عنوان پروژه:

پروکسی سرورهای SIP

و امنیت آن با استفاده از مدل سازی

نام و نام خانوادگی:

استاد راهنما:

رشته و مقطع :

کارشناسی نرم افزار کامپیوتر

شماره دانشجویی:

ترم/سال:


بسم الله الرحمن الرحيم
الحمد لله رب العالمين الرحمن الرحيم مالك يوم الدين
اهدنا الصراط المستقيم صراط الذين
انعمت عليهم غير المغضوب عليهم
ولا الضالين

تقدیم به :

تشکر و قدر دانی:

چکیده

شبکه IMS با معماری مبتنی بر IP و بر اساس استانداردهای موسسه 3GPP در شبکه های سلولی میتواند به عنوان هسته شبکه های NGN مد نظر قرار گیرد. این شبکه سیگنالینگ SIP را برای کنترل ارتباطات کاربر تا شبکه بین گره های سرویس شبکه و سرور ها و پروکسی ها در نظر گرفته است . در شبکه IMS با توجه به الزامی بودن ثبت نام کاربران و اضافه شدن برخی سرآیند ها به سیگنالینگ SIP حملاتی ، متفاوت از VOIP رخ می دهد که منجر به آسیب پذیری ها در پروکسی SIP می شود . یکی از روش های تحلیل آسیب پذیری سیستم ها به منظور ارتقای امنیتی آنها مدل سازی سیستم از طریق روش های مدل سازی موجود می باشد . یکی از روشهای مدل سازی موجود TVRA است که توسط موسسه استاندارد سازی ETSI در سال ۲۰۰۳ پیشنهاد و کامل شده است.

در این روش مرحله به مرحله اهداف امنیتی ، نقاط ضعف سیستم ، سرمایه ها و دارایی های سیستم به همراه تهدیدها و حملات به نقاط ضعف بررسی شده است. با استفاده از این روش پروکسی سرورهای SIP در چارچوب IMS مدل شده است . مدلسازی پروکسی SIP به مشخص شدن آسیب پذیری های آن در سبکه IMS کمک می نماید. تحلیل این آسیب پذیری ها روش بهینه در طراحی و پیاده سازی را به همراه ارتقای امنیتی پروکسی و کاهش هزینه ها به دنبال خواهد داشت . در روند این عمل ابتدا اهداف امنیتی سرور ها ، سرمایه ها و دارایی ها ی منطقی و فیزیکی این سرور ها به همراه نقاط ضعف ، آسیب پذیری ها و حملات شایع بر روی سرور ها بررسی شده و در انتها جدول تمهیدات امنیتی تعریف شده ارایه شده است.

کلمات کلیدی : IMS SIP ، TVRA ، پروکسی سرور SIP ، آسیب پذیری ، تهدید

فهرست مطالب

فهرست اشکال

فهرست جداول

فصل اول:

مقدمه

۱-۱- مقدمه

بهبود امنیت سیستم و افزایش اطمینان از عملکرد آن از دید محرمانگی ، یکپارچگی و احراز هویت مستلزم تعیین نیازمندیها ، اهداف امنیتی ، حملات و تهدید ها می باشد. انجام این مراحل در بهبود پیاده سازی یک سیستم موثر خواهد بود. مدل سازی امنیتی سیستم سرور SIP در شبکه IMS از این طریق یک راه در ارتقای امنیت شبکه و سرورهای پروکسی آن می باشد. در این پژوهش با هدف شناسایی نقاط ضعف امنیتی پروتکل SIP تلاش شده است با استفاده از متودولوژی TVRA رفتار یک پروکسی SIP مدل شود.

۱-۲- طرح مساله

اهمیت امنیت و سرمایه های مادی و مهنوی شرکت های مختلف باعث شده است که تمروزه متدولوژی ها و روش های مختلفی برای ارزیابی ریسک و تهدیدات در سیستم های مختلف وجود داشته باشد. هر چند از نقطه نظر نحوه مدلسازی و نوع پیاده سازی ممکن است تفاوت هایی بین این متدولوژی وجود داشته باشد ولی هدف همه این روش ها ارائه پاسخ مناسب به سوالاتی مشابه سوالات زیر است:

۱- چه مواردی در سیستم نیاز به مراقبت دارند؟

۲- چه مواردی تهدید و آسیب پذیری سیستم هستند؟

۳- پیامد آسیب یا تخریب سیستم چیست؟

۴- چه مواردی برای سازمان ارزشمند است؟

۵- چه کارهایی میتوان در جلوگیری و کاهش هزینه های تخریب سرمایه های سازمان انجام داد؟

به طور خلاصه می توان گفت که هدف نهایی و خروجی اصلی در ارزیابی تهدیدها و ریسک در یک سیستم ، ارائه پیشنهاداتی برای به به حد اکثر رسانیدن حفاظت از محرمانگی ، یکپارچگی و در دسترس بودن است . این

پیشنهادات حفاظتی باید به گونه ای باشد که اختلالی در عملکرد سیستم پایه از نظر سرعت و نحوه استفاده ایجاد نکنند. مراحل اصلی ارزیابی ریسک شامل موارد زیر است :

۱- تعیین محدوده سیستم و دارایی ها

۲- جمع آوری داده ها

۳- تحلیل سیاست ها و رویه ها

۴- تحلیل تهدید ها

۵- تحلیل آسیب پذیری ها

۶- ارزیابی مقبولیت ریسک

استفاده از روش های استانداردی نظیر TVRA می تواند ارزیابی درستی از عملکرد سیستم در زمان وقوع حملات ارائه نماید . مدل TVRA توسط موسسه ETSI به عنوان یک روش مدل سازی سیستم ارائه شده است تا با شناسایی تهدیدات مربوط به سرمایه های سیستم ، تمهیدات امنیتی و حفاظتی ضروری را برای کاهش ریسک ها و ارتقای امنیتی سیستم پیشنهاد دهد . به صورت خلاصه ، در تعریف مدل TVRA می توان گفت : هر سیستمی که طراحی می شود دارای ارزش ها و دارایی هایی است که ممکن است ضعف هایی داشته باشد. تا زمانی که این ضعف ها مورد تهدید قرار نگیرند سیستم مشکلی تدارد. زمانی که تهدید ها و حملاتی بر اساس نقاط ضعف یک سیستم تعریف و عملی شد ، آن سیستم آسیب پذیری هایی خواهد داشت.طراحی هر سیستم اهداف امنیتی تعیین شده ای دارد که این اهداف با تهدید ها مختل می شوند. با مدل نمودن یک سیستم با روش TVRA ارتباط بین نقاط ضعف ، تهدیدها ، اهداف امنیتی و تمهیدات امنیتی به دست می آید . این مدل سازی دارای مراحل زیر است :

۱- تعیین اهداف و نیازمندیهای امنیتی سیستم

۲- تعیین ارزشها و دارایی ها

۳- تعیین ضعف های سیستم

۴- دسته بندی حملات و تهدیدها

۵- تعیین تمهیدات امنیتی

۱-۳- اهداف

با تعیین مراحل ذکر شده در مدل سازی یک سیستم قبل از طراحی آن ، آسیب پذیری های سیستم بدست می آید. این آسیب پذیری ها تابعی وابسته به ارزش ها ، نقاط ضعف ، جملات و تهدیدها و اهداف امنیتی است. با مد نظر قرار دادن آسیب پذیری های بدست آمده از مدلسازی می تئان در زمان پیاده سازی سیستم ، موارد لازم و تمهیدات امنیتی را در نظر گرفت. می توان با کمک جدول نهایی ارائه شده تعادلی بین هزینه ها در زمان طراحی یک پروکسی SIP ایجاد کرد.

۱-۴- ساختار

در این پژوهش ابتدا معرفی مختصری از معماری و ساختار شبکه IMS تعیین جایگاه سرورهای SIP ،ساختار سیگنالینگ SIP ، روش های ثبت نام کاربر و تشکیل مکالمه تشریح می شود. این موارد مختصری از اطلاعات مربوط به تعیین جایگاه سرور ها و موقعیت آن در معماری IMS را نشان داده و چگونگی سیگنالینگ را توضیح می دهد. در بخش بعدی آسیب پذیری ها و روش های ارتقای امنیت ارایه شده .نمونه فعالیت ها و اقدامات انجام شده در مقابله با انواع حملات و تهدیدهای سرورها و فعالیتهای مشابه در بهبود عملکرد امنیتی سیگنالینگ SIP و پروکسی سرورهای آن در شبکه IMS از نظر امنیتی بررسی و تحلیل شده است. هر کدام از این موارد دارای نقاط ضعف و قوتی می باشد که در بخش مربوطه بحث شده است.در بخش بعدی مدل سازی به روش TVRA تشریح می شود و تمام مراحل این استاندارد با توجه به مراجع استاندارد شده مربوطه توضیح داده

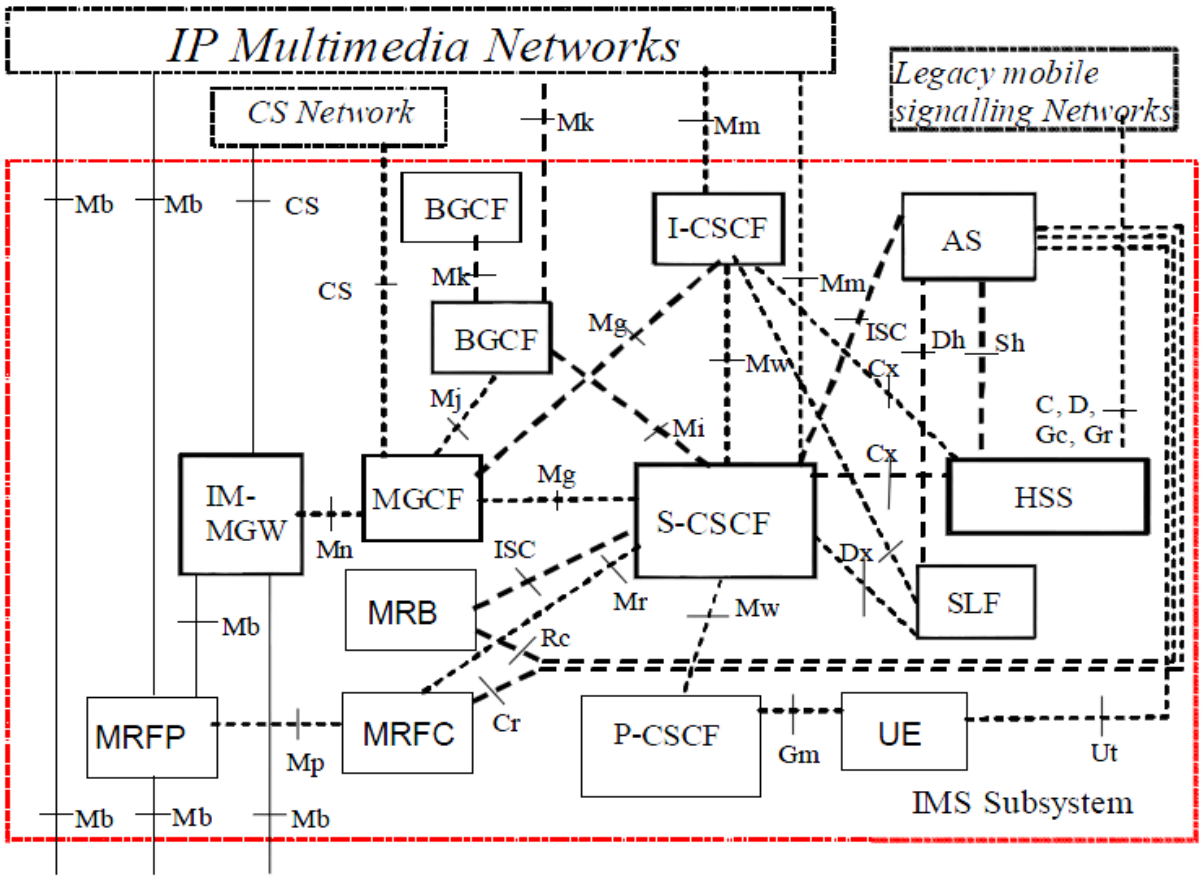
شده است و پس از آن پروکسی SIP مدل شده تشریح شده است و جدول های نهایی مدل شده سرور SIP با توجه به مراحل و موارد تعیین شده ددر استاندارد بدست آمده است. در انتها مراجه و منابه به صورت فهرسا آمده است.

فصل دوم:

مروری بر موضوع

۲-۱- معرفی تاریخچه و معماری و پروتکل های کلیدی IMS

شبکه های ارتباطی بین کاربران دارای فناوری های ارتباطی متفائت می باشد. این فناوری ها نیازمند یک هسته ارتباطی می باشند که تعامل بین آن ها را برقرار نماید.ایجاد تعامل بین فناوری های دسترسی متفاوت مستلزم تعریف واسطهای ارتباطی بین هسته شبکه های متفاوت می باشد. روش دیگری نیز برای این امر می توان پیشنهاد نمود.این روش استفاده از یک هسته مشترک برای تمام فناوری های متفاوت ارتباطی موجود می باشد که فناوری ها در خواستهای ارتباط یک هسته مشترک می باشد که فناوری های ارتباطی IMS را گرغته و تحلیل می نماید . فناوری هسته بی سیم ، سیمی ، ثابت و داده را ارتباط می دهد. این سیستم با استفاده از سیگنالینگ های ارتباطی مختلف نظیر SIP ، به منظور تولید نشست ها ، Diameter برای فر آیند AAA و سیگنالینگ های بخش رسانه نظیر RTP ، SDP فعالیت می کند . معرفی آسیب پذیری های SIP و حملات آن و مدل نمودن آن مستلزم آشنایی اولیه با سیستم IMS و معماری آن می باشد. معماری IMS توسط موسسات 3GPP و ETSI در استانداردها تشریح شده است.استاندارد 3GPP TS23.229 معماری IMS و استاندارد 3GPP TS33.203 معماری امنیتی IMS را تشریح می نماید. پروتکل SIP در اواخر سال ۱۹۹۶ به عنوان یک جزء از مجموعه پروتکلهای Mbone مطرح گردید و در سال ۱۹۷۰ اولین تجربه در انتقال صوت بر روی شبکه های مبتنی بر IP با استفاده از استاندارد SIP به وجود آمد .در این فصل مشخصه های معماری IMS المان ها و عناصر آن را به همراه مختصری از وظایف این عناصر مخصوصا سرور های سه گانه آن را تشریح می نماییم.معماری IMS یک معماری مبتنی بر IP می باشد و سرویس های چند رسانه ای را بر اساس فناوری IP بر قرار می نماید این معماری را موسسه 3GPP تعریف نموده است و بخش کنترل و حامل های رسانه و سیگنالینگهای مربوطه جدا از هم هستند و لایه دسترسی شبکه مستقل از فناوری مربوط می باشد.این معماری توسط 3GPP2،ETSI،ITU-T به عنوان هسته لایه کنترل شبکه های NGN پذیرفته شده است. معماری تابعی در IMS دارای سه سطح کاربرد ، کنترل ، انتقال و دسترسی می باشد که سیگنالینگ SIP در لایه کنترل آن می باشد و ارتباط همه کاربران از طریق IP با این سیگنالینگ با IMS برقرار می شود.



