Teorie a praxe IP telefonie – 2. dvoudenní odborný seminář
Hotel Olšanka, 8. a 9. listopadu 2006

Bezpečnost provozu VoIP

Tomáš VANĚK
pracoviště: Katedra telekomunikační techniky, ČVUT-FEL,
mail: vanekt1@fel.cvut.cz

Abstrakt: *Technologie přenosu hlasu v sítích IP se úspěšně zabydluje mezi širokou veřejností bez ohledu na možná bezpečnostní rizika. Tento článek popisuje některé typy útoků na internetovou telefonii a popisuje stávající mechanismy, které umožňují těmto hrozbám čelit a realizovat bezpečný přenos hlasu se zaměřením na protokol SIP. Součástí příspěvku je i demonstrace odposlechu nezabezpečeného hovoru.*

1 Úvod

Díky zatím nepříliš masovému rozšíření a používání protokolů VoIP (ve srovnání s např. s elektronickou poštou IM, nebo WWW) jsou útoky na VoIP zatím relativně méně časté, ale není žádný důvod se domnívat, že s postupným rozšiřováním těchto služeb nebude počet těchto útoků přibývat. Řadu dnes známých útoků na protokoly lze modifikovat tak, aby jimi bylo možné ohrožovat protokoly VoIP. Protokoly samy jsou sice vybaveny metodami, které dokáží zajistit určitý stupeň zabezpečení, ale v praxi tyto metody nejsou příliš používány. V následujících kapitolách jsou popsány některé možné typy útoků na VoIP protokoly a obecné metody ochrany proti nim (s důrazem na protokol SIP).

2 Útoky na VoIP protokoly

V oblasti internetové telefonie existuje celá řada hrozeb. Cílem útoku mohou být síťová zařízení, servery, operační systémy serverů, aplikace, síťové protokoly, telefony a jejich software. Všechna tato zařízení mohou být cílem útoků, které se principielně nijak neliší od útoků které již dnes existují na stávající servery, protokoly a aplikace. Zde popisované útoky na VoIP protokoly jsou analogií útoků, které již existují proti jiným síťovým protokolům.

Únos registrace / MitM (Man in the Middle) – Registrátor povoluje přístup na základě identity UA. Pole From: , které je součástí záhlaví žádosti SIP o spojení může být libovolně upraveno. Tím lze dosáhnout neoprávněné registrace. Hovory v sítích IP jsou více náchylné na únosy a útoky typu MitM než hovory v klasických telefonních sítích. Útočník v takovém případě naruší spojení a modifikuje

parametry volání. To může proběhnout bez zaznamenání ze strany komunikujících účastníků a útočník tak může sledovat nebo přesměrovávat cizí hovory, případně se vydávat za někoho jiného. Možná obrana – šifrování a testování integrity dat přenášených v signalizačním kanále.

Falšování – Informace o spojení je skoro stejně cenná jako vlastní obsah hovoru. V případě kompromitace signalizačního serveru může získat útočník plnou kontrolu nad vytvářením, správou a rušením příchozích i ochozích hovorů. Může hovory přesměrovávat, zaznamenávat, vkládat pakety s upraveným obsahem. Možná obrana – šifrování a integrita datového spojení, správná konfigurace proxy serverů.

Rušení spojení – útočník může rušit spojení posíláním zpráv BYE. Možná obrana – akceptovat zprávy pouze z autorizovaných zdrojů.

DoS a dDoS útoky – Tento typ útoků se zaměřuje na znepřístupnění určité služby nebo části sítě. Útok je vyvolán velkým počtem požadavků směrovaných na konkrétní službu/server. Typickým cílem DoS útoku budou SIP proxy, které jsou připojené do Internetu. Příkladem může být například vygenerování velkého množství zpráv INVITE (v případě protokolu SIP) a tím zahlcení proxy serveru. V klasické telefonní síti se tento typ útoků takřka nevyskytuje, ale v počítačových sítích lze relativně snadno způsobit přetížení vybraných spojů. Možná obrana – limity pro zpracovávání INVITE zpráv, autentizace uživatelů před posláním INVITE.

