
**دانشکده مهندسی**

**گروه برق**

پایان نامه کارشناسی

**گرایش** : الکترونیک

**عنوان** : بررسی پروتکل SIP و چالشهای امنیتی آن

**استاد راهنما** : دکتر شهرام محمدی

**نگارش** : سیامک حبیب وند

خرداد ۱۳۸۷



سیامک حبیب وند ۸۲٤٤٦۱۲۲

# من از آن دست که می پرورَدَم



# می رویَم ...





سیامک حبیب وند ۸۲٤٤٦۱۲۲

# فهرست

# فصل اول

# Session Initiation Protocol (SIP)

**Today's hottest communication protocol**

## فصل اول : مقدمه

### ۱- ۱- تاریخچه :

طی سالهای گذشته در صنعت مخابرات، مواجه شدن با مسائلی از جمله: افزایش ظرفیت کاربران شبکه مخابراتی، نیاز به سرویس های بیشتر، جدیدتر و کامل تر، وجود زیر ساختی امن و قابل اطمینان، امکان ارتقا و همگام بودن با نیاز های روز و البته قیمت ارزان تر، موجب طراحی های جدید در زیرساخت ها و پروتکل ها شده است.

زمانیPSTN (Public Switched Telephone Network) برای ترافیک صدا و ترافیک اندکی از داده ها از نقطه ای به نقطه دیگر استفاده می شد . اما ترافیک داده ها به طور فزاینده ای رشد کرد و در سال ۱۹۹۹ تعداد بیت های داده ای که جابجا شدند برابر با تعداد بیت های صوتی بوده اند در سال ۲۰۰۲حجم ترافیک داده ها به صورت نمایی رشد کرد ، در حالی که رشد ترافیک صوتی یکنواخت بود .

بسیاری از متصدیان شبکه packet switching علاقه مند شدند صدا را از طریق شبکه دادهای خود انتقال دهند. هزینه تلفن افراد احتمالاً بیشتر از هزینه اینترنت آنهاست . لذا متصدیان



سیامک حبیب وند ۸۲٤٤٦۱۲۲

شبکه دریافتند که از طریق تلفن اینترنتی می توانند درآمد زیادی کسب کنند ، زیرا نیازی به فیبر نوری جدید نیست بنابراین تلفن اینترنتی(صدا از طریق IP ) متولد شد .

شبکه جهانی PSTN با وجود فراگیر بودن در سرتاسر جهان، در سال های اخیر نتوانسته پا به پای رشد سرویس ها پیش بیاید و این جایگاه جدید توسط پروتکل هایی که مناسب نیازهای این زمان هستند می بایست پر شود. در ابتدا این شبکه بر مبنای تکنولوژی Circuit Switching کار می کرده که پس از ثابت شدن مزایای بسیار در Packet Switching ، کم کم جای خود را به این تکنولوژی داده . حتی PSTN نیز نتوانست بی تأثیر از کنار این تغییر بگذرد . از طرفی رشد اینترنت و ارتباطات تحت آن ، هم چنین فراگیر شدن استفاده از IP نه تنها برای اتصال به اینترنت و مزایایی که ارتباط تحت IP از آن برخوردار است همه به این سو پیش می رود که نسل بعدی سیستم های مخابراتی ، سیستم های مبتنی بر IP باشند . از مهم ترین دلایل چنین رویکردی می توان به سادگی تعاریف هر گونه سرویس یا برنامه کاربردی روی این بستر اشاره نمود .

**پیش از ادامه ی بحث خالی از لطف نمی باشد که مروری بر شبکه های Circuit Switching و Packet Switching داشته باشیم :**

## ۲-۱- Circuit switching

شرکت های تلفن بیش از یکصد سال است که از تکنولوژی Circuit Switching استفاده می نمایند . در روش فوق بمحض برقراری ارتباط بین دو نفر ، در تمام مدت زمان مکالمه یک مدار اختصاصی برای آنها در نظر گرفته خواهد شد. بدین ترتیب برای دو نقطه مربوطه یک ارتباط دو سویه ایجاد می گردد . نحوه انجام یک مکالمه صوتی به صورت زیر است :