شکل (۲-۱) معماری تابعی در IMS

توابع مهم شبکه IMS مرتبط با SIP شامل سرور های S-CSCF ، I-CSCF ، P-CSCF ، تابع و سرور داده های کاربران (HSS) می باشد . بین سه سرویس دهنده S-CSCF، P-CSCF اهمیت بیشتری دارند.در این تحقیق سه تابع یاد شده مورد مطالعه قرار می گیرد و سیگنالینگ SIP در ارتباط با کارکردهای این توابع و بررسی و مدل می شود.

۲-۱-۲- معرفی پروکسی P-CSCF

این تابع یکی از سرورهای مهم سیگنالینگ SIP می باشد که اولین نقطه اتصالی کابر به شبکه IMS و سرویس های آن می باشد.این سرور توسط DHCP و یا PDP به دست آمده است و ایجاد ارتباط امن با کاربر را بر عهده

دارد. این سرور با دریافت پروفایل کابر از HSS توسط واسط Cx تشخیص می دهد که آیا یک کاربر اجازه استفاده از سرویسی خاص را دارا می باشد یا نه . مجاز شناسی منابع کاربران ، ارتباطات اضطراری ، کنترل کیفیت سرویس ، مونیتورینگ ، فشرده سازی هدرها و شناسایی I-CSCF جزو وظایف این بخش است و وظیفه دریافت و ارسال پیام های سیگنالینگ را از/به کاربر IMS مهیا می شود. فشرده سازی پیامها ی ارسالی با استفاده از الگوریتم های توافق شده انجام می شود . الگوریتم های مربوط به مکانیزم های امنیتی پروتکل های IPSec ، TLS نیز در این سرور نگهداری می شود. این سرور سر آیند های مربوط به این پروتکل ها را از پیام جدا کرده و آن را برای تحلیل ، به سرور I-CSCF تحویل می دهد . تمام کاربران از طریق این پروکسی به HSS ، S-CSCF متصل می شوند و این پروکسی وظیفه حفاظت از آن دو را برعهده دارد .

۲-۱-۳- معرفی پروکسی I-CSCF

این سرور از طریق HSS متوجه نوع S-CSCF مربوط به کاربر می شود تا درخواست کاربر را به آن سرور ارجاء دهد . مخفی نمودن پیکربندی شبکه IMS ، مهیا نمودن ورود کاربر به شبکه خانه در زمان جابه جایی به شبکه میزبان و محاسباط مربوط به صورت حساب کاربر (CDR) در این سرور انجام می شود . یک شبکه می تواند بیش از یک سرور I-CSCF داشته باشد. این سرور به عنوان یک دروازه برای شبکه IMS می باشد. این سرور وظیفه محافظت از پیکربندی شبکه میزبان را زمانی که پیام شبکه خارجی ارسال می شود بر عهده دارد. در این زمان سرآیندهای route ، record-route ، via رمز می شوند و تنها شبکه هایی که با شبکه میزبان قرارداد دارند کلیدهای رمزگشایی را در اختیار خواهند داشت. به این ترتیب تعداد هاب ها و نوع پیکربندی شبکه خانه (اطلاعات درون- record-route, route) محرمانه باقی می ماند .

۲-۱-۴- معرفی پروتکل S-CSCF

این سرور مهمترین سرور SIP در IMS و به صورت یک سرور state full می باشد. موقعیت و مکان کاربر را مشخص می نماید. ثبت نام کاربر و بهره برداری از آن از سرویس های شبکه را فراهم می نماید. پروتکل احراز هویت IMS AKA با استفاده از بردار احراز هویت ارسال شده از HSS به این سرور اجرا می شود . در زمانی که یک کاربر سرویس (as) بخواهد در مورد یک اتصال و درخواست SIP ارسال شده اطلاعاتی دریافت نماید از این پروکسی کمک میگیرد. اطلاعات دریافت شده از HSS در S-CSCF تحلیل و آنالیز شده و با توجه به این اطلاعات تصمیمات گرفته می شود . هر داده ای به ازای یک سرویس دهنده کاربردی ارسال می شود . این سرور امکان اتمام یک مکالمه را با توجه به اولویت بندی هایی که شبکه اعلام می نماید دارا می باشد . اطلاعات نیز در این سرور نگه داری می شود . این اطلاعات شامل آدرس HSS ، پروفایل کاربر ، آأرس P-CSCF ، دامنه P-CSCF ، شناسه عمومی کاربر ، شناسه خصوصی کاربر و آدرس IP تجهیزات کابر می باشد .

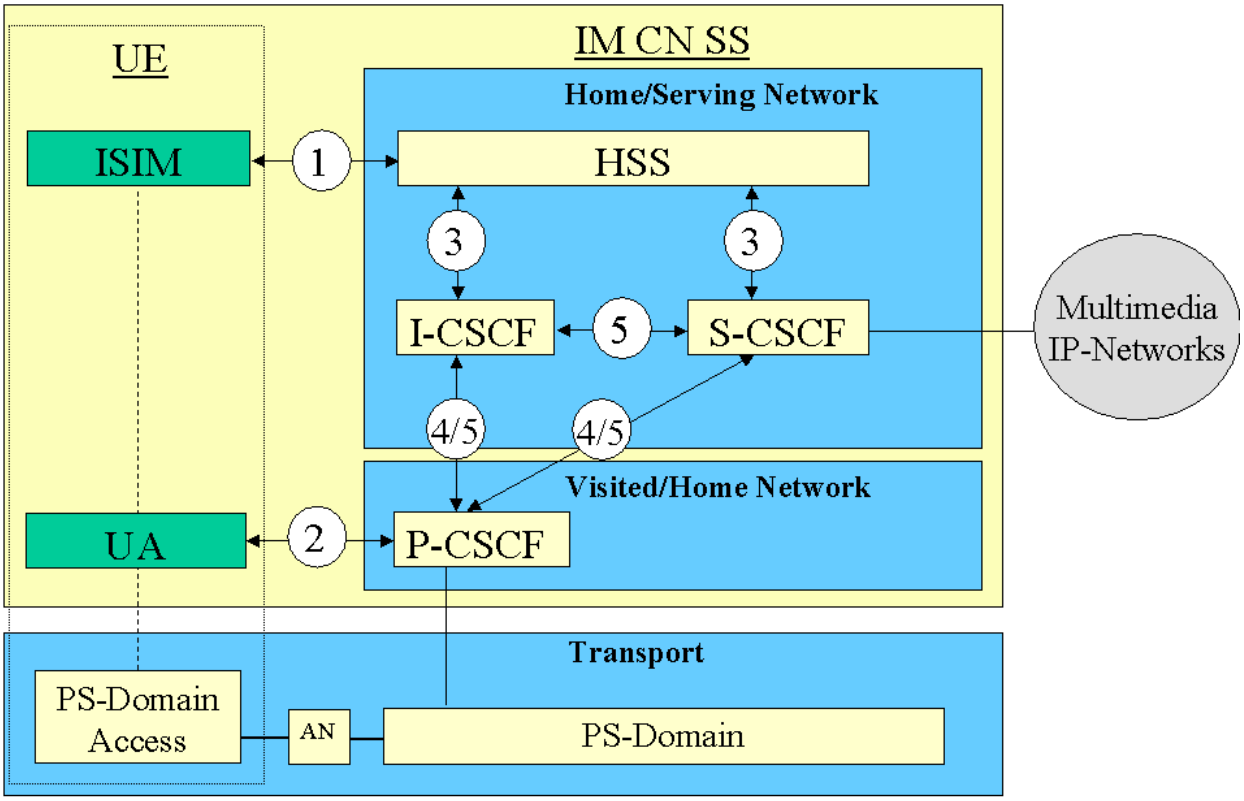
۲-۱-۵- معرفی سرور HSS

این سرور معادل HLR در شبکه 2G،3G می باشد . این تابع پایگاه داده اصلی شبکه IMS می باشد که داده های کاربران Ims ، پروفایل کاربر ، اطلاعات موقعیت کاربر و پروفایل سرور کاربردی در آن نگه داری می شود.

۲-۲- معماری امنیتی IMS

معماری امنیتی شبکه IMS شامل ارتباط امن بین واسط های نوابع آن می باشد . این معماری در استاندارد 3GPP TSS 33.203 تعریف شده است و معماری امنیتی شبکه IMS را از دید موسسه 3GPP مشخص می

نماید . مطابق با استاندارد ذکر شده ، معماری امنیتی IMS دارای پنج بخش ارتباطی امن (SA) بین توابع IMS می باشد که در شکل زیر اشاره شده است. در ادامه بخش های ارتباطی امن اشاره شده در استاندارد را بررسی و مطالعه می نماییم.



شکل (۲-۲) معماری امنیتی IMS

SA1 : احراز هویت دوسویه بین UE (ISIM) و هسته شبکه IMS می باشد و HSS مسوول شناسایی کاربر به سرور S-SCSF می باشد . کاربر دارای یک شناسه خصوصی (IMPI) و حداقل یک شناسه عمومی ماربر (IMPU) می باشد. ارتباط بین HSS و ISIM از طریق IMPI برقرار می شود و پروتکل ارتباطی AKA می باشد.

SA2: یک ارتباط ایمن بین تجهیزات کاربر و سرور P-CSCF برای محافظت از واسط ارتباطی Gm برقرار می نماید احراز هویت داده برقرار می شود به این معنی که داده ای که دسیده است قابل اعتماد و درست می باشد. تعریف واسط ارتباطی Gm در استاندارد 3GPP TS 23.002 تشریح شده است.

SA3 : ارتباط امن بین پروکسی های SIP و HSS را در حوزه شبکه داخلی با واسط ارتباطی (Cx) برقرار می نماید . پروتکل ارتباطی diameter بر روی SCTP به همراه IPSec می باشد.

SA4 : ارتباط امن پروکسی SIP را وقتی کاربر در شبکه میزبان است بین دو شبکه و برقرار می نماید . توضیحات مربوطه در استاندارد 3GPP TS 33 210 تشریح شده است . این ارتباط در زمانی کهP- CSC در شبکه میزبان واقع شده است ؛ اعمال خواهد شد .

SA5 ارتباط امن بین پروکسی های درون شبکه با گره های SIP برقرار می نماید . این ارتباط برای زمانی است که کاربر در حوزه شبکه خانه است . توضیحات مرتبط با آن در استاندارد 3GPP TS 33.210 ارایه شده است.

به این پنج بخش ارتباطی امن دو بخش جدید SA7 ، SA6 نیز اضافه شده است . بخش SA6 ارتباط امن بین کاربردهای نصب شده در بخش تجهیزات کاربر و لایه کاربرد شبکه IMS می باشد .

بخش SA7 نیز ارتباط بین تجهیزات کاربر از طریق شبکه های دسترسی متنوع با شبکه میزبان می باشد .

SA6 : ارتباط امن بین سرورهای کاربردی هسته IMS با کاربردهای نصب شده در UE را برقرار می کند . کاربردهای مبتنی بر HTTP در IMS توسط AS هدایت می شوند . پروکسی احراز هویت AP مسوول انجام این عملیات است . از استاندارد GBA ، GAA و TLS برای ایجاد ارتباط ایمن استفاده می کنند . پروتکل TLS یک کانال امن ایجاد می کند .

SA7 : ارتباط امن کاربر با شبکه IMS از طریق شبکه های دسترسی دیگر نظیر ، UMTS ، NGN،WiMax در زمانی که کاربر در شبکه میزبان قرار دارد را برقرار می نماید .

با بررسی این دامنه های امنیتی جدا شده درون معماری IMS بخش های SA3 ، SA2 جزو مختصات پروژه قرار دارند .پس از معرفی معماری IMS و توابع و عناصر مرتبط با سیگنالینگ SIP ، در ادامه به ساختار سیگنالینگ SIP و معرفی مشخصه های کاربردی آن در IMS خواهیم پرداخت . آشنایی با ساختار این سیگنالینگ در شناسایی آسیب پذیری های آن و ارتقای آمنیت آن مفید خواهد بود .

۲-۳-ساختار سیگنالینگ و ویژگیهای پیام های IMS SIP

پروتکل SIP جزو سیگنالینگ های کنترلی در معماری IMS می باشد . احراز هویت مبدا و مقصد در ارتباط ، احراز هویت یک ارتباط و پشتیبانی از ثبت نام ، اصلاح اطلاعات موقعیت های کاربران ، محرمانگی در سیگنالینگ مکالمه ها و جریانهای داده ای و غیره از وظایف این سیگنالینگ است . استاندارد 3GPP TS24.229 استانداردهای مربوط به اجرای SIP در Ims را توضیح داده است . این سیگنالینگ در دامنه PS و در سطح کاربر IMS مبادله می شود . مطابق با IETF RFC 3261 سیگنالینگ SIP دارای دو حالت در پیامهای ارسالی می باشد . پیامهای ارسالی شامل پیام درخواست و پیام ارسال می باشد . پیامهای در خواست نظیر bye ، invite به منظور ایجاد تغییرات در یک اتصال ارسال می شوند ، در حالی که پیام های پاسخ نظیر ok برای توجه دادن به نتایج ناشی از ارسال در خواست می باشند . پیامهای در خواست شامل شش در خواست option ، ack ، invite bye ، register ، cancel می باشند و پیامهای پاسخ شامل سه دسته پیام 1xx,2xx,3xx,4xx,5xx,6xx می باشند .

آدرس دهی در SIP به صورت URI می باشد.

- یک پیام درخواست SIP حداقل دارای هدر فیلدهای TO,from,Cseq,Call-ID,Max-Forwards,Via می باشد . موارد ذکر شده حداقل هدر فیلدهای ضروری در یک پیام sip می باشد .
- پارامتر via آدرس و مسیری از شبکه است که کاربر پاسخ درخواست هایش را خواهد گرفت .