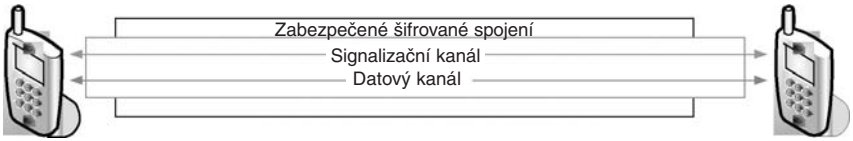
Viry a trójské koně pro VoIP SW a HW – VoIP telefony představují cíle samy o sobě. Přestože se VoIP telefony často tváří jako obyčejný „klasický telefon" ve skutečnosti to je počítač s příslušným softwarem. A tento software může být cílem naprosto stejných útoků jaké se dnes a denně objevují u běžných operačních systémů nebo aplikačního software. Výsledkem takového útoku pak může být nefunkčnost telefonu, nebo jakákoliv nepřátelská akce typu nahrávání telefonních hovorů nebo jejich přesměrování . V případě SW VoIP telefonů je situace naprosto stejná.

SPAM overVoIP – rozesílání nevyžádaných zpráv reklamního charakteru. Možná obrana – kontrola zdrojových adres.

Voice Phishing – získávání osobních dat od důvěřivých lidí. Možná obrana – vzdělávat uživatele.

3 Zabezpečení komunikace protokolu SIP

Problematiku zabezpečení lze rozdělit na dvě části. Zabezpečení signalizačního kanálu a zabezpečení vlastního hovoru. Z tohoto úhlu pohledu lze realizovat několik různých scénářů, které jsou naznačeny na obrázcích jedna až čtyři.

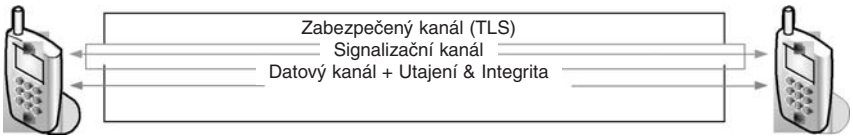


Obrázek 1 – Společné zabezpečení signalizačního a datového kanálu pomocí protokolů nižších vrstev – IPSec

V případě varianty společného zabezpečení signalizačního i hovorového kanálu je nutné před sestavením spojení sestavit bezpečný kanál ve kterém se poté přenáší jak signalizace, tak i užitečná data. Technologií, která zde připadá do úvahy je IPsec. Druhou možností je oddělené zabezpečení signalizačního a datového kanálu. Signalizace může být zabezpečena pomocí S/MIME a vlastní hlasová data pomocí SRTP.

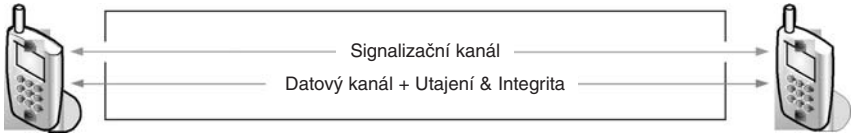
Obrázek 2 – Oddělené zabezpečení komunikace – S/MIME + SRTP

Varianty jedna a dvě jdou zkombinovat tak, jak je znázorněno na obrázku číslo tři, kde zabezpečení signalizačního kanálu je realizováno pomocí protokolů nižších vrstev například TLS a zabezpečení datového kanálu pomocí SRTP.



Obrázek 3 – Kombinované zabezpečení komunikace – TLS + SRTP

Poslední obrázek pak ukazuje použití protokolu zRTP, který je schopen zajistit zabezpečené spojení, i když jsou tyto parametry vyjednány přes nezabezpečený signalizační kanál. Protokol zRTP je nyní posuzován organizací IETF jako draft.



Obrázek 4 – Zabezpečení pouze datového kanálu – zryl

3.1 Zabezpečení SIP signalizace

Protože struktura zpráv protokolu SIP vychází z protokolu http je možné aplikovat bezpečnostní mechanismy dostupné pro HTTP i do prostředí SIPu. URI sips:// pak analogicky s https:// vytváří bezpečný tunel zabezpečený pomocí protokolu TLS. Na druhou stranu lze použít i zabezpečení pomocí S/MIME nebo PGP, které mají svůj původ v e-mailové komunikaci. Poslední zmiňovanou možností je realizace šifrovaných tunelů pomocí rozšíření IPsec, které představuje obecný mechanismus zabezpečení komunikace na úrovni síťové vrstvy. Přehled hlavních způsobů zabezpečení relací SIP je uveden v tabulce 1. V současné verzi SIPu je nepřijatelné používání některých autentizačních metod (HTTP 1.0 nebo PGP), které v původní verzi SIPu byly akceptovány.

