastaven na 1 -> fragmentace povolena a následují další fragmenty
- **Fragment Offset** – označuje polohu fragmentu v původním paketu před fragmentací
- **Time to live** – omezení nekonečného putování v síti, každý hop sníží hodnotu o 1 a pokud je TTL na 0 a paket je zahozen
- **Protocol** – označuje protokol vyšší vrstvy, v našem případě transportní
- **Header Checksum** – kontrolní součet hlavičky paketu
- **Source Address** – zdrojová IP adresa
- **Destination Address** – cílová IP adresa
- **Padding** – výplň [5]

2.1.3.2 IPv6 protokol

Kompletní popis IPv6 protokolu je uveden v dokumentu RFC 2460. Jelikož adresní rozpětí 32 bitů u protokolu IPv4 je nedostačující, vznikl IPv6 protokol. Ovšem nejen z tohoto důvodu. Základním rozdílem oproti IPv4 je tedy adresní prostor, kde IPv6 používá 128bitové adresy. Zvětšení na 128 bitů ovšem bylo nejen z důvodu zvětšení adresového prostoru, ale také tak aby byl možno jej dělit do směrovacích hierarchických domén, které odrážejí topologii moderního internetu. Umožňuje tak flexibilitu při navrhování hierarchických řešení, které v současnosti IPv4 postrádá. Standardizované schéma pro subneting je v IPv6 64 bitů pro síťový prefix a 64 bitů pro identifikaci hosta. [5]

IPv6 má v sobě integrovaný IPsec pro šifrování a autentizaci (podrobněji v kapitole IPsec), který se ovšem u IPv6 moc často nepoužívá, a dále podporu mobilních

připojení (MIPv6). Samotná adresa se skládá z 8 bloků po 4 hexadecimálních číslech. Existují zde 3 typy adres, a to unicast, anycast a mulicast. U paketu byla snaha, aby hlavička byla co možná nejmenší. Její velikost je pevně 40 bitů, tím pádem již paket tento údaj neobsahuje. [6]

IPv6 hlavička:

<table>
<tr><th>bity</th><th>0-3</th><th>4-11</th><th>12-15</th><th>16-23</th><th>24-31</th></tr>
<tr><td>0</td><td>Version</td><td>Traffic class</td><td colspan="3">Flow label</td></tr>
<tr><td>32</td><td colspan="3">Payload lenght</td><td>Next header</td><td>Hop limit</td></tr>
<tr><td>64</td><td colspan="5" rowspan="4">Source address</td></tr>
<tr><td>96</td></tr>
<tr><td>128</td></tr>
<tr><td>160</td></tr>
<tr><td>192</td><td colspan="5" rowspan="4">Destination address</td></tr>
<tr><td>224</td></tr>
<tr><td>256</td></tr>
<tr><td>288</td></tr>
</table>

Obr. 4 IPv6 header [6]

Vysvětlení jednotlivých polí hlavičky IPv6 protokolu:

- **Version –** verze protokolu
- **Traffic class –** úroveň priority (QoS)
- **Flow label –** pro správu QoS; označení paketu, pokud je s ním potřeba speciálně zacházet
- **Payload lenght** – velikost dat; maximální velikost je 64 kB, pokud, se nastaví na 0, pak se jedná o jumbo pakety o velikosti až 4 GB
- **Next header –** identifikace typu hlavičky, která následuje IPv6 hlavičku; typ informace může být buď vyšší protokol (TCP/UDP), nebo jedna z 6 rozšiřujících hlaviček. V případě rozšiřující hlavičky za normální hlavičkou následuje jedna, nebo víc hlaviček se speciálními údaji. Např. směrování (seznam uzlů) a fragmentace.
- **Hop limit –** obdoba TTL u IPv4

- **Source address –** zdrojová adresa
- **Destination address –** cílová adresa [6]

2.1.4 Transportní vrstva

Tato vrstva má za úkol dělit datový tok z aplikace na jednotlivé segmenty a segmenty přijaté sestavovat do dat. PDU transportní vrstvy je segment. Transportní vrstva identifikuje komunikaci jednotlivých aplikací na základě portů, a předává je cílové aplikaci. Adresace je tedy řešena pomocí zdrojového a cílového čísla portu, které je 16bitové v rozsahu <0;65535>. Spojením IP adresy uzlu a zdrojového portu vzniká tzv. socket.
Porty se dělí na 3 kategorie:

- well-known ports – jsou číslovány 0-1023, registrovány organizaci IANA a rezervovány standardizovaným (RFC) základním aplikacím. Např. FTP, Telnet, DNS atd.
- registered ports – jsou číslovány 1024-49151, registrovány organizací IANA ovšem nejsou standardizovány (RFC). Jsou to uživatelské porty jak zdrojové tak cílové
- private/dynamic ports – číslovány 49152-65535, nejsou rezervovány ani registrovány a jsou pro volné použití bez restrikcí [3]

Zodpovědnostmi transportní vrstvy jsou:

- segmentace – dělení toku dat od odesílatele na segmenty
- reassembling – zpětně složení dat na straně příjemce
- identifikace aplikace, pro kterou jsou data určena
- multiplexing – umožňuje komunikovat více aplikacím zároveň
- zapouzdření dat – přidání hlavičky [3]

Nejpoužívanějšími protokoly jsou TCP, UDP a na nich založené další protokoly.

2.1.4.1 TCP

Transmition Control Protocol je definován v dokumentu RFC 793. Je to spojový protokol, protože se před odesláním dat navazuje spojení (three way handshake) s cílovou transportní vrstvou a spojení se ukončuje "dohodou". Je též spolehlivý, protože v hlavičce každého segmentu je pořadové číslo a každý segment je poté příjemcem zpětně potvrzován, resp. blok segmentů. Spojovost a spolehlivost protokolu ovšem zvyšuje režii protokolu, protože je potřeba přenést více informací a při zpětném potvrzování segmentů je síť více zatěžována, takže může dojít ke zmenšení propustnosti a zpomalení komunikace. PDU se nazývá segment. Protokoly používající TCP jsou např. HTTP, FTP, SMTP. [3]

2.1.4.2 UDP

User Diagram Protokol je definován v dokumentu RFC 768. Je to nespolehlivý protokol, jelikož se u segmentů nepoužívají pořadová čísla a ani nejsou zpětně potvrzovány. Dochází tak ke ztrátě dat, což protokol neřeší a popř. to nechává na vyšších vrstvách. Též je nespojový, protože se před odesílání nenavazujeme žádné spojení ani ho neukončuje a neřídí. Tento protokol má velmi nízkou režii oproti TCP a to z důvodu, že není třeba přenášet informace navíc a není třeba zpětně potvrzovat segmenty. PDU se někdy nazývá též datagram. Protokoly používající UDP jsou např. DNS, DHCP, VoIP. [3]

2.1.5 Relační vrstva

Relační vrstva nemá své vlastní PDU, pracuje s daty v tvaru, v jakém přijdou, bez jakéhokoliv rozdělení či řetězení. Jejím základním účelem je organizovat a synchronizovat dialogy mezi relačními vrstvami, které probíhají ve stejnou dobu. Základními funkcemi relační vrstvy jsou:

- zahájení a ukončení dialogu – vrstva je zodpovědná za zahájení dialogu mezi entitami a poté i za ukončení dialogu
- token management – tato funkce je spjatá s komunikací half-duplex, kde vrstva kontroluje, jaká strana drží token, který ji opravňuje a dovoluje komunikovat v čase, zatímco druhá strana čeká, resp. naslouchá

- mapování dialogů relační vrstvy na spojení na transportní vrstvě – tato funkce umožňuje relační vrstvě mapovat mezi spojením na transportní vrstvě a dialogy na relační vrstvě a určit co k čemu náleží [2]

2.1.6 Prezentační vrstva

Prezentační vrstva stejně jako relační vrstva nemá své PDU. Tato vrstva, je odpovědná za způsob jakým jsou data prezentovány aplikační vrstvě. Na začátku komunikace se vyjedná forma, jak budou data přenesena tzv. syntaxe. Po vyjednání pak prezentační vrstva poskytne služby jako:

- komprese
- šifrování
- překlad

To, jaká služba bude použita, záleží na aplikační vrstvě. [2]

2.1.7 Aplikační vrstva

Zodpovědností aplikační vrstvy je definování služeb pro koncového uživatele. Aplikační protokoly se liší v závislosti na tom, jaký specifický typ dat chce uživatel přenášet. Aplikační vrstva také definuje QoS pro každou službu, zajišťuje synchronizaci komunikujících aplikací, identifikaci uživatele a přístup.
Hlavními zodpovědnostmi této vrstvy jsou:

- identifikace služby poskytované koncovému uživateli
- definování QoS prametrů
- definování bezpečnostních mechanizmů jako identifikace a autorizace uživatele
- synchronizace komunikujících aplikací [2]

Běžně používanými protokoly této vrstvy jsou: HTTP, FTP, SSH, SMTP, POP3, Telnet. [3]

2.2 Smart Grid

Smart Grid, neboli Inteligentní sítě jsou sítě, které umožňují regulaci výroby a spotřeby elektrické energie v reálném čase. Jde o spojení informačních technologií a elektrické rozvodné sítě. Základním principem je obousměrná komunikace mezi spotřebiči u koncového uživatele a zdroji elektrické energie v distribuční síti. Tento princip umožňuje pružně reagovat na poptávku po energii a přizpůsobit tomu dodávku.

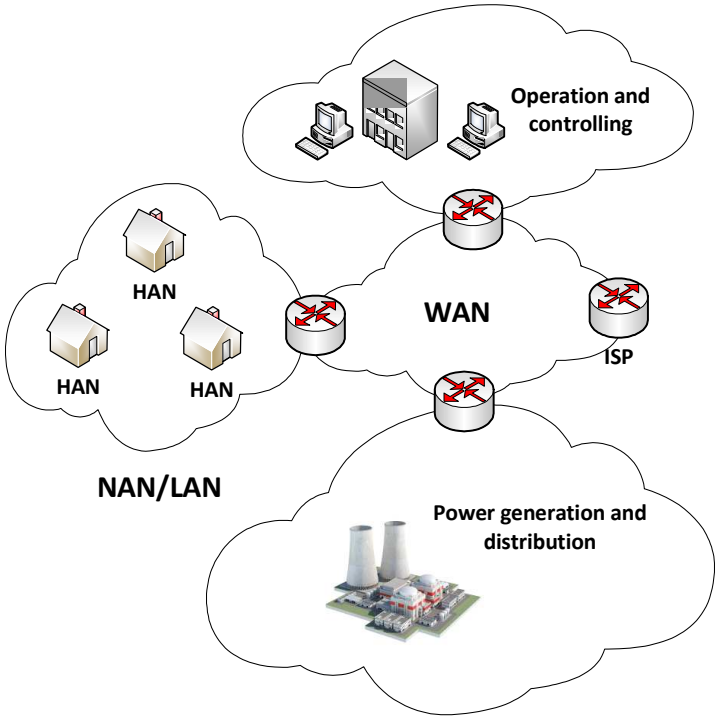
2.2.1 Smysl a funkce

Smart Grid se vyznačuje následujícími charakteristikami. Plnou automatizací, tedy zapojení digitálního a řídicího systému spolu se senzory, pomocí nichž je umožněno monitorování chování sítě, spotřeby, zatížení v reálném čase a kvality dodávek. Dále pak integrací zákazníka, který je vybaven měřidly a zařízeními pro obousměrný tok dat, což umožňuje reagovat na aktuální spotřebu a efektivně využívat elektrické energie při volné výrobní kapacitě. Poslední charakteristikou je adaptace na různé formy výroby elektrické energie. Je umožněno zapojení například větrných a solárních elektráren a dalších výrobních technologií, které jsou decentralizované. Zákazník tak do sítě může dodávat přebytky z vlastní výroby. [7]

2.2.2 Topologie

Nejmenší částí síťové topologie jsou sítě HAN (home area network), které pokrývají např. jednotlivé domácnosti či kanceláře. Součástí těchto sítí mohou být např. chytré pračky, sušičky, větráky. Ty mohou být zapínány, popř. vypínány v závislosti na energetické špičce a přebytcích v energetické síti. Součástí HAN je také tzv. HEMS (home energy smart system), který zákazníkovi umožňuje sledovat spotřebu v reálném čase nebo za určité období. Tento systém komunikuje se smart metrem, který je nainstalován na straně zákazníka. Funguje jako komunikační brána (přístupový bod) pro přenos informací o spotřebě, ceně energie a zprostředkovává řízení chytrých zařízení. Jednotlivé sítě HAN jsou propojeny v síti NAN, která umožňuje datový tok mezi HAN a WAN. Jejím účelem je sběr a tok dat od zákazníků k distributorovi a naopak. Aplikace v NAN sítích mohou

podporovat automatizovanou distribuci, odezvu na poptávku, odečítání ze smart metru, platby, chybovou detekci a komunikaci se zákazníkem. Tento síťový segment se jeví jako kritický vzhledem k různým typům přenášených dat mezi zákazníkem a distributorem. Posledním důležitým segmentem je síť WAN, která agreguje data z jednotlivých NAN sítí. Poskytuje propojení s kontrolním centrem, privátní sítí distributora energie a internetem (možnosti obchodování apod.), funguje tedy jako páteřní síť. [8][9] Níže uvedená ilustrace znázorňuje zjednodušenou síťovou topologii pokrývající nejdůležitější komponenty Smart Gridu z hlediska síťového pojetí.



Obr. 5 - Smart Grid Topologie [14]

V tabulce níže jsou vhodné standardy dle typu sítě:

	Ethernet	WiFi	PLC	ZigBee	DSL	Cellular	WiMax	Optic	Coaxial	Bluetooth
HAN	X	X		X						X
NAN	X	X	X	X	X	X	X		X	
WAN						X	X	X		

Tab. 1 - Standardy pro datovou komunikaci v síťových segmentech [8]

V následující tabulce jsou uvedeny rozsahy rychlosti přenosu pro jednotlivé segmenty v závislosti též na pokryté ploše a rozsah velikosti zasílaných zpráv.