- پس از برداشتن گوشی تلفن یک بوق شنیده می گردد . بوق فوق بمنزله برقراری ارتباط با شرکت تلفن ( مرکز مربوطه ) است .
- با استفاده از سیستم تلفن ، اقدام به شماره گیری می گردد .
- ارتباط مورد نظر از طریق مجموعه ای از سوئیچ ها عبور داده شده تا به مخاطب مورد نظر برسد .
- یک ارتباط بین تلفن شما و مخاطب برقرار و یک مدار فعال می گردد .
- مکالمه با مخاطب مورد نظر در مدت زمان دلخواه انجام می گیرد .
- پس از قطع مکالمه ، مدار فعال شده بین شما و مخاطب غیر فعال خواهد شد .

فرض کنید مدت زمان مکالمه شما ده دقیقه باشد ، در طول مدت زمان فوق مدار ایجاد شده بین دو تلفن بصورت پیوسته فعال خواهد بود. در سیستم های قدیمی مخابراتی ، مکالمه تلفنی با نرخ انتقال اطلاعات ثابت ۱۲۸ کیلوبیت در ثانیه انجام می گرفت . با توجه به اینکه در هر کیلوبایت ، هشت کیلوبیت وجود دارد ، بنابراین در هر ثانیه ۱۶ کیلو بایت و یا در هر دقیقه ۹۶۰ کیلوبایت اطلاعات ارسال می گردد( زمانی که مدار فعال است ) . بنابراین در مدت زمان ده دقیقه ارتباط تلفنی ، مجموع اطلاعات ارسال شده ۹۶۰۰ کیلو بایت ( ۹/۴ مگابایت ) خواهد بود .

در یک مکالمه تلفنی اکثر داده های ارسال شده بیهوده می باشند . زمانی که شما حرف می زنید ، مخاطب صرفاً گوش می دهد . این بدان معنی است که در هر مقطع زمانی ، ازنصف خط ارتباطی بیشتر استفاده نمی گردد. ( سکوت موجود بر روی خط در مدت زمان برقراری ارتباط زیاد خواهد بود ) در این حالت حجم اطلاعات ارسال شده ، به ۴/۷ مگابایت تنزل پیدا خواهد کرد .



سیامک حبیب وند ۸۲۴۴۶۱۲۲

شبکه های مبتنی بر داده از روش Circuit switching استفاده نکرده و در مقابل از روش Packet Switching استفاده می کنند .

# Packet Switching

در روش Packet Switching بر خلاف Circuit Switching که بصورت پیوسته ارتباط را فعال نگه می دارد ، صرفاً در زمان ارسال اطلاعات ( یک بخش کوچک داده که به آن packet گفته می شود ) ارتباط فعال خواهد شد . اطلاعات مربوط به فرستنده به مجموعه ای از Packet تقسیم می گردد . در هر یک از بسته های اطلاعاتی آدرس فرستنده و دریافت کننده اطلاعات قرار خواهد گرفت . دریافت کننده بسته های اطلاعاتی ، اطلاعات را به یکدیگر ملحق تا اطلاعات اولیه بوجود آیند . روش فوق بسیار کارآ بوده و زمان فعال بودن ارتباط بین فرستنده و گیرنده را به حداقل مقدار خود می رساند. بدین ترتیب ترافیک موجود بر روی شبکه نیز کاهش خواهد یافت . کامپیوترهای فرستنده و گیرنده در زمان ارتباط با یکدیگر قادر به دریافت و یا ارسال اطلاعات برای سایر کامپیوترها نیز خواهند بود .

تکنولوژی VoIP از روش Packet Switching استفاده می کند . با استفاده از روش فوق امکان برقراری چندین مکالمه تلفنی فراهم می گردد . با استفاده از Packet Switched ، یک مکالمه ده دقیقه ای ، ده دقیقه کامل از زمان انتقال با نرخ ۱۲۸ کیلوبیت در ثانیه را اشغال خواهد کرد. در روش PSTN ، مکالمه ده دقیقه ای اشاره شده صرفاً حدود ۵ دقیقه زمان انتقال را با نرخ ۱۲۸ کیلوبیت در ثانیه اشغال خواهد کرد . در این حالت ۱۲۸ کیلوبیت در ثانیه برای زمان باقیمانده آزاد خواهد ماند. (با فرض نرخ انتقال ۱۲۸کیلو بیت در ثانیه)

## ۳- ۱-IP تلفنی

IP تلفنی ، ارسال مکالمات تلفنی بر روی یک شبکه مبتنی بر داده است . به تکنولوژی فوق VOIP (Voice Over IP) نیز گفته می شود . امروزه مکالمات صوتی گسترده ای از طریق شبکه های مبتنی بر داده ( نظیر اینترنت ) انجام می گیرد .

