Portál pre odborné publikovanie ISSN 1338-0087

Bezpečnosť IP telefónie

Šumný Marek · Elektrotechnika, Informačné technológie, Študentské práce

19.08.2011

Práca sa venuje problematike bezpečnosti IP telefónie. V úvode sú popísané bezpečnostné protokoly TLS, SRTP a metódy prenosu kľúča MIKEY, ZRTP a SDES. V praktickej časti, ktorá tvorí nosnú časť práce, je opísané softvérové vybavenie pracoviska – ústredňa PBXNSIP a softvérový telefón PhonerLite. Popísané a prakticky demonštrované sú rôzne typy zabezpečenia hlasového toku a signalizácie – úplne nezabezpečená komunikácia, zabezpečenie len signalizácie pomocou TLS, zabezpečenie len hlasového toku pomocou SRTP, plne zabezpečená komunikáciu pomocou TLS a SRTP a napokon je realizované zostavenie SRTP spojenia pomocou ZRTP. V závere je navrhnutý optimálny spôsob zabezpečenia VoIP komunikácie.

1. Úvod

V dnešných časoch rozmachu VoIP telefónie sa stáva jej bezpečnosť nutnosťou. Veľký dôraz sa kladie na rýchlosť prenosu a na kvalitu služieb, no na bezpečnosť sa až tak nemyslí, či už z pohľadu poskytovateľa služieb alebo aj koncového zákazníka. V prípade útoku v klasickej telefónnej siete (PSTN) je nutné sa fyzicky dostať k médiu, čo je dosť obtiažne. Lenže v prípade IP sietí, kedy sa dáta prenášajú cez Internet, tak je o dosť ľahšie zachytiť pakety [1].

Nezabezpečený VoIP hovor môže byť ľahko zneužitý či už formou odpočúvania, moduláciou hovoru alebo ukradnutím citlivých informácii, ktoré sa prenášajú v signalizačných paketoch. Väčšinou sa bezpečnosťou začíname zaoberať až po negatívnej skúsenosti, ktorá môže mať častokrát nevyčísliteľné následky. Bezpečnosť a hlavne prevencia proti útokom by mala byť rovnako dôležitá ako rýchlosť prenosu, či kvalita služieb.

2. Bezpečnostné mechanizmy v prostredí VoIP

2.1. TLS

TLS (Transport Layer Security) je nasledovníkom protokolu SSL, ktorý slúži na vytvorenie bezpečného kanála medzi dvoma komunikujúcimi bodmi. Protokol TLS pracuje na najvyššej úrovni transportnej vrstvy – je nesený transportným protokolom a zapuzdruje celý obsah tvorený vyššími vrstvami. Protokol TLS bol navrhnutý tak, aby zabezpečil ochranu pred odpočúvaním, manipuláciou alebo falšovaním správ. TLS poskytuje autentifikáciu koncových bodov, dát a ich dôvernosť. Pri základnej možnosti

zabezpečenia je autentifikovaný (to znamená, že jeho identita je zaručená) len server, zatiaľ čo klient ostáva neautentifikovaný.

Výsledkom toho je, že koncový užívateľ si môže byť istý, s kým komunikuje. Pri ďalšej úrovni zabezpečenia sú autentifikované obidve strany, čiže obidvaja účastníci si môžu navzájom dôverovať. Obojstranná autentifikácia vyžaduje používanie verejného kľúča (PKI – Public Key Infrastructure). TLS je štandardnou metódou na ochranu SIP signalizácie – zabezpečuje jej autentifikáciu a šifrovanie, takáto metóda sa nazýva SIPS [2]. Ak sú VoIP zariadenia schopné využívať TLS spojenie, prvým krokom je, že klient zostaví TLS spojenie so serverom a až následne v rámci neho si vymieňa SIP signalizačné správy. TLS vyžaduje, aby boli pri dešifrovaní všetky segmenty v správnom poradí a žiadny nechýbal, preto je nesený transportným protokolom TCP.

