PSC2009
24rd International Power System Conference
09-F-DTC-0110
بیست و چهارمین
کنفرانس بین‌المللی برق

راهکارهایی برای افزایش امنیت VoIP

ندا خیری – صوفیا آهنج – مهدیه علی بخشی
کارشناس کامپیوتر– کارشناس ارشد الکترونیک – کارشناس مخابرات
پژوهشگاه نیرو – گروه پژوهشی مخابرات
تهران, ایران

واژه‌های کلیدی: VoIP، فایروال، سیستم تشخیص نفوذ، لیست کنترل دسترسی

چکیده

امروزه تکنولوژی VoIP[1] که در آن انتقال صوت توسط شبکه‌های IP[2] انجام می‌گیرد، یکی از پرکاربردترین تکنولوژی‌ها در ارتباطات تلفنی محسوب می‌شود. هزینه کمتر و انعطاف‌پذیری بیشتر، از مزایای این تکنولوژی است. این تکنولوژی هم‌اکنون در برخی برق‌های منطقه‌ای بر روی شبکه اختصاصی مخابرات آن‌ها بکار گرفته شده و در حال بهره‌برداری می‌باشد. همچنین با راه‌اندازی مخابرات نوری و افزایش ظرفیت مخابراتی در این صنعت، این تکنولوژی در سایر مناطق نیز مورد استفاده قرار خواهد گرفت. این تکنولوژی همراه با مزایای جدیدی که ارائه می‌دهد، ریسک‌های امنیتی نیز در پی دارد و بکارگیری VoIP نباید بدون درنظر گرفتن ملاحظات امنیتی انجام شود. این مساله در صنعت برق به‌دلیل امکان استفاده از آن در DTS دارای اهمیت خاصی می‌باشد. اگرچه سایر ارتباطات VoIP در صنعت برق نیز به‌دلیل آنکه کارمندان، مدیران و مسوولان بخش‌های مختلف همگی به این سرویس دسترسی دارند، دارای اهمیت بالایی می‌باشد.

VoIP در مقابل حملاتی همانند ویروس‌ها، کدهای بدانديش، DoS[3]، مرد در میان و ... آسیب‌پذیر می‌باشد درنتیجه باید به دنبال راهکارهایی برای امن کردن آن بود. این مقاله به شرح مختصری در مورد VoIP و دو پروتکل مهم سیگنالینگ آن می‌پردازد و سپس به بررسی تهدیدات امنیتی و آسیب‌پذیری‌های مرتبط با این پروتکل‌ها پرداخته و در ادامه به‌منظور مقابله با حملات ناشی از این آسیب‌پذیری‌ها، راهکارهای امنیتی ارائه می‌دهد.

[1] Voice over Internet Protocol
[2] Internet Protocol
[3] Denial of Service

۱- مقدمه

VoIP نسخه جدیدی از شبکه‌های تلفن سنتی یا PSTN[1]ها می‌باشد که مکالمه‌های صوت را در بسته‌هایی تحت یک شبکه داده با استفاده از پروتکل اینترنت (IP) انتقال می‌دهد. یکی از دلایل اصلی توسعه VoIP کاهش هزینه‌های مکالمات تلفنی است. مکالمه‌های صوت سنتی بر روی PSTN با استفاده از سوییچینگ مداری ایجاد می‌شوند. در این روش یک مدار یا کانال اختصاصی بین دو طرف قبل از اینکه با همدیگر صحبت کنند برقرار می‌شود. مزیت این روش کیفیت مناسب صوت بدلیل استفاده از یک خط اختصاصی و مشخص است اما این روش بدلیل نیاز به ظرفیت بالای شبکه، گران می‌باشد. توسعه VoIP تغییرات زیادی در ارتباطات تلفنی بوجود آورده است. در این روش برای برقراری مکالمه، سیگنالهای صوت آنالوگ با استفاده از یک مبدل آنالوگ به دیجیتال، دیجیتالی می‌شوند. سیگنالهای صوتی دیجیتال شده در مقابل نویز ایمن‌تر هستند و راحت‌تر می‌توانند کنترل شوند و به شکل دیگری تبدیل شوند. سپس داده‌های دیجیتال به بسته‌هایی تقسیم شده و ارسال می‌شوند. مکانیزم‌های پشتیبانی بلادرنگ و تحویل به موقع باید بر روی بسته‌ها اعمال شود. همچنین پروتکل‌های سیگنالینگ برای ایجاد لینک‌های ارتباطی بین تلفن‌ها مورد نیاز است. در نهایت بسته‌ها دریافت می‌شوند و داده‌های دیجیتالی بازسازی می‌شوند. داده‌های دیجیتال ابتدا از حالت فشرده خارج شده سپس توسط یک مبدل دیجیتال به آنالوگ به سیگنال صوتی تبدیل می‌شوند [۱].

پیاده‌سازی VoIP را می‌توان به روش‌های مختلفی انجام داد که شامل موارد زیر می‌باشند:

- PC به PC. در این روش هر دو گوینده و دریافت‌کننده، از گوشی‌های متصل به PC استفاده می‌کنند.
- PC به PSTN. فقط گوینده از یک گوشی متصل به PC استفاده می‌کند. گیرنده، مکالمه را به روش سنتی دریافت می‌کند.
- PSTN به PSTN. گوینده از یک تطبیق‌دهنده IP روی تلفن سنتی استفاده می‌کند و مکالمه روی تلفن سنتی دریافت می‌شود. اما صوت بر روی یک شبکه IP منتقل می‌شود.
- تلفن IP به PSTN. گوینده از یک تلفن IP استفاده می‌کند و صوت از شبکه IP به شبکه تلفن سنتی از طریق یک گذرگاه[2] منتقل می‌شود.
- تلفن IP به تلفن IP. صوت بر روی یک شبکه IP پایانه به پایانه[3] منتقل می‌شود [۱].

بطور کلی از دلایل استفاده از VoIP می‌توان به موارد زیر اشاره کرد:

- VoIP امکان استفاده از زیرساخت‌های شبکه‌ای موجود برای انتقال هر دو ترافیک صوت و داده را فراهم می‌کند.
- VoIP با کاهش هزینه‌های تعمیر و نگهداری و استفاده از زیرساخت‌های یکسان در انتقال صوت و داده موجب صرفه‌جویی قابل توجهی می‌شود.
- بعضی از کاربردهای VoIP تمامی ویژگی‌های موجود در PBX[4] سنتی را تحت پوشش قرار می‌دهد [۱].

