ملزومات امنیتی پیاده‌سازی IMS SIP سرور امن

افسانه معدنی و نسرین تاج
پژوهشگاه ارتباطات و فناوری اطلاعات- تهران- ایران

چکیده

شبکه IMS توسط ETSI به‌عنوان هستهٔ شبکه‌های نسل آینده تعیین شده است. ساختار هسته این شبکه از دید پیام‌های کنترلی و پروتکل‌های ارتباطی باعث شده امنیت به‌عنوان یک قابلیت ضروری برای نیازمندی‌های آن درآید. پیام‌های کنترلی این شبکه توسط پروتکل SIP منتقل می‌شود که یک پروتکل لایهٔ کاربرد است. به‌دلیل اجباری‌بودن احراز هویت کاربر در زمان ثبت‌نام و به‌دلیل اضافه‌شدن سرآیندهای سیگنالینگ، این شبکه امن‌تر از شبکه‌های رایجی نظیر VOIP است، هرچند آسیب‌پذیری‌های متفاوتی اضافه شده است که منجر به حملات بر روی سرورها می‌شود. این پژوهش بررسی بر روی سرورهای اصلی (x-CSCF) این شبکه را مبتنی بر تهدید، آسیب‌پذیری و تحلیل اثر حمله بر دسترس‌پذیری و محرمانگی انجام می‌دهد. این کار با استفاده از یک روش تحلیل آسیب‌پذیری (TVRA) انجام شده است که مبتنی بر احتمال وقوع حمله و آسیب ناشی از آن است. تهدید به‌دلیل وجود ضعف ایجاد شده و سبب آسیب می‌شود. پس از شناخت سرمایه‌های سامانه، نقاط ضعف‌ها و آسیب‌پذیری تجهیزات و کاربردها، شاخص‌های امنیتی به‌دست می‌آید که در تولید و پیاده‌سازی امن سرورها حایز اهمیت هستند و سبب کاهش هزینه و ارتقای امنیت است. مدل‌سازی از طریق تعریف و یافتن تابعی با متغیرهای (سرمایه منطقی/ نقطه ضعف/ موقعیت/ تهدید و حمله/ هدف امنیتی نقض شده) انجام شد که ارتباط این متغیرها تمهیدات پیش‌گیرانه امنیتی را روشن کرد. حملات رایج سرورها براساس مدل‌سازی گروه‌بندی و به‌ترتیب فراوانی وقوع در جدول مرتب شد. نتایج مدل‌سازی نشان می‌دهد که مهم‌ترین روش‌های سیگنالینگ شامل روش دعوت و ثبت نام هستند که نقش اساسی در رخ‌دادن حملات سیلاب‌سازی و نقض دسترسی دارند و رمزنگاری ارتباط سرور P-CSCF (مهم‌ترین سرور ارتباطی با کاربر) جلوی بسیاری از حملات ناشی از شنود را می‌گیرد. از بین سرورهای سه‌گانه SIP، این سرور نقش کلیدی در ارتقای امنیت و کاهش زمان پردازش در ارتباط‌ها را بر عهده دارد.

واژگان کلیدی: مدل‌سازی امنیتی TVRA ، حملات سیلاب‌سازی سرورهای IMS SIP، معماری و شبکه IMS، تحلیل آسیب‌پذیری.

۱ – مقدّمه

شبکهٔ IMS با معماری مبتنی بر IP و براساس استانداردهای مؤسسه 3GPP در شبکه‌های سلولی به‌عنوان هسته شبکه‌های نسل آینده مدنظر قرار میگیرد. این شبکه سیگنالینگ SIP[1] را برای کنترل ارتباطات کاربر تا شبکه، بین نودهای سرویس شبکه و سرورها و پروکسی‌ها انتخاب کرده است. در این شبکه با توجه به الزامی‌بودن ثبت‌نام کاربران و اضافه‌شدن برخی سرآیندها به این سیگنالینگ، حملاتی متفاوت از شبکهٔ صوت مبتنی بر IP (VOIP) رخ می‌دهد که منجر به آسیب‌پذیری‌ها در سرورهای SIP می‌شود. یکی از روش‌های تحلیل آسیب‌پذیری‌های سامانه‌ها به‌منظور ارتقای امنیتی آن‌ها مدل‌سازی سامانه از طریق روش‌های مدل‌سازی موجود است. امروزه روش‌های استاندارد ارزیابی امنیت سامانه به‌دلیل اهمیت حفاظت از دارایی سامانه‌ها به‌وجود آمده است. هر چند از جنبهٔ نحوهٔ مدل‌سازی تفاوت‌هایی بین روش‌ها وجود دارد، اما هدف، کاهش هزینهٔ تخریب، از طریق تشخیص تهدید و تحلیل

[1] Session Initiation Protocol

آسیب‌پذیری و نفوذ به سامانه است. مدل‌ها و ارزیابی‌های امنیتی پیشنهادهایی را در حفاظت از محرمانگی، یکپارچگی و دسترس‌پذیری دارایی سامانه ارایه می‌دهد. پیشنهاد حفاظتی نباید در عملکرد سامانه پایه از دید سرعت و کارایی خللی ایجاد کند؛ ضمن این‌که منجر به ارتقای امنیتی آن شود. تا زمانی که ضعف‌ها مورد تهدید قرار نگیرند، مشکلی نیست. زمانی که تهدید براساس نقاط ضعف عملی شد، سامانه آسیب‌پذیر می‌شود).

(TS23.228,2014 مدل‌سازی امنیتی TVRA[1] فرآیند ارزیابی را پیشنهاد می‌دهد که نتایج آن در انتخاب طراحی و پیاده‌سازی بهینه مؤثر است (TS 24.229,2010). با توجه به مقدمهٔ گفته شده، در این پژوهش تلاش شده است رفتار سرورهای سه‌گانه SIP با هدف شناسایی نقاط ضعف امنیتی آن در IMS از طریق یک روش مدل‌سازی استاندارد مدل شود. این پروتکل برای ایجاد، کنترل، تغییر یا پایان نشست کاربر شبکه استفاده می‌شود.

گروه‌بندی کلی آسیب‌پذیری سرور از طریق مدل استاندارد به‌صورتی که تمام حملات اشاره شده در مقالات متنوع را شامل شود و ارتقای امنیت، کاهش هزینه و بهبود عملکرد را به دنبال داشته باشد، کار دشواری است. به همین دلیل، یک مطالعهٔ جامع برای مدل امنیتی رفتار پروتکل و سد حملات به‌ترتیب اهمیت و آسیب‌زابودن ضروری است. بنابراین بررسی منابع با هدف یافتن آسیب‌پذیری، حملات رایج و تهدیدهای سرورها شروع شد. طبق آنچه به‌دست آمد، اکثر فعالیت‌های انجام‌شده در این حوزه در جهت یافتن حملات رایج و اجرای سازوکار پیشگیری از حمله به‌منظور ارتقای امنیت بوده است. مدل‌کردن جامع سرور مستلزم همسان‌سازی، تحلیل روش‌ها و یافتن رویکرد جامع تنظیمات است. هر کدام از مقاله‌ها بخشی از حملات را بررسی کرده و راه حلی ارایه داده است که گوشه‌ای از متغیرهای امنیتی مؤثر را روشن کرده است که نمونه کارهای مشابه در بخش دو تشریح می‌شود.

در بخش سه معرفی مدل‌سازی TVRA، در بخش چهار مدل‌سازی سرور IMS SIP به همراه مراحل آن در زیربخش‌ها تشریح می‌شود. در انتهای هر زیربخش موارد مرتبط به‌دست آمده از مدل‌سازی به همراه نتایج آن در جدول‌های مربوطه به تفکیک مراحل قابل مشاهده است. در بخش چهار نتیجه‌گیری و جدول نهایی تابع مدل‌سازی آمده است.

۲- مروری بر کارهای مشابه

در مرجع (TS 33.203,2014)عملکرد سرور در مقابل حملات سیلاب‌سازی[2] و سد سرویس[3] از طریق اضافه‌کردن سازوکار اولویت‌بندی بهبود یافته است. تغییر اولویت در بررسی پیام دریافت شده، زمان پردازش پیام را در زمان حمله سیلاب‌سازی کاهش می‌دهد. سازوکار اولویت‌بندی شامل احراز هویت دو پیام دعوت[4] و ثبت‌نام[5] کاربر ناشناس؛ حذف درخواست کاربر ناشناس به‌جز درخواست‌های دعوت یا ثبت نام و رسیدن به عملکرد تا ۸۶٪ بالاتر به‌دلیل بررسی درخواست کاربر آشنا در صفی جدا از کاربر ناشناس از نتایج این اولویت‌بندی بوده است. این مرجع هرچند نگاشتی بین تهدید سرور SIP و راه حل را نشان می‌دهد؛ اما مدل ارایه شده از پروتکل، بدون استفاده از استاندارد و تنها با مقایسه تأثیر حمله به‌دست آمده است.

در مرجع(TS 33.978,2008) با استفاده از منطق فازی و شبیه‌سازی محیط آزمایش پروتکل در شبکهٔ IMS، مقاومت سرور در مقابل حملات رایج بررسی شده است. جدول نتایج نشان می‌دهد حمله سیلاب‌سازی "ثبت نام" بیش‌ترین عاملی است که منجر به قطع خدمات سرورها (سد خدمات) است و اثر مخرب بالاتری در مقایسه با حمله سیلاب‌ساز "دعوت" دارد.

مدل‌سازی کلّی شبکه IMS در مقاله(Ahmad B,2012) یکی از کارهای موفق است که تحلیلی جامع از آسیب‌پذیری‌های این شبکه ارائه داده است. در این مرجع بردار آسیب‌پذیری با مؤلفه‌های آن معرفی می‌شود که تابعی از سرمایه، تهدید، موقعیت، اهداف امنیتی و حوادث ناخواسته است. نتایج به‌دست آمده نشان می‌دهد که احراز هویت ضعیف و عدم وجود محرمانگی از مهم‌ترین ضعف‌های این شبکه است و روش احراز هویت HTTP با وجود دقت کم‌تر از روش IMS AKA[6]، به‌دلیل سرعت بالاتر مورد استفاده بیشتری دارد (Ahmad B,2012). نمونه‌های دیگری از مدل‌سازی مؤلفه‌ها و سرویس‌های

[1] Threat, Vulnerability and Risk Analysis

[2] Flooding
[3] Denial Of Service
[4] Invite
[5] Register
[6] IMS Authentication Key Agreement

شبکهٔ نسل آینده به روش TVRA در مراجع(Bremler-Bar. A,2006) و(Denver D,2011) وجود دارد.