- پارامتر branch شامل شناسه تراکنش در یک ارتباط می باشد .
- پارامتر to شامل نام کاربر و uri آدرسی می باشد که درخواست ارتباط با آن به سرور ارسال شده است.
- پارامتر from شامل نام کاربر و uri فرستنده درخواست است.
- پارامتر call-id نشان دهنده یک مکالمه و دیالوگ می باشد که شامل تمام مراحل ارتباط یک call و تنظیمات ددوباره و تغییرات تنظیمات در طول یک ارتباط است و شناسه یک نشست می باشد.
- پارامتر Cseq همان sequence number است و شامل متد درخواست یک شمارنده است که با هر بار ارسال درخواست در یک مکالمه افزایش می یابد . پارامتر Cseq برای پاسخ یک شمارنده جداگانه ای دراد و تنها برای درخواست ها است که شمارنده افزایش می یابد .
- پرامتر Max-Forwards برای محدود نمودن تعداد hop های انتقال درخواست است تا زمانی که به مقصد می رسد و با هر بار عبور از یک hop شمارنده آن کم می شود.
- متدهای سیگنالینگ sip همان نوع یک پیام هستند و توضیحات اضافی راجع به نوع درخواست و برخی ویژگی های ارتباط درخواستی توسط کاربر را در بر دارند . هیچ متد اضافی در IMS برای sip تعریف نشده است و تمام متدهای تعربف شده در voip در شبکهIms قابل استفاده می باشند.

۲-۴- تفاوت های سیگنالینگ IMS SIPوVOIP SIP

در ادامه تفاوت ها و ویژگی های سیگنالینگSIP در شبکه IMS با سیگنالینگ در شبکه VOIPتشریح می شود .

۲-۴-۱- کیفیت سرویس

یکی از تفاوت های اصلی این دو شبکه، پشتیبانی از کیفیت سرویس در سیگنالینگاست SIP شبکه IMS که افزایش کارایی سرویس های ارایه شده به کاربران را به دنبال خواهد داشت .کیفیت سرویس مستلزم ذخیره منابع درون شبکه به منظور تامین سطح کیفیت درخواستی کاربر می باشد .با تخصیص منابع لازم در شبکه IMS به سرویس ها، کاربران سطح کیفیت و چگونگی خدمات ارایه شده از شبکه را تعیین می کنند. شبکه IMS با توانایی در ذخیره منابع و یا اولویت بندی ترافیک در ارسال پیام ها به شبکه، امکان ارتقای سطح سرویس را فراهم می نمایند .کنترل سطح سرویس از طریق ارتباط با زیرساخت فیزیکی و کنترل آن امکا نپذیر میشود . تضمین و ارایه کیفیت سرویس درIMS بر عهده سرور P-CSCF و از وظایف این سرور است .

۲-۴-۲- استفاده مفید و موثر از منابع

شبکهIMS به عنوان هسته شبکه‌های سیار نظیرUMTS طراحی شده است. در این شبکه‌ها پهنای باندشبکه محدود است و این یکی از محدودیت‌های موجود در شبکه‌های سیار نسبت به شبکه‌های سیمی‌می‌باشد که استفاده مفید و موثر از منابع را در شبکهIMSالزامی می‌نماید. این محدودیت‌ها بین کاربرو نقطه دسترسی به شبکه شامل انرژی، مقدار ظرفیت CPUسرورها، تجهیزات کاربر و تعدادکاربرانی که منابع را به صورت مشترک استفاده می‌نمایند، می‌باشد. استفاده موثر و کارا از پهنای باند آزاد شبکه یکی از مواردی است که بین IMS SIPو VOIP SIPتفاوت ایجاد می‌نماید.

۲-۴-۴- فشرده سازی پیام ها

به دلیل مبتنی بر متن بودن پیام‌ها در سیگنالینگSIP و ارسال این پیام‌ها در بازه هوایی، فشرده‌سازی‌پیام‌ها، منجر به ذخیره منابع و کاهش پهنای باند اشغالی خواهد شد. کاهش پهنای باند اشغالی یکی ازموضوع‌های مهم در شبکه‌های سیار می‌باشد. مقدار و درصد فشرده‌سازی یک پیام با توجه به

الگوریتم توافق شده و نوع پیام فشرده‌شده می‌تواند تا ۰۸٪ کاهش حجم پیام را در پی داشته باشد.برخی الگوریتم‌های فشرده‌سازی دارای عملیات بازیابی طولانی می‌باشد که سرورP-CSCF را درگیرپردازش‌های خود می‌نماید. یکی از روش‌های حمله در این شبکه ارسال درخواست modifyو تغییرتنظیمات نشست می‌باشد. در این درخواست‌ها مهاجم درخواست استفاده از الگوریتم‌های پیچیده وسنگین می‌نماید و سرور را مجبور می‌کند تا زمان زیادی را در پردازش درخواست‌ها صرف نماید.علاوه بر این موضوع بین درخواست‌های سیگنالینگSIP دو درخواستRegistration, Invite حجم‌بیشتری را نسبت به دیگر درخواست‌های ارسالی از سوی کاربر دارند. به همین دلیل نوع درخواست‌نیز در مقدار و حجم فشرده‌سازی موثر می‌باشد. سرور-P CSCFپارامترهای مربوط به فشرده‌سازی‌پیام‌های SIPو بازخوانی فرم فشرده‌شده را انجام می‌دهد. فشرده‌سازی پیام‌های این سیگنالینگ و الگوریتم‌های مربوطه در،IETF RFC۶۹۸۴ IETF RFC3320 تشریح شده است.

۲-۴-۵- ثبت نام قبل از دعوت ایجاد نشست

به منظور انجام محاسبات مربوط به صورت‌حساب و جلوگیری از سو استفاده از آدرس‌های کاربران،احراز هویت کاربر قبل از ارسال درخواست‌ها به مقصد نهایی انجام می‌پذیرد. به منظور جلوگیری ازاحراز هویت تمام درخواست‌ها، شبکه IMS اقدام به ثبت‌نام کاربر قبل از تنظیم هرگونه نشست‌می‌نماید. در حالی که در RFC۱۶۲۳ کاربر می‌تواند یک مکالمه را بدون ثبت آدرسIP و SIPخود آغاز نماید . ثبت‌نام کاربر قبل از آغاز

هرگونه ارتباط با شبکه، منجر به کاهش بسیاری‌از حملات رایج در VOIP SIPنظیر جعل آدرسIP و سایر شناسه‌ها، کاهش امکان شنود پیام‌ها به دلیل رمزشدن ارتباط و کاهش حملات با شناسه‌های سرقت شده توسط مهاجمان می‌شود.شبکهIMS امکان انتخاب قابلیت احراز هویت همه درخواست‌های کاربران SIPرا دارا می‌باشد. احرازهویت امکان ارتباط کاربر غیرمجاز را کاهش می‌دهد. در صورتی که شبکهIMS احراز هویت‌کاربران SIPرا الزامی نموده باشد، حملات ناشی از آدرس IPجعلی و یا spoofingغیرممکن‌می‌شود، زیرا کاربر از طریق S-CSCFمجبور است با پروتکلDIAMETER و المان HSSاحرازهویت شود(از طریق یکی از الگوریتم‌هایAKAو یا MD۵) و در این فرایند جعلی بودن آدرسIPمحرز می‌شود. به دلیل همین خاصیت ، IMSیک مهاجم امکان جعل هویت و شناسه یک کاربر راندارد. امکان جعل نامSIP و جازدن خود با نام کاربری دیگر نیز وجود ندارد.دایره حملات به شبکه IMSتنها به حملاتی محدود می‌شود که از شناسه‌ها و مشخصات مجاز یک‌کاربر استفاده نموده باشند. البته در دسته‌بندی حملات به سرورهایSIP در ،IMSحملات جعل‌آدرس،IPتنها در زمانی که شبکه شرط عدم احراز هویت پیام‌ها را پذیرفته باشد، می‌تواند انجام پذیرد.می‌دانیم IMSمی‌تواند، ارتباط با کاربر را بدون احراز هویت نیز تعریف نماید. زیرا با احراز هویت‌تمام درخواست‌های SIPارسال شده به ،S-CSCFترافیک واسط s-cscfو HSSافزایش چشمگیری‌می‌یابد. با انتخاب برخی سیگنال‌ها برای احراز هویت، کاهش بار این بخش را خواهیم داشت.واضح‌است که این تفاوتIMS با VOIPباعث ایجاد حملاتی خاص به IMSمی‌شود که در فصل سوم به‌این مهم می‌پردازیم.

۲-۶-۴- امنیت

درIMS برای سیگنالینگ ،SIPهیچ متد دیگری بجز آنچه در RFCهای معمولSIP تعریف شده استوجود ندارد. تنها برای الزامات امنیتی، بر روی سرآیند ،SIPمشخصه‌های یکپارچگی، احراز هویت ومکانیزم IMS AKAاضافه شده است. به این ترتیب تفاوت موجود بین شبکه‌های IMSوVOIP درپیاده‌سازی سیگنالینگ

،SIPهدرفیلـدهای اضـافه شـده در معمـاریIMS بـه منظـور پشـتیبانی سـیگنالینگSIP از سـرویس‌هـای اضـافه شـده در IMSانظیـر کیفیـت سـرویس، فشـرده‌سـازی‌پیام‌ها(۰۲۳۳ RFC،)مکانیزم‌های امنیتی محرمانگی، یکپارچگی، احراز هویت دوسویه وغیره می‌باشـد.این امکانات با کمک بیش از پنجاه سرآیند درIMS قابل دستیابی است. در حالی که متدهای اسـتفاده‌شده درIMS SIP همان متدهای استفاده شده در شبکه‌های دیگر ارتباطی می‌باشند.مکانیزم‌های امنیتی محرمانگی و یکپارچگی با الگوریتم‌های توافق شده بین کاربر و شبکه پیـاده‌سـازی‌می‌شوند. سرورP-CSCF کلید رمزنگاری را از پیام رسیده برداشته و پیام را تحلیـل و پاسـخ مـی‌دهـد.مکانیزم‌های مربوط به احراز هویت دوسویه بین کاربر و شبکه شامل روش‌های متنـوعی مـی‌باشـد کـه بین کاربر وشبکه مورد توافق قرار می‌گیرد. این مکانیزم‌ها شامل موارد زیر می‌باشند.

Early IMS authentication

o

NASS-bundled authentication(NBA)

o

http digest authentication(challenge-based auth.)

o

http digest over TLS, IPSec

o

IMS AKA : AV(Rand(IK,CK), Autn, Xres)

علاوه بر احراز هویت و محرمانگی، یکپارچگی ارتبـاط نیـز در ایـن شـبکه حفـظ مـی‌شـود. الگـوریتم‌یکپارچگی بین کاربر وP-CSCF برای محافظت از سیگنالینگ SIPتوافق می‌شود. ایـن توافـق بـرای‌کلید یکپارچگی برای محافظت از یکپارچگی نیز مـی‌باشـد. حمـلات Replay, Reflectionبـه دلیـل‌تست یکپارچگی پیام دریافت

شده از جانب کاربر و شبکه کاهش می‌یابد. مکانیزم یکپارچگی بین CSCF ها و همچنین بین CSCFها و HSSتوسط امنیت دامنه شبکه در استاندارد ۰۱۲،۳۳ GPP TS۳تعریف شده است.

۲-۵- مکانیزم های امنیتی IMS SIP

سیگنالینگ SIPدر موسسهIETF و با RFC۱۶۲۳ استاندارد شده است . این استانداردداری‌الحاقات بسیاری می‌باشد که پیاده‌سازی آن را در شرایط مختلف و با قابلیت‌های دیگر میسر می‌سازد.الحاقات امنیتی، مکانیزم‌های امنیتی را به منظور دسترسی ایمن کاربران SIPبه سرویس‌ها مهیا نموده‌است . یک کاربر شبکهIMS در پیام ثبت‌نام خود در فیلد سرآیندauthorization نوع مکانیزم‌احراز هویت خود را تعیین می‌نماید. نوع فناوری ارتباطی کاربر به شبکه از طریق محدوده‌آدرسIPکاربر و یا از طریق محتوای فیلد سرآیند P-Access-Network-Infoمشخص می‌شود. پروتکل‌هایی که به عنوان مکانیزم‌های امنیتی در شبکهIMS کاربرد دارند شامل موارد زیر می‌باشند:

Early IMS authentication

در این روش محرمانگی ارتباط بین کاربر و شبکه پشتیبانی نمی‌شود و ارتباطات رمزنمی‌شوند. در زمانی که شبکه تنها با IPv۴پیاده‌سازی شده است و کاربر وشبکه توافق کلید ندارند. درصورتی که سرآیند authorizationدر پیام کاربر وجود نداشته باشد، P-CSCFاز این روش برای احراز هویت کاربر استفاده می‌نماید.

NASS-bundled authentication(NBA)

این مکانیزم مختص به دسترسی کاربران با فناوری‌های پهن‌باند نظیرxDSL در شبکه‌هایNGN دارد. در این شبکه‌های کاربارن شناسهISIM ندارند و از طریق پروتکل احراز هویت در لایه‌انتقال ،NGNامکان دسترسی به شبکه را پیدا می‌نمایند. روشNASS در شبکه‌هایی که لایه انتقال‌مسوول احراز هویت می‌باشد وبا احراز هویت کاربر از طریق مکانیزم مبتنی برEAP لایهIP و با تغییراتی در بخش ثبت‌نامSIP انجام می‌شود. در صورتی که در سرآیند P-Access-Network-Info شرایط تعریف شده مناسب این روش باشد، NBAروش احراز هویت انتخابیP-CSCF خواهد بود.

Http Digest-based authentication (challenge-based auth)

این مکانیزم دو سویه است و در سطح کاربرد، عمل می‌نماید. زمانی که ISIMدر دسترس‌نیست اما امکان احراز هویت از طریق کلمه عبور و نام کاربری برقرار می‌باشد. در این‌حالت‌سیگنالینگSIP محافظت نشده و آسیب‌پذیر خواهد بود. هیچ مکانیزم امنیتی بین کاربر وP-CSCFاجرا نمی‌شود. تنها مکانیزم امنیتی استفاده شده در آن جدول چک آدرس IPکاربر می‌باشد و یک‌حفاظت اولیه در زمان جعل آدرس IP، حمله مرد میانی می‌باشد. در صورتی که سرآیندauthorization در پیام کاربر باشد اما تمهیدات یکپارچگی تعریف نشده باشد، سرورP-CSCF از این‌مکانیزم استفاده می‌نماید.

http digest over TLS, IPSec

در زمانی که ارتباط کاربر و شبکه نیازمند مکانیزم امنیتی محرمانگی و حفظ یکپارچگی‌پیام‌های ارسالی باشد، می‌توان احراز هویت Http digestرا به همراه TLSپیاده‌سازی نمودای‌نمکانیزم امنیت در لایه شبکه و انتقال را نیز برقرار می‌نماید. این ارتباط می‌تواند رمز نشده باشد اما حتماباید یکپارچگی پیام‌های ارسالی تامین گردد. نوع الگوریتم و چگونگی محافظت امنیتی در لایه امنیتیTLS توافق می‌شود. در زمان ثبت‌نام کاربر به شبکه، ارتباط بین P-CSCFو کاربر از طریق TLSمحافظت خواهد شد. امنیت این ارتباط نسبت به زمانی که تنها از پروتکل احراز هویتIMS AKAاستفاده می‌شود، بیشتر است زیرا مهاجم در صورتی که بتواند به پروتکل AKAنفوذ کند نمی‌تواندکلید نشست تولید شده در ارتباط TLSرا حدس بزند. در صورتی

که سرآیند authorizationدر پیام کاربر باشد و پارامتر حفظ یکپارچگی تعریف شده باشد،سرور-P CSCFاز این مکانیزم استفاده می‌نماید.