HTTP základní autentizace

Základní autentizace pomocí HTTP spočívá v přenosu uživatelského jména a hesla v záhlaví hlavičky zprávy http-request. V prostředí SIPu to umožňuje, aby proxy server nebo koncový UA ověřil identitu SIP klienta nebo identitu předchozího SIP proxy serveru. Protože heslo se přenáší v otevřeném tvaru, je možné ho jednoduše odchytit a tím pádem je tato varianta autentizace nebezpečná a ve verzi SIPv2 byla odmítnuta. Dalším důvodem k nepoužívání tohoto způsobu zabezpečení je fakt, že data nejsou žádným způsobem šifrována a anení zajištěna jejich integrita.

Rozšířená HTTP autentizace

Zdokonalená verze základní HTTP autentizace. Funguje na principu výzva-odpověď. Heslo a náhodný řetězec označovaný jako výzva (challenge) jsou přivedeny na vstup hashovací funkce MD-5 nebo SHA-1 a výsledek je poté odeslán.

Tato varianta autentizace je bezpečnější než základní HTTP autentizace, protože zde nedochází k přenosu hesla v otevřeném tvaru. V případě volby slabého hesla je tato metoda náchylná na slovníkový útok. Další nevýhodou je fakt, že žádným způsobem není zajištěno utajení a integrita vyměňovaných zpráv.

Pretty Good Privacy (PGP)

Jednou z dalších možností zabezpečení SIPu (autentizace a šifrování) bylo použití programu Pretty Good Privacy , ale od verze 2 SIPu je tato volba vypuštěna na úkor standardu S/MIME.

S/MIME

MIME formát je určen k použití primárně v e-mailové komunikaci. Definuje, jak mají vypadat jednotlivé zprávy, tak aby mohly být vyměňovány mezi různými poštovními servery. Těla MIME zpráv mohou obsahovat text, obrázky, ale i video a zvuk, což je činí použitelnými také pro IP telefonii. S/MIME standard obsahuje metody pro zabezpečení MIME a to pomocí kontroly integrity a šifrováním. K identifikaci koncového uživatele a jeho veřejného klíce jsou používány X.509 certifikáty. S/MIME zprávy obsahují tedy MIME tělo, které je šifrováno symetricky, a dále symetrický klíc k jejímu dešifrování. Autentizace uživatelů probíhá pomocí certifikátů X.509. Určitý problém představuje šifrování zpráv MIME (např. obsah SDP paketů), protože k šifrování se používá veřejný klíč příjemce, který je potřeba nejprve získat z příslušného certifikátu X.509 a ověřit jejich platnost. Proto se musí tyto klíče získat a ověřit ještě před vlastním přenosem z nějakého veřejného zdroje nebo pomocí speciální SIP zprávy. Dalším problémem je, že certifikační autorita (CA) vydávající certifikáty musí být důvěryhodná pro všechny účastníky komunikace. Protože self-signed certifikáty nezaručují dostatečnou míru bezpečí ,je nutné použít certifikáty vydané některou renomovanou komerční CA (např.Verisign, Thawte,…) což zvyšuje celkové náklady na implementaci.

SIPS

Použití URI (Uniform Ressource Identifier) ve tvaru sips:volany@nejakadomena.cz místo sip:volany@nejakadomena.cz. ve zprávě INVITE indikuje požadavek na zabezpečení celé cesty pomocí protokolu TLS. TLS je mírně inovovaný protokol SSL. Protože každý proxy server na cestě mezi zdrojem a cílem přidává do SIP záhlaví své směrovací informace, musí se zabezpečení pomocí TLS realizovat mezi každými dvěma zařízeními v cestě. Další podmínkou je použití TCP jakožto protokolu transportní vrstvy a existence PKI pro správu certifikátů resp. klíčů.

IP Security (IPsec)

IPsec je zcela obecný nástroj k realizaci bezpečných šifrovaných spojení. Pracuje na síťové vrstvě a je tvořen třemi základními protokoly – AH, ESP a IKE. Pro zabezpečení SIPu lze použít protokoly AH nebo ESP v transportním režimu. Potřebné bezpečnostní asociace (SA) mohou být sestaveny trvale a nezávisle na SIPových UA nebo mohou být vytvářeny podle potřeby samotnými UA nebo proxy servery. Protokol IKE slouží k nastavení bezpečnostních asociací a podporuje jak autentizaci pomocí PSK (předsdílených klíčů), tak i na základě PKI. Varianta s PSK se nehodí pro sítě s velkou fluktuací klientů. Tam se hodí spíše verze s certifikáty X.509 a PKI. Tato varianta je ale náročná nejen z finančního hlediska ale i vyšší obtížnosti konfigurace (v porovnání s PSK).

