Česká zemědělská univerzita v Praze
Technická fakulta

Katedra technologických zařízení staveb

Spolehlivost telefonních komunikátorů systémů PZTS

diplomová práce

Vedoucí diplomové práce: Ing. Zdeněk Votruba Ph.D.

Diplomant: Bc. Petr Beneš

PRAHA 2016

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Petr Beneš

Obchod a podnikání s technikou

Název práce

Spolehlivost telefonních komunikátorů systémů PZTS

Název anglicky

Reliability of telephone dialer in I&HAS

Cíle práce

Posoudit a prakticky ověřit spolehlivost a bezpečnost telefonního komunikátoru poplachového systému především z pohledu možného napadení systému prostřednictvím telefonní linky.

Metodika

1. Porovnat varianty telefonního přenosu, charakteristiky přenosu a komunikátorů.
2. Popsat komunikaci mezi PZTS a tel. komunikátorem
3. Definovat kritické body komunikace a možnosti napadení
4. Ověřit teoretické závěry praktickými testy
5. Vyhodnotit měření a kvantifikovat rizika
6. Navrhnout doporučení z pohledu bezpečnosti a nákladů

Doporučený rozsah práce

50 – 60 stran textu včetně příloh

Klíčová slova

PZTS, datové přenosy, komunikace, bezpečnost

Doporučené zdroje informací

BAZALA, David. Telekomunikace a VoIP telefonie. 1. vyd. Praha: BEN – technická literatura, 2006, 224 s. ISBN 80-7300-201-9

Firemní a obchodní literatura jednotlivých výrobců

HEŘMAN, J., et al.: Elektrotechnické a telekomunikační instalace. Praha: Verlag Dashöfer, 2008. ISSN 1803-0475

JACKSON, Benjamin a Champ CLARK. Asterisk hacking: toolkit and liveCD. Editor Larry Chaffin, Johnny Long. Burlington: Syngress, 2007, xii, 253 s. ISBN 978-1-59749-151-8

JANSEN, Horst a Heinrich RÖTTER. Informační a telekomunikační technika. Vyd.1. Praha: Europa-Sobotáles, 2004, 400 s. ISBN 80-86706-08-7

KŘEČEK, S., et al.: Příručka zabezpečovací techniky. 3.vydání, Blatná : Cricetus, 2006. 313 s. ISBN 80-902938-2-4

MEGGELEN, Jim Van, Jared SMITH a Leif MADSEN. Asterisk: the future of telephony. 1st ed. Sebastopol, Calif.: O'Reilly, 2005, 176 s. ISBN 978-059-6009-625.

UHLÁŘ, Jan. Technická ochrana objektů. Vyd. 1. Policejní akademie české republiky, 2005, 229 s. ISBN 80-725-1189-0

Předběžný termín obhajoby

2015/16 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 20. 1. 2015

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 4. 2015

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 23. 03. 2016

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že diplomovou práci na téma: „Spolehlivost telefonních komunikátorů systémů PZTS“ jsem vypracoval samostatně pod vedením pana Ing. Zdeňka Votruby Ph.D., s použitím literárních pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje diplomová práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

V Praze dne 30. 3. 2016

.....

Petr Beneš

PODĚKOVÁNÍ

Rád bych touto cestou poděkoval panu Ing. Zděnku Votrubovi, Ph. D. za odbornou pomoc, vedení, cenné rady a připomínky při zpracování této DP. Dále bych chtěl velmi poděkovat za ochotu, vstřícnost a poskytnuté informace panu Bohumilu Vrbovcovi ze společnosti T SECURITY, s. r. o., panu Pavlu Čížkovi ze společnosti PALMAFONE, a. s., panu Martinu Pochopovi ze společnosti Šindy, a. s. a panu Ing. Martinu Kavaliérovi zs společnosti PKE ČR s. r. o.

Abstrakt: Cílem této práce je posoudit a prakticky ověřit spolehlivost a bezpečnost komunikátorů z pohledu možného napadení zabezpečovacího systému, který je připojen prostřednictvím telefonní linky na PCO. Jelikož samotný PZTS bez připojení na PCO je pouze akusticko - optické signalizační zařízení, které neřeší komplexní ochranu majetku a nemusí zcela odradit potencionálního pachatele při vnikání do střeženého objektu. V teoretické části jsou popsány jednotlivé přenosové cesty přístupové telefonní sítě, principy komunikace mezi PZTS a PCO, spojovací systémy a jejich signalizace. Dále jsou definována úskalí přenosových cest a jejich možná napadnutelnost. V praktické části je podrobně popsána realizace jedné z možných technik napadení. Tato práce volně navazuje na autorovu Bakalářskou práci „Napadení systémů PZTS pomocí telefonních komunikátorů“ z roku 2014. Práce v žádném případě neslouží jako návod a podklad ke schvalování a páchání trestné činnosti.

Klíčová slova: PZTS, datové přenosy, komunikace, bezpečnost

Reliability of telephone dialer in I&HAS

Abstract: The aim of this study is to evaluate and practically verify the reliability and safety of communicators from the perspective of a potential attack on the security system connected through a telephone line to the ARC (Alarm Receiving Centre). The Intruder and Hold-up Alarm System (I&HAS) itself without being connected to the ACR, is actually an acoustical optical signaling device which does not deal with the comprehensive protection of property and may not fully discourage a potential offender from entering a guarded object. The theoretical part describes the individual transmission paths of the access telephone network, the principles of communication between the I&HAS and ARC, the connection systems and their signaling. The pitfalls of the transmission paths and the possibility of their attack are also defined. The practical part describes the implementation of one of the possible techniques of attack in detail. This paper is an independent continuation of the author's Bachelor's thesis "Attack of I&HAS systems through telephone communicators" from 2014. In no way this paper does not serve as a basis for approving and committing crimes.

Keywords: I&HAS, data transmission, communication, security

Obsah

1 Úvod

Telefonní komunikátory systémů PZTS úzce souvisí s telekomunikačními přenosovými a spojovacími systémy. Cílem práce je poukázat na opomíjenou problematiku telefonních komunikátorů zabezpečovacích ústředen. Běžně dostupná literatura se obecně nezabývá spolehlivostí nebo možnostmi napadení zabezpečovacích systémů, principy telekomunikací jsou v oblasti PZTS (Poplachové zabezpečovací a tísňové systémy) brány jako černá skříňka, která je však podstatnou součástí celku.

Přesné počty objektů připojených pouze pevnou telefonní linkou firmy provozující PCO (pulty centralizované ochrany) z bezpečnostních důvodů nezveřejňují, mělo by se jednat řádově o tisíce objektů. Společnost O2[1] dle výroční zprávy za rok 2015, vydané v únoru 2016, zveřejnila, že fixní hlasové linky využívá celkem 840 tisíc zákazníků.

S rychlým vývojem zejména v oblasti elektrotechnického, počítačového a strojírenského průmyslu, za pomoci rozvoje automatizace a robotizace napříč průmyslovými odvětvími, se za posledních 25 let staly elektrotechnické, strojírenské výrobky a zařízení výrazně dostupnějšími pro širokou veřejnost. Vyvíjí se i samotná zabezpečovací technika, ale naproti tomu, není již problém rychle, levně sehnat a sestavit téměř cokoliv, někdy i s minimálními odbornými znalostmi. V dřívějších dobách bylo pro některé jedince nemyslitelné vlastnit, natož pak navrhnout a jednoduše vyrobit například rušičku signálu, kterou lze v současné době zakoupit za několik tisíc korun prostřednictvím internetu. Stejně tak je možné zakoupit různé vybavení na překonání mechanických zábranových systémů, které by bylo jinak pracné zhotovit bez potřebného vybavení a znalostí, například metalurgie a strojírenství. Vybavení je možné volně zakoupit v internetovém obchodě například na: http://www.locksmith.cz.

Rovněž běžně dostupná výpočetní technika nabízí v současné době, za přispění volně dostupných informací na internetu a nepřeberného množství volně šiřitelného software, tzv. freeware, široké možnosti využití.

V teoretické části práce jsou popsány varianty telefonního připojení, principy přenosu zpráv a komunikace mezi PZTS a PCO. Z důvodu rozsáhlosti telekomunikační techniky a jejích podoborů, zejména spojovací, sdělovací a přenosové techniky, je tato práce zaměřena na nejdůležitější principy přenosu, související s nedostatky ve spojení telekomunikační a zabezpečovací techniky, a jsou uvedeny možné způsoby jejich zneužití. Autor této práce vychází z poznatků a teoretických možností, které uvádí v jeho bakalářské práci. V praktické části práce jsou realizovány vybrané techniky napadení telefonního komunikátoru pomocí telekomunikačního systému.

[1] Společnost O2 Czech Republic a.s. se v roce 2015 rozdělila na dvě části, vznikla tak nová společnost CETIN (Česká telekomunikační infrastruktura a. s.), která převzala technickou infrastrukturu. Přístupovou síť spravují subdodavatelé, převážně společnosti Šindy a. s., a TEMO-TELEKOMUNIKACE a. s.

Pro tento účel byl s využitím softwarové telefonní ústředny Asterisk vytvořen generátor telefonních hovorů a vlastní přijímací pult „PCO“. Před vyvoláním, i v průběhu poplachu, bude telefonní komunikátor prostřednictvím generátoru hovorů atakován příchozími hovory takovým způsobem, aby mu byla znemožněna odchozí komunikace a zamezena možnost kontaktovat PCO předáním poplachové zprávy. Tento princip je znám pod pojmem TDoS (Telephony Denial of Service Attack), distribuovaný telefonní útok, který se se současnými technickými nástroji stává více reálný. Je obdobou známého DDoS (Distributed Denial of Service Attack).

Celá situace je nejprve nasimulována a ověřena v privátní telefonní síti VoIP, především z důvodu potřeby odhadu frekvence a objemu generovaných hovorů v závislosti na čase, následně je proveden praktický test pro ověření chování generátoru v reálné telefonní síti. Cílová PZTS je připojena pevnou telefonní linkou od O2, zdrojové linky generátoru (*trunk*) jsou navázány prostřednictvím VoIP operátora Palmafone. V práci je také naznačen způsob zcela anonymní realizace výše zmíněného útoku. Dále je také v této práci ověřena možnost podvrhnutí přenosové zprávy pomocí SW PBx (Private Branch eXchange) Asterisk Veškeré testy jsou samozřejmě prováděny legálně s ohledem na legislativu. Závěr práce obsahuje shrnutí a výsledky testů.

2 Historie

Již od pradávna se člověk potřeboval chránit a předcházet případnému ohrožení. S potřebou bezpečí, ochrany života a majetku úzce souvisí i potřeba signalizovat, předat informaci a přivolat pomoc. Tyto potřeby jsou stejně staré jako lidstvo samo a jsou jedny z tradičních oborů lidské činnosti, které se neustále vyvíjejí.

Po objevu elektřiny byl v roce 1844 přelomovým vynálezem telegraf pana Samuela Morse, který byl v roce 1847 použit pro signalizaci nebezpečí před požárem ve městě New York. Tato aplikace měla pozitivní dopady na zkrácení doby předání informace. Elektrický zabezpečovací systém byl vynalezen o dvacet let dříve než telefon. První elektrický zabezpečovací systém nechal v roce 1853 patentovat pan Augustus Pope. Svůj patent v roce 1857 prodal obchodníkovi panu Edwinovi T. Holmsovi, který jej neustále zdokonaloval a už v roce 1858 uvedl do provozu první centrály elektrické ochrany, které dnes nazýváme „pulty centralizované ochrany“. Roku 1876 se Alexander Graham Bell domluvil s Edwinem Holmesem a k otestování svého telefonu využil již hotových zabezpečovacích rozvodů. Telekomunikace tedy vděčí za svůj rozvoj právě vynálezu zabezpečovací techniky. Edwin Holms vynalezl první telefonní kontakt a v roce 1877 vybudoval první komerční telefonní ústřednu.[1]

Na území bývalého Československa se první nasazení zabezpečovacího systému datuje k roku 1933, větší rozmach nastal v 50. letech dvacátého století.[2]

Už v roce 1882 se u nás v Praze objevila první telefonní ústředna se spojovatelkou, první telefonní seznam téhož roku měl 98 účastníků. V roce 1908 měla ústředna v Jindřišské ulici 6 000 telefonních přípojek. Největší počet telefonních linek, téměř čtyři milióny byl v ČR zaznamenán v roce 2001. Počet aktivních SIM karet překročil počet pevných linek už v roce 2000.[3]

3 Statistika kriminality krádeží vloupáním v ČR

Podle statistik Policie České republiky (PČR) za poslední dva roky výrazně ubylo krádeží vloupáním (trestní zákoník č. 40/2009 Sb. § 205). Hodnota z roku 2013 je pravděpodobně ovlivněna amnestií, kterou 1. ledna 2013 vyhlásil exprezident Václav Klaus. Samotná statistika PČR je podrobnější a dále se dělí například podle počtu vloupání v jednotlivých v krajích, konkrétních lokalitách, typů objektů, časového období, podle pohlaví, věkových skupin atp.

Objekty PČR rozděluje do 15 kategorií, v tabulce č. 1 je celkový přehled krádeží vloupáním do všech objektů za období let 2010 – 2015, který je sestavený z ročních statistik PČR. V tabulce jsou také uvedeny celkové roční finanční škody a jejich podíl na jedno vloupání. [4]

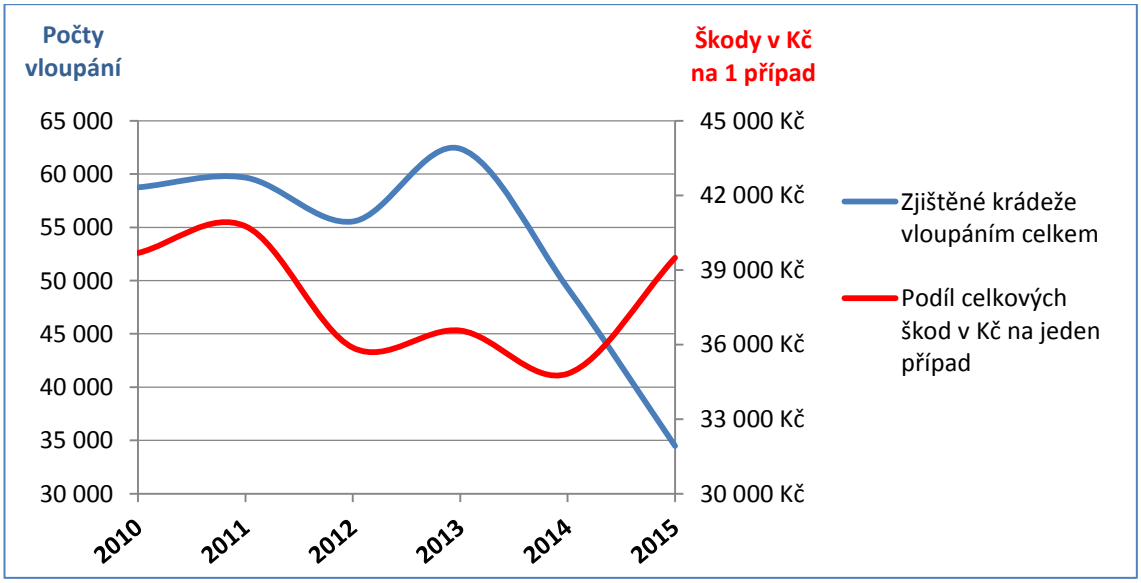
Tabulka 1: Statistiky PČR, krádeže vloupáním v letech 2010 – 2015

Zjištěné krádeže vloupáním do objektů	2010	2011	2012	2013	2014	2015
Zjištěné krádeže vloupáním celkem	58 758	59 672	55 554	62 384	49 304	34 476
Škody (v tis.) Kč celkem:	2 331 750	2 432 184	1 992 898	2 280 919	1 717 078	1 361 501
Podíl celkových škod v Kč na jeden případ	39 684 Kč	40 759 Kč	35 873 Kč	36 563 Kč	34 826 Kč	39 491 Kč

[Zdroj: 4]

Hodnoty tabulky č. 1 jsou znázorněny v grafu č. 1, ze kterého je patrné, že celkový podíl krádeží vloupáním od roku 2013 rapidně klesá. Naproti tomu škody na majetku v přepočtu na jeden případ krádeže vloupáním od roku 2014 strmě stoupají. Z toho je možné usuzovat, že pachatelé se začali přednostně orientovat na movitější objekty.

Graf 1: Vývoj krádeží vloupáním u nejvíce napadaných objektů v letech 2010 - 2015



[Zdroj: 4]

4 Poplachové zabezpečovací a tísňové systémy

Poplachové a Zabezpečovací a Tísňové Systémy (PZTS), anglicky Intruder and Hold-up Alarm System (I&HAS) jsou v současné době dva samostatné obory, které jsou definovány příslušnými normami.

Rozdělení systémů:

1) Poplachový Zabezpečovací Systém (PZS) - IAS (Intruder Alarm System)
2) Poplachový Tísňový Systém (PTS) - HAS (Hold-up Alarm System)

Důležité normy:

- ČSN EN 50131-1 - Poplachové zabezpečovací a tísňové systémy
- ČSN EN 50136 - Poplachové přenosové systémy a zařízení
- ČSN EN 50134 - Poplachové systémy – Systémy přivolání pomoci
- ČSN EN 50131-3 - Poplachové zabezpečovací a tísňové systémy - Ústředny

4.1 Obecná charakteristika PZTS

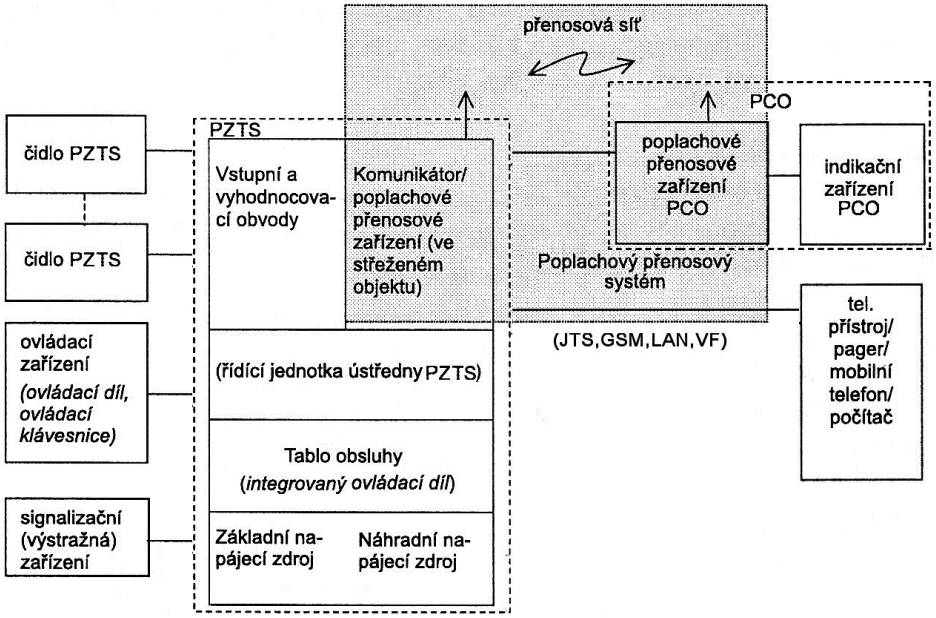
Systém PZTS lze charakterizovat jako soubor prvků, který je schopen akusticky a opticky signalizovat například pokus o narušení střeženého objektu na určeném lokálním nebo vzdáleném místě. Systém je vždy složen z několika prvků, které plní specifické funkce. Základními prvky jsou samotná ústředna PZTS, přenosové prostředky, čidla (detektory), signalizační zařízení a doplňková zařízení.

Ústředna přijímá a vyhodnocuje informace o stavech čidel, indikuje narušené smyčky, poruchové stavy, inicializuje přenos informací, umožňuje napájení ostatních komponent a provádí diagnostiku. Ovládá signalizační, poplachové a doplňkově prostředky, například komunikátor. Může také ovládat elektromechanické a elektromagnetické zámky či jiná elektrická zařízení. Získané informace o stavech zpracovává podle předem definovaných rozhodovacích pravidel. Nastavení vlastností PZTS a konfigurace lze definovat nebo měnit a je závislé na programových možnostech a vnitřním vybavení konkrétního typu daného výrobce.

Čidlo (detektor) reaguje na fyzikální změny a jevy, nežádoucí manipulaci. Signalizační zařízení opticky nebo akusticky vyhlašuje poplach nebo výstrahu. Doplňková zařízení zajišťují další speciální funkce nebo usnadňují ovládání. HW ústředny PZTS tvoří deska plošných spojů, osazená elektrotechnickými součástkami, svorkovnicemi a konektory. Deska je zpravidla umístěna v plastové nebo plechové skříni společně s napájecím zdrojem a záložní baterií. Vnitřní uspořádání ústředny PZTS se u jednotlivých výrobců liší nejen interním provedením, ale i programovými možnostmi. Na desce je vždy umístěna mikroprocesorová řídící jednotka, vstupní a vyhodnocovací obvody a případně i komunikátor. Ostatní obvody

mohou být volitelné v podobě samostatných modulů, s jejichž pomocí lze ústřednu rozšiřovat a přizpůsobit potřebám daného objektu. Patří sem například JTS, GSM a LAN komunikátory dále přídavné moduly vstupů, univerzální moduly výstupů a radiový modul bezdrátových periférií. Blokové schéma vnitřního uspořádání systému PZTS je uvedeno na obrázku č. 1.[1]

Obrázek 1: Schématické znázornění systému PZTS



[Zdroj: 1]

Ústředna se před uvedením do provozu musí nastavit tak, aby definovaná pravidla odpovídala konkrétní instalaci, objektu. Konfiguraci ústředny je možné provádět přes připojenou klávesnici, která nás také informuje o stavech ústředny a v neposlední řadě slouží k ovládání systému, nejčastěji zastřežení/odstřežení.

Novější typy ústředen lze konfigurovat pomocí PC, v němž je nainstalován software, který je dodávaný přímo výrobcem systému. Některé modely umožnují také vzdálenou správu přes webové rozhraní. V tomto případě je však potřeba, aby ústředna byla vybavena také komunikátorem. Ovládání systému je možné provádět i pomocí RFID (Radio Frequency Identification) čipu, dálkového ovladače, SMS příkazem nebo zavoláním do hlasového automatu, kterým disponuje komunikátor ústředny. Někteří výrobci umožňují nově uživatelům částečné ovládání a kontrolu pomocí mobilní aplikace v chytrém telefonu.