Síť	Rozloha	Přenosová rychlost	Velikost zpráv	Odezva
HAN	1-100 m	1-100 Kbps	10-100 byte	sekundy
NAN	100 m-10 km	100 Kbps-10 Mbps	25 byte-2 Mb	1 ms-dny
WAN	10-100 km	10 Mbps-1 Gbps	4-160 byte	1 ms-2 min

Tab. 2 - Charakteristiky jednotlivých sítí [8]

Nutno podotknout, že veliké rozdíly např. ve velikostech zpráv či odezvě jsou způsobeny různými aplikacemi. Např. aplikace pro meter reading mají typickou velikost v řádu bytů, maximálně kilobytů a vyžadují nižší odezvu <15s. Naopak co se týče updatů firmwaru, velikost dat je pak v řádu megabytů a odezva aplikace v řádu dnů. Velké rozdíly jsou také v tom, jak často jsou data posílána. [8]

2.2.3 SGIRM

Smart Grid Inter-operability model je součástí standardu IEEE 2030, který je jakýmsi průvodcem pro inter-operabilitu (schopnost vzájemné spolupráce různých systémů) v síti Smart Grid. SGIRM metodologie poskytuje porozumění, definici, a vedení při návrhu konkrétních implementací komponent Smart Gridu a koncových aplikací. Klíčem k použití standardu IEEE 2030 je určení jednotlivých rozhraní, datových toků a datových charakteristik pro budoucí Smart Grid. [10] SGIRM řeší problematiku ze tří perspektiv IAP (interoperability architectural perspectives):

- energetické systémy (PS-IAP) – tato perspektiva definuje sedm domén společných pro všechny tři hlavní perspektivy: objem výroby, přenos, distribuci, poskytovatele služeb, trhy, řízení operací a zákazníka

- komunikační technologie (CT-IAP) – definuje konektivitu mezi systémy, zařízeními a aplikacemi. Zahrnuje komunikační sítě, výkon, média a protokoly.
- informační technologie (IT-IAP) – definuje kontrolu procesů a toků dat. Zahrnuje technologie, které ukládají, zpracovávají a řídí zabezpečený informační tok. [10]

SGIRM definuje 81 PS-IAP rozhraní, 71 CT-IAP rozhraní a 35 typů datových toků IT-IAP. Na jednotlivých rozhraních též definuje požadavky na úroveň bezpečnosti z hlediska důvěrnosti, integrity a dostupnosti. Specifikuje též požadované hodnoty odezvy a propustnosti. Jak bylo již uvedeno, kritickým segmentem je rozhraní mezi smart metrem a sítí NAN, tedy spojení zákazníka s distributorem. Z hlediska SGIRM je toto rozhraní označeno jako CT-12. Požadavky na úroveň zabezpečení z hlediska důvěrnosti, integrity, a dostupnosti jsou hodnoceny úrovní H (high), tedy nejvyšší. [10]

2.2.4 Bezpečnost

Zvýšená funkcionalita společně s integrací informačních systémů s sebou nese jeden podstatný aspekt a to je bezpečnost kyber-prostoru, zvláště pokud se tradiční systémy, které jsou často fyzicky izolovány, jsou proprietární a uzavřené začnou vyvíjet směrem k více na sítích závislých s otevřenými IP standardy.
Základní tři aspekty bezpečnosti Smart Gridu (platí i obecně) jsou:

- důvěrnost – zajištění důvěrnosti určitého typu dat, tedy zajištění jejich ochrany před přístupen neautorizované entity. V kontextu samotného automatizovaného systému se jedná o méně kritický aspekt, ovšem z pohledu koncového uživatele se jedná o aspekt kritický.
- integrita – zajištění ochrany dat před modifikací či poškozením neautorizovanou entitou. Jak pro samostatný systém, tak pro koncového uživatele je integrita na stejné úrovni důležitosti.
- dostupnost – zajištění, aby potřebná data byla dostupná v určitý čas. Je to klíčový aspekt pro real-timeové systémy (např. kontrolní centrum). [11]

S výše uvedenými aspekty souvisí i další, který je též nedílnou součástí při návrhu bezpečnostních řešení ve Smart Gridu, a to autentizace a nepopiratelnost. Autentizace zajišťuje to, že komunikační entity jsou opravdu ty, za které se vydávají. Nepopiratelnost (non-repudiation) prokazuje to, že určitou akci provedla určitá entita a je za ní odpovědná. [11]

2.2.4.1 Možné typy útoků

Co se typů útoků týče, mohou být následující. Záměrné zpoždění, blokování nebo pozměnění informací o potřebné dodávce energie což vede ke změně množství vyrobené energie. Zpoždění, blokování nebo pozměnění informací o cenách energií či množství potřebné energie při obchodování. Podvodné informace o poptávce či nabídce, což může způsobit blackouty na straně uživatelů a finanční ztráty na obou stranách. Zasílání podvodných bezpečnostních či varovných zpráv nebo narušení privátnosti informací o uživatelích a jejich aktivitách a následně jejich zneužití. [11]

2.2.4.2 Typy útočníků

Důležité je také zmínit motivy či samotné typy útočníků. Jedním typem mohou být útočníci, kterým nejde o poškození ani způsobení škody ale pouze o překonání překážky, či jednoduše je to pro ně výzva. Dalším typem mohou být ti, které k útoku vede zášť či pomstychtivost vůči druhému zákazníkovi s účelem ho poškodit. V dnešní době pak může jít více než kdy jindy o útočníky z řad teroristických organizací, jejichž cílem může být odstřihnutí uživatelů od energie, nebo způsobení nemalých finančních škod v globálním měřítku. Útočníci mohou být též interní např. zaměstnanci nebo špatně vyškolení zaměstnanci, kteří mohou způsobit chtěné či nechtěné škody svým jednáním. Též pak možným útočníkem může být konkurent v oblasti energetiky snažící se zlepšit svou finanční situaci, či získat konkurenční výhodu a znevýhodnit druhou stranu. [12]

2.2.5 Kybernetický zákon

Smart Grid lze na základě zákona **č. 181/2014 sb. o kybernetické bezpečnosti** pod který spadá nařízení **č. 315/2014 sb. odvětvová kritéria pro určení prvku kritické infrastruktury** zařadit do kritické infrastruktury na základě bodu 1) Energetika a bodu 4) Komunikační a informační systémy.

Dále pak vyhláška **č. 316/2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)** v první části definuje úvodní ustanovení.

Část druhá se věnuje bezpečnostním opatřením. Hlava I druhé části pojednává o organizačních opatřeních. Hlava II druhé části se zabývá technickými opatřeními a mimo jiné definuje kryptografické prostředky (§25) resp. jejich stanovení. Hlava III pojednává o bezpečnostní dokumentaci.

Část třetí definuje kybernetický bezpečnostní incident a jejich kategorie vzhledem k jejich dopadům (§30/31).

Čtvrtá část řeší reaktivní opatření a kontaktní údaje resp. jejich oznamování.

Část pátá pak oznamuje účinnost vyhlášky k datu 1. Ledna 2015.

V příloze **č. 1 k vyhlášce č. 316/2014 sb.** je uveden způsob hodnocení aktiv s důrazem na integritu, důvěrnost a dostupnost pomocí čtyř úrovní (Nízká, Střední, Vysoká, Kritická) a následně popisem jejich ochrany.

V příloze **č. 2 k vyhlášce č. 316/2014 sb.** je uveden způsob pro hodnocení dopadů, hrozeb a zranitelnosti z čehož je pomocí funkce vyjádřena úroveň rizika.

Riziko **=** Dopad **X** Hrozba **X** Zranitelnost

V příloze **č. 3 k vyhlášce č. 316/2014 sb.** jsou stanoveny minimální požadavky na kryptografické metody.

2.3 Zabezpečení síťového provozu pomocí VPN

Jako možné řešení se nabízí VPN, neboli využití virtuální privátní sítě. Tento směr má také ekonomický záměr, protože je ekonomicky výhodnější využít již stávající informační struktury, než nákladně budovat vlastní, a navíc na značně velké vzdálenosti. Virtuální privátní síť, krátce VPN je, řešení jak simulovat privátní síť ve veřejné síti, nebo ji oddělit. Virtuální se nazývá proto, že je založena na virtuálním spojení. Největším impulzem pro rozvoj VPN byl mohutný rozvoj internetu, kde se firmám nabízela možnost levného přenosu dat např. mezi pobočkami, ovšem nutila je celkem zásadně řešit bezpečnost svých dat. [15] VPN podporuje primárně 2 typy komunikace: Remote access (host-to-site) a Site-to-site (intranet-extranet).

VPN protokoly řeší bezpečnost následujícími způsoby: autentizací, zachováním integrity dat, anti-replay službami a šifrováním. [16]

2.3.1 VPN protokoly a tunelování

Nejčastější typy protokolů ve VPN jsou tunelovací a šifrovací protokoly. Tunelovací protokoly se používají pro vybudování tunelu mezi dvěma body, mezi kterými chceme přenášet data a šifrovací protokoly pak následně k zašifrování těchto dat. Tunelování je tedy metodou využívanou při budování virtuálních sítí. Je to metoda, při které je specifická část síťové komunikace přenášena po síti speciálně vytvořeným tunelem. Příkladem je nejběžnější typ tunelování mezi zdrojovým a cílovým routerem, a to GRE (Generic Routing Encapsulation). [18] Tunely GRE jsou budovány mezi směrovači páteřní sítě, a jsou vstupními a výstupními body do této páteřní sítě pro jednotlivé části VPN. Paketům putujícím tunelem je přidána hlavička (GRE header) a cílová adresa odpovídající směrovači, který se nachází na konci tunelu. Jde v podstatě o zapouzdření paketu do jiného paketu. Takto zabalený paket poté, co dojde na cílový router je rozbalen (odebrání hlavičky) a pokračuje ke svému cíli podle informací ve své původní IP hlavičce. Ovšem GRE je už dosti starý a využitelný spíše jen pro zapouzdření pokud nepotřebujme řešit bezpečnost. [17]

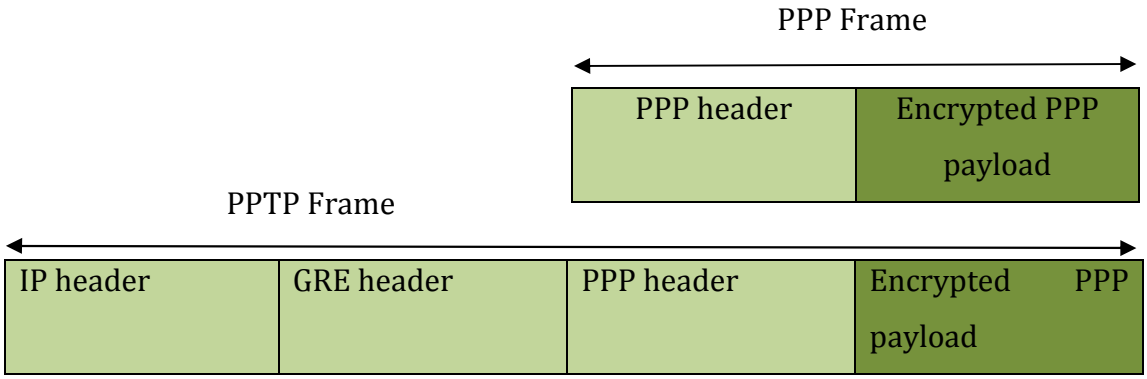
2.3.1.1 PPTP protokol

Point-to-point protokol je rozšířením protokolu PPP. Podrobný popis je v dokumentu RFC 2637. Protokol by vyvinut v rámci konsorcia Accend Communications, Microsoft Corporation, Copper Mountain Networks, 3COM, US Robotics, a několika dalších. PPP protokol poskytuje full-duplex komunikaci mezi dvěma peery, a podporuje širokou škálu spojení mezi routery, bridgy a hosty. PPP protokol před odesláním dat ověřuje uživatele, dále podporuje multiplexing různých protokolů na jedné lince, což umožňuje kompatibilitu mezi dodavatelem a podpůrnými aplikacemi a protokoly. PPTP protokol následně popisuje a řeší jak zabezpečit PPP linku, přes TCP/IP spojení. PPTP umožňuje tunelování PPP skrz síť a zároveň jej nijak nemění. [16]

Velká síla tohoto protokolu je v tom že podporuje non IP protokoly, ovšem nevýhodou je lze vytvořit v rámci dvou bodů jen jeden tunel, a také to, že pokud dva produkty vyhovující PPTP specifikaci šifrují data různým způsobem, stanou se nekompatibilními. [18]

PPTP používá vylepšený GRE tunneling k poskytnutí kontroly toku a zahlcení na lince. PPTP zapouzdřuje již šifrovaný PPP rámec.

Zapouzdření PPP protokolu do PPTP:



Obr. 6 PPTP encapsulation [21]

PPTP podporuje PAP (password authentication protocol) a CHAP (challenge handshake authentication protocol).

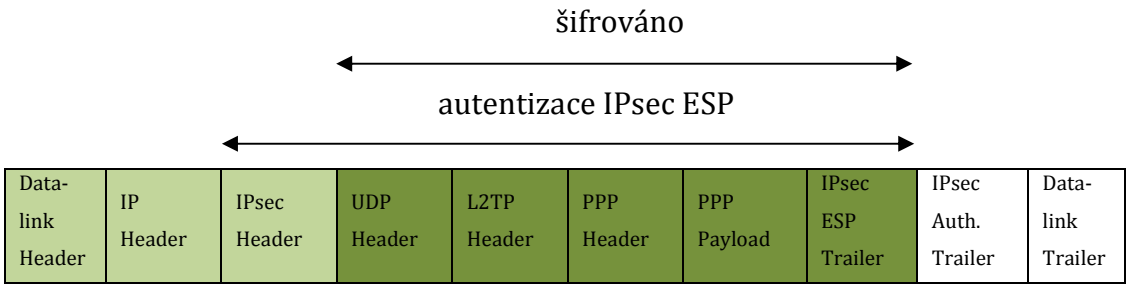
- **PAP** – jednoduchá metoda pro navázání spojení (two-way handshake), jedná se o slabou metodu, jelikož je heslo odesíláno v plain textu a není zde žádná ochrana proti opakování a přehrávání paketů.
- **CHAP** – protokol pro autentizaci, používá se three-way handshake metoda pro navázání spojení (zasílá se zde challenge message), CHAP protokol obsahuje ochranu před opakováním a přehráváním paketů
- **MS-CHAPv1, MS-CHAPv2** – jedná se o postupně vylepšované verze CHAP od Microsoftu [16]

Pro šifrování PPP rámce se používá MPPE (Microsoft point-to-point encryption) v průběhu MS-CHAP. PPTP protokol je navržen tak, aby používal vlastní šifrovací algoritmy, s možností vyjednávání vlastních klíčů. Ovšem, používají se zde obecně známé algoritmy jako DES, 3DES , RC-4.[16]
Nejslabším místem protokolu je autentizace, a také to, že mezi verzemi MS-CHAPv1 a MS-CHAPv2 existuje zpětná kompatibilita. Z prací Jochena Eisingera [20] a Bruce Schneinera [19] vyplívá doporučení nepoužívat PPTP protokol tam, kde je bezpečnost citlivých dat primárním cílem, jelikož se PPTP nejeví jako dostatečně zabezpečený.