لازم به ذکر است ارتباط تصویر نیز با استفاده از همین تکنولوژی و پروتکل‌های مرتبط با آن انجام می‌شود.

۲- پروتکل‌های VoIP

VoIP از دو جزء اصلی تشکیل شده است. یکی سیگنال صوتی که بر روی شبکه منتقل می‌شود و دیگری سیگنالینگ (که شامل پیام‌های مورد نیاز برای کنترل‌کردن عناصر دیگر مکالمه بطور مثال رقم‌های شماره‌گیری مقصد، می‌باشد). هر دو این عناصر از استانداردها و پروتکل‌های مخصوصی استفاده می‌کنند. ساختار اصلی یک مکالمه VoIP، همانند دیگر برنامه‌های کاربردی مبتنی بر IP، دارای معماری لایه‌بندی OSI[5] می‌باشد.جدول ۱، لایه‌بندی و پروتکل‌های مورد استفاده در VoIP را نشان می‌دهد.

[1] Public Switched Telephone Network
[2] Gateway
[3] End-to-End
[4] Private Branch Exchange
[5] Open System Interconnection

جدول۱- پشته پروتکل VoIP و مقایسه آن با مدل OSI

پروتکل VoIP	لایه	هم ارزی با اینترنت	مدل OSI
SIP	۷	HTTP	کاربرد
H.323	۶		نمایش
RTP, RTCP	۵	SSL	ارتباط
UDP	۴	TCP	انتقال
IP	۳	IP	شبکه
Data	۲	Ethernet	داده
Physical	۱	100-Base T	فیزیکی

مطابق این جدول، لایه‌های پایین (لایه فیزیکی و داده) براساس تکنولوژی‌هایی همانند اترنت و WiFi[1] با برنامه‌های کاربردی مبتنی بر اینترنت مثل Web و FTP[2] مرتبط می‌باشند. لایه شبکه، نظیر دیگر برنامه‌های کاربردی توسط پروتکل اینترنت (IP) انتقال اصلی بسته‌های داده (که به عنوان دیتاگرم شناخته می‌شوند) را انجام می‌دهد.

در VoIP از دست رفتن داده یا خطای کم، تأثیر چندانی بر روی کیفیت یا کارایی صوت نمی‌گذارد و در عوض انتقال سریع داده از یک نقطه به نقطه انتهایی دارای اهمیت می‌باشد. پروتکل لایه انتقال UDP[3] ترتیب بسته‌های ورودی را کنترل نمی‌کند و کنترل ترتیب صحیح بسته‌ها بر عهده برنامه کاربردی است بنابراین این پروتکل دارای سرعت بالایی می‌باشد. در حالیکه در ارتباطات TCP، بازگشت ACK تاخیراتی تولید می‌کند. این تاخیر در شرایطی که بسته‌ها گم شوند، بسیار بیشتر می‌شود زیراکه TCP بسته‌های گم شده را دوباره ارسال می‌کند که این عمل سبب ایجاد تاخیر بیشتر می‌شود. لذا پروتکل UDP در مواقعی که تحویل سریع مدنظر است، گزینه مناسبی می‌باشد. البته درصورتی‌که قابلیت اعتماد معیار مهمی باشد، استفاده از TCP[4] به عنوان یک پروتکل انتقال، انتخاب بهتری می‌باشد. در انتقال صوت تحمل چند بسته گم شده بسیار بهتر از تاخیر است. بنابراین برای انتقال صوت در لایه انتقال از UDP به جای پروتکل TCP استفاده می‌شود و پروتکل کنترل انتقال معمول TCP برای ارتباط سیگنالینگ استفاده می‌شود. همچنین سیستم‌های VoIP در لایه ارتباط از پروتکل انتقال بلادرنگ RTP[5] و پروتکل کنترل انتقال بلادرنگ RTCP[6] استفاده می‌نمایند. لایه‌های بالاتر (ارتباط، نمایش و کاربرد) نیز سیگنالینگ مورد نیاز برای یک سیستم ارتباط تلفنی را برقرار می‌سازند. در واقع این پروتکل‌ها کنترل ارتباط بین دو نقطه انتهایی مکالمه به عنوان مثال راه‌اندازی مکالمه و سیگنالینگ مورد نیاز برای انتقال ترافیک بر روی یک شبکه IP را کنترل می‌کنند.

پروتکل‌های H.323 و پروتکل راه اندازی ارتباط (SIP)[7]، دو استاندارد اصلی سیگنالینگ در VoIP هستند. براین اساس دو معماری مختلف برای شبکه‌های VoIP تعریف می‌شود لذا در ادامه به شرح این پروتکل‌ها پرداخته می‌شود [۱].

۲-۱- پروتکل H.323

پروتکل H.323 تدوین شده توسط موسسه ITU-T[8]، ارتباط بین تجهیزات متفاوت تلفنی و چندرسانه‌ای را در شبکه‌های IP برقرار کرده و ارتباط صوت، ویدیو و داده را بصورت بلادرنگ فراهم می‌کند.

چهار نهاد مختلف به‌عنوان واحدهای عملیاتی یک شبکه کامل H.323 تعریف شده‌اند که عبارتند از: نقاط انتهایی (پایانه‌ها)، گذرگاه[9]، محافظ گذرگاه[10] و واحد کنترل چندنقطه‌ای (MCU[11]). نقاط انتهایی (تلفن‌ها، تلفن‌های نرم‌افزاری، پست صوتی، دوربین‌های ویدئویی و ...) امکاناتی هستند که کاربران نهایی با آن‌ها در تعامل می‌باشند. گذرگاه‌ها،

[1] Wireless Fidelity
[2] File transfer protocol
[3] User Datagram Protocol
[4] Transmission Control Protocol
[5] Real Time Protocol
[6] Real Time Control Protocol
[7] Session Initiation Protocol
[8] International Telecommunication Union-Telecom
[9] Gateway
[10] Gate Keeper
[11] Multipoint Control Units

