تحلیل و بررسی تهدیدهای شبکه VoIP

زهره سلطانی
دانشکده کامپیوتر دانشگاه آزاد
واحد نجف آباد
zohreh.soltani@hotmail.com

دکترمسعود رضا هاشمی
دانشکده کامپیوتر دانشگاه صنعتی
اصفهان
hashemim@cc.iut.ac.ir

دکتر مهران شرفی
دانشکده کامپیوتر دانشگاه آزاد
واحد نجف آباد
Mehran_sharafi@iaun.ac.ir

چکیده: VoIP در ارتباطات امروزه شهرت بسیاری کسب کرده است. سرویس VOIP در شبکه های پر سرعت همچون شبکه اینترنت کار می کند بنابراین هر خطر امنیتی که کامپیوتر را تهدید می کند برای این سرویس نیز وجود دارد. در سیستم های VoIP به علت زیر ساختار منابع ، کیفیت شبکه VoIP مانند شبکه PSTN تضمین نشده است ، همچنین از نظر امنیت، VoIP با مشکلات زیادی روبرو است. دو نوع مختلف آرایش VoIP شامل VoIP در شبکه خصوصی و VoIP بر روی شبکه اینترنت است. با دو چالش که نسبت به سیستم سنتی مهم تر است، روبرو است . کیفیت سرویس و امنیت . زمانی که می خواهیم امنیت سیستم VOIP را تحلیل کنیم ابتدا باید تمام تهدید های ممکن آن سیستم را بررسی کنیم . در این مقاله به بررسی حملاتی که شبکه VOIP را تهدید می کند می پردازیم ، سپس این حملات را تحلیل کرده و درنهایت به اثر این حملات در شبکه VOIP می پردازیم.

واژه های کلیدی: VoIP، حملات، تهدیدات اجتماعی، استراق سمع، تاخیر و تغییر، سوء استفاده از سرویس، وقفه سرویس عمدی.

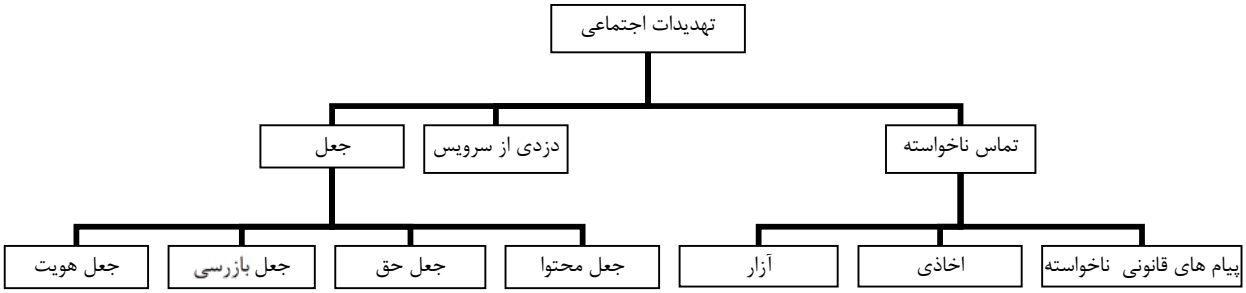
۱- مقدمه

VOIP که با نام IP تلفنی نیز از آن یاد می شود ، امکان استفاده از اینترنت برای مکالمات تلفنی را فراهم می نماید و همواره حملات مختلفی این سرویس را تهدید می کند. به عنوان مثال امکان قطع ارتباط و شنود مکالمات به وسیله افراد نامحرم، دستکاری Caller ID ، دستیابی به اطلاعات محرمانه و مخدوش کردن ارتباط تلفنی نمونه ای از این تهدیدات است. VOIPSA سازمانی است که هدفش بالا بردن امنیت VOIP است . این سازمان در سال ۲۰۰۵ در یک رده بندی جامع تهدیدهای سرویس ها و کاربران را ارائه داد. نکته قابل توجه این است که رده بندی VOIPSA تنها بر روی کاربران و یا فروشندگان تاکید نمی کند، بعضی از این تهدیدها ممکن است بر روی کاربران اعمال شود و نه بر روی فروشندگان . در VOIPSA تهدیدات به شش گروه طبقه بندی می شوند: تهدیدات اجتماعی[1] ، استراق سمع[2]، تاخیر و تغییر[3]، سوء استفاده از سرویس[4]، وقفه سرویس عمدی[5]، بقیه وقفه های سرویس[6]. رده بندی VOIPSA برای تحلیل ریسک کاربرد دارد [۱]. Reykjavik در سال ۲۰۱۱ به تحلیل تهدیدهای سرویس VOIP پرداخت و آن را به گروه های مختلفی تقسیم کرد [۲]. حال به بررسی هر گروه و تهدیدات آن می پردازیم.