IMS AKA : AV(Rand(IK,CK), Autn, Xres)

کامل‌ترین و رایج‌ترین مکانیزم احراز هویت است که محرمانگی، یکپارچگی رانیز پشتیبانی‌می‌نماید که در بخش بعدی تشریح خواهد شد. این روش‌ها با توجه به امکانات کاربر وشبکه در زمان‌ایجاد ارتباط می‌توانند مورد استفاده قرار گیرند. روش‌های اشاره شده علاوه بر تایید یک کاربر به منظور استفاده از سرویس‌های شبکه، امکان حفظ یکپارچگی پیام‌های مبادله شده، محرمانگی داده‌های ارسال شده و دسترسی به آن‌ها را برای کاربران تعریف می‌نماید.در ابتدای احراز هویت کاربر توسط شبکه یک شناسه ارتباطی تعریف شده است که تنهاکاربر و شبکه به آن دسترسی دارند. در ادامه این شناسه و مکانیزم‌های امنیتی احراز هویت، محرمانگی و یکپارچگی ارتباط توضیح داده می‌شود.

۲-۵-۱-شناسهISIM

به منظور اعمال مکانیزم‌های امنیتی بر روی کاربر شبکه، یک شناسه ارتباطی خصوصی بین‌شبکه و کاربر تعریف می‌شود. این شناسه ارتباطی در شبکهISIM۱ نامیده می‌شود. داده‌های امنیتیIMS و توابع آن درون تجهیزات کاربر (UICC۲)ذخیره شده است. کاربران شبکه IMSنمی‌توانندتغییر و اصلاحی در نام دامنه شبکه خانه، شناسه کاربری و کلیدهای مربوط به الگوریتم‌های امنیتی خود در سیم کارت انجام دهند. در ابتدا مجموعه‌ای از روش‌ها و الگوریتم‌های پشتیبانی‌شده توسط دو طرف ارتباط به اشتراک گذارده می‌شود تا در مورد کیفیت ارتباط و نوع الگوریتم‌ها توافق حاصل شود. یکی از انتخاب ها بین شبکه و کاربر توافق شده و ارتباط امن ایجاد خواهد شد. انتخاب ها شامل‌موارد زیر می‌باشند:

- هیچ تابع امنیتی و یا دادهای به اشتراک گذاشته نمی‌شود.

- تنها الگوریتم‌ها به اشتراک گذاشته می‌شوند.
- کلید احراز هویت، مکانیزم چک شماره ترتیبی به اشتراک گذاشته می‌شوند.

کلید احراز هویت، توابع احراز هویت و مکانیزم چک شماره ترتیبی به اشتراک گذاشته می‌شوند.

۲-۵-۲- احراز هویت

یک کاربر IMSدارای اطلاعات و داده‌های مخصوص خود در HSSمی‌باشند که دراستاندارد۳۳،۸۲۲ GPP TS۳تعیین شده است. با تعیین شناسه ارتباطی کاربر، ارتباط با شبکه از طریق‌احراز هویت اولیه کاربر به شبکه شروع می‌شود. احراز هویت کاربر در زمان ثبت‌نام کاربر انجام‌می‌شود و کاربر با ثبت‌نام خود، توسط شبکه مجاز می‌شود تا از سرویس‌های ارتباطی بهره‌مند شود.احراز هویت درIMS به صورت دوسویه است و شبکه نیز به کاربر معرفی می‌گردد. مشخصه‌های‌کاربر توسط واسط ارتباطی Cxاز HSSبه S-CSCFمنتقل می‌شود. پروتکل احراز هویت استفاده‌شده در شبکه با نام IMS AKAمورد بهره‌برداری قرار می‌گیرد. این پروتکل از مشتقات AKAUMTS می‌باشد. تنها در IMS AKAپاسخیRESکه کاربر برای احراز هویت خود به شبکه ارسال‌می‌نماید به صورت رمز شده منتقل می‌شود، در حالی که پاسخ ارسال شده کاربر در UMTS AKAبه‌صورت متن رمز نشده و کاملا آشکار ارسال می‌شود و امکان شنود آن بیشتر می‌باشد.

۲-۵-۳- محرمانگی

با احراز هویت کاربر به شبکه، IMSسرویس‌های درخواستی کاربر را در دسترس او قرار خواهد داد.مکانیزم امنیتی محرمانگی داده در ارتباط بین شبکه و کاربر، با استفاده از الگوریتم‌های رمزنگاری‌انجام می‌شود.

ارتباط بین کاربر و P-CSCFتوسط این الگوریتم‌ها رمز می‌شود. تجهیزات کاربر،الگوریتم‌های رمزنگاری برای استفاده در نشست را برای P-CSCFارسال می‌نماید. مکانیزم‌محرمانگی مبتنی بر IMS AKAمی‌باشد. این سرور تصمیم می‌گیرد الگوریتم مورد استفاده کدام‌باشد و با الگوریتم مورد نظر شبکه نیز تطابق داشته باشد. توافق شبکه و کاربر، شامل کلیدهای رمزنگاری مورد استفاده در حفظ محرمانگی می‌شود. مکانیزم‌محرمانگی‌در3Gpp TS33.203تعیین شده است.

۲-۵-۴- یکپارچگی

یکی از موارد مهم در ارتباط کاربرو شبکه،حفظ یکپارچگی پیام‌های مبادله شده و اطمینان از عدم‌تغییر محتوای پیام انتقالی است. با این مکانیزم، حملات تکرار و بازتاب محدود خواهند شد.یکپارچگی ارتباط کاربر با شبکه می‌تواند با استفاده از پروتکل‌های ارتباطی لایه‌های مختلف نظیر ,IPSec TLSبرقرار شود. این مکانیزم امنیتی می‌تواند از طریق پروتکل‌های احراز هویت تعریف‌شده در بخش‌های قبل نیز به‌دست می‌آید. مطابق با ۱۶۲۳ ،RFCسرورهای SIPمی‌توانند به همراه پروتکل TLSپیاده‌سازی شوند. برای محافظت از محرمانگی و یکپارچگی ارتباط بین سرورها، این‌پروتکل در لایه بالای IPSecقابل اجرا می‌باشد و مشخصه‌های.Session ID, IP address, port Noدر اتصال TLSتعریف می‌شود. در صورتی که پروتکلTLS بر روی سرور قابل ارایه باشد، می‌تواند احراز هویت تشریح شده در 3GPP TS 33.310مورد استفاده قرار گیرد.

۲-۶- ثبت نام کاربر SIP درIMS (IMS AKA)

کاربر شبکهIMS در آغاز ارتباط ملزم به ثبت‌نام اولیه در شبکه به منظور تایید هویت است. الزام‌ثبت‌نام کاربران SIPدر این شبکه تعداد حمله‌های ناشی از جعل هویت کاربر و سایر شناسه‌ها راکاهش می‌دهد.

هرکاربر این شبکه دارای یک شناسه با نامISIM می باشد که در آن تمام پارامترهـای‌ضروری برای احراز هویت کاربر به شبکه هسـته و شناسـایی آن وجـود دارد و در۳۰۲،۳۳ GPP TSتشریح شده است . درون تجهیزات کاربر علاوه بر شناسه ،ISIMتنظیمات اولیه‌ای بـه منظـور مهیـانمودن ثبت‌نام کاربر به هسته شبکه موجـود مـی‌باشـد. ایـن پارامترهـا شـامل شناسـه خصوصـی کـاربر،شناسه عمومی کاربر و آدرس دامنه شبکه خانه که برای درخواست ثبت‌نام کاربرSIP استفاده می‌شود، می‌باشد. هر کدام از این شناسه‌ها در دسترس نباشد، ثبت‌نام کاربر عملی نخواهد بود.پروسیجر ثبت‌نام برای کاربران با استفاده ازAKA IMS در این شبکه اجباری است و ثبت‌نام با استفاده‌از TLSاجباری نیست. احراز هویت کاربر با پروتکل دوسویه AKA IMSبـا پروتکـل احـراز هویـت‌در شبکهUMTS یکسان است. تنها در انتقال پارامترهای پروتکلIMS تفاوت‌هـایی دارد. مقـدارRESمحاسبه شده توسط کاربر نه به صورت رمز نشده همانند UMTSبلکه به صورت مخلوط شدن با بقیـه‌پارامترها برای تولید پاسخ احراز هویت به شبکه ارسال می‌شود .

دسترسی کاربر به شبکهIMS از طریـق سـرورP-CSCF برقـرار مـی‌شـود. تجهیـزات کـاربر، سـرور-P CSCFمربوطه را در دامنه خود می‌یابد و یا از طریقDHCP نـام دامنـه و آدرس IPایـن‌سـروریافـت‌می‌شود و کاربر ثبت‌نام با شبکه را آغاز می‌نماید وتا زمانی که ثبت‌نام تمام نشده باشـد، نشسـت ایجـادنمی‌شود. پورت‌های۰۶۰۵و۱۶۰۵ برای اتصالاتSIP استفاده می‌شود وسرور درخواست‌هـای ثبـت‌نـام‌آمده از دیگر پورت‌ها را از حذفمی‌نماید. تنهـا درخواسـت ثبـت‌نـام اسـت کـه از ایـن پـورت شـنیده‌می‌شود و بقیه درخواست‌ها می‌توانند از پـورت‌هـای دیگـری کـه در هدرفیلـدهای درخواسـتی اشـاره‌می‌شود، انجام پذیرد.کاربر ابتدا سرور p-cscfمربوط بـه خـود را درشـبکه شناسـایی مـی‌نمایـد و سـپس‌پروسـیجری‌بـام‌نـام‌پردازش ثبت‌نام اولیه، شامل ارسال درخواست ثبت‌نـام بـدون مکـانیزم‌هـای امنیتـی اجـرا مـی‌شـود. درصورتی که مکانیزم‌های امنیتی فعال باشند، یک درخواست ثبت‌نام بـه همـراه حفـظ یکپـارچگی پیـام‌ارسال می‌شود. این حالت در زمانی است که احراز هویت به همراه پروتکلTLS اجرا می‌شـودو یـک‌اتصال TLSاز جانب کاربر برای برقراری نشست ایمن برای محافظـت از درخواسـت ثبـت‌نـام، ایجـادشده است . این نشست ایمن شده با

TLS،جانشین اتصالات قبلی می‌شود. پارامترهای احرازهویت سرآیند IMS AKAشامل بخش‌های مختلفی نظیر احراز هویت، مقدار پورت سرور در پارامترپورت میزبان، بخشsend-by در زمانی که روی UDPارسال انجام می‌شود، بخش سرآیند امنیتی کاربر همانند الگوریتم‌های امنیتی محرمانگی و سرآیند امنیتی سرور در پاسخ می‌باشد

۲-۶-۱- مراحل انجام ثبت نام کاربر SIP در شبکه IMS

ثبت‌نام کاربر ، اولین مرحله از آغاز ارتباط با شبکه می‌باشد و معرفی کاربر به شبکه ابتدایی‌ترین‌مرحله در آغاز ارتباط کاربر با شبکه به منظور دریافت سرویس‌های شبکه است. درخواست ثبت‌نام دارای هدر فیلد from, toیکسان می‌باشد زیرا درخواست ثبت‌نام می‌باشد و نه درخواست ایجاد یک‌مکالمه. بنابراین درخواست ثبت‌نام یک کاربر درSIP یک دیالوگ تولید نمی‌کند.ثبت‌نام کاربر در شبکه شامل دو مرحله است. ابتدا ارسال درخواست ثبت‌نام و سپس درخواست تعهدپرداخت۱ می‌باشد. پس از ثبت‌نام، کاربر به شبکه شناسایی شده است. در شبکهGSM کاربر توسط‌شبکه از تحت پوشش بودن خود آگاه می‌شود. در IMSپس از ثبت‌نام، درخواست تحت پوشش‌بودن در شبکه را می‌نماید. این درخواست می‌تواند به عنوان تعهد پرداخت کاربر برای محاسبه‌هزینه‌ها مورد استناد قرار گیرد. سرورP-CSCF با استفاده از Route-headerو سرورSCSCFبااستفاده از Service-Route headerدریافت‌شده در زمان ثبت‌نام، انجام می‌شود و پاسخnotifyازطریقP-CSCF به کاربر ارسال می‌شود. به این ترتیب کاربر از تحت پوشش قرار داشتن توسط شبکه آگاهی حاصل می‌نماید.