سیگنالینگ و انتقال رسانه (صوت و تصویر) را انجام می‌دهند و به صورت واسط به دیگر شبکه‌ها همانندISDN و PSTN ارتباط برقرار می‌نمایند. البته برای ارتباط بین دو ترمینال روی یک شبکه H.323 نیازی به استفاده از گذرگاه نیست. محافظ گذرگاه نیز یک جزء اختیاری در شبکه مبتنی بر پروتکل H.323 می‌باشد که گذرگاه‌های VoIP در آن ثبت‌نام می‌کنند و مهم‌ترین عمل آن، ترجمه آدرس بین آدرس‌های سمبلیک مستعار و آدرس‌های IP می‌باشد. محافظ گذرگاه می‌تواند مغز شبکه H.323 درنظر گرفته شود و در واقع یک نقطه‌ی مرکزی برای تمام تماس‌های داخل شبکه H.323 است. محافظ گذرگاه خدمات مهمی مثل ترجمه آدرس، کنترل پذیرش، مدیریت پهنای باند سیگنالینگ و شمارش تماس‌ها را فراهم می‌کند. مجموعه ترمینال‌ها، گذرگاه‌ها و MCUهایی که یک محافظ گذرگاه کنترل می‌کند به عنوان یک ناحیه شناخته می‌شوند. MCUها نیز کنفرانس‌های چند طرفه را بین سه یا تعداد بیشتری از نقاط انتهایی فراهم می‌کنند. در واقع پروتکل H.323 مجموعه‌ای از رویه‌های ایجاد مکالمه و مذاکره را تعریف می‌کند. مهم‌ترین آن‌ها در برنامه‌های کاربردی VoIP، H.225، H.235، H.245 و اعضای سری‌های سیگنالینگ Q.900 می‌باشند. H.323 گروهی از کد گذارهای صوت برای ارتباطات VoIP، مانند سری‌های G.700 را نیز مشخص می‌کند [۲].

H.225 سیگنالینگ ایجاد مکالمه و خاتمه آن را تعیین می‌کند و شامل آدرس‌های IP مبدا و مقصد درگاه‌ها، کد کشور و اطلاعات درگاه H.245 می‌باشد. همچنین پروفایل ۱ این پروتکل (H.245.1)، پیام‌های RAS[1] شامل سیگنالینگ، پذیرش ثبت نام و وضعیت و اطلاعات رشته رسانه را مشخص می‌کند. H.245 تبادل پیام‌هایی شامل امکانات پایانه، ارتباط رئیس/ مرئوس[2] و اطلاعات کانال منطقی برای رشته‌های رسانه (صوت و تصویر) را مشخص می‌کند.

[1] Registration Admission and Status
[2] Master/Slave

از آن‌جاکه در معماری H.323 منشا درخواست کننده، توسط عملیات رمزنگاری تصدیق نمی‌شود لذا تهدیدات امنیتی برای آن بوجود می‌آید که در استاندارد H.235 به آن پرداخته شده است. پروتکل H.235 نیز مجموعه‌ای از پیام‌ها، رویه‌ها، ساختارها و الگوریتم‌ها برای امن کردن سیگنالینگ، کنترل و ارتباطات رسانه تحت معماری H.323 را پیشنهاد می‌کند. بحث مهم H.235 تهدیدات امنیتی در ارتباطات، شنود شبکه یا روش‌های دیگر منحرف کردن رسانه می‌باشد. حمله‌های مطرح در این پروتکل، صحت پیام‌های یک مکالمه را به خطر می‌اندازند. این تهدید نشان می‌دهد که به سرویس‌های امنیتی نیاز می‌باشد که افراد را قادر به تصدیق کردن هویت منبع درخواست‌ها سازد و بررسی عدم تغییر محتویات پیام‌ها و رشته‌های کنترلی در حین انتقال را انجام دهد. اصولاً تصدیق هویت بر اساس یک راز اشتراک گذاشته شده یا روش‌های مبتنی بر کلید عمومی با گواهی‌نامه‌ها می‌باشد. همچنین برای امن کردن پیام‌ها، پروتکل‌های TLS[3] (TLS، جانشین لایه سوکت امن(SSL)[4] و بر اساس SSL 3.0 می‌باشد) و IPSec[5] (امنیت IP) پیشنهاد می‌شوند. IPSec اغلب اطلاعات سربار مهم را نیز علاوه بر بار مفید رمز می‌کند درحالیکه TLS فقط بار مفید بسته را رمز می‌کند بنابراین رمزنگاری TLS، آدرس IP را بدون رمز نگه می‌دارد. H.235 دارای تعدادی پروفایل‌های امنیتی است که هر پروفایل به صورت یک ماژول شامل مجموعه‌ای از اصطلاحات، تعاریف، خواسته‌ها و رویه‌ها می‌باشد. پروفایل‌ها می‌توانند توسط سرویس‌های امنیتی که هر پروفایل خاص پشتیبانی می‌کند، متمایز شوند. سرویس‌های امنیتی پشتیبانی شده در این پروفایل‌ها عبارتند از: تصدیق هویت، عدم انکار، صحت، محرمانگی، کنترل دسترسی و مدیریت کلید. در هر پروفایل امنیتی سرویس‌های امنیتی برای مقابله با یک سری از حملات تعریف می‌شوند. برای مثال در پروفایل اصلی H.235.1 حمله‌های زیر خنثی می‌شوند:

[3] Transport Layer Security
[4] Secure Socket Layer
[5] Internet Protocol Security

- حمله‌ی مرد در میان[1]. سرویس تصدیق صحت پیام سطح کاربرد، از چنین حمله‌ای جلوگیری می‌کند.
- حمله‌ی تکرار[2]. استفاده از مُهر زمانی و دنباله عددی باعث جلوگیری از چنین حمله‌ای می‌شود.
- فریبکاری[3]. تصدیق هویت کاربر مانع از این حمله می‌شود.
- دزدیدن ارتباط. برای جلوگیری از این حمله از تصدیق صحت برای پیام‌های سیگنالینگ می‌توان استفاده کرد [۲].

در این استاندارد بحث‌های امنیتی مرتبط با حمله‌های DoS (ممانعت از سرویس) در نظر گرفته نمی‌شوند.