۳- معرفی مدل‌سازی TVRA

استانداردسازی این روش، قبل از ۲۰۰۳ آغاز و در نگارش‌های ETSI 102 165-1، ETSI TR 187 002 و ETSI TR 187 011 به‌طور رسمی ارایه شد. این مدل‌سازی یک روش طراحی سامانه‌ای در تحلیل آسیب‌پذیری سرمایه‌ها، تهدید امنیت و نقاط ضعف است که مدلی تعریف‌شده از سامانه را به همراه تحلیل آن به ارمغان می‌آورد و بیان‌گر آسیب‌پذیری، ضعف و تهدید سامانه است و در هفت مرحله روشن می‌شود.

۱) تعیین اهداف امنیتی
۲) تعیین نیازمندی‌های سامانه
۳) تعیین فهرست دارایی‌ها
۴) گروه‌بندی تهدید و آسیب پذیری‌ها
۵) کمی‌سازی تهدید برای اولویت‌بندی
۶) تعیین مخاطره
۷) تعیین تمهیدات پیش‌گیرانه

مدل به‌دست آمده با یافتن مراحل پیش‌گیری از حمله و تهدید، طراحی را بهبود می‌بخشد (TS23.228,2014). یکی از نقاط کلیدی در موفقیت این روش، توانایی در برقراری ارتباط بین اجزای مختلف سامانه و نیازمندی‌ها و اثر متقابل این دو بر هم است. در طراحی هر سامانه از تعداد خاصی از کاربردها و توابع پشتیبانی می‌شود. هر کدام از این کاربردها و توابع دارای یک ارزش و یک هزینه برای کاربر یا شبکه است. همچنین هر سامانه دارای ارزش و دارایی‌های خاصی است. هر ارزش نیز ضعفی دارد که ممکن است توسط یک تهدید مورد حمله قرار بگیرد. هر یک از ضعف‌های سامانه به‌صورت یک یا چند مخاطره نمایان می‌شوند. هر مخاطره اجازه یک یا چند حمله را به مهاجم می‌دهد که منجر به آسیب‌رسانی و واردکردن هزینه به سامانه می‌شود. هر حمله را می‌توان از طریق یک اقدام پیش‌گیرانه سد کرد تا از آسیب‌پذیربودن سامانه از آن ضعف جلوگیری کرد. انجام تمهیدات پیش‌گیرانه، مخاطرهٔ سامانه را کاهش می‌دهد و نیازمند یک یا چند تابع برای پیاده‌سازی است. هر تابع که به این منظور پیاده‌سازی می‌شود، خود یک ارزش و دارایی سامانه محسوب می‌شود و می‌بایست دوباره در طراحی لحاظ شود. زیرا ممکن است یک آسیب‌پذیری جدید به سامانه اضافه کند(TS23.228,2014). به این ترتیب طراحی یک سامانه، بهینه خواهد شد و مدل‌سازی تکرار می‌شود تا از ارزش‌های ایجادشدهٔ جدید در مقابل آسیب‌پذیری‌های جدید حفاظت کند و این چرخه تا زمانی که تمام مخاطرات سامانه حذف شود، ادامه می‌یابد. در نتیجه، مقدار مخاطرات ارزش‌ها اندازه‌گیری می‌شود و نیازمندی‌هایی تعیین می‌شود تا مقدار مخاطرات را کاهش دهد و سامانه بهینه تحویل شود(TS23.228,2014). لازم به ذکر است که آسیب‌پذیری‌ها با ضعف‌ها تفاوت‌هایی دارد. مجموعه‌ای از ضعف‌ها را که می‌تواند توسط مهاجم برای حمله استفاده شود، آسیب‌پذیری می‌نامیم.

۴- مدل‌سازی سرور IMS SIP

در روش مدل‌سازی TVRA، مدل‌سازی امنیتی سامانه‌ها در هفت گام پیشنهاد شده است که براساس نیاز و نوع کاربرد، تعدادی از گام‌ها را می‌توان با یکدیگر ترکیب و یا حذف کرد. در این مقاله مدل‌سازی با گام‌های اصلی و با هدف تحلیل جامع آسیب‌پذیری سرور تهیه شده است که هر کدام از زیربخش‌های این مرحله به تشریح ستونی از جدول (۴-۴) (جدول نهایی مدل‌سازی) می‌پردازد که در انتهای بخش به‌صورت کامل درج شده است. آسیب‌پذیری‌ها در پروتکل به‌صورت تابعی با مؤلفه‌های زیر نوشته می‌شود:

(سرمایه منطقی/ نقطه ضعف/ موقعیت/ تهدید و حمله/ هدف امنیتی نقض شده)

نتیجهٔ ارتباط متغیرهای این تابع منجر به یافتن و تشخیص تمهیدات امنیتی پیش‌گیرانه می‌شود. این تابع از طریق تعریف مدل‌سازی و با اجرای مراحل چندگانه مدل‌سازی سرورها به‌دست آمده است. متغیرهایی که تابع مدل‌سازی به آن وابسته می‌باشد، از درون مراحل زیر به‌دست آمده است.

۴-۱ مرحلهٔ تعیین هدف و نیاز امنیتی سرورها

در ابتدای مدل‌سازی، هدف و نیازمندی امنیتی تعیین شده است. هدف امنیتی، مشخصه‌هایی از سامانه به‌منظور محافظت از دادهٔ انتقالی یا ذخیره شدهٔ آن است(ETSI TR 187 002,2011). هدف امنیتی تعیین‌شده شامل محرمانگی، یک‌پارچگی، حسابرسی، دسترس‌پذیری و احراز هویت است. علاوه‌بر این موارد می‌توان اهداف امنیتی دیگری نیز در مدل‌کردن سرور نام‌برده قرار داد. این اهداف بر اساس

X.805 شامل موارد کنترل دسترسی، حریم خصوصی و امنیت ارتباطات می‌شود(ETSI TR 187 011,2008).

• **محرمانگی:** محرمانگی پروتکل در سرورهای آن از طریق رمز پیام ارسالی بین تجهیزات کاربر و سرور انجام می‌پذیرد. از طریق پروتکل توافق‌شده با کاربر در زمان ارسال پیام ثبت نام، محتوای پیام رمزگذاری می‌شود. به‌عنوان مثال، درصورتی که پروتکل ارتباطی کاربر با شبکه روش IMS AKA باشد، ارتباط به‌صورت رمزشده با کلید Ck منتقل می‌شود و محتوای پیام قابل شنود نخواهد بود؛ زیرا کلید Ck تنها در اختیار سرورهای P-CSCF[1]، S-CSCF و کاربر است(ETSI TR187 014,2009). علاوه‌بر رمزنگاری محتوا، استفاده از IPSec و تونل‌زنی در لایهٔ انتقال و لایهٔ IP نیز در تأمین محرمانگی ارتباط، مؤثر است. محرمانگی در ارتباط کاربر، به‌شدّت وابسته به امنیت پروتکل احراز هویت و توافق کلید است. نقاط ضعف سرور و پروتکل باعث بروز تهدید می‌شوند که سرمایه و دارایی موجود را تهدید می‌کند. دارایی‌ها همان محتوای اطلاعاتی پروتکل و پیام است.

• **یک‌پارچگی:** برای اطمینان از یکپارچگی پیام، دو سازوکار تعریف شده است(ETSI TS 102 165-1,2011):

۱- سازوکار IMS AKA یا HTTP digest به همراه یکپارچگی و حفظ مشخصات نشست در بالای لایهٔ انتقال با پروتکل TLS[2]

۲- استفاده از تونل‌زنی به روش IPSec به‌شرط عدم استفاده از سرور NAT

سرور S-CSCF[3] با دو روش یاد شده؛ در صورت تغییر پیام، قادر به تشخیص تغییر پیام می‌شود. در روش احراز هویت HTTP digest، حفاظت از یکپارچگی اختیاری است. استفاده از پروتکل TLS با توافق در نوع الگوریتم و چگونگی محافظت امنیتی، انجام می‌شود. به این ترتیب در زمان ثبت‌نام کاربر، ارتباط بین سرور و کاربر محافظت خواهد شد. امنیت این ارتباط نسبت به زمانی که پروتکل احراز هویت IMS AKA به‌تنهایی استفاده می‌شود، بیش‌تر است زیرا مهاجم درصورتی‌که بتواند به پروتکل احراز هویت نفوذ کند، نمی‌تواند کلید نشست تولیدشده در ارتباط TLS را حدس بزند(ETSI TS 102 165-1,2011). سازوکار استفاده از IPSec ESP[4] با رمزنگاری سرآیندها، احراز هویت و محرمانگی پیام را به همراه یک‌پارچگی ارتباط تضمین می‌کند. در این روش به‌دلیل ترجمه نشانی‌های کاربران در سرور NAT[5] و تغییر محتوای پیام، یک‌پارچگی حفظ نمی‌شود. این موضوع یکی از دشواری‌های مطرح در حفظ یک‌پارچگی ارتباط است که پژوهش در آن ادامه دارد.

• **حسابرسی:** موضوع مهم مطرح‌شده در یک سرور، حسابرسی کاربران است. ارتباط هر کاربر با شبکه با توافق هزینهٔ لازم برای هر کاربر امکان‌پذیر می‌شود. در مقابل، شبکه موظف است به تمامی کاربران مجاز، خدمات درخواستی را ارائه دهد. سرور I-CSCF[6] اطلاعات مربوط به شارژ کاربر را به سرآیند پیغام SIP می‌افزاید. اطلاعات حسابرسی نظیر P-charging-Vector و P-charging-address توسط P-CSCF در زمان ثبت‌نام به سرآیند پیام اضافه می‌شود. این داده‌ها توسط I-CSCF ذخیره می‌شود. درصورتی که شناسهٔ حسابرسی وجود نداشته باشد، این شناسه توسط سرور I-CSCF تولید می‌شود. سرآیندها و مؤلفه‌های مربوط به حسابرسی نیز در این سرور اضافه می‌شوند. پروتکل SIP تمام تراکنش‌های موفق و ناموفق کاربر و شبکه را در گزارشی با ذکر علت تهیه می‌کند. این قابلیت پروتکل به تهیه‌کنندگان خدمات در زمینهٔ حسابرسی کمک زیادی می‌کند. هر چند موضوع حسابرسی در زمان مدل‌کردن یک تک‌سرور پروتکل که بحث این مقاله است، ممکن است موضوعیتی نداشته باشد؛ اما از موارد مهمی است که در مدل‌سازی مؤثر است. به‌طور مثال در سرور I، اطلاعات شارژینگ به سرآیند پیام افزوده می‌شود.

