فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال سوم، شماره‌ی ۱ (بهار ۱۳۹۳): صص ۹۵ – ۱۱۳

ارائه مدل‌های امنیتی برای تهدیدها و آسیب‌پذیری شبکه‌های نسل آتی مبتنی بر IMS

مهرداد نجفی نوکاشتی[۱]
ضرغام رستمی[۲]

تاریخ دریافت: ۱۳۹۲/۱۰/۰۳
تاریخ پذیرش: ۱۳۹۲/۱۲/۲۳

چکیده

امنیت زیرسیستم چندرسانه‌ای IP (IMS) به عنوان هسته اصلی شبکه‌های نسل آتی(NGN)، بسیار حیاتی و مهم است. IMS، یک نمونه معماری در پیاده‌سازی شبکه‌های نسل آتی است که به عنوان هسته اصلی NGN محسوب می‌گردد. با استفاده از این زیرسیستم، کاربران ثابت و سیار به راحتی می‌توانند به سرویس‌های مختلف دسترسی پیدا کنند. بنابراین موضوع تعیین تشخیص تهدیدات و آسیب‌پذیری‌های IMS بسیار مهم است. در حال حاضر برخی از نتایج تحقیقات در مورد پژوهش‌های امنیتی IMS وجود دارد، اما مبتنی بر یک مدل نظام‌مند نمی‌باشد. در این مقاله پس از تجزیه و تحلیل و استفاده از روش مدل‌سازی استاندارد TVRA به اهداف امنیتی مناسب دست یافته و از بین آن‌ها مدل‌های امنیتی جهت دارایی‌های مختلف IMS ارائه شده است. این مدل‌های امنیتی برای پژوهشگران و طراحان شبکه‌های نسل آتی بسیار موثر و حائز اهمیت خواهد بود.

کلید واژه‌ها: *آسیب‌پذیری، اهداف امنیتی، IMS، SIP، NGN*

۱- مربی برق- مخابرات دانشکده علوم ومهندسی دفاعی، دانشگاه افسری امام حسین(ع)، mnnokashti@yahoo.com
۲- استادیار برق- مخابرات دانشکده فاوا، دانشگاه جامع امام حسین(ع)، zrostami@yahoo.com

۱- مقدمه

IMS[۱] یک معماری توسعه یافته به وسیله ۳GPP[۲] است که سرویس‌های چندرسانه‌ای هم‌گرا را در یک شبکه موبایل IPcore ارائه می‌کند. به عبارت دیگر استاندارد IMS به وسیله ۳GPP تعیین شده تا رسماً در معماریNGN به منظور ارائه سرویس‌های چندرسانه‌ای روی شبکه‌های موبایل و ثابت IP مورد استفاده قرارگیرد. این زیرسیستم توسط چند استاندارد جهانی مانند TISPAN، ITU[۳] پذیرفته شده و توسعه یافته است. IMS یک هسته در اجزاء معماری NGN به حساب می‌آید که ارائه سرویس‌های چندرسانه‌ای مبتنی بر SIP در ترمینال‌های NGN را به عهده دارد. سرویس‌های محاوره‌ای از قبیل تلفن صوتی و تصویری، SMS[۴]، Push-to-talk، Share و MMS نمونه‌هایی از سرویس‌هایی هستند که توسط IMS ارائه می‌شوند (۳GPP۲۳۲۲۸ ,۲۰۰۹:۱۷-۲۴).

روشIMS، یک‌پارچگی این سرویس‌ها به یک روش واحد، بر اساس پروتکل اینترنت در شبکه‌های با ساختار دست‌یابی باز و استقلال فناوری دست‌یابی اساسی، در میان ابزارهای مختلف، به صورت هم زمان می‌باشد.

این شبکه، سیگنالینگ SIP را برای کنترل ارتباطات کاربر تا شبکه بین گره‌های سرویس شبکه و سرورها و پروکسی‌ها در نظر گرفته است. در شبکه IMS با توجه به الزامی بودن ثبت‌نام کاربران و اضافه شدن برخی سرآیندها به سیگنالینگ SIP، و با توجه به این که IMS شبکه‌ای با معماری باز است، حمله‌هایی رخ می‌دهد که منجر به آسیب‌پذیری آن می‌شود (Sher M. ,۲۰۰۷:۷-۹). بنابراین برای تجزیه و تحلیل ضعف‌ها و نقاط قوت و هم‌چنین شناسایی آسیب‌پذیری‌های IMS، از مدل استاندارد TVRA، استفاده نموده و در نهایت، مدل‌های امنیتی برای دارایی‌های مختلف شبکه‌های نسل آتی مبتنی بر IMS، پیشنهاد و ارائه می‌نماییم.

