بسمه تعالی

تهدیدات امنیتی VoIP

فهرست مطالب

1 چکیده

انتقال صدا از طریق پروتکل اینترنت (VoIP[1]) یک فناوری تلفن جدید است که استفاده از آن امروزه به سرعت رو به افزایش است. این فناوری دارای ویژگی‌های بیشتر، انعطاف‌پذیری بالاتر و همچنین هزینه‌ی کمتر نسبت به تلفن‌های سنتی می‌باشد. با این وجود، سیستم‌های VoIP دارای معماری، پروتکل‌ها و پیاده‌سازی پیچیده‌تر می‌باشند و بنابراین امکان استفاده‌ی نادرست از آن‌ها بیشتر است.

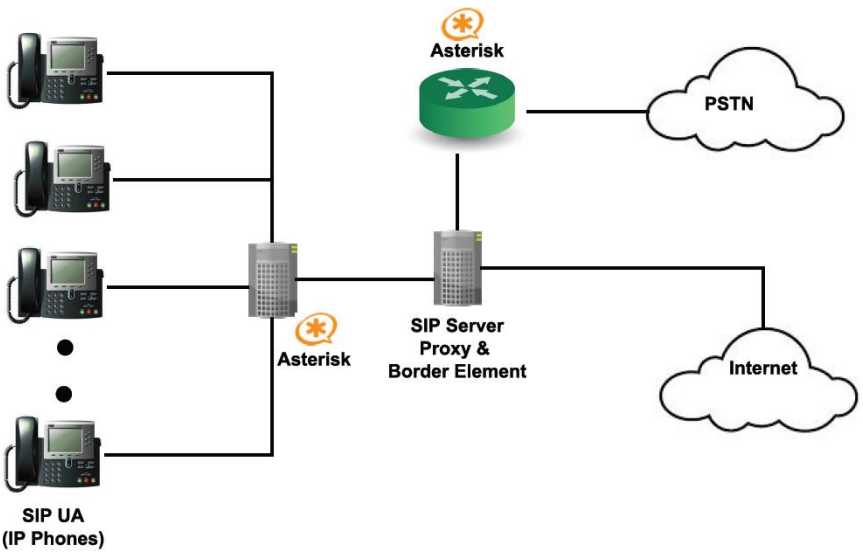
در این گزارش پس از مقدمه‌ای در مورد VoIP و پروتکل‌های استفاده شده در آن، به بررسی تهدیدات و آسیب‌پذیری‌های بالقوه در یک محیط VoIP می‌پردازیم؛ این آسیب‌پذیری‌ها شامل آسیب‌پذیری‌های مربوط به تلفن‌ها و سوئیچ‌ها می‌باشد. همه‌ی تهدیدات در همه‌ی سازمان‌ها وجود ندارند. یک شرکت تجاری ممکن است در درجه‌ی اول نگران کلاه‌برداری باشد در حالی‌که یک اداره‌ی دولتی به منظور حفظ حریم خصوصی یا نگرانی‌های مربوط به امنیت ملی، نیاز به جلوگیری از افشای اطلاعات حساس دارد. تهدیدات و آسیب‌پذیری‌های تشریح شده در این گزارش کلی هستند و ممکن است به همه‌ی سیستم‌ها قابل اعمال نباشند. اما تمامی این آسیب‌پذیری‌ها توسط سازمان‌هایی گزارش شده‌اند که سیستم‌های VoIP را پیاده‌سازی کرده‌اند.

[1] Voice over Internet Protocol

2 ارتباطات چندرسانه‌ای از طریق IP

2-1 مقدمه

ارتباطات چندرسانه‌ای از طریق پروتکل اینترنت، به دلیل سادگی و انعطاف‌پذیر بودن سوئیچینگ بسته از طریق پروتکل اینترنت، به سرعت در حال رشد است. تلفن IP که با نام VoIP شناخته شده است، یکی از موضوعات داغ در این زمینه است. در حالت کلی، سرویس‌های VoIP مبتنی بر پروتکل‌های سیگنالینگ استاندارد (مانند پروتکل آغاز نشست (SIP[2])، H.323، پروتکل کنترل دروازه‌ی رسانه (MGCP[3])) و نیز رسانه‌ی انتقال هستند. یک شبکه‌ی VoIP به صورت کلی در شکل 1 نشان داده شده است.



شکل 1 یک شبکه‌ی VoIP در حالت کلی

2-2 مزایای استفاده از VoIP

VoIP یک سرویس جدید است که به منظور بهبود بخشیدن به ارتباطات صوتی قدیمی از طریق ارتباطات داده‌ای ایجاد شده است. VoIP امکان انتقال داده، تصویر و ویدئو را به صورت همزمان فراهم می‌آورد. در ادامه برخی مزایای استفاده از VoIP به صورت خلاصه آمده است.

---

[2] Session Initiation Protocol
[3] Media Gateway Control Protocol

- **صرفه‌جویی در هزینه:** به جای استفاده از خطوط مخابراتی تجاری، از خطوط داده‌ی شبکه‌ی اینترنت استفاده می‌شود و در نتیجه هزینه‌ی ارتباطی کاهش پیدا می‌کند.
- **قابلیت گسترش:** VoIP به آسانی به هر تعداد از کاربران با هر موقعیت جغرافیایی قابل گسترش است. می‌توان از منابع و شبکه‌های موجود برای پیاده‌سازی آن استفاده کرد.
- **پیاده‌سازی آسان:** ارتباطات صوتی توسط هر سازمان دارای شبکه‌های کامپیوتری قابل پیاده‌سازی است.
- **همکاری و ادغام با دیگر برنامه‌های کاربردی:** به آسانی می‌توان برخی پروتکل‌ها را به صورت مشترک با دیگر برنامه‌های کاربردی استفاده کرد.
- **قابلیت جابجایی سرویس:** کاربران می‌توانند از هر مکانی به سرویس‌های مورد نظر خود دسترسی داشته باشند.
- **واسط کنترل کاربر:** بیشتر سیستم‌های VoIP دارای واسط‌های کنترلی و یا واسط گرافیکی کاربر هستند. این واسط‌ها استفاده از سیستم را برای کاربران آسان می‌نماید.
- **قابلیت حمل تلفن:** کاربران با رفتن یا حرکت به هر مکانی، نیاز به تغییر جزییات ارتباطی خود ندارند.

3 پروتکل آغاز نشست

پروتکل SIP پرطرفدارترین پروتکل سیگنالینگ برای سرویس‌های تلفن مبتنی بر IP می‌باشد. این پروتکل همچنین توسط 3GPP[4] به عنوان پروتکلی برای برنامه‌های کاربردی چندرسانه‌ای در شبکه‌های موبایل 3G، انتخاب شده است. SIP به دلیل انعطاف‌پذیری و قدرت توصیفی خود، نه تنها برای VoIP و تلفن اینترنتی، بلکه برای تعداد زیادی از برنامه‌های کاربردی مبتنی بر نشست مانند اغلب جریان‌های چندرسانه‌ای، چت، و سایر سرویس‌های وب ادغام شده با تلفن و صدا، نیز مورد پشتیبانی قرار گرفته است. SIP (RFC 3261) یک پروتکل سیگنالینگ لایه‌ی کاربرد است که از آن برای ایجاد، تغییر و

[4] Third-Generation Partnership Project

خاتمه‌ی نشست‌های چندرسانه‌ای بین دو یا چند شرکت‌کننده (ممکن است یک تماس تلفنی ساده‌ی دوطرفه باشد یا یک نشست کنفرانس چندرسانه‌ای مشارکتی) در یک شبکه‌ی مبتنی بر IP استفاده می‌شود. این پروتکل یک پروتکل مبتنی بر درخواست-پاسخ است.

همان‌طور که گفته شد SIP یک پروتکل لایه‌ی کاربرد است. این پروتکل می‌تواند انتقال را از طریق TCP/IP یا UDP/IP انجام دهد. SIP قابلیت استفاده در همه‌ی شبکه‌های مبتنی بر IP را دارد. داده‌ی صوتی از طریق پروتکل انتقال زمان حقیقی (RTP[5]) به گیرنده فرستاده می‌شود. بسته‌های RTP در بسته‌های IP قرار داده شده و از طریق اینترنت انتقال پیدا می‌کنند.