2.2. SRTP

Protokol SRTP (Secure Real Time Protocol) je profil pre RTP protokol, ktorý zabezpečuje dôveryhodnosť, integritu a autentifikáciu pre RTP prevádzku. Toto zabezpečenie funguje ako pre unicast, tak aj pre multicast aplikácie. V porovnaní s protokolom RTP, protokol SRTP poskytuje naviac dve polia: Authentication tag a MKI. Authentication tag je šifrovaný kontrolný súčet hlavičky a tela RTP paketu. Toto pole je odporúčané a chráni pakety od neautorizovanej zmeny obsahu. Pole MKI (Master Key Identifier) je nepovinné a identifikuje master key, od ktorého sú odvodené tajné symetrické kľúče session keys slúžiace na šifrovanie a/alebo autentifikáciu multimediálneho obsahu.

Z dôvodu bezpečnosti sa session keys v pravidelných intervaloch menia, aby útočník nemohol zhromaždiť príliš veľa dát zašifrovaných jedným kľúčom. Výhodou tohto mechanizmu je, že pre jednu reláciu stačí počas celého jej trvania preniesť len jeden master key. K tomu je použitá jedna z metód na výmenu kľúča, ako je protokol MIKEY, protokol ZRTP alebo mechanizmus SDES.

Na zaistenie dôveryhodnosti prenášaných dát sa používa symetrická kryptografická metóda AES-CTR (counter mode), ktorá pracuje ako generátor pseudonáhodných kľúčov. AES-CTR je vďaka svojej stavbe vhodná pre prenos multimediálne nepotvrdzovaného prenosu. Algoritmus umožňuje príjemcovi spracovať prijaté pakety v dopredu neurčenom poradí, čo je požadované pri použití real-time aplikácii, kde pakety nemusia byť vždy spoľahlivo doručené.

Na zaistenie autentifikácie prenášaných dát je použitý algoritmus HMAC-SHA-1. Týmto algoritmom je vytvorený kontrolný súčet z hlavičky a obsahu SRTP paketu. Táto hodnota sa uloží do pola authentication tag. Vzhľadom na to, že pri prenose sa kladie dôraz na čo najmenšiu šírku prenosového pásma je výsledný kontrolný súčet skrátený z 80 na 32 bitov. [3]

2.3. MIKEY

Protokol SRTP nedokáže sám zabezpečiť výmenu kľúčov („Key Management“), na tento účel využíva iný protokol. Jedným z takých môže byť napríklad MIKEY (Multimedia Internet Keying). Tento protokol býva zapuzdrený v protokole SDP (Session Description Protokol), ktorý obsahuje SIP správa INVITE alebo 200 OK. Celý

jeho obsah je však nešifrovaný, okrem dohodnutia bezpečnostných parametrov (šifrovacie a autentifikačné algoritmy) prenáša priamo aj master key, preto sa predpokladá zabezpečenie SIP signalizácie (napr. pomocou TLS alebo S/MIME).

2.4. ZRTP

ZRTP je definovaný ako protokol na ustanovenie kľúčov pre SRTP. Pracuje formou Diffie-Hellmanovho algoritmu na výmenu kľúčov a je realizovaný v rovine RTP spojenia, ktoré bolo predtým zostavené nejakým iným signalizačným protokolom, napríklad SIP. Výsledkom je vytvorenie zdieľaného tajomstva, z ktorého sú následne generované kľúče pre SRTP spojenie (D-H algoritmus patrí do kategórie nesymetrického šifrovania). Hlavnou črtou ZRTP je teda to, že sa nespolieha na signalizáciu SIP, ktorá je tiež schopná ustanovenia kľúčov, ani na služby žiadneho iného servera.

Dôvodom je, že výmena kľúčov pomocou signalizačných správ môže byť viditeľná pre ktorékoľvek zariadenie, ktoré je súčasťou zostavovania spojenia a ktoré je v ceste medzi koncovými bodmi (server). To zvyšuje šancu na útok, v tomto prípade by sa jednalo najmä o útoky typu „man in the middle“. Miesto toho je výmena kľúčov realizovaná iba medzi dvoma koncovými bodmi prostredníctvom RTP toku, takže kľúč poznajú len ony. Výhodné je to aj z pohľadu, že na zabezpečenie výmeny kľúčov alebo na správu kľúčov nepotrebujeme žiadnu tretiu stranu.