2.3.1.2 L2TP protokol

Layer Two Tunneling Protocol vznikl kombinací protokolů PPTP a L2F (Cisco) a spojením toho nejlepšího co nabízejí. Kompletní popis protokolu je v dokumentu RFC 2661 a dále pak s rozšířeními v RFC 3193 a RFC 3931. Protokol pracuje na 2. síťové vrstvě. L2TP zapouzdřuje PPP rámce tak, že mohou být posílány přes sítě IP, X. 25, ATM nebo Frame Relay. Protokol používá UDP zprávy při komunikaci skrz IP sítě jak pro správu tunelu, tak i pro tunelovaná data. Princip L2TP je jednoduchý, koncové zařízení naváže PPP spojení se serverem LAC (L2TP Access Concenrator), následně pak LAC naváže IP tunelové spojení se zařízením, s kterým chce komunikovat koncové zařízení, to se nazývá LNS, na kterém se provádí autorizace a autentizace. [23]

Samotný protokol neumožňuje šifrování dat ani autentizaci, a proto je využíván pouze k vytvoření tunelu, o šifrování a autentizaci se postará jiný protokol nejčastěji IPsec. V tomto případě se pak jedná o L2TP over IPsec. [18]
Struktura paketu L2TP zabezpečeném IPsec:



Obr. 7 L2TP over IPsec [22]

Autentizace, která probíhá při vytváření tunelu, musí používat stejný mechanismus jako PPP spojení, tudíž PAP, CHAP, MS-CHAP atd. [22]
Formát hlavičky L2TP protokolu:

0	1	2	3	4	5	6	7	8	9	0	1	12-15	16-31
T	L	x	x	S	x	O	P	x	x	x	x	Ver	Lenght
Tunel ID													Session ID
NS (Optional)													NR (Optional)
Offset Size													Offset Padding (Optional)

Obr. 8 L2TP header [23]

Vysvětlení jednotlivých polí L2TP hlavičky:

- **T** – typ zprávy; 0 – datová zpráva, 1- kontrolní zpráva.
- **L** - přítomnost pole Lenght, které určuje celkovou délku; 1 – pro kontrolní zprávu
- **x** – pro budoucí rozšíření, jsou nastaveny na 0 a ignorovány
- **S** – pokud je nastavena 1, značí to přítomnost polí NS a NR. Pro kontrolní zprávu musí být nastavena 1
- **O (Offset)** – pokud je nastavena 1, značí to přítomnost pole Offset Size. Pro kontrolní zprávy musí být nastavena 0

- **P (Priority)**- pokud je nastavena 1, datová zpráva má vyšší prioritu v sekvenčním zpracování a přenosu
- **Ver** – verze protokolu, hodnota 1 je určena pro zachytávání L2F paketů
- **Lenght** – celková délka zprávy i s hlavičkou
- **Tunel ID** – identifikátor tunelu
- **Session ID** – identifikátor uživatelského spojení
- **NS** – indikuje sekvenční číslo, které je očekáváno v další kontrolní či datové zprávě
- **NR** - indikuje sekvenční číslo, které je očekáváno v další kontrolní zprávě
- **Offset Size and Padding** - specifikuje počet oktetů následujících po L2TP hlavičce, kde je očekáván začátek dat. Samotná data uvnitř Offset Padding nejsou definována. Jestliže je přítomno pole Offset, L2TP hlavička končí za posledním oktetem Offset Padding. [23]

Nejaktuálnější verzí je nyní L2TPv3. [24]

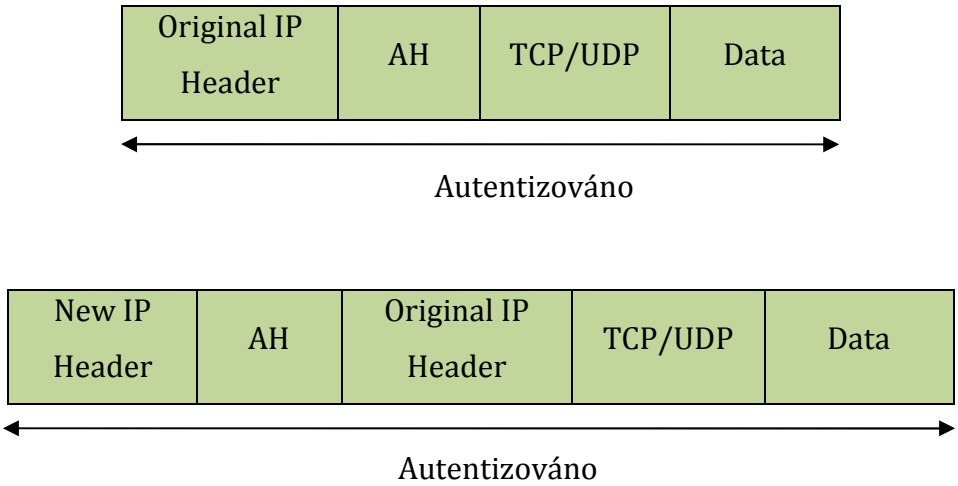
2.3.1.3 IPsec

IPsec, neboli Internet Protocol Security je standardizovaná sada protokolů umožňující zabezpečení IP komunikace mezi dvěma koncovými systémy, vytvářet šifrované tunely, a to jak mezi dvěma routery, tak i mezi hostem a routerem (tzv. Site-to-site a Remote access), vznik je datován do roku 1995. Doplňuje IPv4 protokol, jelikož pracuje na 3. vrstvě ISO/OSI modelu, tedy na vrstvě síťové. Popis protokolu je uveden v dokumentu RFC 6071. Umožňuje autentizaci, vyjednávání kryptografických metod, šifrování v komunikaci. IPsec v zásadě neurčuje to, jaké algoritmy používat, ale pouze definuje vyjednávací mechanizmy. Je tedy možno v rámci IPsec používat velké množství standardních protokolů a algoritmů. [25]
IPsec je možno provozovat ve dvou módech, první je tunelovací a druhý transportní. V tunelovacím módu se šifruje celý paket včetně hlavičky a doplňuje se nová hlavička. V transportním módu, se zašifrují pouze přenášená data, IP hlavička se ponechá a přidá se IPsec hlavička. [26]
V IPsec můžeme najít 3 hlavní protokoly, a to AH, ESP a AS. [25]

AH protokol

Authentication Header zabezpečuje integritu přenášených paketů (pomocí hashe), autentizaci odesílatele a ochranu proti replay-útokům. Neumožňuje žádné šifrování. [26]

Formát datagramu v transportním a tunelovacím módu:



Obr. 9 AH v transportním a tunelovacím módu [23]

Formát hlavičky AH protokolu:

0-7	8-15	16-31
Next Header	Payload Lenght	Reserved
Sequence Parameters Index (SPI)		
Sequence Number Field		
Authentication Data (Variable)		

Obr. 10 AH header [23]

Vysvětlení jednotlivých polí hlavičky AH protokolu:

- **Next Header** – číslo specifikující typ zabezpečených dat, tedy číslo vnořeného protokolu
- **Payload Lenght** – délka záhlaví, měřeno v násobcích 4 bajtů minus 2
- **SPI** – index pravidla určující použitý typ komunikace, autentizaci

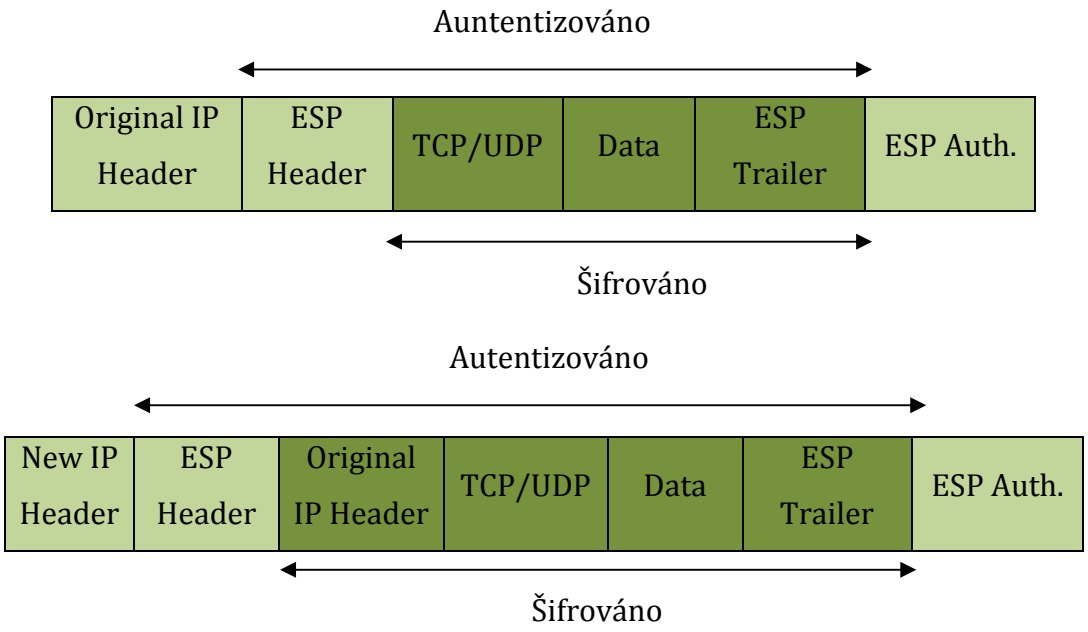
- **Sequence Number Field** – pořadové číslo paketu, ochrana před opakováním paketů, číslováno od 1
- **Authentication Data** – kontrolní součet přenášených dat [26]

V AH se používá HMAC (Hashed Message Authentication Code), pro zajištění integrity hashovací funkce MD5 nebo SHA a pro autentizaci RSA nebo PSK (pre-shared key).

ESP protokol

Encapsulating Security Payload zabezpečuje šifrování dat, je možná také autentizace a zajištění integrity dat, což je závislé na tom, zda se obě strany dohodnou na použití authentication pole. ESP může být použit samostatně, nebo společně v kombinaci s AH. [26]

Formát paketu v transportním a tunelovacím módu:



Obr. 11 ESP v transportním a tunelovacím módu [26]

Hlavička protokolu ESP:

0-7	8-15	16-23	24-31
Security Parameters Index (SPI)			
Sequence Number Field			
Payload Data			
Padding			
		Padding Lenght	Next Header
Authentication Data (Variable)			

Obr. 12 ESP header [23]

Vysvětlení jednotlivých polí hlavičky ESP protokolu

- **SPI** – index pravidla určující typ komunikace, autentizaci a šifrování
- **Sequence Number Field** – pořadové číslo paketu, ochrana před opakováním paketů, číslováno od 1
- **Payload Data** – chráněná data původního IP paketu, zahrnuje data pro ochranu
- **Padding** – výplň pro šifrování, tak aby data pasovala do bloku šifry
- **Padding Lenght** – velikost výplně
- **Next Header** – číslo specifikující typ zabezpečených dat, tedy číslo vnořeného protokolu
- **Authentication Data** - kontrolní součet přenášených dat [26]

Pro šifrování a dešifrování zpráv se používají symetrické klíče. V ESP je možno použít např. následující symetrické šifry: 3DES, Blowfish, AES. Integrita je řešena pomocí hashovacích funkcí MD-5 nebo SHA. Autentizace bývá řešena pomocí RSA nebo PSK (pre-shared key).

AS (Security Asociation)

Skupina algoritmů, které poskytnou parametry pro bezpečnou komunikaci pomocí AH a ESP. Používá ISAKMP Framework (Internet Security Association and Key

Management Protocol), který popisuje vzájemnou výměnu dat mezi dvěma komunikujícími stranami. A IKE (Internet Key Exchange), který vyměňuje vlastní kryptografický materiál. [26] IKE je tedy vnořen do ISAKMP. Zajistí se tak vyjednání atributů, které obsahují dobu platnosti klíče, kompresi, zvolený šifrovací algoritmus a způsob zapouzdření. Vyjednávání zde probíhá šifrovaně. [25]

2.3.1.4 OpenVPN

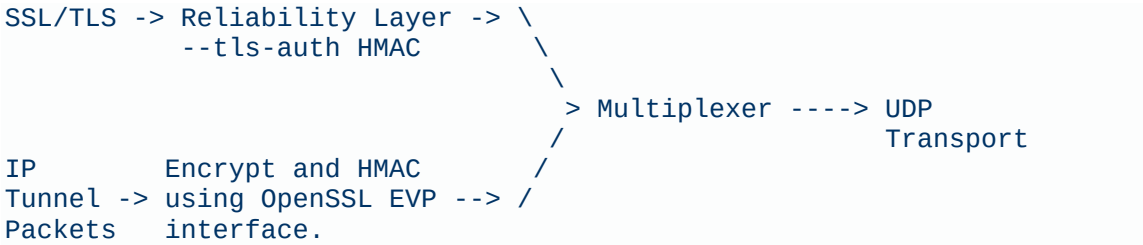
OpenVPN, také nazývána jako SSL-based VPN je open source řešení VPN založené na SSL/TLS protokolu. Jelikož je SSL/TLS navrženo pro spolehlivý transport, tak OpenVPN poskytuje spolehlivou transportní vrstvu přes UDP. Původně bylo vyvinuto Jamesem Yonanem a první verze 0.90 vydána v roce 2001 pod GPL (General Public Licence). Nynější nejnovější verze je již 2. 3. 10.
Zajištění šifrování, autentizace a integrity dat je řešeno využitím HMAC a OpenSSL knihovny společně s virtuálním zařízením TUN a TAP, které je jakými rozhraním mezi softwarem uživatelské úrovně a operačním systémem pro přenos paketů. [27] OpenVPN používá pro komunikaci dva kanály: řídící a datový. Řídící kanál je určen pro výměnu konfiguračních informací, hashovacích algoritmů, šifrovacích klíčů při navazování spojení a jeho udržování (je periodicky obměňován). Datový kanál je určen pro přenos samotných dat. Řídící kanál je šifrován a zabezpečen pomocí SSL/TLS a datový kanál pomocí vlastního šifrovacího protokolu. Komunikace mezi dvěma koncovými body může být uskutečněna dvěma způsoby, a to buď pomocí TCP nebo UDP. Obě tyto možnosti mají své výhody a nevýhody a v posledku záleží na typu komunikace, která je uskutečňována přes VPN tunel a následně pak výběru jedné z možností. [28]
Existují zde 2 autentizační módy:

- **Static Key** – používá předsdílený statický klíč
- **TLS** – používá SSL/TLS + certifikát pro autentizaci a výměnu klíčů

Ve statickém módu je vygenerován předsdílený klíč mezi dvěma peery před vytvořením tunelu. Obsahuje 4 nezávislé klíče HMAC send, HMAC receive, encrypt a decrypt. V TLS módu je použita oboustranná autentizace (každá strana se musí

prezentovat vlastním certifikátem). Následně je pak náhodně vygenerován šifrovací/dešifrovací a HMAC klíč pomocí OpenSSL funkce a vyměněn pomocí SSL/TSL spojení. Poté následuje již samotné zašifrování paketů. [28]

Znázornění výše uvedeného procesu:



Obr. 13 OpenVPN multiplexing [29]

Funguje zde multiplexing SSL/TLS spojení a šifrovanými tunelovanými daty. [29]

OpenVPN podporuje širokou škálu šifrovacích a hashovacích algoritmů. Pro každý kanál je tedy možno nakonfigurovat sadu šifer, které budou použity. Bitová velikost šifry je do 256bitů (např. AES256) a klíče do 512bitů (např. HMAC SHA512). [28] V rámci OpenVPN je možno použít následující šifry: 3DES, AES, Blowfish, Camelia. Co se týče hashovacích funkcí k zajištění integrity, tak jsou k dispozici SHA a MD5.

2.3.1.5 MPLS VPN

MPLS (Multiprotocol Label Switching) je standardizovaná technologie, která urychluje doručování paketů v síti, přes různé protokoly jako je IP, ATM, Frame Relay za pomoci přepínání značek. MPLS odděluje směrování od samostatného doručování. Doručování je řešeno na rozhraní linkové a síťové vrstvy. [30]

Základním principem je to, že existuje síť MPLS provozovaná providerem, a tato síť je využívána klientskými sítěmi pro vzájemnou komunikaci. Router LSR (label switching router) na okraji MPLS sítě, také označovaný jako „ingress“, přidělí příchozímu paketu značku (štítek), která je následně používána pro předávání mezi routery v MPLS síti. Každý LSR router má svou tabulku značek a provádí předávání paketů právě na základě těchto tabulek. Všechny pakety označené stejnou značkou jsou posílány stejnou cestou v síti (LSP – Label Switched Path) až dorazí na druhý koncový router MPLS sítě označovaný také jako „engress“, kde

je mu značka odebrána a paket je poté standardně doručován do svého cíle. Výměna informací o přidělených značkách je mezi routery vyměňovaná pomocí LDP (label distribution protocol) protokolu, který má dnes již řadu dalších rozšíření např.: signalizaci cesty s omezeními nebo explicitní směrování na základě RSVP pro řízení provozu. Oddělení jednotlivých zákazníků využívajících MPLS síť je řešeno pomocí VRF (virtual routing and forwarding). [31] MPLS VPN tedy označuje spojení MPLS a VPN. Jsou zde 2 základní typy: Layer 2 MPLS VPN a Layer 3 MPLS VPN.