1-3 مؤلفه‌های SIP

SIP از یک مدل سرویس‌گیرنده/سرویس‌دهنده پیروی می‌کند که دارای مؤلفه‌های اصلی زیر است:

- **عوامل کاربری (UA[6]):** یک عامل کاربری SIP، یک نقطه‌ی انتهایی منطقی در شبکه است که برای ایجاد یا دریافت پیام‌های SIP و در نتیجه مدیریت یک نشست SIP به کار می‌رود. عامل کاربری خود یک عنصر سرویس‌گیرنده (UAC[7]) و یک عنصر سرویس‌دهنده (UAS[8]) دارد. UAC مسئول ایجاد درخواست‌ها بوده و UAS، پردازش و پاسخ به هر درخواست تولید شده توسط یک UAC را بر عهده دارد. SIP UA می‌تواند شامل سرویس‌گیرنده‌های سبک‌وزن مناسب برای قرار دادن در وسایل کاربر نهایی، مانند گوشی‌های موبایل یا PDAها و یا برنامه‌های کاربردی مانند تلفن‌های نرم‌افزاری باشد.
- **سرویس‌دهنده‌های SIP:** کار اصلی سرویس‌دهنده‌های SIP کمک به عوامل کاربری برای برقرار کردن نشست‌ها و یا انجام دیگر کارها می‌باشد. همچنین ارسال پیام‌ها به

---

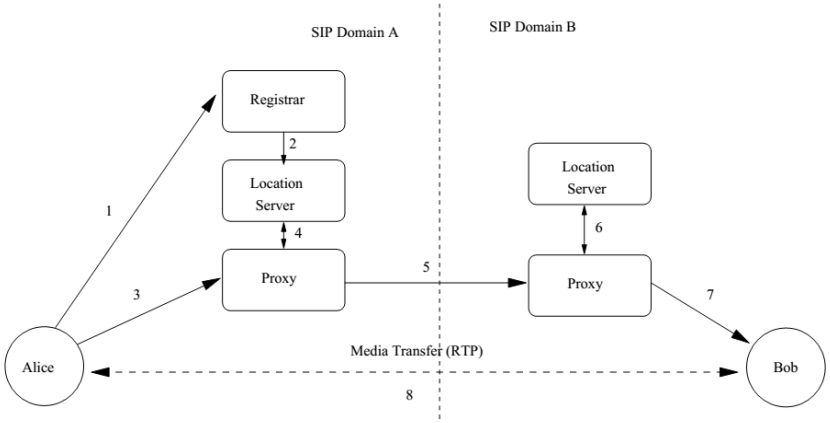
[5] Real-time Transport Protocol
[6] User Agents
[7] User Agent Client
[8] User Agent Server

دیگر سرویس‌دهنده‌ها با استفاده از پروتکل‌های مسیریابی از وظایف این سرویس‌دهنده است.

- **سرویس‌دهنده‌ی پروکسی:** سرویس‌دهنده‌ی پروکسی یک موجودیت میانی است که هم در نقش سرویس‌دهنده و هم در نقش یک سرویس‌گیرنده با هدف ایجاد درخواست‌ها از طرف دیگر سرویس‌دهنده‌ها عمل می‌کند. یک سرویس‌دهنده‌ی پروکسی در اصل مسئول مسیریابی است، یعنی کار آن این است که درخواست را به موجودیت دیگری که نزدیکتر به عامل کاربری هدف است ارسال کند.
- **سرویس مکان:** یک سرویس مکان توسط یک سرویس‌دهنده‌ی پروکسی یا سرویس‌دهنده‌ی تغییر مسیر SIP برای به دست آوردن اطلاعات در مورد موقعیت ممکن پذیرنده‌ی تماس، مورد استفاده قرار می‌گیرد. به این منظور، سرویس مکان یک پایگاه داده از نگاشت‌های آدرس SIP به آدرس IP را نگه‌داری می‌کند.
- **سرویس‌دهنده‌ی تغییر مسیر:** سرویس‌دهنده‌ی تغییر مسیر در طول فرآیند آغاز نشست برای تعیین آدرس وسیله‌ی پذیرنده‌ی تماس استفاده می‌شود. همچنین در مورد هاپ بعدی سرویس‌دهنده به UA تماس‌گیرنده، اطلاع می‌دهد. سپس UA تماس‌گیرنده با هاپ بعدی سرویس‌دهنده به صورت مستقیم تماس برقرار می‌کند.
- **سرویس‌دهنده‌های ثبت‌کننده[9]:** UAها به منظور اعلام حضورشان در شبکه با سرویس‌دهنده‌های ثبت‌کننده تماس برقرار می‌کنند. یک سرویس‌دهنده‌ی ثبت‌کننده‌ی SIP پایگاه داده‌ای شامل مکان‌ها و تنظیمات کاربران است. این سرویس‌دهنده درخواست‌های ثبت‌نام SIP را پذیرفته و اطلاعاتی مانند آدرس SIP و آدرس IP تخصیص یافته را به آن متصل می‌کند.

در شکل 2 تعامل مؤلفه‌های پروتکل SIP در حالت کلی نشان داده شده است.

[9] Registrar servers



شکل 2 تعامل مؤلفه‌های SIP

2-3 آدرس‌های SIP

کاربران در محیط SIP توسط شناسه‌های منبع یکنواخت (URIs[10])، مشخص می‌شوند. قالب یک SIP URI مشابه یک آدرس ایمیل است، این آدرس به صورت کلی شامل یک نام کاربری و نام دامنه است. در واقع، یک SIP URI به یک آدرس ترمینال نگاشت می‌شود. بخش نام کاربری می‌تواند یک رشته یا یک شماره باشد، به عنوان مثال دو آدرس زیر نمونه‌هایی از SIP URI هستند.

sip:bob@chicago.com

sip:1234567890@chicago.com

3-3 قالب پیام‌های SIP

SIP یک پروتکل مبتنی بر متن است، اطلاعات مبادله شده توسط این پروتکل از طریق رشته‌ای از کاراکترها کد می‌شوند. پیام‌های SIP به خطوطی از کاراکترها تقسیم می‌شوند که محدوده‌ی هر خط توسط دو کاراکتر CR[11] و LF[12] (CRLF)، مشخص می‌شود.

دو نوع پیام SIP وجود دارد: پیام درخواست و پیام پاسخ. هر دوی این پیام‌ها شامل یک خط شروع، یک یا چند فیلد سرآیند، یک خط خالی که نشان‌دهنده‌ی انتهای فیلدهای سرآیند است، و

[10] Uniform Resource Identifiers
[11] Carriage Return
[12] Line Feed

یک بدنه‌ی پیام اختیاری هستند. فیلدهای سرآیند از یک نام فیلد تشکیل شده‌اند، سپس کاراکتر ":" آمده و در ادامه مقدار فیلد مشخص می‌شود، در نهایت فیلد با CRLF خاتمه می‌یابد. بدنه‌ی پیام به صورت خیلی ساده از خطوطی از کاراکترها تشکیل شده است.

یک پیام SIP شامل دو نوع سرآیند است، سرآیند اجباری و اختیاری. یک فیلد سرآیند ممکن است برای یک نوع خاص از پیام اجباری باشد در حالی‌که برای سایر پیام‌ها اختیاری باشد. به عنوان مثال، فیلد سرآیند Contact برای یک پیام درخواست INVITE اجباری است در حالی‌که برای سایر پیام‌های درخواست اختیاری است. علاوه بر این، بعضی سرآیندها تنها یکبار می‌توانند در یک پیام ظاهر شوند (مانند From، To، Call-ID و غیره)؛ چندین بار حضور آن‌ها در یک پیام باید منجر به ایجاد خطا شده و پیام باید نادیده گرفته شود. متأسفانه، برخی از این قوانین به صورت کامل در پیاده‌سازی‌های پروتکل SIP در نظرگرفته نمی‌شوند و در نتیجه ممکن است که پیام‌های دارای خطا از یک گره به گره دیگر در شبکه انتقال پیدا کنند.

پروتکل SIP دارای 14 تابع درخواست مختلف می‌باشد (توابع در جدول 1 فهرست شده‌اند) که می‌توانند از طریق یک خط درخواست[13] فراخوانی شوند. شکل 3 یک مثال از پیام درخواست INVITE را نشان می‌دهد که از نظر نحوی درست و از نظر مفهومی بامعنی است. کد پاسخ یک عدد صحیح سه رقمی است که در محدوده‌ی 100 تا 699 می‌باشد و نشان‌دهنده‌ی نوع پاسخ است. شش کلاس از پاسخ‌ها وجود دارد:

- **پاسخ‌های موقت (1xx):** این کدها نشان می‌دهند که درخواست دریافت شده ولی نتیجه‌ی پردازش آن هنوز مشخص نیست.
- **پاسخ‌های موفق (2xx):** این کدها نشان می‌دهند که درخواست به صورت موفقیت‌آمیز پردازش و پذیرش شده است.

[13] Request-line

- **پاسخ‌های تغییر مسیر (3xx):** این پاسخ‌ها برای تغییر مسیر تماس استفاده می‌شوند و معمولاً حامل اطلاعاتی در مورد موقعیت جدید کاربر هستند.
- **پاسخ‌های شکست سرویس‌گیرنده (4xx):** این پاسخ‌ها نشان می‌دهند که مشکل از طرف فرستنده است.
- **پاسخ‌های شکست سرویس‌دهنده (5xx):** این پاسخ‌ها نشان می‌دهند که مشکل از طرف سرویس‌دهنده است.
- **پاسخ‌های شکست سراسری (6xx):** این پاسخ‌ها نشان می‌دهند که درخواست در هیچ سرویس‌دهنده‌ای قابل انجام نیست. به عنوان مثال کاربر اصلاً نمی‌خواهد در نشست شرکت کند.

جدول 1 توضیح توابع SIP

تابع	توضیح
REGISTER	برای ثبت یک حساب کاربری از طریق آدرس IP و URIهای مورد نظر کاربر استفاده می‌شود.
INVITE	برای برقراری یک نشست بین کاربران استفاده می‌شود.
ACK	تبادل قابل اعتماد پیام بین کاربران را تأیید می‌کند.
CANCEL	نشست در حال انجام را لغو می‌کند.
BYE	نشست بین دو کاربر را خاتمه می‌دهد.
OPTIONS	برای به دست آوردن اطلاعات در مورد قابلیت‌های سرویس‌دهنده‌ها، بدون آغاز یک تماس، استفاده می‌شود.
INFO	برای ارسال اطلاعات بین نشست استفاده می‌شود.
PRACK	برای تصدیق پاسخ‌های موقت استفاده می‌شود.
UPDATE	اطلاعات نشست را به‌روز رسانی می‌کند.
REFER	به انتقال یک کاربر به URI کمک می‌کند.
SUBSCRIBE	برای تقاضای هشدار از هشداردهنده استفاده می‌شود.
NOTIFY	برای هشدار مشترک در مورد یک رویداد جدید استفاده می‌شود.
MESSAGE	بدنه‌ی پیام‌ها را انتقال می‌دهد.
PUBLISH	برای انتشار یک رویداد به سرویس‌دهنده استفاده می‌شود.