۲- روش استاندارد مدل TVRA

برای تحلیل تهدیدها، ریسک‌ها و آسیب‌پذیری‌های یک سیستم ارتباطی، روش طراحی سیستمی تحت عنوان «روش مدل‌سازی TVRA[۵]» توسط استاندارد ETSI TISPAN معرفی و به صورت رسمی ارائه

۱. IP Multimedia Subsystem
۲. Third Generation Partnership Project
۳. International Telecommunication Union
۴. Short Message Service
۵. Threat Vulnerability & Risk Analysis

شده است. این روش، مدلی تعریف شده از سیستم را به همراه تحلیل آن ارائه می‌نماید که بیانگر آسیب‌پذیری‌ها، ضعف‌ها و تهدیدهای آن سیستم است. اطلاعات حاصل از این روشِ تحلیل و مدل‌سازی، با اقدامات پیش‌گیرانه[1] (اقدامات متقابل) در مقابل آسیب‌پذیری‌ها، در پیاده‌سازی یک سیستم کارا بسیار مفید خواهد بود (ETSI TS۱۰۲۱۶۵۱ ,۲۰۰۶) و (ETSI TR۱۸۷۰۰۲ ,۲۰۱۰) و (ETSI TR۱۸۷۰۱۱ ,۲۰۰۸).

روش مدل‌سازی TVRA، بر اساس تجزیه و تحلیل آسیب‌پذیری‌ها، تهدیدها و آنالیز ریسک انجام می‌شود. اصول مدل نمودن در TVRA شامل موضوعات زیر می‌باشد که در شبکه مدل شونده، تعیین و مشخص خواهندشد.(DeMeer J. , ۲۰۱۱: ۳-۷)

اهداف امنیتی[2]:

مشخص نمودن اهداف امنیتی (ابعاد امنیتی) ، اساس بررسی آسیب‌پذیری‌های یک سیستم است. اهداف امنیتی شامل تشخیص هویت، محرمانگی، یک‌پارچگی، حسابرسی، دسترس‌پذیری، کنترل دسترسی، خصوصی‌سازی و امنیت ارتباطی می‌باشد. این اهداف در سیستم، ثابت می‌باشند.

دارایی[3]:

هر چیزی که برای سیستم ارزشمند باشد در این بخش قرار می‌گیرد مثل دارایی فیزیکی (تجهیزات)، دارایی منطقی (اطلاعات موجود در درون تجهیزات).

ضعف[4]:

سیستم‌ها ضعف‌هایی دارند که توسط مهاجمان مورد سوء استفاده قرار می‌گیرند. این ضعف‌ها می‌توانند به عنوان یک تهدید برای سیستم محسوب شوند.

حادثه ناخواسته[5]:

حادثه ناخواسته (اتفاق‌پیش‌بینی‌نشده) نظیر از دست‌دادن محرمانگی، یک‌پارچگی و یا دسترس‌پذیری می‌باشد. به محرمانگی، یک‌پارچگی و تشخیص هویت، مثلث امنیت (CIA) گفته می‌شود چرا که امنیت مبتنی بر این سه عنصر است.

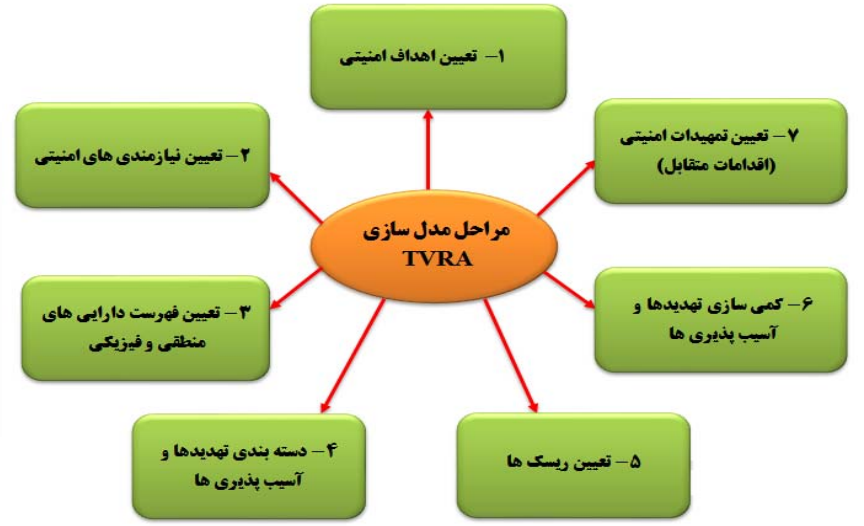
۱. Counter measure
۲. Security Objective
۳. Asset
۴. Weakness
۵. Unwanted Incident

تهدید[1]:

تهدیدهایی مثل شنود که سیستم با آن مواجه می‌باشد می‌تواند موجب زیان به سیستم و یا شبکه شوند.