۲- تهدیدات اجتماعی

در این تهدید مهاجم خود را به عنوان یک موجودیت مورد اعتماد نشان می دهد و اطلاعات غلط به کاربر نهایی ارائه می دهد . مطابق شکل۱ تهدیدات اجتماعی به سه گروه دسته بندی می شوند.

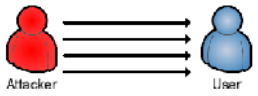
[1] Social Threats
[2] Eavesdropping
[3] Interception and Modification
[4] Service Abuse
[5] Intentional Interruption of Service
[6] Other Interruptions of Service



شکل ۱- تهدیدات اجتماعی

۲-۱ تماس ناخواسته [1]

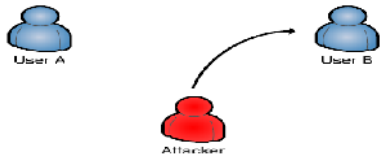
هر تماسی که نیاز به به توافق قبلی برای ورود و یا رد توافق برای تماسهای خارجی باشد و به عنوان تماس خارجی پذیرفته نشود ، تماس ناخواسته نامیده می شود. پیام های قانونی ناخواسته شامل هرزه نگاری قانونی ، تبلیغات و یا پیامهای نا خواسته می باشد. در بیشتر حالات مطابق شکل۲ مهاجم توده ای از پیام های اسپم به کاربر می فرستد که در حدود ۹۵ درصد این ایمیلها به عنوان اسپم شناخته می شود[۳].



شکل۲- حمله مهاجم

۲-۲ جعل [2]

تعریف درست از جعل عبارت است از بیان با لغات که مطابق حقیقت نیستند . همانطور که در شکل مشاهده می شود مهاجم با ارائه اطلاعات غلط به کاربرB ادعا می کند که کاربر A است . مهاجم به منظور رسیدن به اطلاعات غیر قابل دستیابی، دستیابی به تماس و استراق سمع از این روش استفاده می کند و به علت جعل هویت به هدفش دست می یابد .



شکل۳- جعل

۲-۳ دزدی از سرویس [3]

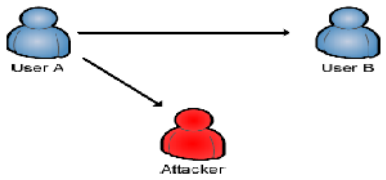
دزدی از سرویس برای هر استفاده ای بدون پرداخت پول انجام می شود. دزدی از سرویس ممکن است با هک کردن سیستم یا با تغییر دادن اطلاعات صورتحساب صورت گیرد. بیشتر حملات اصلی به صورت غیر قانونی خصوصیات تولید کننده سرویس را ارائه می دهد.

---

[1] Unwanted Contact
[2] Misrepresentation
[3] Theft of Service

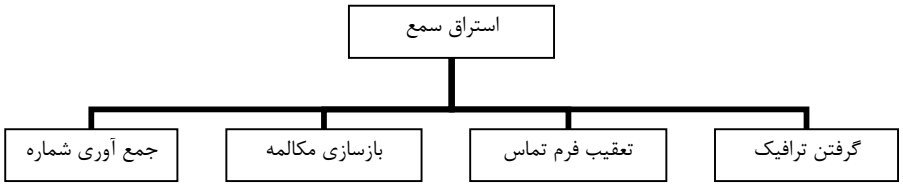
۳- استراق سمع[1]

استراق سمع هنگامی اتفاق می افتد که مهاجم جریان داده را بین دو یا چندین کاربر بدون هشدار یا اعلام اشتراک مـی گـذارد ، همچنـین مطـابق شکل۴ مهاجم به مکالمات بین کاربران دسترسی می یابد .