INVITE sip:user2@server2.com SIP/2.0] Start Line
Via:SIP/2.0/UDP pc33.server1.com;branch=z9hG4bK776
Max-Forwards : 70
To : user2 sip:user2@server2.com
From : user1 <sip: user1@server1.com>;tag=19283017
Call-ID : a84b4c76e66710@pc33.server1.com
CSeq : 3121 INVITE
Contact : sip:user1@pc33.server1.com] Headers

o= user1 2890844526 IN IP4 pc33.server1.com
s = Session SDP
c = IN IP4 157.24.25.137
t = 0 0 : sip:user1@pc33.server1.com
m = audio 49172 RTP/AVP 0
a = rtpmap:0 PCMU/8000] Message Body

شکل 3 مثالی از یک پیام SIP INVITE صحیح

4-3 سیگنالینگ SIP

SIP یک پروتکل مبتنی بر الگوی درخواست-پاسخ است. توالی زیر مثال ساده‌ای از رویه‌ی برقراری تماس در SIP را نشان می‌دهد.

- برای آغاز یک نشست، تماس‌گیرنده (یا UAC) یک درخواست با SIP URI مربوط به بخش پذیرنده‌ی تماس ارسال می‌کند.
- اگر سرویس‌گیرنده موقعیت بخش مقصد را بداند، می‌تواند درخواست را به صورت مستقیم به آدرس IP او ارسال کند. در غیر این صورت سرویس‌گیرنده می‌تواند درخواست را به یک سرویس‌دهنده‌ی شبکه‌ی SIP ارسال کند که به صورت محلی پیکربندی شده است. سرویس‌دهنده تلاش خواهد کرد که مشکل موقعیت کاربر پذیرنده‌ی تماس را حل کرده و درخواست را به او ارسال کند. راه‌های زیادی برای این کار وجود دارد، مانند جستجوی DNS یا دسترسی به پایگاه‌های داده. علاوه بر این، سرویس‌دهنده ممکن است یک سرویس‌دهنده‌ی تغییر مسیر باشد و موقعیت کاربر پذیرنده‌ی تماس را به سرویس‌گیرنده‌ی تماس‌گیرنده برگرداند تا او خود به صورت مستقیم برای برقراری تماس تلاش کند. در حین جریان موقعیت‌یابی یک کاربر، سرویس‌دهنده‌ی شبکه‌ی SIP می‌تواند تماس را به دیگر سرویس‌دهنده‌ها تغییر مسیر داده تا زمانی که به

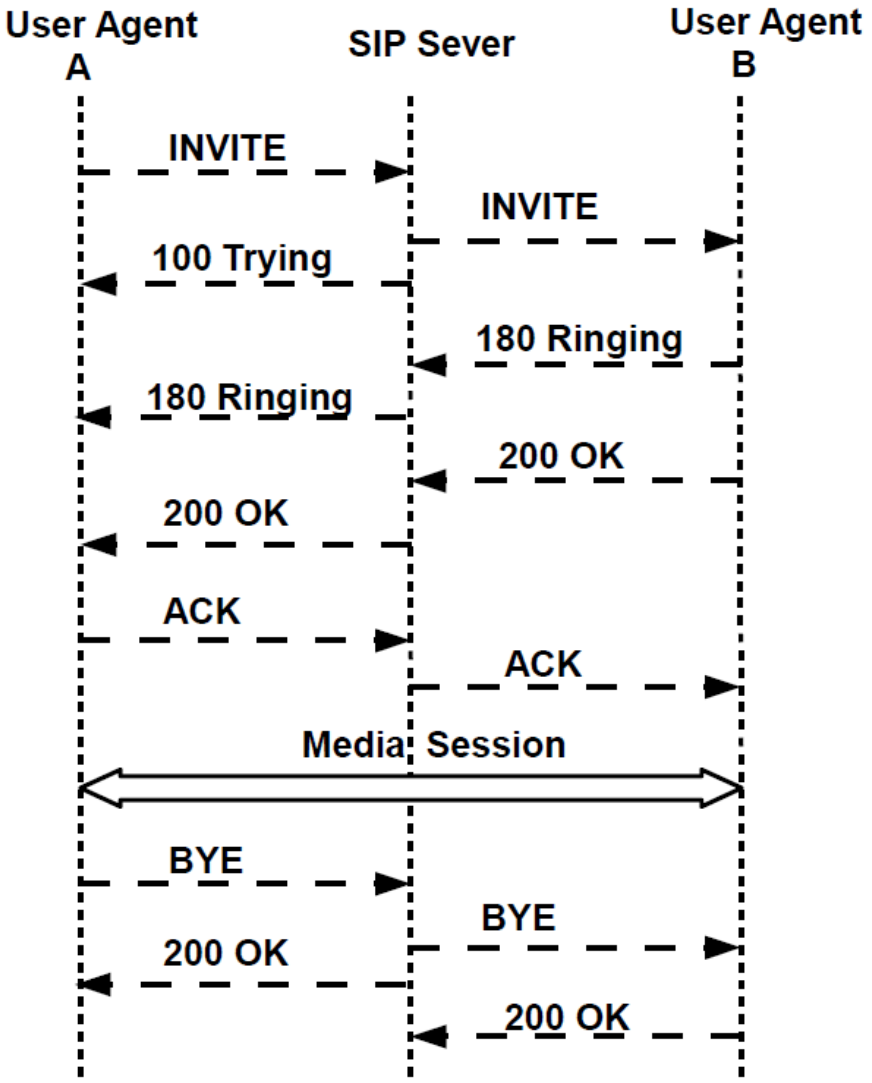
سرویس‌دهنده‌ای برسد که بتواند آدرس IP کاربر پذیرنده‌ی تماس را پیدا کند.

- پس از پیدا کردن کاربر پذیرنده‌ی تماس، درخواست به او ارسال شده و چندین گزینه به وجود می‌آید. در ساده‌ترین حالت، سرویس‌گیرنده‌ی تلفن کاربر درخواست را دریافت کرده و تلفن کاربر زنگ می‌خورد. اگر کاربر پاسخگوی تماس باشد، سرویس‌گیرنده به درخواست پاسخ داده و ارتباط برقرار می‌شود. اگر کاربر تماس را نپذیرد می‌توان نشست را به یک سرویس‌دهنده‌ی پست صوتی[14] یا یک کاربر دیگر تغییر مسیر داد.

5-3 برقراری نشست

شکل 4 یک مثال از فرآیند تماس از عامل کاربری A به عامل کاربری B را نشان می‌دهد. یک نشست زمانی آغاز می‌شود که UAC کاربر A یک پیام INVITE را به سرویس‌دهنده‌ی پروکسی مناسب ارسال می‌کند که در آن تقاضای ارتباط/صحبت با کاربر B را دارد. سرویس‌دهنده‌ی پروکسی فوراً یک پیام پاسخ "TRYING 100" را به UAC کاربر A ارسال کرده تا به او اطلاع دهد که پیام INVITE دریافت شده و تلاش برای پیدا کردن موقعیت کاربر B و ارسال درخواست به UAC او ادامه دارد. در نهایت، وقتی که کاربر B درخواست را دریافت می‌کند و تماس را پاسخ می‌دهد، UAC کاربر B با پیام "OK 200" پاسخ داده و ارتباط برقرار می‌شود. سپس جریان‌های رسانه به صورت مستقیم بین UAC کاربر A و UAC کاربر B مبادله می‌شوند. نشست با ارسال یک پیام BYE از طرف UAC کاربر A یا UAC کاربر B به سرویس‌دهنده خاتمه پیدا می‌کند. این پیام با یک پیام OK 200 از UAC طرف مقابل پاسخ داده می‌شود.

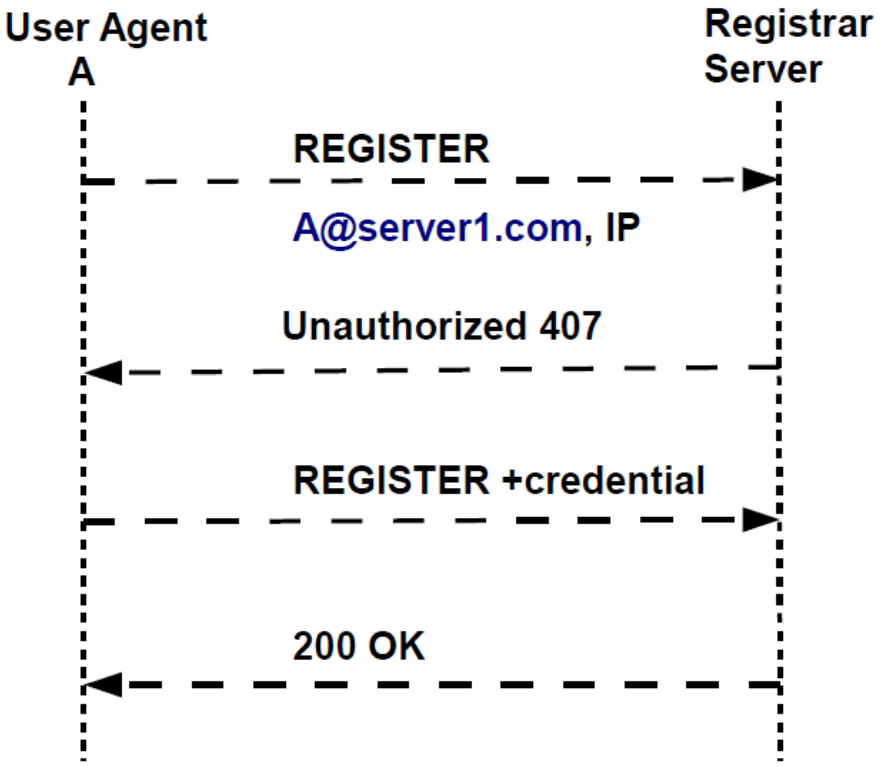
[14] Voice mail server



شکل 4 مثالی از یک نشست چندرسانه‌ای SIP

6-3 ثبتنام SIP

اولین قدم برای یک عامل کاربری برای استفاده از سرویس مبتنی بر SIP این است که موقعیت واقعی خود را در قالب یک آدرس IP معرفی کند. در نتیجه، کاربر نیاز دارد که ترکیب آدرس SIP و آدرس IP فعلی خود را در سرویس‌دهنده‌ی ثبت‌کننده‌ی SIP مربوط به دامنه‌ی خود ثبت کند. یک مثال از روال ثبتنام در شکل 5 نشان داده شده است.