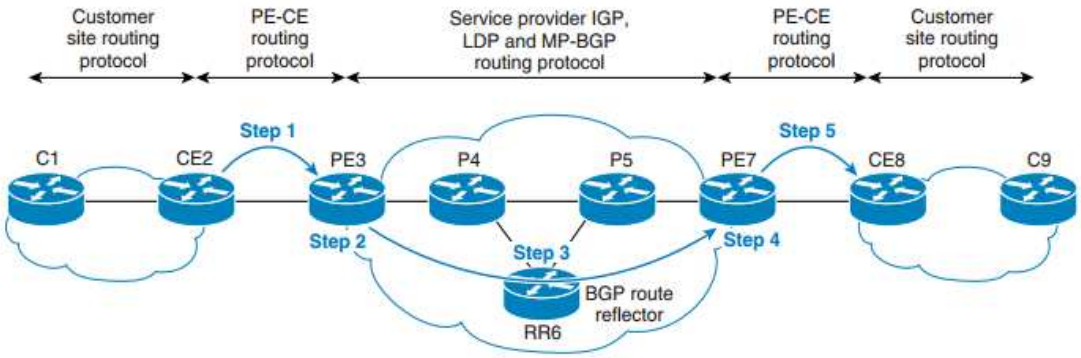
V Layer 2 MPLS VPN je datový tok uskutečňován mezi CE (koncový router/switch zákazníka) a PE (koncový router/switch providera) na linkové vrstvě OSI modelu, poté je tunelován přes MPLS síť providera a na konci znovu převeden zpět na formát linkové vrstvy. Routování a obsluha síťové vrstvy je prováděna na CE, kdežto PE se o routování nestará, zajímá ho pouze linková vrstva. Oba dva switche/routery musí být nakonfigurovány tak aby odeslaly data do správného tunelu. [32]

V Layer 3 MPLS VPN, nebo také BGP/MPLS VPN oproti Layer 2 MPLS VPN již provider řídí routování a zákazník musí sdílet informace o své síti. Zároveň pak musí PE používat BGP protokol aby bylo možno komunikovat s CE, kde mohou být různé routovací protokoly. Toto řešení umožňuje komunikovat pouze pomocí IP protokolu, a proto jiný typ komunikace musí být tunelován.

Komunikace probíhá následovně:

CE odešle paket na PE. PE paket přijme a podívá se do VRF tabulky přiřazené aktuálnímu rozhraní. Následně přiřadí 2 štítky, jeden identifikuje zákazníkovu VPN a druhý je štítek pro tunelování přes MPLS. Následně je paket odeslán přes MPLS síť a na koncovém PE se identifikuje podle štítku VPN, dle VRF se paket pošle na správné rozhraní a je doručen na CE do cílové sítě. [33]

Pro přiblížení je na obrázku níže uveden příklad Layer 3 MPLS VPN:



Obr. 14 Layer 3 MPLS VPN [33]

Co se týče šifrování v MPLS VPN, tak není nijak řešeno a bývá proto využíváno technologie IPsec buď mezi PE-PE nebo CE-CE.

2.4 Šifrování a hash

Šifrování komunikace jako takové je neoddělitelnou součástí při budování VPN, jelikož je třeba mít data oddělena od ostatního provozu a zároveň také zabezpečena tak, aby je případný útočník nemohl zneužít či je poškodit. Vytvoření samotného tunelu totiž mnohdy bezpečnost řešit nemusí, jako tomu je například u L2TP protokolu, který pouze tunel vytváří ovšem o šifrování se stará protokol jiný (IPsec v tomto případě).

Hashovací funkce se používá tam, kde je potřeba ověřit integritu dat. Výstupem takovéto funkce je hash. Jedná se o funkci jednocestnou, která transformuje libovolně dlouhý vstup na výstup konstantní délky, který jednoznačně odpovídá vstupu. Jednocestná funkce značí to, že technicky je výsledek spočten velice snadno a rychle, ovšem zpětně určit z výstupu vstup je prakticky nemožné (zatím). [26] Zde je patrný i rozdíl oproti šifrování, kde je požadováno také to, aby šifrovanou zprávu bylo možno dešifrovat a přečíst. Nejpoužívanější funkce jsou již dříve často zmiňované SHA a MD-5.

2.4.1 Typy šifrování

V počítačových sítích se využívá dvou typů šifrování, symetrického a asymetrického. Rozdíl je zde v použití šifrovacích klíčů. Níže jsou popsány základní charakteristiky obou typů.

2.4.1.1 Symetrické šifrování

Využívá se zde jeden sdílený soukromý klíč jak pro zašifrování tak i dešifrování. Výhodou symetrického šifrování je, že je obecně velice rychlé a lze jej použít efektivně pro velký objem dat. Slabým místem symetrického šifrování je to, že je třeba, aby si dvě komunikující strany klíč bezpečně vyměnily. [34]

$$\text{Šifrovací transformace: } f: M \xrightarrow{k} C$$

$$\text{Dešifrovací transformace: } f^{-1}: C \xrightarrow{k} M \text{ ,}$$

kde M je vstup, k je klíč a C šifrovaný výstup.

Tedy dešifrování zprávy za pomoci klíče k je $D_k(C)=D_k(E_k(M))$. [34]

2.4.1.2 Asymetrické šifrování

Zde se využívají dva klíče, veřejný a soukromý klíč. Veřejný klíč se používá pro zašifrování a soukromý pro dešifrování. Oba tyto klíče jsou na sobě svým způsobem matematicky závislé. Nevýhodou asymetrického šifrování je jeho pomalost a tedy nevhodnost pro velký objem dat. Výhodou pak je to, že není potřeba řešit bezpečnou výměnu klíčů oproti symetrickému šifrování. Pro ověřování pravosti klíče se používají certifikáty. [34] Oproti symetrickému šifrování zde neplatí inverze, neboť k šifrování a dešifrování jsou použity různé klíče. Dešifrování zprávy *Dk(C)≠Dk(Ek(M))*. Soukromý klíč je odvozen z veřejného za pomocí jednocestné funkce:

$$f: pq \rightarrow n,$$

kde p a q jsou prvočísla a n je jejich součin. Jedná se o součin velice vysokých prvočísel, takže rozklad n na činitele je velice obtížný, ne-li nemožný, protože zatím nebyl nalezen žádný algoritmus, který by toto úspěšně řešil. V praxi se používá kombinování obou typů šifrování. Tedy samotná zpráva je šifrována symetricky a náhodný symetrický klíč je poté zašifrován asymetricky. V praxi je nejrozšířenější metoda RSA (Rivest-Shamir-Adleman). [26]

2.4.2 Šifrovací klíč

Šifrovacím klíčem se rozumí informace, která určuje průběh algoritmu při šifrování či dešifrování, tedy to jak je zpráva transformována. Šifrovací klíč má svoji délku, která ovlivňuje jak dobu potřebnou k zašifrování resp. dešifrování, tak také sílu klíče (odolnost) např. při útoku hrubou silou. Délka klíče se uvádí v bitech, běžně používané velikosti klíčů jsou 128 bitů, 192 bitů a 256bitů. [35] Důležitý je také výběr klíče, který by měl být co nejvíce náhodný a měl by být vybrán z co nejvíce možností. Pro samotnou distribuci klíčů je možno použít buď RSA, nebo D-H (Diffie-Hellman) metod.

2.4.3 Typy symetrických šifer

Co se týče symetrických šifer, dělí se na blokové a proudové. Základní rozdíl je v tom, jak pracují s daty. Blokové šifry mají různé módy v závislosti na jejich použití.

2.4.3.1 Blokové šifry

Pracují s bloky dat pevné velikosti. Tedy vstupní data jsou rozdělena do bloků (typicky se používají bloky 64 nebo 128bitové) a tyto bloky jsou každý zvlášť šifrovány pomocí stejného klíče. Nejdůležitějšími parametry blokových šifer je velikost bloku a délka šifrovacího klíče. Blokové šifry mají různé módy, které jsou užitečné, pokud je třeba šifrovat nejen N-bitové bloky, ale také libovolnou bitovou posloupnost, přičemž jsou k dispozici jen pevné N-bitové bloky. Tyto módy jsou v podstatě způsoby jak použít blokové šifry v daném systému. [36]

ECB (electronic codebook) – tento mód umožňuje to, že pokud se šifrují stejné bloky textu, šifruje se vždy na jeden a ten samý šifrovaný blok což umožní použít překladovou tabulku s indexy (codebook). To je ovšem veliká nevýhoda jelikož protože pokud se podaří nalézt více shodných šifrovaných bloků, tak je zřejmé že ukrývají stejný text a v jistém smyslu to může poodkrývat obsah. Útočník také může vyměňovat, vkládat nebo vyjímat bloky. Tato metoda se používá velmi zřídka. [36]

CBC (cipher block chaining) – oproti módu předchozímu zavádí CBC vzájemnou zpětnou závislost bloků na sobě. Tedy tak, že předtím než je blok šifrován, tak je modifikován předchozím blokem, a až poté šifrován. První blok je modifikován náhodnou veličinou IV. Výsledkem je tedy i to, že šifrovaný text by měl být náhodný, a jelikož je text před šifrováním modifikován již náhodným šifrovaným blokem stává se tento text náhodným již před šifrováním. [36]

CFB a OFB (cipher-feedback mode a output-feedback mode) – oba tyto módy převádí šifru na šifru proudovou. Blokovou šifru používají k vygenerování hesla, které se XORuje na plaintext. Používá se zde náhodná inicializační hodnota IV,

pomocí které, se nastaví automat do náhodné polohy a tento automat poté produkuje posloupnost hesla. Automat poté pracuje tak, že heslo, které vznikne (OFB) nebo šifrový text (CFB) směřuje na vstup blokové šifry a po zašifrování vznikne následující blok hesla. Vlastnosti OFB jsou identické s čistou (synchronní) proudovou šifrou. CFB má kombinaci vlastností CBC a proudové šifry. [37]

CTR (counter mode) – principielně podobný OFB, převádí blokovou šifru na synchronní proudovou šifru. Délka periody hesla je dána délkou periody čítače. Využívá se zde také náhodné veličiny IV, po jejímž načtení do čítače a následném zašifrování vzniká první blok hesla. Poté se aktualizuje čítač, nejčastěji se přičítá jednička a začne se generovat další blok hesla. Tento mód nemá samosynchronizaci a tudíž zde na sobě bloky nejsou závislé a výpadek předchozího šifrového textu znamená následné špatné odšifrování textu zbylého. [37]

2.4.3.2 Proudové šifry

Proudová šifra na rozdíl od šifry blokové šifruje zvlášť každý znak plaintextu. Dalo by se říci, že proudové šifry jsou blokové šifry o velikosti bloku 1 bit. Rozdíl oproti blokovým šifrám, které šifrují každý blok pomocí stejné transformace $E_k(D_k)$, kde *k* je šifrovací klíč, je ten, že proudové šifry generují pomocí klíče nejprve nějakou posloupnost *h(1), h(2)*..., a poté je každý znak zpracován pomocí různých transformací v závislosti na různých posloupnostech h, tedy $E_{h(i)}$. Šifrovaný text vzniká sloučením jednotlivých znaků otevřeného textu a hesla. Proudové šifry mohou být dvojího typu, a to synchronní a asynchronní. [38]

U synchronní proudových šifer generované heslo nezávisí na plaintextu, ani na šifrovém textu. Příjemce a odesílatel musí být synchronizováni, jelikož výpadek jednoho znaku šifrového textu při dešifrování naruší veškerý následující otevřený text a dojde k chybnému dešifrování. [38]

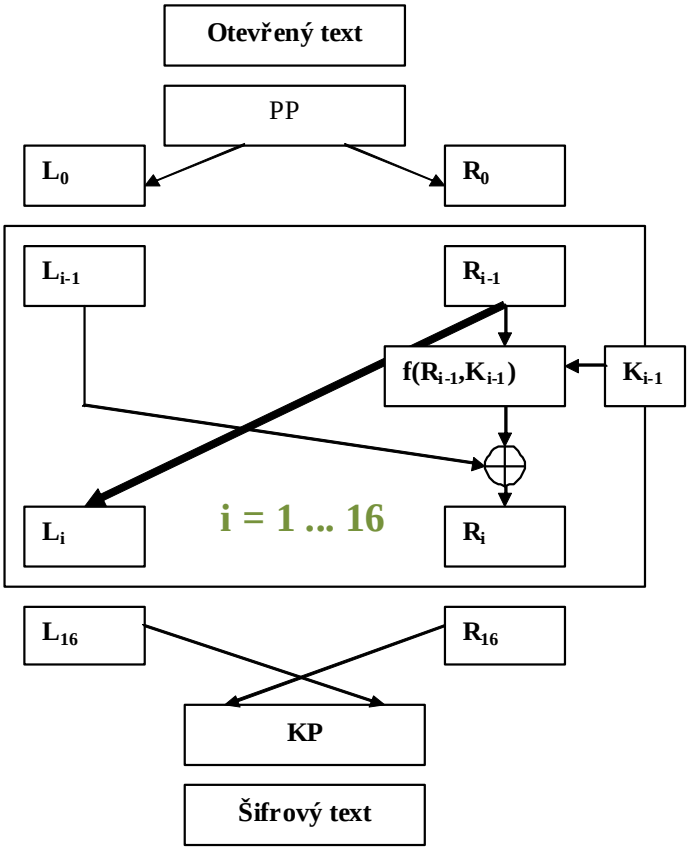
Naopak u šifry proudové asynchronní (samosynchronizující se) se heslo generuje pomocí klíče a *n* předchozích znaků šifrového textu. Tím pádem se výpadek některého znaku šifrového textu projeví celkem na *n* sousledných znacích plaintextu, ale další otevřené znaky budou již správně dešifrovány. [38]

2.4.4 Symetrické šifrovací algoritmy

Pro šifrování zpráv v komunikaci VPN je standardně používáno symetrických šifer, vhledem k jejich rychlosti. Pro výměnu klíčů pak bývá použito šifry asymetrické.
V dalších kapitolách jsou popsány symetrické šifry DES, 3DES, Blowfish, AES a RC-4.