• **دسترس‌پذیری:** دسترس‌پذیری از موضوعات مهم دیگری است که در مدل‌سازی امنیتی سرورها باید دخالت داده شود. طبق آنچه در(Denver D,2011) آمده است، دسترس‌پذیری در سامانه اطمینان از دسترسی کاربران مجاز به منابع، خدمات وکاربردهای سامانه است. آسیب‌پذیری سرورها در مقابل حملات سیلاب‌ساز از جمله مهم‌ترین ضعف‌های موجود در سرورهای P و S در بحث دسترس‌پذیری است. کاهش تهدیدات ناشی از حملات سیلاب‌ساز منجر به افزایش دسترس‌پذیری سرورها می‌شود. سیاست‌های ارتقای امنیت سرورها از طریق اضافه‌کردن سامانهٔ تشخیص نفوذ و یا تعریف الگوریتم‌های مقایسه و کنترل ترتیب پیام‌های ارسالی از کاربر انجام می‌شود تا از

[1] Proxy -Call Session Control Function
[2] Transport Layer Protocol
[3] Serving-Call Session Control Function
[4] IPSec Encapsulating Security Payload
[5] Network Address Translation
[6] Interrogating-Call Session Control Function

دسترسی کاربر مجاز به منابع و ایمن‌بودن مسیر دسترسی اطمینان حاصل شود. تمهیداتی نظیر تعیین نسبت محاسباتی بین تعداد پیام‌های دعوت(invite)با تعداد پیام (ok یا۲۰۰) ارسالی و به‌دست‌آمدن تعداد نشست‌های نیمه‌باز یکی از روش‌های تشخیص حملات طوفان‌زای ثبت نام است(ITU_T X.805, 2003). موارد ذکر شده تمهیداتی است که حملاتی با هدف نقض دسترس‌پذیری را کنترل می‌کند. بررسی بیش‌تر این تمهیدات در مراحل بعدی مدل‌سازی سرورها انجام خواهد شد. در این مرحله تنها قصد بررسی اهداف امنیتی و نه تمهیدات حفاظتی آنها را داریم.

• **احراز هویت**: آخرین هدف امنیتی، البته نه کم‌اهمیت‌ترین آن، که در مرحلهٔ اول مدل‌سازی مورد بررسی قرار می‌گیرد، احراز هویت است. احراز هویت کاربر جزو مراحل ضروری اولیه به‌منظور ارتباط در شبکه است. لازم به ذکر است این اجبار در شبکه‌های صوتی مبتنی برIP وجود ندارد و کاربر می‌تواند بدون احراز هویت اولیه اقدام به ارسال درخواست کند. احراز هویت از طریق سازوکارهای توافق‌شدهٔ شبکه با کاربر و با توجه به سرآیند Authorization موجود در پیام ثبت نام صورت می‌گیرد. پس از احراز هویت کاربر سرآیند P-Asserted-Identity به پیام پروتکل اضافه می‌شود که اعلام‌کنندهٔ اعتماد سرورP به کاربر است تا همهٔ درخواست‌های کاربر احراز هویت نشود زیرا موجب اتلاف منابع است(Rebahi. Y,2008). با اضافه‌شدن این سرآیند امکان پی‌گیری مشخصات فرستنده حتی در زمان درست‌نبودن مقدار FROM پیام فراهم می‌شود(ETSI TS 102 165-1,2011). این ویژگی از حملهٔ دزدیدن جلسه ممانعت خواهد کرد؛ زیرا پیام با توجه به پیشینهٔ ثبت نام کاربر و نه آنچه مهاجم در سرآیند پیام تنظیم کرده است، منتقل خواهد شد. در شبکه، احراز هویت یک فرآیند دوسویه بین کاربر و شبکه است. به این معنی که علاوه‌بر آن‌که کاربر ملزم است تا مجازبودن خود را با استفاده از روش‌های توافقی به شبکه اثبات کند، شبکه نیز مجازبودن خود را به کاربر ثابت می‌کند. درصورت استفاده از روش IMS AKA احراز هویت دوسویه بین کاربر و شبکه صورت می‌پذیرد. جدول (۴-۱) گروه‌بندی اهداف امنیتی را در یک سرور با استفاده از ایده‌های موجود در مدل‌سازی نشان می‌دهد. طبق آنچه در جدول (۴-۱) اشاره شده است، هر هدف امنیتی با پیاده‌سازی و اجرای سازوکارهای مربوطه، یک یا چند سرور را درگیر می‌کند. با بررسی عملکرد مربوط به سرورهای سه‌گانه، سرورهایP و S نسبت به سرورI دارای مسئولیت متعدد و بیشتری هستند. مسیریابی یک ارتباط و تعیین سرور محلی هر کاربر و محاسبات شارژ و صورت‌حساب کاربر و اطلاعات جابجایی کاربر بین دو شبکه، از وظایف اصلی سرور I است. درحالی‌که وظیفهٔ تأیید مجازبودن/ نبودن کاربر، تأیید نوع خدمات و تعیین سطح خدمات مجاز هر کاربر، اطلاعات مربوط به شناسه‌ها و کلیدهای احراز هویت، محرمانگی در سرورهایP و S است. این دو سرور تولید یک ارتباط، قطع ارتباط (بنابه خط‌مشی[1] شبکه) و حفظ کیفیت خدمات و الگوریتم‌های محاسباتی مربوطه را برعهده دارند(ETSI TS 102 165-1,2011).

موارد پنج‌گانهٔ اشاره‌شده اهداف امنیتی سرورها در شبکه را بررسی کرده است. این موارد با بروز حملات نقض می‌شوند و به این ترتیب امنیت نقض می‌شود. در زیربخش بعدی دارایی‌ها و ارزش‌های سرورها بر طبق روش مدل‌سازی بررسی می‌شود تا ارتباط متغیرهای موجود در تابع آسیب‌پذیری‌ها روشن شود.

۴-۲- مرحلهٔ تعیین سرمایه و دارایی سرورها

هر سامانه دارای سرمایه‌ها و ارزش‌هایی است که از آن محافظت می‌شود. مشخصهٔ هر دارایی شامل نوع دارایی (فیزیکی، منطقی، انسانی)، نوع فناوری، سطح داده‌های مرتبط با فناوری، زمان و طول دوره معتبربودن آن دارایی است. در مدل‌کردن یک سامانه فرض بر آن است که تمام دارایی‌های سامانه دارای ضعف هستند(TS23.228,2014). در این بخش دارایی‌ها و سرمایه‌های سرورها بررسی می‌شود و در مراحل بعدی حملات و تهدیدهای تعریف‌شده بر روی سرمایه‌ها مطالعه می‌شوند. این حملات نقاط ضعف موجود در سرمایه‌ها و دارایی‌ها را نشانه گرفته و آسیب‌پذیری را به سامانه تحمیل می‌کنند.

طبق مرجع (TS23.228,2014)دارایی‌ها به سه نوع دارایی فیزیکی، منطقی و انسانی تقسیم شده‌اند که بخش دارایی انسانی در مدل‌سازی سرورهای پروتکل موردی ندارد؛ زیرا یک سرور با مؤلفه‌های ارتباطی شبکه‌ای آن مدل می‌شود. دارایی‌های فیزیکی و منطقی براساس نوع حملهٔ تعریف‌شده اهمیت دارند. محتوا و اطلاعات درون دارایی‌های فیزیکی را سرمایهٔ منطقی می‌نامند. سرورهای سه‌گانه دارای یک سرمایهٔ فیزیکی است که همان تجهیز

[1] Policy

مربوط بـه سـرور اسـت. تجهیـزات سـخت‌افـزار و سـاختار فیزیکی که سیستم‌عامل، کاربردها، برنامه‌ها و سیاست‌هـای امنیتی بر روی آن نصب می‌شود و فعال است. درواقـع ایـن سرمایه فیزیکی تمام سرمایه منطقی موجـود در سـرورها را پشتیبانی سخت‌افزاری می‌نماید.

سرمایه‌های منطقی سرور شـامل مؤلفـه‌هـای احـراز هویت، کلیـدهای محرمانگی/یـک‌پـارچگی، کلیـد نشسـت، مقادیر سرآیندها و روش پیام پروتکل، داده‌های مربـوط بـه تنظیمات IPSec/ TLS ، شناسـه‌هـای کـاربران و اطلاعـات مربوط به الگوریتم‌ها نظیر الگوریتم فشرده‌سازی/ رمزنگاری است. این سرمایه‌ها با بررسـی پیـام پروتکـل و مؤلفـه‌هـای درگیر در تکمیل یک تراکنش و نقش هر کـدام از سـرورها به‌دست آمده است. تمام یا بخشی از این سرمایه‌ها در زمان تشکیل نشست پروتکـل و اسـتفاده از خـدماتی بـا کیفیـت تعریف‌شده در شبکه، کاربرد دارد.

جدول (۴-۲) سرمایهٔ منطقی سرورهای سه‌گانـه را براساس نقشی که در ارتباط پروتکلی دارنـد؛ تقسـیم کـرده است. در این جدول سرمایه منطقی سیستم‌عامل، کاربردها، برنامه‌ها و سیاست‌های امنیتی در هـر سـه سـرور مشـترک است.

(جدول۴- ۱): اهداف امنیتی یک سرور SIP در TVRA

هدف امنیتی	سرور مسئول (x-CSCF)	نیازمندی امنیتی
احراز هویت	P/S-SCF	سرآیند authorization در پیام ثبت نام
محرمانگی	P/S-SCF	رمز پیام با کلید CK سازوکار IMS AKA از طریق تونل‌زنی IPSec
یک‌پارچگی	P/S-SCF	-کلید IK سازوکار IMS AKA در P-CSCF -از طریق پروتکل TLS -از طریق تونل‌زنی با IPsec
حسابرسی	P/S-SCF	-اضافه‌کردن سرآیندحسابرسی‌در I-CSCF
دسترس‌پذیری	I/S-SCF	-سازوکار احراز هویت IMS AKA -سازوکار کنترلی محاسباتی

بـا بررسـی مشخصـه‌هـا و حمـلات رایـج بـر روی سرورهایIMS SIP، جدول زیر به‌عنوان سرمایه‌های منطقـی دخیل در آسیب‌پذیری‌ها به‌دست آمده اسـت. ایـن جـدول مشخصه‌هایی از سرمایه‌های منطقی سرورها را گـروه‌بنـدی کرده است که در ایجاد حملات شایع‌تر مؤثر می‌باشند.