4.2 Základní rozdělení ústředen PZTS

Obecně lze dělit ústředny PZTS podle stupně zabezpečení, počtu smyček a způsobu připojování smyček. [1]

Podle stupně zabezpečení:

- nízké - stupeň zabezpečení (1)
- nízké až střední - stupeň zabezpečení (2)
- střední až vysoké - stupeň zabezpečení (3)
- vysoké - stupeň zabezpečení (4)

Rozdělení podle počtu smyček:

- malé (1 – 5 smyček)
- střední (6 – 12 smyček)
- velké (více jak 12 smyček)

Podle způsobu připojení smyček:

- drátové
- sběrnicové
- bezdrátové
- hybridní

4.3 Stupně zabezpečení

Norma ČSN EN 50131-1 a oborové předpisy pojišťoven stanovují kritéria na funkčnost systémů PZTS podle níže uvedených hledisek:[1]

- přístupové úrovně
- provozování
- vyhodnocení
- detekcí
- napájení
- zabezpečení proti sabotáži
- monitorování
- propojení
- záznamu událostí

V následující tabulce č. 2. je v levé části zobrazeno rozdělení objektů podle tříd prostředí dle ČSN EN 50131-1, které je potřeba brát v úvahu při návrhu zabezpečení pro konkrétní objekt. Národní bezpečnostní úřad (NBÚ) přiřazuje typům technických prostředků vlastní kategorie. Stupeň rizika č. 1 není tímto úřadem vůbec certifikován, viz pravá část tabulky.

Tabulka 2: Stupně zabezpečení dle ČSN a NBÚ

ČSN 50131-1		Předpokládaný typ narušitele	NBÚ			
Stupeň	Riziko		TYP tech. prostředku PZTS	do 31. 12. 1999	od 1. 1. 2000	Bodová hodnota
1	nízké	Předpoklad je, že narušitel má malou znalost PZTS a omezený sortiment dostupných nástrojů (chaty, byty, rodinné domy, garáže).	-	-	-	-
2	nízké až střední	Narušitel má již určité znalosti o PZTS, ale omezený sortiment základních přenosných přístrojů, například multimetr (komerční objekty).	**Typ 2**	DŮVĚRNÉ	D	2 body
3	střední až vysoké	Narušitel je obeznámen s PZTS, má úplný sortiment základních přenosných přístrojů a elektronických zařízení (zbraně, ceniny, informace, narkotika).	**Typ 3**	PŘÍSNĚ TAJNÉ	T	3 body
4	vysoké	Narušitel je schopen nebo má možnost zpracovat podrobný plán vniknutí, má kompletní sortiment zařízení včetně prostředků pro náhradu rozhodujících prvků PZTS (zejména objekty národního a vyššího významu).	**Typ 4**	-	PT	4 body

[Zdroj: 1]

4.4 Způsoby předání poplachové signalizace

Způsoby předání poplachové signalizace je možné u PZTS rozdělit do tří kategorií na lokální, autonomní a dálkovou.[2]

Lokální signalizace: je akustická nebo optická, či jejich kombinace, a nachází se v chráněném prostoru nebo jeho těsné blízkosti. V případě poplachu plní funkci preventivní a informační. Preventivní funkce představuje v praxi akustickou signalizaci tzv. „signalizace na náhodu“, a předpokládá se, že pachatel uteče nebo zareaguje náhodný občan zavoláním na PČR.

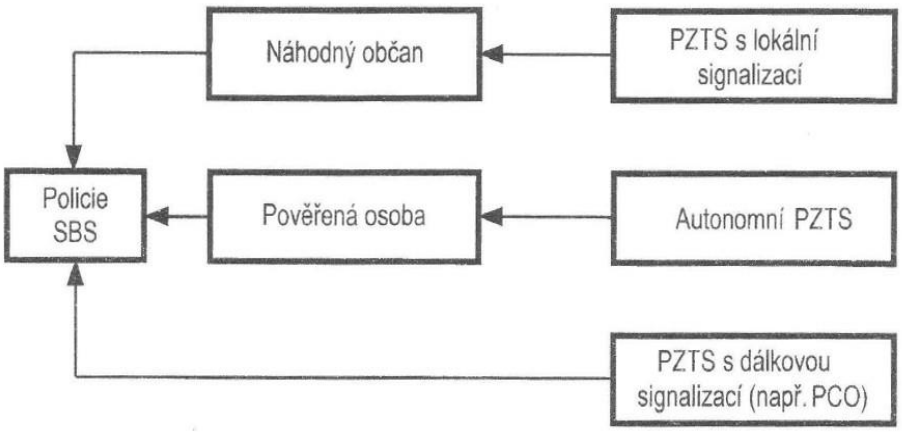
Jednou z možností je i vyvedení poplachového signálu PZTS k pověřené osobě například pomocí automatického telefonního komunikátoru, který v případě poplachu předá telefonickou zprávu policii nebo majiteli objektu, může se také jednat o tzv. volání do kapsy. Informační funkce je možnost pověřené osoby nebo náhodného občana vzdáleně pozorovat pachatele. Takováto informace může vést k dopadení pachatele.[2]

Autonomní signalizace: je akusticko-optická signalizace zakončena u stálé služby, hlídače, který se nachází v objektu a zároveň reaguje na signál nebo může provést zákrok.[2]

Dálková signalizace: má výstup vyveden u stálé služby, která má smluvní vztah s majitelem nebo uživatelem objektu. Služba provádí dozorování a případně i zákrok na objektu a ve většině případů se jedná o dohledové centrum, zvané Pult Centralizované Ochrany (PCO).[2]

Na obrázku č. 2 jsou blokově znázorněny způsoby předání poplachové informace, která je předána PČR nebo soukromé bezpečnostní službě (SBS).

Obrázek 2: Schéma způsobu předání poplachové informace



[Zdroj: 2]

5 Systémy centralizované ochrany

Systémy centralizované ochrany (SCO) tvoří objekty, které jsou samy chráněny PZTS a zároveň soustřeďují poplachové signály od vzdálených PZTS do jednoho centra, na pulty centralizované ochrany (PCO). Vytvoření SCO zahrnuje vedle výstavby vlastního PCO dle norem ještě mnoho dalších opatření, například zásahovou dokumentaci, kvalifikovanou výjezdovou skupinu, která podmiňuje efektivní provoz celého systému. Momentálně se pro PCO používá nové označení „Dohledové a Poplachové Přijímací Centrum (DPPC). V této práci bude však nadále používána více zažitá zkratka PCO. V současnosti se na území ČR nachází okolo 200 soukromých firem provozujících PCO. Každé PCO však není zcela identické, liší se technickým vybavením, velikostí i kvalitou služeb. Na největší PCO v ČR jsou připojeni řádově desítky tisíc zákazníků. Vedle soukromých firem existují také PCO, která jsou provozována PČR nebo obecní (městskou) policií. [2]

Na pulty PČR jsou připojovány zejména významné objekty s vyššími riziky, jako například banky, kulturní památky, jaderná zařízení. O napojení objektu rozhoduje zpravidla ředitel PČR daného okresu nebo města, ve kterém jsou pulty umístěny nebo obsluhovány. Informace o napojených objektech podléhají utajení, zásah na objektu je bezplatný. Pulty obecní (městské) jsou zpravidla zřizována u center tísňového volání (CTV), která slouží pro záchranné složky. Připojují se pouze zcela nekomerční objekty, které jsou majetkem města a neslouží ani částečně ke komerčním účelům, připojení si hradí provozovatel daného objektu.[2]

5.1 Pult centralizované ochrany

Samotná PZTS je vlastně akusticko - optické signalizační zařízení, které neřeší komplexní ochranu majetku. PZTS je například vybavená pouze sirénou a tudíž nemusí potencionálního pachatele zaručeně odradit. Je tedy vhodné, aby objekt vybavený PZTS, ve kterém se nenachází stálá služba a pokud ano, tak pro její zálohu, byl připojen k PCO. V praxi je tedy vhodná kombinace dálkové a lokální signalizace.

PCO je dispečerské pracoviště se stálou obsluhou 24 hodin denně, slouží jako centrum pro příjem a vyhodnocování zpráv ze střežených objektů, PZTS. Moderní PCO musí být z důvodu bezpečnosti samo zabezpečeno, monitorování provádí jiná firma provozující služby PCO. Kromě poplachových a tísňových zpráv se nejčastěji na PCO přenášejí pravidelné kontrolní zprávy z objektů. Pro přenos zpráv z PZTS na PCO je využíváno několik různých přenosových cest: JTS (Jednotná Telekomunikační Síť), GSM (Global System for Mobile Communication), WAN (Wide Area Network) a radiová síť.

Požadavky na provozovatele PCO stanovují příslušné vyhlášky a normy. Od roku 2011 je pro dohledová a poplachová centra platná norma ČSN EN 50518. Norma vymezuje požadavky, které musí provozovatelé splnit a je složena celkem ze tří částí:

- **ČSN EN 50518 - 1** Dohledová a poplachová přijímací centra – Část 1: Umístění a konstrukční požadavky
- **ČSN EN 50518 - 2** Dohledová a poplachová přijímací centra - Část 2: Technické požadavky
- **ČSN EN 50518 - 3** Dohledová a poplachová přijímací centra - Část 3: Pracovní postupy a požadavky na provoz

ČSN EN 50518 - 1: Norma stanovuje například minimální požadavky na návrh, konstrukci a zařízení pro budovy, ve kterých má probíhat monitorování, příjem a zpracování signálů (zpráv) z PZTS. Dohledové centrum musí splňovat předepsané tloušťky obvodového zdiva, výplně oken s balistickou a protipožární odolností. Musí být vybaveno zařízením na detekci plynu, automatizovanou zálohou napájení atp.

Požadavky se vztahují také na dálkovou konfiguraci, v nichž například více systémů může přenášet informace do jednoho nebo více přijímacích center. Dále na případy jediného centra určeného pro monitorování a zpracování poplachů generovaných jedním nebo více poplachovými systémy nalézajícími se v témže perimetru příslušného místa.[5]

ČSN EN 50518 - 2: V normě jsou stanoveny požadavky na příjem signálu, pravidla komunikace, ochrany osobních údajů, postupy pro dispečera a pravidla pro nouzový provoz. Dále norma stanovuje požadavky na čas pro příjem a zpracování signálu přijímacího systému, který musí splňovat tato kritéria:[6]

- Tísňové zprávy musí být zpracovány do 30 [s] u 80 % přijatých zpráv, a nejpozději do 60 [s] u 98,5 % přijatých zpráv
- Všechny ostatní poplachy musí být zpracovány do 90 [s] a to u 80 % přijatých zpráv a nejpozději do 180 [s] u 98,5 % přijatých zpráv

ČSN EN 50518 – 3: Tato část normy stanovuje požadavky na postupy, provoz, povinnosti a personální obsazení. Dále sem patří požadavky na výcvik, odbornou způsobilost, bezpečnostní prověření, správu databází, pracovní dokumentaci, údržbu, evakuační postupy, likvidaci údajů, roční kontrolní audit a v neposlední řadě počty operátorů, kteří musí být neustále přítomni.[7]

5.2 Přijímací zařízení PCO

Zpráva z PZTS je na PCO přijata autonomním přijímacím zařízením - „pultem“, zařízení pro příjem zpráv může být také integrované v PC ve formě rozšiřujících hardwarových karet. Přijímací pulty využívají pro komunikaci různé typy přenosových technologií. Například s PCO JABLOTRON SECURITY, a. s., komunikuje přes 80 % všech připojených objektů pomocí GSM/GPRS technologie. Princip přenosu na PCO s nejvíce využívanými přenosovými technologiemi je blokově znázorněn na následujícím obrázku č. 3.

Obrázek 3: Princip přenosu na PCO

[Zdroj: Vlastní]

Autonomní pult je hardware s řídící mikroprocesorovou jednotkou, který je osazen vstupy pro technologie JTS, GSM, IP (WAN), případně jejich kombinacmi. Pult přímo zpracovává přijatá data z PZTS a je schopen samostatného provozu nebo komunikuje s řídícím serverem, jehož součástí je databáze, sloužící pro ukládání a archivaci zpráv. Autonomní pulty mohou být vybaveny tiskárnou a LCD displejem, z něhož lze přímo odečítat data o stavu pultu i zprávy z objektů v číselném formátu.

Designové zpracování hardware se liší dle výrobce, může být i v rackovém provedení. Pult v PC typu ATX je osazen jednou nebo více integrovanými kartami pro příjem zpráv z JTS, GSM, a IP (WAN) sítě. Karty se připojují na sběrnici ISA, PCI, případně jsou zhotoveny jako externí zařízení s možností připojení přes USB, RS232 atp. Data z objektu jsou přenášena v číselném formátu, v řídícím serveru se k těmto datům přiřadí i popisky, které byly do databáze na serveru zadány pověřenou osobou při převzetí nového objektu. Přiřazená data obsahují informace jako jméno, adresu, kontaktní údaje oprávněných osob, přístupové cesty k objektu, popis smyček, atp.

Pulty dle výrobců disponují širokou škálou nastavení a je pouze na jejich provozovatelích zda je využijí. Poplachové zprávy z objektů se většinou zpracovávají v došlém pořadí, nebo podle přiřazených priorit. Neúplné přenosové zprávy nejsou zaznamenávány a předávány ke zpracování. Z důvodu náhodných nebo zlomyslných volání (obsazování linek), je možné u pultů nastavit dobu vyzvednutí po přijetí hovoru. Každé PCO toto řeší individuálně, běžně se tyto časy pohybují mezi 30 – 120 [s].

Počítač operátora (klient) PCO je vybaven speciálním monitorovacím softwarem, který komunikuje s řídícím serverem. Přijaté zprávy se spolu s dalšími údaji o objektu přehledně zobrazují na monitoru klientské stanice. Operátor (dispečer), který přijal zprávu z objektu, se řídí vnitřními pravidly PCO v závislosti na sjednaných službách objednaných zákazníkem a provádí patřičné kroky.

Například v případě poplachu z objektu vyšle na místo zásahové vozidlo s výjezdovou skupinou, která provede kontrolu objektu a případné zajištění pachatele. Poté operátor

telefonicky kontaktuje zákazníka a informuje ho o vzniklé situaci. V případě zjištěného pachatele operátor informuje PČR a zásahová jednotka vyčká na místě, dokud PČR nedorazí. Dále se ještě čeká do příjezdu poškozeného zákazníka. Některá PCO komunikují přímo s výjezdovou skupinou, která tak zároveň supluje funkci operátora a celý proces je tako mnohem pružnější. Případně se využívá kombinace obojího. Moderní bezpečnostní centrum je v případě výpadku energetické sítě plně soběstačné, napájení důležitých elektrických spotřebičů a HW vybavení zajišťují záložní zdroje (baterie), dostatečnou zálohu ještě tvoří diesel agregáty.

6 Komunikační protokoly - přenosové formáty

Komunikační protokoly slouží k přenosu zprávy z PZTS (objektu) na PCO, usnadňují identifikaci objektu a lze pomocí nich rozlišit ID objektu konkrétní události, sekce a zóny. Zpráva se skládá z posloupnosti číselných kódů oddělených mezerami. Obsažená informace ve zprávě závisí na použitém přenosovém formátu zprávy, na výrobci a případně vnitřních pravidlech PCO. U PZTS lze nastavit ID objektu, číslo zóny a kódy událostí, přičemž některé kódy mohou být již přednastaveny výrobcem.

Komunikačních protokolů je velké množství a jejich vývoj úzce souvisí s vývojem telekomunikační sítě. Můžeme je rozdělit do dvou skupin na pulsní a tónové DTMF (Dual Tone Multi Frequency). Pulsní formát je univerzální a historicky starší, DTMF formát je rychlejší, začal se využívat s příchodem digitalizace telefonní sítě.

6.1 Impulsní přenosové formáty

Telefonního číslo se vytáčí přerušováním účastnické smyčky. Doba přerušení smyčky je 62 [ms], doba propojení smyčky je 38 [ms], max. počet impulsů za 1 [s] je 10. Tento počet se generuje vytočením nuly, přenosová rychlost se udává v bps (bits per second).

Impulsní volbu by bylo možné nalézt také u některých starších instalací, kde byla pro zálohu telefonní linky použita analogová GSM brána, která pro přenos zprávy používala hovorové pásmo, ve kterém při použití DTMF docházelo ke zkreslení. Impulsní formáty lze rozdělit na rozšířené a nerozšířené. Rozšířený formát přenáší 15 a více kódů. Vzniká rozšířením stávajícího kódu z předchozího oběhu dat, čímž se získá dvoumístný hlásící kód. Může být přenášen s paritou (dva oběhy dat), nebo bez parity (čtyři oběhy dat).[8]

Celkem existuje 15 operačních kódů, přičemž každý z nich může mít až 15 zónových nebo uživatelských identifikátorů. Parita znamená číslo, které je zahrnuto ve zprávě, ovšem není programovatelné, generuje se automaticky a ve zprávě se přenáší navíc pouze jedno číslo. Pomocí paritního čísla se ověřuje úplnost přenášené zprávy. Využití paritního čísla je rychlejší, oproti přenosu bez parity, protože zkracuje celkovou dobu přenosu.

Pokud PCO vyhodnotí, že paritní číslo je korektní, uzná přenos za platný a ukončí přenos. Paritní číslo získáme součtem samostatných číslic například, součtem čísel 123 31 dostaneme výsledné číslo 10. Odečteme jej od nejbližšího násobku čísla 15, tzn. 15 – 10 = 5. Výsledkem je paritní číslo 5, tzn., že přenášený kód bude vypadat následovně: 123 31 5. Rozšířené hlášení se používalo, pokud bylo potřeba při obnově zastřežení/odstřežení identifikovat uživatele nebo zónu.[8]

Příklad rozšířeného formátu (3x2 nebo 4x2):

AAA EZ nebo AAA EZ, kde AAAA je tří nebo čtyřmístné číslo, E – programovatelný operační kód, Z – identifikátor zóny případně uživatele, druhý programovatelný kód. Impulsní přenosové formáty se dělí na: [8]

Nerozšířené (Extended):

- ADEMCO SLOW, SILENT KNIGHT: 10 bps, HANDSHAKE 1400 [Hz], 3x1, 4x1, 4x2
- DCI, FRANKLIN, SESCOA, VERTEX: 20 bps, HANDSHAKE 2300 [Hz], 3x1, 4x1, 4x2
- RADIONICS: HANDSHAKE 2300/1400 [Hz], 3x1, 4x2 (s paritou/bez parity)
- SILENT KNIGHT FAST: 20 bps, 1400 [Hz] HANDSHAKE, 3x1

Rozšířené:

- ADEMCO SLOW, SILENT KNIGHT: 10 bps, HANDSHAKE 1400 [Hz], 3x1
- DCI, FRANKLIN, SESCOA, VERTEX: 20 bps, HANDSHAKE 2300 [Hz], 3x1
- RADIONICS: HANDSHAKE 2300/1400 [Hz], 3x1 (s paritou/bez parity)
- SILENT KNIGHT FAST: 20 bps, HANDSHAKE 1400 [Hz], 3x1, 4x1 a 4x2

6.2 Přenosové formáty – DTMF

DTMF tónová volba se přenáší v hovorovém pásmu, které má šířku 300 – 3400 [Hz]. Tvoří ji celkem šestnáct znaků, deset číslic a šest nenumerických znaků. Každému znaku je přiřazena dvojice tónů, jejich křížovou kombinací dostaneme výslednou frekvenci tónu. Na obrázku č. 4 je znázorněna DTMF klávesnice, která je schválena podle ITU-T (International Telecommunication Union – Telecommunication).[9]

Obrázek 4: DTMF klávesnice

	1209 [Hz]	1336 [Hz]	1477 [Hz]	1633 [Hz]
697 [Hz]	1	2	3	A
770 [Hz]	4	5	6	B
852 [Hz]	5	8	9	C
941 [Hz]	*	0	#	D

[Zdroj: 9]

V následující tabulce č. 3 je uvedena skladba DTMF používaná u přenosového formátu ADEMCO CID, která využívá pouze 15 dvojic tónů.

Tabulka 3: Frekvence DTMF tónů ADEMCO CID

Frekvence DTMF tónů ADEMCO CID														
697	697	697	770	770	770	852	852	852	941	941	941	697	770	852
1209	1336	1477	1209	1336	1477	1209	1336	1477	1336	1209	1477	1633	1633	1633
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A, 0**	**B (*)**	**C (#)**	**D**	**E**	**F**

[Zdroj: 10]

6.2.1 Přehled DTMF formátů

- ADEMCO 4x1, 4x2 Express
- ADEMCO Contact ID
- FBII Superfast 4x3x1
- SIA

6.2.2 ADEMCO Contact ID

Je hodně používaný DTMF protokol pro přenos zpráv pomocí telefonní linky, přenáší více informací a kromě zóny poplachu obsahuje i typ zóny. Formát zprávy je přesně stanoven, tvoří jej sekvence tónů vzájemně časově posunutých, které jsou odděleny přesnými mezerami.