آسیب‌پذیری[2]:

مجموعه‌ای از ضعف‌های درون سیستم را که می‌تواند توسط مهاجم مورد تهدید قرار گیرد آسیب‌پذیری می‌نامیم. در روش مدل‌سازی TVRA، قدم به قدم مشخصه‌های مختلف یک سیستم بررسی می‌شوند تا ریسک‌ها، حمله‌ها و آسیب‌پذیری‌های آن سیستم به دست آمده و احتمال حوادث مخرب در آن مشخص شوند و اقدامات پیش‌گیرانه از آن‌ها تعیین شود (Collier M. ,۲۰۰۵: ۳). این مدل‌سازی، شامل هفت مرحله مختلف جمع‌آوری، تحلیل و پردازش می باشد که درشکل(۱) نشان داده شده است.



شکل ۱ـ مراحل مدل‌سازی TVRA

شناخت ضعف‌ها، تهدیدها و تحلیل و بررسی آسیب‌پذیری‌های IMS و توجه دادن طراحان در زمان پیاده‌سازی سیستم به این آسیب‌پذیری‌ها، می‌تواند به طراحی و پیاده‌سازی سیستمی امن‌تر منجر شود.

۱. Threat

۲. Vulnerability

۳- اهداف و نیازمندی‌های امنیتی IMS

تعیین اهداف و نیازمندی‌های امنیتی جزء مراحل اولیه مدل‌سازی می‌باشد. اهداف امنیتی، مشخصه‌هایی از سیستم به منظور محافظت از داده‌های انتقالی و یا ذخیره شده در آن است. این اهداف امنیتی طبق استاندارد TS۱۰۲.۱۶۵ شامل تشخیص هویت (احراز هویت)، محرمانگی (قابلیت اعتماد)، یک‌پارچگی (تمامیت داده)، حساب‌رسی و دسترس‌پذیری، و بر اساس استاندارد X.۸۰۵ شامل موارد کنترل دسترسی، خصوصی‌سازی (اختفاء) و امنیت ارتباطی نیز می‌باشد. (ETSI TS۱۰۲۱۶۵۱ ,۲۰۰۶) و (Acharya H. R. ,۲۰۰۷: ۵-۱۱).در ادامه هر کدام از این اهداف امنیتی تعریف شده است.

تشخیص هویت:

تشخیص هویت جزء مراحل ضروری اولیه جهت ارتباط با شبکه است و باعث می‌شود تا شبکه به درخواست‌های غیرمجاز پاسخ ندهد. این کار از طریق مکانیزم‌های تشخیص هویت توافق شده شبکه با کاربر و با توجه به سرآیند Authorization واقع در پیام SIP ارسالی کاربر به سرور P-CSCF صورت می‌گیرد.

محرمانگی:

محرمانگی سیگنالینگ از طریق رمز نمودن پیام‌های ارسالی بین تجهیزات کاربر و پروکسی انجام می‌پذیرد. محتوای پیام از طریق پروتکل انتخابی در زمان ارسال پیام Registration از جانب کاربر می‌تواند به صورت رمزشده باشد. به عنوان مثال در یک بستر IMS، در صورتی که پروتکل ارتباطی کاربر با شبکه IMS روشIMS AKA باشد، ارتباط SIP به صورت رمز شده برقرار می‌شود و محتوای پیام SIP قابل شنود نخواهد بود.

یکپارچگی:

یک‌پارچگی پیام در پروتکل SIP از طریق پروتکل تشخیص هویت IMS AKA و یا از طریقTLS پروتکل لایه انتقال، تعیین می‌شود. در دو روش یاد شده در صورت ایجاد تغییراتی در پیام SIP، سرور S-CSCF قادر به تشخیص تغییر و اصلاح در پیام می‌شود.

حسارسی:

موضوع حساب‌رسی کاربران به معنی قابلیت حساب‌رسی از عملکرد سیستم است. ارتباط هر کاربر با شبکه با تعریف شارژ لازم برای هر کاربر امکان‌پذیر می‌شود. شبکه نیز موظف است به تمامی کاربران مجاز، سرویس مورد نظر را ارائه دهد. این موضوع از موارد مهمی است که در مدل‌سازی، مدنظر قرار می‌گیرد. I-CSCF اطلاعات مربوط به شارژ کاربر را به سرآیند پیغام SIP می‌افزاید.

دسترس‌پذیری:

دسترس‌پذیری در سیستم، اطمینان از دسترسی کاربران مجاز به منابع، سرویس‌ها و کاربردهای سیستم می‌باشد. سیاست‌های امنیتی ارتقای امنیت از طریق اضافه نمودن IDS/SIP و یا تعریف تمهیداتی در بررسی پیام‌های ارسالی از کاربر انجام می‌شود تا از دسترسی کاربر مجاز به منابع و ایمن بودن مسیر دسترسی اطمینان حاصل شود.