2.4.4.1 DES

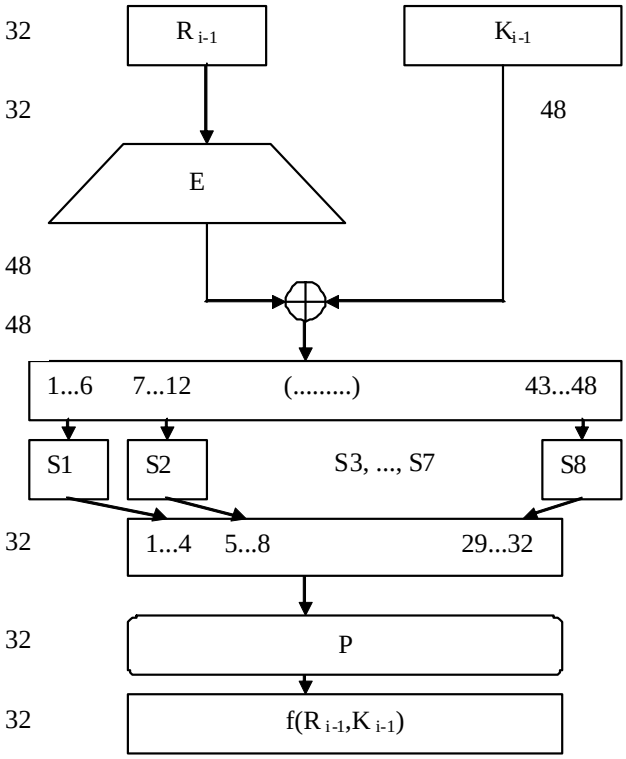
DES neboli Data Encryption Standard je symetrická bloková šifra, jejíž délka bloku je 64 bitů. Klíč má délku 56 bitů. Tento standard byl zveřejněn roku 1977 v USA jako standard po ochranu citlivých dat. DES je šifra používající 16 iterací (rund) $E_{k(16)} * E_{k(15)} *... * E_{k(1)}$. Klíč je při inicializaci a za chodu distribuován na 16 iteračních klíčů *k(16)...k(1)*, které jsou 48bitovými řetězci. Po první, tedy počáteční permutaci (PP) se blok rozdělí na dvě poloviny (L a R) po 32 bitech. Poté se při každé iteraci transformuje L a R na nové L a R v závislosti na různých iteračních klíčích. Po poslední iteraci se aplikuje konečná permutace (KP). [39]



Obr. 15 DES algoritmus [38]

DES je konstruován pro snadnou hardwarovou implementaci, je to tzv. Feistelova šifra, takže šifrování a dešifrování pobíhá stejně, jen je obráceno pořadí iteračních klíčů.

Iterační funkce $f(R_{i-1},K_{i-1})$ probíhá tak, že se načtou iterační klíče na vstup, poté se provede substituce na základě 4bitových znaků a následně se vše transponuje na úrovni bitů. Čímž se zajistí tzv. difůze, která znesnadňuje zkoumání vazby a závislosti mezi otevřeným a šifrovaným textem, a dále konfůze jejímž smyslem je učinit statistické vlastnosti šifrového textu a klíče co nejsložitější. [38]



Obr. 16 DES funkce F [38]

Co se týče zmíněných substitucí, jsou to tzv. S-Boxy, které zajišťují nelinearitu v DES. Pokud by se substituce vynechali, bylo by možné vyjádřit vztahy mezi otevřeným textem, šifrovým textem a klíčem lineárními rovnicemi, což by bylo nežádoucí. V současnosti je DES již nevyhovující kvůli délce svého klíče, který byl prolomen hrubou silou. [38] Nahradil jej jeho nástupce 3DES.

2.4.4.2 3DES

3DES je nástupce již nevyhovujícího DES. Z názvu lze vytušit, že funkcionalita 3DES spočívá v provedení algoritmu DES třikrát po sobě s různými klíči. Jde tedy o umělé prodloužení klíče. Existují tři varianty jak 3DES použít: [38]

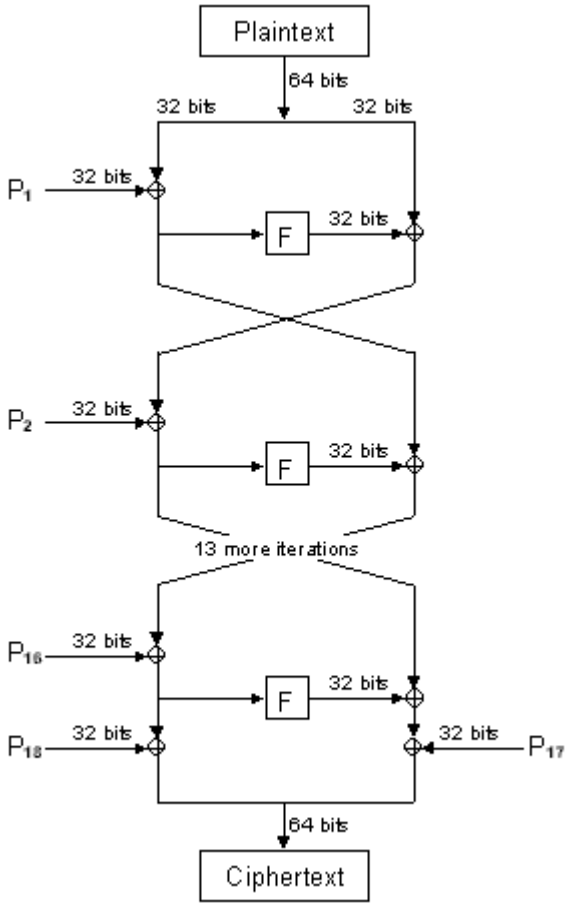
- **3DES-EEE3** – provádí se trojité šifrování se třemi různými klíči, délka klíče je tedy 168 bitů
- **3DES-EDE3** – zde provádí se šifrování, pak dešifrování a poté znovu šifrování pomocí tří různých klíčů
- **3DES-EEE2 a 3DES-EDE2** – tyto dva případy jsou stejné v principu jako předchozí dva, s tím rozdílem že klíč první je stejný jako klíč třetí [40]

Plyne z toho, že 3DES může mít délku klíče buď 112 bitů v případě totožných dvou klíčů, nebo 168 bitů při použití tří různých klíčů. Vzniklý klíč je tak dostatečně dlouhý a garantuje bezpečnost i dnes, ovšem v porovnání se svým nástupcem resp. alternativou AES, je značně pomalý co se týče výpočetní doby (z důvodu trojitého provádění DES). [40]

2.4.4.3 Blowfish

Blowfish je symetrická bloková šifra, jejímž autorem je Bruce Schneier, který ji publikoval roku 1993 jako náhradu za již zastaralý DES a dodnes je stále efektivní i když ji zastiňuje AES. S výhledem do budoucna to ovšem vypadá, že je Blowfish na ústupu. Blowfish je nepatentovaná šifra a je volně dostupná. Velikost bloku je pevných 64 bitů a klíč je možno použít od 48 do 448 bitů. Podobně jako u DES se používá 16 iterací. Princip Blowfish je takový, že vstupní klíč při započetí šifrování je transformován na několik podklíčů v celkové délce 4168 bytů. Je použito 18 *P* polí, z nichž každé má velikost 32 bitů, a 4 S-Boxy z nichž každý box má 256 32bitových položek. Čtyři S-Boxy tvoří, resp. vykonávají F funkci.

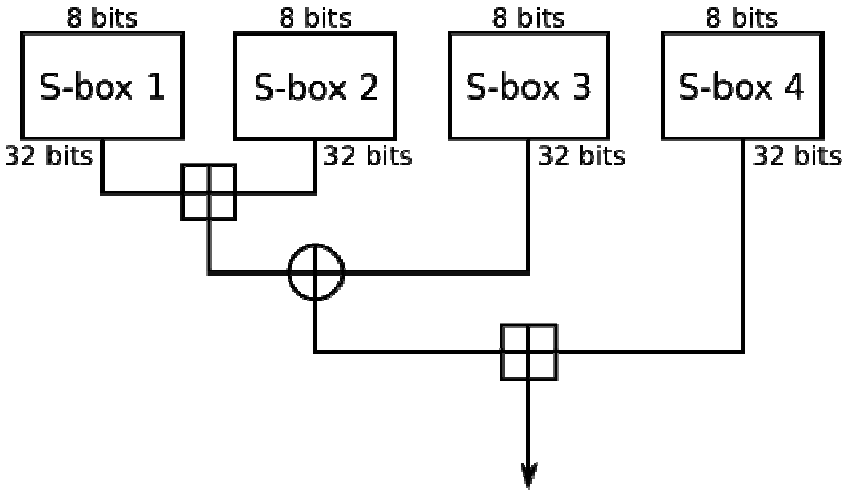
Znázorněný průběh při šifrování:



Obr. 17 Blowfish algoritmus [41]

Každý S-Box má 8bitový vstup a 32bitový výstup. Všechny boxy jsou poté inicializovány pevným řetězcem hexadecimálních číslic čísla π. Po inicializaci je prvních 32 bitů klíče XORováno s prvním polem *P1* (první 32bitový box), poté dalších 32 bitů klíče je XORováno s druhým polem *P2* atd.., dokud nedojde z XORování všech bitů klíče se všemi poli *P*. Dešifrování probíhá tak že pole *P* použijí reversně. [41]

Na obrázku níže jsou znázorněny 4 S-Boxy které vykonávají funkci F:



Obr. 18 Blowfish funkce F [41]

2.4.4.4 AES

Advanced Encryption Standard resp. Rijndaelův algoritmus je v současnosti nejrozšířenějším standard pro šifrování. V roce 2000 byla vybrána z 5 finalistů (MARS, RC-6, Rijndael, Twofish, Serpent) jako federální šifrovací standard v USA. Je to symetrická bloková šifra o velikosti bloku 128 bitů a délce klíče 128, 192 nebo 256 bitů. Na rozdíl od 3DES a Blowfish není založena na Feistelově šifře. AES provádí určitý počet iterací v závislosti na délce klíče. Pokud je klíč 128bitový, provádí se 10 iterací, pokud 192bitový tak 12 iterací a při 256bitovém klíči je prováděno 14 iterací. Důležitým prvkem AES je jeho tzv. stav což je matice 4x4 uvedená na obrázku níže. [42]

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,4}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Obr. 19 Matice 4x4 tzv. stav [42]

Algoritmus probíhá následovně:

1. **Expanze klíče** - tedy odvození podklíčů ze vstupního klíče. 128bitový klíč je expandován jako pole o 44 záznamech 32bitových slov. Každá 4 slova pak slouží jako klíč pro jednu iteraci. Rozdělení klíčů závisí na S-Boxu.
2. **Inicializace**
    a. přidání podklíče - přidá se podklíč, takže je každý byte stavu zkombinován s podklíčem za pomoci operace XOR
3. **Iterace**
    a. záměna bitů – zajišťuje se nelinearita, každý byte v matici je nahrazen pomocí 8bitového S-Boxu, z matice M vznikne matice M´

b. prohození řádků – operace na úrovni řádků, první řádek se neposouvá, druhý řádek se posune o pozici doleva, třetí řádek o 2 pozice doleva a čtvrtý o 3 pozice také doleva
c. kombinace sloupců – povede se kombinace 4 bytů v každém řádku, funkce přijme na vstupu 4 byty a na výstupu vrátí též 4 byty, zajistí se tak dostatečná náhodnost
d. přidání podklíče

4. **Konečná část**
   a. záměna bitů
   b. prohození řádků
   c. přidání podklíče [42]

2.4.4.5 RC-4

RC-4 je klasická symetrická proudová šifra vymyšlená Ronaldem Rivestem ze společnosti RSA DSI, který je mimo jiné spoluvynálezcem asymetrické šifry RSA. Vstupem je klíč o velikosti 1 až 256 bytů. Tento klíč je použit k inicializaci stavového 256bytového vektoru *S* s prvky *S(0), S(1)...S(255)*. Pro inicializaci je pak vytvořen přechodný vektor *T* a celá inicializace vypadá následovně:

```
for i = 0 to 255 do
S[i] = i;
T[i] = K[i mod keylen]; [43]
```

Kde keylen je délka klíče. Vektor *T* je pak použit pro určení počáteční permutace *S* tak, že se postupuje od *S(0),* až do *S(255)* a provádí se záměna *S(i)* s dalším bytem z *S* v závislosti na *T(i):*

```
j = 0;
for i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]); [43]
```

Poté co je inicializace hotová následuje generování streamu. Zde se již vstupní klíč nepoužívá. Provádí se od *S(0),* do *S(255),* a pro každé *S(i)* se provádí znovu záměna s dalším bytem z *S* a generují se hodnoty *k*:

```
i, j = 0;
while (true)
        i = (i + 1) mod 256;
        j = (j + S[i]) mod 256;
        Swap (S[i], S[j]);
        t = (S[i] + S[j]) mod 256;
        k = S[t]; [43]
```

Tato hodnota *k,* se poté při šifrování XORuje s následujícím bytem plaintextu. Dešifrování se provádí XORováním následujícího bytu šifrového textu. [43]
I přesto že je tato šifra velice rychlá, v současnosti je doporučeno již od této šifry upustit na základě nedávné kryptoanalýzy [44] a následném doporučení v RFC 7465 dokumentu vydaném IETF v roce 2015. Doporučení se týká TLS.

3 Praktická část

V následujících kapitolách je popsán výběr VPN a způsobu šifrování pro zabezpečení síťového povozu Smart Gridu, tedy na rozhraní mezi smart metrem a sítí NAN, které je specifikováno v rámci SGRIM jako CT-12. Výběr bude proveden na základě charakteristik jednotlivých VPN, dále pak budou specifikovány požadavky na kryptografické prostředky s ohledem na přílohu č. 3 vyhlášky č. 316/2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).
Poslední částí bude otestování vlivu kryptografických metod na propustnost linky a odezvu a jejich vzájemné porovnání.

3.1 Určení vhodné VPN

V rámci této práce bylo představeno 5 možných řešení VPN, a to PPTP, L2TP, IPsec, Open VPN a MPLS VPN. MPLS VPN vzhledem k tomu, že se svou povahou výrazně liší od ostatních výše uvedených, by mohla být vhodnější pro použití na páteřní WAN síti, propojující hlavní velké segmenty Smart gridu, jelikož je dobře škálovatelná a značně urychluje komunikaci, která je zde vysoce žádoucí.
Co se týče L2TP, jakožto protokolu pracujícím na linkové vrstvě, který umožňuje zapouzdřit data pro přenos po jiných sítích než IP, tak jeho bezpečnost je závislá na použití IPsec. Pro využití na daném rozhraní se jeví jako čistý IPsec lepší z hlediska možného menšího overheadu, jelikož jsou data zapouzdřována jednou oproti L2TP/IPsec.
Dalším možným kandidátem je PPTP, ovšem ten se jeví jako zastaralý a z hlediska bezpečnosti již není doporučen. Hlavním důvodem je to, že neposkytuje ochranu integrity dat, která je jedním z hlavních požadavků v rámci Smart Gridu.
OpenVPN jako open source řešení je dnes velice rozšířené a používané jako varianta k IPsec. Stejně jako IPsec nabízí silné šifrování, autentizaci a zajištění integrity. Ovšem pro využití ve Smart Gridu se jeví jako moudřejší použití IPsec vhledem k jeho komplexnosti, která bývá mnohdy označována spíše za jeho nevýhodu. Dále pak OpenVPN vyžaduje pro svou konfiguraci instalaci klienta.

IPsec bývá z velké části na mnoha zařízeních (routerech apod.) implementován a umožňuje dobrou interoperabilitu mezi různými zařízeními. Je též aplikačně nezávislý. Jako možné dobré řešení je tedy vybrán IPsec.