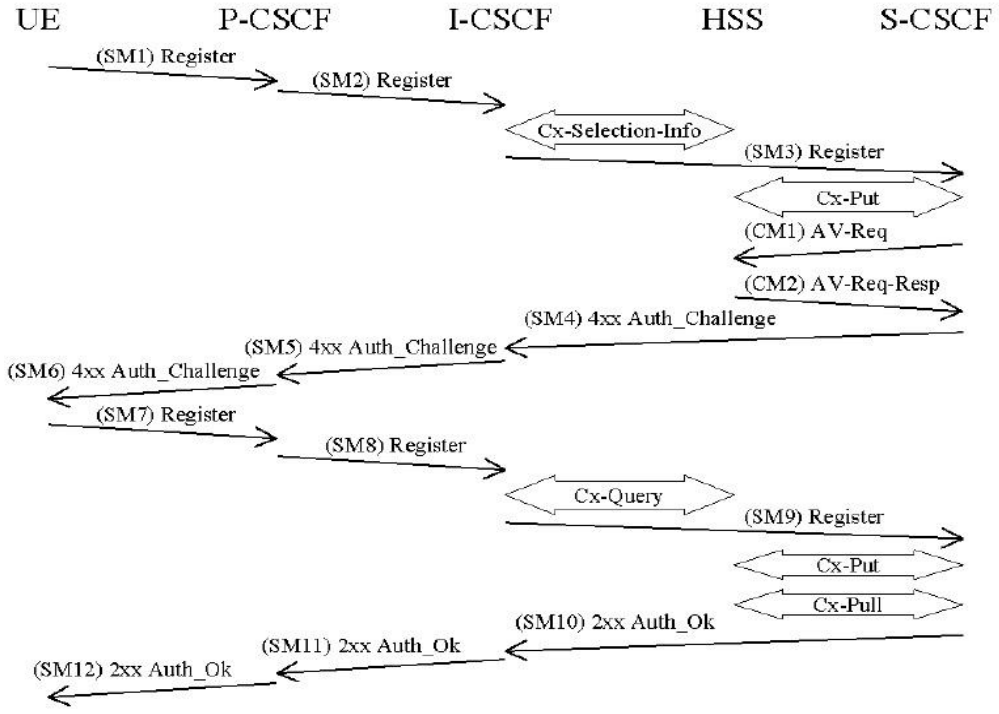
در ابتدا کاربر یک اتصال از طریقIP را انجام داده و گره اتصالی به IMSرا از طریقP-CSCF پیدامی‌کند. پس از شناساییP-CSCF کاربر درخواست ثبت‌نام خود را به آن می‌فرستد. این درخواست‌توسط پروکسی پردازش می‌شودو از نام دامنه برای یافتن آدرسIP پروکسیI-CSCF استفاده‌می‌کند و بهHSS متصل

می‌شود تا قابلیت‌ها و مشخصه‌های مورد نیازS-CSCF را انتخاب نماید. پس‌از یافتن I-CSCFدرخواست ثبت‌نام به S-CSCFارسال می‌شود. پروکسیS-CSCF پاسخ کاربر رادر مورد چالش و پاسخ چک می‌کند و در صورت صحت آن پروفایل کاربر را از HSSدانلود کرده‌و پاسخ۲۰۰ یا okرا ارسال می‌نماید. به صورت دورهای این ثبت‌نام باید به روز شود تا اتصال کاربربه شبکه باقی بماند. کلیدهای محرمانگی و یکپارچگی برای IMS AKAتوسط SIPمنتقل می‌شود.

بردار احراز هویت شامل RAND,XRES,CK,IK,AUTNهمانند توضیحات ۳۳،۳۲۰۱ TS GPPتولید می‌شود و ISIMو HSSمقدار SQNISIMو SQNHSSرا دنبال می‌نمایند تا درمبادله‌پیام‌هاپیامی اضافه و یا کم نشود و احتمال خطای Replay, Redirectکاهش یابد.

۲-۶-۲- دیاگرام ثبت نام در IMS از طریق IMS AKA

احراز هویت کاربر از طریق پروسیجر ثبت‌نام کاربر توسط شبکه انجام می‌گیرد. علاوه بر آن تجهیزات‌کاربر مکانیزم‌های امنیتی تعریف شده در RFC۹۲۳۳ مربوط به ارتباط امن از طریق IPSecواستاندارد ۳۰۲،۳۳ TS۳ GPPپارامترهای مورد نیاز در بخش امنیتی شروع ارتباط ضمیمهHراپشتیبانی می‌نماید. مشخصات ارتباطی در بخشIMS IPSec, TLS, AKA هر کدام یک نوع ارتباطایمن کاربر با شبکه را تعریف نمودهاند. ارتباط کاربر با شبکه می‌تواند شامل تمام فیلدهای امنیتی‌مربوط به این سه پروتکل امنیتی باشد. وجود هر کدام از این مکانیزم‌های امنیتی، ایمنی در لایه مربوطه‌را برای کاربر به ارمغان می‌آورد. فرآیند ثبت‌نام یک کاربر SIPدرIMS در ادامه مرحله به مرحله‌تشریح شده است. کلیه پیام‌های SIPاز میان اتصال امنیتی IPSecبین کاربر و پروکسیP-CSCFمبادله می‌شوند



شکل (۲-۳) احراز هویت کاربر با شبکه IMS AKA

کاربر با پروتکل ارتباطی خاصی به شبکهIMS متصل شده و آدرسP-CSCF را کشف می‌کنـد.کاربر پیام ثبت‌نام را به شبکه خانه برای انجام فرآیند ثبت‌نام ارسال مـی‌کنـد. بـا ارسـال ایـن پیـام،پروکسی ،I-CSCFپروکسی-S CSCFرا از طریق ارتباط با HSSبدسـت مـی‌آورد. پروکسـی -CSCFS بر اساس موقعیت کاربر و یا نوع سرویس درخواستی آن(ـویدیو، صوت، داده ...) مشخص‌می‌شود. یک شبکه می‌تواند دارای چندین -S CSCFباشد که معمولا S-CSCFمعادل بـرای هـرکاربر، پروکسی نزدیک به آن از نظر موقعیت می‌باشد. عامل مـوثر دیگـر در ارتبـاط بـاSCSCFخاص،اولویت‌های تامین‌کننده سرویس می‌باشد. در صورتی که -S CSCFپاسـخ I-CSCFرا به هر دلیلی ندهد، کاربر پاسخ ۶۰۰busy everywhere را ارسال می‌نماید.

اطلاعات مربوط به احراز هویت کاربر از HSSبرداشت می‌شود. این اطلاعات همان بردار AKAمـی‌باشـد. مرحلـه بعـدی احـراز هویـت کـاربر IMSاز طریـقIMS AKA مـی‌باشـد[۱۰۱]. کـاربردرخواست ثبت‌نـام را بـه همـراه شناسـه عمـومی خـود درونFROM,TO پیـام قـرار داده و بـرای‌سرورP-CSCF ارسال می‌نمایـد. آدرس دامنـه خانـه کـاربر از طریـق شناسـهISIM ویـا USIMوکاربرد نصب شده درون UEبه‌دست می‌آید

.پس از ارسال درخواست ثبت‌نام، کاربر پیام۱۰۴ را دریافت می‌نماید. این پیام یک چالش برای احرازهویت کاربر می‌باشد:

• کاربر مقدار xMACمحاسبه شده خود را با پارامتر MACبدست آمده ازAutn مقایسه می‌نماید و مقدارSQN بدست آمده از Autnپیام چالش نیز باید در محدوده مناسب باشد.

• در صورتی که هدر امنیتی سرور استاندارد۳۰۲،۳۳ ۳GPP TSدر هدر پیام ثبت‌نام‌کاربر موجود نباشد، کاربر پروسیجر احراز هویت آغاز شده را لغو کرده و یک پیام ثبت‌نام جدید با Call-IDجدید می‌فرستد.

• در صورتی که هدر امنیتی سرور استاندارد۳۰۲،۳۳ (۳GPP TSدر هدر پیام ثبت‌نام‌کاربر موجود باشد:

oپارامترهایRES,CK,IK را از مقدار تصادفیRAND محاسبه می‌نماید.

o کاربر بر اساس متغیرهایی که در پیام۱۰۴ دریافت می‌نماید، یک تنظیمات موقت امنیتی‌برای این ثبت‌نام تعریف می‌نماید. این تنظیمات با الگوریتم‌ها و مکانیزم‌های پیشنهادی P-CSCF که توسط کاربر نیز پشتیبانی می‌شود، انجام می‌شود. در این تنظیمات ازکلیدهای مشترکCK,IK در صورتی که از رمزنگاری در ارتباط پشتیبانی شده باشد،بهره برده می‌شود. یک مدت زمان اعتبار SIPبرای تنظیمات امنیتی کاربر تعریف می‌شود که درون تایمر مربوطه تنظیم می‌شود.

o یک درخواست ثبت‌نام جدید با تنظیمات امنیتی حاصل ارسال می‌شود. در این زمان کاربر شامل یک هدر احراز هویت نیز می‌باشد.

در این زمان پارامترهای realmبا پارامتر آمده از هدر احراز هویت wwwپر می‌شود. پارامتر usernameشناسه خصوصی کاربر و پارامترresponse با مقدار ، RESپارامتریuri با نام دامنه،SIP

پارامتر algorithmو nonceبا پاسخ۱۰۴ آمده از سرور جایگزاری می‌شوند.پس از ارسال پاسخ مربوطه، قبل از انقضای زمان تایمر، پاسخ OKاز شبکه ارسال می‌شود. در صورت عدم ارسال و یا ارسال forbiddenثبت‌نام ناموفق محسوب خواهد شد.پارامترهای تعریف شده در بالا بخش احراز هویت امنیتی هدر یک پیام ثبت‌نام در IMSپشتیبانی شده‌توسط SIPمی‌باشد. هدر پیام ثبت‌نام علاوه بر احراز هویت دارای بخش‌های دیگری نیز می‌باشد که‌در ادامه می‌آید.یک شماره پورت سرور برای هر هدر ارتباط و یک مقدار پورت در پارامتر-send byاضافه می‌شود.یک بخش هدر برای حفاظت از یکپارچگی و محرمانگی در لایهIPSec و الگوریتم‌های آن و با آخر محتوای هدر امنیتی رسیده در پاسخ از آخرین احراز هویت موفقیت‌آمیز می‌باشد

تمام پیام‌های SIPپروکسی‌های P-CSCF,S-CSCFهر دو کاربر را می‌پیمایند. این پیام‌ها فشرده‌سازی شدهاند. در مورد جریان داده و نوع کدک بین دو کاربر توافق نمودهاند. در نهایت کاربردوم صدای بوق را می‌شنود و اتصال را برقرار نموده و نشست تولید می‌شود.

فصل سوم:

آسیب پذیری ها و رو شهای ارتقای امنیت سرورها

۳-۱- مقدمه

ساختارIMS دارای آسیب‌پذیری‌های متنوعی می‌باشد زیرا کاربران در این شبکه همیشه به صورت‌برخط متصل می‌باشند و استفاده از نسخهSIP با ساختار باز آن را نسبت به حملات ،DOS, DDOS Floodingآسیب‌پذیر نموده است. موسسه۳GPPدر زمینه‌های احراز هویت دوجانبه درشبکه ،IMS AKAمکانیزم‌های کنترل دسترسی، حفظ محرمانگی در زمان ثبت‌نام، ربودن نشست،حمله مرد میانی۱، شنود و حمله ربودن۲، سعی فراوان نموده و تمهیداتی اندیشیده است اما درمقابل‌حملهflooding و حمله تغییر محتوای پیام‌ها نظیر SQL injectionتمهیداتی ندارد. معماریIMSدرشبکه از سه جهت مورد حمله قرار می‌گیرد:

۱- دسته اول بر اساس شبکهIP می‌باشد نظیر حملات ،replay, DOS, Spoofing, sniffing middle man می‌باشد.

۲- دسته دوم به علت طبیعت و ساختارSIP در لایه کاربرد است نظیر ،bogus terminate bogus register

۳- دسته سوم شامل حملاتی ناشی از ترکیب استفاده از SIPدر شبکه و آسیب‌پذیری‌های‌مختلف شبکهVOIP و رسانه‌های کاربردی می‌باشد نظیر overflow SQL injection, bufferحملات مربوط به دامنه تعریف شده در پروژه، حملاتی می‌باشند که وابسته به ماهیت سیگنالینگSIPو کارکرد آن در معماری شبکهIMS می‌باشد. آسیب‌پذیری‌های اشاره شده جزو عمده تهدیدهای این‌شبکه می‌باشد. در بخش بعدی تهدیها در سرورهای SIPرا بررسی خواهیم نمود. حملات مربوط به ،RTPحملات مبتنی بر IPو حملات مبتنی بر ساختار SIPاین سه دسته را تشکیل می‌دهندکه دودسته اول جزو قلمرو پروژه قرار ندارند.

۳-۲- آسیب پذیری ها در پروتکل AKA شبکه IMS

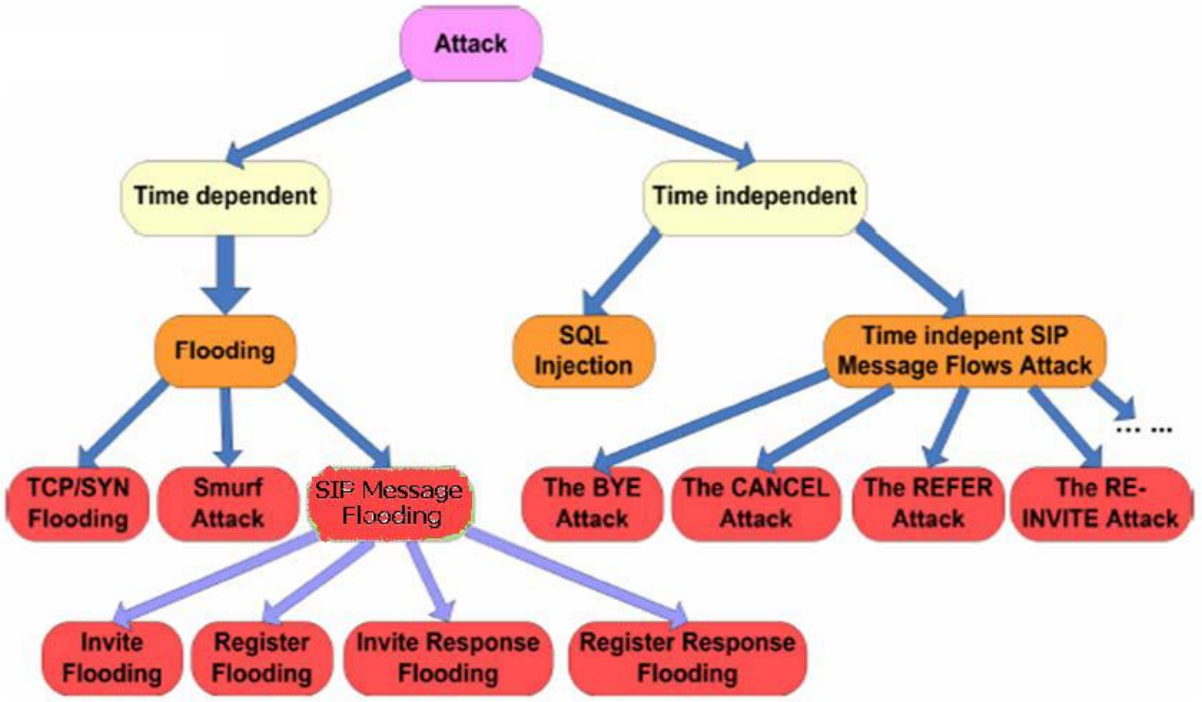
احراز هویت بین کاربران IMSو سرور ، P-CSCFیک ارتباط ایمن بین آن‌ها را ایجادمی‌نماید. در برخی مقالات در زمینه روش احراز هویت درIMS با نامAKA انتقاداتی وجود دارد وضعف‌های AKAمنجر به کاهش امنیت در این بخش می‌شود. پروتکل AKAدر مقابل BSهای‌جعلی آسیب‌پذیر می‌باشد. مهاجم می‌تواند ترافیک مکالمه یک کاربر را از یک شبکه به شبکه دیگراز طریق جریان ،AKAمنتقل نماید و مسیر جریان یک مکالمه را به مقصدی که خودمایل‌استراهنمایی نماید. یک مهاجم می‌تواند از بردارهای احراز هویت خراب شده در یک شبکه برای جعل‌نمودن و استفاده در شبکه دیگر بهره ببرد. از این طریق شبکه مورد حمله، می‌تواند برای شبکه‌های‌دیگر آسیب‌پذیری‌هایی ایجاد نماید. انتقال مکالمه در بین شبکه‌های زمانی که سطح امنیت پشتیبانی‌شده در دو شبکه یکسان نباشد، با موفقیت بالاتری قابل انجام خواهد بود. این آسیب‌پذیری در SA۱ (بخش۲-۲) تعریف می‌شود. برای بهبود عملکرد IMSدر این بخش مقاله‌ها و راه‌کارهای متفاوتی‌ارایه شده است و در حوزه کاری پروژه قرار نمی‌گیرد.