## روش های استفاده از VoIP

برای استفاده از VoIP ، چهار حالت متفاوت وجود دارد :

- **کامپیوتر به کامپیوتر** . ساده ترین روش استفاده از VoIP است . شرکت های متعددی ، خدمات فوق را ارائه می دهند. برای استفاده از روش فوق به نرم افزار مربوطه ، میکروفن ، بلندگو ، کارت صدا و خط ارتباطی با سرعت مناسب ( خطوط DSL و یا مودم های کابلی ) نیاز خواهد بود. MSN Explorer یک نمونه از نرم افزارهای مربوطه در این زمینه است .
- **کامپیوتر به تلفن** . با استفاده از روش فوق می توان از طریق کامپیوتر با هر شخص که دارای یک خط تلفن است ، ارتباط برقرار کرد. برای استفاده از روش فوق به یک نرم افزار سرویس گیرنده نیاز خواهد بود . نرم افزار فوق اغلب بصورت رایگان در اختیار علاقه مندان قرار می گیرد مثلاً نرم افزار Net۲Phone .
- **تلفن به کامپیوتر** . برخی از شرکت ها ، شماره تلفن های خاصی را بمنظور تماس کاربران معمولی تلفن با کامپیوتر فراهم نموده اند . نصب یک نرم افزار خاص بمنظور انجام عملیات فوق ، بر روی کامپیوتر سرویس گیرندگان ، الزامی است .
- **تلفن به تلفن** . با استفاده از Gateways می توان با هر تلفن استاندارد در سطح دنیا ارتباط برقرار کرد. برای استفاده از سرویس فوق که توسط برخی از شرکت ها ارائه می گردد ، می بایست در ابتدا با یکی از Gateway های مربوط به آنان تماس برقرار کرد . در ادامه شماره تلفن

مورد نظر خود را مشخص و نهایتا" توسط شرکت مربوطه امکان برقراری ارتباط با استفاده از یک شبکه مبتنی بر IP فراهم خواهد شد . در این روش ، لازم است که در ابتدا از یک شماره خاص استفاده گردد . ( شماره مربوط به Gateway شرکت ارائه دهنده خدمات فوق ) .

اکثر سازمانها و موسسات با نصب سیستم های VoIP امکان استفاده از IP تلفنی را برای کاربران خود فراهم نموده اند . تکنولوژی فوق با سرعت در حال رشد و گسترش همگانی است . کیفیت بالا و هزینه پایین از مهمترین دلایل فراگیر شدن تکنولوژی فوق است .

فرض کنید که شرکت شما دستگاه مورد نظر بمنظور استفاده از سرویس VoIP را خریداری و نصب کرده باشد .

در شرکت مربوطه صدها تلفن و یک PBX Private branch exchange نیز نصب شده است . PBX سوئیچی است که از آن بمنظور ارتباط مجموعه ای از تلفن ها به یکدیگر و به یک یا چندین خط خارج از شرکت استفاده می گردد. PBX ها معمولاً در سازمانها و موسسات بکار می روند زیرا استفاده از یک PBX ارزانتر از اتصال یک خط خارجی به هر تلفن در سازمان می باشد . در ضمن برای ارتباط درون سازمانی ( ارتباطهای زیر مجموعه PBX ) کافیست سه یا چهار رقم شماره گیری شود .

در مثال فوق PBX بصورت یک gateway است .