(جدول۴- ۲): سرمایه‌های سرورهای x-CSCF در مدل‌سازی TVRA

سرمایه‌فیزیکی	سرمایه‌منطقی
سرور P-CSCF	سیستم عامل، کاربردها؛ برنامه‌ها و سیاست امنیتی
	اطلاعات سرآیند P-Asserted-Identity
	آدرس IP و URI کاربر
	اطلاعات SA مربوط به IPsec - اطلاعات سازوکار TLS
	اطلاعات QoS ، Sigcomp, billing، policy
	اطلاعات سرآیند P-visited-Network-ID
	اطلاعات سرآیند P-charging-Vector
	اطلاعات سرآیند path برای مسیریابی پیام توسط S-CSCF
	اطلاعات سرآیند (Call-ID, Cseq, contact, Via, TO, Route, Record Route, from)
	اطلاعات روشRegister/ Invite/ Cancel/ Bye/ Update
سرورI-CSCF	سیستم عامل، کاربردها؛ برنامه‌ها و خط مشی‌های امنیتی
	مسیر پیام در سرآیند Path تا کاربر در S-CSCF اضافه شود.
	اطلاعات billing درI-CSCF در زمان roaming
	آدرس P-CSCF معادل مشخص‌شده هر کاربر
	اطلاعات مربوط به اختفا پیکره‌بندی شبکه
	ذخیره اطلاعات مسیر انتقال پیام در record-route
سرورS-CSCF	سیستم عامل، کاربردها؛ برنامه‌ها و سیاست‌های امنیتی
	اطلاعات مربوط به Call-ID، اطلاعـات ISIM، آدرس IP کاربر
	شناسه عمومی و خصوصی کاربران (IMPI,IMPU)
	اطلاعات شناسه عمومی کاربر در P-Associated-URI
	اطلاعات accounting در I-CSCF (P-Charging-Vector)
	اطلاعات Call-ID در S-CSCF
	ذخیره service route در P-CSCF (آدرسS-CSCF)
	اطلاعات integrity-check در سرآیند authorization
	شماره پورت ارتباطی با کاربر و سایر سرورها

در بین روش‌های پیام پروتکل، پنج روش پیام ثبت نام، دعوت، Bye، Cancel و Update (روش پیام‌های مشخص شده جدول (۴-۳) مهم‌ترین‌ها هستند؛ زیرا بر روی اطلاعات این پیام‌ها در زمان ارسال حملات تعریف شده است که این حملات در شبکه‌های موجود پیاده‌سازی‌شده نیز قابل رصد است و اتفاق می‌افتد. در بین حملات، روش پیام‌های ثبت نام و دعوت در حملات سیلاب‌آسا و روش پیام‌های Cancel و Bye در حملات مربوط به نقض دسترس‌پذیری (سد خدمات) استفاده می‌شوند. این حملات در مرحلهٔ بعدی مدل‌سازی بررسی خواهند شد.

به‌منظور انعطاف پروتکل در پشتیبانی از سرویس‌های متنوع تعریف‌شدهٔ شبکه؛ تعداد سرآیندهای زیادی علاوه‌بر سرآیندهای معمول پروتکل وجود دارد. طبق بررسی انجام‌شده بالغ بر پنجاه و دو سرآیند در این شبکه وجود دارد(ETSI TS 102 165-1,2011). سرآیندهای اشاره‌شده در جدول از دیگر سرمایه‌های منطقی آن است و جزو مشخصه‌های تعیین‌کننده یک نشست می‌باشند. تغییر یا شنود آنها، حملاتی را در شبکه به‌وجود می‌آورد. به‌ازای تمام سرمایه‌های منطقی، ستون سرمایه فیزیکی، معادل دستگاه و تجهیز فیزیکی سرور است و دارای یک سطر به نام سخت‌افزار سرور است جدول (۴-۲). با توجه به محدوده تعریف‌شده در تابع مدل‌سازی سرورها در جدول (۴-۳) جمع‌بندی می‌شود.

(جدول۴- ۳): سرمایه‌های سرور SIP

سرمایه فیزیکی	سرمایه منطقی
سرورهای P - CSCF I - CSCF S - CSCF	مؤلفه‌های احراز هویت کاربر و شبکه
	کلیدهای محرمانگی، یک‌پارچگی، نشست
	مؤلفه‌های تنظیمات TLS و IPSec
	مؤلفه‌های الگوریتم‌ها نظیر الگوریتم فشرده‌سازی/ رمزنگاری
	روش پیام‌های Register، Invite، Cancel، Bye و Update
	سرآیندهای Call-id، Cseq، Via, To, Route,Record Route, Contact

۴-۳- مرحلهٔ تعیین ضعف و آسیب‌پذیری

پس از تعیین سرمایه‌های سامانه، مرحلهٔ بعدی در مدل‌سازی، تعیین نقاط ضعف سامانه است. نقاط ضعف عوامل نامطمئنی هستند که در زمان طراحی، پیاده‌سازی و پیکربندی سرور وجود دارند و می‌توانند توسط مهاجمان برای طراحی حمله، استفاده شوند(TS33.203,2014). به این ترتیب ارتباط ضعف‌ها با حمله طراحی شده، به‌دست می‌آید. این ارتباط همان آسیب‌پذیری سامانه نامیده می‌شود.

مادامی‌که یک دارایی، دارای نقطه ضعفی و احتمال حمله به آن وجود داشته باشد، در معرض خطر یا مخاطره قرار دارد. اهمیت یک آسیب‌پذیری منوط به دو مقدار است. مقدار اول سطح ارزش و دارایی یک سامانه است. هر دارایی در یک سامانه، یک سطح اهمیتی دارد که احتمال وقوع حملات با توجه به نقاط ضعف آن متفاوت است. مقدار دوم، احتمال وقوع حمله به آن دارایی است. هر چه حملات بیشتر باشند، آن ضعف، آسیب‌پذیری پر اهمیت‌تری تلقی می‌شود. این دو مقدار درجه و اهمیت ضعف و آسیب‌پذیری را تعیین می‌کند.

یکی از ضعف‌های سرورها عدم وجود سازوکار کنترل‌کننده پیام‌های ارسالی از سوی کاربران است. ارسال تعداد زیاد درخواست در یک زمان محدود از تمهیداتی است که مهاجم می‌تواند به‌منظور کاهش دسترس‌پذیری سرور انجام دهد. ارسال تعداد بالای پیام به سرور باعث می‌شود تا منابعی نظیر پهنای باند، حجم حافظه و توان پردازشی زیادی صرف مدیریت این درخواست‌ها شود. به این ترتیب سرورکه در اغلب موارد نیز همانP است؛ به‌طور کامل درگیر پردازش این پیام‌ها شده است. نکتهٔ مهم این آسیب‌پذیری، امکان ارسال پیام‌های متعدد دعوت و ثبت نام به‌صورت پی‌درپی به سرور P است و به‌دلیل عدم پیاده‌سازی سامانهٔ امنیتی در سرور (به‌عنوان نمونه عدم وجود پیش‌پردازش[1] پیام) دچار انباشت درخواست‌ها به‌دلیل عدم پردازش شده و سد خدمات رخ می‌دهد. به‌خصوص این‌که دو پیام دعوت و ثبت نام بالاترین زمان پردازشی را به سرور تحمیل می‌نمایند. آسیب دیگر این است که صف ایجاد شده موجب حذف درخواست‌ها به‌دلیل ترافیک و زمان انتظار زیاد می‌شود که این امر نیز دسترس‌پذیری سرور را کاهش می‌دهد؛ زیرا از سرویس‌دهی مناسب آن کاسته است.

نقطهٔ ضعف دیگر سرور، امکان انتخاب روش احراز هویت ضعیف (X. Deng,2009) در ارتباط کاربر با شبکه است. مهاجم با حذف سرآیند احراز هویت پیام ثبت نام در زمان عدم پشتیبانی یک‌پارچگی، سرورP را مجبور به ایجاد ارتباط بدون رمزنگاری می‌کند. با حذف این سرآیند، شبکه روش احراز هویت بدون رمزنگاری نظیر

[1] pre-parsing

Early IMS authentication را انتخاب می‌نماید تا بتواند به کاربر(مهاجم) مربوطه سرویسی ارایه دهد. در زمانی که پیام ثبت نامی بدون سرآیند احراز هویت باشد، شبکه پایین‌ترین سطح احراز هویت (Early IMS authentication) را انتخاب می‌نماید. مشخصه این روش، احراز هویت بدونIPSec و IPv6 و بدون داشتن سرآیند احراز هویت می‌باشد. در این روش، رمزنگاری ارتباط پشتیبانی نمی‌شود و پیام ارتباطی رمزشده نیست؛ که این نیز منجر به شنود پیام خواهد شد. این سازوکار احراز هویت یکی از ضعیف‌ترین سازوکارهای امنیتی در شبکه است. ریشه این آسیب‌پذیری در عدم وجود رمزنگاری است. همان‌طور که می‌دانیم امکان فشرده‌سازی پیام در شبکه به‌منظور آزادسازی پهنای باند اشغالی و کاهش حجم پیام وجود دارد. مهاجم با انتخاب یک الگوریتم فشرده‌سازی سنگین، سرور را مجبور به انجام پردازش سنگین الگوریتم کاهش حجم و مشغول‌کردن پردازش‌گر سرور می‌نماید. این شرایط تحمیلی دسترس‌پذیری سرورP را کاهش می‌دهد. در زمینه انتخاب الگوریتم فشرده‌سازی درصورتی‌که کاربر مجبور به انتخاب یکی از الگوریتم‌های پیشنهادی سرور باشد، نمی‌تواند الگوریتم سنگینی را به سرور تحمیل نماید. در مواردی که کاربر بتواند علاوه‌بر الگوریتم‌های سرور، الگوریتم خودش را تحمیل نماید، این حمله قابل اعمال است. نقاط ضعف بررسی‌شده تنها نمونه‌ای از موارد موجود است. در برخی موارد سازوکارهای امنیتی اضافه‌شده به پیام که به‌منظور ارتقای امنیت به کار می‌روند، سربار پردازشی پیام را افزایش می‌دهند. به‌عنوان نمونه، اگر پروتکلSIP بر روی TCP منتقل شود، در آن صورت استفاده از TLS امکان‌پذیر خواهد بود؛ زیرا بستر TLS باید TCP باشد؛ ولی مشکل اصلی در سربار پردازشی TLS است. به‌طور عمومی در شبکه‌های مبتنی برSIP، ارتباطات بین سرورها را با به‌کارگیری TLS امن می‌نمایند و ارتباطات کاربران را رویUDP نگه می‌دارند. پروتکل TLS با مبادلهٔ اعتبارنامه‌های کاربران، احراز هویت دوسویه را انجام می‌دهد و برروی TCP منتقل می‌شود. به این ترتیب درصورتی‌که بخواهیم از این سازوکار امنیتی استفاده کنیم، مجبور می‌شویم تا اطلاعات را بر روی پروتکل اتصال‌گرای TCP منتقل کنیم که اتصالات زیادی بین کاربر و سرور-P CSCF ایجاد می‌شود که سربار پردازشی به بار می‌آورد.