3.2 Požadavky na kryptografické algoritmy

V rámci použití IPsec je třeba na základě zákona o kybernetické bezpečnosti určit, které z funkcionalit a jejich stupně je možno použít k zabezpečení Smart Gridu, jakožto kritické infrastruktury. Jedná se o zajištění důvěrnosti, integrity a též autentizace pomocí kryptografických metod. Následující tabulka obsahuje přehled těchto funkcionalit v rámci protokolů AH a ESP.

Protokol	**AH**	**ESP**
Důvěrnost	X	3DES, Blowfish, AES
Integrita	MD5, SHA	MD5, SHA
Autentizace	PSK, RSA	PSK, RSA
Diffie-Hellman	Group 1-24	Group 1-24

Tab. 3 - IPsec přehled funkcionalit v rámci protokolů AH a ESP

Na základě přílohy č. 3 vyhlášky č. 316/2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) je nutno určit které kryptografické metody a jejich úrovně jsou vyhovující.

3.2.1 Důvěrnost

Pro zajištění důvěrnosti zákon ze tří výše uvedených šifer povoluje použití všech tří: 3DES, Blowfish, AES a klade na ně následující požadavky.

- **3DES** – využití při délce klíčů 168 bitů, doporučeno postupně přecházet na AES
- **Blowfish** – využití při délce klíčů minimálně 128 bitů
- **AES** - využití při délce klíčů 128, 192 a 256 bitů

Pro uvedené šifry jsou pak specifikovány povolené šifrovací módy CTR, OFB, CBC, CFB.

3.2.2 Integrita

Pro zajištění integrity zákon neumožňuje použití hashovaní funkce MD5, shledává ji tedy jako již nedostačující. Druhou z uvedených možností, tedy SHA, povoluje v různých variantách s ohledem na velikost výstupu v bitech.

- **SHA-2**
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512
  - SHA-512/224
  - SHA-512/256
- **SHA-3**
  - SHA3-224
  - SHA3256
  - SHA3-384
  - SHA3-512

Co se týče SHA-1, zákon již její použití neumožňuje, pouze v případě nutnosti ověření již existujícího elektronického podpisu apod. Dále pak pro SHA-2 a SHA-3

definuje módy pro zajištění integrity: HMAC, CBC-MAC-EMAC, CMAC a CBC-MAC-X9.19.

3.2.3 Autentizace

Pro autentizaci je možno použít PSK (pre-shared key) nebo RSA. Zákon nezohledňuje PSK. Obecně je pre-shared key považován za méně zabezpečený než RSA. Pro RSA specifikuje délku klíčů 2048 bitů a to jak při použití pro digitální podpis, tak pro asymetrické šifrování.

3.2.4 Diffie-Hellman

Poslední z uvedených funkcionalit je Diffie-Hellman algoritmus pro zajištění výměny klíčů. Zákon umožňuje použití Diffie-Hellman pouze při použití délky klíčů 2048 bitů a více. V případě ECDH (eliptic curve diffie-hellman) pouze pro využití s klíči 224 bitů a více. Diffie-Hellman je v závislosti na délce klíče a typu označen číslem skupiny (group).

- DH-1 (768bit DH)
- DH-2 (1024bit DH)
- DH-5 (1536bit DH)
- DH-14 (2048bit DH)
- DH-15 (3072bit DH)
- DH-16 (4096bit DH)
- DH-19 (256bit ECDH)
- DH-20 (384bit ECDH)
- DH-24 (2048bit DH/DSA) [45]

Z výše uvedených údajů v porovnání se zákonem vyplývá, že Diffie-Hellman group 1, 2 a 5 již nejsou povoleny. Umožněno je použití Diffie-Hellman group 14, 15, 16, 19, 20 a 24.

3.2.5 Zhodnocení zjištěných požadavků

Pomocí výše uvedeného uplatnění zákona č. 181/2014 o kybernetické bezpečnosti, přílohy č. 3 vyhlášky č. 316/2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) vyplynuly následující specifikace při použití IPsec jako prvku pro zabezpečení síťové komunikace ve Smart Gridu.

Protokol	**AH**	**ESP**
Důvěrnost	X	3DES – 168bit* Blowfish – 128bit AES – 128bit AES – 192bit AES – 256bit
Integrita	SHA-2 - 224-512/256bit SHA-3 – 224-512/256bit	SHA-2 – 224-512/256bit SHA-3 – 224-512/256bit
Autentizace	PSK >=RSA 2048bit	PSK >=RSA 2048bit
Diffie-Hellman	DH-14 DH-15 DH-16 DH-19 DH-20 DH-24	DH-14 DH-15 DH-16 DH-19 DH-20 DH-24

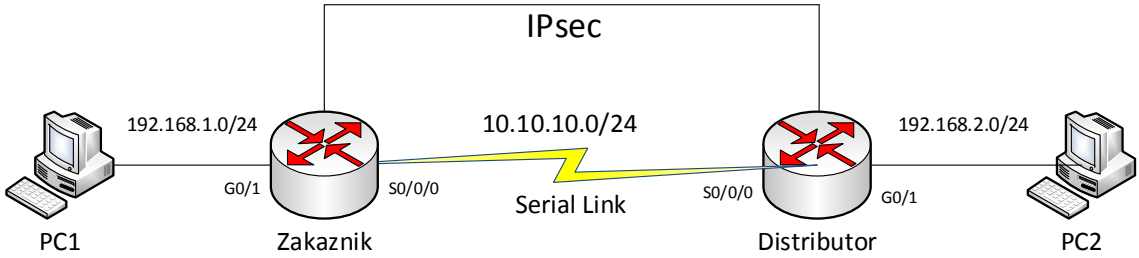
*doporučeno přejít na AES

Tab. 4 – Specifikace podle zákona o kybernetické bezpečnosti pro IPsec

3.3 IPsec analýza

Jako simulační prostředí pro testování zatížení linky nasazením IPsec byly použity 2 Cisco routery řady 2900, přesněji modely 2911 propojené sériovou linkou 2 Mbps. Ta byla zvolena vzhledem k povaze simulovaného rozhraní. Na straně každého routeru byla připojena jedna stanice. Mezi routery byl nakonfigurován IPsec tunel a poté byla mezi jednotlivými stanicemi testována propustnost linky programem Jperf a odezva programem Iperf.

Testovací topologie:



Obr. 20 - IPsec topologie

3.3.1 Konfigurace IPsec

Nejdůležitějším bodem je samotná konfigurace, která byla rozdělena do šesti bodů. Jednalo se o konfiguraci pro samotné navázání spojení mezi routery a stanicemi, a následně pak konfigurace IPsec

1) Jako první bylo nutno přiřadit ip adresy jednotlivý sériovým rozhraním a též rozhraním pro připojení hostů na obou routerech označených jako Zakaznik a Distributor.

```
Zakaznik(config)#interface serial 0/0/0
Zakaznik(config-if)#ip address 10.10.10.1 255.255.255.0
Zakaznik(config-if)#no shutdown
```

```
Distributor(config)#interface serial 0/0/0
Distributor(config-if)#ip address 10.10.10.2 255.255.255.0
Distributor(config-if)#no shutdown

Zakaznik(config)#interface gigabitEthernet 0/1
Zakaznik(config-if)#ip address 192.168.1.1 255.255.255.0
Zakaznik(config-if)#no shutdown

Distributor(config)#interface gigabitEthernet 0/1
Distributor(config-if)#ip address 192.168.2.1 255.255.255.0
Distributor(config-if)#no shutdown
```

2) Dále pak bylo nutno nakonfigurovat na sériových rozhraních access listy, které slouží pro určení toho, z jaké sítě do jaké má být komunikace šifrována.

```
Zakaznik(config)#access-list 101 permit ip 192.168.1.0
0.0.0.255 192.168.2.0 0.0.0.255

Distributor(config)#access-list 101 permit ip 192.168.2.0
0.0.0.255 192.168.1.0 0.0.0.255
```

3) Třetím bodem už je první část konfigurace samotného IPsec. Je třeba nakonfigurovat jednotlivé parametry v rámci ISAKMP. Je třeba specifikovat algoritmus pro šifrování, integritu, vyjednání klíčů a také způsob autentizace. Popř. také dobu platnosti vyjednaných parametrů, po jejímž uplynutí se musí vyjednání zopakovat.

```
Zakaznik(config)#crypto isakmp policy 100
Zakaznik(config-isakmp)#encryption aes256
Zakaznik(config-isakmp)#authentication pre-share
Zakaznik(config-isakmp)#group 16
Zakaznik(config-isakmp)#hash sha512
Zakaznik(config-isakmp)#lifetime 3600
Zakaznik(config)#crypto isakmp key ipseckey address
10.10.10.2
```

```
Distributor(config)#crypto isakmp policy 100
Distributor(config-isakmp)#encryption aes256
Distributor(config-isakmp)#authentication pre-share
Distributor(config-isakmp)#group 16
Distributor(config-isakmp)#hash sha512
Distributor(config-isakmp)#lifetime 3600
Distributor(config)#crypto isakmp key ipseckey address
10.10.10.1
```

4) Dalším bodem je specifikovat jaké protokoly budou použity, jestli AH, ESP nebo AH+ESP, společně s nadefinováním, jaké šifrovací a hashovací metody budou v rámci těchto protokolů použity.

```
Zakaznik(config)#crypto ipsec transform-set ipsecvpn ah-
sha512-hmac esp-aes256 esp-sha512-hmac

Distributor(config)#crypto ipsec transform-set ipsecvpn ah-
sha512-hmac esp-aes256 esp-sha512-hmac
```

5) Předposledním bodem je vytvoření mapy, která asociuje výše uvedené konfigurace. Je definováno, který transform-set bude použit v mapě. Mezi kterými sítěmi se bude šifrovat, k tomu slouží nakonfigurované access listy. Mezi kterými body je tunel vytvářen. Jak dlouho bude trvat, než bude třeba vyjednat novou asociaci.

```
Zakaznik(config-crypto-map)#crypto map ipsecmap 100 ipsec-isakmp
Zakaznik(config-crypto-map)#set peer 10.10.10.2
Zakaznik(config-crypto-map)#set transform-set ipsecvpn
Zakaznik(config-crypto-map)#match address 101
Zakaznik(config-crypto-map)#set session-key lifetime seconds
1800
Zakaznik(config-crypto-map)#set pfs group16
```

```
Distributor(config-crypto-map)#crypto map ipsecmap 100 ipsec-
isakmp
Distributor(config-crypto-map)#set peer 10.10.10.1
Distributor(config-crypto-map)#set transform-set ipsecvpn
Distributor(config-crypto-map)#match address 101
Distributor(config-crypto-map)#set session-key lifetime seconds
1800
Distributor(config-crypto-map)#set pfs group16
```

6) Posledním bodem je aktivování nakonfigurované mapy na rozhraních, mezi kterými je třeba mít zabezpečený provoz.

```
Zakaznik(config)#interface S0/0/0
Zakaznik(config-if)#crypto map ipsecmap

Distributor(config)#interface S0/0/0
Distributor(config-if)#crypto map ipsecmap
```

Je též důležité neopomenout zkontrolovat na rozhraních, mezi kterými je vytvořeno šifrované spojení, zda je povolen provoz protokolů AH, ESP a ISAKMP, tedy IP protokol 50, 51 a UDP 500.

3.3.2 Test odezvy

Testování proběhlo na vytvořené IPsec tunelu při použití šifrovacích algoritmů 3DES, AES128, AES192 a AES256. Šifra Blowfish nebyla dostupná, jelikož se na těchto Cisco routerech nepoužívá. Pro všechny čtyři případy byla pro zajištění integrity dat použita hashovaní funkce SHA512. Autentizace zajištěna pomocí PSK pro testovací účely.

Jako testovací nástroj byl použit Iperf. Protokol pro měření byl použit TCP. Pro každý typ šifrovacího algoritmu bylo provedeno dvacet měření pro pakety velikosti 64 bytů a 1500 bytů.

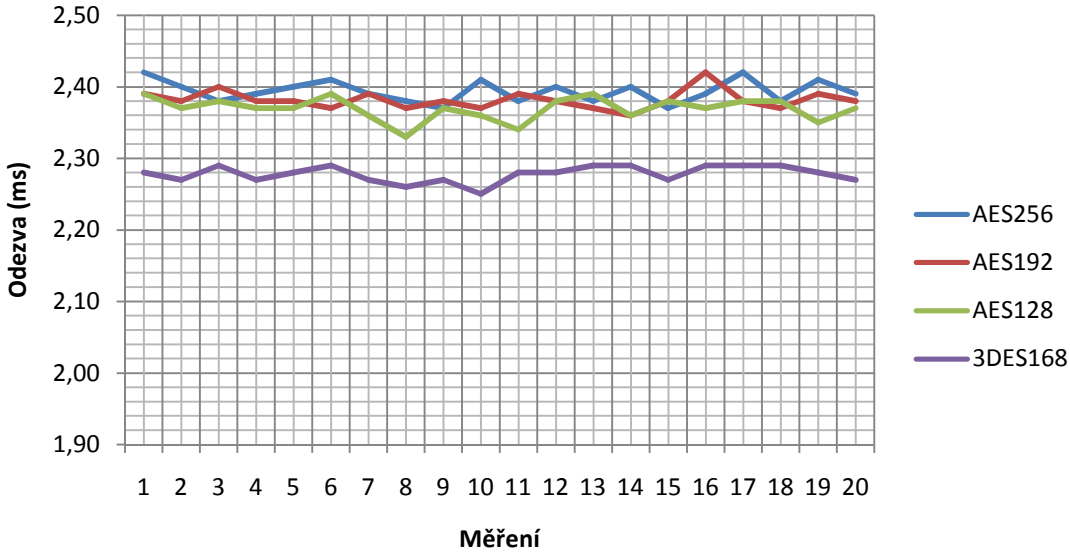
Výsledky měření pro pakety velikosti 64 bytů znázorněné v tabulce.

Algoritmus	**Odezva (ms)**		
	Min.	Prům.	Max.
Plain text	1,138	1,154	1,181
3DES	2,264	2,278	2,295
AES128	2,355	2,370	2,382
AES192	2,367	2,382	2,396
AES256	2,371	2,394	2,418

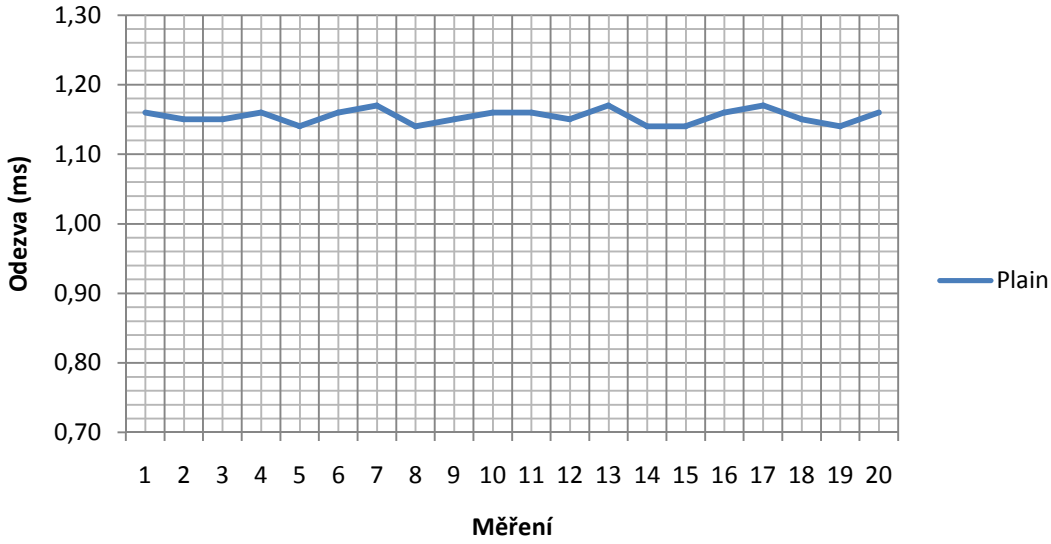
Tab. 5 - Odezva 64bytové pakety

Z výsledků měření je patrné, že nejnižší odezva byla naměřena při nešifrované komunikaci. U šifrované komunikace v závislosti na použitém algoritmu se zvýšila odezva o 1,124-1,24 ms oproti nešifrované komunikaci.