۲-۲- پروتکل SIP

پروتکل راه اندازی شبکه (SIP) تدوین شده توسط موسسه IETF[4]، یک پروتکل سیگنالینگ لایه کاربرد برمبنای کد اسکی است که به‌منظور راه اندازی ارتباط‌های محاوره‌ای روی یک شبکه IP بکار می‌رود و هدف آن برقراری، نگهداری و خاتمه دادن جلسات بین دو یا بیشتر نقطه انتهایی می‌باشد. SIP با چند پروتکل دیگر IETF مثل پروتکل توصیف جلسه (SDP)[5]، پروتکل جریان بلادرنگ (RTSP)[6] و پروتکل اعلام جلسه (SAP)[7] استفاده می‌شود. این پروتکل به تعیین مکان، امکانات و میزان دردسترس بودن یک کاربر و تنظیم و مدیریت یک ارتباط می‌پردازد. دو جزء اصلی که توسط پروتکل SIP بکار می‌رود، عامل‌های کاربر و سرورهای آن می‌باشد. البته عامل کاربر می‌تواند در نقش مشتری که درخواست‌ها را تولید می‌کند یا سرور که به درخواست‌ها پاسخ می‌دهد عمل کند. سرور SIP می‌تواند در نقش‌های متفاوت پراکسی، ثبت کننده[8] و redirect عمل کند.

[1] Man-in-the-Middle
[2] Replay
[3] Spoofing
[4] Internet Engineering Task Force
[5] Session Discovery Protocol
[6] Real Time Streaming Protocol
[7] Session Announcement Protocol
[8] Registrar

همانند پروتکل H.323، پروتکل SIP نیز از پروتکل UDP استفاده می‌کند. همچنین در این معماری به منظور برقراری امنیت بین برنامه‌های کاربردی که روی یک شبکه IP ارتباط برقرار می‌کنند، می‌توان از پروتکل امنیت لایه انتقال (TLS) جهت امن کردن پیام‌های سیگنالینگ و تصدیق صحت استفاده کرد. پروتکل‌های توصیف ارتباط، انتقال بلادرنگ، کنترل گذرگاه رسانه و بلادرنگ رشته‌ای نیز پروتکل‌هایی هستند که SIP برای فرستادن داده، کنترل کردن رسانه و دسترسی به وسایل مختلف از آن‌ها استفاده می‌کند. همچنین از SRTP[9] جهت اطمینان به قابلیت اعتماد و محرمانگی RTP استفاده می‌شود [۲].

افراد بسیاری SIP را بسیار قویتر از H.323 و راه حل بسیار انعطاف پذیرتر، ساده‌تر، آسانتر برای انجام، مناسبتر برای پشتیبانی وسایل کاربر و مناسب‌تر جهت تکمیل ویژگی‌های پیشرفته می‌دادند. این فاکتورها برای فروشنده تجهیزات یا اپراتور شبکه از اهمیت زیادی برخوردار است. سادگی به این معناست که محصولات و سرویس‌ها می‌توانند سریعتر پیشرفت کنند و بسیار سریعتر در دسترس قرار گیرند.

۳- بررسی تهدیدات و آسیب‌پذیری‌های VoIP

از آن جا که VoIP مبتنی بر شبکه‌های IP نرمال است، برنامه‌های کاربردی VoIP دارای نقاط ضعف مربوط به پروتکل IP خواهند بود. حوزه مسائل امنیتی در کاربردهای VoIP درمقایسه با شبکه تلفن سوئیچی عمومی (PSTN) که از خطوط اختصاصی جهت برقراری ارتباط استفاده می‌نماید، به میزان قابل ملاحظه‌ای بزرگتر است. علاوه بر این، پروتکل‌های اختصاصی که بسیاری از شرکت‌های مبتنی بر VoIP از آن‌ها استفاده می‌کنند، موجب آسیب‌پذیرتر شدن مشتریان در مقابل انواع حملات می‌شوند [۳].

[9] Secure RTP

۳-۱- آسیب‌پذیری‌های پروتکل VoIP

آسیب‌پذیری‌های VoIP ناشی از آسیب‌پذیری پروتکل‌های آن (SIP, H.323, RTP) و نیز مسائل همگرایی صوت و داده به شرح زیر می‌باشد:

- سرورهای SIP که سرویس‌های VoIP را ارائه داده و اطلاعات مکالمه را ثبت می‌نمایند نسبت به حملات نرم‌افزاری بداندیش و فعالیت‌های هک بسیار حساس هستند. از آنجاکه ترافیک SIP در فرم پایه‌ای خود یک متن ساده و بدون رمز است بنابراین ترافیک صوتی نسبت به Packet Snifferها آسیب‌پذیر بوده و این اجازه را به یک مهاجم می‌دهد که بسته‌ها را به منظور دستکاری مکالمه، جعل کند. ترافیک SIP به منظور حفاظت از Caller IDها، اطلاعات صورتحساب و غیره بایستی رمز شود. همچنین این پروتکل نسبت به انواع حملات DoS بطور مثال حمله BYE نیز آسیب‌پذیر می‌باشد، در این حمله هکر با فرستاندن پیغام‌های غیرمجاز، یک طرف ارتباط را قانع به قطع ارتباط می‌نماید درحالیکه طرف مقابل از این امر بی‌اطلاع بوده و به ادامه ارتباط می‌پردازد [۳].

مسئله دیگر در رابطه با SIP مربوط به NAT می‌باشد، از آنجاکه SIP اطلاعات آدرس را در فریم داده خود کپسوله می‌کند و معمولا NAT در لایه شبکه اتفاق می‌افتد لذا اطلاعات آدرس بطور اتوماتیک اصلاح نمی‌شوند و بنابراین رشته رسانه، اطلاعات آدرس صحیح مورد نیاز برای ادامه اتصال را نخواهد داشت. به این جهت فایروال‌ها که معمولا همراه با تابع NAT می‌باشند رشته رسانه را قسمتی از مبادلات SIP در نظر نخواهند گرفت و آن را حذف می‌کنند.

- همانطور که ذکر شد، قابلیت اعتماد، تمامیت و... در H.323 با پرفایل‌های مختلف H.235 قابل دستیابی می‌باشند و بطور کلی می‌توان گفت که H.323 یک پروتکل نسبتا امن است و نیاز به ملاحظات امنیتی زیادی ندارد. مسئله مهم در خصوص ترافیک پروتکل H.323 این است که این پروتکل همانند SIP با مشکلات یکسانی هنگام مواجهه با تابع NAT برخوردار است. بنابراین لازم است آدرس صحیح و شماره درگاه به منظور برقراری یک اتصال مکالمه‌ای، به نقاط انتهایی ارسال شود [۳]. مساله جدی دیگر برای شبکه‌های H.323 این است که این پروتکل تقریباً همواره از طریق درگاه‌های پویا مسیردهی می‌شود که برای فایروال‌هایی که مختص VoIP نیستند، کاملا چالش‌برانگیز است.