Komunikace je složena celkem ze tří částí: [10]

- **Handshake** (tzv. potřesení rukou) začátek komunikace
- **Message** (zpráva) obsah zprávy
- **Acknowledgement** (potvrzení) KISSOFF – potvrzení zprávy, jeden tón

Uspořádání časování: pauza (mezera) před a při posílání dat musí být mezi 250 – 300 [ms], od ukončení uvítacího tónu (HANDSHAKE) nebo po ukončení od potvrzení (KISSOFF).[10]

Handshake: po vyzvednutí linky ho vyšle protistrana (PCO). Slouží pro zahájení přenosu, skládá se ze dvou tónů, vzájemně oddělených mezerou, která má zpoždění od 0.5 max. do 2.0 [s]:[10]

- tón 1400 [Hz] +/-3 %; trvání 100 [ms] +/- 5 %
- pauza trvá 100 [ms] +/- 5 %
- tón 2300 [Hz] +/- 3 %; trvání 100 [ms] +/- 5 %

Message (obsah zprávy): tolerance doby tónu a mezery musí být mezi 50 – 60 [ms]. Nula se vysílá jako číslice 10, v kontrolním součtu zprávy znamená číslo 10 a vizuálně je zobrazována jako číslo 0.[10]

Acknowledgement - Kissoff: frekvence potvrzovacího tónu je 1400 [Hz] o délce 400 [ms], přípustná odchylka v toleranci +/- 3 %, doba trvání tónu musí činit minimálně 750 [ms], maximálně 1 [s].[10]

Časový interval mezi zprávami: vysílač po vyslání zprávy ještě čeká 1.25 [s] na potvrzovací tón. Po obdržení tónu kontroluje délku tónu, která musí trvat minimálně 400 [ms], aby byl přijat za platný. Po přijetí potvrzovacího tónu vysílač čeká na konec tónu dalších 250 až 300 [ms], než začne posílat další zprávu. Pokud není potvrzovací tón do 1.25 [s] detekován, vysílač zprávu znovu zopakuje.[10]

Formát obsahu zprávy u protokolu ADEMCO Contact ID je uveden v následující tabulce č. 4, posloupnost zprávy vypadá takto: **ACCT MT QXYZ GG CCC S**.[10]

Tabulka 4: Obsah zprávy formátu ADEMCO Contact ID

Formát zprávy: ACCT MT QXYZ GG CCC S	
ACCT	4 čísla pro ID objektu (0 – 9, B – F)
MT	typ zprávy pro Contact ID = 18 nebo 98. Nové přijímače preferují 18.
Q	Typ zprávy, 1 = nová událost, otevřeno/nestřeženo, 3 = nová obnova, střežení, zavřeno/střeženo, 6 = již vysílaná zpráva (Status report)
XYZ	kód události (3 hex. čísla 0 – 9, B – F)
GG	Číslo podsystému, skupiny (0 – 9, B – F)
CCC	číslo zóny nebo číslo kódu pro otevřeno / zavřeno (3 hex. čísla 0 – 9, B – F), 000 - znamená, že zónu nebo uživatele nelze určit
S	kontrolní součet vytvořený následovně (součet všech číslic + S) MOD15 = 0

[Zdroj: 10]

6.3 Komunikace mezi PCO a PZTS – Ademco CID

U přenosového formátu Ademco CID obsahuje zpráva ID objektu a kód události. Každá zpráva je komunikátorem PZTS vysílána jednotlivě podle pořadí ve frontě. Níže je popsán přenos zprávy mezi telefonním komunikátorem PZTS a PCO prostřednictvím JTS. Data jsou přenášena formátem Ademco Contact ID v následujícím pořadí:

1) Komunikátor PZTS obsadí telefonní linku

2) Vytočí první naprogramované telefonní číslo

3) Pult vyzvedne hovor a vyšle, tzv. „pískne“ uvítací tón HANDSHAKE:

- **a)** tón – 1 400 [Hz] (tolerance +/- 5 %)
- **b)** pauza – 100 [ms] (tolerance +/- 5 %)
- **c)** tón – 2 300 [Hz] (tolerance +/- 5 %)

4) Po obdržení HANDSHAKE komunikátor začíná přenášet zprávu

5) Pult provede ověření pomocí kontrolního součtu

6) Jestliže pult vyhodnotí přenos jako platný, vyšle KISSOFF, potvrzovací tón 1400 [Hz] o délce 400 [ms]. Ten se opakuje pro každou zprávu, pokud není komunikátorem potvrzovací tón do 1.25 [s] detekován, zavěsí a vytočí druhé zadané telefonní číslo pro komunikaci. Pokud ani toto není k dispozici, vytočí opět první telefonní číslo. Tento proces se opakuje, dokud nedojde k vyčerpání zadaných pokusů. Čítač pokusů komunikátoru se nuluje vždy po obdržení KISSOFF.

7) Po přijetí potvrzovacího tónu komunikátor čeká ještě 250 až 300 [ms], než začne posílat další zprávu

8) Pokud PZTS nemá další zprávu k přenosu, komunikátor zavěsí

Příklad přenášené poplachové zprávy z objektu, který má identifikační číslo (ID) 2222 a vznikl poplach v podsystému 1 a zóně číslo 15 je uveden v tabulce č. 5.[10]

Tabulka 5: Ukázka zprávy a základní skupiny kódů

Objekt ID 2222 hlásí poplach v podsystému 1 na zóně 15					
Formát odeslané zprávy na PCO - 2222 18 1131 01 015 8					
2222	Objekt ID 2222				
18	Formát zprávy Ademco CID				
1131	1 – Poplach, 131 – Hlídací zóna				
01	Podsystém č. 1				
015	Zóna č. 15				
8	Kontrolní součet: (1+2 + 3 + 4) + (1 + 8) + (1 + 1 + 3 + 1) + (10 + 1) + (10 + 1 + 5) = 52 nejbližší vyšší číslo dělitelné 15 je 60. Výsledek kontrolního: 60 – 52 = 8				
Základní skupiny kódů událostí					
1xx	**2xx**	**3xx**	**4xx**	**5xx**	**6xx**
Lékař	Požár	poruchy	Střeženo/ nestřeženo	Vyřazení / odpojení	Testy
Požár	Voda		Dálkový přístup		
Přepadení	Plyn		Kontrola přístupu		
Narušení	Mimořádný dohled				
Všeobecné					
24 hodin					

[Zdroj: 10]

6.4 SIA DC-09

Norma SIA DC-09 je velice obsáhlá, popisuje komunikaci po IP. Pro přenos zpráv využívá strukturu, ve které lze přenášet i jiné přenosové formáty. V přeneseném slova smyslu tvoří kontejner, do kterého lze zapouzdřit i starší typy komunikačních formátů. Vnitřních typů zpráv je doporučeno zatím 13 ADM-CID, SIA-DCS, SIA-PUL, ADM-42E atd. Přijímače PCO mohou využívat jednotný formát pro zobrazení se strukturou XML (DOM-XML), která může být rozšířena o data objektů z databáze PCO.

Využití lze v praxi najít i pro starší komunikátory, které neumí komunikovat po IP. Jedná se o komunikátor (převodník), který již zvládá komunikaci po IP a lze k němu připojit starší typy PZTS, EPS pomocí telefonního komunikátoru, nebo sběrnice RS 232/485. Tento IP komunikátor je tedy nadřazený a přebírá zprávy z připojených zařízení, které následně předává na PCO po IP. Certifikovaný komunikátor s těmito vlastnostmi dodává v ČR například firma ATISGROUP pod názvem Twincom.

Výhodou SIA DC-09 je sjednocení komunikace PZTS, EPS atd. a výrobců, tato norma se používá v 16 státech EU. Dalšími nespornými výhodami je synchronizace času, obousměrná komunikace, rozšíření možnosti identifikace objektu, například pomocí MAC a IP adresy, minimalizace zneužití, možnost šifrování zpráv, šifrování lze nastavit individuálně i pro konkrétní objekt. Dále mohou zprávy obsahovat upřesnění bloku, kanceláře atp.[11]

Norma SIA DC-09 je velice obsáhlá. Dokument, ve kterém je podrobně popsána má celkem 44 stran. Níže je popsán základní formát zprávy. SIA DC-09.

<LF><CRC><0LLL><"id"><seq><Rrcvr><Lpref><#acct>[<pad>|data][x.data]<timestamp><CR>

LF	vstupní znak - řádek, kódování ASCII přenášen jako binární hodnota 0x0A
CRC	spolu s „CR“ na konci uvozuje zprávu, počítá se z části zprávy od uvození ID, při šifrování se výpočet provede až nakonec, data jsou doplněna náhodně
0LLL	udává délku zprávy, znaky se započítávají stejně jako u „CRC“
"id"	obsahuje použitý formát a informaci zda bylo použito šifrování
seq	číslo přiřazené vysílačem ke každé zprávě, přijímací zařízení odesílá toto číslo zpět
Rrcvr	volitelný prvek, slouží pro možné rozšíření, skládá se z ASCII „R“, následováno 1-6 HEX ASCII čísly. Pokud není ve zprávě využito, nechá se volné
Lpref	předčíslí, slouží pro možné rozšíření identifikace, je složen ASCII znaků „L“ je následováno 1-6 HEX ASCII čísly. Pokud není využito, přenáší se pouze „L0“
#acct	trvale přiřazené ID vysílače, se skládá z ASCII „#“, následuje 3-16 ASCII číslic, nekoresponduje s protokolem DC-07
pad	používá se při šifrování, tak aby násobek byl 16
data	všechna data obsažená ve zprávě včetně znaků „[" a "]“, formát závisí na ID
x.data	umožňuje přidat další informace, začíná vždy znakem ASCII, který označuje typ obsahu pole
timestamp	časové razítko, formát: <_HH:MM:SS,MM-DD-YYYY>, dovolená časová odchylka může být v rozmezí +20/-40 [s]
CR	návratová značka ASCII

7 Přenosové prostředky

Přenosové prostředky umožňují propojení zabezpečovacích systémů k PCO, z pohledu přenosového prostředí je můžeme rozdělit na drátové a bezdrátové. Podle druhu trasy je možné rozdělit přenosové prostředky na:

- přenos přímou linkou (trvalý spoj)
- přenos telefonní linkou (vytáčený spoj)
- přenos bezdrátový (rádiový, optický)
- přenos v IP sítích
- přenos v sítích NN (nízké napětí)

Tato práce je zaměřena především na telefonní komunikátory využívající k přenosu JTS komunikující přes klasickou pevnou telefonní linku nebo její nadstavbové technologie xDSL, ISDN.

V případě přenosu zprávy přes telekomunikační sítě (JTS nebo GSM) je potřeba brát v úvahu, že telefonní operátoři negarantují tzv. „dovolatelnost“. V zákoně o elektronických komunikacích č. 127/2005 Sbírky, § 64 vyúčtování ceny, reklamace, odstavec č. 12 je uvedeno: „*Pokud službu bylo možno využít jen částečně, anebo ji nebylo možno využít vůbec pro závadu technického nebo provozního charakteru na straně podnikatele poskytujícího službu, je tento povinen zajistit odstranění závady a přiměřeně snížit cenu nebo po dohodě s účastníkem, který je koncovým uživatelem, zajistit poskytnutí služby náhradním způsobem. Podnikatel poskytující službu elektronických komunikací není povinen nahradit jejím uživatelům škodu, která jim vznikne v důsledku přerušení služby nebo vadného poskytnutí služby*“.[13]

7.1 Přístupová síť

V ČR se označuje se zkratkou JTS (Jednotní telekomunikační síť) je možné se setkat také s převzatým označením PSTN (Public Switched Telecommunication Networks) což znamená veřejné komutované telekomunikační sítě. Telefonní komunikátory jsou koncovým telekomunikačním zařízením, které je připojeno metalickými kabely s měděnými vodiči (jádry) o průměrech 0,4; 0,6; 0,8 [mm] s polyethylenovou izolací podle normy IEC 60708 zavedena v ČSN EN 60708, historicky se ještě používají kabely s izolací vzduch – papír.

Kabelové vedení od ústředny k účastníkovi by nemělo přesáhnout odpor 20 [Ω] (útlum vedení), čímž je limitována jeho délka. Vedení může být uložené v zemi, kabelových komorách, kolektorech, v některých případech se stále vyskytuje nadzemní „sloupové“ kabelové vedení. Na trase vedení smí být maximálně jeden přechod z menšího průměru jádra do většího směrem od ústředny.

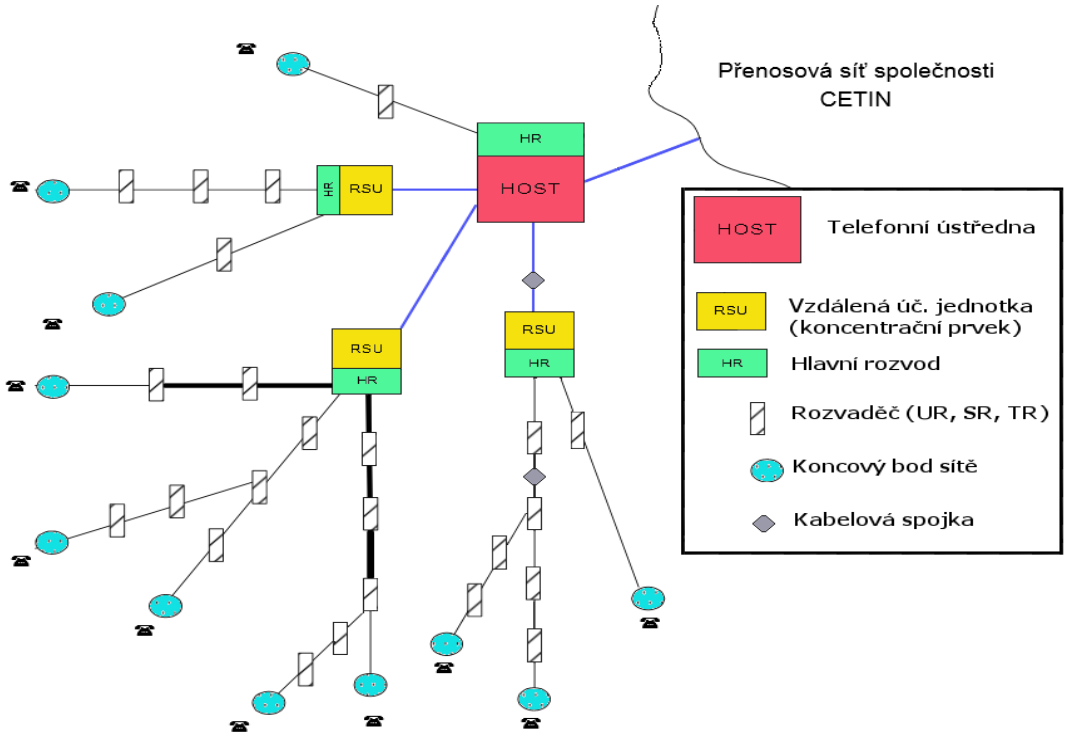
7.1.1 Pevná telefonní síť

Struktura pevné telefonní přístupové sítě se skládá z několika komunikačních bodů, které jsou hierarchicky uspořádány. Koncové telekomunikační zařízení, v tomto případě komunikátor PZTS je koncovým místem sítě a je připojen přes účastnickou zásuvku, která je koncovým bodem sítě. Účastnická telefonní zásuvka slouží pro zakončení dvouvodičového vedení „páru“, z nichž jeden vodič se nazývá „a drát“ a druhý „b drát“. Pro účastnické vedení se také používá termín „přípojka“. Prostřednictvím koncového zařízení je kabelovým vedením účastník připojen k uzlu sítě, který tvoří lokální telefonní ústředna (uzel sítě) tzv. HOST.

7.1.2 Místní sítě

Příklad topologie místní sítě je znázorněn na obrázku č. 5. Na trase kabelového vedení se mezi účastníkem a hostem nachází další soustřeďovací body. Směrem od účastníka je obvykle prvním soustřeďovacím bodem účastnický rozvaděč (UR), který má kapacitu řádově desítky telefonních (účastnických) párů. Následujícím bodem obvykle bývá síťový rozvaděč (SR), jehož kapacita je řádově stovky párů, po něm následuje traťový rozvaděč (TR) s kapacitou řádově až tisíce párů. TR muže být také samostatná místnost v určitém objektu.

Obrázek 5: Topologie místní telefonní sítě



[cit. 2016-03-13] Zdroj: https://www.cetin.cz/documents/10182/54786/MMO+-+P%C5%99%C3%ADloha+12+-+Technick%C3%A1+specifikace.pdf/c0a0dfbf-1ffb-42cc-bc06-46c3e1bc5e57

Dalším bodem je HR (hlavní rozvod) RSU (Remote Subscriber Unit) vzdálená účastnická jednotka, která tvoří mezistupeň mezi kabelovým vedením od účastníka a vedením směrem do ústředny. Před HR je ještě kabelovna, která slouží pro usnadnění

manipulace, uspořádání a dělení kabelů pomocí kabelových spojek. RSU je koncentrační prvek sloužící pro vícenásobné využití kabelového vedení v poměru cca 960:60. RSU je připojen pomocí PCM (pulsně kódovaná modulace) systému, tzv. digitálního okruhu 2 Mbit/s. To znamená, že kapacita od RSU směrem k ústředně (HOST) je 16 x menší než kapacita od RSU k účastníkům, RSU může být součástí HOST. V praxi se koncentrace liší dle potřeb operátora, kde roli hraje konkrétní potřeba dané lokality.

Rozvaděče jsou vystrojeny svorkovnicemi (KRONE), které zakončují příchozí a odchozí kabely. Pomocí těchto svorkovnic je možné propojit přívodní a odchozí kabel podle potřeby, svorkovnice se propojují tzv. ranžírováním - dvoužilovým izolovaným vodičem. Na obrázku č. 6, jsou zobrazeny rozvaděče, první dva zleva UR a zprava SR.

Obrázek 6: Příklady telefonních rozvaděčů UR a SR

[Zdroj: Vlastní]

Na kabelovém vedení se také nachází kabelové spojky, které spojují kabely nebo je větví do menších svazků. Počet, rozmístění a kapacita rozvaděčů je závislá na místních podmínkách a hustotě zástavby. V některých případech může být UR i SR připojen přímo na RSU nebo HOST, pokud se nachází blízko a není důvod budovat další bod sítě. Telefonní rozvaděče jsou zabezpečeny pouze pomocí mechanických zábranných systémů a nejsou nijak hlídány.

7.2 Telefonní linky

Firmy provozující PCO nezveřejňují z bezpečnostních důvodů celkové počty objektů, které jsou v současné době stále připojeny pouze přes telefonní linku. Řádově by se mělo jednat o tisíce objektů. Společnost O2 dle výroční zprávy z roku 2015, „Internet a pevné linky“ provozuje celkem 795 tisíc xDSL přípojek, z toho 438 tisíc VDSL přípojek. Počet xDSL přípojek vzrostl oproti roku 2014 o 2 tísíce. Kolik zákazníků využívá současně s internetem i telefonní služby se ve zprávě neuvádí. Podle vybraných provozních ukazatelů by mělo fixní hlasové linky využívat celkem 840 tisíc zákazníků. Ve zprávě nejsou rozděleny segmenty trhu, proto není možné určit podíl soukromých a firemních zákazníků. Všeobecně známou nevýhodou telefonních linek je, že v případě poruchy na vedení nelze realizovat přenos z PZTS na PCO.[14]

7.2.1 Pevná linka

Pevnou linku HTS (hlavní telefonní stanice) tvoří dvouvodičové vedení tzv. „pár“, s dvěma vodiči, „a-b dráty“. Hlas je přenášen v hovorovém pásmu 0,3 – 3,4 [kHz]. Ke spojení hovoru dochází na telefonní ústředně, která sestaví spojení. Hovoříme tedy o přepojování okruhů, tzv. komutaci. Jedná se tedy o spoj, který není trvalý a ke spojení dochází až v případě požadavku, typicky vytočením požadovaného telefonního čísla. V souvislosti s pevnou telefonní linkou se také používá převzaté označení POTS (Plain Old Telephone Service), FXS (Foreign eXchange Subscriber) příchozí vedení, FXO (Foreign eXchange Office) odchozí vedení. Telefonní linka je napájena přímo z telefonní ústředny stejnosměrným napětím o velikosti 48 [V], vyzváněcí napětí je střídavé o velikosti 75 [V] a frekvenci 25 [Hz].

Koncem roku 2002 byla v ČR dokončena digitalizace veřejné telefonní sítě, jednalo se hlavně o digitalizaci telefonních ústředen, které vzájemně komunikují digitálně. Přípojky pevných linek jsou stále analogové. Digitální ústředny nabízejí více funkcí pro účastníka, například zobrazení čísla volajícího, DTMF volbu (pulsní volba je stále akceptována), nebo příjem SMS. Zaslaná SMS určena pro pevnou linku je zachycena telefonní ústřednou, která jí převede z textu na řeč, zavolá ji účastníkovi a interpretuje hlasovým automatem.

Hovory a přenos zpráv z PZTS jsou zpoplatňovány dle sazby operátora poskytujícího pevné telefonní linky. Náklady na zřízení a samotný provoz telefonní linky byly dříve vysoké, proto se kontrolní zpráva přenášela obvykle jednou za 24 hodin. Nevýhodou pevných linek je, že při poruchách vedení může dojít k chybám při přenosu zpráv. Zanedbatelná není ani snadná možnost napadení telefonních rozvaděčů UR a SR. V současnosti je pevná linka spíše na ústupu a v brzké době by ji měla nahradit VoIP telefonie. Cena za klasickou pevnou linku u O2 s tarifem neomezeného volání, v rámci ČR je v současné době 299 Kč vč. DPH.

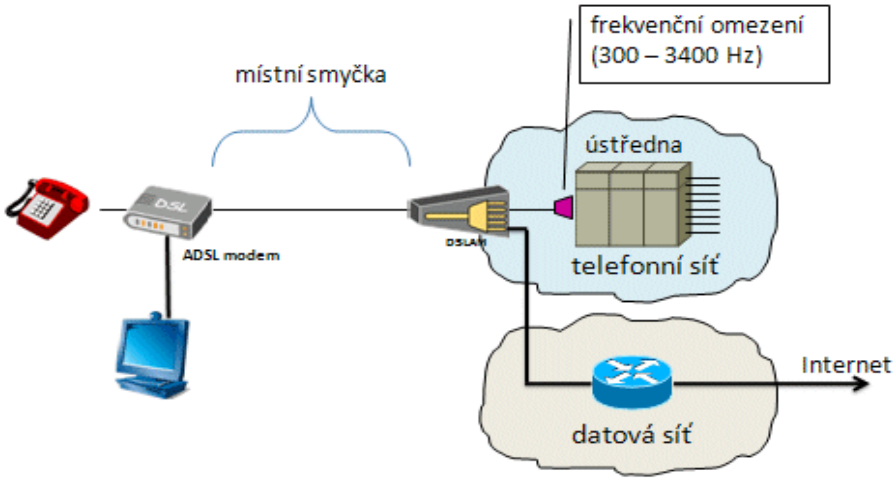
7.2.2 xDSL

Technologie xDSL slučuje data a hlas zároveň, jedná se o tzv. konvergenci. Princip přenosu, spojování hovorů, vedení i napájení je stejné jako u klasické pevné linky. Data neprochází přes telefonní ústřednu, ale jsou od hovoru na straně účastníka oddělena filtrem. Na straně ústředny se data slučují s hovorovým pásmem do vedení. Filtr u účastníka je tzv. „splitr“, což je pásmová propusť, která rozbočuje zvlášť vedení pro telefon a zvlášť pro data, směrem do modemu. Na straně ústředny se nachází také filtr a dále DSLAM (Digital Subscriber Line Access Multiplexer), který umožňuje připojení k internetu. DSLAM sdružuje více účastníků do datového toku pomocí MUX (Multiplexer), zde tedy dochází k tzv. agregaci.