Výsledky odezvy v průběhu všech dvaceti měření jsou znázorněné v grafech níže. Z hlediska čitelnosti grafu byla šifrovaná komunikace znázorněna v jiném grafu než nešifrovaná komunikace.



Obr. 21- Průměrná odezva IPsec 64bytové pakety



Obr. 22 - Průměrná odezva plain text 64bytové pakety

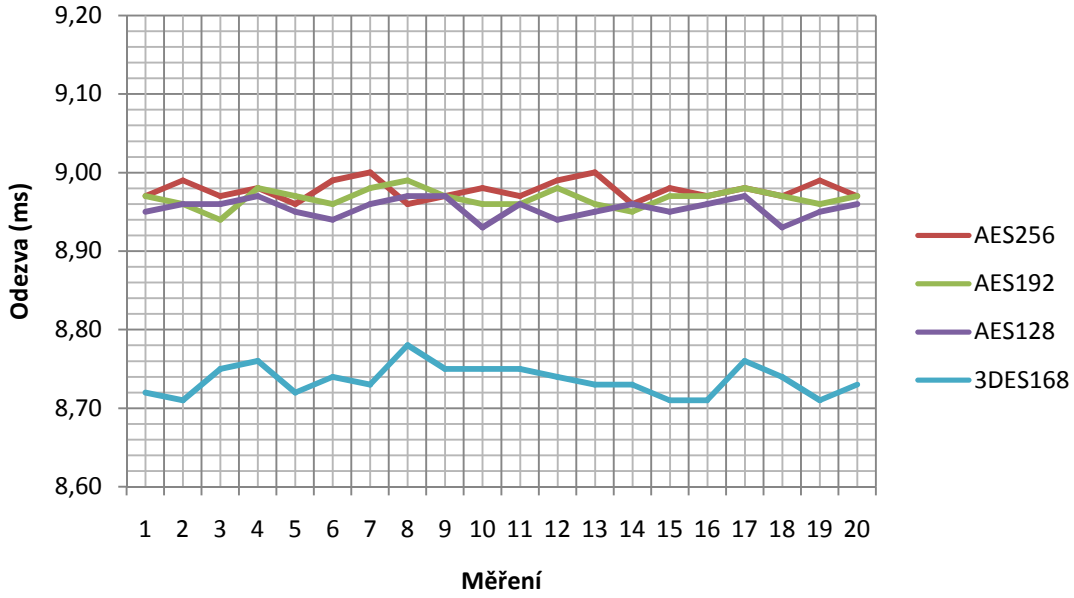
Výsledky měření pro pakety velikosti 1500 bytů:

Algoritmus	Odezva (ms)		
	Min.	Prům.	Max.
Plain text	6,267	6,277	6,291
3DES168	8,712	8,736	8,753
AES128	8,940	8,955	8,974
AES192	8,954	8,968	8,988
AES256	8,964	8,978	9,002

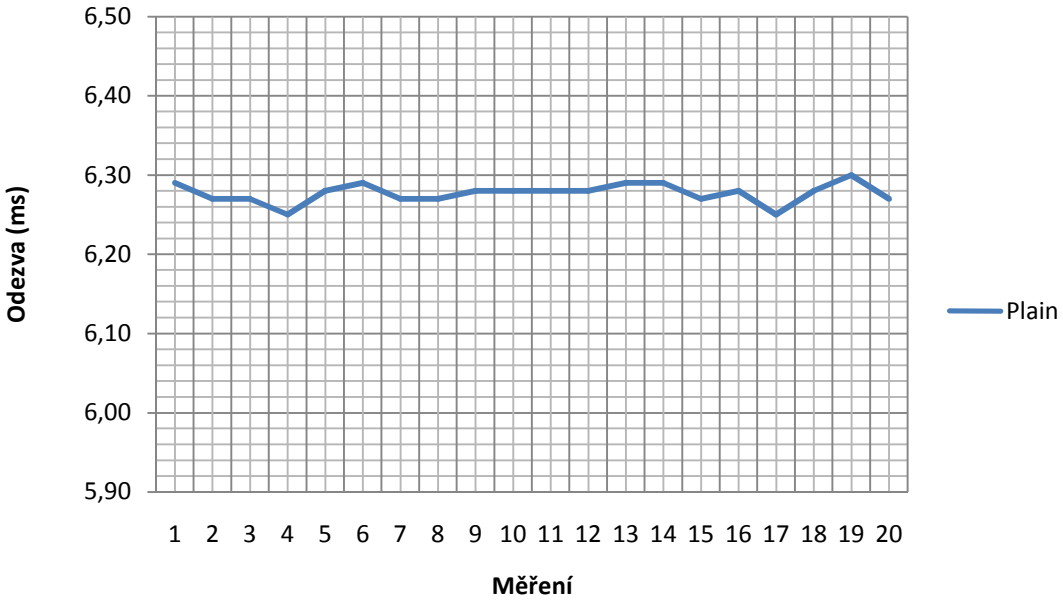
Tab. 6 - Odezva 1500bytové pakety

Jako u předchozího případu je vidět že nejnižší odezva byla naměřena u nešifrované komunikace, nicméně rozdíl v průměrné odezvě mezi šifrovanou a nešifrovanou komunikaci byl větší, a to v rozmezí od 2,459 ms od 2,701 ms.

Výsledky odezvy v průběhu všech dvaceti měření jsou znázorněné v grafech níže. Z hlediska čitelnosti grafu byla jako u předchozího případu šifrovaná komunikace znázorněna v jiném grafu než nešifrovaná komunikace:



Obr. 23 - Půměrná odezva IPsec 1500bytové pakety



Obr. 24 - Průměrná odezva plain text 1500bytové pakety

3.3.3 Zhodnocení testu odezvy

Z výsledků měření je patrné že velikost paketů má značný vliv na odezvu vzhledem k použití sériové linky. Co se týče šifrované komunikace, vlivem IPsec overheadu se průměrná odezva pohybovala v rozmezí, od 2,278 ms do 8,978 ms v porovnání s nešifrovanou komunikací kde byla odezva v rozmezí od 1,154 ms do 6,277 ms.
V porovnání vlivu šifrovacího algoritmu na odezvu si vedl nejlépe 3DES s délkou klíčů 168 bitů kde byl rozdíl oproti AES s délkami klíčů 128, 129 a 256 bitů v rozmezí od 0,092 ms do 0,242 ms, tedy v řádu desetin milisekund. Z porovnání jednotlivých variant AES o délkách klíčů 128, 192 a 256 bitů plyne, že nejrychlejší je AES128 poté AES192 a nejpomalejší je AES256, což je logické vzhledem k tomu že se liší jen délkou klíčů. Rozdíl mezi těmito třemi variantami byl v rozmezí 0,01-0,024 ms, tedy v řádu setin milisekund. To je porovnáním s předchozím porovnáním 3DES168 a variant AES zanedbatelné.

3.3.4 Test propustnosti linky

Testování proběhlo na vytvořené IPsec tunelu při použití šifrovacích algoritmů 3DES, AES128, AES192 a AES256. Též proběhlo měření na lince bez použití šifrování. Jako nástroj pro měření byl použit Jperf. Jako protokol byl použit TCP pro

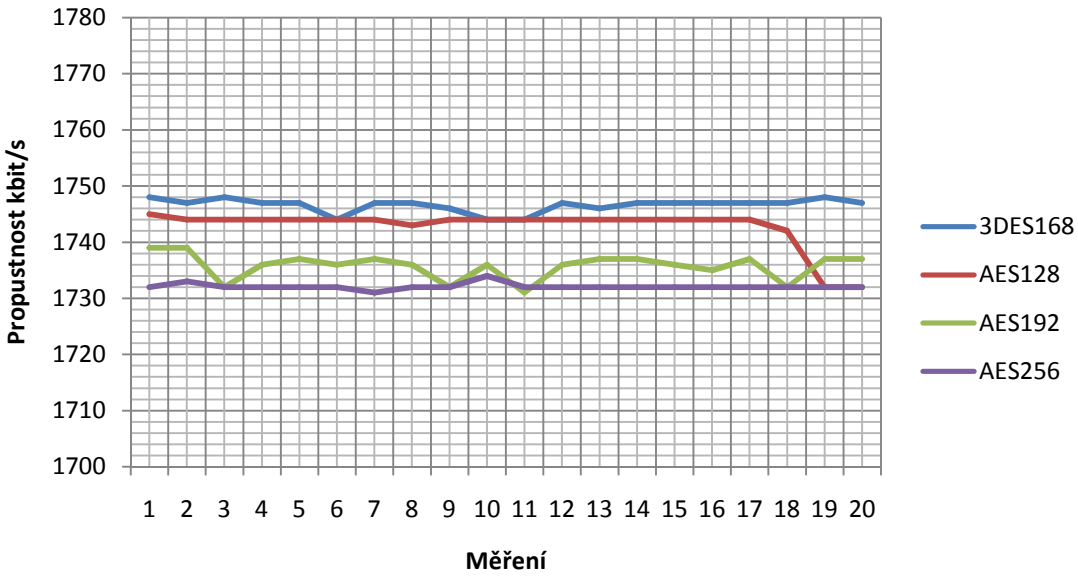
zajištění spolehlivosti. Měření proběhlo při zaslání souboru velikost 1Megabyte, tato velikost byla vybrána s ohledem na velikosti zasílaných dat v síti Smart Grid. Bylo provedeno dvacet měření v jednom směru pro každý algoritmus při šifrované komunikaci, též i bez použití šifrování.

Výsledky průměrných propustností linky:

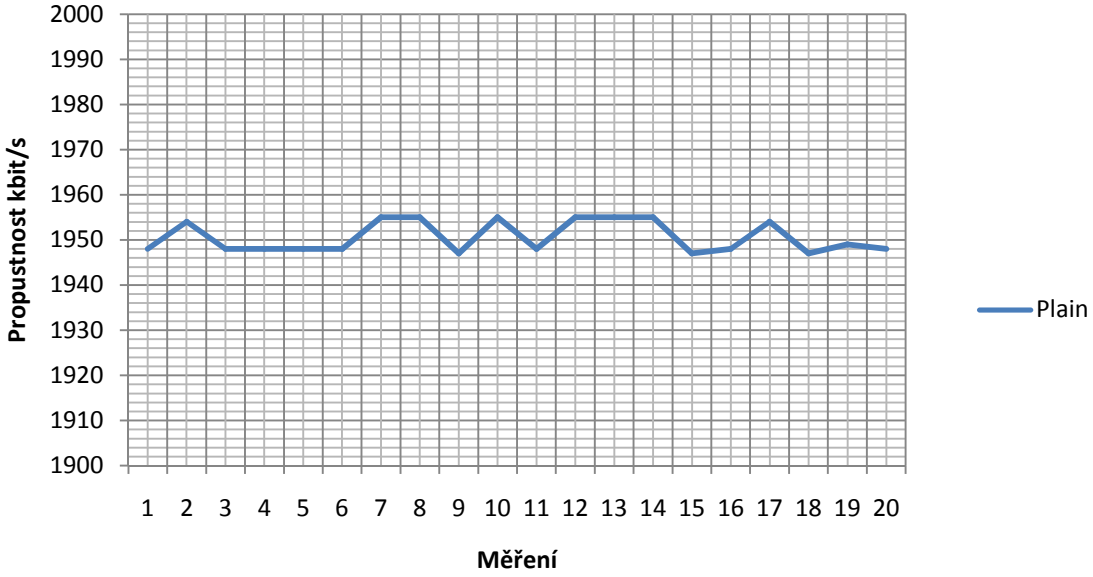
	Plain text	3DES168	AES128	AES192	AES256
Průměrná propustnost kbit/s	1950,60	1746,60	1742,70	1735,75	1732,1

Tab. 7 - Průměrné propustnosti linky

V grafech níže jsou pro lepší představu uvedeny průměrné propustnosti všech dvaceti měření. Rozdělení na dva grafy má stejný důvod jako u měření odezvy.



Obr. 25 - Průměrná propustnost IPsec



Obr. 26 - Průměrná propustnost plain text

3.3.5 Zhodnocení testu propustnosti linky

Z výše zaznamenaných měření vyplývá, že bez použití IPsec je propustnost sériové 2Mbps linky 1950,60 kbit/s, tedy využití z 97,53 %. S nasazeným IPsec byla průměrná propustnost od 1732,1 kbit/s do 1746,6 kbit/s tedy využití linky z 86,6 % až 87,33 %. Srovnání propustnosti linky bez nasazení IPsec a s nasazením IPsec vede k závěru, že v důsledku IPsec overheadu se sníží propustnost linky o 10,2 % až 10,93 %.

Ze srovnání propustností naměřených v závislosti na použitých šifrovacích algoritmech vyplývá, že při použití algoritmu 3DES168 je linka nejméně zatížená. Nejvíce je pak linka zatížená při použití AES s délkou klíčů 256 bitů. Rozdíl mezi AES256 a 3DES168 činí 14,5 kbit/s. Rozdíly mezi naměřenými propustnostmi jednotlivých variant AES byly v rozsahu od 3,65 kbit/s do 10,6 kbit/s.

4 Shrnutí výsledků

Smart Grid je na základě zákona o kybernetické bezpečnosti klasifikován jako kritická infrastruktura, je tedy nutné zajistit bezpečnost komunikace kryptografickými prostředky, jak tomu tento zákon ukládá. Jako dobré řešení se nabízejí VPN. Z možných VPN byl vybrán IPsec pro zabezpečení datové komunikace, který nabízí širokou škálu možností pro zabezpečení z hlediska autentizace, integrity a důvěrnosti. Zde je nutno připomenout, že v rámci Smart Gridu je třeba zajistit i dostupnost, zvláště v kritických segmentech jako například simulované rozhraní mezi smart metrem a sítí NAN. Toto IPsec neřeší, nemá k tomu žádný nástroj, je tedy na místě použití jiných nástrojů po zajištění dostupnosti, jako např. firewally, záložní cesty či recovery systémy.

Na základě zákona o kybernetické bezpečnosti bylo určeno, které šifrovací algoritmy, hashovací funkce a jejich módy je možno použít z těch, jež IPsec nabízí a které již ne. Dále pak i různá doporučení. Otázkou je, jak tyto požadavky budou dodržovány v praxi.