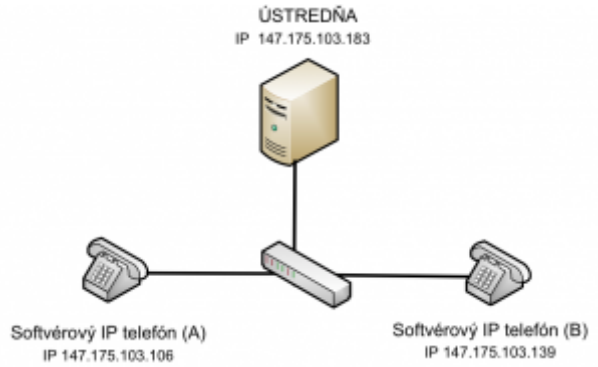
Ďalšou črtou je to, že vytvorené kľúče sú len dočasné a po ukončení komunikácie sa jednoducho vymažú, čím sa odbúrava potreba správy kľúčov aj na samotných koncových zariadeniach. ZRTP podporuje „oportunistické zabezpečenie“, čo znamená, že sa automaticky spustí ak ho podporujú obe koncové zariadenia. Je to veľmi mladý, ale zato potenciálny bezpečnostný protokol, resp. vylepšenie. Vyvinutý bol v roku 2006 Phillom Zimmermanom a jeho spolupracovníkmi a postupne sa rozširuje jeho implementácia na zariadenia. Možno ho nájsť najmä v OpenSource prostredí.

2.5. SDES

SDES (Security Descritpions) je metóda zavádzajúca priamo do SDP nový atribút, ktorým sa vymieňajú a dohadujú bezpečnostné parametre pre SRTP, okrem iného aj samotný master key. Tieto údaje však nie sú nijak šifrované, podobne ako pri MIKEY, pretože SDES sa spolieha na nižšiu vrstvu zabezpečenia ako TLS (SIPS) alebo S/MIME, ktoré majú zabezpečiť telo SIP a SDP správy [4].

3. Praktická časť

V tejto časti by som rád prakticky ukázal rozdiel medzi zabezpečenou a nezabezpečenou prevádzkou IP telefónie. Pokus som realizoval v sieti katedry telekomunikácii, kde boli vyčlenené 3 počítače – jeden poslúžil ako ústredňa a dva ako softvérové IP telefóny. Na každý počítač som nainštaloval program Wireshark, ktorým som odchytával pakety a neskôr ich analyzoval. Zostavenie pracoviska je znázornené na Obr. 1.



Obr. 1. Schéma zapojenia

3.1. Softvérové vybavenie

Pri výbere VoIP ústredne som mal veľa možností. Existuje kvantum VoIP ústrední od rôznych výrobcov, ktoré sú platené, ale aj zadarmo („freeware“) – o.i. aj tzv. „open source“ aplikácie. Pri výbere ústredne som sa riadil najmä požiadavkou, aby podporovala protokoly TLS a SRTP, no výhodou bolo aj grafické rozhranie a jednoduchá konfigurácia.

Jednou z najznámejších open source softvérových ústrední je ASTERISK, ktorá je navrhnutá pre operačný systém Linux. Grafické rozhranie GUI na ASTERISK sa nazýva ASTERISK NOW. Problém, ktorý sa vyskytol pri konfigurácii tejto ústredne bol, že ASTERISK NOW je grafické rozhranie pre distribúciu ASTERISK 1.6, ktorá, žiaľ, nepodporuje zabezpečenie pomocou TLS. Podpora zabezpečenia TLS začína až od distribúcie ASTRISK 1.8. Napokon som sa rozhodol pre inštaláciu VoIP ústredne PBXNSIP, ktorá je momentálne súčasťou SNOM ONE.

3.2. VoIP ústredňa PBXNSIP

VoIP ústredňa PBXNSIP, ktorú odkúpila firma SNOM TECHNOLOGY AG, sa momentálne nazýva SNOM ONE. Na rozdiel od ústrední typu ASTERISK, ktoré sú open source aplikácie, SNOM ONE je platená VoIP ústredňa, ktorá však ponúka freeware verziu SNOM ONE free. Táto freeware verzia je obmedzená len pre 10 VoIP čísel, čo je pre naše potreby postačujúce.

Táto ústredňa je typu „back-to-back user agent“ (B2BUA), čo znamená, že všetky pakety prechádzajú cez ústredňu, či už sa jedná o signalizačné pakety alebo následný prenos hlasu medzi dvoma VoIP telefónmi. Pomocou tejto vlastnosti môže priamo ústredňa riadiť prevádzku a VoIP telefóny sú od seba úplne nezávislé. Keďže celá prevádzka ide cez ústredňu, každý VoIP telefón môže používať rozdielne nastavenie a nemusí byť závislý od iného účastníka. Dôležitý bezpečnostný aspekt pri tomto type ústredne je aj ten, že telefóny si navzájom nevidia svoje IP adresy.