- ترافیک بار مفید VoIP بصورت بسته‌های RTP منتقل می‌شود. بعد از مبادله سیگنالینگ، RTP مسئول انتقال بسته‌های صوتی می‌شود. از طرفی RTP پایش بار مفید خود را از طریق دنباله عددی و مُهر زمانی انجام می‌دهد. این ویژگی برای کاربردهای مربوطه به انتقال بلادرنگ داده مثل انتقال صوت مناسب است ولی متاسفانه RTP کیفیت سرویس را برای سرویس‌های بلادرنگ تضمین نمی‌نماید. درواقع RTP به سرویس‌های لایه پایین‌تر متکی است. مهاجمین می‌توانند بسته‌های RTP را با محتوای غیرمفید ارسال نمایند. این کار به این معنی است که هر دو بار مفید و سربار با اعداد تصادفی جایگزین شده و به سمت هدف ارسال می‌شوند. این حمله می‌تواند کیفیت صوت را کاهش داده و یا تجهیزات را از کار بیندازد. یک روش برای کشف این حمله، بررسی شماره‌های متوالی در بسته‌های RTP پی‌درپی می‌باشد. اگر این توالی نامنظم باشد، می‌توان آن را به عنوان وجود یک حمله تلقی نمود. همچنین در خصوص امنیت RTP، پروتکل SRTP وجود دارد که در واقع یک پروفایل پروتکل RTP است که امنیت را برقرار می‌نماید [۳].

- هر چند که همگرایی شبکه‌های صوتی و داده یکی از مزایای اصلی سیستم‌های VoIP می‌باشد، این مزیت تبدیل به یک مشکل امنیتی مهم در سیستم‌های VoIP شده است. VoIP در مقابل حملات مشهوری همانند حملات DoS و حملات تصدیق که شبکه داده را تهدید می‌کنند آسیب‌پذیر می‌باشد. حالت مطلوب این است که در صورت وقوع اتفاقی در شبکه داده، شبکه صوتی همچنان به کار خود ادامه دهد. اگر شبکه‌های صوتی و داده یک شبکه ترکیبی باشند، در این صورت هر تهدیدی، موجب ایجاد نقص همزمان در هر دوی آنها خواهد شد [۳].

۳-۲- حملات مطرح در VoIP

با توجه به آسیب‌پذیری‌های بیان شده، حملاتی متوجه VoIP می‌باشد که در این بخش به معرفی و بررسی برخی از انواع آن می‌پردازیم.

۳-۲-۱- حمله مرد در میان

حمله مرد در میان به حمله‌ای اطلاق می‌شود که در آن یک متجاوز بدون اطلاع هیچ یک از طرفین، قادر به خواندن و تغییر پیام‌های بین دو طرف باشد. استراق سمع، جعل بسته و تکرار، انواع این حمله می‌باشند و تهدیدات امنیتی در برابر قابلیت اعتماد و یکپارچگی محسوب می‌شوند، زیرا این نوع حملات می‌توانند بسته‌های داده‌ی صوتی را در دسترس افراد غیرمجاز قرار داده و یا محتوای مکالمات را تغییر دهند [۳].

۳-۲-۲- حملات DoS و DDoS[1]

حملات DoS و DDoS به حملاتی اطلاق می‌شود که به موجب آن‌ها از دسترسی مجاز به یک سرویس شبکه، ممانعت به عمل آید. سرریز بافر، حمله SYN و حمله Smurf انواع این حمله می‌باشند که موجب ایجاد تهدیدات امنیتی برای دسترس‌پذیری شبکه می‌شوند. حملات DoS و DDoS همچنین می‌توانند سیستم‌های VoIP را مورد هدف قرار دهند. این حملات شامل ارسال درخواست قطع از یک میزبان (حالت DoS) و یا از تعدادی میزبان (حالت DDoS) به یک سرور یا تلفن است [۳].

۳-۲-۳- پیام‌های بی معنی[2] در VoIP

یک مساله پنهانی، پیام‌های توخالی و بی معنی ناخواسته در VoIP می‌باشد. مشابه سیستم‌های پست الکترونیک، VoIP نیز نسبت به پیام‌های توخالی و بی معنی ناخواسته مستعد است. اگر یک کاربر VoIP هر روز مکالمات زیادی را از یک تولیدکننده پیام‌های صوتی بی‌معنی دریافت نماید، برای استفاده از تکنولوژی VoIP بی‌میل خواهد شد [۳].

[1] Distributed Denial of Services
[2] Spam

۳-۲-۴- حمله کد بداندیش

یک ویروس، بخشی از یک کد بداندیش می‌باشد که بدون اطلاع کاربر به سیستم‌های کامپیوتری اعمال شده و برخلاف میل کاربر اجرا می‌شود. از آنجاکه تمامی برنامه‌های کاربردی VoIP، دارای آدرس IP می‌باشند و اداره مکالمات صوتی را بر عهده دارند لذا خطر ویروس در آن‌ها افزایش می‌یابد. بنابراین یک حمله ویرویسی می‌تواند در برنامه‌های کاربردی VoIP بسیار موثر باشد. حملات ویروسی می‌توانند تهدیدات امنیتی برای یکپارچگی و دسترس‌پذیری شبکه VoIP محسوب شوند [۳].

۳-۲-۵- حمله دسته‌های ولگرد[3]

حمله دسته‌های ولگرد به حملاتی اطلاق می‌شود که در آنها مهاجمین با هدف دسترسی به تجهیزات و منابع فرد دیگر دست به اقدامات فریبکارانه می‌زنند. متجاوزین از طریق اضافه کردن یک دسته جدید از برنامه‌های کاربردی VoIP، هویت دیجیتالی را جعل نموده و سپس هویت یک مشترک مکالمه را مورد استراق سمع قرار می‌دهند. حملات دسته‌های ولگرد یک تهدید امنیتی برای قابلیت اعتماد VoIP محسوب می‌شوند، زیرا در این حالت مهاجمان بصورت غیرمجاز به یک شبکه IP دسترسی پیدا می‌کنند [۳].