شکل 5 مثالی از روال ثبتنام SIP

4 آسیبپذیریها، تهدیدات و خطرات امنیتی VoIP

همانطور که گفته شد VoIP قابلیت استفاده از شبکه را افزایش داده، هزینه و زمان را کاهش داده و سرویسهای جدیدی را تضمین میکند. VoIP با هزینهی کمتر سرویسها را به مکانهای دور گسترش میدهد. همچنین VoIP سرویسهای چندرسانهای جدیدی مانند مکالمه مبتنی بر PC و کنفرانس چندرسانهای مبتنی بر وب را فراهم میکند.

شبکههای بستهای به منظور موفقیتآمیز بودن عملیات خود نیاز به تعداد زیادی از پارامترهای قابل تنظیم دارند. از آنجایی که VoIP یک شبکهی بستهای محسوب میشود به پارامترهایی مانند آدرسهای IP و MAC مربوط به ترمینالهای صوتی، آدرس مسیریابها و دیوارهای آتش، و نرمافزارهای

مخصوص VoIP مانند مدیریت تماس[15] و دیگر برنامه‌های استفاده شده برای مکان ومسیر تماس نیاز دارد. بیشتر این پارامترهای شبکه‌ای هر زمان که یک مؤلفه‌ی شبکه شروع به کار مجدد می‌کند و یا زمانی که یک تلفن VoIP راه‌اندازی مجدد شده یا به شبکه اضافه می‌شود، به صورت پویا برقرار می‌شوند. از آنجایی که در یک شبکه مکان‌های بسیاری با پارامترهای قابل تنظیم پویا وجود دارند، یک نفوذگر محدوده‌ی وسیعی نقاط آسیب‌پذیر بالقوه را برای حمله پیش رو دارد. در نتیجه، با وجود این‌که VoIP مزایای زیادی دارد، مشکلات امنیتی را نیز پیش روی ما می‌گذارد. در این قسمت به تشریح برخی مسائل امنیتی در VoIP می‌پردازیم. روش‌های مختلف زیادی وجود دارد که برای حمله به VoIP می‌تواند مورد استفاده قرار گیرد. برخی حملات سعی در سرقت اطلاعات دارند در حالی‌که برخی دیگر تلاش می‌کنند تا شبکه را از کار بیاندازند.

1-4 طبقه‌بندی IETF

این قسمت بر اساس طبقه‌بندی حملات VoIP پیشنهاد شده در IETF[16] دنبال شده است. در این طبقه‌بندی تهدیدات امنیتی به چهار بخش تقسیم شده است. در این قسمت فقط آسیب‌پذیری‌ها، تهدیدات و حملات مرتبط به پروتکل SIP شرح داده شده است.

1-1-4 تهدیدات وقفه در سرویس

حملات این دسته پهنای باند شبکه، ظرفیت سرویس‌دهنده یا کیفیت سرویس را مورد هدف قرار می‌دهند. این دسته به صورت عمده شامل حملات جلوگیری از سرویس (DoS[17]) هستند که هدف آن‌ها جلوگیری یا کاهش سطح دسترسی کاربر قانونی به یک سرویس یا منابع شبکه می‌باشد. VoIP نسبت به حملات DoS از سایر سرویس‌های اینترنت حساس‌تر است و این به خاطر ماهیت زمان حقیقی[18] بودن انتقال پیام‌ها است. حملات DoS ممکن است به صورت توزیع شده انجام شوند و وابسته به هدف مهاجم به

[15] Call Manager
[16] Internet Engineering Task Force
[17] Denial of Service
[18] Real time

موجودیت‌های مختلفی هدایت شوند (مانند سرویس‌دهنده‌ها و کاربران نهایی). در ادامه به بررسی حملات DoS شناخته شده در سرویس‌های VoIP مبتنی بر SIP می‌پردازیم.

4-1-1-1 پیام‌های SIP فازی

پیام‌های SIP فازی پیام‌هایی هستند که به نشست‌های SIP معتبر، صحیح و قانونی تعلق ندارند. این پیام‌ها ممکن است زمانی تولید شوند که پیاده‌سازی‌های پروتکل SIP یا برنامه‌های کاربردی به صورت کامل با استانداردها سازگار نیست و یا در کد پیاده‌سازی خطاهایی وجود داشته باشد. علاوه بر این، مهاجمان می‌توانند به صورت هوشمند پیام‌های SIP را دستکاری کنند تا از مشکلات امنیتی موجود در سیستم هدف استفاده برده و یا از نقاط ضعف SIP بهره‌برداری کنند.

به خاطر قالب متنی پیام‌های پروتکل SIP پیام‌های فازی به آسانی قابل تولید هستند. در واقع، روش‌های نامحدودی برای دستکاری پیام‌های SIP وجود دارند. می‌توان آن‌ها را به صورتی تغییر داد که فقط با نحو گرامر تعیین شده توسط پروتکل به صورت کامل مطابقت نداشته باشند (malformed)، و یا از نظر نحوی درست باشند ولی از نظر مفهومی دارای خطاهایی باشند. مثالی از پیام SIP از نوع malformed در شکل 6 نشان داده شده است که در آن آدرس معتبری برای گیرنده وجود ندارد. در حالت معمول، سرویس‌دهنده‌ای که این پیام را دریافت می‌کند باید با "Bad Request" به آن پاسخ داده و آن را نادیده بگیرد. هرچند، تحت شرایط خاص، سرویس‌دهنده ممکن است در پردازش پیام‌های بیشتر با شکست مواجه شود یا در مجموع آن را دچار مشکل کند.

```
INVITE sip: null SIP/2.0
Via:SIP/2.0/UDP pc33.server1.com;branch=z9hG4bK776
Max-Forwards : 70
To :  user2 <sip:user2@server2.com>
From :  user1 <sip: user1@server1.com>;tag=19283017
Call-ID : a84b4c76e66710@pc33.server1.com
CSeq :  312159  INVITE
Contact : null
```

شکل 6 یک مثال از پیام SIP با خطای نحوی

پیام‌های SIP که از نظر نحوی بدون مشکل هستند نیز ممکن است دارای خطاهای مفهومی باشند. این پیام‌ها ممکن است بدون معنی باشند، قابل تفسیر نباشند، مبهم باشند، منجر به بن‌بست شوند و غیره. به عنوان مثال، شکل 7 یک پیام SIP با یک تابع درخواست ناشناخته، یک URI ناشناخته در Request-URI، فاقد فیلد سرآیند الزامی Call-ID، فیلدهای عددی با مقادیر خیلی بزرگ، و چندین ورودی برای سرآیندهایی که باید فقط یک ورودی داشته باشند (مانند سرآیند From)، را نشان می‌دهد. این پیام از نظر نحوی معتبر است اما سرویس‌دهنده‌ای که آن را دریافت می‌کند در پردازش آن با شکست مواجه خواهد شد. ممکن است سرویس‌دهنده تحلیل زمان‌بری را برای تعیین نوع پیام درخواست و اطلاعات مورد نیاز برای تعیین مسیر و پردازش درخواست انجام دهد. علاوه بر این، مهاجمین می‌توانند با وارد کردن اطلاعات بی‌معنی یا اشتباه در فیلدهای مختلف یک پیام SIP، از مشکلات امنیتی موجود در سیستم هدف سوءاستفاده کرده و انواع مختلفی از حملات را انجام دهند. از طرف دیگر، یک کاربر مخرب می‌تواند کد SQL را به پیام‌های SIP تزریق کرده، که با اجرا در سیستم هدف به آن آسیب بزند (مانند به‌روزرسانی یا حذف یک ورودی در جدول شامل اطلاعات کاربری). شکل 8 یک مثال از پیام SIP با تزریق کد SQL توسط یک کاربر مخرب را نشان می‌دهد. هدف این کاربر مخرب به دست آوردن دسترسی غیرمجاز به پایگاه‌داده‌ی پروکسی SIP است.

```
NewMethod unknown: unknown-uri SIP/2.0
Via:SIP/2.0/UDP pc33.server1.com;branch=z9hG4bK776
Max-Forwards : 7593
To : user2 <sip:user2@server2.com>
From : user1 <sip: user1@server1.com>;tag=19283017
CSeq : 312159 NewMethod
Contact : sip:user1@pc33.server1.com
From : user3 <sip: user3@server3.com>;tag=1485717
```