کنترل دسترسی:

کنترل‌دسترسی بخش دیگری در اهداف امنیتی است. در صورت ثبت‌نام یک کاربر سرآیندی به نام P-Asserted-Identity توسط P-CSCF به پیام اضافه می‌شود که نشان می‌دهد کاربر ثبت‌نام موفق داشته است و پروکسی‌های دیگر در شبکه از دسترسی این کاربر به امکانات شبکه ممانعت نمی‌کنند.

خصوصی‌سازی:

خصوصی‌سازی یعنی اطمینان از این که، شناسایی و استفاده از شبکه به صورت محرمانه انجام شده و از طریق استفاده از رمزنگاری و یا سرورهای NAT سعی در مخفی نگه داشتن آدرس‌های IP و سایر مشخصات شبکه‌ای می‌شود.

امنیت ارتباطی:

امنیت ارتباطی، اطمینان از انتقال امن یک پیام می‌باشد. ارتباط بین HSS و سرورها از طریق پروتکل‌های IPsec و IMAP امن می‌شود. این پروتکل‌ها در امنیت هسته IMS تعریف شده‌اند.

۴- تعیین فهرست دارایی‌ها و ارزش‌های IMS

در شبکه IMS، دارایی‌های فیزیکی، شامل تجهیزاتِ کاربر (SIP Phone، کامپیوتر و یا تلفن همراه)، سرورهای SIP، پایگاه داده HSS و سرور کاربردی (AS) است. این دارایی‌های فیزیکی شامل کاربردها، محتوا و برنامه‌های نصب‌شده‌ای به نام دارایی منطقی هستند که به کمک آن نقش تجهیزات در سیگنالینگ تعریف می‌شود (Chalamalsetty K. ,۲۰۰۹: ۸-۱۲).

۵- دسته‌بندی نقاط ضعف، تهدیدها و آسیب‌پذیری‌های IMS

نقاط ضعف، عوامل نامطمئنی هستند که در زمان طراحی، پیاده‌سازی، و پیکربندی سیستم وجود دارند و می‌توانند توسط مهاجمان برای طراحی حمله استفاده شوند. به این ترتیب نقاط ضعف تبدیل به آسیب‌پذیری در یک سیستم خواهند شد. با تعیین نقاط ضعف و تهدیدها می‌توان به آسیب‌پذیری‌های یک سیستم دست یافت.

مکانیزم‌های امنیتی تعریف شده در شبکه IMS که با سیگنالینگ SIP در ارتباط می‌باشند، شامل IPSec، TLS، AKA IMS و Early IMS Auth هستند. هر کدام از این روش‌ها، بخشی از امنیت ارتباط با سرور پروکسی SIP را برقرار می‌نمایند. واضح است که این روش‌ها دارای نقاط ضعف و آسیب‌پذیری‌هایی نیز می‌باشد. در ادامه ضعف‌های هر کدام از این روش‌ها تشریح خواهد شد (Sisalem D., ۲۰۰۹, Kuthan J. و Hunter M.T. ,۲۰۰۷).

- **IPSec:** این مکانیزم امنیتی، بین سرور P-CSCF و UE، انتقال امن پیام‌های کاربر را بر عهده دارد. IPSec بر روی IPv۴ و IPv۶ پیاده‌سازی می‌شود. به منظور داشتن IPهای کافی در IPv۴ از یک سرور NAT استفاده می‌شود. به دلیل تغییرات اعمال شده درون NAT بر روی پیام‌های ارسالی، مکانیزم‌های یک‌پارچگی اضافه شده از طریق IPSec به سرآیند پیام SIP مختل می‌شود. این موضوع از نقاط ضعف مکانیزم امنیتی IPSec در سیگنالینگ SIP است.

- **TLS:** مکانیزم دیگری است که در IMS استفاده می‌شود. با مبادله اعتبارنامه‌های کاربران، تشخیص هویت دوسویه در این پروتکل انجام می‌شود. TLS بر روی TCP اجرا می‌شود. در حالی که اولویت ارتباط سیگنالینگ SIP از طریق UDP می‌باشد. به این ترتیب در صورتی که بخواهیم از TLS استفاده نماییم، مجبور می‌شویم تا سیگنالینگ SIP را نیز بر روی TCP منتقل نماییم که این نقطه

ضعف استفاده از مکانیزم امنیتی TLS می‌باشد. درضمن، تعداد زیادی اتصال TCP بین کاربر و P-CSCF به وجود خواهد آمد که ترافیک را افزایش می‌دهد.