Datová rychlost je ovlivněna vzdáleností účastníka od ústředny, s rostoucí vzdáleností klesá. DSLAM může být také jako předsunutá jednotka, tzv. remote DSLAM. Pokud je vzdálenost účastníků od ústředny větší, předsunutím DSLAMu se zlepší datová propustnost. Výhoda ADSL nebo VDSL oproti klasické telefonní lince je v možnosti

zálohování komunikace přes internet, pokud je linka (hovorové pásmo) obsazena. Princip připojení xDSL linky je znázorněn na obrázku č. 7.

Obrázek 7: Princip xDSL připojení



[cit. 2016-03-13] Zdroj: http://www.earchiv.cz/b07/b0700001.php3

7.2.2.1 ADSL

V ČR se momentálně používá verze ADSL2+ (Asymetrics Digital Subscrieber Line), šířka pásma pro přenos hlasu je 0,3 – 3,4 [kHz], pro data je 4 [kHz] - 2,2 [MHz]. ADSL2+ je asymetrická a může dosahovat rychlosti až 24 Mbit/s pro příjem a 4 Mbit/s pro odesílání dat. Optimální vzdálenost od ústředny, DSLAMu cca 2 [km].

7.2.2.2 VDSL

Současná verze VDSL2 (Asymetrics Digital Subscrieber Line), šířka pásma pro přenos hlasu je 0,3 – 3,4 [kHz], pro data 3,4 [kHz] - 17 [MHz]. Datová rychlost je asymetrická o rychlosti až 100 Mbit/s příjem a 60 Mbit/s pro odesílání. Optimální vzdálenost od ústředny, DSLAMu cca 1 [km].

7.2.3 ISDN

Digitální síť integrovaných služeb neboli ISDN (Integratet Services Digital Network) je telefonní síť se signalizací DSS1 (Digital Subscriber System No. 1), dle ITU se rozhraní označuje Q. 931. Využívá principu PCM s časovým multiplexem TDM (time division multiplex). ISDN oproti klasické telefonní lince nabízí další funkce, např.: velmi rychlé sestavení spojení do 2 [s], více telefonních čísel, konferenční hovory, přesměrovat hovory, možnost přidržení hovoru, zpětného volání atd.

7.2.3.1 Euro ISDN2

Euro ISDN2 BRI (Basic Rate Interface) používá stejné dvouvodičové vedení jako pevná linka. Pro přenos hlasu a dat slouží dva nezávislé B kanály s rychlostí 64 kbit/s, jeden řídící D-kanál s rychlostí 16 kbit/s pro přenos signalizace. Po B kanálech lze uskutečnit současně dva nezávislé hovory, jeden kanál využít pro přenos dat a druhý pro hovor. Případně lze

využít oba kanály B pro přenos dat, celková rychlost je potom součtem rychlostí obou B kanálů tzn. 128 kbit/s. S pořízením ISDN2 od společnosti O2 jsou účastníkovi přiřazena čtyři telefonní čísla, lze přiřadit až osm čísel. V případě připojení PZTS přes ISDN2 je výhodou, že může mít přiděleno vlastní telefonní číslo a samostatný B kanál. Další výhodou ISDN2 je oproti pevné lince a ADSL, že nelze snadno odposlechnout.

7.2.3.2 Využití D-kanálu pro přenos dat

V současné době O2 ani jiný operátor tuto službu nenabízí, jednalo se o technologií ISDN AO/DI (AlwaysOn/Dynamic), výhodu představoval trvalý dohled ze strany PCO. Pro přenos zpráv z PZTS bylo možné u linky Euro ISDN2 využít paketového přenosu dat po D kanálu, který nevyužívá celého přenosového pásma a je trvale připojen protokolem X. 25 a Frame Relay s rychlostí 9600 b/s.

7.2.3.3 Euro ISDN 30

Euro ISDN 30 - PRI (Primary Rate Interface) u O2 je služba označována jako Euro ISDN 30 (30B + D). Pro připojení se používají dva páry vedení dle CCITT (ITU-T) G. 703, z nichž jeden slouží pro příjem a druhý pro vysílání, koncepce vychází z normy pro linku E1. ISDN 30 používá účastnickou signalizaci DSS1, disponuje celkem 32 kanály s celkovou rychlostí 2048 kbit/s. Pro přenos hlasu nebo dat slouží 30 B-kanálů s rychlostí 64 kbit/s, jeden D-kanál 64 kbit/s je signalizační a jeden označovaný jako 0 s rychlostí 64 kbit/s je synchronizační. ISDN 30 slouží pro připojení větších firem, hotelů nebo call center vybavených pobočkovými ústřednami.

7.2.4 E1

Princip je E1 je obdobný jako u ISDN 30, protože ISDN30 z ní vychází. E1 je založena na hierarchii PDH (plesiochronní digitální hierarchie). Jednotlivé linky E1 se dají sdružovat do řádů, nultý řád představuje jeden kanál 64 kbit/s, prvý řád má 30 kanálů - E1 rychlost 2,048 Mbit/s, druhý řád má 120 kanálů – E2 rychlost 8,448 Mbit/s, třetí řád má 480 kanálů – E3 rychlost 34,368 Mbit/s, čtvrtý řád 1920 kanálů – E4 rychlost 139,264 Mbit/s, pátý řád 7680 kanálů – E5 rychlost 564,992 Mbit/s. Trasy s E1 se používají mezi ústřednami případně k připojení ostatních operátorů. V současné době se využívá síťová signalizace SS7 (Signaling System No. 7), která je nezávislá na hovorovém signálu, tzn. při dotazu na spojení, se tedy neobsazuje hovorový kanál.

7.2.5 VoIP

VoIP (Voice over IP) je hlas přenášen prostřednictvím paketů, po sítích LAN, WAN, MAN. VoIP využívá protokolů TCP, UDP a RTP, kde jsou zakódované fragmenty samotného hlasu. Pro úsporu místa je hlas komprimován pomocí kodeků s různou úrovní komprese například G. 711, G. 723, G. 726, G. 729. SIP (Session Initiation Protocol), protokol inicializace relací je na sedmé, aplikační vrstvě modelu ISO/OSI.

SIP je obdoba telefonní signalizace a provádí dohled nad telefonním hovorem vždy vedeným z bodu A do bodu B. Nevýhodou přenosu po IP je tzv. latence, kdy dochází ke zpožďování paketů při přenosu. Toto lze do určité míry odstranit použitím vyrovnávací paměti tzv. jitter buffer. Odposlech SIP lze realizovat např. využitím software Wireshark, přičemž hovor nelze odposlechnout v reálném čase a je potřeba mít přístup k dané síti.

7.3 Ochrana přenosových cest

Telefonní vedení musí být zakončeno přímo ve střeženém objektu v ústředně PZTS a chráněno tak, aby nebylo jednoduše dostupné. Venkovní vedení musí být dostatečně zajištěno, aby jej nebylo možné snadno poškodit, lehce dostupná místa je potřeba zabezpečit mechanickou zábranou, např. ocelovým plechem nebo trubkou. Nadzemní telefonní linky musí být chráněny přepěťovou ochranou, napájení NT rozhraní ISDN linky je potřeba zálohovat. Komunikátor musí být schopen trvale detekovat stav telefonní linky, nikoliv pouze napájení. Je vhodné využívat zálohování přenosových cest, např. komunikátor s kombinací IP a GSM/GPRS.

7.4 Komunikátory

Princip komunikace po telefonní lince je u všech výrobců téměř stejný, ještě před cca 12 lety komunikovala většina PZTS po telefonních linkách, ne všude však byla telefonní linka dostupná. Telefonní komunikátory byly převážně integrovanou součástí systému PZTS, některé instalace byly dodatečně osazovány záložními GSM branami. V současné době je tomu naopak a více se využívá komunikace přes GSM a IP sítě, tento trend souvisí s lepší dostupností a klesajícími cenami těchto technologií. Nejznámějšími výrobci zabezpečovacích systémů jsou v ČR tyto firmy DSC, FBII, Galaxy, Paradox, Jablotron.

7.4.1 JA-80V Kombinovaný komunikátor LAN a telefonní linka

Výrobce Jablotron dodává komunikátor JA-80V, viz obrázek č. 8, jako rozšiřující modul pro systémy PZTS řady 80. Komunikátor je propojen s ústřednou přes sběrnicí RS 485, může komunikovat prostřednictvím IP sítě protokolem IP CID nebo po telefonní lince protokolem Ademco Contact ID. Telefonní část umí také reportovat události prostřednictvím hlasové zprávy až na osm telefonních čísel. Umožnuje dálkovou zprávu zavoláním. Lze nastavit konkrétní číslo pro přístup, časovou prodlevu před vyzvednutím nebo tuto funkci zcela vypnout, komunikátor pak nereaguje na žádný příchozí hovor.[15]

Umožňuje předávat data na 2 PCO, pravidelné hlášení lze nastavovat po minutách v rozsahu 00:00 – 24:00 hod. Připojení LAN s rozhraním RJ45 umožňuje komunikaci se dvěma PCO. V objektu ho lze umístit před firewallem, zařízení musí mít vlastní IP adresu, naslouchá na portu č. 71, jedná se o uzavřené řešení, komunikuje pouze s PCO Jablotron.

Komunikátor není průchozí a nelze za něj jednoduše připojit další telefonní zařízení. Nastavení komunikátoru připojeného k ústředně se provádí buď z klávesnice nebo pomocí PC

programu OLink 2.0 a vyšší, který je dodávaný výrobcem. Tento model je možné pořídit v současné době např. za cenu 2 256 Kč bez DPH v e-shopu www.kvalitnialarmy.cz.[15]

Obrázek 8: Komunikátor JA-80V

[Zdroj: Vlastní]

7.4.2 JA-80X Kombinovaný komunikátor LAN a telefonní linka

Tento model komunikátoru je navržen jako rozšiřující modul pro systémy Jablotron řady 80, pro komunikaci se zabezpečovací ústřednou využívá rozhraní RS 485. Komunikátor disponuje možností detekce oznamovacího tónu, lze za něj připojit další telekomunikační zařízení, například telefonní přístroj. Umí detekovat telefonní linku, oznamovací tón a umožňuje nastavení citlivosti příjmu signálu z telefonní linky. Zprávu dokáže předat na 2 telefonní čísla protokolem Ademco Contact ID, periodické hlášení nelze nastavit, kromě PCO lze předávat hlasové zprávy až na 5 telefonních čísel. Umožňuje vzdálenou zprávu pomocí DTMF, číslo pro vzdálený přístup je možné nastavit individuálně s reakční dobou vyzvednutí hovoru, přijmutí příchozího hovoru je možné vypnout.

Komunikátor může být zapojen v kombinaci s GSM/GPRS komunikátorem JA-80Y, zprávy lze potom posílat současně přes telefonní linku a GSM síť, případně může být nastaven jako záloha pro GSM. Nastavení komunikátoru se provádí stejně jako u předchozího modelu. Tento komunikátor (viz obrázek č. 9) je v současné době možné koupit např. za 1 273 Kč bez DPH v e-shopu www.axlelectronics.cz.[15]

Obrázek 9: Komunikátor JA-80X

[Zdroj: Vlastní]

7.4.3 TWIN-COM

Komunikátor TWINCOM je samostatný LAN/GPRS komunikátor a je určený pro bezpečnostní systémy. Komunikuje pomocí TCP/IP dle požadavků normy SIA DC-09 a TNI 33 4592, záložně může komunikovat prostřednictvím SMS. Komunikátor disponuje dvěma programovatelnými vyváženými vstupy, jedním sabotážním vstupem, jedním reléovým výstupem, sériovou linkou RS485. Součástí je vlastní napájecí zdroj s možností připojení záložní baterie. Kontrolní zprávy jsou přes ethernet přenášeny každých 90 [s], u GPRS je tento interval volitelný.

Výhoda tohoto komunikátoru (viz obrázek č. 10) spočívá v možnosti připojení PZTS, která má k dispozici pouze telefonní komunikátor a tím se rozšíří její komunikační možnosti. TWIN-COM pak funguje jako převodník a bohužel umožňuje přijmout pouze Ademco CID. Nastavení komunikátoru se provádí přes webové rozhraní. Tento komunikátor stojí aktuálně v roce 2016 např. 5 628 Kč bez DPH na e-shopu www.atisgroup.cz.[16]

Obrázek 10: Komunikátor TWINCOM

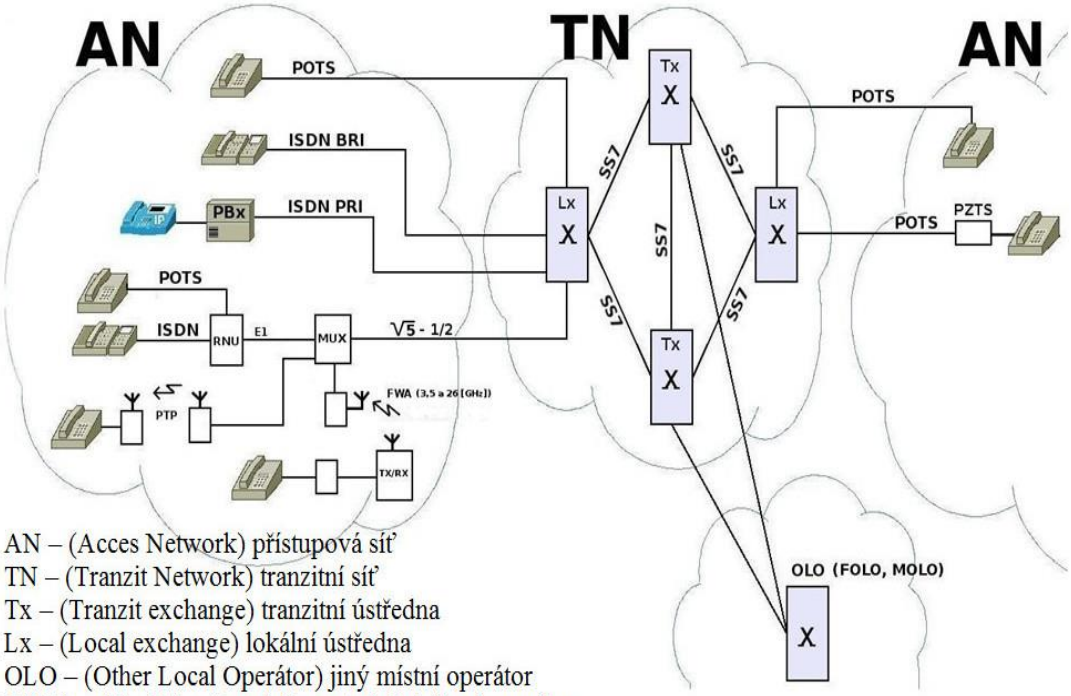
[Zdroj: 16]

8 Spojovací systémy

Tranzitní telefonní síť je složena z veřejných, mezinárodních, tranzitních a lokálních (HOST) telefonních ústředen, které mezi sebou komunikují pomocí signalizace SS7. V ČR se nachází 3 mezinárodní ústředny společnosti CETIN, které jsou kombinované, tzn. zároveň tranzitní (Tx) a zčásti mohou být také HOST. Jedna se nachází v Praze 3 a je zálohována ústřednou ve Stodůlkách v Praze 5, třetí meziměstská ústředna je umístěna v Brně. Přístupová telefonní síť s napojením do tranzitní sítě je obecně znázorněna na obrázku č. 11. Přístupová síť zahrnuje veškerá koncová zařízení.

Celkem by se na našem území mělo nacházet 8 tranzitních a 140 lokálních (HOST) ústředen. Na tranzitní ústředny (Tx) jsou připojeny lokální ústředny (Lx), tzv. HOST. Na úrovni těchto ústředen (Lx) jsou připojeni ostatní operátoři, tzn. mobilní (MOLO), VoIP (FOLO) atp. Lepší alternativní (VoIP) operátoři jsou k ústřednám HOST připojeni linkami E1 se signalizací SS7. Na trhu se však bohužel vyskytují i případy, kdy se firma se čtyřmi přípojkami EURO ISDN2 (BRI) prohlašuje za alternativního operátora, tzn. je připojena malou kapacitou na úrovni přístupové sítě.

Obrázek 11: Topologie přístupové a tranzitní tel. sítě



AN – (Acces Network) přístupová síť
TN – (Tranzit Network) tranzitní síť
Tx – (Tranzit exchange) tranzitní ústředna
Lx – (Local exchange) lokální ústředna
OLO – (Other Local Operátor) jiný místní operátor
FOLO – (Fix Other Local Operator) jiný fixní operátor
MOLO – (Mobile Other Local Operator) jiný mobilní operátor
MUX – (Multiplexer) distribuční bod
BS – (Base Station) základnová stanice
FWA – (Fixed Wireless Access) pevný bezdrátový přístup (P2Mt)
RNU – (Remote Network Unit) vzdálená účastnická jednotka

[cit. 2016-03-13] Zdroj: Převzato z http://pandatron.cz/?tv=42

8.1 Ústředny IV. generace

Současní telefonní operátoři v ČR pro pevné sítě používají digitální ústředny IV. generace – S12 (Alcatel) a EWSD (Siemens). Naproti tomu mobilní operátoři používají již telefonní ústředny V. generace na principu VoIP. Předpokládá se, že ústředny IV. generace budou v dohledné době nahrazeny ústřednami na principu IP (V. generace). Spojovací systémy EWSD jsou používány jako HOST, tranzitní i mezinárodní ústředny. Tento typ ústředen provozuje Cetin a T-Mobile, který v roce 2014 získal dvě EWSD ústředny fúzí se společností GTS, které se nachází v Praze a Brně. Systém S12 vlastní v ČR pouze společnost Cetin a využívá ji jako HOST nebo jako tranzitní ústřednu. Možnosti systému jsou podobné jako u EWSD, koncepce je však odlišná.[17]

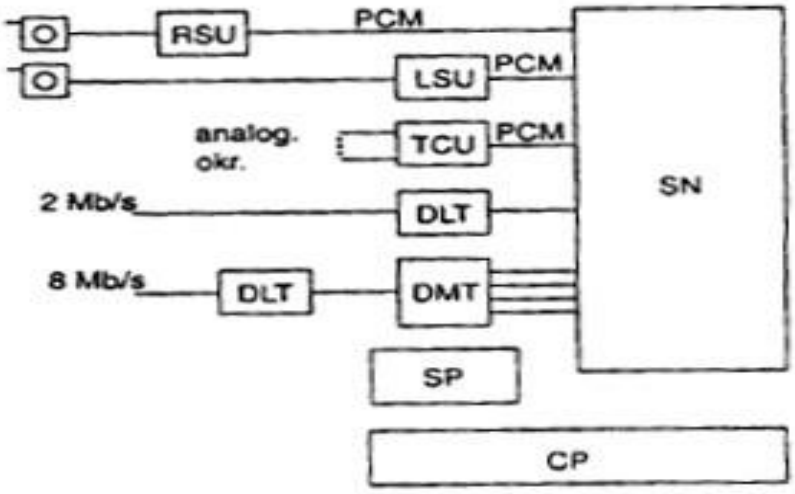
Spojovací systémy IV. generace jsou plně modulární a snadno rozšiřitelné. Systémy pracují s programovým řízením a spojovacím polem s časovým dělením, tzv. multiplex, modulace PCM. Systém EWSD používá decentralizované řízení spojovacího systému a systém S12 distribuované řízení. Každá telefonní ústředna je propojena E1 okruhy, minimálně ze dvou stran a sestavování hovorů probíhá odděleně signalizací SS7. V případě analogové přípojky se analogový signál převádí na digitální v účastnických sadách US, které jsou umístěny v účastnických skupinách, US jsou zároveň koncentračními poli. Ústředna systému EWSD typu HOST má běžně kapacitu 600 000 přípojek a zvládne provozní zatížení až 100 000 [erl] (tzn. počet hovorů po dobu jedné hodiny). Tranzitní ústředna EWSD má běžně 240 000 přípojných bodů. Počet signalizačních kanálů v jedné ústředně je cca 1 500.[18]

8.2 Obecné uspořádání digitálního spojovacího systému

Obecný princip spojovacího pole je znázorněn na obrázku č. 12. Účastnické přípojky se připojují jako místní (LSU) nebo vzdálené (RSU) skupiny. Skupiny jsou běžně připojeny k centrálnímu spojovacímu poli (SN) multiplexem, PCM 1. řádu (PCM 30/32) nebo PCM 2. řádu (PCM 120/128). Každý spojovací systém používá první nebo druhý způsob, připojení skupin však musí být jednotné. To platí pro všechny přípojné relace. Dvouvodičové nebo čtyřvodičové analogové okruhy jsou připojeny přes (TCU), sady analogových spojovacích vedení, sady mají A/D převodníky. Digitální okruhy jsou připojeny přes (DLT), sady digitálních spojovacích vedení, které jsou linkovým zakončením těchto vedeni a slouží pro přizpůsobení přenášených signálů PCM a synchronizaci signálů z příchozích vedení.[18]

Digitální spojování je vždy čtyřvodičové. Účelem digitálního spojovacího pole (SN) je spojování kanálů s rychlostí 64 kbit/s, přenos informací je obousměrný a tvoří ho dvě cesty, každá je pro jeden směr. Zařízení pro zpracování signalizace (SP) přijímá příchozí signalizaci z jednotlivých vedení a předává ji do programového řízení (CP). Následně (SP) přijímá signalizaci z (CP) a vysílá ji do jednotlivých vedení. [18]

Obrázek 12: Obecné schéma spojovacího pole



[Zdroj:18]

RSU (Remote Subicriber Unit) - vzdálená účastnická skupina, koncentrátor; **LSU** (Local Subscriber Unit) - místní účastnická skupina; **TCU** (Trunk Connection Unit) - sada analogových spojovacích vedeni; **DLT** (Digital Line Terminal) - sada digitálních spojovacích vedení; **CP** (Central Processor) - programové řízeni; **SP** (Signal Processing) - zpracováni signalizace; **SN** (Switching Network) - centrální digitální spojovací pole

8.2.1.1 Požadavky na digitální spojovací pole

Digitální spojovací pole má za účel propojovat kanály o rychlosti 64 kbit/s, v případě multiplexu PCM 1. řádu se jedná o 32 kanálových intervalů, celkem 32 x 64 kbit/s. Každý z 32 kanálů je vzorkován 8 000 x za 1 [s], vzorek je převeden na 8 bitový kód, tzn., že každých 125 [μs] se přenese jedno osmibitové slovo, tzv. rámec. Doba pro nasnímání vzorku jednoho kanálu je 3,9 [μs]. Výstupy spojovacího pole jsou tvořeny multiplexy, každý má celkem 32 kanálových intervalů.[18]

Digitální spojovací pole musí umožnit:[18]

- Prostorové spojovací pole S (Space) musí umožnit směrování osmibitových slov přicházejících v určitém kanálovém intervalu vstupního multiplexu do stejného kanálového intervalu libovolného výstupního multiplexu.
- Časové digitální spojovací pole T (Time) umožňuje změnu kanálového intervalu při směrování sledu osmibitových slov ze vstupního multiplexu do libovolného výstupního multiplexu.