شکل 7 یک مثال از پیام SIP صحیح از نظر نحوی ولی دارای خطای مفهومی

```
INVITE sip:user2@server2.com SIP/2.0
Via:SIP/2.0/UDP pc33.server1.com;branch=z9hG4bK776
Max-Forwards : 70
To :  user2 <sip:user2@server2.com>
From :  user1 <sip: user1@server1.com>;tag=19283017
Call-ID : a84b4c76e66710@pc33.server1.com
CSeq :  312INVITE
Contact :  sip:user1@pc33.server1.com
Authorization:Digest username="malicious';
Update subscriber set first_name='malicious' where
username='malicious'
--realm="195.251.164.23",  algorithm="md5"
```

شکل 8 مثالی از یک پیام SIP که کد SQL در آن تزریق شده است

4-1-1-2 حمله‌ی سیل‌آسا

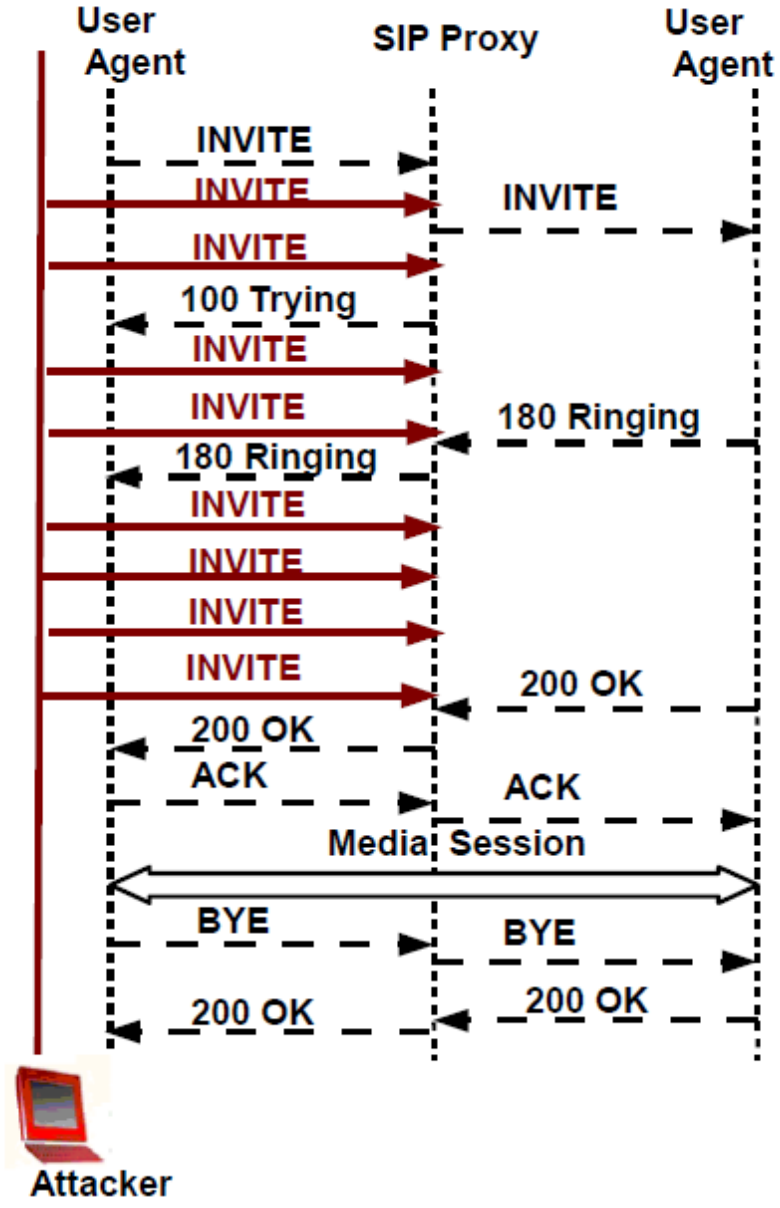
یک سناریوی رایج برای حمله‌ی DoS در VoIP مبتنی بر SIP، حمله‌ی پیام سیل‌آسا است. در این حمله کاربران مخرب تعداد زیادی پیام درخواست INVITE/REGISTER را به سرویس‌دهنده‌ی SIP یا هر موجودیت دیگر در SIP ارسال می‌کنند. بنابراین سیستم هدف به شدت مشغول به پردازش درخواست‌های تماس از کاربران مخرب می‌شود و در نتیجه قادر به پردازش درخواست‌های تماس قانونی نخواهد بود. بسته‌های قانونی یا نادیده گرفته می‌شوند یا با سرعت خیلی پایین پردازش می‌شوند، در نتیجه سرویس VoIP غیرقابل استفاده خواهد بود.

حملات سیل‌آسا همچنین ممکن است با وجود سازوکارهای احرازهویت اتفاق بیفتند. در چنین سناریوهایی، پس از دریافت پیام‌های درخواست INVITE/REGISTER، پروکسی/ثبت‌کننده با یک چالش پاسخ داده و منتظر می‌ماند که درخواست با اطلاعات احرازهویت صحیح دوباره ارسال گردد. مهاجم می‌تواند پیام‌های INVITE/REGISTER را ارسال کرده و سپس فرآیند دست‌تکانی را متوقف کند. در ادامه در مورد دو سناریو از حملات سیل‌آسای رایج توضیح داده شده است.

4-1-1-2-1 حمله‌ی سیل‌آسای INVITE

کاربران مخرب حمله‌ی سیل‌آسای INVITE را با ارسال تعداد زیادی پیام SIP INVITE به سرویس‌دهنده‌ی SIP، ایجاد می‌کنند. توسط این نوع از حمله، سرویس‌دهنده‌ی SIP به شدت مشغول به پردازش این پیام‌های INVITE نادرست از مهاجم می‌شود و در نتیجه قادر به پردازش درخواست‌های تماس قانونی نخواهد

بود. شکل 9 یک مثال از این سناریوی حمله‌ی سیل‌آسای پیام SIP/INVITE را نشان می‌دهد.

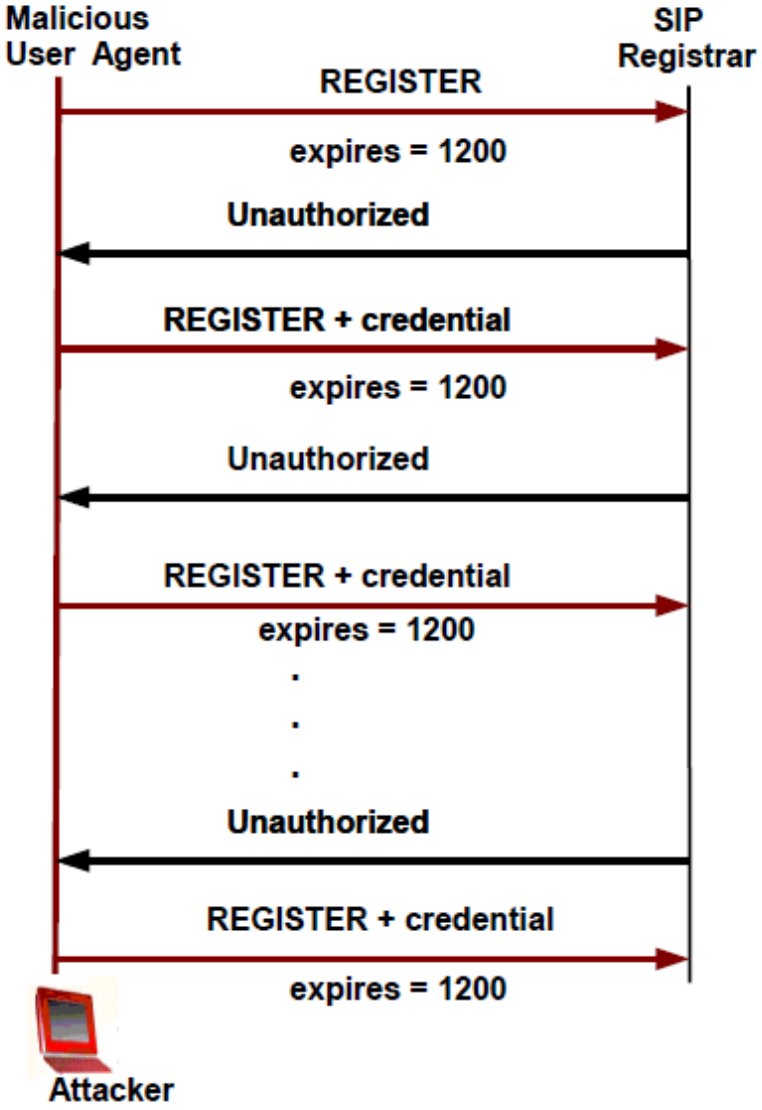


شکل 9 مثالی از حمله‌ی سیل‌آسای پیام SIP/INVITE

4-1-1-2-2 حمله‌ی سیل‌آسای REGISTER

یکی از عناصر اصلی شبکه در زیرساخت‌های VoIP مبتنی بر SIP، سرویس‌دهنده‌ی ثبت‌کننده است که درخواست‌های ثبت‌نام SIP را از کاربران می‌پذیرد. یک درخواست SIP REGISTER، یک انقیاد جدید را بین آدرس SIP کاربر و یک یا چند آدرس تماس (آدرس‌های IP)، اضافه می‌کند. بنابراین کاربر می‌تواند از سرویس تلفن تأمین شده استفاده نماید. زمانی که مهاجم موفق به فلج

کردن ثبت‌کننده شود (به عنوان مثال با ارسال تعداد بسیار زیادی درخواست ثبت‌نام جعلی)، به آسانی موجب یک حمله‌ی DoS می‌شود. یک کاربر مخرب با این هدف این حمله را انجام می‌دهد که کلمه‌ی عبور کاربران قانونی را حدس بزند یا در فرآیند ثبت‌نام سرویس‌دهنده تأخیر ایجاد کند. با مسدود کردن پیام‌هایی که از منابع ناشناخته می‌آیند می‌توان از به وجود آمدن این موقعیت‌ها اجتناب کرد. شکل 10 چنین سناریوی حمله‌ای را نشان می‌دهد.