Způsoby autentizace: PSK – Pre Shared Key PKI – Public Key Infrastructure	Autentizace	Utajení	Integrita	
HTTP 1.0	PSK	NE	NE	heslo se přenáší v otevřeném tvaru; odmítnuto ve verzi SIPv2
HTTP 1.1	PSK	NE	NE	autentizace typu C/R pomocí MD5
PGP	PKI	ANO	ANO	odmítnuto ve verzi SIPv2
S/MIME (Secure MIME)	PKI	ANO	ANO	odesílatel musí mít k dispozici veřejný klíč příjemce jinak nelze šifrovat
TLS (sisp:)	PKI	ANO	ANO	všechny aplikace i proxy servery musí používat TLS
IPsec (IP Security)	PKI	ANO	ANO	musí podporovat proxy servery

Tabulka 1 – Možnosti zabezpečení signalizace SIP

3.2 Zabezpečení RTP streamů

Hlasové (ale i obrazové) streamy se v IP sítích přenášejí pomocí protokolu RTP (Real-Time Protocol), který jako transportní protokol používá UDP. Aby měla vysílací strana informace o kvalitě přijímaného proudu, příjemce v pravidelných intervalech odesílá pomocí RTCP (Real Time Control Protocol) zprávy obsahující potřebné informace parametrech spojení. Protože audio a video přenosy jsou velmi citlivé na zpoždění (delay) a kolísání zpoždění (jitter) nesmí žádná metoda, kterou budeme zabezpečovat data (ať již z hlediska utajení nebo integrity) nijak vý-

znamně ovlivňovat tyto parametry (tzn. zpoždění a jitter). Existují dva standardizované kryptografické protokoly, které vyhovují tomuto zadání a jsou k dispozici a jeden, který je zatím ve stádiu draftu. Jedná se o protokoly SRTP, IPsec a zRTP.

Secure RTP (SRTP)

Secure Real-time Transport Protocol (SRTP) představuje rozšíření RTP. Základním cílem je pro RTP a RTCP pakety zajistit utajení, autentizace a ochranu proti replay útokům (útok opakovaným přehraním zpráv). O utajení se stará moderní algoritmus AES v režimu CTR, který nijak nezvětšuje velikost přenášených dat. Data jsou na druhé straně zvětšena o autentizační hlavičku, která každý paket navýší o 10B.

IPsec

IPsec představuje druhou možnost jak zabezpečit datový proud na úrovni síťové vrstvy. Zde je možné využít stejných SA jaké se použily při zabezpečení signalizačního kanálu. Hlavní nevýhodou je velká

režie IPsecu (37B na RTP paket v případě šifrování pomocí 3DES a 53B na RTP paket v případě použití algoritmu AES-128) a špatná schopnost průchodu IPsec paketů skrz NAT.

zRTP

zRTP je rozšíření standardního RTP. Popisuje implemtaci Diffie-Hellmanova algoritmu pro výměnu klíčů, který umožňuje vygenerovat sdílenou tajnou informaci, kterou lze poté použít k sestavení zabezpečeného spojení pomocí SRTP. Jedním z autorů je známý Phil Zimmermann. 5. března 2006 byl odeslán návrh doporučení zRTP do IETF a v současné době je posuzován. Jednou z výhod zRTP je skutečnost, že k sestavení zabezpečeného spojení nepotřebuje PKI nebo předsdílené klíče (PSK). Původní Diffie-Hellmannův algoritmus byl náchylný na útok typu MitM (Man-in-the-Middle). Z toho důvodu používá zRTP mechanismu SAS (Short Authencication String), který tuto zranitelnost napravuje. Spočívá ve výpočtu hashe dvou Diffie-Hellmanových hodnot. Každá strana si spočítá hodnotu SAS na své straně komunikačního řetězce. Jiným kanálem (např. telefonním) si sdělí vypočtenou hodnotu SAS. Pokud jsou stejné, pak s velkou pravděpodobností není kanál předmětem útoku.. Útočník může pouze odhadovat jaké SAS má odeslat a již při malých velikostech SAS je jen málo pravděpodobné, že jeho útok nebude odhalen. Pro SAS délky 16 bitů je pravděpodobnost odhalení více než 99,9985% (1:65535). Dalším prvkem zvyšujícím odolnost proti MitM útokům je tzv. kontinuita klíčů. Obě strany si uchovávají hashe z klíčů použitých v daném hovoru aby je v příštím hovoru smíchaly se sdílenou tajnou informací vyměněnou