Centrální spojovací pole ústředny je realizováno použitím samotného časového pole T a může být také vícečlánkové. Jednotlivé články jsou řazeny za sebou a tvoří je moduly T a S, jedná se například o tříčlánkové pole TST nebo STS. Samotné prostorové pole S je z důvodů velkého vnitřního blokování pro řešení spojovacího pole ústředny nevyhovující. Pro velké systémy se např. u EWSD používá pětičlánkové pole TSSST.[18]

8.3 Signalizace ve spojovacích systémech

Signalizace v telekomunikačních sítích slouží k obsluze, sestavení/ukončení hovoru a dohledu nad spojením, liší se podle použité technologie. Rychlost sestavení spojení je daná rychlostí a použitým typem signalizace. Obecně lze signalizaci rozdělit podle úrovně sítě následovně:

- **účastnická signalizace** – na vedení, mezi telefonem a ústřednou
- **mezistupňová** - vnitřní signalizace ústředen
- **síťová** - signalizace mezi ústřednami

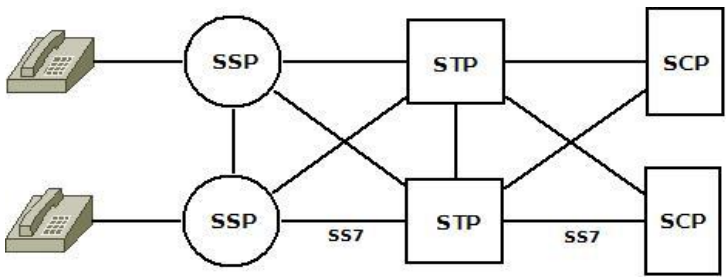
Podle způsobu přenosu se signalizace dělí na:

- **Přidruženou signalizaci** – signalizace je součástí hovorového kanálu nebo společným signalizačním kanálem, CAS (Channel associated signaling), typicky sítě IDN (ISDN) kanál D, č. 16.[18]
- **Společnou signalizaci** – „centralizovaná“ – tato signalizace probíhá mimo hovor ve vyhrazeném signalizačním kanálu CCS (Common channel signaling). Na tomto principu je založena signalizace SS7. Signalizační kanál PCM 30/32 64 kbit/s je schopen, kromě kanálu „0“, obsloužit 1000 i více kanálů, tzn., že jeden kanál dokáže obsloužit více jak 31 přidružených PCM 30/31, záleží však na druhu provozu (hovor/data).[18]

8.3.1 Signalizace SS7

Signalizační systém SS7 je určen pro digitální přenos signalizačních zpráv po páteřních telekomunikačních sítích, národních i mezinárodních. Pracuje s digitálním přenosem signalizačních zpráv s přenosovou rychlostí 64 kbit/s. Koncepce SS7 do jisté míry vychází z modelu OSI. Signalizační zpráva obsahuje např. číslo volajícího, volaného, atd. Signalizační zprávy jsou posílány přes signalizační kanály, které mohou být, kromě kanálu „0“, libovolné. Signalizační informace se přenáší v tzv. multirámci jednou za 2 [ms]. Signalizace se přenáší mezi signalizačními body (viz obrázek č. 13), které tvoří lokální (HOST), kombinované a tranzitní ústředny. Signalizační systém SS7 je možné provozovat ve všech úrovních digitálních sítí pro přenos signalizace mezi ústřednami včetně pobočkových ústředen.[18]

Obrázek 13: Blokové schéma komponent signalizace SS7



[Zdroj:19]

8.3.1.1 Signalizačních body

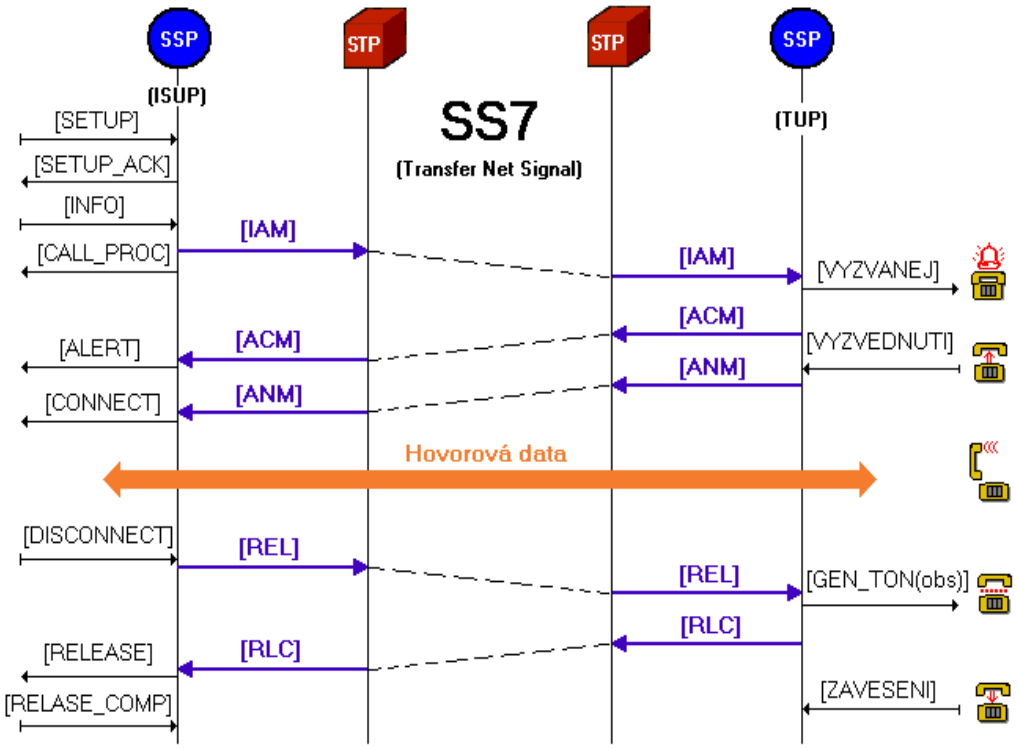
Signalizační body jsou rozděleny na:

- **SSP** (Service Switching Point) – každý signalizační bod SP může být zdrojový nebo cílový a slouží k převodu ostatních signalizací na signalizaci SS7.[19]
- **STP** (Signalling Transfer Point) – tranzitní signalizační bod rozšiřuje spojovací možnosti sítě a slouží pro směrování zpráv v síti, je tvořen funkčním blokem. Signalizace, které přicházejí a odcházejí z ústředny, procházejí přes tento blok. Signalizační kanály a signalizační body tvoří signalizační síť. Každý signalizační bod má svůj kód SCP (Service Control Point).[19]
- **SCP** (Service Control Point) – slouží pro správné směrování k jiným operátorům, obsahují záznamy o telefonních číslech.[19]

8.3.2 Sestavení a zrušení telefonního hovoru

Sekvenční diagram na obrázku č. 14 znázorňuje princip sestavení a zrušení hovoru mezi dvěma účastníky s telefonní přípojkou typu ISDN2 využívající signalizací DSS1 na levé straně a analogovou přípojkou na pravé straně obrázku. Na straně analogového účastníka jsou použity signály rozhraní U, spojení probíhá mezi dvěma ústřednami a jedná se pouze o signalizační výměnu.

Obrázek 14: Sestavení hovoru mezi ISDN2 a analogovou přípojkou



[Zdroj: 19]

Spojení probíhá následovně: Požadavkem [SETUP] volající žádá o uskutečnění hovoru, SSP odpoví [SETUP_ACK] a žádá o doplnění čísla volaného, to je předáno zprávou [INFO], ústředna číslo vyhledá pomocí SCP a vyšle požadavek [IAM] k cílovému STP. Cílová ústředna vyšle [IAM] a ověří, zda volaný není obsazen nebo v poruše atp. Zpráva [CALL_PROC] vlevo se používá, pokud se hovor směruje k jinému operátorovi, jedná se o požadavek na vyčkání, kdy je volaným například mobilní telefon, prodlužuje se odezva. Pokud je volaný dostupný, vyšle zdrojové ústředně zprávu [ACM], současně volající vyzvání, přijetí [ACM] na zdrojové ústředně se přeloží do signalizace DSS1 na [ALERT], volajícímu se začne generovat vyzváněcí tón. Další zprávu vysílá příjemce [ANM], volaný vyzvednul a nyní probíhá hovor.[19]

K ukončení spojení dojde zavěšením volajícího, zdrojová ústředna vyšle zprávu [DISCONNECT], která je konvertována z DSS1 na SS7 jako [REL]. Cílová ústředna odpoví [RLC] jako potvrzení ukončení relace. Poslední výměna u DSS1 je [RELEASE] a [RELEASE_COMP] s terminálem ISDN. Doba přenosu jedné zprávy je závislá na vytížení signalizační sítě, může nabývat hodnot v rozmezí jednotek [ms] až po stovky [ms]. Běžně však celková doba pro sestavení hovoru u ISDN trvá do 2 [s].[19]

8.3.3 Frekvence návěstních tónů

Návěstní tóny slouží k signalizaci, informují účastníky o stavu telefonní linky. Jedná se o přerušované akustické signály, které informují účastníka o jejím stavu. Jednotlivé stavy a jejich tóny se liší frekvencí a dobou přerušení.

Přehled cyklů základních návěstních tónů: [20]

- **oznamovací:** 330 [ms] 425 [Hz]; 330 [ms] pauza; 660 [ms] 425 [Hz]; 660 [ms] pauza
- **vyzváněcí:** 1 [s] 425 [Hz]; 4[s] pauza
- **obsazovací:** 330 [ms] 425 [Hz]; 330 [ms] pauza
- **napojovací:** 330 [ms] 425 [Hz]; 330 [ms] pauza; 330 [ms] 425 [Hz]; 1,5 [s] pauza
- **odkazovací:** 330 [ms] 950 [Hz]; 30 [ms] pauza; 330 [ms] 1400 [Hz]; 30 [ms] pauza; 330 [ms] 1800 [Hz]; 1 [s] pauza

8.4 Obsluhový systém

Návrhy obsluhových systémů (OS) vycházejí z teorie hromadné obsluhy. Pomocí Erlangovy rovnice se vypočte pravděpodobnost provozního zatížení systému tak, aby byly uspokojeny příchozí žádosti, tedy hovory vstupující do systému a ústředny. Vstupní žádosti, toky proudící do OS, tvoří provozní zatížení o intenzitě „**A**“, které jsou tvořeny požadavky „**s**“ ze zdrojů od volajících. Z toho jsou některé požadavky uspokojeny okamžitě nebo za určitou dobu a mají za následek výstupní tok, odchozí hovory ze systému „**Y**“. V telefonních sítích je běžně výstupní tok roven vstupnímu, neuspokojené žádosti tvoří ztráty s hustotou „**Z**“. V reálném provozu nejsou vstupní toky „**A**“ pravidelné a mají určitý časový

odstup mezi jednotlivými žádostmi „**s**“, jedná se tedy o náhodný stochastický tok. Pokud jsou vstupní toky „**A**“ konstantní, jde o deterministický tok. [17]

Vstupní tok se dále dělí na:[17]

- stacionární: nemění se s časem
- ordinární: v jednom okamžiku se nevyskytne více než jedna žádost
- nezávislost: souvisí s počtem zdrojů a dobou trvání obsluhy

8.5 Provozní zatížení

Hodnota provozního zatížení je kvantitativním parametrem OS. Vyjadřuje dobu obsazení všech linek OS po dobu jedné hodiny „T“. Objem provozního zatížení se dělí na nabízený, přenesený a odstupující (ztracený). Přenesené zatížení „Y“ (výkon) se udává jako celková doba obsazení na „N“ linkách, „Nx“ je průběh obsazení v čase a vyjadřuje také počet spojovacích cest. Intenzitu provozního zatížení jedné obsluhové linky vyjadřuje jednotka 1 [erl]. Postup výpočtu provozního zatížení vyjadřuje následující vzorec:[17]

$$\mathrm{Y} = \frac{1}{T} \int_{\mathrm{t_0}}^{\mathrm{t_0}+T} \mathrm{N}_{x \times dt} \quad [erl] \qquad (1)$$

Při návrhu OS je potřeba brát v úvahu nejvyšší provozní zatížení. Cílem je rozložení zátěže během dne tak, aby byly eliminovány výkyvy. Hlavní provozní hodina (HPH) je definována jako čtyři sledy 15-ti minutových intervalů s největším zatížením. Měření probíhá každých 15 minut a v úvahu se bere vždy nejvyšší součet čtyř vzorků v řadě. HPH se počítá zvlášť pro každý den v týdnu. Během dne je v HPH odbaveno přibližně 15 % všech hovorů, jejichž průměrná doba na jeden hovor je 120 [s], více než 50 % z celkových hovorů trvá méně než 30 [s].[17]

8.6 Asterisk

Asterisk je VoIP softwarová ústředna V. generace s paketovým přenosem dat. Tuto softwarovou ústřednu lze provozovat na více OS a je volně dostupná jako distribuce GNU GPL (General Public Licence). Asterisk je velmi flexibilní, univerzální a nabízí více funkcí než starší a mnohem nákladnější PBx systémy. Samozřejmostí je snadná integrace a propojení se starším analogovým rozhraním.

Asterisk je navržen tak, aby snadno propojil telefonní hardware se software nadstavbové aplikace, databáze, a umožnil například ovládání telefonu pomocí PC se zobrazením informace o příchozím hovoru s doplňujícími daty z databáze. Asterisk podporuje např. protokoly SIP, IAX a H. 323 a kodeky G. 711 (alaw), G. 711 (ulaw), G. 723, G. 726, G. 729, GSM, iLBC (internet Low Bitrate Codec), LPC10, Speex, dále také podporuje signalizaci SS7. Pro přenos DTMF využívá signalizační metody RFC2833, INBAND, SIP INFO. Asterisk je možné programově rozšířit přes tzv. AGI (Asterisk Gateway Interface) nebo přímo

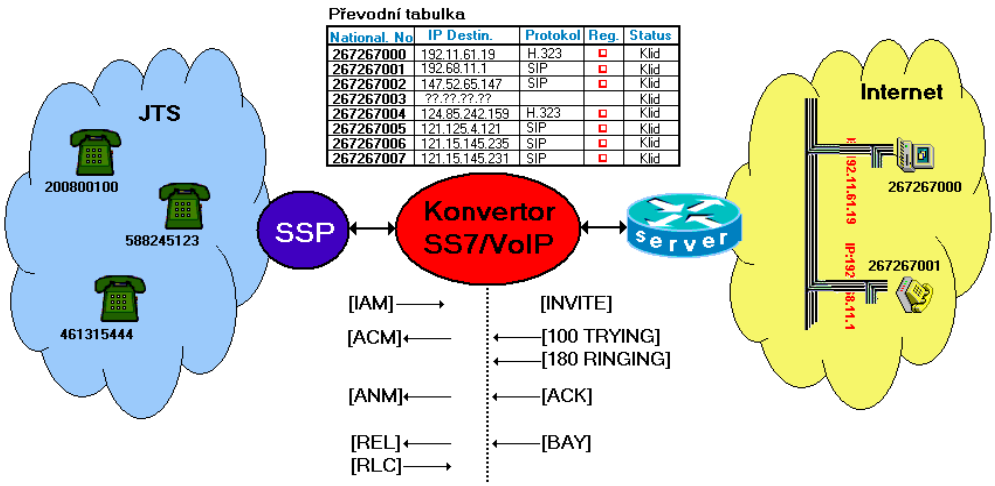
programově řídit pomocí AMI (Asterisk Manager Interface). Asterisk je možné využít například pro tyto aplikace:

- interaktivní hlasový průvodce (IVR - server)
- konferenční server
- PCO aplikace alarm reciever přenosový formát ADEMCO CID
- překlad telefonních čísel
- prediktivní volič (Predictive dialer)
- řazení hovorů do front se vzdáleným zprostředkovatelem
- VoIP gateway (SIP, IAX, H. 323)
- voicemail služby s adresářem (hlasová schránka)

8.7 Přechod mezi VoIP a JTS

Na následujícím obrázku č. 15 je znázorněn princip přenosu telefonního hovoru z JTS do VoIP sítě, a přechod signalizace SS7 na SIP. Tento přechod na obrázku, který je znázorněn jako konvertor, zajišťuje překlad telefonních čísel na IP adresy. Konvertor může být také např. PBx Asterisk.

Obrázek 15: Přechod mezi JTS a VoIP sítí



[Zdroj: 19]

Propojení hovoru mezi pevnou a IP sítí popisuje pan Bazala takto:“ *Signalizace SS7 zajistí, že po vytočení čísla 267267002 je nalezen správný SSP, kterému je toto číslo přiděleno. Zde se generuje zpráva [IAM]. VoIP konvertor zprávu přijme a začne prohledávat svou převodní tabulku, zda se v ní číslo vyskytuje. Pokud číslo nenalezne nebo nalezne a zjistí, že není registrované, vyšle zprávu [REL]. Pokud je vše v pořádku, konvertuje příchozí [IAM] na signál dle uvedeného protokolu z registrace. V tomto případě na [INVITE]. Dalším úkolem VoIP konvertoru je také optimalizovat doplňující parametry. Jedná se především o určování kodeků a udržování jejich kompatibility během hovoru. Konvertor VoIP je softwarově velmi variabilní a může řešit služby jako pobočková ústředna, účtování hovorů, hlasové schránky apod.*“. [19]

9 Kritické body komunikace

Možnými způsoby napadení telefonních komunikátorů a obecně zabezpečovacích ústředen, se nezabývá žádná běžně dostupná literatura. Způsoby napadení komunikátorů je možné rozdělit na možnosti známé z praxe a technicky realizovatelné. PCO si nevedou žádnou statistiku o napadení objektů prostřednictvím telefonních linek.

9.1 Známé možnosti napadení

Následující příklady napadení jsou souhrnem z praxe telefonních mechaniků a techniků zabývajících se instalacemi PZTS. Týkají se převážně samotného vedení nebo přístupových bodů sítě. Předpokladem pro tento typ útoku je pachatelova částečná znalost přístupové sítě a její struktury. V praxi se tyto případy vyskytují výjimečně. U jednoho PCO byly zaznamenány tři případy v průběhu cca 15 let. Naproti tomu, telefonní mechanici spravující oblast Prahy západ a část středních Čech, se setkávají s úmyslným poškozením telefonních rozvaděčů nebo vedení, a to v průměru 5 krát za rok.

9.1.1 Přerušení vedení hrubou silou

Problémem přístupové sítě je, že není chráněna a vedení je někdy snadno dostupné a rozvodné skříně jsou zabezpečeny pouze mechanickými zámky. Nejjednodušší způsob zamezení komunikace je přerušení telefonního vedení na jeho trase, nebo v rozvodných skříních UR nebo SR. V praxi byly zaznamenány případy, kdy pachatel poškodil telefonní linku hrubou silou, vypáčil UR a přeřezal přívodní kabel. Předcházet těmto napadením není zejména u vedení jednoduchá záležitost. Do jisté míry by bylo možné zajistit vzdálené střežení rozvaděčů. Před několika lety o tom provozovatel přístupové sítě uvažoval, některé rozvaděče byly z výroby osazeny dveřními kontakty, tento záměr se však nikdy neuskutečnil, pravděpodobně nebyl z hlediska nákladů rentabilní.

9.1.2 Poškození koncového telefonního zařízení přepětím

Telefonní linka má napájení 48 – 75 [V], Euro ISDN 97 [V], sdělovací kabely jsou schopny přenést napětí v řádu stovek voltů. Přepěťové ochrany pro elektrické přístroje upravuje norma ČSN EN 61643, přepěťová ochrana třídy III (D), přímá ochrana spotřebiče, přepětí pod 1,5 [kV]. V období letních měsíců běžně dochází k případům, kdy vlivem výboje blesku dojde k poškození koncového telefonního zařízení. Přírodu je možné napodobit a blesk nahradit vhodným zařízením, které je schopné z nízkého vstupního napětí vygenerovat vysoké výstupní napětí. Izolační zkouška sdělovacích kabelů se provádí napětím 500 [V], například přístrojem Megmet PU 371.

Z praxe jsou známy případy, kdy telefonní mechanik při měření izolačních odporů opomněl odpojit koncové telefonní zařízení, a vlivem přepětí tak došlo k jeho poškození. Některé telefonní komunikátory jsou buď z výroby, nebo až dodatečně vybaveny svodičem přepětí (bleskojistkou), která po nepřímém úderu blesku může být poškozena a je potřeba ji vyměnit.

9.1.3 Systémová mezera

Poplachy na PCO se odbavují podle došlého pořadí, nebo jejich priorit. K překonání nějakého systému nemusí být vždy potřeba technických znalostí. Někdy stačí změnit úhel pohledu a místo koncentrace na dílčí části se zaměřit na systém jako celek. Tato změna může pozorovateli přinést nové poznatky a značnou úsporu času. Sledováním systému zabezpečování objektů může pachatel snadno zjistit informace o střeženém objektu, časy dojezdů a chování výjezdových skupin. Samotné upozornění, např. reklamní samolepka na dveřích objektu s odkazem na střežící firmu, může mít i negativní dopad.

Následující případ byl zaznamenán jedním PCO a svou povahou patří do sociálního inženýrství. Organizovaná skupina pachatelů cíleně vyvolávala poplachy na vybraných objektech připojených ke stejnému PCO. Záměrem bylo způsobit chaos a vytížit výjezdové skupiny za účelem odvedení pozornosti od zájmového objektu, což jim umožnilo získat více času potřebného k setrvání v objektu a jeho bezproblémové opuštění.

Pachatelé v tomto případě věděli, jakou kapacitou zásahových skupin disponuje dané PCO. V praxi některé PCO měly vlastní zásahové skupiny nebo využívaly subdodavatele, kterých nebylo mnoho, a jejich vozový park disponoval maximálně deseti vozidly. S příchodem projektu „KRUH“, firmy Zásahová služba s. r. o., došlo k celorepublikovému sjednocení většiny zásahových služeb a nastavení jejich standardů. Služby jsou poskytovány provozovatelům PCO. Síť „KRUH“ čítá celkem 200 zásahových vozidel a v případě výskytu abnormálního počtu poplachů tak mohou reagovat pružněji.