Takýto typ ústredne však môže mať aj nevýhodu, a to takú, že si nie sme istí bezpečnosťou pri prenose dát medzi druhým účastníkom a ústredňou, napriek tomu, že prevádzka medzi nami a ústredňou je maximálne zabezpečená. Problémom môže byť aj relatívne vyšší nárok na procesorový výkon ústredne, a to hlavne v prípade zabezpečenej hlasovej komunikácie pomocou SRTP, kedy dochádza v ústredni k tzv. „SRTP transcoding“ (iba v prípade výmeny SRTP kľúča cez SDES, pri použití ZRTP je SRTP spojenie vytvorené priamo medzi volajúcimi účastníkmi aj napriek B2BUA

architektúre ústredne). To znamená, že ústredňa musí odšifrovať SRTP dáta a ak druhá strana podporuje SRTP, tak ich na výstupe znova zašifruje. [5]

Ústredňu PBXNSIP je možné nainštalovať aj na operačný systém Windows. Nastavenie a konfigurácia je zabezpečená pomocou webového rozhrania cez http://localhost. Táto ústredňa po správnom nakonfigurovaní beží non-stop na pozadí.

Ústredňa PBXNSIP podporuje bezpečnostné protokoly TLS a SRTP. Protokol TLS vyžaduje digitálny certifikát a používanie súkromného kľúča na bezpečnú prevádzku. Pri použití bezpečnostného protokolu SRTP, ústredňa PBXNSIP podporuje bezpečnostný mechanizmus na výmenu kľúča SDES, ale, žiaľ, nepodporuje MIKEY. Na tento fakt som si musel dať pozor pri výbere softvérového IP telefónu, pretože niektoré softvérové IP telefóny podporujú prenos kľúčov pomocou SDES a iné zasa pomocou MIKEY, pričom táto kompatibilita je veľmi dôležitá. Pri použití protokolu ZRTP na výmenu kľúča by mala byť ústredňa transparentná, no pri niektorých typoch ústredne ZRTP napriek tomu nefunguje. PBXNSIP je jednou z nich (okrem iného aj Asterisk [6]), no tento problém sa dá obísť pomocou mechanizmu „ZRTP Masquerade“.

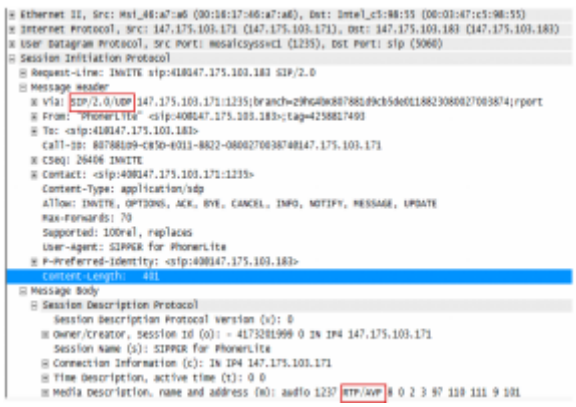
3.3. Softvérový IP telefón

Ako softvérový VoIP telefón som si vybral program PhonerLite (verzia 1.87). Jedná sa o aplikáciu, ktorá beží pod operačným systémom Windows, pracuje so signalizačným protokolom SIP a je freeware. Z bezpečnostného hľadiska tento VoIP telefón podporuje TLS pre zabezpečenie signalizácie a protokoly SRTP a ZRTP. Pre výber aplikácie Phonerlite som sa rozhodol hlavne preto, lebo podporuje zabezpečenie SRTP . Na výmenu kľúčov využíva mechanizmus SDES, tak isto ako VoIP ústrednňa PBXNSIP, čím je dosiahnutá vzájomná kompatibilita. Zároveň podporuje mechanizmus ZRTP Masquerade, zatiaľ síce len priamym dopísaním riadku „ZRTP_Masquerade=1“ do konfiguračného súboru sipper.ini. [7]

4. Sledovanie VoIP prevádzky

4.1. Nezabezpečená VoIP komunikácia

Na Obr. 2 je zobrazený obsah odchyteného paketu medzi IP telefónom a ústredňou PBXNSIP. Keďže je komunikácia nezabezpečená, paket je kompletne čitateľný. Jedná sa o správu INVITE protokolu SIP, ktorý sa prenáša pomocou protokolu UDP.