- **IMS AKA:** افشای شناسه کاربر زمانی که این شناسه به صورت رمز نشده بر روی کانال ارتباطی منتقل می‌شود، یکی از نقاط ضعف می‌باشد. علاوه بر افشای شناسه کاربر موقعیت و مکان کاربر نیز افشاء می‌شود و محرمانگی موقعیت او را از بین می‌برد و امکان ردیابی آن را توسط مهاجم ایجاد می‌کند. افشای الگوریتم‌های رمزنگاری و یک‌پارچگی و یا به دست آمدن کلیدهای Ck و IK توسط مهاجم نیز ضعف دیگر می‌باشد.

- **Early IMS Auth:** در این نوع از مکانیزم امنیتی، تشخیص هویت بدون IPSec و IPv۶ و بدون داشتن سرآیند Authentication اجرا می‌شود.

۵-۱-تمهیدات امنیتی

سرور پروکسی P-CSCF با دریافت درخواست Invite مسیر ارسال پیام را با آنچه در Record-Route ثبت نموده است، مقایسه می‌نماید. در صورتی‌که این دو مقدار منطبق نباشند، پیام مربوطه حذف شده و ۴۰۰ Bad Request ارسال می‌شود. از این طریق پیام‌هایی که با آدرس مبداء، به جز آدرس مبداء کاربر ارسال می‌شوند، حذف می‌شود و امکان حمله جعل آدرس IP از بین می‌رود. این مکانیزم امکان جعل آدرس IP و دسترسی غیرمجاز به شبکه را سد می‌کند. به منظور مقابله با حمله Middle Man سرور P-CSCF آدرس مسیر طی‌شده توسط پیام را که در Record-Route ذخیره شده است، چک می‌کند. در زمان ثبت‌نام کاربر مسیر پیام Register در HSS ذخیره شده و تحویل S-CSCF می‌شود. این داده‌ها از طریق انتقال پیام ۲۰۰Ok توسط P-CSCF فهرست می‌شود تا انتقال همه پیام‌های رسیده از کاربر مورد نظر از آن مسیر انجام شود.

اگر از سرور P-CSCF پیامی با مسیری به‌جز Record-Route ثبت شده دریافت نماید، آن مسیر را در پیام اصلاح نموده و به مقصد ارسال می‌نماید. در این صورت از Session Hijacking جلوگیری خواهد شد. مهاجم در این حمله، نشست ایجاد شده در یک ارتباط را با تغییر مشخصه‌ها به سمت مهاجم منتقل می‌نماید.

شناسه عمومی کاربر در P-Associated-ID توسط S-CSCF اضافه می‌شود. آدرس S-CSCF معادل هر کاربر در هر مکالمه، توسط Service-route ذخیره شده است. این شناسه در P-CSCF معادل با آدرس مقدار Service-route ذخیره می‌شود. در صورتی‌که مهاجم، پیام Invite یا هر پیام دیگری را (با شناسه Register شده سرقتی) بفرستد پروکسی P-CSCF بدون در نظرگرفتن آن چه که مهاجم در هِدر پیام جعلی خود قرار داده است پیام را با توجه به شناسه موجود و مقدار معادل Service-Route فهرست خود مسیریابی می‌نماید و به مقصد می‌رساند و از ایجاد یک نشست جعلی با مقصدی که مهاجم در نظر دارد جلوگیری می‌نماید.

برای مقابله با حمله Session Hijacking و Register Hijacking، رمز نمودن پیام انتقالیSIP، یکی از راه‌های پیشنهادی می‌باشد.

پروتکل‌های IPSec و TLS برای رمزنمودن پیام‌های انتقالی به کار می‌رود. IPSec رمز نمودن انتها به انتها را انجام می‌دهد اما TLS برای رمز نمودن انتقال بین دو شبکه مفید است. TLS محرمانگی، یک‌پارچگی و تشخیص هویت ارتباط را بر عهده دارد و برای مقابله با Register Hijacking پیشنهاد می‌شود. TLS در ارتباط با شبکه‌های دیگر مورد استفاده قرار می‌گیرد و می‌تواند از شنود پیام Register ممانعت نموده و از افشای شناسه‌های اعتباری کاربر جلوگیری نماید و این از نقاط قوت TLS می‌باشد (Chalamalsetty K. ,۲۰۰۹) و (Deng X. , shore M. ,۲۰۰۹).

۶- ارائه مدل‌های امنیتی مبتنی بر IMS

با توجه به تشریح و شناخت دارایی‌ها، ضعف‌ها، تهدیدها، حوادث ناخواسته و اهداف امنیتی، این موارد را، به صورت جدول (۱) تحت عنوان مدل‌های امنیتی برای شبکه IMS ارائه می‌نماییم. در این جدول، به ترتیب، ضعف، تهدید، حادثه ناخواسته و هدف امنیتی خاص را برای دارایی خاص شبکه IMS، مشخص می‌کنیم. دارایی‌های مشخص در IMS، با توجه به نوع ضعف، تهدید و حادثه خاص، دارای هدف امنیتی مشخصی می‌باشند. جهت درک بهتر مدل‌های امنیتی که در جدول (۱) مشخص شده‌اند، به صورت بلوک دیاگرام‌های جداگانه در شکل‌های (۲) الی (۶)، ترسیم می‌نماییم.