۳-۲-۶- حمله DHCP[4]

پروتکل DHCP یا پیکربندی پویای میزبان، پروتکلی است که به منظور پیکربندی شبکه مشتری‌ها و ایستگاه‌های کاری طراحی شده است. در سرور DHCP آدرس‌های IP و اطلاعات دیگر پیکربندی بصورت خودکار به هر وسیله اختصاص داده می‌شود. یک کامپیوتر بداندیش در شبکه می‌تواند درخواست‌های فراوانی را به یک سرور DHCP ارسال کرده و سرور را تحت فشار قرار دهد که تمامی آدرس‌های IP را تخصیص دهد. به این حملات، حملات

[3] Rogue Sets
[4] Dynamic Host Configuration Protocol

DHCP اطلاق می‌شود. حملات DHCP موجب ایجاد یک تهدید امنیتی برای دسترس‌پذیری شبکه می‌شوند، زیرا چنین حملاتی می‌توانند موجب قطع یا توقف عملکرد عادی برنامه‌های کاربردی VoIP شوند. درحقیقت این حمله از نوع DoS می‌باشد [۳].

۳-۲-۷- حمله Flash Crowd

Flash Crowd به معنی ارسال تعداد بسیار زیادی درخواست ناگهانی به یک سرور و از نوع حمله DoS می‌باشد. این حمله قادر به تحت فشار قرار دادن سیستم‌های VoIP می‌باشد [۳].

۳-۲-۸- حمله Pharming

در حمله Pharming یک فرد به منظور دستیابی به اطلاعات از طریق یک صفحه وب و معمولاً بوسیله پست الکترونیک یا تبادل لحظه‌ای پیام با یک درخواست ظاهراً قانونی به مشتری متصل می‌شود. Pharming از آسیب‌پذیری DNS[1] به منظور گمراه نمودن ارتباطات مشتری یک سرور دور دست استفاده می‌کند. به عنوان مثال این حمله می‌تواند سرقت اطلاعات حیاتی از مشتریان شرکت بوسیله یک فرد مهاجم باشد با ایجاد این باور در مشتریان که آنها با یکی از نمایندگان یا وکلای شرکت تماس گرفته‌اند. نوع دیگر حمله Pharming بر روی VoIP، گمراه نمودن شمار زیادی از مکالمات به یک ناحیه خاص به منظور ارتکاب به یک DDoS است [۳].

۳-۲-۹- حمله Botnet

به منظور راه‌اندازی یک حمله DDoS، مهاجم ابتدا چندین سیستم آسیب‌پذیر را جستجو می‌کند. این فرآیند جستجو معمولاً بصورت اتوماتیک از طریق مرور سیستم‌های دوردست و جستجوی آسیب‌پذیری‌های بالقوه انجام می‌شود. هنگام یافتن یک آسیب‌پذیری، می‌توان از آن به منظور توقف سیستم استفاده کرد. بدین منظور مهاجم برنامه‌های کنترل از راه دور با نام "bot" را به این سیستم‌ها ارسال می‌نماید. پس از استقرار این برنامه‌ها در سیستم‌های آلوده به bot، این سیستم‌ها منتظر آمدن دستوراتی از هدایت‌گر bot به منظور خرابکاری می‌مانند. از این‌رو، یک هدایت‌گر bot می‌تواند تعداد زیادی از سیستم‌های به خطر افتاده در مقابل یک هدف را هدایت نماید. شبکه متشکل از این کامپیوترهای آلوده به bot، "botnet" نامیده می‌شود. برنامه‌های کاربردی VoIP مثل Vonage و Skype می‌توانند فرصت‌های بهتری را برای مهاجمان در کنترل کامپیوترهای آلوده به bot ایجاد نمایند [۳].

۳-۲-۱۰- حمله Toll Fraud

در این حمله یک کاربر انتهایی VoIP، از سرور VoIP به منظور برقراری تماس غیرمجاز از طریق PSTN سنتی استفاده می‌نماید. برای مثال کنترل دسترسی ناکارامد می‌تواند به تجهیزات ولگرد اجازه برقراری تماس غیرمجاز (از طریق فرستادن درخواست‌های VoIP به برنامه‌های کاربردی پردازشگر تماس) را بدهد. [۳].

۴- ارائه راهکارهای امنیتی برای VoIP

با وجود اینکه صرفه‌جویی در هزینه و مدیریت آسان در ترکیب ترافیک صوت و داده بر روی ساختارهای فیزیکی یکسان از مزایای اصلی همگرا شدن می‌باشد, با این وجود در طول فاز طراحی معماری VoIP، جداسازی منطقی ترافیک صوت و داده دارای اهمیت بسزایی می‌باشد. علت این مساله آن است که رویدادهای شبکه و پدیده‌های امنیتی همانند کرم‌واره‌ها و حملات DoS در صورت اثرگذاری بر روی یک شبکه، برروی دیگری اثر نگذارند. در عمل گزینه‌های متعددی برای انجام این جداسازی منطقی وجود دارد. استفاده از VLAN[2]ها، فایروال‌های مخصوص VoIP، گذرگاه‌های لایه

[1] Domain name server

[2] Virtual LAN

کاربرد، مسیریاب‌ها و سوییچ‌ها از جمله این راه‌حل‌ها می‌باشند. همچنین لیست‌های کنترل دسترسی (ACL)[1] نیز می‌توانند جهت کنترل دسترسی به تجهیزات به‌کار روند. ACLها عموما به منظور حق ورود یا خروج به یک واسط بکار می‌روند و ابزار قدرتمندی برای تفکیک VoIP از ترافیک‌های دیگر می‌باشند. از میان این روش‌ها فایروال‌ها و لیست‌های کنترل دسترسی برای امنیت شبکه از اهمیت بسزایی برخوردارند [۲].

برای برقراری امنیت شبکه VoIP، نظارت بر ترافیک و تجهیزات، از جمله موضوعات کلیدی می‌باشند (برای مثال برای جلوگیری از حمله BYE). بدین منظور می‌توان از سیستم‌های تشخیص نفوذ مبتنی بر شبکه (NIDS)[2] و میزبان(HIDS)[3] و تست‌های نفوذ و آسیب پذیری استفاده کرد [۲].

همچنین به منظور امن‌سازی سیستم‌های مبتنی بر SIP از آن جایی که ساختار پیام SIP بر اساس HTTP می‌باشد، می‌توان تمامی اقدامات امنیتی موجود برای HTTP را به جلسات SIP نیز اعمال نمود یا به عبارت دیگر از HTTPS استفاده کرد. همچنین می‌توان از IPsec برای رمزنگاری در لایه شبکه و ساختار کلید عمومی (PKI[4]) جهت تصدیق صحت استفاده نمود. علاوه بر آن می‌توان TLS را جهت تصدیق با امضاء دیجیتال و رمزنگاری پیام‌های سیگنالینگ بکار برد. یکی از معمول‌ترین راه‌ها برای امن سازی ارتباط، استفاده از VPN و دیگر روش‌های تونلینگ می‌باشد. همچنین برای امن‌سازی مدیریت از راه دور و بررسی کنترل دسترسی از IPSec و SSH[5] استفاده می‌شود(SSH به عنوان یک مکانیزم امن و رمز شده برای ورود به اجزای مختلف شبکه شناخته می‌شود) [۲].