نمونه‌ای از نقاط ضعف در زیر اشاره شده است:

- ارتباط بدون رمزنگاری کاربر با سرورP-CSCF
- عدم وجود پیش‌پردازش پیام‌های تکراری مهاجم
- زمان‌پردازش طولانی روش پیام دعوت و ثبت نام
- انتخاب احراز هویت ضعیف توسط کاربر و اجبار به برقراری ارتباط بدون تعریف یک‌پارچگی
- انتقال بدون رمزنگاری/ احراز هویت بدون رمزنگاری
- انتخاب الگوی سنگین فشرده‌سازی/ افزایش پردازش
- وجود ضعف در سازوکارهای امنیتی اضافه‌شده
- عدم احراز هویت پیام‌ها (به‌جز پیام ثبت نام)

۴-۴- مرحلهٔ گروه‌بندی حملات و تهدیدهای سرورها

مرحلهٔ بعدی مدل‌سازی بررسی و تعیین حملات رایج سرورهاست. مهاجمان از نقاط ضعف بحث‌شده استفاده کرده و حملات بر روی سرورها را تعریف و اجرا می‌نمایند. با تعیین حملات و تهدیدها درواقع ستون دیگری از جدول (۴-۴) مشخص خواهد شد. ستون حملات و تهدید با توجه به نقاط ضعف و تدوین سناریوهای حمله توسط مهاجمان کامل شده است. می‌توان از طریق تعریف راه‌کار احتمال وقوع حملات را کاهش داده؛ آسیب‌پذیری‌های سامانه را حفاظت کرد.

با توجه به نقاط ضعف تشریح‌شده در گام قبل، حملات و تهدیدهای معادل بررسی می‌شود. هر نقطه‌ضعفی که منجر به تعریف حمله می‌شود و آسیب‌پذیری را به سامانه تحمیل می‌نماید، جزو مواردی است که در زمان پیاده‌سازی سامانه لحاظ می‌شود تا با تعریف تمهیدات امنیتی مناسب احتمال وقوع حمله به حداقل کاهش یافته و سامانهٔ امنی پیاده‌سازی شود. در مدل‌سازی TVRA حملات بر روی سامانه‌های ارتباطی به چهار گروه تقسیم شده است. مشخص است که در سامانه‌های مختلف درصد و احتمال وقوع هر کدام از این حملات با هم متفاوت است. در مدل‌سازی سرور با بررسی مقاله‌ها و روش‌های اجرایی کاهش حملات در پروتکل به این نتیجه رسیده‌ایم که برخی از حملات این گروه‌بندی چهارگانه در سرورهای-x CSCF عملی بوده است.

در ادامه ابتدا حملات گروه‌بندی‌شدهٔ مدل‌سازی تشریح شده است و سپس گروه‌بندی ما برای حملات رایج بر روی سرورها تشریح خواهد شد. این تقسیم‌بندی با توجه به فراوانی وقوع و تعدد مقالات بحث‌شده راجع به آن حملات به‌دست آمده است. حملات در مدل‌سازی به

حملات ناشی از شنود پیام، حملات مربوط به دست‌کاری محتوای پیام، حملات منجر به سد خدمات و انکار خدمات تقسیم می‌شوند. حملات ناشی از شنود ارتباط که دزدیده‌شدن اطلاعات و داده‌ها از تبعات آن است، در زمانی که ارتباط بین کاربر و سرورP رمز نباشد، انجام می‌پذیرد. ایجاد ارتباط بدون رمزنگاری به هر دلیلی که باشد، احتمال شنود داده‌های منتقل‌شده را به‌وجود خواهد آورد. این حمله محرمانگی ارتباط و امنیت حریم خصوصی را نقض می‌کند. نقض اهداف امنیتی از تبعات وقوع حملات است.

حملات مربوط به دست‌کاری پیام در زمانی که یک‌پارچگی پیام انتقالی وجود ندارد، امکان‌پذیر خواهد بود. عدم تعریف یک‌پارچگی پیام از شرایطی است که ممکن است در ارتباط از طریق پروتکل به‌وجود آید. نمونه‌ای از این شرایط می‌تواند زمانی باشد که کاربر از روش Early IMS Authentication استفاده کرده است.

حملات منجر به سد خدمات، دسترس‌پذیری سرورهای x-CSCF را نقض کرده و امکان خدمات‌دهی به کاربر را مختل می‌نمایند. هدف مهاجم در این حمله اشغال پهنای باند شبکه، اشغال فضای حافظه اختصاصی و مشغول‌کردن سرور به انجام حجم زیاد محاسباتی و پردازشی است. در هر سه مورد اشاره‌شده سرور از وظیفه اصلی خود باز می‌ماند و سد سرویس اتفاق خواهد افتاد. حملات ناشی از انکار سرویس، در زمانی که محاسبات مربوط به شارژ و هزینه اختصاصی هر کاربر درست محاسبه نشود و امکان ردگیری وجود نداشته باشد به‌وجود می‌آید. این بحث‌های حقوقی در زمان عدم تعریف سازوکارهای ردگیری رفتار ارتباطی کاربر به‌وجود می‌آید.

حملات به سرورها به‌ترتیب اولویت و فراوانی در مقالات بررسی‌شده در این پژوهش به‌صورت سد خدمات (حملات طوفان‌زا)، حملات ناشی از شنود و در رده آخر حملات مربوط به دست‌کاری پیام و انکار هستند که این دو حمله نسبت به حملات طوفان‌زا و شنود، فراوانی کمتری در مقالات بررسی‌شده داشته‌اند. حملات طوفان‌زا به‌دلیل نقض دسترس‌پذیری سرورها منجر به سد خدمات می‌شوند. حملات مربوط به شنود علاوه‌بر نقض محرمانگی، می‌توانند دست‌کاری پیام را نیز در پی داشته باشند. دست‌کاری، اصلاح و یا تغییر پیام تنها در زمان عدم وجود یک‌پارچگی میسر است. ارسال تعداد زیاد پیام دعوت و ثبت‌نام به سرور P حملات سیلاب‌سازی ثبت نام و حملات سیلاب‌سازی دعوت را به‌وجود می‌آورد. هدف این حملات اشغال منابع و ساختارهای سرورهاست که منجر به سد خدمات و نقض دسترس‌پذیری است. طولانی‌بودن زمان پردازش و افزایش بار سرور از زیان‌های دیگر این حمله است. بالابودن زمان پردازش ثبت نام و دعوت به این حمله سرعت می‌بخشد. در این حملات کارایی منابع سرور کاهش یافته و کاربران مجاز نمی‌توانند سرویس دریافت نمایند. ارسال چندین درخواست ثبت‌نام به سرور از طریق نشانی جعلی یا نشانی شنودی و اشتغال سرور به پاسخ‌های 401 Un Authorized نیز نمونه‌ای از حملات طوفان‌زاست.

در نوع دیگری از حملات طوفان‌زا تعداد زیادی پیام دعوت و ثبت نام ارسال می‌شود و هدف به‌دست آوردن اعتبارها و مشخصه‌های مربوطه از طریق قربانی است. این حملات با نام‌های Invite Response و Register Response یاد می‌شوند. هدف مهاجم در این حملات بر خلاف حملات بررسی‌شده در قبل، سد خدمات نیست؛ بلکه در این نوع درخواست‌ها، با بررسی نوع جواب سرورها و ارسال پیامی دیگر، کشف مشخصه و کلمهٔ عبور هدف است. اغلب پیام‌های دعوت در حمله Invite Response، به‌منظور دریافت و ربودن کلمهٔ عبور استفاده می‌شوند و پیام‌های ثبت نام ارسالی به سرور در حمله Register Response برای دریافت اعتبارنامه و مشخصه‌های مربوطه هستند. جدول (۴-۴). حمله دیگری که منجر به سد خدمات می‌شود، اجبار سرور P-CSCF در انتخاب الگوریتم‌های محاسباتی برای یک‌پارچگی و یا الگوریتم‌های فشرده‌سازی سنگین است. فشرده‌سازی پیام که می‌تواند تا ۸۰٪ حجم پیام ارسالی را کاهش دهد، از طریق توافق کاربر و این سرور اجرا می‌شود. مهاجم می‌تواند سرور را وادار کند تا از الگوریتم سنگین با بار پردازشی بالا استفاده کند که این حمله نیز دسترس‌پذیری سرور را کاهش خواهد داد.

از دیگر حملات، بهره‌جویی از احراز هویت ضعیف و شنود پیام در سرور P است. شنود پیام؛ مشخصه‌ها و اطلاعاتی از نشست را به مهاجم می‌دهد. مهاجم می‌تواند از طریق اطلاعات شنودشده، پیام‌هایی جعلی را به شبکه ارسال کند که مشخصه‌های مربوط به یک نشست جاری را دربرداشته باشد. حملهٔ پایان مکالمه با رونوشت اطلاعات مربوط به شناسه و اضافه‌کردن آنها در یک درخواست جعلی Bye، دیالوگ جاری را به‌صورت اجباری تمام می‌کند (ETSI TS 102 165-1,2011)همچنین از طریق ارسال پیام بی‌موقع نظیر پیام Bye و یا Cancel و تغییر جریان پیام‌ها

از روند جاری، سرویس‌دهی مختل می‌شود. این نوع از حمله به یک مکالمه جاری بدون اجازهٔ دو کاربر مجاز خاتمه خواهد داد و این حمله نوع دیگر سد خدمات است که تنها با ارسال یک پیام و نه جریانی از پیام، اتفاق افتاده است. سد خدمات در این حمله نه از طریق مشغول‌کردن منابع شبکه و یا اشغال پهنای باند بلکه از طریق ختم غیرمجاز یک نشست جاری صورت می‌پذیرد. ریشهٔ پیاده‌سازی این حمله براساس شنود پیام بوده و طبق بررسی انجام‌شده می‌دانیم شنود مشخصات ارتباطی جزو دومین دسته حملات به سرور از بعد فراوانی است.

یکی از موارد دیگر وقوع شنود استفاده از روش احراز هویت Early IMS Authentication است که در آن پیام انتقالی رمز نمی‌شود. بدون رمزنگاری پیام، کاربران غیرمجاز می‌توانند سیگنالینگ و یا رسانه یک ارتباط را بدون آن‌که شناسایی شوند، شنود نمایند و با استفاده از اطلاعات حساسی نظیر شناسهٔ خصوصی کاربر، به سرور شبکه آسیب برسانند. اطلاعات شنودشده به‌منظور ایجاد یک پیام جدید مورد استفاده قرار می‌گیرند.