pomocí Diffie-Hellmanova algoritmu. Tento postup zajistí, že pokud nebyl MitM útok vedený v prvním hovoru, nemůže být úspěšný ani v žádném dalším.

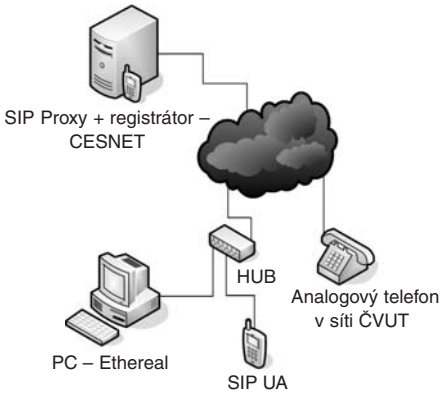
Způsoby autentizace: DH – Diffie-Hellman PSK – Pre Shared Key PKI – Public Key Infrastructure	Autentizace	Utajení	Integrita	
SRTP (Secure RTP)	PSK	ANO	ANO	Klíče se musí dopředu distribuovat nějakým jiným způsobem
zRTP (Zimmermann RTP)	DH	ANO	ANO	klíče jsou dohodnuty pomocí modifikovaného DH algoritmu / není schválen IETF
IPSec (IP Security)	PKI	ANO	ANO	Není nutné integrovat IPsec do SIP aplikace, pokud je peer důvěryhodný

Tabulka 2 – Možnosti zabezpečení RTP proudů

4 Zachycení a následná rekonstrukce VoIP hovoru

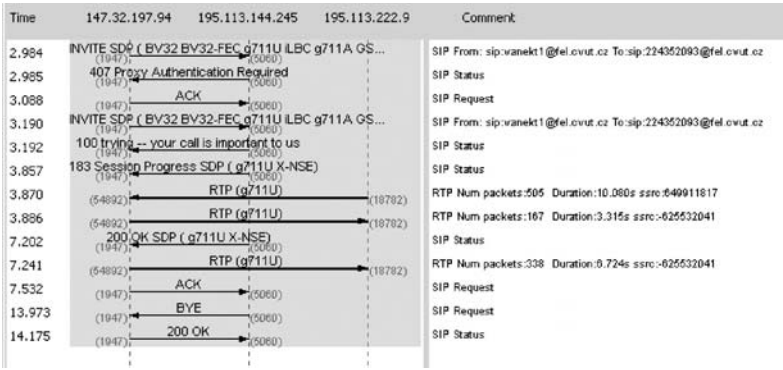
Odposlech hovoru realizovaného pomocí VoIP lze poměrně jednoduše realizovat i bez zvláštního vybavení. Následující postup se týká pouze protokolu SIP, ale lze ho jednoduše aplikovat na H.323 i jiné protokoly VoIP. Jedinou podmínkou, kterou musíme splnit je přístup k fyzickému médiu, po kterém probíhá hovor. K zachycení paketů použijeme program Ethereal. Tento program vyvíjený pod GPL licencí umožňuje zaznamenávat a analyzovat nejrůznější protokoly používané v počítačových sítích.

Obrázek 5 znázorňuje zapojení pracoviště. Základem je PC s Etherealem a SIP telefon připojený do společného hubu. Tím bylo umožněno, aby Ethereal mohl odposlouchávat spojení mezi SIP telefonem a analogovým telefonem, který představoval druhou komunikující stranu. Pokud bychom místo hubu použili switch, při normálním provozu by byl odposlech nemožný. Existují však různé útoky na úrovni linkové vrstvy, které ve svých důsledcích odposlech umožní. Jde např. o ARP cache poisoning, kdy se veškerý datový tok přesměruje přes útočníkovo PC nebo MAC flooding, kdy se zaplní tabulka MAC adres ve switchi a ten se pak začne chovat jako hub. Proti těmto útokům samozřejmě existují postupy nástroje na obranu, ale bývají implementovány pouze u dražších switchů. Z VoIP telefonu byl uskutečněn hovor na telefon připojený do sítě ČVUT. Tento hovor byl současně zaznamenáván na PC pomocí již zmiňovaného programu Ethereal.