9.1.4 Závěrné časy telefonních ústředen

Jde o nastavení, které volanému umožňuje během hovoru zavěsit hovor a následně ho opět vyzvednutím sluchátka přijmout. V případě, že má volaný doma tzv. „paralelku“ (dva telefony), může takto přecházet od jednoho telefonu ke druhému bez rozpadu hovoru, pokud ale zavěsí volající, hovor se okamžitě rozpadne. Z pohledu ústředny se jedná o dočasné pozastavení hovoru. Závěrný čas hovoru u pevné linky od O2 trvá cca 60 [s]. Pokud tedy zavoláme na PZTS, můžeme po tuto dobu blokovat obsazením telefonní linku, komunikátor se bude chovat tak, že se pokusí zavěsit. Při dalším jeho opětovném vyzvednutí se na ústředně nastaví nový časový interval na 60 [s].

Historicky jde o typické nastavení veřejných telefonních ústředen O2 v ČR, u jiných operátorů se mohou časy a nastavení lišit, například mobilní sítě toto neumožňují.

Společnost O2 neumožňuje svým zákazníkům požádat o změnu tohoto nastavení. Dalším úskalím v tomto případě je, že při nevyzvednutí příchozího hovoru zařízení vyzvání celkem 150 [s], dokud ho automaticky nepřeruší ústředna operátora. Jediné možné řešení je SW úprava komunikátoru samotným výrobcem, která by umožnila volitelně přiřazovat zpoždění jednotlivým pokusům, například odložení druhého pokusu o 70 [s], třetího o 155 [s].

Lze také provést změnu linky na Euro ISDN2, ale v době psaní této práce byla tato linka nabízena pouze firmám.

9.2 Technické možnosti napadení

Níže uvedené principy napadení telefonních komunikátorů nebyly pravděpodobně realizované v praxi a vychází ze současných technických možností a dostupného vybavení. Samotný tzv. TDoS útok byl již v zahraničí zaznamenán a hovoří se o něm jako o potencionální hrozbě.

9.2.1 Distribuovaný telefonní útok

Jedná se o hromadné volání na cílové telefonní číslo. K podobné situaci dochází, když v některém z rádií vyhlásí telefonní soutěž a na avizované telelefonní číslo se nelze dovolat. V tomto případě se jedná spíše o stochastický tok volání, protože volající jednají náhodně a jejich počet nelze předem určit, pravděpodobnost dovolat se není zanedbatelná. Současně i volaný, v tomto případě moderátor v rádiu, který by chtěl uskutečnit odchozí hovor, má nemalou šanci vyzvednutím obsadit telefonní linku, obdržet oznamovací tón, provést volbu a být spojen.

Co by se tedy stalo v případě, že by se jednalo o konstantní deterministický tok volání, tedy o zautomatizovaný distribuovaný telefonní útok, tzv. TDoS? Je potřeba vzít v úvahu chování telefonního komunikátoru, který se snaží opakovaně uskutečnit odchozí hovor a obdržet obsazovací tón tím, že zavěšuje linku.

Odpověď na tuto otázku není zcela jednoznačná. Do celé problematiky vstupuje více neznámých, na základě kterých vyvstávají další otázky. Tedy, jaká je potřeba minimální frekvence hovorů, celková kapacita a typ telefonních linek, aby cílové číslo při každém pokusu o odchozí hovor přijalo vždy námi vygenerovaný telefonní hovor? Ovlivňuje vzdálenost volajícího od volaného v rámci telefonní sítě, je lepší být co nejblíže volanému, tzn. být připojen přes jednoho operátora na stejné telefonní ústředně jako cílové číslo?

Pravděpodobnost úspěchu nelze zcela jednoznačně určit nebo předpovědět a je potřeba zcela vyloučit možnost přetížení veřejné telefonní ústředny typu HOST atd., která zvládne bez problémů 100 000 hovorů. Dále přetížení koncentračních bodů sítě, např. RSU, PCM na které je umístěno cílové číslo. Opět se jedná o velký počet generovaných hovorů, řádově desítky až stovky. Pro potencionálního útočníka neznalého přístupové sítě by bylo obtížné zjistit informaci o přesné trase telefonní linky, natož v praxi ověřit přetížení koncentračních bodů. Předpokládáme ale, že útočník zná cílové telefonní číslo, na kterém je PZTS umístěna.

K automatickému generování většího počtu hovorů je možné využít SW PBx Asterisk, která disponuje funkcí tzv. automatického odchozího volání (auto-dial out). Pomocí této funkce je možné realizovat generátor telefonních hovorů. Spouštění a ovládání generátoru je možné ovládat vzdáleně po IP síti nebo telefonem pomocí DTMF volby. Malou nevýhodou Asterisku je, že hovory jsou řazeny sekvenčně, nelze tedy vygenerovat více odchozích volání

přesně ve stejnou dobu. Tento fakt je možné případně kompenzovat využitím více serverů PBx Asterisk za pomoci například virtualizace a centrálního spouštění zpětného volání u virtuálních PBx, například skriptem.

Aby potencionální útočník byl zcela anonymní, má několik možností. Může využít ústřednu někoho jiného včetně jejích telefonních linek, pokud tedy disponuje potřebnými znalostmi a dokáže prolomit zabezpečení serveru. Podobné případy zneužití VoIP PBx jsou známé i z praxe. Další možností je pronajmutí zahraničního serveru a telefonních linek (trunk) VoIP. Některé větší společnosti již akceptují platbu v digitální měně, tzv. Bitcoinech. Pronájem serveru a nákup Bitcoin měny lze uskutečnit pod falešnou identitou, pomocí anonymizační síťě TOR a hidden Net, s využitím technik sociálního inženýrství, o kterých autor více pojednává ve své bakalářské práci. Alternativní VoIP operátoři běžně umožňují online registraci, osobní údaje se dostatečně neověřují a platbu za SIP trunk lze provést anonymně složením hotovosti přímo v bance. Kvalitní alternativní operátoři VoIP jsou připojeni do JTS linkami typu E1 se signalizací SS7. Někteří umožňují z jednoho telefonního čísla (trunku) vést až 10 současných hovorů. Minutu hovoru v rámci pevných linek v ČR je ve špičce možné uskutečnit, v současné době už od 0,49 Kč a mimo špičku od 0,25 Kč, účtováno je po vteřině (1+1), minimální vklad uskutečněný převodem na účet poskytovatele činí 100 Kč.

9.2.2 Podvrhnutí komunikace

Současné pulty disponují širokými možnostmi nastavení, záleží však na jejich provozovatelích, zda tyto funkce využívají. Některá PCO neúplné nebo náhodné přenosové zprávy z objektů, přenášené po telefonních linkách automaticky vyřazují a obslužný software na ně nereaguje. Většinou jsou způsobeny technikem, chybným nastavením při servisu. Historicky některé pulty rozpoznávaly pouze ID objektu a byly provozovány několik let po úplné digitalizaci telefonních ústředen, která byla dokončena na území ČR v roce 2002 a umožnila zobrazovat příchozí telefonní číslo. Toto nastavení by bylo možné teoreticky zneužít s cílem vyvolat chaos, podobně jako je popsáno v kapitole 9.1.3. Výhodou pro potenciálního útočníka je, že není potřeba fyzické přítomnosti u jednotlivých objektů, podvrhnuté poplachy by generoval automat z cizích telefonních linek.

Pokud by potencionální útočník měl informaci o nastavení pultu, používaných telefonních číslech, posloupnosti číslování ID objektů a případně i jejich umístění, mohl by generováním podvrhnutých poplachových zpráv zaměstnat PCO a výjezdové skupiny. SW ústředna Asterisk disponuje aplikací „SendDTMF“, která dokáže generovat DTMF volbu s možností nastavení délky a rozestupu jednotlivých tónů. Dále také aplikací např. AMD (Answering Machine Detection), která dokáže rozpoznat přítomnost stroje nebo člověka na telefonní lince. Ve spojitosti s funkcí automatického odchozího volání „auto-dial out“ je teoreticky možné generovat hovory, které budou přenášet DTMF zprávy. Generování událostí je možné zautomatizovat například PHP skriptem, kterým se pomocí AGI (Asterisk Gateway Interface) rozšíří programové možnosti Asterisku.

10 Vyhodnocení možností napadení

Z teoretických poznatků je patrná návaznost jednotlivých telekomunikačních prostředků a jejich souvislosti. Z praktických možností napadení by bylo vhodné ověřit odolnost ochrany proti přepětí komunikátoru, vezmeme-li ale v úvahu, že pokud se útočník dostane k vedení nebo rozvaděči, stačí mu linku pouze přerušit. Ostatní praktické možnosti není potřeba dále zkoumat, jelikož již byly realizovány, nebo jsou zřejmé. Z technických možností napadení je nejvíce zajímavý a pravděpodobný distribuovaný telefonní útok, protože současné technologické prostředky umožňují jeho realizaci. Bude mu proto věnována největší pozornost v praktické části, dále bude také ověřena možnost podvrhnutí komunikace z falešného zařízení.

Z teorie vyplívá, že doba potřebná pro sestavení hovoru se bude lišit s narůstajícím počtem spojovacích bodů v závislosti na použité přenosové technologii, signalizaci a vytížení spojovacího systému. Rozdíl může činit až stovky [ms]. Výsledný čas potřebný pro sestavení hovoru je tedy součtem všech zpoždění jednotlivých spojovacích bodů. To znamená, že na celkovou dobu sestavení hovoru má patrný vliv vzdálenost volajícího od volaného, technologické přechody, signalizace a typ telefonní linky. Jinak řečeno, rychlejší sestavení hovoru proběhne například u volajícího s ISDN linkou, který volá na ISDN linku, oproti volání z analogové linky.

Současně pro generátor hovorů (server) umístěný v síti WAN platí, že kvalita i rychlost navazování hovorů záleží na propustnosti a zpoždění IP sítě, které taktéž závisí na počtu jejích prvků. Proto je namístě použít spolehlivé a rychlé připojení k internetu, SIP trunk navázat u kvalitního VoIP operátora, který je v ideálním případě propojen do JTS linkami E1 se signalizací SS7. Výhodou je, že v případě obsazení, vyzvánění napadané linky jedním vygenerovaným hovorem, ostatní generované hovory zatěžují pouze signalizaci, tzn., neobsazují hovorové kanály. Z důvodu propustnosti JTS je vhodné generovat volání mimo HPH spojovacích systémů, optimální je například pátek večer, kdy je nízký provoz.

Předpokládáme, že útočník zná pouze výrobce zařízení, telefonní číslo pevné linky PZTS a ví, že komunikace není zálohována jinou cestou. Nemá informaci o typu linky, nastavení komunikátoru, jeho reakci na příchozí hovory a použitém přenosovém formátu. Proto uvažujeme nejbezpečnější nastavení, kde na lince je umístěn pouze komunikátor, linka je typu ISDN2, která umožňuje rychlé zavěšení hovoru (závěrné časy nejsou nastaveny). Příchozí hovor může vyzvánět maximálně 150 [s], komunikátor nereaguje na příchozí hovory (nevyzvedává), má zapnutou detekci telefonní linky a oznamovacího tónu. V případě připojení analogového zařízení přes linku Euro ISDN 2 je možné nejrychleji sestavit telefonní hovor do 2 [s].

Cílem je blokování odchozí komunikace komunikátoru a znemožnění předání poplachové zprávy na PCO. Víme, že komunikátor je v klidovém stavu zavěšen, na příchozí hovor nereaguje, ale je jím vyzváněn. V případě poplachu chce komunikátor uskutečnit

odchozí volání, pokud je však současně vyzváněn příchozím voláním, nemůže ho jednoduše odmítnout, jako je tomu například v mobilní síti. Znamená to, že každý pokus komunikátoru o odchozí volání je podmíněn jeho vyzvednutím a v případě jeho vyzvánění je roven přijmutí hovoru. V praktické části je tedy nutné ověřit frekvenci a celkový počet hovorů, které je potřeba vygenerovat v závislosti na propustnosti JTS. Dále je potřeba zjistit minimální HW požadavky na realizaci generátoru hovorů (serveru) a porovnat rychlosti sestavení spojení u vybraných VoIP operátorů.

11 Praktické řešení

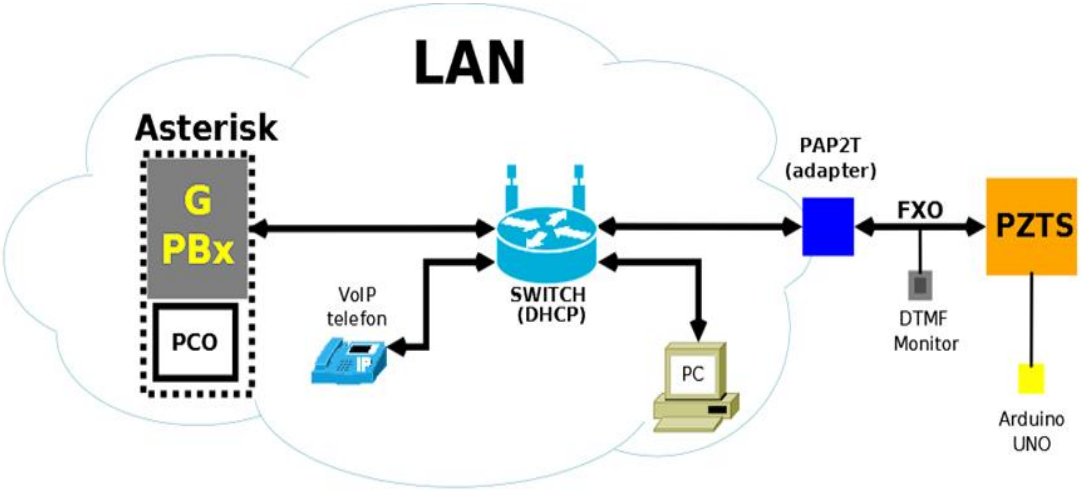
V praktické části této práce bude jako první realizován distribuovaný telefonní útok s cílem zamezit komunikátoru PZTS v předání poplachové zprávy na PCO. Celý test bude nejdříve proveden v uzavřené telefonní síti VoIP z důvodu odhadu frekvence a počtu generovaných hovorů v závislosti na čase, výsledky budou následně ověřeny v síti JTS. Dále bude testována možnost podvrhnutí přenosové zprávy na přijímací pult (PCO) vyslané ze SW telefonní ústředny Asterisk.

11.1 Popis řešení telefonního útoku

Test na simulované telefonní síti VoIP je znázorněn na následujícím obrázku č. 16. Asterisk obstarává zároveň generátor hovorů a příjímací pult (PCO) a je připojen přes Wi-Fi. Nejprve bude ověřeno, zda příjímací pult, běžící na SW Asterisk bez problémů, přijímá zprávy z komunikátorů. Celá síť (LAN) bude propojena přes router, který slouží k přidělování IP adres (DHCP) a je branou do internetu s rychlostí připojení 100/100 Mbit/s. PZTS JA-82K je připojena do VoIP sítě přes adapter Linksys PAP2T, který jí zajišťuje analogové telefonní připojení. Adaptér bude nastaven tak, aby odpovídal parametrům klasické telefonní linky. Na analogovém vedení je paralelně připojen DTMF monitor, který zároveň slouží jako odposlech linky.

Po spuštění generátoru hovorů bude na PZTS simulován pohyb pachatele pomocí časového spínače, který tvoří Arduino s reléovým modulem. Kontakty časového spínače jsou připojeny k PZTS jako dvě okamžité drátové smyčky. Po jeho spuštění rozvažují smyčky každých 30 [s]. V případě, že komunikátor přijme vygenerovaný hovor, bude mu Asteriskem přehrávána nahrávka. PC slouží jako terminál ke vzdálenému ovládání Asterisku, VoIP telefon je pouze pro monitorování stavů kanálů (odposlech) na PBx. Testovány budou dva telefonní komunikátory JA-80V a JA-80x.

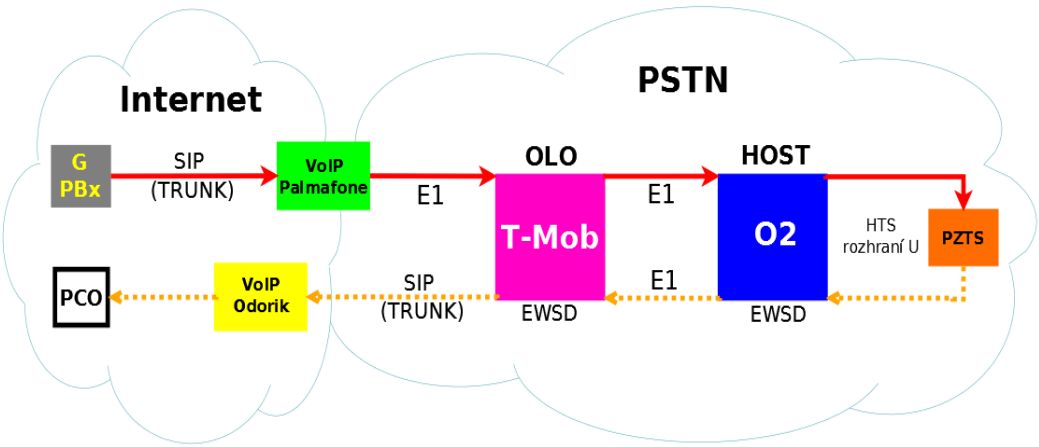
Obrázek 16:Simulovaná telefonní síť



[Zdroj: Vlastní]

Po zjištění potřebného počtu hovorů a frekvence v simulované telefonní síti bude toto nastavení ověřeno v reálné telefonní síti. Topologii připojení generátoru s možností volání ve skutečné telefonní síti popisuje obrázek č. 17. Generátor uskutečňuje hovory ve směru červené šipky. Komunikátor PZTS bude volat ve směru oranžové šipky. PZTS je připojena telefonní linkou Euro ISDN2. Generátor hovorů bude mít navázaný VoIP trunk u operátora Palmafone.cz s možností uskutečnit celkem až 20 současných hovorů. Operátor Palmafone.cz je připojen přímo k operátorovi T-Mobile linkami typu E1. PZTS bude připojena přes linku EURO ISDN2 (rozhraním NT1+ na port a/b1) u operátora O2. PCO (Asterisk) bude mít navázán trunk s možností až 10 současných hovorů přes operátora Odorik.cz, který je propojen přes SIP trunk s operátorem T-Mobile. Testy v telekomunikační síti proběhnou v nočních hodinách z důvodu dostupnosti a minimálního provozního zatížení telefonní sítě. Před samotným testem v síti JTS bude proveden test rychlosti sestavení spojení u jednotlivých operátorů.

Obrázek 17:Princip volání v reálné telefonní síti



[Zdroj: Vlastní]

11.1.1 Použité zařízení

Níže následuje seznam techniky, která byla použita k finálním testům. V případě Asterisku bylo otestováno více HW s cílem zjistit nároky na výpočetní výkon. Test rychlosti sestavení hovorů a test podvrhnutí falešné poplachové zprávy byl prováděn na jiném HW, SW byl použit stejný.

11.1.1.1 Server Asterisk

Hardware: Raspberry Pi 2, model B, CPU: Broadcom BCM2836 900MHz ARM Cortex-A7 quad-core, RAM: 1GB LPDDR2 SDRAM, 4x USB 2.0, HDMI. SD karta Kingston 32 GB, rychlost čtení 90 MB/s, zápis 80 MB/s. Externí HDD 2,5“, SATA III, Kingston 30GB SSDNow S200, rychlost čtení 500 MB/s, zápis 100 MB/s. Wi-Fi USB Adaptér, Edimax Wireless Nano, frekvence 2,4 [GHz], USB 2.0. Zdroj: Jmenovitý výkon: 10 [W], výstupní proud: 2.0 [A], vstupní napětí: 90 – 264 [V] AC, napětí: 5 [V] DC, konektor micro USB.

Software: OS Raspbian Jessie, 4. 1. 19, PHP, Asterisk verze 13. 7. 2. Příklady nejdůležitějších konfiguračních skriptů SW Asterisk jsou uvedeny v přílohách této práce.

11.1.1.2 Zabezpečovací systém - PZTS

Jablotron JA-82K splňuje 2. stupeň bezpečnosti dle ČSN EN 50131. Ústředna je určena pro malé až střední instalace s max. 50 uživateli. Systém je možné rozdělit na 2 podsystémy s možností připojení až 50 smyček, z toho 14 může být drátových. Paměť ústředny zaznamená až 256 událostí. Napájecí zdroj 700 [mA], záložní akumulátor 12 [V], kapacita 2,4 [Ah]. Bezdrátová klávesnice s LCD displejem 2 x 16 znaků pro ústředny JA-8x pracuje na frekvenci 868 [MHz] s protokolem Oasis, obsahuje RFID čtečku 125 [kHz]. K napájení slouží dvě lithiové baterie CR14505 (AA 3,0V). Klávesnice je určena pro ovládání a programování systému, umožňuje připojení dveřního detektoru. Komunikátory JA-80V a JA-80x určené pro ústředny Jablotron řady 80 se připojují k systému JA-82K sběrnicí RS485. Oba typy komunikátorů jsou podrobněji popsány v kapitole 7.4.

11.1.1.3 Časový spínač

Arduino je vývojová programovatelná deska osazená mikrokontrolérem ATmega 328, EEPROM 1KB, paměť 32kB - flash, 2kB SRAM, programovací jazyk Wiring. Deska disponuje 6 analogovými vstupy a 14 digitálními I/O, výstupy - výstupy. Dvojitý reléový modul, vstupní napětí 5 [V], spínací proud až 10 [A].

11.1.1.4 Router

Router TP-Link TL-WDR3600Duální Wi-Fi router 2,4GHz a 5GHz s přenosovou rychlostí až 300 Mbps, splňuje standardy 802.11 a/b/g/n, součástí je čtyřportový LAN switch 10/100/1000 Mbps.

11.1.1.5 Stolní počítač

Vzhledem k povaze celého testu není potřeba žádný speciální počítač, PC slouží pouze jako terminál k nastavování a ovládání ostatních zařízení. Je možné použít jakýkoliv dostupný počítač se síťovým adaptérem a rozhraním RJ45 nebo Wi-Fi. Operačním systémémem Linux s grafickým prostředím, případně OS Windows s programem Putty (SSH klient).