شنود مشخصه‌های ارتباطی می‌تواند منجر به سرقت شناسه کاربر (Register Hijacking) شود.

ارسال پیام ثبت نام علاوه‌بر زمان شروع اتصال کاربر به شبکه در زمان‌های دیگری نظیر تغییر موقعیت کاربر و به‌روزرسانی موقعیت کاربر نیز اتفاق می‌افتد. درصورتی‌که مهاجم بتواند شناسه خصوصی یک کاربر ثبت نام‌شده را به‌دست آورد، می‌تواند درخواست ثبت‌نام به شبکه دهد و سرور S با دریافت این پیام از جانب کاربر ثبت نام‌شده، حس می‌کند که کاربر به‌دلیل تغییر موقعیت، پیام ثبت نام را ارسال کرده است. بنابراین موقعیت جدید (موقعیت مهاجم) به‌عنوان موقعیت جدید کاربر مجاز تلقی و ذخیره می‌شود و ارتباط آن بدون احراز هویت مجدد ثبت می‌شود و کاربر واقعی ارتباط را از دست می‌دهد. مهاجم با ثبت نام در شبکه می‌تواند از تمام خدمات کاربر مجاز بهره‌مند شود و ثبت‌نام کاربر مجاز از بین می‌رود(Rebahi. Y,2008). این حمله دسترس‌پذیری را نقض می‌کند و منجر به سد خدمات می‌شود. نحوه انجام این حمله به این صورت است که مهاجم خود را به‌عنوان کاربر احراز هویت‌شده معرفی می‌نماید و این کار از طریق شنود مشخصات کاربر انجام می‌شود. استفاده از ابزار پویش برای به‌دست آوردن برخی اطلاعات مفید برای مهاجمان نظیر نسخه سیستم‌عامل‌های سرورهای CSCF، پیکربندی ساختار شبکه IMS و غیره نیز از نمودهای شنود است. این تهدیدها در زمانی که محافظت از محرمانگی سیگنالینگ و رسانه وجود ندارد و احراز هویت و سازوکارهای کنترلی کارا در شبکه موجود نیست، انجام‌پذیر می‌شود. از نمونه مثال‌های مربوط به دست‌کاری پیام، حمله‌های مربوط به اضافه‌کردن یک دستور به متن پیام ارتباطی است. حمله نفوذ در SQL[1] یکی از روش‌های این حمله است که در زمان آغاز احراز هویت کاربر انجام می‌شود و علاوه‌بر تغییر متن پیام، عدم سرویس‌دهی شبکه را نیز موجب می‌شود.

حملات انکار خدمات در شبکهٔ IMS فراوانی کم‌تری دارد. با توجه به سرآیندهای تعریف‌شده در IMS SIP که سرورهای I و P مسئول ثبت استفاده کاربر از سرویس‌های شبکه می‌باشند، این حملات در IMS نسبت به VOIP کمتر انجام می‌شود. درصورت استفاده از سازوکار امنیتی امضای دیجیتال می‌توان مقابله با انکار خدمات را در شبکه انجام داد و رسیدن پیام به مقصد (گرفتن سرویس) و ارسال پیام توسط فرستنده (درخواست سرویس) را اثبات کرد.

گروه‌بندی‌های تشریح‌شده از حملات با توجه به مقالات موجود و روش‌های مقابله با حملات به سرورهای SIP به‌دست آمده است. ترتیب ذکرشده در حملات، در واقع به‌ترتیب فراوانی وقوع حملات در این شبکه است.

تا این قسمت از توضیحات مرحله حملات و تهدیدهای سروهایSIP در شبکه IMS مورد نقد و بررسی قرار گرفته است. این مرحله از مدل‌سازی به ما نشان داد، فراوانی حملات طوفان‌زا که منجر به سد خدمات می‌شود، نسبت به سایر حملات بیشتر است. حملات شنود و دست‌کاری پیام که نقض محرمانگی و یک‌پارچگی را به دنبال دارند، در درجه بعدی اهمیت حملات در این سرورها قرار دارند. این حملات در ستون تهدیدها و حملات جدول (۴-۴) تشریح شده است. حملات بررسی شده حملاتی است که تنها در پروتکل پیاده‌سازی‌شده در شبکه IMS وجود خواهد داشت و این حملات در پروتکل SIP شبکه‌های مبتنی بر IP تعریف نشده باشند. پروتکل شبکه IMS به‌دلیل برخی تمهیدات اجباری نظیر احراز هویت کاربر و غیره با پروتکل شبکه مبتنی برIP تفاوت‌هایی دارد. حملاتی که در IMS انجام می‌شود:

- استفاده از الگوریتم سنگین فشرده‌سازی پیام با هدف سد خدمات

[1] SQL Injection

(جدول۴-۴): خلاصه مدل‌سازی سرورهای سه‌گانه SIP موجود در IMS با استفاده از TVRA

سرمایه منطقی سرورها	نقاط ضعف	موقعیت	تهدیدها و حملات	هدف‌امنیتی نقض شده	تمهیدات امنیتی
روش پیام cancel/bye	ارتباط بدون رمزنگاری با P-CSCF	پیام SIP	شنود-سد سرویس با cancel/bye جعلی	یکپارچگی- دسترس‌پذیری	- اجبار احراز هویت پیام cancel/bye در زمان نبود محرمانگی - محدودیت در انتخاب روش‌های Early IMS Auth، NBA و HTTP basic Auth در مورد کاربر با QOS بالا
روش پیام دعوت و ثبت‌نام	عدم پیش‌پردازش	S/P-CSCF	سد سرویس/ حمله سیلاب‌سازی	محرمانگی	- روش‌های محاسباتی ریاضی ○ بررسی بار پردازنده در پردازش بسته SIP ○ بررسی رابطه تعداد بسته‌ها در تراکنش SIP - روش‌های داده کاوی (نظیر شبکه بیزین، الگوریتم ژنتیک) - روش‌های تعریف ماشین حالت (نظیر بررسی ماشین‌حالت SIP)
روش پیام دعوت و ثبت‌نام	زمان پردازش طولانی	S/P-CSCF	سد سرویس/ حملات سیلاب‌سازی ثبت نام/ دعوت	محرمانگی- دسترس‌پذیری	
روش پیام ثبت نام	احراز هویت ضعیف- عدم یکپارچگی	پیام SIP	SQL/ Injection	دسترس‌پذیری	- بررسی متن پیام برای کلماتی که در حملات SQL مهم هستند. به‌طور مثال علامت (؛) به همراه کلمات cut، copy و delete
سرآیندهای SIP (Via ،Cseq ،Call-Id)	انتقال بدون رمز و یا احراز هویت بدون رمز	پیام SIP	شنود- دست‌کاری پیام	محرمانگی- یکپارچگی- دسترس‌پذیری	- پشتیبانی اجباری یکپارچگی در HTTP digest - رمز نگاری اجباری با TLS در زمان registration - استفاده از TLS و IPSec ESP در حفاظت امنیت ارتباط

- سرقت ثبت نام به‌دلیل عدم احراز هویت پیام ثبت نام تکراری
- حملهٔ طوفان‌زای دعوت[17]
- حمله طوفان‌زای ثبت نام
- سد خدمات به‌دلیل ارسال cancel/bye جعلی در زمانی که پیام رمز نمی‌شود.
- شنود پیام در زمان انتخاب احراز هویت ضعیف به‌دلیل عدم پشتیبانی از رمزنگاری
- تحمیل بار پردازشی بالا و اشغال پهنای باند به‌دلیل استفاده از روش احراز هویت سنگین نظیر IMS AKA یا الگوریتم فشرده‌سازی سنگین

در ادامه حملاتی که در شبکه انجام نمی‌شود فهرست می‌نماییم:

- شنود/ سرقت پیام زمانی که رمزنگاری تعریف شده است.
- اصلاح/ تغییر پیام زمانی که یکپارچگی تعریف شده باشد.
- جعل IP فرستنده به‌دلیل ثبت آدرس معادل کاربر در سرور IMS
- جعل شناسه کاربری به‌دلیل ثبت شناسه در زمان ثبت نام
- سرقت شناسه به‌دلیل ثبت شناسه هر کاربر در P-CSCF

گام بعدی مدل‌سازی سرورها، تعیین اقدامات پیش‌گیرانه امنیتی مقابله با این حملات است. این اقدامات روش‌های اجرایی پیاده‌سازی در کاهش احتمال وقوع حمله و حفاظت از ارزش‌ها و دارایی‌های شبکه است. قبل از ورود به گام بعدی جدول نهایی مدل‌سازی جدول (۴-۴) را در انتهای بخش اضافه می‌نماییم تا هم مروری بر کارهای انجام شده تا این مرحله باشد و هم نشان‌دهنده اجمالی تمهیدات پیش‌گیرانه معادل هر بخش باشد.

۴-۵- تعیین تمهیدات پیش‌گیرانه

آخرین مرحله مدل‌سازی و تحلیل آسیب‌پذیری‌ها؛ یافتن اقدامات پیش‌گیرانه امنیتی در مقابله با حملات و کاهش

[17] Invite Flooding

آسیب‌پذیری سرورهاست. اقدامات پیش‌گیرانه اضافه‌شده می‌بایست بار پردازشی کمی بر سیستم وارد نمایند.

پروتکل SIP مکانیزم امنیتی خاصی در ارتقای عملکرد آن پیشنهاد نداده است(Russell. T,2008). در بین سرورها، سرورهای P و S بالاترین تأثیر و نقش در ارتباط شبکه با کاربر را دارند. ارتقای امنیتی سرور P به‌عنوان دروازه ورودی ترافیک SIP به هسته شبکه IMS، می‌تواند جزو راه کارهای بنیادی در بهبود امنیت سرورهای این شبکه باشد و کارایی این سامانه با استفاده از اندازه‌گیری تفاوت تأخیر زمانی پاسخ‌گویی به یک درخواست مجاز در هر دو حالت ترافیک (پاک و حمله) سرور است.