هدف از ارایه امنیت در دسترسی به ،IMSجلوگیری از دسترسی کاربران و ترافیک احراز هویت‌نشده به شبکه می‌باشد. دسترسی به هسته شبکه در چارچوب ،IMSتنها از طریق احرازهویت‌ترافیک‌امکان‌پذیر می‌باشد. کاربر احراز هویت می‌شود و یا اتصال امن بین کاربر و شبکهIMS ایجاد می‌شود.در حال حاضر در ،G۳تمام اتصالات به صورت رمز شده و احراز هویت شده می‌باشند. در معماری ارایه شده درTISPAN و ارتباطات سیمی این موارد الزامی نیست و در آینده الزامی خواهد شد. طبق‌آنچه در مرجع‌گفته شده است، شبکهIMS امکان انتخاب قابلیت احراز هویت‌همه‌درخواست‌های کاربران SIPرا دارا می‌باشد. با احراز هویت تمام درخواست‌هایSIP ارسال شده به ،S-CSCFترافیک واسط ارتباطی به نامCx که واسط بین S-CSCFو HSSمی‌باشد، افزایش‌چشمگیری می‌یابد. با انتخاب برخی سیگنال‌ها برای احراز هویت، کاهش بار این بخش را خواهیم‌داشت. در صورتی که شبکهIMS احراز هویت کاربران SIPرا الزامی نموده باشد، حملات ناشی ازآدرسIP جعلی و یا spoofingغیرممکن می‌شود، زیرا کاربر از طریق S-

CSCFمجبور است باپروتکلDIAMETER و المان HSSاحراز هویت شود(از طریق یکی از الگوریتم‌هایAKAو یاMD۵) و در این فرایند جعلی بودن آدرسIP محرز می‌شود. با درنظر گرفتن این مورد تنها مهاجمانی‌که بخش احراز هویت IMSرا با موفقیت انجام دادهاند می‌توانند حملاتی انجام دهند. در این موردملات ایجاد شده با حملات حوزهVOIP مشترک خواهند بود.

۳-۳- آسیب پذیری ها در ارتباط سرورهای SIP با کاربر

پیدا کردن یک دسته‌بندی کلی برای تمام آسیب‌پذیری‌های سرورهایSIP به صورتی که تمام‌حملات اشاره شده در مقالات متنوع را شامل شود، کار دشواری است. به صورت کلی حملات به دو دسته مستقل از زمان و وابسته به زمان تقسیم می‌شوند. حملات وابسته به زمان نظیر حملاتfloodingاست که شامل register, register response, Invite Response است. حملات مستقل‌از زمان حملاتی که نیازمند گذشتن زمان خاصی برای پدید آمدن نتیجه نیستند. مثال‌هایی ازاین‌حملات نظیر حملات تغییر محتوای یک پیام ارسالی (SQL injection) و یا حملات ارسال پیام بی‌موقع نظیرCancel, Bye, Re-Inviteمی‌باشد. در شکل زیر این دسته‌بندی نشان داده شده است.



شکل (۳-۱) دسته بندی حملات در معماری IMS

حملـه‌هـای مسـتقل از زمـان نظیـر attackSQL injection, Tear-Down, modification attack, cancel نیز می‌باشند. در ادامه، حملات وابسته به زمان بررسـی شـده و سـپس حمـلات مسـتقل از زمان بررسی می‌شود.

۳-۳-۲- حمله وابسته به زمان

این حمله با ارسال بیش از اندازه یک پیام خـاص، بـه سـرورSIP و مشـغول نمـودن منـابع شـبکه بـرای‌پردازش این پیام‌ها ایجاد می‌شود و نمودی از حمله DOSمی‌باشد و توان پردازشی و محاسباتی سروررا مختل می‌نماید. سرورهای SIPنسبت به floodingبیشترین ضعف را دارد. ایجاد مکانیزم‌های‌امنیتی نباید تاخیر زیادی به سرور تحمیل نماید. تاخیر زیاد به معنـی ضـعیف‌تـر شـدن سـرور در مقابـل‌حملات DOSاز نوع floodingمی‌باشد. بنابراین پیاده‌سازی مکانیزم‌های امنیتی اضافه شده نباید زمان پردازش زیادی را به سیستم اضافه نمایند. در ادامه انواع حمله‌های DOSبررسی می‌شود.حملات DOSپهنای باند سیستم را اشغال می‌کند، زمان پردازش

اضافی به سیستم تحمیل می‌نماید وباعث می شود سیستم کارایی خود را از دست بدهد. حملات DOSبا هدف از بین بردن دسترس‌پذیربودن سرورها انجام می‌پذیرد. این کار با ارسال مداوم و پی در پی پیام‌های مجاز به سرور و مشغول‌نمودن آن و یا ارسال پیام‌های SIPبه همراه سرآیندهای malformedمی‌باشد. نوع اول حمله راfloodingنیز نام می‌برند که در بخش قبل بررسی شده است. منابعی که در حملهDOS مورد تهدیدواقع می‌شود شامل حافظه، پهنای باند و عملکردCPU می‌باشد. هر سرور SIPدرخواست را در بافر درونی خود کپی میکند تا آن را پردازش نماید. این موارد را در ادامه توضیح می‌دهیم:

حافظه: مقدار بافر و مشخصه‌های آن به حالت سرور) (state full, statelessبستگی دارد.در statelessبعد از شناسایی مقصد و ارسال پیام، بافر پاک می‌شود در حالی که در state fullداده‌های مربوط به ، sessionو یا transactionبه دلایل امنیتی و یا نیازمندیهای شبکه ذخیره ونگهداری میشود.

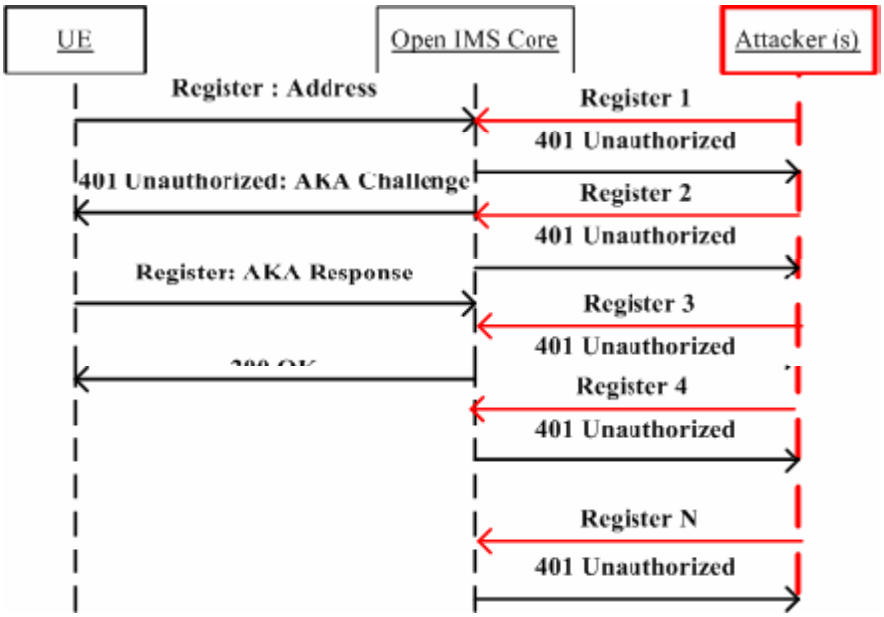
پهنای باند: با محدود شدن لینک‌های دسترسی به سرورها به دلیل افزایش درخواست های agentها،پیام‌های SIPاز بین خواهند رفت. و ممکن است زمانsetup time بیشتری لازم باشد. حفاظت از پهنای باند از مشخصه‌های لایه انتقال است و به SIPمربوط نمی‌باشد .

CPU: پس از دریافت پیام، توسطCPU پردازش می‌شود. و ارسال می‌شود. بسته به متن و نوع پیام وسیاست‌های سرور و مقدار واقعی ظرفیت ، CPUیک پردازش و مهندسی مناسب ضروری می‌باشد.متن SIPرمز نمی‌شود.به دلیل امکانات زیاد SIPهمانند عدم حساسیت به بزرگ و کوچک بودن‌حروف، اینترهای بین خطوط فواصل و خطوط اضافی حدود ۰۱ درصد ازCPU صرف پردازش وتجزیه پیام‌ها می‌شود. حملات DOSدر مکانیزم‌هایی که از احراز هویت خلاصه و مختصر استفاده‌نمودهاند، موفق‌تر عمل می‌نمایند. می‌توان از سرورهای چند پردازشگری نظیرSER۱ استفاده نمود.باعث حمله Brute force

attacks ارسال تعداد زیادی درخواست با from, to متفاوت به بافر سرورSIPمی‌شود. مکانیزم‌های اندازه‌گیری نظیر مونیتورینگ و فیلترینگ می‌تواند مفید باشد.

۳-۳-۲-۱- Register flooding attack

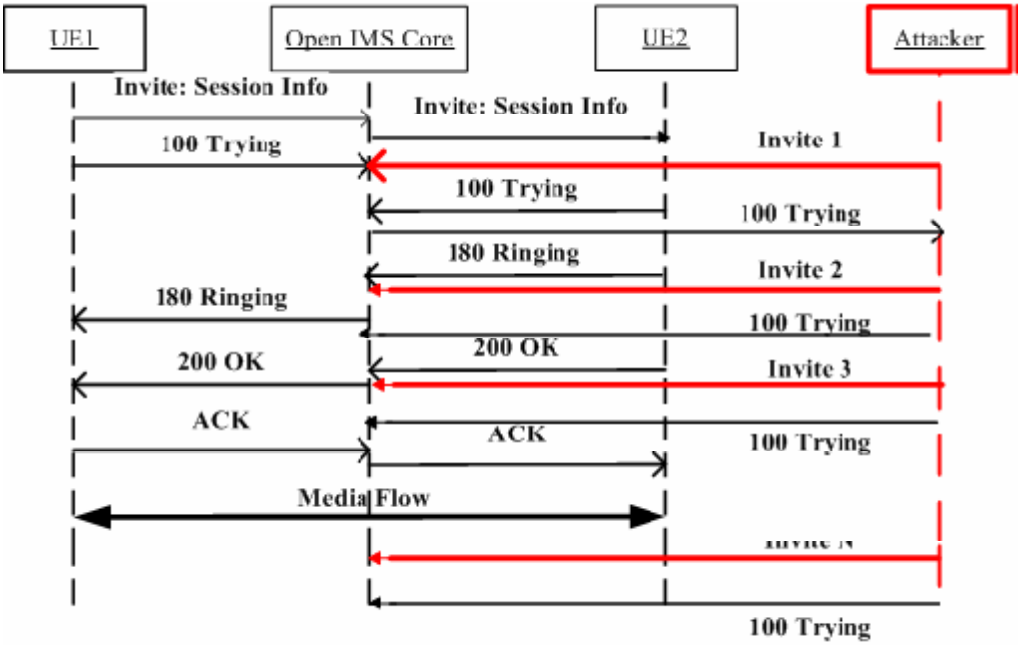
ارسال چندین درخواست registerبه پروکسی از طریق آدرس‌های SIP URI شنود شده و یا جعلی‌و مشغول نمودن آن به پاسخ‌های ۴۰۱unauthorizedاین حمله رخ می‌دهد. این حملـه منـابع IMSرا از کارایی دور ساخته و کاربران مجاز نمی‌توانند سرویس‌های مجاز را دریافت نمایند.



شکل (۳-۲) register flooding attack

Invite Flooding Attack -۲-۲-۳-۳

این حمله شبیه حمله قبل می‌باشد. با ارسال تعداد زیادی از درخواست‌هایSIP Invite به منظور ربودن‌نشست یک ارتباط عمل می‌نماید.



شکل (۳-۳)invite flooding attack

INVITE Response and REGISTER Response Flooding -۳-۲-۳-۳

در این حمله بر خلاف حملات گفته شده در قبل هدف وقفه در سرویس‌دهی هدف نیست بلکه‌هدف بدست آوردن اعتبارها و مشخصه‌های مربوطه از طریق قربانی است. اغلب پیام‌هایinvite به‌منظور دریافت و ربودن کلمه عبور برای احراز هویت می‌باشد. پیام‌هایregister ارسالی‌به‌پروکسیSIP برای دریافت اعتبارنامه و مشخصه‌های مربوطه می‌باشد در این بخش حملات مستقل از زمان تشریح می‌شود.