Obrázek 5 – Schéma zapojení pro odposlouchování hovorů

Z dat, která jsme získali odposlechem je již velmi jednoduché si vyfiltrovat ty pakety, které nás zajímají. V rámci analýzy VoIP lze určit komunikující strany, použité kodeky , zobrazit zpoždění a jiter, najít příslušné RTP streamy, a mnoho dalších informací. Jednou z možností je i uložení vlastních dat přenášených protokolem RTP. Tato data již neobsahují nic jiného nežli digitalizovaný hlas. Pokud byl použit kodek G.711 je možné přímo z Etherealu uložit zvuková data ve formátu .au , která lze poté přehrát např. v programu WinAmp. V případě, že komunikující strany používají kodek, který Ethereal zatím nezná (např. G.729ab, G.723, iLBC…) je možné hlasový záznam získat o něco složitější konverzí pomocí dalších programů jako jsou rtpplay [4] a JMStudio [5].



Obrázek 6 – Detail zachycený hovoru v Etherealu

Na obrázku č. 6 vidíme, že všechny zprávy vyměněné mezi komunikujícími uzly byly v otevřené podobě a jsou tedy snadno dekódovatelné. Tím pádem mohou útočníkovi poskytnout celou řadu cenných informací. Jediným bezpečnostním prvkem v ukázkové komunikaci je autentizace volajícího účastníka vůči SIP proxy serveru. Autentizace probíhá na základě znalosti jména a hesla. Heslo se neposílá v otevřeném tvaru, ale hashované pomocí funkce MD5.

5 Závěr

Přestože možnosti zabezpečení VoIP komunikace existují, v praxi se používají takřka výjimečně. Otázka zabezpečení není v současnosti zřejmě jak pro operátory, tak pro klienty natolik důležitá, aby se jí důsledně věnovali. S dalším rozšiřováním IP telefonie však důraz na zabezpečení bude jistě narůstat a snad se tedy již brzy dočkáme doby, kdy schopnost realizovat zabezpečený hovor bude stejně důležitá jako nízká cena a vysoký MOS. Trochu paradoxně je nyní z hlediska odposlechů nejlepší používat uzavřený a proprietární protokol Skype, u kterého je přenos vždy šifrovaný algoritmem AES s klíčem délky 256 bitů. Výměna klíčů je pak zabezpečena pomocí algoritmu RSA. I když ani zde si samozřejmě nemůže být uživatel jistý zda program neobsahuje nějaká zadní vrátka a „velký bratr“ neposlouchá…

Literatura

[1] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries.: Security Considerations for Voice Over IP Systéme, NIST Special Publication 800-58, [online, cit. 2006-10-15]. Dostupné z: <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf >

[2] Phil Zimmermann, ZRTP: Extensions to RTP for Diffie-Hellman Key Agreement for SRTP, [online, cit. 2006-10-17]. Dostupné z: <http://zfone-project.com/docs/draft-zimmermann-avt-zrtp-01.txt>

[3] M. Baugher , E. Carrara, D. McGrew et al., RFC 3711 – The Secure Real-time Transport Protocol (SRTP), [online cit. 2006-10-17]. Dostupné z: <http://www.ietf.org/rfc/rfc3711.txt>

[4] rpplay, <http://www.cs.columbia.edu/~hgs/rtp/rtpplay.html>

[5] JMStudio, <http://java.sun.com/products/java-media/jmf/2.1.1/jmstudio/jmstudio.html>

[6] Marek V., Ochrana VoIP proti odposlechu, Bakalářská práce, ČVUT-FEL, 2006.

[7] J. Rosenberg et al., RFC 3261 – SIP: Session Initiation Protocol, IETF, [online cit. 2006-10-16]. Dostupné z: < http://www.ietf.org/rfc/rfc3261.txt >

[8] J. Arkko et al.: RFC 3329 – Security Mechanism Agreement for the Session Initiation Protocol (SIP), IETF, [online cit. 2006-10-18]. Dostupné z: <http://www.ietf.org/rfc/rfc3329.txt>