با توجه به حملات بررسی‌شده، حمله طوفان‌زا تهدید عمده سرور P است. به‌همین دلیل پیشنهاد می‌شود که از یک سامانهٔ پیش‌پردازش به‌عنوان یک دیوار آتش در سرور P استفاده شود. ایجاد سازوکارهای امنیتی نباید تأخیر زیادی به سرور تحمیل نماید. تأخیر زیاد به معنی ضعیف‌ترشدن سرور در مقابل حملات طوفان‌زاست. بنابراین پیاده‌سازی سازوکارهای امنیتی اضافه‌شده نباید زمان پردازش زیادی را به سامانه اضافه کنند و باید کم‌ترین زمان ممکن را از CPU چه در زمان پاک و چه در زمان حمله بگیرد. یک روش، اضافه‌شدن سامانه بیرون از سرور و در نقش دیوار آتش است تا به بررسی بسته‌های ارسالی کاربر به منظور کشف حملات بپردازد. این روش سبب تأخیر در ایجاد مکالمه می‌شود. روش دیگر اضافه‌کردن این سامانه درون‌سرور و به‌صورت پردازش‌گر موازی پیام است. این سامانه با توجه به نوع حملات معمول بر سرور P نظیر حملات طوفان‌زا، شنود و دست‌کاری پیام، راه‌کار مناسبی در پیش می‌گیرد. اولویت‌بندی پردازش پیام، کنترلی بر حملات طوفان‌زاست. تمهیداتی نظیر تعیین حد آستانه ۸۰٪ از فعالیت پردازنده سرور و حذف درخواست‌های جدید پس از عبور پردازنده از این حد آستانه، کاهش اولویت پیام‌های دعوت (Invite) جدید در این حالت، اولویت در حفظ نشست جاری نسبت به تشکیل نشست جدید، کاهش بار پردازش سرور P را در پی خواهد داشت. این تمهیدات مجموعه راه‌کارهای پیشنهادی است در زمان حمله طوفان‌زا که منجر به اشغال منابع شبکه و سد خدمات می‌شود. در زمان اضافه‌بار سرورها عملیات زیر انجام می‌شود:

- احراز هویت کاربران مجاز ادامه می‌یابد.
- درخواست‌های ثبت نام/ دعوت از جانب کاربران مجاز (قبلاً احراز هویت موفق داشته‌اند) قبول می‌شود.
- پیام ثبت نام از کاربران ناشناخته مسدود می‌شود زیرا این پیام‌ها ممکن است منجر به اضافه‌بار شده باشند.
- گزارشی از حملهٔ تشخیص‌داده‌شده ارایه می‌شود.

طبق بررسی‌های انجام‌شده اقدامات امنیتی پیش‌گیرانه در ادامه پیشنهاد شده است:

- در حملهٔ Cancel وBye مهاجم از طریق شنود، مشخصه‌های ارتباطی مکالمه را به‌دست می‌آورد و پیام‌های جعلی را برای ایجاد سد خدمات می‌فرستد. این پیام‌ها احراز هویت نمی‌شوند. پیشنهاد می‌شود علاوه‌بر پیام ثبت نام، این دو پیام نیز احراز هویت شود. راه حل دیگر، استفاده از رمزنگاری باکمک TLS به‌منظور جلوگیری از شنود است. الزامی‌بودن احراز هویت تمام درخواست‌های کاربران، قبل از استفاده از خدمات شبکه، هر چند یک سازوکار کنترلی قوی در حذف جعل شناسه کاربر و یا حملهٔ جعل نشانی و دست‌کاری پیام است؛ اما باعث افزایش حجم پردازش سرور می‌شود و پیشنهاد عملیاتی نیست. به همین دلیل تنها احراز هویت اجباری این دو پیام در زمان عدم رمزنگاری پیام برای مقابله با حملهٔ سد خدمات کافی است.
- انتخاب روش احراز هویت بدون حفظ محرمانگی جزو ضعف‌های عمدهٔ سرور P محسوب می‌شود و بهتر است امکان انتخاب این روش‌ها در ارتباط کاربر محدود شود و یا در صورت انتخاب، کنترل بیشتری بر روی سرویس‌های ارایه‌شدهٔ شبکه اعمال شود.
- یکی از روش‌های ارتقای امنیت سرور شبکه، استفاده از پروتکل‌های IPSec وTLS است که استفاده از پروتکل IPSec دشوار و پرزحمت است؛ زیرا سربار اضافی به‌دلیل رمزنگاری به روشIPSec-ESP را تحمیل می‌کند. درحالی‌که امن‌کردن با روشTLS سربار کمتری در سیگنالینگ ایجاد می‌کند. اضافه‌کردن سرآیندهای مربوط به پروتکل‌های IPSec و TLS به پیام نیز در حفظ یک‌پارچگی و محرمانگی ارتباط مؤثر و کاراست. این سازوکارها در مقابل حملات شنود که گاهی دست‌کاری پیام را نیز سبب می‌شود، مفید واقع می‌شوند.
- پیشنهاد می‌شود روش TLS در سرورهای با توان پردازشی بالای P و روش IPSec در زمان تعامل بین دو شبکه به کار رود. این پیشنهادها به‌دلیل خاصیت‌های هر کدام از این سازوکارهای امنیتی است.
- پیشنهاد می‌شود از روش احراز هویت HTTP digest

authentication تنها در حالتی استفاده شود که یک‌پارچگی ارتباط لحاظ شده باشد تا از انواع حملات دست‌کاری پیام جلوگیری شود. همان‌طورکه می‌دانیم این روش امکان احراز هویت بدون پشتیبانی از یک‌پارچگی را نیز مهیا می‌سازد. انتخاب احراز هویت با یکی از دو روش HTTP digest authentication وIMS AKA با توجه به نیازمندی‌های شبکه و کاربر صورت پذیرد. این نیازمندی‌ها قبلاً در سرورP بررسی شده و نوع ارتباط کاربر با شبکه نهایی شود. درصورتی‌که زمان پردازش پیام برای سرور اهمیت داشته باشد، از روش HTTP digest authentication استفاده شود زیرا این روش به‌طور کامل با پروتکل سازگار بوده و طول پیام‌ها را افزایش چشم‌گیری نمی‌دهد. درحالی‌که روش IMS AKA طول پیام را به مقدار زیادی افزایش داده و تعداد پیام‌های مبادله‌شده برای احراز هویت کاربر در این روش بیشتر از روش قبل است. با توجه به این مشخصات انتخاب روش دوم بار پردازشی بیش‌تری را به سرور P و S منتقل می‌کند. البته در حالت کلی IMS AKA امنیت بالاتری را نسبت به روش دیگر مهیا می‌کند اما لزوماً رایج‌ترین روش نیست (Ahmad B, ۲۰۱۲).

- در زمانی‌که ثبت نام کاربر تکرار می‌شود سرور S، احراز هویت کاربر را انجام نمی‌دهد و تنها به بازنشانی زمان‌سنج ثبت نام اکتفا می‌نماید، باید تمهیدی برای جلوگیری از این حالت اندیشیده شود. به این دلیل پیشنهاد شد در صورت بالانبودن بار پردازشی سرور P تمام پیام‌های ثبت‌نام احراز هویت شوند.
- از تمهیدات امنیتی دیگر، محدودیت در انتخاب الگوریتم سنگین در سرویس فشرده‌سازی پیام (SigComp) است. این راه‌کار در زمان افزایش حجم پردازش سرور، مفید است. تعیین اولویت‌ها در تمهیدات امنیتی به‌صورتی‌که هم اهداف امنیتی و هم اهداف طراحی سامانه را با کم‌ترین هزینه و بیشترین امنیت لحاظ نماید، می‌تواند در تکمیل مدل‌سازی مؤثر باشد.
- احتمال افشا، شنود و تحلیل ترافیک در تمام دارایی‌های منطقی وجود دارد. برای مقابله با این حمله که محرمانگی، حریم خصوصی و کنترل دسترسی را در شبکه نقض می‌نماید، توصیه می‌شود رمزنگاری پیام در تمام شرایط، یک اجبار باشد و امکان ارتباط بدون رمزنگاری، تاحد امکان محدود شود. رمزنگاری برای مقابله با حمله سرقت نشست و سرقت ثبت نام نیز مفید است.
- پروتکل SIP سازوکار کنترل طول پیام ندارد و این ضعف باعث استفاده غیرمجاز از پروتکل و افزایش تأخیر زمان شروع و افزایش زمان پردازش سرورها می‌شود. برای کاهش بار پردازشی سرور P بهتر است برای این مورد سازوکاری اندیشیده شود، زیرا در زمان بار زیاد سرور، تعداد پیام‌های پردازش‌شده کاهش می‌یابد.
- ثبت‌نام و احراز هویت کاربر در شبکهٔ IMS در شروع اتصال به شبکه اجباری است(Sisalem. D,2009). با احراز هویت تمام درخواست‌های ارسالی به سرور S ، ترافیک واسط (Cx) بین سرور S و HSS[18] و زمان تحمیلی پردازش در سرورهای P و S افزایش چشم‌گیری می‌یابد. در حالت احراز هویت تمام درخواست‌ها توسط پروکسی سرور P ، تعداد پیام‌های پردازش شده به میزان۵۷٪-۷۰٪کاهش خواهد یافت(Wang D.,2009). به این ترتیب دسترس‌پذیری سرورها که یکی از اهداف امنیتی است، نقض خواهد شد. این نتیجه‌گیری نشان می‌دهد احراز هویت تمام درخواست‌ها عملیاتی نیست. به همین دلیل باید روش و راه‌کار دیگری برای جلوگیری از آسیب‌پذیری‌های ناشی از جعل پیام‌ها با استفاده از شنود مشخصات نشست اندیشیده شود. بدین ترتیب مدل پروتکلSIP در شبکه IMS با استفاده از یک متدولوژی مدل‌سازی امنیتی به‌منظور روشن‌شدن آسیب‌پذیری‌های آن انجام می‌شود.

در جدول (۴-۴) خلاصه‌ای از مراحل طی‌شده به‌منظور مدل‌سازی امنیتی سرورهای IMS SIP نشان داده شده است. این جدول دارای ستون‌های مربوط به گام‌های مدل‌سازی است.

در زمانی که چندین سرور S وP در یک شبکه IMS وجود دارد، سرور I با مشخص‌کردن سرور S معادل کاربر، نشانی P معادل را در آن اضافه می‌نماید تا ارتباط بین کاربر و شبکه محدود به سرورهای موجود در ارتباط باشد.