شکل 10 مثالی از حمله‌ی سیل‌آسا در مقابل سرویس‌دهنده‌ی ثبت‌نام SIP

4-1-1-3 ربودن تماس

ربودن تماس[19] زمانی اتفاق می‌افتد که مهاجم از پیام‌های SIP به منظور ربودن یک تماس موجود به سمت یک پروکسی/نقطه‌ی انتهایی دیگر، استفاده کند. این حمله مستلزم آن است که مهاجم سرآیند SIP مناسب به منظور موفقیت‌آمیز بودن ربودن را جایگزین نماید.

4-1-1-4 تمام کردن تماس

تمام کردن تماس[20] زمانی اتفاق می‌افتد که مهاجم از پیام‌های SIP (به عنوان مثال پیام CANCEL/BYE) به منظور خاتمه دادن به یک تماس موجود استفاده می‌کند. این کار با جایگزین کردن سرآیند SIP مناسب انجام می‌شود.

4-1-1-4-1 حمله‌ی جلوگیری از سرویس CANCEL

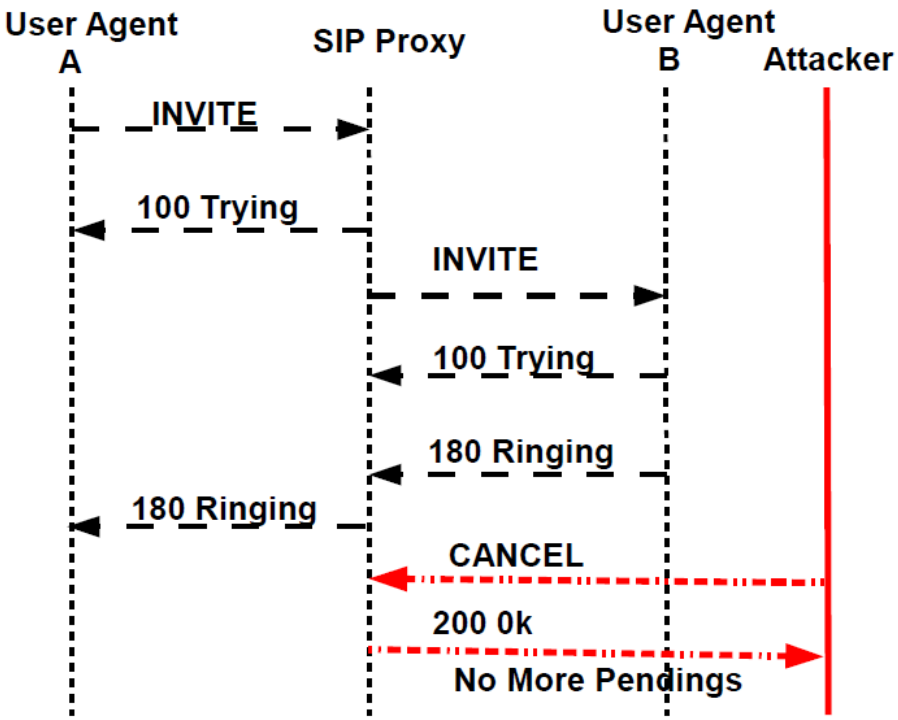
حمله‌ی CANCEL به خاتمه دادن غیرمجاز یک تماس برقرار نشده بین دو کاربر اشاره می‌کند. درخواست CANCEL برای خاتمه دادن به جستجوها یا تلاش‌های تماس منتظر، استفاده می‌شود. به بیان دقیق‌تر، این پیام از UAS می‌خواهد که درخواست پردازش را متوقف کرده و یک پاسخ خطا را برای آن برگرداند. درخواست CANCEL همچنین ممکن است توسط کاربر یا سرویس‌دهنده‌های پروکسی، زمانی که برقراری تماس در حال انجام است تولید شود.

شکل 11 یک سناریوی حمله جلوگیری از سرویس CANCEL را نشان می‌دهد. همان‌طور که مشاهده می‌شود ابتدا برای آغاز یک تماس جدید کاربر A یک پیام درخواست INVITE را به کاربر B ارسال می‌کند. به محض دریافت پیام INVITE، پروکسی SIP کاربر B یک پاسخ "100 Trying" را به A می‌فرستد که نشان‌دهنده‌ی آن است که درخواست تماس در حال پردازش است. وقتی تلفن B شروع به زنگ خوردن می‌کند، یک پیام "180 Ringing" به A فرستاده می‌شود تا او را از در حال انجام بودن برقراری تماس مطلع سازد. در این زمان مهاجم به آسانی می‌تواند یک پیام CANCEL جعلی را به سرویس‌دهنده ارسال کند. بدون احرازهویت مناسب،

---

[19] Call hijacking
[20] Call teardown

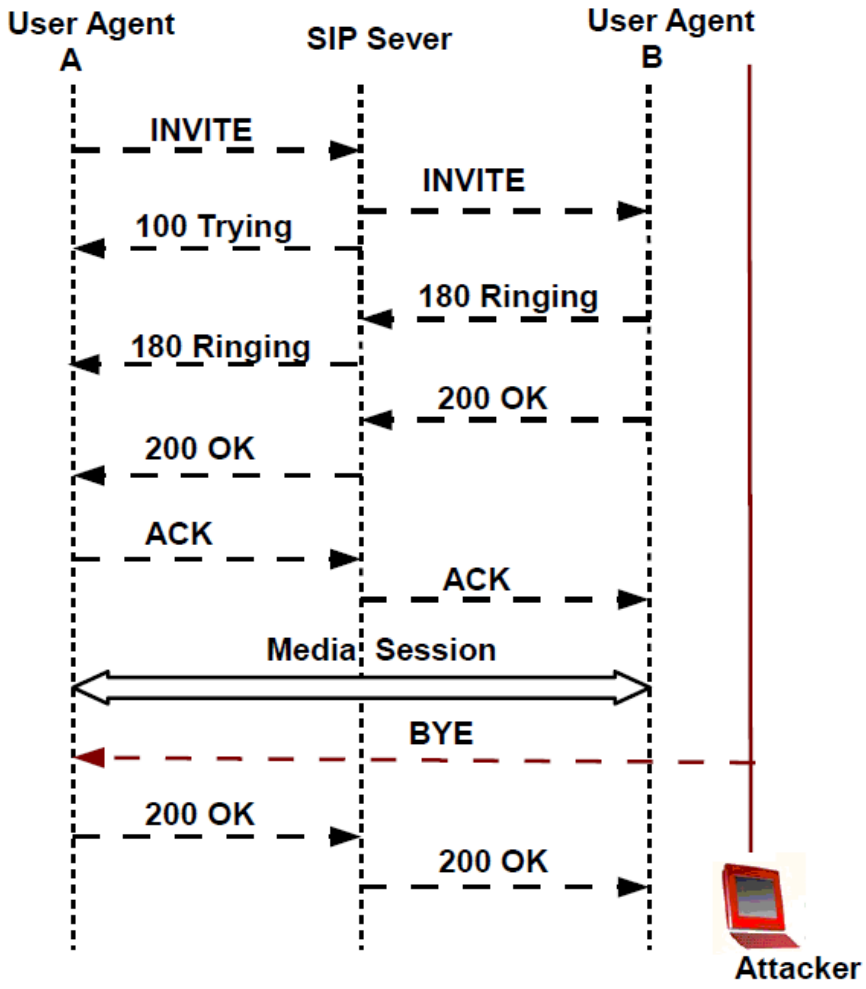
سرویس‌دهنده نمی‌تواند بین پیام CANCEL جعلی و واقعی تفاوت گذارد و بنابراین فرض می‌کند که درخواست CANCEL از یکی از کاربران A یا B ارسال شده است. به محض دریافت پیام CANCEL، سرویس‌دهنده فرآیند برقراری تماس بین کاربران A و B را خاتمه می‌دهد.



شکل 11 مثالی از حمله‌ی جلوگیری از سرویس CANCEL

2-4-1-1-4 حمله‌ی جلوگیری از سرویس BYE

یک نشست برقرار شده بین دو کاربر، به محض دریافت پیام BYE از هر کدام از آن‌ها خاتمه پیدا می‌کند. پیام BYE یک پیام انتها به انتها است که توسط کاربران شرکت‌کننده در نشست فرستاده می‌شود. حمله‌ی BYE به خاتمه‌ی غیرمجاز یک تماس برقرار شده بین کاربران اشاره می‌کند. شکل 12 یک سناریوی حمله‌ی جلوگیری از سرویس BYE را نشان می‌دهد. در این شکل یک تماس بین کاربر A و B با فرآیند دست‌تکانی سه‌مرحله‌ای (پیام‌های INVITE، 200 OK و ACK) برقرار شده است. ناگهان، یک کاربر مخرب یک پیام BYE را به یکی از کاربران A یا B ارسال می‌کند. پس از دریافت این پیام کاربر که نمی‌تواند اصلی یا جعلی بودن آن را تشخیص دهد، آن را اصلی در نظر گرفته و تماس برقرار شده قبل از فرا رسیدن موعد مقرر خاتمه پیدا می‌کند.