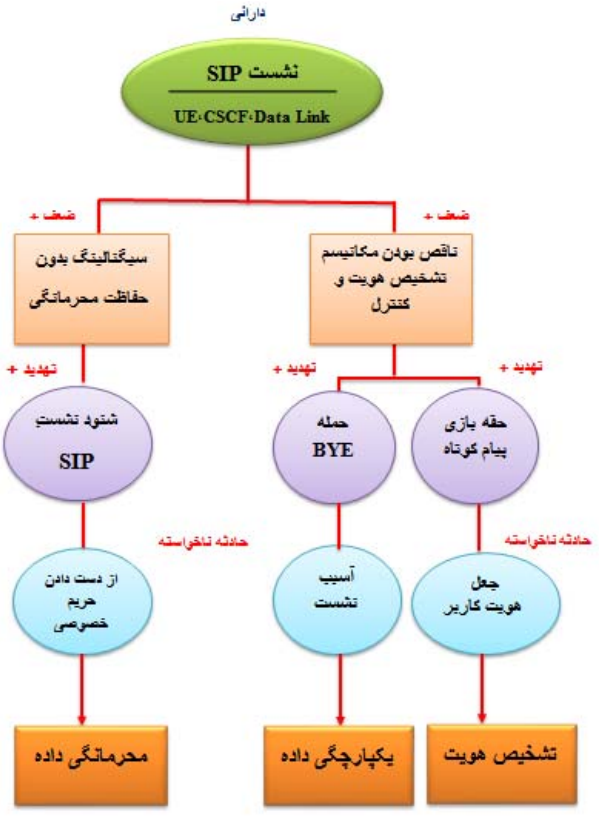
همان‌طور که مشاهده می‌شود به هر گروه از دارایی‌های IMS، ضعف‌ها و تهدیدهایی وارد می‌گردد که باعث بروز حادثه ناخواسته‌ای در سیستم می‌شود. برای مقابله با این حمله‌ها، یک هدف امنیتی مطلوب ارائه می‌شود تا ازآسیب‌پذیری سیستم جلوگیری شود. این بلوک دیاگرام‌ها، هرکدام مربوط به نوع خاصی از دارایی‌های IMS می‌باشند که باید هدف امنیتی خاصی برای آن لحاظ شود.

جدول ۱ـ آسیب‌پذیری‌های IMS به همراه تهدیدات امنیتی معادل

هدف امنیتی	حادثه ناخواسته	تهدید	ضعف	دارایی
محرمانگی داده	از دست دادن حریم خصوصی	شنود نشست SIP	سیگنالینگ بدون حفاظت محرمانگی	نشست SIP
یکپارچگی داده	آسیب نشست	حمله BYE	سیگنالینگ بدون حفاظت محرمانگی	نشست SIP
تشخیص هویت	جعل هویت کاربر	حقه‌بازی پیام کوتاه	ناقص بودن مکانیزم تشخیص هویت و کنترل	نشست SIP
دسترس پذیری	انکار سرویس کاربران	سرریزی ثبت نشست	عدم وجود آدرس IP عمومی برای عناصر شبکه	پشته پروتکل SIP
محرمانگی داده	از دست دادن حریم خصوصی	Scan	ناقص بودن مکانیسم تشخیص هویت و کنترل	ساختار توپولوژی شبکه
دسترس‌پذیری	انکار سرویس کاربران	حمله تزریق SQL	ناقص بودن مکانیسم تشخیص هویت و کنترل	پروفایل کاربر شبکه
محرمانگی داده	سرقت اطلاعات	شنود داده‌های RTP	مسیر انتقال داده، محرمانگی نداشته باشد	سطح کاربر لایه کاربرد
تشخیص هویت	سرقت هویت	حملات Dictionary	حفاظت از هویت، ناقص باشد	سطح کنترل لایه کاربرد

حال در ادامه، طریقه رسیدن به اقدام امنیتی مناسب جهت مقابله با آسیب‌پذیری وارده به سیستم، با توجه به جدول فوق مورد بررسی و تجزیه و تحلیل قرار می‌گیرد.