شکل۴- حمله استراق سمع

مطابق شکل۵ استراق سمع به چهار گروه دسته بندی می شود.



شکل۵- حملات استراق سمع

۳-۱ تعقیب فرم تماس[2]

عبارت است از تعقیب غیر مجاز فرم تماس کاربر . این تعقیب سبب می شود مهاجم اطلاعات تماس قربانی را تحلیل و تجزیه کنـد و از آن بـه نفـع خودش استفاده کند ،به طوریکه مهاجم می تواند مطلع شود که قربانی با چه کسی بوده است و این می تواند در بعضی جهات به مهاجم کمک کند . دلیل این حملات می تواند دزدی ، اخاذی و جاسوسی باشد.

۳-۲ گرفتن ترافیک[3]

در گرفتن ترافیک مهاجم ترافیک ورودی و خروجی را می گیرد و استراق سمع می کند .

۳-۳ جمع آوری شماره[4]

مجموعه ای غیرمجاز شناسه ها است که معمولا به صورت شماره های تلفن هستند. مهاجم تماسهای ورودی و خروجی را مانیتور می کند به منظور آنکه پایگاه داده ای از شناسه های قانونی بسازد. این پایگاه داده ها می توانند برای حملات دیگر از جمله SPIT ، تماسهای کلاه برداری و حملات استفاده شوند.

۳-۴ ترمیم یا بازسازی[5]

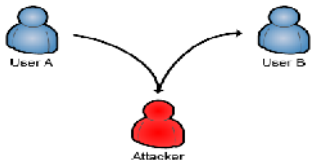
بازسازی به مانیتورینگ ، رکورد ، ذخیره ، شناسایی ، تفسیر ، ترجمه غیر مجاز هر قسمتی از گفتگو رسانه بدون رضایت مالک است.

---

[1] Eavesdropping
[2] Call Pattern Tracking
[3] Traffic Capture
[4] Number Harvesting
[5] Reconstruction

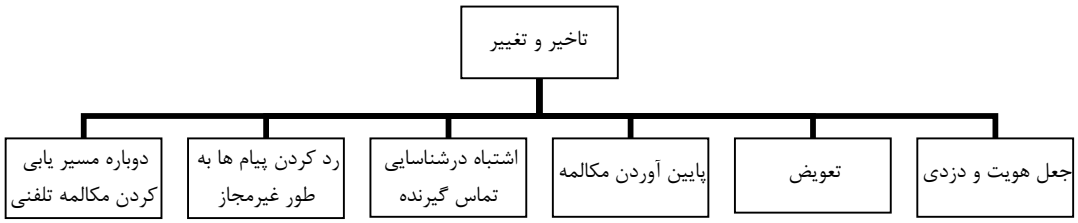
۴- تاخیر و تغییر

تهدیدها در این گروه حملاتی را تعریف می کنند که مهاجم می تواند ترافیک بین دو یا چند نقطه نهایی را به تاخیر بیانـدازد و یـا تغییـر دهـد . در شکل ۵ جایی که مهاجم ترافیک بین دو نقطه را به تاخیر می اندازد ، در سناریو رسم شده است . مهاجم قدرت پیادسازی تهدید ها را دارد.



شکل۶- حمله تاخیر و تغییر

مطابق شکل۷ تاخیر و تغییر به شش گروه دسته بندی می شود.



شکل۷- حملات تاخیر و تغییر

۴-۱ رد کردن پیام ها به طور غیرمجاز

به هر متد غیر مجازی که عنصرهای اصلی VoIP مثلا SIP یا H.323 را تغییر جهت می دهد رد کردن پیام ها به طور غیرمجـاز گفتـه مـی شـود. نتایج این حملات تاخیر در تماس ، خطا در کاربرد ، قطع شدن تماس و به طور کلی رد سرویس می باشد . یک نمونه از این حملات زمانی است کـه مهاجم تمام ورودی از سازمان های خاص از جمله بیمارستان ها ، بانک را رد می کند.