۵- نتیجه‌گیری به همراه کارهای آتی

مدل‌سازی سامانه قبل از طراحی و پیاده‌سازی آن باعث به‌دست‌آمدن نقاط ضعف و محدودیت‌های طراحی می‌شود. دارایی سامانه با آسیب‌پذیری ارتباط دارد و آسیب‌پذیری‌ها متشکل از ضعف‌ها و تهدید است و مدل‌سازی قبل از پیاده‌سازی باعث کاهش هزینه به‌همراه ارتقای امنیت

[18] Home Subscriber Server

می‌شود. تحلیل محدودیت‌ها و نقاط ضعف، انتخاب‌ها و تصمیم‌گیری‌های پیاده‌سازی را روشن، منطقی و نهایی می‌نماید و روش‌های بهینه پیاده‌سازی با توجه به کاربری سامانه مشخص می‌شود. مشخص‌شدن آسیب‌پذیری‌ها توجه طراحان را در زمان پیاده‌سازی جلب کرده و می‌تواند به طراحی و پیاده‌سازی سرورهای امن‌تر منجر شود. طبق تحلیل آسیب‌پذیری‌های سرورها، در این مقاله مشخص شد که حملات ناشی از شنود، دست‌کاری و تغییر، سد خدمات و انکار خدمات در این پروتکل می‌تواند انجام شود که با توجه به مراجع و نتایج به ترتیب شیوع حمله سد سرویس، شنود، دست‌کاری پیام و در انتها انکار سرویس در پروتکل انجام می‌گیرد. از حمله سد خدمات که دسترس‌پذیری را مختل می‌نماید، به حملات طوفان‌زا که آسیب اصلی را به سرورهای P و S وارد می‌نمایند، می‌توان اشاره کرد. از بررسی آسیب‌های ناشی از این تهدید؛ استفاده از روش احراز هویت رمزشده یکی از بهترین راه‌کارهای پیشنهادی است که نه تنها سازوکاری پیش‌گیرانه از حمله است، بلکه از حملات شنود و دست‌کاری پیام نیز به‌دلیل استفاده از احراز هویت رمزشده جلوگیری می‌کند. راه‌کار مناسب دیگر، تهیه سامانه‌ای برای محاسبه نسبت پیام‌های (دعوت وok) دریافتی در سرور P است که در جلوگیری از حملات طوفان‌زا پیشنهاد می‌شود و سابقهٔ پیاده‌سازی و اجرا نیز دارد. به این معنی که یک سامانهٔ پیش‌پردازش تعبیه می‌شود تا تعداد و نوع پیام‌های ارسالی به سرور را قبل از شروع پردازش، شمارش و محاسبه نماید و با تشکیل یک الگوریتم و تعیین حد آستانه، در صورت رسیدن تعداد و نوع پیام‌ها به این حد آستانه، از پردازش پیام توسط سرور ممانعت می‌نماید. ضرورت دارد این تمهید امنیتی پیش از پردازش پیام در سرورP انجام پذیرد. روش اجراشده در این سامانه می‌تواند هر کدام از روش‌های محاسباتی ریاضی نظیر بررسی بار پردازنده در پردازش بسته و یا بررسی رابطه تعداد بسته‌ها در تراکنش پیام‌ها باشد. همچنین روش‌های داده‌کاوی نظیر شبکه بیزین یا الگوریتم ژنتیک نیز مفید خواهد بود. روش‌های محاسباتی مبتنی بر ماشین حالت هم راه‌کار دیگر است. خلاصه نتایج استخراجی از مدل‌سازی سرورهای سه‌گانه به‌منظور رسیدن به تمهیدات امنیتی در قالب جدول (۴-۴) تشریح شد. علاوه‌بر این جدول در بخش ۴ نیز تمهیدات امنیتی حاصل از مطالعه رفتار حملات و ترافیک سرورها پیشنهاد شده است. بعد از حمله سد خدمات، حمله شنود به‌دلیل عدم وجود رمزنگاری در ارتباط است. این حمله در صورت استفاده از احراز هویت ضعیف و عدم پشتیبانی از رمزنگاری و یک‌پارچگی در ارتباط رخ می‌دهد و محرمانگی را نقض می‌کند.

تمهید امنیتی به‌دست‌آمده و قابل اجرا برای این حمله، پشتیبانی اجباری یک‌پارچگی در Http digest، رمزنگای در زمان ثبت‌نام کاربر است. برای جلوگیری از شنود در زمان ارسال پیام‌های cancle, bye در زمان عدم وجود رمزنگاری، اجبار در احراز هویت این دو پیام است. همان‌طور که می‌دانیم، تنها پیام دعوت احراز هویت می‌شود و سایر پیام‌ها اجباری در احراز هویت ندارند.

طبق بررسی روش‌های احراز هویت، پیشنهاد می‌شود کاربرانی که از سرویس کیفیت سرویس استفاده می‌کنند، اجازه انتخاب روش‌های Early IMS Auth، NBA و HTTP basic Auth را به‌دلیل ضعیف‌بودن سازوکار امنیتی و امکان ایجاد حمله شنود، نداشته باشند و در انتها پیام‌های ثبت نام بدون سرآیند احراز هویت اجازهٔ پردازش نداشته باشند.

پیشنهادهای ذیل می‌تواند کارهای آتی قابل اجرا در ادامهٔ این پژوهش باشد:

بررسی اثر اضافه‌شدن تمهیدات پیش‌گیرانه بر امنیت و کارایی سامانهٔ مدل‌شده از کارهایی است که پس از مدل‌سازی انجام می‌شود. به‌عنوان نمونه آسیب‌پذیری‌ها و تهدیدهای خاص حاصل از اضافه‌کردن سازوکار امنیتی IPSec, TLS, Sigcomp به سامانه چیست و اثر آن بر سرعت کارکرد سرورها و کارایی آنها چه خواهد بود. این بررسی باعث می‌شود تا سازوکارهای امنیتی جدیدی که به‌عنوان اقدامات پیش‌گیرانه به سامانه اضافه می‌شوند آسیب‌پذیری‌های کم‌تری داشته باشند و سامانهٔ مدل‌شده با TVRA در پیاده‌سازی عملیاتی‌تر باشد.

پس از مدل‌سازی و تعیین آسیب‌پذیری‌های سرور، مدل‌سازی مراحلTVRA از طریق برنامه UML می‌تواند مرحله بعدی پژوهش باشد. استفاده از نمودارهای حالت کلاس(class)، مورد کاربرد و شیء این نرم‌افزار مدل‌سازی، منجر به تحلیل سامانه به‌صورت منظم می‌شود. این شناسایی در تعریف فهرست عملیاتی تمهیدات امنیتی مؤثر است. ادغام مراحل مدل‌سازی با نمودارهای حالت، محدودهٔ روشنی از چالش‌ها در پیاده‌سازی سرورهای سه‌گانه پروتکل را به ارمغان خواهد آورد.

از دیگر بخش‌هایی که این روش مدل‌سازی مفید است و هنوز فعالیتی در آن صورت نپذیرفته است،

مدل‌کردن تعامل بین سرورها در دو شبکهٔ IMS در زمان جابه‌جایی کاربر به شبکهٔ میزبان است. تعیین حملات مهم، آسیب‌پذیری‌های پروتکل در ایجاد ارتباط در زمان جابه‌جایی، تعیین تمهیدات امنیتی با توجه به تفاهم‌نامه تعامل دو شبکه و امکانات موجود در شبکهٔ میزبان از جمله مواردی است که مدل‌سازی جابه‌جایی کاربر بین دو شبکه را به چالش می‌کشد.

۶- مراجع

3GPP TS 23.228, 3rd Generation Partnership Project Technical Specification Group Services and System Aspe-cts; (IMS); stage 2 (Release 13), 2014.

3GPP TS 24.229 V9.3.1, 3rd Generation Partnership Project Technical Specification Group Core Network and Term-inals; IP multimedia call control protocol based on (SIP) and (SDP); 2010.

3GPP TS 33.203 V12.8.0 , 3rd Generation Partnership Project Technical Specification Group Services and System Aspe-cts; 3G Security; Access security for IP-based services (releases 12), 2014.

3GPP TS 33.978, 3rd Generation Partnership Project Tech-nical Specification Group Services and System Aspects; Security aspects of early IMS; Release8, 2008.

Ahmad B, Abdulrahman A, Nadine A, Muhammad E, " Security analysis and Delay Evaluation for SIP-Based mob-ile mass examination system"", International Journal of Next-Generation Networks(IJNGN) Vol.4,No.1, 2012.

Bremler-Bar. A., Halachmi-Bekel. R., Kangasharju. J, " Unregister Attacks in SIP ", 2nd IEEE workshop on Secure Network Protocols(NPSec), CA, 2006.

Denver D. Neco V," Vulnerability Discovery & Analysis within the Open Source IMS Core" SATNAC conference, Lon-don, 2011.

ETSI TR 187 002, Telecommunications and Internet Converged Services and Protocols for Advanced Netw-orking (TISPAN) Threat and Risk Analysis, 2011.

ETSI TR 187 011, (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards -guide, method and application with examples, 2008.

ETSI TR 187 014, (TISPAN); eSecurity; User Guide to eTVRA web-database, 2009.

ETSI TS 102 165-1, Telecommunications and Internet converged Services and Protocols for Advanced Netw-orking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis, 2011.

International Telecommunication Union; Telecommuni-cation Standardization Sector of ITU, "Security architecture for systems providing end-to-end comm-unications", ITU_T X.805, 2003.

Rebahi. Y., Sher. M., Magedanz. T., "Detecting flooding attacks against (IMS) networks," Computer Systems and Applications(AICCSA), pp.848-851, 2008.

Russell. T., The IP Multimedia Subsystem(IMS); Ses-sion Control & Other Network Operations, published by Mc Graw Hill, 2008.

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

Wang D., Liu C., Model-based Vulnerability Analysis of IMS Network, Journal of Networks, VOL. 4, NO. 4, 2009.

X. Deng, M. Shore, "Advanced Flooding Attack on a SIP Server", the International Conference on Availability, Reliability and Security, 2009.

افسانه معدنی فارغ التحصیل کارشناسی ارشد رشته مهندسی فناوری ارتباطات و اطلاعات گرایش مخابرات امن از علم و صنعت در سال ۸۹ و کارشناسی الکترونیک از دانشگاه صنعتی امیرکبیر است. زمینه‌های تحقیقاتی ایشان امنیت شبکه و اطلاعات، مدیریت رویدادهای امنیتی و شبکه‌های مخابراتی سیار است.

نشانی رایانامهٔ ایشان عبارت است از:

madani@itrc.ac.ir

نسرین تاج فارغ التحصیل کارشناسی ارشد رشته مهندسی فناوری ارتباطات و اطلاعات گرایش مخابرات امن از علم و صنعت در سال ۸۸ و کارشناسی کامپیوتر دانشگاه آزاد واحد جنوب تهران است. زمینه‌های تحقیقاتی ایشان امنیت شبکه و اطلاعات، محرمانگی و مدیریت فناوری اطلاعات و زیرساخت کلید عمومی است.

نشانی رایانامهٔ ایشان عبارت است از:

taj.ict@gmail.com