شکل 12 مثالی از حمله‌ی جلوگیری از سرویس BYE

2-1-4 تهدیدات استفاده‌ی نادرست از سرویس

مثال‌هایی از چنین تهدیداتی تقلب و اجتناب از پرداخت صورتحساب می‌باشد. بدین ترتیب مهاجم می‌تواند از سرویس‌های تلفن VoIP بدون هیچگونه پرداختی استفاده کند.

- **تقلب تلفنی**[21] : اصطلاح "تقلب تلفنی" در صورتی استفاده می‌شود که یک شخص هزینه‌هایی را با استفاده یک تلفن ربوده شده تولید کند. در این حالت، یک مهاجم می‌تواند خود را به جای یک تلفن IP معتبر جا زده و از شبکه‌ی VoIP برای تماس‌های راه دور رایگان

[21] Toll fraud

استفاده کند. مثال‌هایی از چنین حملاتی ربودن سیستم تلفن یک شرکت توسط یک شخص سوم می‌باشد.

این نوع از حیله‌ها ویژگی‌هایی دارند که آن‌ها را به‌ویژه برای کلاهبردارن جذاب می‌کنند. مهم‌ترین این ویژگی‌ها آن است که خطر محلی‌سازی[22] در این حملات کم است. دلیل این امر این است که کل عملیات از راه دور انجام می‌شود و بنابراین فرآیند محلی‌سازی زمان‌بر و گران است. علاوه بر این به تجهیزات پیچیده‌ای برای انجام آن نیاز نیست.

- **تکرار نشست:** در این حمله مهاجم می‌تواند نشست قبلی یک کاربر را، به منظور دستیابی به منابع غیرمجاز تکرار کند.

4-1-3 تهدیدات رهگیری[23] و تغییر

این تهدیدات موقعیت‌هایی را شامل می‌شود که یک نفوذگر به صورت غیرقانونی و بدون احرازهویت از قسمت‌های مربوطه، به سیگنالینگ (راه‌اندازی تماس) یا محتوای یک نشست VoIP گوش دهد و یا در صورت امکان جنبه‌هایی از نشست، همزمان با اجتناب از شناسایی شدن، را تغییر دهد. حملات استراق‌سمع[24] و مردی در میانه (MITM[25]) در این طبقه قرار می‌گیرند. نمونه‌هایی از این نوع حملات ضبط ترافیک، حفره‌ی سیاه تماس[26]، مسیریابی مجدد تماس، تغییر مکالمه و غیره می‌باشند.

4-1-4 تهدیدات اجتماعی

تهدیدات اجتماعی حملاتی هستند که در محدوده‌ی نمایش اشتباه اطلاعات به همراه تولید ارتباطات ناخواسته با هدف مزاحمت ایجاد کردن برای کاربران و یا حتی دزدیدن اطلاعات شخصی آن‌ها قرار می‌گیرند. این نوع تهدیدها مستقیماً علیه انسان‌ها به کار گرفته می‌شوند. از آنجایی که واژه‌ی

---

[22] Localization
[23] Interception
[24] Eavesdropping
[25] Man In The Middle
[26] Call black holing

ناخواسته به ترجیحات کاربر محدود می‌شود، این تهدیدها را با عنوان اجتماعی طبقه‌بندی می‌کنند. به همین دلیل شناسایی این نوع حملات دشوار می‌باشد. در ادامه به بررسی مثال‌هایی از این نوع حملات می‌پردازیم.

- **SPIT**[27]: این نوع از حملات معمولاً به انتقال ناخواسته‌ی پیام‌های صوتی از طریق بازاریابی تلفنی، فیشینگ[28]، یا تقلب اشاره می‌کند. نوشتن برنامه‌ی کاربردی تولید تماس هرزنامه[29] آسان است. در اغلب موارد تماس‌های هرزنامه توسط ماشین‌های برنامه‌نویسی شده یا باتنت‌ها تولید می‌شوند. به عنوان مثال یک UA در SIP ممکن است آغازگر تعداد زیادی تماس به صورت موازی باشد. اگر یک تماس برقرار شد، برنامه‌ی کاربردی هرزنامه یک ACK را تولید کرده و سپس یک اعلان ضبط شده را پخش می‌کند. پس از اتمام اعلان نیز به تماس خاتمه می‌دهد. این نوع برنامه‌های کاربردی معمولاً به صورت کامل توسط نرم‌افزارها و مؤلفه‌های نرم‌افزاری آماده ساخته می‌شوند، قابل اجرا بر روی یک کامپیوتر شخصی هستند و نیاز به هیچ تجربه‌ی خاصی ندارند.
- **فیشینگ VoIP (Vishing[30])**: واژه‌ی vishing به فیشینگ در محیط VoIP اطلاق می‌شود. در حالت کلی، فیشینگ به حملاتی اشاره می‌کند که مهاجم خود را به جای یک بخش سوم قابل اعتماد جا زده و برای به دست آوردن اطلاعات محرمانه‌ی قربانیان تلاش می‌کند. در محیط VoIP یک مهاجم می‌تواند با جعل یک کاربر یا شرکت، اطلاعات محرمانه‌ی نادرست یا گمراه‌کننده را ارائه داده و به این ترتیب به اطلاعات شخصی و مالی دسترسی پیدا کند. از طرف دیگر، مهاجم می‌تواند با وعده‌ی جایزه دادن به کاربر، او را به یک پاسخگوی

---

[27] Spam over Internet Technology
[28] Phishing
[29] Spam
[30] Voice phishing

صوتی تعاملی (IVR[31]) که مطمئن به نظر می‌رسد هدایت کرده و سعی در به دست آوردن اطلاعات شخصی او نماید.

2-4 طبقه‌بندی NIST

مطابق با طبقه‌بندی NIST حملات روی VoIP محرمانگی، صحت و دسترس‌پذیری را مورد هدف قرار می‌دهند.

1-2-4 محرمانگی و حریم خصوصی

محرمانگی به این مفهوم است که حریم خصوصی اطلاعات، اطلاعات حساس مانند نام کاربری و کلمه عبور، اطلاعات مالی، اطلاعات امنیتی و غیره باید مورد حفاظت قرار گیرد. معمولاً یک حمله روی VoIP با هدف خرابی سرویس، سرقت سرویس و یا از بین بردن حریم خصوصی انجام می‌شود. در سیستم‌های تلفن سنتی حفاظت فیزیکی برای محرمانگی اطلاعات وجود دارد و بنابراین دسترسی به تجهیزات فیزیکی مانند خطوط فیزیکی تلفن و سوئیچ‌های تلفن مشکل است. در حالی‌که در VoIP داده‌ی صوتی از طریق اینترنت انتقال داده می‌شود و بنابراین هر شخص با یک کامپیوتر و یک مودم توانایی دسترسی به داده‌ی صوتی را دارد، همچنین گره‌های زیادی در یک شبکه وجود دارند. بنابراین حفظ محرمانگی در VoIP بسیار مشکل است. آدرس‌های IP شبکه، نوع سیستم‌عامل، نگاشت گسترش[32] تلفن به آدرس IP و پروتکل‌های ارتباطی، مثال‌هایی از اطلاعاتی هستند که ممکن است حساس به نظر نرسند ولی می‌توانند کار مهاجم را آسان‌تر کنند.

1-1-2-4 آسیب‌پذیری کلمه عبور پیش‌فرض

معمولاً سوئیچ‌ها نام کاربری و کلمه عبور پیش‌فرض دارند، مانند root/root یا admin/admin. یک مهاجم با سطح دسترسی به واسط مدیریتی سوئیچ، می‌تواند تمامی بسته‌های روی یک پورت را به دیگری بازتاب دهد. در این حالت اجازه‌ی استراق سمع غیرمستقیم و غیرقابل‌توجه برای همه‌ی ارتباطات فراهم می‌شود. عدم تغییر کلمه‌عبور پیش‌فرض یکی از متداول‌ترین

[31] Interactive Voice Responder
[32] Extension

اشتباهاتی است که توسط کاربران بی‌تجربه انجام می‌شود. در صورت امکان، دسترسی از راه دور به واسط گرافیکی کاربر باید غیرفعال گردد تا از استراق سمع نشست‌های مدیریتی با متن آشکار جلوگیری به عمل آید. برخی دستگاه‌ها علاوه بر دسترسی از راه دور توسط یک واسط مرورگر وب، امکان اتصال مستقیم از طریق USB را نیز فراهم می‌کنند. غیرفعال کردن port mirroring روی سوئیچ را نیز باید در نظر گرفت.

4-2-1-2 آسیب‌پذیری استراق سمع کلاسیک

اضافه کردن یک ابزار ضبط بسته یا تحلیل‌گر پروتکل به شبکه‌ی VoIP، استراق سمع ترافیک صدا را آسان می‌کند. غیرفعال کردن هاب‌ها روی تلفن‌های IP و نیز گسترش یک سیستم هشدار برای مطلع کردن مدیر شبکه زمانی که ارتباط یک تلفن IP با شبکه قطع می‌شود، تشخیص این نوع حمله‌ها را ممکن خواهد کرد.