۴-۲ دوباره مسیر یابی کردن مکالمه تلفنی[1]

در این حمله مهاجم با تغییر دادن اطلاعات مسیر یابی ،جهت تماس را از یک یا چندین نقطه نهایی در پیام پروتکل تغییر مـی دهـد . علـت تغییـر مسیر ممکن است به پیام های غیر قانونی در ارتباطات و یا رد کردن پیام های قانونی باشد .

به عنوان مثال هنگامی که مهاجم تماس های ورودی از بانک را دوباره مسیر یابی می کند و تلاش می کند اطلاعات مهم از کاربر را بـه دسـت آورد مثلا شماره PIN

۴-۳ تعویض یا مبادله[2]

همانطور که از اسمش مشخص است به هر تعویض غیر مجاز از ارتباط اشاره می کند. مهاجم بعضی یا تمام ارتباطات بین نقاط انتهایی را عوض مـی کند، به منظور اینکه شناسه را به طور نادرست ارائه دهد و یا اطلاعات نا مناسب تحویل دهد .این حملات می تواند بی نهایت بـرای کـاربر خطرنـاک باشد. در بسیاری از حالات، کاربر گمان می کند با فرد مورد اعتماد صحبت می کند و اطلاعات مهم به مهاجم می دهد.

۴-۴ پایین آوردن مکالمه[3]

[1] Call Rerouting
[2] Alternation
[3] Conversation Degrading

منظور از پایین آوردن مکالمه کاهش غیر مجاز در کیفیت سرویس هر ارتباطی است. مهاجم بسته های رسانه را متوقف می کند و سپس بـه منظـور تولید تاخیر و پراکندگی تاخیر دستکاری می کند. دلیل این حملات ناامیدی کاربر و یا صدمه زدن به اعتبار SP است .

۵-۴ جعل هویت و دزدی[۱]

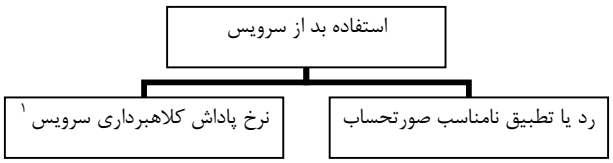
جعل هویت و دزدی شامل هر تغییری در ارتباطات به منظور جعل هویت کاربر مورد اعتماد یا دزدیدن ترافیک به طور کامل است .

۶-۴ اشتباه درشناسایی تماس گیرنده [۲]

در این تهدید مهاجم کاربر را فرا می خواند و سیگنال شناسه نادرست را مدیریت می کند. به عنوان مثال مهاجم خود را به عنوان کارمنـد بانـک یـا فرد مورد اطمینان دیگر معرفی می کند و درخواست شماره PIN یا هر اطلاعات مهم دیگر را می کند . قربانی با احتمال زیاد اگر شماره بانک را ببیند ، این اطلاعات را می فرستد.

۵- استفاده بد از سرویس[۳]

این تهدید هر نوع فعالیت نادرستی را پوشش می دهد. این تهدید مطابق شکل۸ به دو گروه تقسیم بندی می شود.



شکل۸- حملات استفاده بد از سرویس

۵-۱نرخ پاداش کلاهبرداری سرویس [۴]

عمل فریب کسی به گرفتن تماس با شماره جایزه ای که هیچ پاداشی و سرویسی برای آن در نظر گرفته نشده است. شماره جایزه داده شـده مقـدار هزینه بالایی را برای مالک این شماره، به همراه دارد. .مهاجم راههای متعددی برای فریب دادن کاربران به تماس با این شماره دارد و یک راه معروف به وسیله تبلیغات غلط است .

۵-۲ رد یا تطبیق نامناسب صورتحساب[۵]

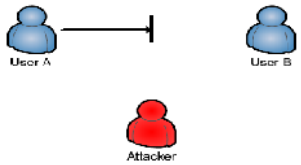
این تهدید هر متد غیر قانونی که سبب جلوگیری از شارژ سرویس یا صورتحساب می شود را شامل می شود.