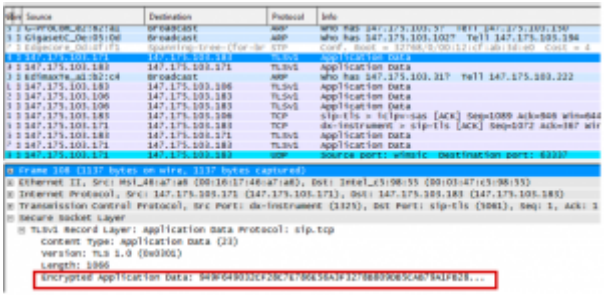
Obr. 2. Odchytený paket SIP správy INVITE

V poli Media Description vidíme údaj **RTP/AVP**, jedná sa teda o nezabezpečený prenos hlasu cez RTP. Skratka AVP znamená „Audio Video Profile“. Z odchyteného paketu môžeme vyčítať IP adresu softvérového telefónu 147.175.103.171 , port cez ktorý komunikujeme 1235, softvér aký používame – User-Agent: SIPPER for PhonerLite, SIP URI adresu 40@147.175.103.183 a mnoho iných pre potencionálneho útočníka dôležitých informácii. Takisto je možné pomocou Wiresharku jednoducho odfiltrovať RTP pakety a následne ich prehrať ako zvukovú stopu.

4.2. Zabezpečenie signalizácie pomocou TLS bez zabezpečenia hlasových dát

Ústredňa aj softvérový IP telefón PhonerLite podporujú zabezpečenie signalizácie pomocou TLS. Hlasové pakety vidíme vo Wiresharku ako UDP, ale dokážeme ich dekódovať ako RTP pakety, ktoré sú čitateľné rovnako ako pri nezabezpečenom spojení. Jedine signalizácia je zabezpečená, jej zašifrovaný obsah vidíme na Obr. 3 ako Encrypted Application Data.

Z tohto dôvodu nebolo možné vo Wiresharku využiť funkciu VoIP Calls, ktorá dokáže mapovať VoIP komunikáciu a takisto dokáže prehrať RTP pakety. Vo Wiresharku vidíme signalizačné pakety ako nečitateľné TLS, teda tak ako putujú sieťou. Avšak na samotnom softvérovom telefóne, pri použití Debug módu, môžeme vidieť odšifrované SIP správy, teda tak ako ich „vidí“ softvérový IP telefón. V poli Via môžeme vidieť text **SIP/2.0/TLS** a v poli m=audio vidíme, že sa jedná o nešifrovaný prenos hlasových dát **RTP/AVP**.



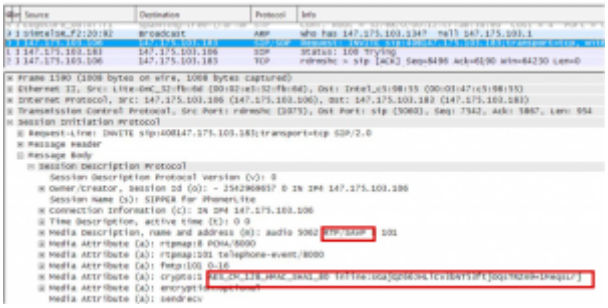
Obr. 3. Zašifrovaný obsah signalizačných SIP správ

4.3. Zabezpečenie komunikácie pomocou SRTP bez zabezpečenia signalizácie

Pri nastavení obidvoch IP telefónov tak, že na prenos hlasového toku sa používa protokol SRTP (s dohodnutím kľúčov pomocou metódoy SDES) a na prenos signalizácie TCP alebo UDP, čiže signalizácia je nezabezpečená, sa môžeme stretnúť so zaujímavým javom. Pakety sú zabezpečené len jedným smerom, a to od ústredne k softvérovému IP telefónu, ktorý inicioval spojenie (IP telefón A – 147.175.103.106). Aby sme zistili, čo je príčinou tohto správania sa, je potrebné pozrieť sa pozrieť na signalizačné SIP správy.