11.1.1.6 Adaptér Linksys PAP2T

Telefonní VoIP adaptér s jedním LAN portem RJ45 umožňuje připojení dvou analogových telefonů přes porty RJ 12, které jsou nezávislé. Podporuje SIP protokol a kodeky G. 711, G726, G. 729, G. 723. Umožňuje konfiguraci pomocí webového prohlížeče.

11.1.1.7 VoIP telefon

Pro tento test byl použit IP telefon WELL SIP-T20, LCD displej 2 x 16 znaků, 2 SIP účty, 2x RJ45, DHCP server, kodeky G. 711, G. 722, G. 723, G. 726, G. 729. Telefon je použit pouze pro monitorování (odposlech) kanálové komunikace, je možné použit běžný VoIP telefon s kodekem G. 711.

11.1.1.8 DTMF monitor

DTMF tester, viz obrázek č. 18 je určen pro sledování komunikace PZTS a testování DTMF tónů. Je vybaven LCD displejem 2 x 16 znaků a vestavěným reproduktorem pro monitorování telefonní linky. Nezávislé napájení zajišťuje baterie 9 [V].

Obrázek 18: DTMF monitor Matilda

[cit. 2016-03-23] Zdroj: http://www.matilda.unas.cz/_firma/dtmfmon.html

11.1.1.9 ISDN NT1+

NT1+ sphairon je zařízení pro zakončení linky Euro ISDN2, rozhraní U konektorem RJ12 NT lze konfigurovat telefonem pomocí DTMF kódů. Pro připojení ISDN zařízení jsou k dispozici dva konektory RJ 45 označené jako S/T. Také je možné připojení dvou analogových telefonních zařízení (komunikátorů) konektory RJ12 (a/b1 ,a/b2), oběma telefonům je možné přiřadit vlastní telefonní čísla.

11.1.2 Realizace generátoru hovorů

S využití SW Pbx Asterisk byl vytvořen generátor hovorů, který dokáže generovat odchozí volání v požadovaném množství s možností nastavení časového odstupu jednotlivých hovorů. Pomocí aplikace „alarm receiver“, která je součástí Asterisku a umí přijímat zprávy s formátem ADEMCO CID, byl zprovozněn vlastní příjímací pult (PCO). Bylo otestováno, že bez problémů přijímá zprávy z komunikátorů.

Funkci generátoru hovorů zajišťuje jednoduchý PHP skript (*start.php*), který lze spouštět pomocí vstupních proměnných z příkazového řádku. Tento skript obsahuje čítač „for“ a v Asterisku spouští funkci zpětného volání (originate). Skript spustí proces, který zavolá na předem definované číslo, a po jeho vyzvednutí mu začne přehrávat předem určenou nahrávku tak dlouho, dokud protistrana nezavěsí.

Jedinou zásadní úpravou Asterisku byla změna nastavení délky odchozího hovoru u aplikace „originate“, která je spouštěna z příkazové řádky, standardně je nastaveno 30 [s]. Úprava se týká přepsání hodnoty *(#define TIMEOUT 30*) ve zdrojovém kódu Asterisku (*res_clioriginate.c*). Důvodem je, že pevná telefonní linka vyzvání celkem 150 [s], hodnota byla nově nastavena s rezervou na 240 [s]. Po této úpravě je nutné Asterisk opět zkompilovat. Spouštění skriptu s cílem vygenerovat po dobu jedné hodiny jeden hovor za sekundu vypadá následovně: *root@pbx: ~# php start.php 3600 1000000*

```
/* start.php */
#!/usr/bin/php
<?php
$arg1 = $argv[1]; // vstupní proměnná určuje počet hovorů
$arg2 = $argv[2]; // vstupní proměnná určuje pauzu mezi hovory v [μs]
for($c=0; $c<$arg1; $c++){
$out = shell_exec('/usr/sbin/asterisk -rx "originate SIP/272660xxx@voipoperator application playback music"');
        usleep($arg2);
      };
?>
```

Skript je možné spouštět více způsoby, např. z PC terminálu, pomocí SMS, nebo s malou úpravou pomocí AGI zavoláním z telefonu do příslušné exten. Níže následuje příklad nastavení *extension.conf,* která umožňuje spouštět skript zavoláním.

```
;Extension.conf
[start]
exten => _X.,1,Answer(); přijmutí hovoru
exten => _X.,n,set(AGISIGHUP=no); toto nastavení zajistí, že skript pokračuje i po ukončení hovoru
exten => _X.,n,AGI(start.php,3600,1000000); spuštění skriptu
exten => _X.,n,Hangup(); zavěšení hovoru
```

Pomocí AMI je možné realizovat sofistikovanější skript, který by kontroloval navázání hovoru s protistranou „answered“ a pozastavil na předem definovanou dobu čítač. Záměrem však bylo realizovat co nejjednodušší řešení.

Postupným testováním různého HW s využitím monitorovacích nástrojů (iotop, htop, nload) bylo ověřeno, že pro zprovoznění generátoru hovorů (serveru Asterisk) vyhovuje Raspberry Pi 2. Podmínkou pro použití Raspberry je vypnutí logování záznamu hovorů CDR (Call Data Records) v *cdr.conf.*

Bylo zjištěno, že při větším počtu generovaných hovorů je zápis na SD kartu limitován kapacitou I/O. Toto je možné vyřešit použitím externího USB disku, který pak slouží pro běh OS. Při generování hovorů každých 100 [ms] bylo zatížení CPU necelých 30% a využití paměti RAM nepřesáhlo 100 MB. Maximální datový tok na LAN byl přibližně kolem 200 kBit/s pro odchozí data a max. 170 kBit/s u příchozích dat.

11.1.3 Test rychlosti sestavení hovoru

Při vytáčení z běžného telefonního přístroje dochází při sestavení hovoru k prodlevě v samotném přístroji z důvodu asynchronní DTMF volby. Telefonní přístroje jsou nastaveny tak, aby provedly volbu až po zadání poslední číslice, přičemž mají nastavenu prodlevu mezi stisky tlačítek přibližně na 3 [s]. I při volbě z paměti telefonu přístroj nevolí okamžitě.

Pro ověření rychlosti sestavení hovoru u vybraných VoIP operátorů byly na ústředně Asterisk navázány trunky a byla připojena linka Euro ISDN2 s využitím HW karty Openvox B200P. Volání bylo nejprve uskutečněno pro každého operátora ve směru z VoIP na ISDN2,

(viz tabulka č. 6) a potom obráceně z ISDN2 na VoIP (viz tabulka č. 7). Pro doplnění je v tabulce č. 8 uvedeno volání ve smyčce, tzn. otočení hovoru na ústředně operátora. Všechny uvedené hodnoty jsou průměrem 10 náhodných volání pro každého z operátorů. Test probíhal v odpoledních hodinách. Jelikož Asterisk neumožňuje měření času v [ms], byl čas získán ze systému takto:

```
;Extension.conf
exten => _x.,1,Set(time=${SHELL(date +"%H:%M:%S %5N"):0:-1}); nastavení času ze systému do proměnné
exten => _x.,n,Set(CDR(time)=${time}); uložení obsahu proměnné do logu
```

Tabulka 6: Test rychlosti sestavení hovoru z VoIP sítě na linku ISDN2

Volání na ISDN2 [s]			
zdroj	**cíl**	**průměr**	**medián**
Palmafone.cz	ISDN2	0,7651	0,7510
Odorik.cz	ISDN2	1,2815	1,2770
můjtelefon.cz	ISDN2	1,2890	1,2935

[Zdroj: Vlastní]

Tabulka 7: Test rychlosti sestavení hovoru z ISDN2 do VoIP sítě

Volání z ISDN2 [s]			
zdroj	**cíl**	**průměr**	**medián**
ISDN2	Palmafone.cz	0,2077	0,2075
ISDN2	Odorik.cz	0,2948	0,2795
ISDN2	můjtelefon.cz	1,3926	1,3535

[Zdroj: Vlastní]

Tabulka 8: Test rychlosti sestavení hovoru ve stejné telefonní síti

operátor – operátor [s]			
zdroj	**cíl**	**průměr**	**medián**
Palmafone.cz	Palmafone.cz	0,1581	0,1515
můjtelefon.cz	můjtelefon.cz	0,1438	0,1685
ISDN2	ISDN2	0,4713	0,3725
Odorik.cz	Odorik.cz	0,5875	0,3445

[Zdroj: Vlastní]

Z měření vyplývá, že sestavení hovoru je rychlejší z pevné telefonní sítě do VoIP sítě. Pravděpodobným důvodem je, že u VoIP hraje roli samotné vytížení sítě a někteří operátoři nemají dostatečnou kapacitu. Dalším možným důvodem je, že hovor není směrován přímou cestou a je dále přepojován přes ústředny jiných operátorů, protože provozovatelé mají provize za příchozí hovory. Z testu nejlépe vychází operátor Palmafone.cz, který je skutečně připojen přímo k operátorovi T-Mobile linkami E1. Měření je pouze orientační a do jisté míry může být zkresleno obtížným získáváním času z Asterisku. Rychlost samotné signalizace nelze takto určit a její čas je zahrnut v celkovém výsledku naměřené hodnoty.

11.2 Test generátoru

Postup testování: Testovány byly celkem dva komunikátory JA-80x a JA-80V, určené pro systémy Jablotron řady 80. Výchozí frekvence generování hovorů byla stanovena na jeden hovor za 2 [s]. Byly vyzkoušeny všechny možné varianty nastavení komunikátorů. Pokud komunikátor hovor přijal, byla mu přehrávána nahrávka. Jako nejvhodnější se ukázalo přehrávat hudbu, proběhl test s přehráváním oznamovacího tónu, ale na komunikátor neměl žádný podstatný vliv. Jedna z testovaných možností byla přesměrovat komunikátor po vyzvednutí do přijímacího pultu (alarmreceiver), ale ukázalo se, že je výhodnější držet komunikátor vyzvednutý, dokud to lze, protože po přenosu zprávy komunikátor zavěsí. Testy komunikátorů probíhaly opakovaně. V případě, že se komunikátoru podařilo dovolat na přijímací pult, byla zvýšena frekvence generování hovorů o 0,5 [s]. Oba komunikátory byly takto testovány několik hodin. Na PZTS JA-82K byly po zastřežení systému automaticky v okamžitých smyčkách způsobovány poplachy každých 30 [s]. Generátor hovorů byl vždy spuštěn před vyvoláním poplachu.

11.2.1 Nastavení a reakce komunikátorů

Oba komunikátory byly otestovány proti PCO běžícím na PBx Asterisk, přenosové zprávy z PZTS se podařilo předat vždy bez problémů. Za komunikátory nebylo připojeno žádné další telefonní zařízení. Možnost volání na předem definovaná čísla byla vypnuta.

11.2.1.1 JA-80x

Nejvhodnější nastavení u tohoto komunikátoru bylo zapnutí nastavení detekce linky a oznamovacího tónu. Vyzvedávání příchozích hovorů bylo zakázáno a byla nastavena okamžitá reakce při poplachu. Dokud na PZTS nebyl vyvolán poplach, komunikátor nepřijímal příchozí hovor. Po vyvolání poplachu, komunikátor rozpoznal, že je vyzváněn. Zareagoval tak, že na 1 [s] vyzvedl a zavěsil. Poté za cca 2 [s] opět vyzvedl a to i v případě, že byl vyzváněn. Do přijatého hovoru se snažil uskutečnit odchozí volání vysláním DTMF volby. Komunikátor poté zůstal takto vyzvednutý 55 – 56 [s]. Tato situace se opakovala, dokud byl komunikátor atakován příchozími hovory.

11.2.1.2 JA-80V

U komunikátoru JA-80V byla zapnuta detekce linkových kódů. Bohužel bylo zjištěno, že při nastavení možnosti nevyzvedávat se v případě poplachu za současného vyzvánění, vůbec nepokusí o odchozí volání. Byla tedy nastavena možnost přijímat hovor, při tomto nastavení se komunikátor snažil o spojení. Po vyzvednutí hovoru komunikátor čekal 60 [s] než opět zavěsil. Prodleva přijmutí příchozího hovoru byla nastavena na 5 [s], aby se zkrátila doba mezi pokusy o spojení. Komunikátor tedy nejprve přijal hovor a zůstal vyzvednutý 60 [s]. Po zavěšení se pokusil uskutečnit odchozí volání, i když byl vyzváněn. Do přijatého hovoru se snažil uskutečnit odchozí volání vysláním DTMF volby. Komunikátor poté zůstal vyzvednutý 42 – 102 [s]. Výhodou tohoto nastavení bylo, že komunikátor při pokusu uskutečnit odchozí volání dokázal zavěsit a vyzvednout za méně než 1 [s].

11.2.2 Výsledky měření

V uzavřené telefonní síti bylo zjištěno, že pro zamezení možnosti odchozího volání u komunikátoru JA-80x je dostačující generovat jeden hovor za 1 [s]. Pro JA-80V je potřeba generovat dva hovory za 1 [s]. Zjištěné nastavení generátoru bylo opakovaně testováno na každém z komunikátorů po dobu pěti hodin. Následnými testy v reálné telefonní síti se podařilo zjistit, že toto nastavení je dostačující. Každý komunikátor byl v JTS testován celkem 90 minut. V tabulce č. 9 a č. 10 jsou pro oba komunikátory uvedeny zjištěné hodnoty z prvního testu, který trval 30 minut, druhý test trval 60 minut. Celkový čas testu (PZTS) je odlišný z důvodu doběhu hovorů a způsobu zaokrouhlování času Asteriskem.

Tabulka 9: Výsledek testu v JTS, komunikátoru JA-80x

Komunikátor JA-80x		
	Popis	**hodnoty**
Generátor	počet hovorů za 1 [s]	1
	Počet vygenerovaných volání	1800
	Počet zodpovězených volání	58
	Počet odmítnutých volání (obsazeno)	1742
Komunikátor	celkový čas vyzvednutí [s]	1627
	celková doba všech vyzvánění před vyzvednutím [s]	219
	Počet krátkých zavěšení - 1 [s]	29
	Počet vyzvednutí s časem obsazení 55 [s]	26
	Počet vyzvednutí s časem obsazení 56 [s]	3
	Počet pokusů o odchozí volání na PCO	58
	Počet spojených volání na PCO	0
PZTS	Počet vyvolaných poplachů	61
	Celkový čas testu [s]	1846

[Zdroj: Vlastní]

Tabulka 10: Výsledek testu v JTS, komunikátoru JA-80V

Komunikátor JA-80V		
	Popis	**hodnoty**
Generátor	Počet hovorů za 1 [s]	2
	Počet vygenerovaných volání	3600
	Počet zodpovězených volání	76
	Počet odmítnutých volání (obsazeno)	3524
Komunikátor	celkový čas vyzvednutí [s]	1806
	celková doba všech vyzvánění před vyzvednutím [s]	160
	Počet vyzvednutí s časem obsazení 42 [s]	62
	Počet vyzvednutí s časem obsazení 60 [s]	10
	Počet vyzvednutí s časem obsazení 102 [s]	4
	Počet pokusů o odchozí volání na PCO	76
	Počet spojených volání na PCO	0
PZTS	Počet vyvolaných poplachů	64
	Celkový čas testu [s]	1966

[Zdroj: Vlastní]

11.3 Navrhovaná opatření proti telefonnímu útoku

Nejjednodušším řešením obrany proti telefonnímu útoku směrovanému na telefonní komunikátor je častější přenos kontrolní zprávy na PCO. Tomuto způsobu nahrává změna nabídky společnosti O2, která v lednu 2016 zavedla nové tarify s neomezeným voláním, v rámci ČR je za 299 Kč vč. DPH. U testovaného komunikátoru JA-80V se nabízí využití komunikace po LAN a telefonní část nechat pouze jako záložní. Komunikátor JA-80x je možné doplnit GSM komunikátorem JA-82Y, jeho cena je v současné době 5 480 Kč bez DPH. Dalším možným opatřením je využití komunikátoru TWINCOM, viz kapitola 7.4.3, který u starších typů komunikátorů rozšíří jejich komunikační možnosti a zpráva je pak přenášena po LAN/GPRS zabezpečeným formátem dle SIA DC-09. Jeho cena je v současné době 5 628 Kč bez DPH. Nejdražší možností je výměna celého systému za novější, jelikož modernější PZTS nabízí více možností, cena však závisí na počtu použitých komponent.

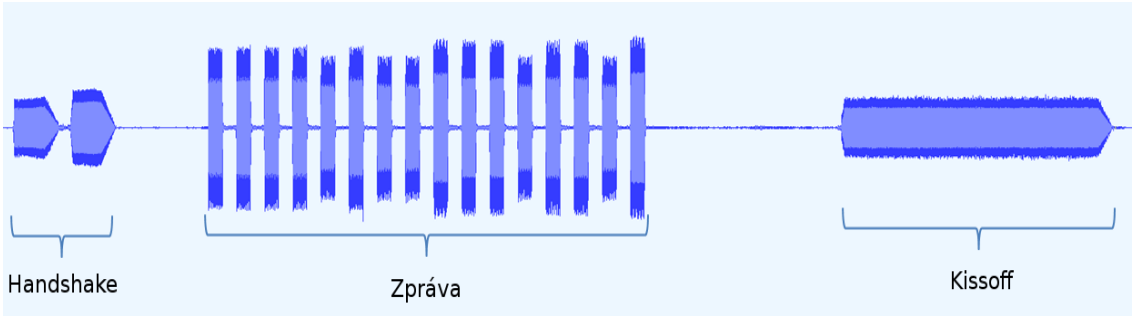
11.4 Podvrhnutí přenosové zprávy na PCO

Při přenosu zprávy linkou ISDN2 z komunikátoru JA-80V na PCO (Asterisk) byl pořízen audio záznam. Přijímací pult Asterisk byl připojen přes trunk Odorik.cz. Pomocí programu Audacity (audio editor) byl záznam komunikace analyzován. Příklad audio záznamu je uveden na obrázku č. 19.

Naměřeny byly následující délky tónů a jejich rozestupy:

- handshake - tón 150 [ms], pauza 50 [ms], tón 150 [ms]
- pauza - 330 [ms]
- zpráva - délka a rozestup mezi tóny - tón 55 [ms], pauza 45 [ms]
- pauza - 780 – 1120 [ms]
- kissoff - tón 950 [ms]
- pauza - 275 [ms]

Obrázek 19: Audio záznam přenosové zprávy



[Zdroj: Audacity]

V Asterisku byla připravena jednoduchá contexts, která má za úkol reagovat na přítomnost pultu a následně mu podvrhnout zprávu vysláním DTMF sekvence. Délky tónů a rozestupy

bylo potřeba upravit. Příklad nastavení jednotlivých exten následuje níže. Spouštění z konzole Asterisku pomocí funkce originate:

*raspberrypi*CLI>originate SIP/21122xxx@odorik extension s@komunikator*

```
;Extension.conf
[komunikator]
exten => s,1,Answer(); přijmutí hovoru
exten => s,n,Set(TIMEOUT(absolute)=60); celková délka trvání této exten
exten => s,n,WaitForSilence(800,1,1); pauza (čeká na ticho 800 [ms,] po uplynutí této doby exten pokračuje)
exten => s,n,WaitForNoise(100); HANDSHAKE část 1 (čeká na zvuk 100 [ms], pokud není, exten nepokračuje)
exten => s,n,WaitForNoise(100); HANDSHAKE část 2 (čeká na zvuk 100 [ms], pokud není, exten nepokračuje)
exten => s,n,WaitForSilence(330,1,1); pauza (čeká na ticho 330 [ms], po uplynutí této doby exten pokračuje)
exten => s,n,SendDTMF(555518313001001#,45,55); vyšle DTMF sekvenci, délka tónu 55 [ms], pauza 45[ms]
exten => s,n,WaitForNoise(700,1,1);KISSOFF (čeká na zvuk 700 [ms], po uplynutí této doby exten pokračuje)
exten => s,n,WaitForSilence(275,1,1); pauza (čeká na ticho 275 [ms], po uplynutí této doby exten pokračuje)
exten => s,n,SendDTMF(555518113001002A,45,55); vyšle DTMF sekvenci, délka tónu 55 [ms], pauza 45[ms]
exten => s,n,Wait(2); čeká 2 [s]
exten => s,n,Hangup; zavěšení hovoru
```

Celý test podvrhnutí přenosové zprávy byl nejdříve realizován na uzavřené VoIP síti. Zpráva šla bez problémů přenášet z ISDN do VoIP sítě odorik.cz. Po úspěšných pokusech byl Asterisk propojen přes VoIP trunk odorik.cz.

Proběhlo testování oproti skutečnému přijímacímu pultu s typovým označením TLR4, které zajistilo nejmenované PCO. Ukázalo se, že přenos DTMF (zprávy) přes VoIP je velice problematický, každý VoIP operátor používá jiný formát přenosu DTMF. S různým nastavením metod přenosu DTMF (RFC2833, INBAND) byly postupně vyzkoušeni všichni VoIP operátoři uvedení v kapitole 11.1.3, zprávu se však nepodařilo předat. Následně byla zpráva přenášena přes linku ISDN2. Přenos zprávy přes linku ISDN2 na PCO s pultem TLR4 se podařil zcela náhodně pouze jednou. Přijímací pult Asterisk (alarmreceiver) má pravděpodobně nastaveny větší tolerance délek a rozestupů tónů. Do jisté míry by bylo možné Asterisk ještě programově upravit, bylo by však potřeba mít skutečný pult fyzicky k dispozici.

12 Závěr

Cílem práce bylo posoudit a prakticky ověřit spolehlivost a bezpečnost telefonních komunikátorů poplachového systému především z pohledu možného napadení systému prostřednictvím telefonní linky. V první části práce jsou popsány jednotlivé přenosové cesty přístupové telefonní sítě, principy komunikace mezi PZTS a PCO, přenosové formáty, charakteristiky přenosu zpráv, spojovací systémy a jejich signalizace. Dále jsou definována úskalí přenosových cest a jejich možná napadnutelnost. Z práce je patrná návaznost jednotlivých telekomunikačních prostředků a jejich souvislostí se zabezpečovacími systémy. Byly popsány kritické body komunikace při přenosu zpráv a naznačen způsob anonymní realizace telefonního útoku.