شکل (۲): در صورتی که دارایی فیزیکی IMS، شامل تجهیزات کاربر، سرور CSCF و اتصال داده و دارایی منطقی IMS نیز شامل نشستِ SIP باشد و در همین حال ضعفی تحت عنوان سیگنالینگ بدون حفاظت محرمانگی و نیز تهدیدی تحت عنوان شنود نشست SIP به سیستم وارد شود که باعث به وجود آمدن حادثه ناخواسته‌ای به نام از دست دادن حریم خصوصی گردد، بهترین اقدام امنیتی برای مقابله با این آسیب‌پذیری، محرمانگی داده است. حال اگر ضعف وارد شده به سیستم برای همین دارایی، ضعفی تحت عنوان ناقص بودن مکانیسم تشخیص هویت و کنترل باشد و تهدیدی به نام حمله Bye به سیستم وارد شود که سیستم دچار حادثه ناخواسته‌ای به نام آسیب نشست شود، مطلوب‌ترین اقدام امنیتی برای مقابله با این آسیب‌پذیری، یکپارچگی (بی نقصی) می‌باشد و چنانچه با همین ضعف وارده، تهدیدی تحت عنوان حقه بازی پیام کوتاه به سیستم وارد شود، سیستم با حادثه ناخواسته‌ای به نام جعل هویت کاربر مواجه می‌شود که بهترین اقدام متقابل برای مقابله با این آسیب‌پذیری، تشخیص هویت است.



شکل ۲ـ آسیب‌پذیری نشست SIP در IMS

شکل(۳): در صورتی که دارایی فیزیکی IMS، شامل تجهیزات کاربر، سرور CSCF و سرور کاربرد، و دارایی منطقی IMS نیز شامل SIP Protocol Stack باشد و در همین حال ضعف سیستم این باشد که عناصر شبکه، آدرس IP عمومی داشته باشند و تهدیدی نیز تحت عنوان سرریزی ثبت نشست (SIP Register Flooding) به سیستم وارد شود که باعث به وجود آمدن حادثه ناخواسته‌ای به نام انکار سرویس کاربران گردند، بهترین اقدام امنیتی برای مقابله با این آسیب‌پذیری، دسترس‌پذیری است.

شکل ۳ـ آسیب‌پذیری پشته پروتکل SIP در IMS

شکل(۴): در صورتی که دارایی فیزیکی IMS، شامل سرور CSCF، سرور داده‌های کاربران و سرور کاربرد، و دارایی منطقی IMS نیز شامل ساختار توپولوژی شبکه باشد و در همین حال ضعفی تحت عنوان ناقص بودن مکانیسم تشخیص هویت و کنترل به سیستم وارد شود و تهدیدی نیز تحت عنوان Scan به سیستم وارد شود که باعث به وجود آمدن حادثه ناخواسته‌ای به نام از دست دادن حریم خصوصی گردند، بهترین اقدام امنیتی برای مقابله با این آسیب‌پذیری، محرمانگی داده است.

شکل ۴ـ آسیب‌پذیری ساختار توپولوژی شبکه در IMS

شکل(۵): در صورتی که دارایی فیزیکی IMS، شامل سرور داده‌های کاربران، و دارایی منطقی IMS نیز شامل پروفایل کاربر شبکه باشد و در همین حال ضعفی تحت عنوان ناقص بودن مکانیسم تشخیص هویت و کنترل به سیستم وارد شود و تهدیدی نیز تحت عنوان حمله تزریق SQL به سیستم وارد شود که باعث به وجود آمدن حادثه ناخواسته‌ای به نام انکار سرویس کاربران گردند، بهترین اقدام امنیتی برای مقابله با این آسیب‌پذیری، دسترس‌پذیری است.

شکل ۵ ـ آسیب‌پذیری پروفایل کاربر در IMS

شکل(۶): در صورتی که دارایی IMS، سطح کاربر لایه کاربرد باشد و مسیر انتقال داده، محرمانگی نداشته باشد (ضعف) و شنود داده‌های RTP به عنوان تهدید به سیستم وارد شود که باعث به وجود آمدن حادثه ناخواسته‌ای به نام سرقت اطلاعات گردند، بهترین اقدام امنیتی برای مقابله با این آسیب پذیری، محرمانگی داده است.

شکل ۶ ـ آسیب‌پذیری سطح کاربر لایه کاربرد در IMS

شکل(۷): در صورتی که دارایی IMS، سطح کنترل لایه کاربرد باشد و حفاظت از هویت، ناقص باشد (ضعف) و حملات Dictionary به عنوان تهدید به سیستم وارد شود که باعث به وجود آمدن حادثه ناخواسته‌ای به نام سرقت هویت گردند، بهترین اقدام امنیتی برای مقابله با این آسیب‌پذیری، تشخیص هویت است.