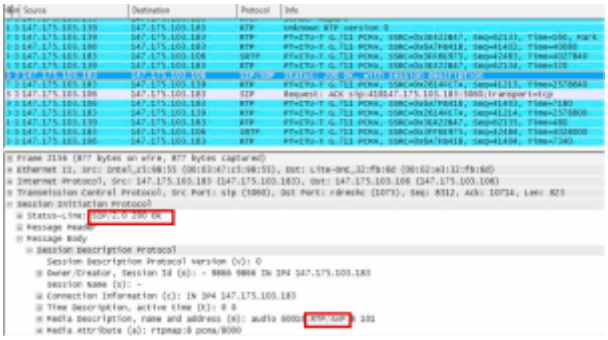
IP telefón A vyšle SIP správu INVITE (Obr. 4), kde je zapuzdrená správa protokolu SDP a v ňom je požiadavka na SRTP spojenie (konkrétne RTP/SAVP („Secure Audio Video Profile“)). Zároveň sa je tu čitateľný aj samotný master key (inline=) , ktorý sa posiela v nezašifrovanej forme, teda odchytením dokážeme dešifrovať celý nasledujúci hlasový prenos. V takomto prípade je teda použitie SRTP bezvýznamné. Okrem iného môžeme vidieť aj požiadavku na šifrovacie a autentifikačné algoritmy, ktoré chce IP

telefón A používať.



Obr. 4. Zachytený protokol SDP v správe INVITE

Od ústredne príde tomu istému softvérovému IP telefónu odpoveď 200 OK (Obr. 5), v ktorej je však už len údaj **RTP/AVP**, teda požiadavka na normálny RTP prenos.



Obr. 5. Zachytený protokol SDP v správe 200 OK

Napriek tomu, že aj na IP telefóne B sme nastavili prenos hlasu cez SRTP, tak ústredňa zostavila spojenie s IP telefónom B (147.175.103.139) už len ako RTP/AVP, čiže nezabezpečene. Hlasové dáta sú potom prenášané nasledovným spôsobom:

- od ústredne k IP telefónu A cez SRTP (pretože IP telefón A si v správe INVITE vyžiadal SRTP spojenie),
- opačným smerom od IP telefónu A do ústredne cez RTP (pretože ústredňa v SIP správe 200 OK žiadala RTP spojenie),
- obojsmerný prenos medzi ústredňou a IP telefónom B cez RTP (pretože ústredňa vo svojej správe INVITE adresovanej IP telefónu B žiada len RTP spojenie)

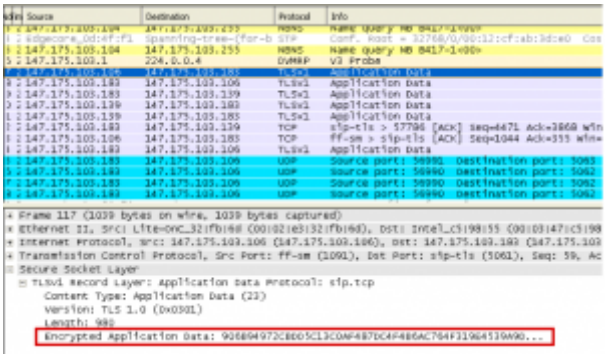
Naskytá sa otázka, prečo dochádza k takémuto správaniu, aj napriek tomu, že ústredňa aj IP telefóny podporujú SRTP spojenie a na oboch IP telefónoch bolo nastavené použitie SRTP. Odpoveď je taká, že prenos cez SRTP všetkými smermi ústredňa podporuje len v prípade, ak je zabezpečená aj signalizácia, napríklad cez TLS. Je logické, že nemá zmysel šifrovať hlasový tok, keď si útočník dokáže jednoducho odchytiť kľúč posielaný v nezašifrovanom stave a následne pomocou neho celý hlasový tok odšifrovať.

Môžme považovať skôr za nedostatok IP telefónu, že podporuje prenos cez SRTP bez zabezpečenej signalizácie. Na druhej strane môžme túto možnosť aspoň využiť pre potreby výskumu. Preto by som navrhoval, aby v takomto prípade softvérový telefón užívateľa upozornil, že hlasová komunikácia nebude bezpečná a odporučil užívateľovi použitie protokolu TLS na zabezpečenie signalizácie.