فصل چهارم:

روش مدلسازی TVRA

۴-۱- مقدمه

تحلیل و بررسی ریسک‌های یک سیستم، راه‌حلی برای ضمانت یک طراحی امن است که بابهره‌گیری از روش‌های استاندارد می‌توان طراحی مطمئن‌تری داشت. روش مدل‌سازیTVRA یک‌روش طراحی سیستمی۱، است که توسط ETSI TISPANبرای تحلیل تهدیدها، ریسک‌ها وآسیب‌پذیری‌ها در یک سیستم کامپیوتری ارایه شده است. این روش، مدل‌سازی و تحلیل ریسک قبل‌از سال۳۰۰۲ آغاز شده است و در استانداردهای مختلفی از جمله۱-۵۶۱ ۶۰۱ ،ETSI ۲۰۰ETSI ۷۸۱ TRو ETSI TR ۷۸۱ ۱۱۰به صورت رسمی و با کمک ارایه مثال‌هایی ارایه شده‌است. روشTVRA مدلی تعریف شده از سیستم را به همراه تحلیل آن به ارمغان می‌آورد که مدل‌بدست آمده بیانگر آسیب‌پذیری‌ها، ضعف‌ها و تهدیدهای آن سیستم است و می‌تواند توسط مدیرسیستم ویا طراح آن برای طراحی یک سیستم امن مورد استفاده قرار بگیرد. اطلاعات حاصل از این‌روش تحلیل ومدل‌سازی، در پیاده‌سازی یک سیستم کارا، با اقدامات پیشگیرانه در مقابل‌آسیب‌پذیری‌ها بسیار مفید خواهد بود. تحلیل آسیب‌پذیری‌های یک سیستم یکی از اطلاعاتی است‌که با بررسی طرح TVRAاز یک سیستم به دست می‌آید. در ،TVRAهفت مرحله مختلف‌جمع‌آوری، تحلیل و پردازش داده وجود دارد که در آن قدم به قدم مشخصه‌های مختلف یک سیستم‌بررسی می‌شوند تا آسیب‌پذیری‌ها، ریسک‌ها و حملات آن سیستم به دست آمده و احتمال اتفاقات‌مخرب در آن مشخص شوند و اقدامات پیشگیرانه از آن‌ها تعیین شود. نتایج این روش مدل‌سازی وتحلیل به عنوان ابزاری برای شناسایی پتانسیل ریسک‌های بالقوه موجود در سیستم‌ها که احتمال حمله‌در آن‌ها وجود دارد، به کار می‌رود. مدل به دست آمده از سیستم در یافتن مراحل پیشگیری ازآسیب‌پذیری‌ها، حملات و تهدیدها می‌تواند مورد بهره‌برداری واقع شود و طراحی سیستم را بهبود بخشد . اقدامات پیشگیرانه می‌توانند در طراحی‌های بعدی به عنوان نقاط ضعف جدید سیستم‌های‌قبلی در سیستم‌های جدید طراحی شده، مورد بازبینی و ارزیابی قرار گیرند. یکی از نقاط کلیدی درموفقیت این روش و سایر روش‌های طراحی سیستمی، توانایی در برقراری ارتباط بین اجزای

مختلف‌سیستم، نیازمندی‌های آن و اثر متقابل این دو بخش بر روی یکدیگر است. این مدل‌سازی ازسیستم‌های ارتباطی، دارای هفت مرحله زیر است (شکل۴-۱).

۱) تعیین اهداف امنیتی

۲) تعیین نیازمندی‌های امنیتی

۳) تعیین فهرست دارایی‌های منطقی و فیزیکی

۴) دسته‌بندی تهدیدها و آسیب‌پذیری‌ها

۵) کمی‌سازی تهدیدها و آسیب‌پذیری‌ها با هدف تعیین اولویت

۶) تعیین ریسک‌ها

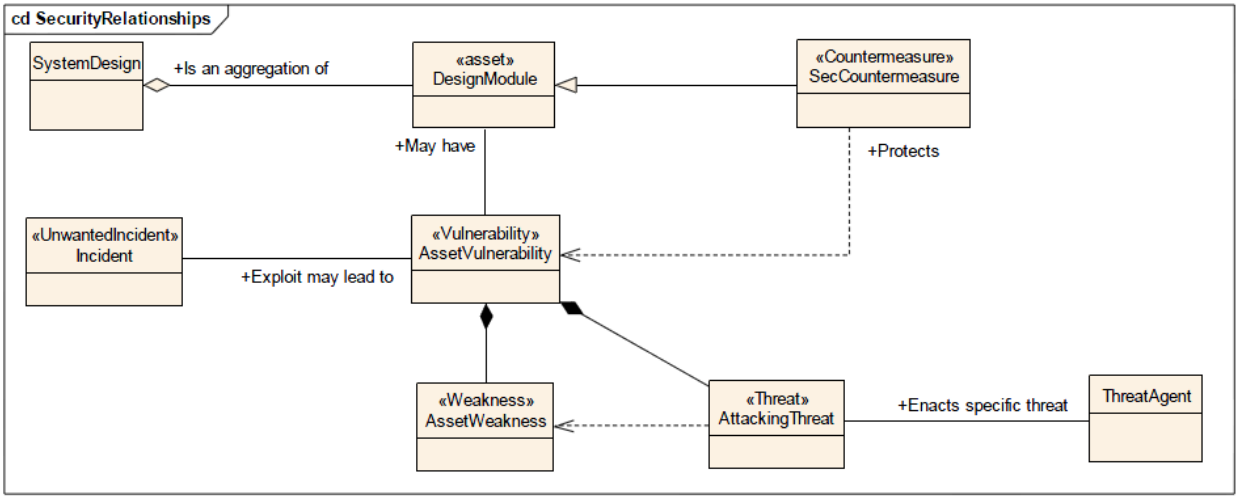
۷) تعیین اقدامات متقابل

شکل (۴-۱)

مدل پروتکل سیگنالینگSIP با استفاده از روشTVRA منجر به مشخص شدن آسیب‌پذیری‌هایSIPمی‌شود و توجه دادن طراحان در زمان پیاده‌سازی سیستم به این آسیب‌پذیری‌ها،می‌تواند به‌طراحی و پیاده‌سازی سرورهای SIPامن‌تر منجر شود. در ادامه این بخش، پس از معرفی و تشریح‌روش مدل‌سازی ،TVRAیک نمونه از مدل‌سازی این روش برای تحلیل آسیب‌پذیری‌ها آورده‌می‌شود و مراحل انجام مدل‌سازی با استفاده از TVRAدر تحلیل یک شبکه بررسی می‌شود.

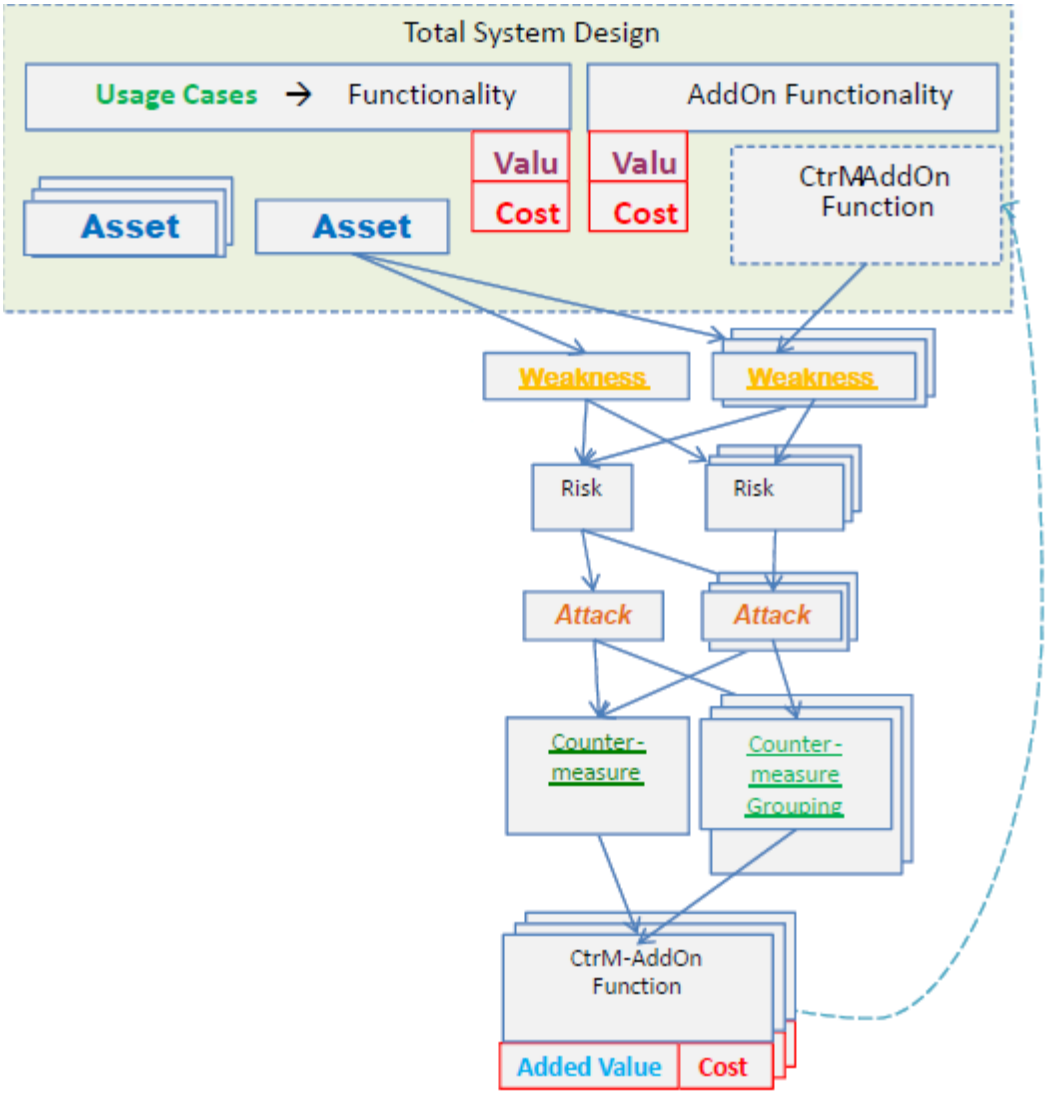
۴-۲- مراحل و چرخه مدل سازی TVRA

طراحی یک سیستم مشخصات سیستم در زمان پیاده‌سازی را نشان می‌دهد.مدل‌سازیTVRA ارتباط بین آسیب‌پذیری و دارایی سیستم، ارتباط بین نقاط ضعف، تهدیدها ومقیاس‌ها را به همراه تعیین ریسک‌ها در طراحی سیستمی نشان می‌دهد. در شکل زیر این ارتباط‌تعریف شده است. دسته‌بندی‌های موجود مدل‌سازی طبق آنچه در استاندارد ۵۶۱ ۲۰۱ ETSI TSآمده است، رابطه بین دارایی‌های سیستم، تهدیدها، ضعف‌ها،آسیب‌پذیری‌ها و اقدامات پیشگیرانه باطراحی سیستمی در شکل زیر نشان داده شده است



شکل (۴-۲) مدل امنیتی TVRA

طراحی سیستمی، مجموعه‌ای از دارایی‌هاست. دارایی‌های سیستم با آسیب‌پذیری‌ها ارتباط‌دارد و آسیب‌پذیری‌ها متشکل از ضعف‌ها و تهدیدهاست. اقدامات پیشگیرانه بخش خاص شده‌ای ازمجموعه دارایی‌هاست. اقدامات پیشگیرانه به آسیب‌پذیری‌های یک سیستم بستگی دارد. هدف ازطراحی سیستمی مناسب، کاهش هر چه بیشتر حوادث ناخواسته در زمان پیاده‌سازی است. در طراحی‌هر سیستم از تعداد خاصی از کاربردها و توابع پشتیبانی می‌شود. هر کدام از این کاربردها و توابع‌دارای یک ارزش و یک هزینه برای کاربر و یا برای شبکه هستند. همچنین هر سیستم دارای ارزش‌هاو دارایی‌های خاصی است. هر ارزش و دارایی نیز دارای ضعف‌هایی هستند که ممکن است توسطیک تهدید مورد حمله قرار بگیرند. هر یک از ضعف‌هایسیستم به صورت یک یا چند ریسک نمایان‌می‌شوند. هر ریسک اجازه یک یا چند حمله را به مهاجم می‌دهد که منجر به آسیب‌رسانی و واردکردن هزینه جبران به سیستم می‌شود. هر حمله را می‌توان از طریق یک اقدام متقابل و پیشگیرانه۱ سدنمود تا از آسیب‌پذیر بودن سیستم از طریق یک ضعف جلوگیری نمود. به طور کلی در طراحی‌سیستم تلاش می‌کنیم تا با انجام اقدامات پیشگیرانه، ریسک‌های سیستم را کاهش دهیم . اقدامات‌پیشگیرانه شامل طراحی دوباره دارایی‌های سیستم و یا ارتقای امنیتی آن‌ها می‌باشد.



شکل (۴-۳) مراحل مدلسازی TVRA

هر اقدام متقابل نیازمند یک یا چند تابع برای پیاده‌سازی می‌باشد. هر تابع که به این منظورپیاده‌سازی‌می‌شود خود یک ارزش و دارایی در سیستم محسوب می‌شود و می‌بایست دوباره در طراحی سیستم‌درنظر گرفته شود. زیرا ممکن است یک آسیب‌پذیری جدید به سیستم اضافه نماید . به این ترتیب‌طراحی یک سیستم، بهینه خواهد شد و مدل‌سازی دوباره تکرار می‌شود تا از ارزش‌های ایجاد شده‌جدید در مقابل آسیب‌پذیری‌های جدید حفاظت نماید و این چرخه تا زمانی که تمام ریسک‌های‌سیستم حذف شود، ادامه خواهد یافت. این چرخه‌ای است که یک مدل‌سازی TVRAطی می‌نماید تایک سیستم بهینه را تحویل دهد. در نتیجه این چرخه، مقدار ریسک‌های ارزش‌ها اندازه‌گیری می‌شودو نیازمندی‌هایی تعیین می‌شوند تا مقدار

ریسک‌ها را کاهش دهند . لازم به ذکر است که‌آسیب‌پذیری‌ها با ضعف‌ها تفاوت‌هایی دارند. مجموعه‌ای از ضعف‌ها که می‌تواند توسط مهاجم‌مورد تهدید قرار گیرد را آسیب‌پذیری می‌نامیم. در ادامه روش مدل‌سازیTVRA و مراحل آن طبق آنچه در منابع ۲۰۰ ۷۸۱ ETSI TR آمده است، بررسی و معرفی خواهد شد.

۴-۳- مراحل طراحی سیستم از طریق مد لسازی TVRA

مدل‌سازی یک سیستم به منظور استفاده از نتایج آن در زمان طراحی سیستم و برای‌کاهش‌آسیب‌پذیری‌ها و افزایش مقاومت سیستم در برابر حوادث ناخواسته در زمان پیاده‌سازی موثر است. دراین بخش مراحل مدل‌سازی و بخش‌های موجود در آنرا بررسی می‌نماییم.