۶- وقفه سرویس عمدی[۶]

تهدیدات در این گروه همانطور که در شکل۹ دیده می شود، هدفشان ایجاد وقفه برای کاربران در استفاده از سرویس VOIP است . در بیشـتر ایـن حالت ها مهاجم هدف مشخصی ندارد. مهمترین انگیزه برای این حملات عصبانی کردن قربانی است . وقفه برنامه ریزی شده به صورت های مختلفی انجام می شود. تهدید های رد سرویس به خصوص در شبکه VOIP باید در مقیاس وسیعی از تهدید های وقفه برنامه ریزی شده مـورد توجـه قـرار گیرد[۴].

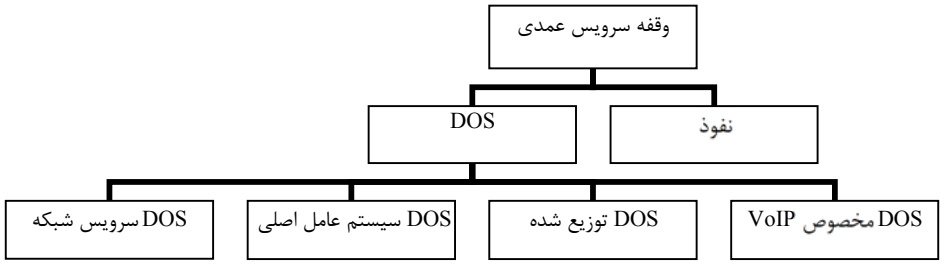
---

[1] Conversation Impersonation and Hijacking
[2] False Caller Identification
[3] Service Abuse
[4] Premium Rate Service Fraud
[5] Improper Bypass or Adjustment to Billing
[6] Intentional Interruption of Service



شکل۹- حمله وقفه سرویس عمدی

لیست تهدید وقفه سرویس عمدی مطابق شکل۱۰ تقسیم بندی می شود.



شکل۱۰- حملات وقفه سرویس عمدی

۱-۶ DOS [1]

رد سرویس یا DOS در دنیای کامپیوتر همانند هکر ها خیلی مشهور هستند و در طی سالیان به صورت های مختلف برای رد کاربران در استفاده از سرویس ها استفاده شده اند.هدف از حملات رد سرویس، غیر قابل دسترس کردن منابع کامپیوتر از کاربرانی که قصد دستیابی به آن را دارند، است .به علت آنکه VoIP بر مبنای IP است و همچنین نسبت به حملات رد سرویس آسیب پذیر است ، راههای مختلفی است که مهاجم می تواند این سرویس را رد کند . این تهدید ها به ۴ گروه تقسیم می شوند[۵]:

۱-۱-۶ DOS توزیع شده [2]

DOS توزیع شده حمله ای است که اغلب هزاران یا حتی میلیون ها کامپیوتر به یک هدف حمله می کنند . معمولا مهاجم از تعدادی کامپیوتر بدون اجازه مالکشان که botnet نامیده می شود، استفاده می کند. این botnet ها توسط یک مدیر کنترل می شوند و قدرتشان برای حمله به یک هدف به کار برده می شود.

۲-۱-۶ DOS سیستم عامل اصلی یا میان افزار [3]

عموما بیشتر سیستم عامل ها مشهور یا میان افزار ها که نسبت به تهدیدهای جدید یا ویروس ها آسیب پذیرترند برای VOIP استفاده می شوند. شرکت ها محصولاتشان را مرتب به روز می کنند، اما هکر ها به صورت راهی برای رخنه به سیستم و آسیب پذیری پیدا می کنند.

۳-۱-۶ DOS سرویس شبکه [4]

در این تهدید مهاجم به اجزاء شبکه یا سرویسی که سرویس های VOIP به آن بستگی دارند ، حمله می کند و به طور مثال باعث سرریزی روتر ها ، سویچ ها و پروکسی ها می شود ، همچنین باعث می شود آنها قادر نباشند به درستی کار کنند و بنابراین هر سرویس VOIP ای که از این اجزاء شبکه می گذرد، متوقف می شود.