استفاده از VPN به منظور امن ساختن همه ارتباطات HTTP با فایروال‌های VoIP برای اهداف مدیریتی یا در غیراینصورت استفاده از HTTPS از ملاحظات امنیتی پیشنهادی دیگر می‌باشد.

آموزش مدیران و اپراتورها در زمینه ابزارها و تکنیک‌های جدید و اطمینان یافتن از اینکه همه سیستم‌های شبکه مقاوم و به‌روز هستند، همچنین انتخاب کلمه‌های عبور مناسب و اطمینان یافتن از اینکه آنتی‌ویروس‌های سیستم به‌روز می‌باشند، از دیگر اقدامات امنیتی است.

درصورت استفاده از VLAN، اطمینان یافتن از اینکه همه تلفن‌های IP و تلفن‌های نرم‌افزاری در VLAN صوت قرار دارند و غیرفعال کردن درگاه‌های VLAN که غیر قابل استفاده هستند از دیگر ملاحظات امنیتی می‌باشد.

غیر فعال کردن درگاه شبکه داده در داخل تلفن VoIP هنگامی که از آن استفاده نمی‌شود و مجوز داشتن برای استفاده از تلفن‌های نرم‌افزاری IP. و ممنوع شدن نصب و استفاده خصوصی از تلفن‌های نرم‌افزاری دیگر نیز از موارد امنیتی می‌باشند که باید به آنها توجه نمود.

امن ساختن سرورهای حیاتی VoIP توسط دستورالعمل‌های کاربردی و امن‌سازی همه ارتباطات مدیریتی از راه دور به سرورهای حیاتی VoIP از دیگر موارد امنیتی می‌باشد که باید به آن توجه کافی نمود.

داشتن گواهی‌نامه در همه تلفن‌های IP، تلفن‌های نرم‌افزاری و سخت‌افزارها و نرم‌افزارهای سرور VoIP نیز با استفاده از ساختار کلید عمومی جهت تصدیق می‌تواند به امنیت شبکه VoIP کمک بسزایی نماید.

همچنین جهت مقابله با حمله DoS علاوه بر طراحی مناسب شبکه و در نظر گرفتن پهنای باند کافی، می‌توان از غیرفعال نمودن درگاه‌های غیر ضروری، فایروال‌ها و SCTP[6] استفاده نمود. پروتکل SCTP که یکی دیگر از پروتکل‌های لایه انتقال می‌باشد، از مقاومت بالایی در مقابل حملات DoS برخوردار است. همچنین SCTP می‌تواند از طریق "TLS over SCTP" یا "SCTP over IPSec" از سرویس‌های امنیتی بیشتری بهره‌مند شود.

[1] Access Control Lists
[2] Network Intrusion Detection Systems
[3] Host-based intrusion detection systems
[4] Public Key Infrustructure
[5] Secure Shell
[6] Stream Control Transmission Protocol

در ادامه به ذکر نکاتی در خصوص فایروال‌ها، سیستم‌های تشخیص نفوذ و تست‌های نفوذ و آسیب‌پذیری به منظور استفاده بهینه از آن‌ها می‌پردازیم.

۴-۱- فایروال‌ها

همانطور که بیان شد، از فایروال برای تفکیک کردن VoIP از داده برروی شبکه‌های داخلی استفاده می‌شود. به دو دلیل استفاده از فایروال‌های عمومی درخصوص VoIP مناسب نمی‌باشد. اولین عامل این است که حد بین داخل شبکه VoIP از خارج آن یا حد بین شبکه‌های مورد اعتماد و غیرقابل اعتماد به طور واضح معلوم نیست. دومین عامل مربوط به این مطلب است که اکثر فایروال‌های عمومی برای پردازش مناسب بسته‌ها و ارتباطات VoIP به خوبی عمل نمی‌کنند، مخصوصا اگر این ارتباطات و بسته‌ها رمز شده باشند. ارتباطات H.323 و SIP برای فایروال‌های عمومی مشکل‌ساز می‌باشند. در H.323، بسته‌ها به صورت ASN.1 PER کد می‌شوند. همچنین در این پروتکل و پروتکل SIP، تابع NAT[1] اغلب آدرس IP واقعی نقاط انتهایی را مخفی می‌کند. همچنین صوت و سیگنالینگ روی کانالهای متفاوتی اتفاق می‌افتند که بعضی از آنها به صورت پویا ایجاد می‌شوند در نتیجه باید از فایروال‌های مخصوص H.323 و SIP که این مشکلات را برطرف می‌نمایند استفاده کرد و همه تلفن‌های PC را در پشت یک فایروال یا ACL قرار داد تا ترافیک VoIP را بررسی کنند.

۴-۲- سیستم‌های تشخیص نفوذ مبتنی بر شبکه (NIDS) و میزبان (HIDS)

همانطور که ذکر شد، سیستم‌های تشخیص نفوذ مبتنی بر شبکه و میزبان به منظور نظارت بر ترافیک بکار می‌روند.

NIDS برای هشدار دادن به مدیران هنگامی که ترافیک، بدذات یا غیرمجاز تشخیص داده می‌شود طراحی شده‌اند و معمولاً برطبق روش‌هایی که برای تشخیص حمله بکار می‌برند به دو دسته مبتنی بر امضا یا تشخیص بد رفتاری دسته‌بندی می‌شوند. NIDSهای مبتنی بر امضا اساسا شنودگرهای شبکه همراه با یک پایگاه داده از امضاهای حمله می‌باشند. روش دوم استفاده از سنسورهای NIDS می‌باشد که شامل پیش‌پردازشگرهایی هستند که دائما شبکه را برای رفتارهای غیرعادی بازرسی می‌کنند. این رفتارهای غیر عادی برای تشخیص پویشگرهای درگاه، ردیاب‌های شبکه توزیع شده، گونه‌های جدیدی از سرریزهای بافر و حمله‌های DoS مؤثر هستند. NIDSها باید در مکانی قرار گیرند که بتوانند حداکثر بررسی ترافیک بحرانی را انجام دهند. در محیط‌های VoIP، NIDSها یک لایه اضافی از دفاع را مهیا می‌کنند [۲].