4.4. Zabezpečenie signalizácie pomocou TLS a hlasových dát pomocou SRTP

Pri zabezpečení signalizácie pomocou TLS už nedokážeme SIP správy vo Wiresharku prečítať. Hlasové pakety tu vidíme ako UDP, napriek tomu, že sú SRTP – ako však bolo spomenuté vyššie, PhonerLite má možnosť pomocou nástroja Debug zobraziť signalizáciu tak, ako ju prijal/vyslal. V nej vidíme jednak informáciu o zabezpečení signalizácie **SIP/2.0/TLS**, ale taktiež údaj **RTP/SAVP** a master key v správach INVITE aj v 200 OK, a to v oboch smeroch. Znamená to, že medzi IP telefónom A a ústredňou a tak isto aj medzi ústredňou a IP telefónom B prebieha hlasová komunikácia prostredníctvom zabezpečeného SRTP toku.

Prenos, pri ktorom zabezpečíme dátový tok pomocou protokolu SRTP a zároveň aj signalizáciu pomocou protokolu TLS, je z hľadiska bezpečnosti aj z hľadiska efektívnosti najlepší. Pri protokole SRTP treba dať veľký dôraz na prenos kľúčov, preto je použitie protokolu TLS na zabezpečenie signalizácie nevyhnutné (ako som ukázal na predchádzajúcom príklade, použitie SRTP bez bezpečnej výmeny kľúčov je bezpredmetné). Takúto kombináciu zabezpečenia (TLS + SRTP) nám podporuje aj ústredňa aj náš IP telefón.

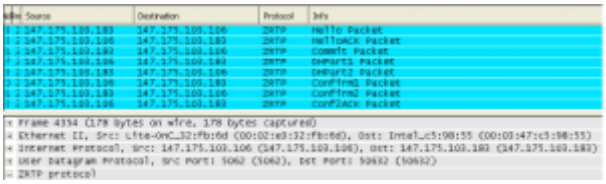


Obr. 6. Zachytené pakety pri plne zabezpečenej komunikácii

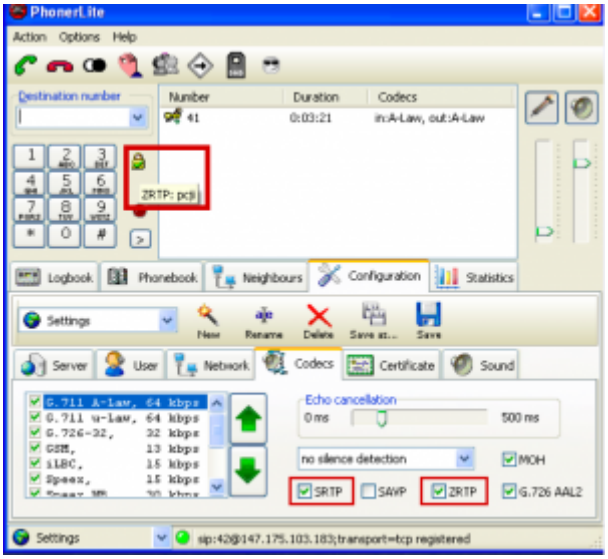
4.5. Zabezpečenie hlasových dát s využitím protokolu ZRTP

Druhá alternatíva k vytvoreniu SRTP spojenia je využitie protokolu ZRTP. Na Obr. 7 je znázornený priebeh vytvárania spojenia pomocou ZRTP. Tento protokol, ktorý pracuje súčasne s protokolom SRTP, pomáha pri vzájomnej výmene kľúčov, pri ktorej využíva Diffie-Hellmanov algoritmus. Táto výmena kľúčov nie je závislá od signalizačného protokolu SIP, ktorý, ak je nezabezpečený, dokážeme ľahko prečítať, ale je realizovaná v rovine RTP spojenia.

Na Obr. 8 vidíme, ako nám PhonerLite ukazuje, že výmena kľúčov bola realizovaná pomocou protokolu ZRTP (ikonka zámku a nápis **ZRTP:pcji**). Ak by softvérový IP telefón nepodporoval výmenu kľúčov pomocou protokolu ZRTP, dokážeme ho aj napriek tomu zrealizovať napríklad doplnkovým programom Z-Lite. Z-Lite nie je softvérový IP telefón, ale len doplnok, ktorý sa stará o zostavenie ZRTP spojenia, a je na softvérovom IP telefóne nezávislý. Tak isto ZRTP spojenie je úplne nezávislé od ústredne. Tento druh zabezpečenia hlasovej komunikácie sa tiež javí ako dostatočne bezpečný a efektívny.