V porovnání měření odezvy dosáhl nejlepšího výsledku algoritmus 3DES s délkovou klíče 168 bitů a to jak pro pakety velikosti 64 bytů tak 1500 bytů. Při měření s pakety o velikosti 1500 bytů bylo zvýšení odezvy způsobené IPsec overheadem větší než u 64bytových paketů. Též při porovnání naměřených propustností vyšel z testu nejlépe 3DES. Tento výsledek je možno přisoudit tomu, že 3DES pracuje s menšími velikostmi bloku než AES, a též jeho délka klíče 168 bitů (což je v podstatě efektivních 112 bitů) je menší než u AES. Obecně pak linka vykazovala dobré hodnoty propustnosti při nasazeném IPsec. V porovnání s nezabezpečenou komunikací se zde projevilo snížení o 10,2 % až 10,93 %. Pro praktické použití s výhledem do budoucna je ovšem AES v porovnání s 3DES z hlediska úrovně bezpečnosti jednoznačnou volbou, neboť sice zatěžuje linku více, ovšem tyto rozdíly hodnot propustností jsou v řádech desítek kbit/s a odezvách v řádech desetin milisekund, což je zanedbatelné.

5 Závěry a doporučení

Cílem práce bylo přiblížení síťové komunikace, která je stěžejním prvkem Smart Gridu, a představit, jak tuto komunikaci zabezpečit. Příkladem bylo zaručení bezpečného přenosu informací mezi zákazníkem a distributorem, konkrétněji mezi smart metrem a NAN (Neighbour Area Network), kde je vyžadována nejvyšší úroveň důvěrnosti, integrity a dostupnosti. Podařilo se určit k tomu vhodný nástroj IPsec a prozkoumat jeho vliv na komunikaci, v rámci čehož bylo provedeno i srovnání šifrovacích algoritmů.

V průběhu výzkumu se ukázalo jako dobré nejen představit možnosti zajištění důvěrnosti, integrity popř. i autentizace, ale též se podívat, jak na tuto problematiku nahlíží zákon. To pak umožnilo definovat požadavky na důvěrnost, integritu a provést konfiguraci tak, aby byly v souladu se zákony České Republiky a bylo zajištěno odpovídající úrovně bezpečnosti.

Vzhledem k dosaženým výsledkům bych doporučil nasazení IPsec na zabezpečení této komunikace, jeví se jako bezpečné a komplexní řešení. Jako možné rozšíření výzkumu či oblasti zájmu ve spojitosti se Smart Gridem by mohlo být vhodné prozkoumat možné způsoby pro zajištění dostupnosti, jelikož je to nedílnou součástí bezpečnostního požadavku, který IPsec sám o sobě neřeší. Též pak komplexněji zmapovat způsoby zajištění integrity či autentizace, které jsou popsány spíše okrajově.

Jako poslední věc bych zmínil, že Smart Grid jako dosti nová technologie je stále ve fázi návrhu a testování. Má velký potenciál, ovšem i se svými možnými riziky. Čas ukáže, jestli se podaří plně začlenit tuto technologii do běžného života.

6 Seznam použité literatury

[1] BOUŠKA, Petr. OSI model. Www.samuraj-cz.com [online]. 2007 [cit. 2015-08-19]. Dostupné z: http://www.samuraj-cz.com/clanek/osi-model/

[2] ALANI, Mohammed M. Guide to OSI and TCP/IP models. Cham: Springer, 2014, x, 50 pages. ISBN 9783319051529.

[3] Internetworking. New York: Springer, 2013, pages cm. ISBN 9783642353918.

[4] BOUŠKA, Libor. TCP/IP - model, encapsulace, paket vs. rámec: Ethernetová hlavička. *Www.SAMURAJ-cz.com* [online]. 2007 [cit. 2016-04-09]. Dostupné z: http://www.samuraj-cz.com/clanek/tcpip-model-encapsulace-paketu-vs-ramec/

[5] SHONIREGUN, Charles A. Synchronizing Internet Protocol Security (SIPSec). New York: Springer, 2007, xiv, 223 p. Advances in information security, 34. ISBN 0387685693-.

[6] BOUŠKA, Petr. TCP/IP - Internet Protocol Version 6 - IPv6. Www.samuraj-cz.com [online]. 2009 [cit. 2016-02-20]. Dostupné z: http://www.samuraj-cz.com/clanek/tcpip-internet-protocol-version-6-ipv6/

[7] SLAVÍK, Jakub. Víte co to je, a jak funguje smart grid? [online]. [cit. 2016-01-30]. Dostupné z: http://www.proelektrotechniky.cz/vzdelavani/22.php

[8] KUZLU, Murat, Saifur RAHMAN a Manisa PIPATTANASOMPORN. Communication network requirements for major smart grid applications in HAN, NAN and WAN. Computer Networks [online]. 2014, 67, 74-88 [cit. 2016-04-02]. ISSN 1389-1286. Dostupné z: http://www.sciencedirect.com/science/article/pii/S1389128614001431

[9] HO, Quang-Dung. Wireless communications networks for the smart grid. New York: Springer, 2014. ISBN 9783319103464.

[10] SPONSOR, IEEE Standards Coordinating Committee 21 on Fuel Cells. IEEE guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS), end-use applications and loads. New York, N.Y: Institute of Electrical and Electronics Engineers, 2011. ISBN 9780738167275.

[11] ENISA Smart Grid Security Recommendations. *ENISA* [online]. 2012 [cit. 2016-04-03]. Dostupné z: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf/view

[12] ALOUL, Fadi, A.R. AL-ALI, Rami AL-DALKY, Mamoun AL-MARDINI a Vassim EL-HAJJ. International Journal of Renewable Energy and Smart Grid (IJRESG). *International Journal of Smart Grid and Clean Energy*[online]. 2012, **1**(1) [cit. 2016-04-03]. ISSN 2315-4462. Dostupné z: http://www.ijsgce.com/uploadfile/2012/1011/20121011121836539.pdf

[13] DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING TEXAS TECH UNIVERSITY. Introduction to smart grid [online]. 2012 [cit. 2016-01-30]. Dostupné z: http://www.ee.ucr.edu/~hamed/Smart_Grid_Topic_2_Smart_Grid.pdf

[14] WENYE, Wang a Lu ZHUO. Cyber Security in the Smart Grid: Survey and Challenges [online]. [cit. 2016-01-31]. Dostupné z: http://www.ece.ncsu.edu/netwis/papers/12WL-COMNET.pdf

[15] LUHOVÝ, Karel. Svět síťí: historie, definice a důvody budování VPN [online]. 2003 [cit. 2016-01-31]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=VPN-1-historie-definice-a-duvody-budovani-612003

[16] RAO, Umesh Hodeghatta a Umesha NAYAK. The InfoSec handbook: an introduction to information security. New York, New York: Apress, 2014. Expert's voice in information security. ISBN 9781430263821

[17] LUHOVÝ, Karel. Svět síťí: tradiční model tunelování [online]. 2003 [cit. 2016-01-31]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=VPN-5--tradicni-model-tunelovani-2012003

[18] An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN. Photonic Network Communications [online]. 2016, 31, 13 [cit. 2016-02-20]. ISSN 1572-8188. Dostupné z: http://link.springer.com/journal/11107

[19] SCHREINER, Bruce. Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2). Schreiner on security [online]. UC Berkeley, 1999 [cit. 2016-02-20]. Dostupné z: https://www.schneier.com/cryptography/archives/1999/09/cryptanalysis_of_mic_1.html

[20] EINSINGER, Jochen. Exploiting known security holes in Microsoft’s PPTP Authentication Extensions (MS-CHAPv2) [online]. University of Freiburg, 2001 [cit. 2016-02-20]. Dostupné z: http://penguin-breeder.org/pptp/download/pptp_mschapv2.pdf

[21] Protokol PPTP (Point-to-Point Tunneling Protocol). Tech Net [online]. 2016 [cit. 2016-02-20]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc738852(v=ws.10).aspx

[22] Layer Two Tunneling Protocol and Internet Protocol Security. MICROSOFT CORPORATION. Tech Net [online]. 2016 [cit. 2016-02-20]. Dostupné z: https://technet.microsoft.com/en-us/library/cc958047.aspx#mainSection

[23] MALIK, Saadat. Network security principles and practices. Indianapolis, Ind.: Cisco, 2003. ISBN 1587050250.

[24] Introduction to L2TPv3. ProL2TP [online]. 2016 [cit. 2016-02-20]. Dostupné z: http://prol2tp.com/documentation.php?page=l2tpv3.html

[25] BOUŠKA, Petr. Virtual Private Network. Www.SAMURAJ-cz.com [online]. 2011 [cit. 2016-02-21]. Dostupné z: http://www.samuraj-cz.com/clanek/vpn-1-ipsec-vpn-a-cisco/

[26] DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: bezpečnost: bezpečný web a pošta, firewaly a proxy-servery, kódování a kryptografické postupy, atributové certifikáty, Kerberos. 2. aktualiz. vyd. Praha: Computer Press, 2003, xvi, 571 s. ISBN 80-7226-849-x.

[27] Trustworthy computing and services: International Conference, ISCTCS 2012, Beijing, China, May 28 - June 2, 2012, revised selected papers. 1st ed. New York: Springer, 2013. ISBN 3642357946.

[28] F. CRIST, Eric a Jan JUST KEIJSER. Mastering OpenVPN. Birmingham: Packt Publishing, 2015. ISBN 1-78355-314-6.

[29] OPENVPN TECHNOLOGIES, INC. OpenVPN: Security Overview [online]. 2016 [cit. 2016-02-27]. Dostupné z: https://openvpn.net/index.php/open-source/documentation/security-overview.html

[30] Ivan Pepelnjak, Jeff Apcar, jim Guichard. MPLS and VPN Architectures, Volume II. : Cisco Press, 2003. ISBN 1-58705-112-5.

[31] Vývoj paketových sítí a postavení MPLS. Svět Sítí [online]. 2006 [cit. 2016-02-28]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Vyvoj-paketovych-siti-a-postaveni-MPLS-2472006

[32] Understanding Using MPLS-Based Layer 2 and Layer 3 VPNs on EX Series Switches: MPLS-Based Layer 2 VPNs. Juniper Networks [online]. 2013 [cit. 2016-02-28]. Dostupné z: http://www.juniper.net/documentation/en_US/junos12.3/topics/concept/mpls-ex-series-vpn-layer2-layer3.html

[33] Layer 3 MPLS VPN Enterprise Consumer Guide Version 2. CISCO SYSTEMS, INC. Cisco [online]. 2008 [cit. 2016-02-28]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/L3VPNCon.html

[34] O'REGAN, Gerard. Mathematics in computing: an accessible guide to historical, foundational and application contexts. New York: Springer, 2013. ISBN 9781447145349.

[35] Šifrování - úvod do problematiky. ROOT.CZ [online]. [cit. 2016-03-12]. Dostupné z: http://www.root.cz/clanky/sifrovani-uvod-do-problematiky/

[36] LARS R. KNUDSEN, MATTHEW J.B. ROBSHAW., Lars R. Knudsen, Matthew J.B. Robshaw. The block cipher companion. Heidelberg: Springer-Verlag Berlin Heidelberg, 2011. ISBN 9783642173424.

[37] KLÍMA, Vlastimil. Mody činnosti blokových šifer a hašovací funkce [online]. 2007 [cit. 2016-03-12]. Dostupné z: http://crypto-world.info/klima/mffuk/Symetricka_kryptografie_III_2007.pdf

[38] KLÍMA, Vlastimil. Základy moderní kryptologie - Symetrická kryptografie II. [online]. 2005 [cit. 2016-03-12]. Dostupné z: http://crypto-world.info/klima/mffuk/Symetricka_kryptografie_II_2006.pdf

[39] STALLINGS, William. Cryptography and network security: principles and practice. 4th ed. Upper Saddle River, N.J.: Pearson/Prentice Hall, c2006. ISBN 0131873164.

[40] DHIR, Amit. Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs [online]. 2000 [cit. 2016-03-17]. Dostupné z: http://www.xilinx.com/support/documentation/white_papers/wp115.pdf

[41] KUMAR KURMI, Pawan a Rahul JAIN. IMAGE ENCRYPTION AND DECRYPTION USING BLOWFISH ALGORITHM WITH RANDOMNUMBER GENERATOR [online]. School of Information Technology Engraining, VIT University, Vellore-14, Tamilnadu, India, 2014, , 7 [cit. 2016-03-18]. ISSN 0975-766X. Dostupné z: http://www.ijptonline.com/wp-content/uploads/2015/02/7164-7170.pdf

[42] Announcing the ADVANCED ENCRYPTION STANDARD (AES) [online]. Federal Information Processing Standards Publications, 2001 [cit. 2016-03-18]. Dostupné z: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[43] STALLINGS, William. *THE RC4 STREAM ENCRYPTION ALGORITHM* [online]. 2005, 9 [cit. 2016-03-18]. Dostupné z: http://chemistry47.com/PDFs/Cryptography/RC4%20Stream%20Cipher/Tutorials/THE%20RC4%20STREAM%20ENCRYPTION%20ALGORITHM.pdf

[44] ALFARDAN, Nadhem J., Daniel J. BERNSTEIN, Kenneth G. PATERSON, Bertram POETTERING a Jacob C. N. SCHULDT. *On the Security of RC4 in TLS* [online]. Washington, D.C., USA, 2013 [cit. 2016-03-19]. Dostupné z: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_alfardan.pdf

[45] Configuring Internet Key Exchange for IPsec VPNs. *Cisco* [online]. Cisco Systems, Inc., 2012 [cit. 2016-04-16]. Dostupné z: http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/15-2mt/sec-key-exch-ipsec.htm

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2015/2016

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Ildža Daniel	Horská 65, Trutnov - Horní Staré Město	I1300701

TÉMA ČESKY:

Šifrování komunikace v IP sítích

TÉMA ANGLICKY:

Encrypting communication in IP networks

VEDOUCÍ PRÁCE:

Ing. Ondřej Hornig - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem práce je podrobně představit možnosti zabezpečení datové komunikace pomocí šifrování a nastínit slabé a silné stránky jednotlivých možností. Podkladem práce v teoretické části musí být popis komunikace v dnešních IP sítích včetně protokolů, které se běžně používají. Výsledkem praktické části práce bude porovnání možností šifrování, stupně jejich zabezpečení a navržení ideálního řešení pro použití v komunikaci datových sítí energetické přenosové soustavy.

SEZNAM DOPORUČENÉ LITERATURY:

DOSTÁLEK, Libor.; KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualizované vydání, Brno: Computer Press, a.s., 2008. 488 s. ISBN 978-80-251-2236-5.

HICKS, Michael. Optimizing Applications on Cisco Networks. 1. vydání. Indianapolis: Cisco Press, 2004. 384 s. ISBN: 978-1-58705-153-1.

HUCABY, David. CCNP SWITCH 642-813 Official Certification Guide. 1. vydání. Indianapolis: Cisco Press, 2011, 533 s. ISBN 978-1-58720-243-8.

RANJBAR, Amir. Troubleshooting and Maintaining Cisco IP Networks (TSHOOT). 1. vydání. Indianapolis: Cisco Press, 2010. 392 s. ISBN: 978-1-58705-876-9.

Podpis studenta: ..... **Datum:** 12.10.2015

Podpis vedoucího práce: ..... **Datum:** 12.10.2015