V druhé části práce je popsána realizace generátoru telefonních hovorů s využitím SW Asterisk. Bylo ověřeno, že možnost napadení komunikátoru přes telefonní linku je reálná a telefonnímu komunikátoru byla znemožněna odchozí komunikace na celých 60 minut. K provedení celé akce případnému útočníkovi stačí zprovoznit generátor hovorů na mini PC napájeném z power banky. Celé zařízení může umístit například do podhledu nějaké restaurace, která nabízí zdarma Wi-Fi připojení. Cena za samotné mini PC Raspberry model Pi 2 je v současné době 999 Kč vč. DPH. Byly navrhnuty možné způsoby, jak zamezit telefonnímu útoku nasměrovanému proti komunikátoru PZTS. I když pevné linky budou v budoucnu nahrazeny VoIP technologiemi, popsaný princip telefonního útoku (TDoS) zůstane stejný a je možné tvrdit, že bude i více pravděpodobný.

Dále byl popsán možný způsob podvrhnutí přenosové zprávy s využitím SW Asterisk. Test přenosu zprávy byl uskutečněn oproti reálnému přijímacímu pultu s typovým označením TLR4. Tento pokus umožnilo realizovat nejmenované PCO. Zprávu se však nepodařilo přenést, bylo by potřeba větších programových úprav SW Asterisk a mít fyzicky k dispozici výše zmíněný přijímací pult. K přenosu bylo potřeba využít klasického telefonního připojeni, přenos zprávy (DTMF) přes VoIP nebylo možné provést.

13 Použitá literatura a internetové zdroje

[1] KŘEČEK, S. *Příručka zabezpečovací techniky*. 3. vydání, Blatná: Cricetus, 2006. 313 s. ISBN 80-902938-2-4.

[2] UHLÁŘ, Jan. *Technická ochrana objektů – díl 2.: elektrické zabezpečovací systémy II*. Vyd. 1. Policejní akademie české republiky, 2005, 229 s. ISBN 80-7251-189-0

[3] KOŽUŠNÍK, Marek. Výkřik techniky. První telefonní ústředna stála v domě U Richterů. In: *Mobil.idnes.cz* [online]. 2012 [cit. 2016-03-15]. Dostupné z: mobil.idnes.cz/historie-telefonu-v-praze-096-/mob_tech.aspx?c=A120811_1815436_praha-zpravy_skr

[4] Policie České Republiky: Kriminalita. POLICIE ČR. [online]. 2016 [cit. 2016-03-13]. Dostupné z: http://www.policie.cz/statistiky-kriminalita.aspx

[5] ČSN EN 50518-1. *Dohledová a poplachová přijímací centra - Část 1: Umístění a konstrukční požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010.

[6] ČSN EN 50518-2. *Dohledová a poplachová přijímací centra - Část 2: Technické požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.

[7] ČSN EN 50518-3. *Dohledová a poplachová přijímací centra - Část 3: Pracovní postupy a požadavky na provoz*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2012

[8] LENIA SPOL. S R.O. Firemní literatura. Praha, 2004

[9] JANSEN, Horst a Heinrich RÖTTER. *Informační a telekomunikační technika.* Vyd. 1. Praha: Europa-Sobotáles, 2004, 400 s. ISBN 80-86706-08-7

[10] VRBOVEC, Bohumil. Ademco Contact ID Protokol SIA DC - 05 – 1999.09.: směrnice č: AGA 002. In: DUFEK, Jiří. Ademco Contact ID Protokol SIA [online]. Praha: AGA, Freyova 27, 190 00 Praha 9, 2007 [cit. 2014-03-17]. Dostupné z: http://www.t-security.cz/www.t-security_htm_files/AGA_002_ID_contact.pdf

[11] VRBOVEC, Bohumil. *Bezpečný přenos informací mezi prostředky asistivních technologií a centry pomoci* [online]. Tábor, 2014, 12 [cit. 2016-03-11]. Dostupné z: http://www.mpsv.cz/files/clanky/19596/BPI.pdf

[12] Digital Communication Standard – Internet Protocol Event Reporting: ANSI/SIA DC-09-2013: Internet Protocol Událost Report ing [online]. USA: The Security Industry Association, 2013, 44 [cit. 2016-03-12]. Dostupné z: http://www.siaonline.org/SiteAssets/Standards/Intrusion%20Subcommittee/DC-09%20Preparing%20for%20ANSI%20Public%20Review.pdf#search=SIA%20DC-09

[13] Česká Republika. Sbírka zákonů: Sbírka zákonů č. 127 / 2005. In: 127. Praha: Tiskárna Ministerstva vnitra, 2005, roč. 2005, č. 127, 43, s. 1354. ISSN 1211-1244. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=4641

[14] O2 Czech Republic a.s. O2 Czech Republic a.s. VÝROČNÍ ZPRÁVA 2015. In: *O2: Výroční a pololetní zprávy* [online]. 2016 [cit. 2016-03-09]. Dostupné z: http://www.o2.cz/file_conver/462173/VZ15_CZ_18_02.pdf

[15] Jablotron S R.O. Firemní literatura. Praha, 2016

[16] TWIN-COM: LAN/GPRS KOMUNIKÁTOR PRO BEZPEČNOSTNÍ SYSTÉMY INSTALAČNÍ A PROVOZNÍ PŘÍRUČKA. ATIS group s.r.o., 2015

[17] VOZŇÁK, Miroslav. Spojovací systémy. 1. vyd. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2009. ISBN 978-80-248-1961-7

[18] SVOBODA, Jaroslav a Heinrich RÖTTER. *Telekomunikační technika – díl 2.: průřezová učebnice pro odborná učiliště a střední školy*. 1. vyd. Praha: Nakladatelství Hüthig, 1999, 142 s. ISBN 80-901-9364-1

[19] BAZALA, David. *Telekomunikace a VoIP telefonie*. 1. vyd. Praha: BEN - technická literatura, 2006, 224 s. ISBN 80-7300-201-9

[20] Tónová volba. *Wikipedia* [online]. 2013 [cit. 2016-03-14]. Dostupné z: https://cs.wikipedia.org/wiki/T%C3%B3nov%C3%A1_volba

[21] GONCALVES, Flavio. *Configuration Guide for Asterisk PBx*. 2007. USA: V. Office Networks Ltda., 2007. 237 s. ISBN 978-85-906904-2-9

[22] VOZŇÁK, Miroslav. Voice over IP. 1. vyd. Ostrava: VŠB - Technická univerzita Ostrava, 2008. ISBN 978-80-248-1828-3.

[23] WIJA, Tomáš; ZUKAL, David; VOZŇÁK, Miroslav. [online]. 2005 [cit. 2014-01-07]. Dostupné z: http://archiv.cesnet.cz/akce/20051115/pr/voz05_asterisk.pdf

[24] Beneš, P. *Napadení systémů PZTS pomocí telefonních komunikátorů*. 2014. Bakalářská práce. Česká zemědělská universita. Technická fakulta. Katedra technologických zařízení staveb.

[25] HEŘMAN, J., TRINKEWITZ, Z., et al.: *Elektrotechnické a telekomunikační instalace*, 2006, Verlag Dashofer, ISBN 80-86897-06-0

[26] JACKSON, Benjamin a Champ CLARK. *Asterisk hacking*: toolkit and liveCD. Editor Larry Chaffin, Johnny Long. Burlington: Syngress, 2007, xii, 253 s. ISBN 978-1-59749-151-8.

[27] MEGGELEN, Jim Van, Jared SMITH a Leif MADSEN. *Asterisk: the future of telephony*. 1st ed. Sebastopol, Calif.: O'Reilly, 2005, 176 s. ISBN 978-059-6009-625.

[28] SVOBODA, Jaroslav a Heinrich RÖTTER. *Telekomunikační technika – díl 1.: průřezová učebnice pro odborná učiliště a střední školy*. 1. vyd. Praha: Nakladatelství Hüthig, 1998, 136 s. ISBN 80-901936-3-3.

[29] SVOBODA, Jaroslav a Heinrich RÖTTER. *Telekomunikační technika – díl 3.: průřezová učebnice pro odborná učiliště a střední školy*. 1. vyd. Praha: Nakladatelství Hüthig, 1999, 136 s. ISBN 80-901-9367-6.

14 Seznam zkratek

ADSL	Asymmetric Digital Subscriber Line (Asymetrická digitální účastnická přípojka)
AGI	Asterisk Gateway Interface (Brána umožňující rozšíření programových možností PBx Asterisk)
AMI	Asterisk Manager Interface (Řídíci rozhraní PBx ASterisk)
AN	Acces Network (Přístupová síť)
AO/DI	Always On/Dynamic (Technologie umožňující přenášet data po D-kanále)
ATA	Analog Telephone Adapter (Analogový telefonní adaptér na VoIP)
ATX	Advanced Technology Extended (formát základních desek PC)
BRI	Basic Rate Interface (Přípojka ISDN)
CCITT	Commité Consultatif International Télégraphique et Téléphonique (Stálá podkomise ITU pro telegrafii a telefonii)
CAS	Channel Associated Signalling (tel. signalizace přiřazena k hovorovým kanálům)
CSS	Common Channel Signallling (tel. signalizace se společným sig. kanálem)
ČTU	Český telekomunikační úřad
DDoS	Distributed Denial of Service (Distribuovaný útok způsobující odmítnutí služby oběti)
DHCP	Dynamic Host Configuration Protocol (přiděluje IP adresy pomocí DHCP protokolu)
DPPC	Dohledové a Poplachové Přijímací Centrum
DSLAM	Digital Subscriber Line Access Multiplexer (rychlé připojení k internetu po telefonní lince technologií xDSL)
DSS1	Digital Subscriber Signalling Systém No. 1 (Digitální účastnický „signalizační“ systém č. 1)
DTMF	Dual Tone Multi Frequency (Tónová volba)
E1	Multiplexní digitální telefonní linka prvního řádu, 32 přenosových kanálů
EWSD	Elektronisches Wählsystem Digital (Digitální spojovací systém, výrobce Siemens)
EZS	Elektrická Zabezpečovací Signalizace, po roce 2002 též označení pro Elektrické Zabezpečovací Systémy (V souč. se nepoužívá, nahrazeno PZTS)
FOLO	Fix Other Local Operator (Jiný fixní operátor)
FWA	Fixed Wireless Access (Pevný bezdrátový přístup)
FXO	Foreign eXchange Office (Odchozí vedení – připojení koncového telefonního zařízení)

FXS	Foreign eXchange Subscriber (Příchozí vedení - analogová telefonní linka)
GNU	GNU is Not UNIX (Volně šiřitelný software)
GPL	General Public License (Generální veřejná licence - software, který lze zdarma používat i modifikovat)
GPRS	General Packet Radio Services (Integrace datových služeb do sítě GSM)
GSM	Global System for Mobile Communication (Globální Systém pro Mobilní komunikaci)
HAS	Hold-up Alarm Systém (Poplachový Tísňový Systém - PTS)
HPH	Hlavní provozní hodina (Telekomunikace – zatížení telefonní ústředny)
HTS	Hlavní telefonní stanice. (Pevná linka)
HW	Hardware (v informatice: součástky, hmatatelné technické vybavení)
IAS	Intruder Alarm Systém (Poplachový Zabezpečovací Systém - PZS)
IAX	Inter Asterisk eXchange (Protocol PBx Asterisk)
IP	Internet Protocol (Internetový protokol)
ISA	Industry Standard Architecture (počítačová sběrnice)
ISDN	Integrated Services Digital Network (Digitální síť s integrovanými službami)
ISO	International Standards Organization (Organizace pracující na modelu OSI)
ITU	International Telecommunication Union (Mezinárodní telekomunikační unie)
IVR	Interactive Voice Response (Interaktivní hlasová odezva)
JTS	Jednotná telekomunikační síť (Anglický ekvivalent je zkratka POTS)
HOST	Lokální veřejná telefonní ústředna, dříve uzlová tel ústředna UTU
LAN	Local Area Network (Lokální počítačová síť)
LCD	Liquid crystal display (Displej z tekutých krystalů)
Lx	Local exchange (Lokální ústředna)
MAN	Metropolitan Area Network (Metropolitní počítačová síť)
MMS	Multimedia Messaging Service (Multimediální zpráva)
MOLO	Mobile Other Local Operator (Jiný mobilní operátor)
MSN	Multiple Subscribe Number (Vícenásobné účastnické číslo ISDN přípojky)
MUX	Multiplexer (slučuje více signálů do jednoho)
NAT	Network Address Translation (Překladač IP adres)
NT	Network Terminator (zakončení ISDN linky)

OLO	Other Local Operátor (Jiný místní operátor)
OS	Operating Systém (Operační systém)
P2Mt	Point to Multipoint (Více násobné spojení z jednoho bodu do více bodů)
PBx	Private Branch eXchange (Pobočková ústředna)
PC	Personal computer (osobní počítač)
PCI	Peripheral Component Interconnect (počítačová sběrnice)
PCM	Pulse Code Modulation (Pulzně kódová modulace)
PCO	Pult centrálizované ochrany (počítačová sběrnice)
PČR	Policie České republiky
PIR	Pasiv Infra Red detector (Pasivní infračervený detektor)
POTS	Plain Old Telephone Service (Pevná telefonní linka)
PRI	Primary Rate Interface (Přípojka ISDN)
PSTN	Public Switched Telecommunication Networks (Veřejné komutované telefonní sítě, v ČR je ekvivalent zkratka JTS)
PTP	Point To Point (Spojení z bodu do bodu)
PZTS	Poplachové zabezpečovací a tísňové systémy (Dříve nazývané EZS)
RFID	Radio Frequency Identification (Identifikace pomocí rádiové frekvence)
RNU	Remote Network Unit (Vzdálená účastnická jednotka)
RSU	Remote Subscriber Unit (vzdálená jednotka pro připojení účastníků tel. sítě)
RTP	Real-time Transport Protocol (Protokol standardizující paketové doručování dat po internetu)
S12	Systém 12, Digitální spojovací systém, výrobce Alcatel
SASTP	Stand Alone Signaling Transfer Point (Samostatný signalizační převáděcí bod)
SCP	Service Control Point (Servisní Kontrolní Bod – signalizace SS7)
SCO	Systém centralizované ochrany
SIP	Session Initiation Protocol (Protokol inicializace relací)
SLA	Service Level Agreement (Smlouva o poskytování úrovně a kvality služby)
SMS	Short Message Service (Krátká textová zpráva)
SW	Software (v informatice znamená: počítačové programy, nehmotné vybavení PC)
SR	Síťový rozvaděč
SS7	Signaling System No. 7 (Signalizační systém č. 7)

SSP	Service Switching Point (Servisní přepínací bod – signalizace SS7)
STP	Service Transfer Point (Servisní převáděcí bod – signalizace SS7)
TDoS	Telephony Denial of Service (Telefonní útok způsobující odmítnutí služby oběti)
TN	Tranzit Network (Tranzitní telefonní síť)
TR	Traťový rozvaděč
Tx	Tranzit exchange (Tranzitní telefonní ústředna)
UDP	User Datagram Protocol (Protokol pro přenos dat)
UR	Účastnický rozvaděč
USB	Universal Serial Bus (Univerzální sériová sběrnice PC)
UTP	Unshielded Twisted Pair (Nestíněná kroucená dvojlinka - kabel)
UTU	Uzlová telefonní ústředna
VDSL	Very High Speed DSL (velmi rychlá Digitální účastnická přípojka)
VoIP	Voice over Internet Protocol (přenos digitalizovaného hlasu v těle paketů)
VPN	Virtual Private Network (Virtuální soukromá síť)
WAN	Wide Area Network (Rozlehlá počítačová síť)
xDSL	Digital Subscriber Line (Digitální účastnická přípojka)
ZAU	Kabelový závěr (Běžně instalovaný v rozvaděčích UR, SR a TR)

15 Seznam obrázků

16 Seznam tabulek

17 Seznam příloh

Příloha 1: Asterisk – extensions.conf

```
[general]
static=yes
writeprotect=yes
autofallthrough=no
clearglobalvars=no
priorityjumping=no
language=cz

[globals]

[default]

[inter]
include => monitor
include => alarm
include => komunikator
include => start

exten => _1XX,1,Set(CDR(userfield)=inter)
exten => _1XX,n,Dial(SIP/${EXTEN},600,rt)
exten => _1XX,n,GoTo(dialstatus,s-${DIALSTATUS},1)

[komunikator]
exten => s,1,Answer()
exten => s,n,Set(TIMEOUT(absolute)=60)
exten => s,n,WaitForSilence(100,1,1)
exten => s,n,WaitForNoise(140,1,1);HANDSHAKE 1
exten => s,n,WaitForNoise(140,1,1);HANDSHAKE 2
exten => s,n,WaitForSilence(250,1,1);pauza (338)
exten => s,n,SendDTMF(555518313001001#,45,55)
exten => s,n,WaitForNoise(920,1,1);KISSOFF (950)
exten => s,n,WaitForSilence(240,1,1); pauza (275)
exten => s,n,SendDTMF(555518113001002A,45,55)
exten => s,n,WaitForNoise(920,1,1);KISSOFF (950)
exten => s,n,WaitForSilence(240,1,1); pauza (275)
exten => s,n,SendDTMF(555518113001001B,45,55)
exten => s,n,WaitForSilence(3000)
exten => s,n,Hangup

[alarm]
exten => _211222XXX,1,Answer()
exten => _211222XXX,n,Ringing()
exten => _211222XXX,n,Wait(2)
exten => _211222XXX,n,Set(CDR(userfield)=PCO1)
exten => _211222XXX,n,Alarmreceiver()
exten => _211222XXX,n,Hangup()

exten => _212222XXX,1,Answer()
exten => _212222XXX,n,Ringing()
exten => _212222XXX,n,Wait(2)
exten => _212222XXX,n,Set(CDR(userfield)=PCO2)
exten => _212222XXX,n,Alarmreceiver()
exten => _212222XXX,n,Hangup()

[monitor]
exten => _555,1,NoOp()
exten => _555,n,Set(CDR(userfield)=spy)
exten => _555,n,Chanspy(all,qo)
```

```
exten => _8XXX,1,NoOp()
exten => _8XXX,n,Set(CDR(userfield)=spy)
exten => _8XXX,n,Chanspy(SIP/${EXTEN:2},qo)

[from-odorik]
exten => 123456,1,Macro(odorik,PCO1)
exten => 456321,1,Macro(odorik,PCO2)

[macro-odorik]
exten => s,1,Answer
exten => s,n,Ringing()
exten => s,n,Wait(1)
exten => s,n,Set(CDR(userfield)=${ARG3})
exten => s,n,Alarmreceiver()
exten => s,n,Hangup()

[start]
exten => _333,1,Answer()
exten => _333,n,set(AGISIGHUP=no)
exten => _333,n,AGI(start.php,100,1000000)
exten => _333,n,Wait(200)
exten => _333,n,Hangup()

[dialout]
exten => _[26]XXXXXXXX,1,Set(CALLERID(number)=211222xxx)
exten => _[26]XXXXXXXX,n,Set(CDR(userfield)=OUT)
exten => _[26]XXXXXXXX,n,Set(CDR(destination)=${EXTEN})
exten => _[26]XXXXXXXX,n,Dial(SIP/${EXTEN}@odorik,180,t)
exten => _[26]XXXXXXXX,n,GoTo(dialstatus,s-${DIALSTATUS},1)

[dialstatus]
exten => _s.,1,Playtones(busy)
exten => _s.,n,Hangup(${HANGUPCAUSE})
```

Příloha 2: Asterisk – sip.conf

```
[general]
context= default
allowguest=yes
alwaysauthreject=yes
registertimeout=20
registerattempts=0
bindport=5060
bindaddr=0.0.0.0
srvlookup=yes
disallow=all
allow=alaw
language=cz
tonezone=cz
canreinvite=no
limitonpeer = no
useragent=PBX
;relaxdtmf=yes
dtmfmode=rfc2833
;dtmfmode=inband
callerid = unknown
subscribecontext = default
notifyringing = yes

[odorik1]
host=sip.odorik.cz
username=123456
fromuser=123456
secret=password
type=friend
insecure=invite
context=from-odorik
qualify=yes
sendrpid=yes
register=123456:password@sip.odorik.cz/123456

[odorik2]
host=sip.odorik.cz
username=654321
fromuser=654321
secret=password
type=friend
insecure=invite
context=from-odorik
qualify=yes
sendrpid=yes
register=654321:password@sip.odorik.cz/654321

[110]
type=friend
context=inter
host=dynamic
canreinvite=no
username=110
secret=password
callerid=110 <110>
dtmfmode=rfc2833
nat=no
qualify=yes
call-limit=1
```

Příloha 3: Asterisk – alarmreceiver.conf

```
[general]
; Specify a timestamp format for the metadata section of the event files
timestampformat = %a %b %d, %Y @ %H:%M:%S %Z
;
; Specify a command to execute when the caller hangs up
; Default is none
;eventcmd = yourprogram -yourargs ...
;eventcmd = /var/spool/asterisk/tmp/alarm/after_alarm_event.php
;
; Specify a spool directory for the event files. This setting is required
; if you want the app to be useful. Event files written to the spool
; directory will be of the template event-XXXXXX, where XXXXXX is a random
; and unique alphanumeric string.
; Default is none, and the events will be dropped on the floor.
;
eventspooldir = /var/spool/asterisk/alarm_events
;
; The alarmreceiver app can either log the events one-at-a-time to
individual
; files in the spool directory, or it can store them until the caller
; disconnects and write them all to one file.
; The default setting for logindividualevents is no.
;
logindividualevents = no
;
; The timeout for receiving the first DTMF digit is adjustable from 1000
msec.
; to 10000 msec. The default is 2000 msec. Note: if you wish to test the
; receiver by entering digits manually, set this to a reasonable time out
; like 10000 milliseconds.
fdtimeout = 2000
;
; The timeout for receiving subsequent DTMF digits is adjustable from
; 110 msec. to 4000 msec. The default is 200 msec. Note: if you wish to
test
; the receiver by entering digits manually, set this to a reasonable time
out
; like 4000 milliseconds.
sdtimeout = 200
;
; Wait for the connection to settle post-answer. Adjustable from 500 msec.
to 10000 msec.
; The default is 1250 msec.
answait = 1250
; When logging individual events it may be desirable to skip grouping of
metadata
;no_group_meta = yes
; The loudness of the ACK and Kissoff tones is adjustable from 100 to 8192.
; The default is 8192. This shouldn't need to be messed with, but is
included
; just in case there are problems with signal levels.
;
loudness = 6000
; The db-family setting allows the user to capture statistics on the number
of
; calls, and the errors the alarm receiver sees. The default is for no
; db-family name to be defined and the database logging to be turned off.
;
db-family = yourfamily:
; End of alarmreceiver.conf
```