از gateway بمنظور ارتباط دستگاههای موجود در دو شبکه متفاوت استفاده می گردد. PBX یک Gateway است . ( چون سیگنال های استاندارد circuit-switching هر یک از تلفن ها را به داده های دیجیتال بمنظور ارسال از طریق یک شبکه مبتنی بر IP و Packet Switching تبدیل می نماید )

روش برقراری یک مکالمه از طریق یک شبکه Packet-Switching و با استفاده از VoIP بصورت زیر است :

- دریافت کننده را فعال تا از طریق آن یک سیگنال برای PBX ارسال گردد .
- PBX سیگنال را دریافت و یک بوق آزاد را برای فرستنده ارسال می دارد .
- فرستنده اقدام به شماره گیری تلفن مخاطب مورد نظر را می نماید. شماره فوق در ادامه توسط PBX بصورت موقت ذخیره می گردد .
- PBX در رابطه با نحوه تطبیق شماره دریافتی با شخص مورد نظر اقدامات لازم را انجام خواهد داد . درفرآیند تطبیق ، شماره مورد نظر به آدرس IP دستگاه دیگر که "میزبان IP" نامیده می گردد ، ملحق می گردد. "میزبان IP" عملاً یک PBX دیجیتالی دیگر است که به سیتم تلفن محلی که با آن ارتباط برقرار شده ، نصب شده است . در موارد خاصی که مخاطب از یک سرویس گیرنده VoIP مبتنی بر کامپیوتر استفاده می نماید ، "میزبان IP" ، سیستمی است که قصد برقراری ارتباط با آن وجود دارد .
- یک session بین PBX اداره تماس گیرنده و "میزبان IP" برقرار می گردد. هر سیستم می بایست از پروتکل ها مشابه بمنظور برقراری ارتباط استفاده نماید.
- مکالمه به مدت زمان مورد نظر انجام می گیرد.در زمان برقراری مکالمه ، PBX شرکت شما و میزبان IP مخاطب ، بسته هایی اطلاعاتی را ارسال و یا دریافت می دارند .
- مکالمه به اتمام رسیده و دریافت کننده غیرفعال می گردد .
- پس از قطع ارتباط ، مدار( ارتباط ) موجود بین تلفن تماس گیرنده و PBX آزاد می گردد .
- PBX سیگنالی را برای میزبان IP ارسال و خاتمه مکالمه را اعلام می نماید.

**دانشجویان محترم:**

**جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.**

اما در نوع Data Firewall که برای حفاظت یک شبکه از اینترنت یا سایر شبکه‌ها بکار می‌رود ، Firewall دیتا معمولاً در لایه‌های IP و UDP/TCP عمل کرده و مشخص می‌نمایند که چه نوع ترافیکی و چه سیستمی اجازه دارد تا ارتباط برقرار نماید. این نوع firewall لایهٔ Application را مانیتور نمی‌کنند. برای اینکار می‌توان از سایر محصولات مانند email content monitor یا web firewall استفاده نمود. فایروال دیتا مواردی را برای SIP درنظر دارد به گونه‌ای که از پورتهای IP مجزائی برای سیگنالینگ و دیتا استفاده می‌نماید. SIP آدرسهای پورت مدیا را در SDP قرار می‌دهد که فایروال باید با آگاهی از SIP، NAT را انجام دهد.

**NAT** ، ( برگرفته از Network Address Translation ) ، مکانیزمی برای ترجمه آدرس است . اکثر کاربران اینترنت با سرعت بالا از NAT استفاده می نمایند . تکنولوژی فوق به منظور تامین امنیت کاربران ، آدرس داخلی آنان را از دید شبکه های خارجی مخفی نگه می دارد .

با وجود تمام این اوصاف حتی اگر دیوارآتش کاملاً پیکربندی گردد، باز هم مشکلات امنیتی فراوانی وجود دارد . برای مثال همانطور که دیدیم دیوارآتش در برابر حملات DOS آسیب پذیر بود .

## ٤-٦-پیشنهادات

امنیت در SIP با امنیت IP پایه و همچنین VOIP شروع می‌شود. امنیت در SIP را می‌توان با استفاده از سیستم‌هایی که TCP/IP را برای سیگنالینگ پشتیبانی می‌نمایند توسعه داد. با این کار Spoof نمودن پیامهای SIP برای یک حمله‌کننده خیلی مشکل‌تر خواهد شد.