Obr. 7. Zachytené ZRTP pakety vo Wiresharku



Obr. 8. Nastavenie softvétového telefónu pre použitie ZRTP

5. Záver a zhodnotenie práce

Pri výbere VoIP ústredne a softvérových IP telefónov treba klásť veľký dôraz na ich vzájomnú kompatibilitu. Aj keď ústredňa i IP telefón podporujú zabezpečenie pomocou SRTP, problém môže nastať v spôsobe výmeny kľúčov. Niektoré aplikácie podporujú výmenný mechanizmus pomocou SDES, iné zasa pomocou protokolu MIKEY. Naša ústredňa podporovala síce len mechanizmus SDES, no ten sa vďaka svojej jednoduchosti stáva dominantným spôsobom výmeny SRTP kľúča vo VoIP aplikáciách. Pre použitie ZRTP medzi dvoma softvérovými telefónmi bolo zas potrebné aplikovať metódu „ZRTP masquerade“, inak toto spojenie ústredňa blokovala.

Pri testovaní zabezpečenia hlasu pomocou SRTP s tým, že signalizácia ostala nezabezpečená, sa ukázalo, že takéto zabezpečenie je nefunkčné, pretože nedošlo k bezpečnej výmene kľúčov. Ústredňa bez upozornenia posielala pakety ako RTP, nie ako SRTP. Pre neznalého používateľa je to pomerne nebezpečné, pretože sa mylne domnieva, že jeho hlasová komunikácia je zabezpečená, no napriek tomu nie je. V tomto prípade je na mieste návrh, aby IP telefón upozornil na fakt, že SRTP bez zabezpečenia výmeny kľúčov nemusí byť ústredňou podporované a ak aj je, tak sa stále jedná o málo bezpečnú formu komunikácie. Preto by mal IP telefón navrhnúť aj použitie TLS na zabezpečenie signalizácie.

Ako najvhodnejšiu formu zabezpečenia môžeme vyhodnotiť kombináciu protokolu SRTP, ktorý dokáže zabezpečiť prenos hlasového toku, spolu s bezpečnostným protokolom TLS, ktorý dokáže zaručiť bezpečný prenos signalizácie a tým aj výmenu kľúčov pre protokol SRTP. Zároveň je overená plná kompatibilita zvolenej ústredne a softvérového telefónu pre tento prípad. Výmena kľúčov môže plnohodnotne fungovať aj bez zabezpečenia signalizácie, a to pomocou protokolu ZRTP. Napriek tomu treba

myslieť na to, že v signalizácii sa nachádza stále veľa citlivých informácii, takže vždy treba zvážiť aj jej zabezpečenie.

6. Odkazy na literatúru

1. Vozňák, M., Řezáč, F.,“Security Risks in IP Telephony“, CESNET 2010
2. Rosenberg, J.,Schulzrinne, H., Camarillo, G., „SIP: Session Initiation Protocol“, IETF RFC 3261, June 2002 http://www.ietf.org/rfc/rfc3261.txt
3. Baugher, M., McGrew, D., Cisco Systems, Inc. „The Secure Real-time Transport Protocol (SRTP)“, IETF RFC 3711, March 2004, http://www.faqs.org/rfcs/rfc3711.html
4. VOCAL Technologies, 2011, http://www.vocal.com/security/sdes.html
5. PBXNSIP, Inc 2005-2011, [online] http://kiwi.pbxnsip.com/index.php/Main_Page
6. SWADVISORY, [online] http://www.swadvisory.com/cryptocalls/index.php?option=com_content&view=article&id=229&Itemid=355
7. Sommerfeldt, H., PhonerLite, [online] http://www.forum.phoner.de/YaBB.pl?num=1286529596/0
8. Zmolek, A., et al., “Practical VoIP Security”, Syngress Publishing, ISBN 1597490601, June 2006
9. Kuhn, R.D., „Security Consideration for Voice over IP Systems“, NIST Special Publication 800-58, January 2005

Spoluautorom článku je Ing. Adam Tisovský , Katedra Telekomunikácií, Fakulta Elektrotechniky a Informatiky, Slovenská Technická Univerzita, Ilkovičova 3, Bratislava 812 19

Práca bola prezentovaná na Študentskej vedeckej a odbornej činnosti (ŠVOČ 2011) v sekcii Telekomunikácie I. a získala **Diplom dekana**, ISBN 978-80-227-3508-7