شکل ۷ ـ آسیب‌پذیری سطح کنترل لایه کاربرد IMS

۷- نتیجه‌گیری

در این مقاله ابتدا ساختار شبکه IMS بررسی شد. سپس به تشریح روش استاندارد مدل‌سازی TVRA، به منظور تجزیه و تحلیل آسیب‌پذیری‌های سیستم پرداخته شد. در ادامه با الگوبرداری از این مدل‌سازی، و هم‌چنین با شناخت ضعف‌ها، تهدیدها، حوادث ناخواسته و بررسی دارایی‌های منطقی و فیزیکی IMS، و در نهایت با تعیین اهداف امنیتی، مدل‌های امنیتی برای دارایی‌های مختلف شبکه IMS، ارائه گردید.

موارد ذکر شده که شامل آسیب‌پذیری دارایی‌های مختلف شبکه IMS به همراه تمهیدات امنیتی مربوطه است به عنوان مدل‌های امنیتی برای دارایی‌های مختلف شبکه IMS به صورت بلوک دیاگرام‌های جداگانه ارائه گردید.

همان‌طور که در این مدل‌های امنیتی مشاهده شد به هر گروه از دارایی‌های IMS، ضعف‌ها و تهدیدهایی وارد می‌شود که باعث بروز حادثه ناخواسته‌ای در سیستم می‌گردد. بنابراین برای مقابله با هر یک از این حمله‌ها، یک هدف امنیتی مطلوب ارائه تا آسیب‌پذیری سیستم کاهش یابد.

کتابنامه

Acharya H. R (۲۰۰۷)," Subscriber Authentication in IMS", Motorola Software Technical Journal, IPCOM۰۰۰۱۵۹۷۹۶d.

Chalamalsetty K. (۲۰۰۹), "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.

Collier M. (۲۰۰۵), "Basic Vulnerability Issuse for SIP Security", whitepaper.

DeMeer J. (۲۰۱۱), "The ETSI TVRA Security-Measurement Methodology by means of TTCN-۳ Notation " , ۱۰th TTCN-۳،User Conference June.

Deng X. , Shore M.(۲۰۰۹), "Advanced Flooding Attack on a SIP Server", the International Conference on Availability, Reliability and Security.

ETSI TS۱۰۲۱۶۵-۱ (۲۰۰۶), Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part ۱: Method and proforma for Threat, Risk, Vulnerability Analysis.

ETSI TR۱۸۷۰۰۲ (۲۰۱۰), Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN) Threat and Risk Analysis.

ETSI TR۱۸۷۰۱۱(۲۰۰۸), Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-۱۵۴۰۸-۲ requirements to ETSI standards –guide, method and application with examples.

Ehlert S., Rebahi Y., and Magedanz T. (۲۰۰۹), "Intrusion Detection System for Denial-of-Service Flooding Attacks in SIP Communication Networks", Intenational Journal of Security in Networks, ۴(۳).

Geneiatakis D. , Kambourakis G. , Dagiuklas T. , Lambrinoudakis C. , Gritzalis S. ,(۲۰۰۵) "SIP Security Mechanisms: A state-of-the-art review" , In Proc. ۵th International MetworkConfernce (INC).

Hunter M.T., Clark R.J. , Park F.S. (۲۰۰۷), "Security Issues with the IP Multimedia Subsystem (IMS)" September.

IETF RFC۳۳۲۹, Arkko j., Torvine V. n, camarillo G., Niemi A.(), HaukkT. A.(۲۰۰۳), “Security mechanism Agreement for the Session Initiation Protocol(SIP)”.

Russell T.(۲۰۰۸), The IP Multimedia Subsystem (IMS) Session Control & Other Network Operations, published by McGraw Hill.

Sher M. (۲۰۰۷), “Secure Service Provisioning(SSP) Framework for IP Multimedia Subsystem(IMS)”, Master Thesis, Electrical engineering and computer science at the Technical University of Berlin.

Sher M., Magedanz T.(۲۰۰۷),” Protecting IP Multimedia Subsystem (IMS) Service delivery Platform From Time Independent Attacks”, The IEEE International Symposium on Information Assurance and Security (ISIAS’۰۷).

Shim D. , Shim C. (۲۰۰۴), “Voice Spam Control with Gray Scaling,” ۱th Workshop on Securing Voice over IP, December.

Sisalem D., Floroiu J., Kuthan J., Abend U., SchulzrinnH. E.(۲۰۰۹), SIP Security, published by Jhon Wiley.

Sisalem D., Kuthan J., Fokus F.(۲۰۰۹), “DENIAL OF SERVICE ATTACKS AND SIP INFRASTRUCTURE, Attack Scenarios and Prevention Mechanisms”.

۳GPP TS۲۳۲۲۸ (۲۰۰۹), ۳rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage ۲ (Release ۱۰).

۳GPP TS۲۴۲۲۹ V۹.۳.۱ (۲۰۱۰-۰۳), ۳rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage ۳ (Release ۹).