۴-۳-۱-تعیین اهداف امنیتی

اولین مرحله از مدل‌سازیTVRA تعیین اهداف و مقصود نهایی از طراحی سیستمی می‌باشد. اهدافامنیتی، مشخصه‌هایی تعیین شده از سیستم به منظور محافظت از اطلاعات انتقالی، دریافتی و یا ذخیره‌شده می‌باشد. هدف و اجزای امنیتی یک سیستم باید به صورت دقیق تعریف و تعیین شده باشد.استفاده از این اهداف و اجزای امنیتی در مراحل بعدی مدل‌سازی، به منظور به‌دست آمدن نقاط‌ضعف و تهدیدهای سیستم مفید هستند. اهداف امنیتی در طول مدل‌سازی قابل تغییر نیست و این‌مرحله مبنای تحلیل آسیب‌پذیری‌های یک سیستم می‌باشد. نمونه اهداف امنیتی طبق‌استاندارد۵۶۱ ۲۰۱ TSشامل محرمانگی، یکپارچگی، حسابرسی ، دسترس‌پذیری واحرازهویت‌تعیین شده است. اهداف امنیتی در طول طراحی یک سیستم ثابت است و تغییر نمی‌کند و بالاترین‌سطح نیازمندی‌های طراحی سیستم در

تعیین اقدامات پیشگیرانه در کاهش ریسک‌ها می‌باشد .این اهداف امنیتی در هر سطح دارای مشخصه‌ها و تعریف‌های جداگانه‌ای هستند که دراستاندارد۵۰۸. ITU-T Xتشریح شده است . به عنوان مثال احراز هویت و شناسایی یک کاربر قبل‌از سرویس‌دهی توسط شبکه یکی از الزامات و اهداف امنیتی طراحی سیستمی می‌باشد. یک کاربرغیر مجاز شبکه نمی‌تواند خود را به عنوان یک کاربر مجاز معرفی نماید. این کاربر نمی‌تواند امکانات‌شبکه را مورد استفاده قرار داده و از سرویس‌ها و کاربردهای آن استفاده نماید. تعیین صحت و احرازهویت یک کاربر با استفاده از شناسه‌های منحصر به فردی که برای کاربران تعریف می‌شود، انجام‌می‌شود. این شناسه و همچنین روش احراز هویت یک کاربر در هر شبکه و سیستم روش‌های متفاوتی‌دارد.

۴-۳-۲- تعیین نیازمندی های امنیتی

نیازمندی‌های تعریف شده در این مرحله از مدل‌سازیبر اساس اهداف امنیتی تعریف شده در مرحله‌قبل تعیین می‌شود. نیازمندی‌های امنیتی اقدامات و بلوک‌هایی است که نشان می‌دهد کدام هدف امنیتی به دست خواهد آمد.

۴-۳-۳- تعیین سرمایه ها و دارایی های سیستم

هر سیستم دارای سرمایه‌ها و ارزش‌هایی است که از آن محافظت می‌شود. مشخصه هر دارایی شامل‌نوع دارایی (فیزیکی، منطقی، انسانی)، نوع فناوری، سطح داده‌های مرتبط با فناوری، زمان و طول‌دوره معتبر بودن آن دارایی می‌باشد. در مدل نمودن یک سیستم فرض بر آن است که تمام دارایی‌های‌سیستم دارای ضعف باشند . یک دارایی،مادامی‌که نقطه ضعفی دارد و احتمال حمله به آن وجوددارد، در معرض خطر یا ریسک قرار دارد. اهمیت یک آسیب‌پذیری منوط به مقدار سطح ارزش ودارایی و احتمال استفاده از ضعف برای حمله دارد. هر چه ضعف یک سیستم در معرض حمله بیشتری‌باشد، آن ضعف سیستم، آسیب‌پذیری پر

اهمیت‌تری تلقی می‌شود. هر دارایی در یک سیستم، یک‌سطح اهمیتی دارد که احتمال وقوع حملات بر روی آن‌ها متفاوت است. شدت وقوع حملات به سه‌سطح(۱-۲-۳) شامل پایین، متوسط و بالا در تقسیم‌بندی شده است. آنطورکه‌دراین‌روش‌مدل‌سازی عنوان شده است، ارتباط بین ارزش‌ها می‌تواند یک ارتباط چندگانه باشد و یک ارزش و دارایی به چندین دارایی دیگر وابسته باشد.

مقدار	شدت	توضیحات
۱	پایین (Low)	صدمه و خسارت مختصر و ناچیزی از حمله به هدف بوجود آمده است.
۲	متوسط (Medium)	صدمه و خسارت وارد شده به کاربر یا شبکه نمی‌تواند نادیده گرفته شود.
۳	بالا (High)	صدمه به هدف موردنظر شدید است و اساس فعالیت، آسیب شدید دیده است.

جدول (۴-۱) شدت حمله

۴-۳-۴- دسته بندی آسیب پذیری ها و تهدیدها

بررسی و تحقیق دقیق سیستم، یک سری از ضعف‌های امنیتی را در آن مشخص می‌نماید.زمانی که مهاجم بتواند از آن ضعف‌ها سوء استفاده نماید و حمله‌ای به سیستم انجام پذیرد،سیستم درآن بخش آسیب‌پذیر است. به ازای هر ضعف موجود در سرمایه‌های سیستم، احتمال یک حمله وجوددارد. از جمع مولفه‌های این جدول، مقدار پتانسیل حمله به دست می‌آید. مولفه‌های توصیف یک تهدید و آسیب‌پذیری شامل زمان- تجربه- دانش و ابزار می‌باشد.

۴-۳-۵- تعیین ریسک ها

شناسایی یک حمله می‌تواند یک عامل در شناسایی ریسک سیستم و یا شناسایی ارزش‌های موردتهدید حملات باشد. تحلیل ریسک‌های سیستم، نشان می‌دهد کدام یک از تهدیدهای بررسی شده دربخش آسیب‌پذیری‌ها و حملات ممکن و اجرایی می‌باشد. وزندهی به ریسک‌ها و شناسایی وکمینه‌کردن احتمال هر تهدید موفق می‌تواند فعالیت‌های مربوطبه این مرحله از مدل‌سازی باشد. دراین مرحله مرجع پتانسیل وقوع هر کدام از تهدیدهایبیان شده در بخش تحلیل ریسک درمدل‌سازی را تعریف می‌نماید. به این معنی که هر چه مقدار پتانسیل وقوع حمله بالاتر باشد،تهدیدمربوطه خطرناک‌تر است. در زیر نمونه‌ای از تحلیل‌هایمورد بحث در این مرجع که به کمینه‌سازی‌پتانسیل تهدید وقفه در سرویس‌دهی کمک می‌کند، آورده شده است. در این بخش، حمله وقفه درسرویس‌دهی، مهاجم دسترس‌پذیری یک سیستم را مختل می‌کند تا کاربران به بخش‌های مجازسیستم و سرویس‌های آن دسترسی نداشته باشند. روش TVRAمقادیر متفاوت را به سطوح متفاوت زیر مرتبط می‌نماید.

۱- مقدار ۰: یک نمونه از حمله مشاهده شده هاست.

۲- مقدار۱: نمونه حمله ای باشد توسط میانه مشاهده شده است.

۳- مقدار۲: نمونه حمله ای باشد تا بالا مشاهده شده است.

استفاده از این مقادیر و مقادیر پایین، متوسط و بالای بدست آمده برای ارزش‌ها درمرحله احتمال‌وقوع(مرحله۳)، مقادیر شاخصی را به عنوان معرف حملات مشخص می‌نماید.مقادیر این جدول و احتمال وقوع(مرحله ۳)یک مقیاس برای اندازه‌گیری ریسک‌پذیری ارزش‌ها تعیین می‌نماید. ارزش‌هایی که مورد حمله واقع می‌شوند، دارای ریسک‌های متفاوتی هستند.

۴-۳-۶- تعیین تمهیدات امنیتی

اقدامات امنیتی دارایی‌هایی هستند که به یک سیستم به منظور کاهش ریسک اضافه می‌شوند. هدف‌اقدامات امنیتی، کاهش احتمال حملات و کاهش وقوع حمله می‌باشد. اقدامات امنیتی معمولا به‌صورت تغییرات درونی در یک سیستم استاندارد معرفی می‌شود. روش TVRAریسک‌های امنیتی رامشخص می‌نماید اما نمی‌تواند به صورت اتوماتیک اقدامات امنیتی را تعیین نماید. این عمل نیازمندتجربه و نظارت بر روی سیستم نیز می‌باشد. اقدامات پیشگیرانه می‌توانند در طراحی‌های بعدی به‌عنوان نقاط ضعف جدید در سیستم مورد بازبینی و ارزیابی قرا گیرند. مکان پیاده‌سازی اقدامات امنیتی می‌تواند در هر جای سیستم باشد. اقدامات امنیتی می‌توان در یک استاندارد دیگر منتشر گردد.

۴-۳-۷- کمی سازی تهدیدها برای اولویت بندی

پس از تعیین تهدیدها و ریسک‌های سیستم، دسته‌بندی و اولویت‌بندی اقدامات امنیتی بر اساس اهمیت‌تهدیدها بررسی می‌شود. این اولویت‌بندی از طریق کمی‌سازی تهدیدها بر اساس مقدار خسارت آن‌ها به سیستم انجام می‌شود. تهدیدهای با آسیب بالا به سیستم جزو تهدیدهای اصلی سیستم قرار می‌گیرندو اقدامات امنیتی مقابله با آن‌ها در دسته‌بندی اقدامات امنیتی جزو اقدامات اولیه و اساسی خواهد بود.

۴-۴- نتیجه گیری و فعالیتهای آتی مدلسازی سرور پروکسی SIP در چارچوب IMS

در ایـن پـژوهش مـدلی از آسـیب‌پـذیری‌هـای سیسـتم سـرورهایSIP بـا توجـه بـه اسـتاندارد مدل‌سازیTVRA تشریح شد.

۴-۴-۱- نتیجه گیری

پیدا کردن یک دسته‌بندی کلی بـرای تمـام آسـیب‌پـذیری‌هـای سـرورهایSIP بـه صـورتی کـه تمـام‌حملات اشاره شده در مقالات متنوع را شامل شود، کار دشواری است. به صورت کلی حملات به دودسته مستقل از زمـان و وابسـته بـه زمـان تقسـیم مـی‌شـوند. حمـلات وابسـته بـه زمـان نظیـر حمـلاتflooding‌است که شامل register, register response, Invite Response است. حمـلات مسـتقل‌از زمان حملاتی که نیازمند گذشتن زمان خاصی بـرای پدیـد آمـدن نتیجـه نیسـتند. مثـال‌هـایی ازایـن‌حملات نظیر حملات تغییر محتـوای یـک پیـام ارسـالی SQL injectionو یـا حمـلات ارسـال پیـام‌بی‌موقع نظیرCancel, Bye, Re-Inviteمی‌باشـد. هـر کـدام از ایـن حمـلات، یکـی ازدارایـی‌هـای‌موجود سرور SIPدر شبکهIMS را مورد تهدید قرار می‌دهند.ثبت‌نام کاربر در شبکهIMS اجباری است و تمام درخواست‌های ارسالی باید احـراز هویـت شـوند. بـا احراز هویت تمام درخواست‌های ارسال شدهSIP به ،S-CSCFترافیک reference pointبـه نـامCxکه واسط بین S-CSCFو HSSمی‌باشد افزایش چشمگیری می‌یابد. این در حالی است کـه‌مـی‌دانـیم‌بالاترین زمان پردازش در پروکسی ،SIPاختصاص به پیامهایinvite, register دارد، به این ترتیب بـااحراز هویت تمام درخواست‌ها تعداد درخواست‌های پردازش شـده توسـط پروکسـی SIPبـه میـزان۷۵٪-۰۷٪ کاهش می‌یابد.یکی از روش‌های ارتقای امنیت سرورSIP در ،IMSاستفاده از IPsecاسـت کـه دشـوار و پرزحمـت‌است زیرا منجر به تحمیل سربار اضافی به دلیل رمزنگاری به روشIPsec-ESP می‌شود. در حـالی کـه‌امن نمودن با روشTLSسربار کمتری نسبت بهIPsec ایجاد می‌کند و از الگـوریتمPKI بهـره

مـی‌بـرد.بنابراین TLS به ترIPsec و باید از TCPبرای انتقال استفاده شود.نقطه ضعف دیگر پروکسی SIP، امکان انتخاب روش‌های احراز هویت ضعیف در ارتباط کـاربرSIP با شبکهIMS است. یک مهاجم می‌توانـد بـا حـذف هـدر Authorizationاز پیـام registrationکاربر، پروکسی P-CSCFشبکه را مجبور به ایجاد ارتباط حتی بـدون رمزنگـاری در شـبکه نمایـد. بـاحذف این هدر شـبکه روش احـراز هویـتearly IMS authentication را انتخـاب مـی‌نمایـد. بـدین‌ترتیب تهدید معادل با این نقطه ضعف در زمانی که عملـی شـود یـک آسـیب‌پـذیری را بـه پروکسـی تحمیل می‌نماید و منجر به شنود پیامهای ارسالی و از بین رفتن محرمانگی در ارتباط خواهد شد.

۴-۴-۲- فعالیتهای آتی :

پس از مدل سازی و آسیب‌پذیری‌های سیسـتم سـرورهای SIP، مـدل‌سـازی مراحـلTVRA از طریـق‌برنامهUMLمی‌توانـد مرحلـه بعـدی پـژوهش باشـد. بـرای بدسـت‌آمـدن ، use case viewاسـتفادهازدیاگرام‌های UMLنظیر ،use case diagrams class diagramsوobject diagrams منجر به تحلیـل‌سیستم برای شناسایی دارایی‌های آن می‌شـود. ایـن شناسـایی در تعریـف فهرسـت عملیـاتی تمهیـداتامنیتی موثر است. از جمله فعالیت هـای قابـل انجـام در ادامـه ایـن پـژوهش ادغـام مراحـل TVRAبـامدل‌سازی با دیاگرام‌های UMLمی باشد که دیاگرامهای تعریف شده،محدوده روشنی از چالش‌ها درپیاده‌سازی سرورهای سه‌گانهSIP در IMSرا به ارمغان خواهد آورد.

مراجع

[۱]ETSI TS 102 165-1, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis,2006

[۲]ETSI TR 187 002, Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) Threat and Risk Analysis, 2010

[۳]GPP TS 23.228, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS);Stage 2 (Release 10)

[۴]K. Chalamalsetty, " Architecture for IMS Security to Mobile: Focusing on Artificial Immune System and Mobile Agents Integration", Master thesis, School of Computing Blekinge Institute of Technology, Sweden, 2009

[۵]D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, H. Schulzrinne, SIP Security, published by Jhon Wiley,2009

[۶]J. Rosenberg, H. Schulzrinne," Reliability of Provisional Responses in Session Initiation Protocol (SIP)" IETF Request for Comments (RFC) 3262, 2002

[۷]T. Russell, The IP Multimedia Subsystem (IMS) Session Control & Other Network Operations، published by Mc Graw Hill,2008