---

[1] Denial of Service
[2] Distributed DOS
[3] Underlying operating system or firmware DOS
[4] Network Services DOS

۶-۱-۴ DOS مخصوص VOIP [1]

تمام تهدید ها در این گروه مخصوص VOIP هستند . این تهدیدها از آسیب پذیری پروتکل های VOIP ، نرم افزار کامپیوترهای مقصد استفاده می کنند.

۶-۲ نفوذ فیزیکی [2]

نفوذ فیزیکی تهدیدی را توصیف می کند که شخص غیرمجاز ، با نقشه محافظت شده دست می یابد. اگر آن نقشه به دست مهاجم آید ، با متـدهای مختلف می تواند خرابی جدی در سیستم VOIP به وجود آورد.

این نقشه می تواند در فرم سرمایه در دسترس مثل وسیله یا ساختمان باشد و یا در فرم سرمایه غیر قابل دسـترس مثـل لایـه فیزیکـی مـدل OSI باشد.

۷- نتیجه گیری

همانطور که مشاهده می کنید سیستم VoIP توسط حملات زیادی تهدید می شود. این تهدیدات اثر متفاوتی بر روی سیستم VoIP می گذارند. اثر تهدید جعل بالا است. مهاجم می تواند به اطلاعات مختلفی دست یابد که برای کاربر مضر باشد به عنوان مثال شماره های PIN اطلاعات شرکت و غیره. در تهدید دزدی از سرویس اثر تهدید بی اندازه است. اگر مهاجم بتواند حمله را پیادسازی کند، می تواند سرمایه ای به ارزش میلیون ها دلار دزدی کند. اثر تهدید تماس ناخواسته پایین است. این حمله با احتمال زیاد کاربر را عصبانی می کند و باعث می شود کـاربر تمـاس را رد کند. اثر تهدید تعقیب فرم مکالمه تلفنی پایین است. مهاجم تنها می تواند اطلاعاتی درباره شماره های تماس گرفته شده توسط کـاربر بـه دست آورد وهمچنین تنها می تواند اطلاعاتی درباره ماهیت تماس بدست آورد اما هیچ صراحتی درباره آن تماس وجود ندارد (جاسوسی ، اخاذی). اثر تهدید گرفتن ترافیک متوسط است. مهاجم تنها به مکالمات گوش می دهد اما قادر نیست آن را تغییر دهـد . اثـر تهدیـد جمـع آوری شماره بالا است. اطلاعات در پایگاه داده جمع می شود و برای حملات، مصارف مهمتر و خطرناک اسـتفاده مـی شـود. اثـر تهدیـد بازسازی بسیار بالا است. مهاجم می تواند مکالمات را بگیرد، اطلاعتی روی آن اضافه کند یا آن را تغییر دهد، همچنین هویت آن را جعل کند و به اطلاعات حساس دست یابد به عنوان مثال شماره شناسایی و شماره PIN. اثر تهدید رد کردن پیام ها به طور غیرمجاز و تغییر جهت مکالمـه در مسیر دیگر بالا است. مهاجم می تواند کیفیت سرویس را کاهش دهد و یا تمام سرویس را انکار کند. اثر تهدیـد پـایین آوردن مکالمـه در سایز و اندازه پایین است. مهاجم کیفیت سرویس را به طور موقت کاهش می دهد که برای کاربر ناراحت کننده است ولی تهدیدی برای آن وجـود ندارد. اثر تهدید جعل هویت و دزدی بسیار بالا است. مهاجم می تواند به اطلاعـات ارزشـمند دسـت پیـدا کنـد. . اثـر تهدیـد نـرخ پـاداش کلاهبرداری سرویس پایین است. اگر مهاجم از تهدید به مقدار زیادی استفاده بد کند، توسط SP مورد توجه قرار مـی گیـرد. اثـر تهدیـد غرق تماس کردن کاربر پایین است. این حمله تنها به یک کاربر در یک زمان صورت می گیرد بنابراین ضربه حداقل است، همچنین می تواند بقیـه وسایل از سرویس را از کار بیاندازد (اینترنت و کامپیوتر). اثر تهدید غرق درخواست کردن نقطه انتهایی متوسط است. این حمله هـدفش نقطـه نهایی است، اگر حمله از PSTN بیاید می تواند به پردازشگر تماس ضربه بزند . اثر تهدید پیام ها و درخواست های بد ریخت پـایین اسـت. در یک زمان این حمله کاربر را به هدف می گیرد. . اثر تهدید سوء استفاده از کیفیت سرویس پایین است. این حمله باعـث پـایین آوردن کیفیـت سرویس می شود اما باعث رد یا قطع کردن جریان داده نمی شود . اثر تهدید پیام های تقلیدشده بالا است. مهاجم مـی توانـد از آسـیب پـذیری پروتکل ها برای فرستادن بهره ببرد که مکالمه را وقفه دهد یا به پایان برساند. اثر تهدید دزدی تماس بالا است. این حمله می تواند به طور کلی کاربران را برای گرفتن سرویس منع کند. اثر تهدید رد سرویس های شبکه بسیار بالا است. این حمله بر روی اجزاء شبکه یا سرویس هایی که VOIP به آن بستگی دارد، انجام می شود. حمله موفق می تواند برای چندین کاربر سرویس را خاموش کند. اثر تهدید رد سرویس سیستم عامل اصلی / میان افزار بالا است. این حمله شامل ویروس ها و کرم ها می باشد که حمله بر روی سیستم عامل مـی توانـد سـرویس VOIP را