HIDSها برنامه‌های کاربردی هستند که بر روی اطلاعات جمع شده از سیستم‌های کامپیوتری شخصی عمل می‌کنند. اکثر نرم افزارهای HIDS، یک پایگاه داده از فایل‌ها و ویژگی‌های سیستم را در یک حالت شناخته شده ایجاد و از این پایگاه برای بررسی هر تغییر سیستمی استفاده می‌کنند. نظارت HIDS روی رسانه VoIP، سرورهای پراکسی و ثبت نام مهم می‌باشد و باید در نصب اولیه در نظر گرفته شود [۲]. همچنین ارتباطات بین اجزای IDS (سنسورها و کنسول مدیریت) باید رمز شده باشد.

۴-۳- تست نفوذ و آسیب‌پذیری

تست نفوذ و آسیب‌پذیری، ابزار مفیدی برای تعیین وضعیت امنیتی یک سازمان می‌باشد. تست‌های نفوذ معمولاً در مقابل امکانات دفاعی محیط و برای اطمینان از صحت عملکرد آن‌ها می‌باشند در حالی که تست‌های آسیب‌پذیری در مقابل سیستم‌های خاص (میزبان، برنامه کاربردی یا شبکه‌ها) انجام می‌شوند. نتایج تست آسیب‌پذیری و نفوذ فقط وضعیت امنیتی در طول دوره انجام تست را منعکس می‌کند. تغییرات هرچند کم در زمینه‌های معماری و مدیریتی، لحظاتی پس از تست نفوذ، می‌تواند پروفایل امنیتی سیستم را تغییر دهد [۲].

تلفن‌های IP خاصی وجود دارند که برای تست کردن گذرگاه‌های VoIP و پراکسی‌های SIP و ثبت کننده‌ها مفید

[1] Network Address Translation

می‌باشند. تعداد زیادی سایت (مثل sipxphone و YATE)، تلفن‌های نرم‌افزاری SIP را که کاملاً قابل پیکربندی هستند در اختیار قرار می‌دهند. هنگام تست آسیب‌پذیری شبکه‌های VoIP، لازم نیست تا هر تلفن IP تست شود. تست کردن یک تلفن IP از هر شرکت سازنده، اغلب کافی است بدلیل اینکه پیکربندی آن‌ها از لحاظ عملکرد یکسان می‌باشد [۲].

۵- نتیجه گیری

با توجه به رشد روزافزون تکنولوژی VoIP پیش‌بینی می‌شود که استفاده از این تکنولوژی در صنعت برق بیش از پیش مورد توجه قرار گیرد. پس از ظهور این تکنولوژی و با همگرایی شبکه‌های صوت و داده، مسائل امنیتی داده به عنوان مسائل امنیتی صوت نیز مطرح شدند. برای بی‌اثر نمودن تهدیدات امنیتی VoIP، لازم است از یک نقشه یا طرح خوش‌ساختار استفاده شود. این طرح باید دارای رمزنگاری صوت، تصدیق هویت، فایروال‌های مختص صوت و قابلیت تفکیک ترافیک داده و صوت باشد. همچنین سرورهای صوتی و سایر اجزای شبکه‌های VoIP باید به لحاظ فیزیکی نسبت به مهاجمین در امنیت کامل قرار داشته باشند. بطور کلی به منظور حفاظت از شبکه‌های VoIP راهکارهای زیر توصیه می‌شوند:

- آموزش مدیران و اپراتورها در زمینه ابزارها و تکنیک‌های جدید
- اطمینان یافتن از اینکه همه سیستم‌های شبکه شده (بطور مثال سرورهای حیاتی VoIP)، دارای آنتی‌ویروس‌ها مقاوم و به‌روز هستند و انتخاب کلمه‌های عبور مناسب برای سیستم‌ها
- جداسازی ترافیک صوت و داده توسط VLANها، فایروال‌ها و لیست‌های کنترل دسترسی
- نصب و نظارت بر سیستم‌های تشخیص نفوذ مبتنی بر میزبان و مبتنی بر شبکه
- تحلیل وقایع ثبت شده از سیستم‌های تشخیص نفوذ، فایروال‌ها، مسیریاب‌ها، سرورها و وسایل دیگر شبکه
- قرار دادن همه تلفن‌های PC در پشت یک فایروال یا ACL تا ترافیک VoIP را بررسی کنند.
- همه ارتباطات HTTP به فایروال‌های VoIP باید از طریق یک VPN تونل شوند یا در غیراینصورت از HTTPS استفاده شود.
- استفاده از IPSec یا SSH برای همه دسترسی‌های مدیریت و نظارت از راه دور
- در صورت استفاده از VLAN غیرفعال کردن درگاه‌های VLAN که غیر قابل استفاده هستند و اطمینان یافتن از اینکه همه تلفن‌های IP و تلفن‌های نرم‌افزاری در VALN صوت قرار دارند.
- غیرفعال کردن درگاه شبکه داده در داخل تلفن VoIP هنگامی که از آن استفاده نمی‌شود.
- ممنوع شدن نصب و استفاده خصوصی از تلفن‌های نرم‌افزاری
- داشتن گواهی نامه در همه تلفن‌های IP، تلفن‌های نرم‌افزاری و سخت‌افزارها و نرم‌افزارهای سرور VoIP یک شبکه
- قرار دادن NIDS در محلی که بتوان ترافیک حیاتی را به طور مؤثر نظارت کرد و رمزنمودن ارتباطات بین اجزای IDS (سنسورها و کنسول مدیریت)
- طراحی مناسب شبکه جهت مقابله با حمله Dos به طور مثال در نظر گرفتن پهنای باند کافی، فایروال‌ها و SCTP جهت مقابله با DoS

مراجع

[۱].Jane Dudman, Gaynor Backhouse, " Voice over IP: what it is, why people want it, and where it is going ", JISC Technology and Standards Watch, September 2006.

[۲].Thomas Porter, Jan Kanclirz, Andy Zmolek, Antonio Rosela, Michael Cross, Larry Chaffin, Brian Baskin, Choon Shim, "Practical VoIP Security", Copyright © 2006 by Syngress Publishing, www.syngress.com.

[۳].Syed A.Ahson, Mohammad Ilyas,"VoIP Handbook; Applications, Technologies, Reliability, and Security", CRC Press, Taylor & Francis Group, 2009.