همچنین می‌توان آنرا با استفاده از یک استاندارد امنیتی مانند TLS افزایش داد (RFC٢٢٤٦) که در این حالت می‌توان یک authentication قوی بین اجزای SIP برقرار نمود. این استانداردها باید در تمامی اجزای سیستم SIP پیاده شود. هنگامیکه یک استاندارد امنیتی مانند TLS استفاده

می‌شود نباید از تجهیزاتی که قادر به پشتیبانی آن نیست استفاده شود. استفاده از اجزای ناامن مانند یک تلفن SIP ارزان حملات توضیح داده شده در بالا را ممکن می‌سازد.

به نظر می‌رسد که گروههای کاری SIP درحال حرکت به سمتی هستند که در آن برای حفاظت سیگنا لینگ از TLS و برای حفاظت مدیا از Secure RTP (SRTP) استفاده شود. به عبارت دیگر وقتی سیگنالینک SIP در یک شبکه نامطمئن از طریق پروکسی انجام می‌شود، همین استانداردها باید بکار گرفته شود که در این حالت نیاز است که فایروال بتواند TLS را پشتیبانی نماید. اگر این استاندارد استفاده نشود، سیگنالینگ باید از طریق پروکسی‌های حفاظت نشده انجام شود. این خود نیاز به فایروالهای SIP-Optimized را نشان می‌دهد که سیستم SIP داخلی را از حملات حفاظت می‌نماید. وظایفی که باید برای فایروال درنظر داشت عبارتند از :

۱- کنترل نمودن پیامهای SIP ورودی و خروجی از حملات لایهٔ application و حذف پکتهای زیان‌بخش :

- کنترل تلاشهای خارجی برای registration hijacking
- کنترل پیامهای SIP ناقص
- بررسی هدرهای VIA و RECORD-ROUTES
- جلوگیری از درخواستهای زیان‌بخش تخریب‌کننده

۲- درصورت امکان ، پشتیبانی از TLS و سایر موارد امنیتی استاندارد.

۳- کنترل تعداد تماسهای همزمان.

۴- حفظ QOS برای تمامی پکتهای مدیا. درنظر گرفتن تقدم برای پکتهای مدیا و حفظ QOS برای آنها.

## ۵-۶- نتیجه :

انتظار می‌رود که در آینده، SIP پروتکل مورد استفاده در VOIP باشد و مانند سایر پروتکلهای VOIP، به سختی قابل امن شدن می‌باشد. SIP یک پروتکل درحال تکامل بوده و در آن امنیت به صورت built-in نمی‌باشد. SIP نسبت به حملات معمول VOIP و همچنین حملات مختص SIP، آسیب‌پذیر می‌باشد. سیستم SIP را می‌توان بوسیله اقدامات انجام شده برای امنیت VOIP و استفاده از امنیت استاندارد بر روی تمامی اجزای سیستم به خوبی امن نمود. هنگامیکه در یک شبکه نامطمئن از SIP استفاده می‌شود باید تمامی استانداردها را لحاظ کرد. استفاده از فایروالهای بهینه شده برای SIP که در آن از امنیت استاندارد استفاده شده ( بالطبع در مواردی نیز بالاجبار از امنیت استاندارد وسیع نمی‌توان بهره جست ) به خوبی بهترین حفاظت را مهیا می‌نماید.



سیامک حبیب وند ۸۲۴۴۶۱۲۲

**مراجع :**

[۱]seedorf,jon, “sip security , status quo and future issues”university of hamburg

[۲] Georgios Zervas, Yixuan Qin, Reza Nejabati, Dimitra Simeonidou, FrancoCallegati, Aldo Campi, Walter Cerroni,”sip protocol”

[۳] “computer Networks” , Andrew S.Tanenbaum,Third Edition, Prentice-Hall, ۱۹۹۶.

[٤] H. Park, Multi-Protocol Authentication for SIP Network, ComputerCommunications (۲۰۰۸)

RFCs
RFCs Title
RFC ۱۸۸۹ RTP: A Transport Protocol for Real-Time Applications
RFC ۲۳۲۷ SDP: Session Description Protocol
RFC ۲۵٤۳ SIP: Session Initiation Protocol
RFC ۳۲٦۱ SIP: Session Initiation Protocol
And other RFCs



سیامک حبیب وند ۸۲٤٤٦۱۲۲