[1] VoIP specific DOS
[2] Physical Intrusion

خاموش کند. اثر تهدید رد سرویس توزیع شده بی اندازه است. صدها یا هزاران کامپیوتر یا تلفن بدون اطلاع صاحبشان استفاده می شوند تا یک سیستم را غرق درخواست کنند و آن را به طورکامل خاموش کنند. در حالت خاص اگر هدف مرکز تماس اضطراری باشد، خطرناک است . اثر تهدید نفوذ فیزیکی بی اندازه است. اگر مهاجم به مناطق محدود شده دسترسی داشته باشد می تواند به سیستم ضربه بزند. اثر تهدید کمبود برق بسیار بالا است. اگر برق پشتیبان، کار گذاشته نباشد ، سرویس VOIP به طور کامل خاموش خواهد شد. اثر تهدید نقص منابع پایین است. خطا در نرم افزار / سخت افزار می تواند به سرویسVOIP به طور موقتی ضرر بزند . این خطا ها به آسانی با میان افزار جدید و یا به روز کردن سیستم حل می شوند. ویروس ها همچنین باعث نقص و عیب در منابع می شوند و با احتمال زیاد ضرر بیشتری به بقیه قسمتها می زنند. اثر تهدید تاخیر عملکرد شناسایی پایین است. باعث عصبانیت کاربر می شود اما اثر دیگری ندارد. اثر تهدید ناتوانی در گرفتن تماس های اضطراری بسیار بالا است. ناتوانی در تماس اضطراری موجب ضرر جدی یا حتی مرگ تماس گیرنده می شود[۶] [۷].

مراجع

[1] VoIPSA, " VoIP Security and Privacy Threat Taxonomy", 2005.
[2] Reykjavik, "Risk analysis on VoIP systems", master thesis, University of Iceland, Faculty of Industrial Engineering, June 2011.
[3] Phithakkitnukoon.S,Dantu.R, Baatarjav.E, “VoIP Security-Attacks and Solutions”, Information Security Journal,2008.
[4] Persky.D, VoIP Security Vulnerabilities, Sans Institute 2009
[5] Park, "Voice over IP Security", Cisco Press, 2008.
[6] Lawecki, " VoIP Security in Public Networks", University of Stuttgart.
[7] Sengar, H,Wijesekera, D, Wang, H, " VoIP Intrusion Detection Through Interacting Protocol State Machines", International Conference , pp.393-402, 2006.