4-2-1-3 سمی‌سازی حافظه نهان ARP و ARP سیل‌آسا

از آنجایی که اغلب سیستم‌ها احرازهویت کوچکی دارند، یک نفوذگر ممکن است بتواند به یک کامپیوتر در شبکه‌ی VoIP وارد شده و به منظور آسیب رسانی به حافظه‌ی ARP فرستنده‌ی ترافیک دستور ARP را ارسال کند. یک حمله‌ی ARP سیل‌آسا روی سوئیچ می‌تواند شبکه را نسبت به استراق‌سمع گفتگوها آسیب‌پذیر کند. همه‌پخشی پاسخ‌های ARP می‌تواند به تعداد زیادی از حافظه‌های نهان ARP آسیب برساند. آسیب‌رسانی به حافظه‌ی نهان ARP امکان تغییر مسیر ترافیک به منظور شنود ترافیک داده و صدا را فراهم می‌آورد. استفاده از سازوکارهای احرازهویت موجب دسترسی فیزیکی محدود به شبکه‌ی VoIP می‌شود.

4-2-1-4 واسط‌های سرویس‌دهنده‌ی وب

هم سوئیچ‌ها و هم ترمینال‌های صوتی VoIP به احتمال زیاد یک واسط سرویس‌دهنده‌ی وب به منظور انجام کارهای مدیریتی محلی یا از راه دور دارند. ممکن است یک مهاجم بتواند متن آشکار بسته‌های HTTP را شنود کرده و اطلاعات محرمانه را به دست آورد. البته باید به شبکه‌ی محلی که سرویس‌دهنده در آن قرار دارد دسترسی داشته باشد. در صورت امکان نباید از سرویس‌دهنده‌ی HTTP استفاده کرد. در صورت نیاز به استفاده از یک سرویس‌دهنده‌ی وب به منظور انجام کارهای مدیریتی راه دور، استفاده از پروتکل HTTPS مطمئن‌تر است.

4-2-1-5 آسیب‌پذیری Netmask تلفن IP

مانند آسیب‌پذیری حافظه‌ی نهان ARP، مهاجم می‌تواند با تخصیص mask زیرشبکه و آدرس مسیریاب به تلفن موجب شود که بیشتر یا همه‌ی بسته‌های انتقال یافته، به آدرس MAC او ارسال شوند. استفاده از سازوکار فیلتر کردن توسط دیوار آتش، می‌تواند احتمال این حمله را کاهش دهد. همچنین دسترسی راه دور به تلفن‌های IP یک خطر جدی است.

4-2-1-6 آسیب‌پذیری نگاشت گسترش به آدرس IP

کشف آدرس IP متناظر با یک گسترش تنها به یک تماس با آن گسترش و گرفتن پاسخ نیازمند است. یک تحلیل‌گر پروتکل یا ابزار ضبط بسته که به هاب روی دستگاه تماس اضافه شده باشد، این توانایی را دارد که به مجرد برقراری تماس بسته‌های ارسالی از دستگاه هدف را مشاهده کند. دانستن آدرس IP یک گسترش خاص در حالت عادی اهمیتی ندارد اما موجب می‌شود که سایر حمله‌ها آسان‌تر انجام شود. به عنوان مثال اگر یک مهاجم بتواند بسته‌های شبکه‌ی محلی را از طریق سوئیچ استراق‌سمع کند، با داشتن آدرس IP تلفن هدف به آسانی می‌تواند بسته‌های ارسال شده و دریافت شده توسط او را تشخیص دهد. بدون دانستن آدرس IP تلفن هدف، انجام عملیات مهاجم خیلی دشوارتر شده و به زمان بیشتری نیاز خواهد داشت. این زمان بیشتر ممکن است منجر به کشف حمله شود. با غیرفعال کردن هاب بر روی تلفن IP می‌توان از این نوع حمله جلوگیری کرد.

4-2-2 صحت

صحت اطلاعات به این مفهوم است که امکان دستکاری آن‌ها توسط کاربر غیرمجاز وجود ندارد. به عنوان مثال، کاربران خواستار این هستند که از عدم تغییر شماره حساب بانکی‌شان مطمئن باشند و یا کلمات عبور تنها باید توسط کاربر یا مدیر امنیتی مجاز تغییر داده شود. سوئیچ‌های مخابرات باید از صحت داده‌ها و پیکربندی سیستم خود محافظت نمایند. با توجه به توانمندی مجموعه ویژگی‌های موجود در سوئیچ‌ها، یک مهاجم با آگاهی از پیکربندی سیستم می‌تواند به سرعت به سایر اهداف خود دست یابد. به عنوان مثال، آسیب‌رسانی یا حذف اطلاعات مربوط به IP شبکه استفاده شده توسط یک سوئیچ VoIP منجر به یک حمله‌ی فوری جلوگیری از سرویس می‌شود.

خود سیستم امنیتی می‌تواند قابلیت استفاده‌ی نادرست از سیستم را به وجود آورد. علاوه بر این محدود کردن قابلیت ردیابی و قرار دادن درهای پشتی برای نفوذگران که از آن‌ها در دیدارهای بعدی خود استفاده کنند، نیز از دیگر قابلیت‌های سیستم امنیتی است. به این دلیل، سیستم امنیتی باید به دقت مورد حفاظت قرار گیرد.

تهدیدهای صحت شامل هر تهدیدی است که در آن توابع سیستم یا داده‌ها، به صورت تصادفی و یا در نتیجه‌ی یک عملیات مخرب، ممکن است آسیب ببینند. استفاده‌ی نادرست ممکن است توسط کاربران قانونی یا نفوذگران انجام شود.

یک کاربر قانونی ممکن است یک تابع عملیاتی نادرست یا غیرمجاز را انجام دهد و موجب تغییرات زیان‌بار، حذف، یا افشای داده و نرم‌افزار سوئیچ گردد. این تهدید به دلایل مختلفی به وجود می‌آید، به عنوان مثال ممکن است سطح دسترسی تخصیص به یک کاربر بیشتر از مقدار نیاز او برای انجام فعالیت‌هایش باشد.

نفوذ- یک نفوذگر ممکن است خود را به عنوان یک کاربر قانونی نشان داده و عملیات مربوط به کاربر قانونی را انجام دهد. به عنوان مثال، نفوذگر ممکن است از سطح مجوز یک کاربر قانونی استفاده کرده و از طریق انجام عملیات زیر به سیستم آسیب بزند:

- افشای اطلاعات محرمانه.
- تخریب سرویس با دستکاری نرم‌افزار سوئیچ.
- سقوط سوئیچ.
- حذف تمام اثرات نفوذ (به عنوان مثال با دستکاری لاگ‌های امنیتی) به منظور کاهش احتمال شناسایی نفوذ.

وضعیت نا امن- یک سوئیچ در زمان‌های خاصی ممکن است، به دلیل قرار نگرفتن در یک وضعیت امن، آسیب‌پذیر شود. به عنوان مثال:

- پس از شروع به کار مجدد سیستم، ویژگی‌های امنیتی قدیمی ممکن است به وضعیت پیش‌فرض و نا امن تنظیم شده باشند و ویژگی‌های جدید تخصیص پیدا نکرده باشند. (به عنوان مثال، همه‌ی کلمات عبور قدیمی به کلمه عبور پیش‌فرض سیستم برگردانده شده باشد، درحالی‌که کلمات عبور جدید تخصیص پیدا نکرده است.) این مشکل به

هنگام بازیابی اطلاعات سیستم پس از وقوع یک حادثه نیز ممکن است به وجود آید.

- سوئیچ به هنگام نصب و تا زمانی که ویژگی‌های امنیتی پیش‌فرض آن تغییر داده نشده است، آسیب‌پذیر است.

4-2-2-1 حمله‌ی قرار دادن سرویس‌دهنده‌ی DHCP

در اغلب موارد این امکان برای مهاجم وجود دارد که با بهره‌برداری از پاسخ‌های DHCP که در زمان راه‌اندازی یک تلفن IP ارسال می‌شود، پیکربندی تلفن هدف را تغییر دهد. به محض این‌که تلفن IP درخواست یک پاسخ DHCP کرد، سرویس‌دهنده‌ی DHCP جعلی می‌تواند یک پاسخ با فیلدهای داده‌ای که شامل اطلاعات نادرست است برای او ارسال نماید. این حمله می‌تواند منجر به حمله‌ی مردی در میانه بر روی دروازه‌ی IP-رسانه و تلفن‌های IP شود. روش‌های زیادی برای راه‌اندازی مجدد تلفن از راه دور وجود دارد. به عنوان مثال می‌توان به ping سیل‌آسا و MAC spoofing اشاره کرد.

برای جلوگیری از این نوع حملات در صورت امکان باید از IP ایستا برای تلفن‌های IP استفاده کرد. در این صورت ضرورت استفاده از سرویس‌دهنده‌ی DHCP از بین می‌رود. علاوه بر این، با استفاده از یک سیستم تشخیص نفوذ مبتنی بر وضعیت می‌توان بسته‌های سرویس‌دهنده‌ی DHCP را فیلتر کرد و دریافت این بسته‌ها را فقط از سرویس‌دهنده‌ی قانونی مجاز در نظر گرفت.

4-2-2-2 حمله‌ی قرار دادن سرویس‌دهنده‌ی TFTP

این امکان برای مهاجم وجود دارد که با بهره‌برداری از پاسخ‌های TFTP[33] که در زمان تنظیم مجدد یک تلفن IP ارسال می‌شود، پیکربندی تلفن هدف را تغییر دهد. یک سرویس‌دهنده‌ی TFTP جعلی می‌تواند قبل از این که سرویس‌دهنده‌ی قانونی قادر به ارسال پاسخ باشد، اطلاعات جعلی را ارسال نماید. این حمله به مهاجم امکان تغییر در پیکربندی تلفن IP را برای مهاجم به وجود می‌آورد. مشابه با حالت قبل، با استفاده از یک سیستم تشخیص نفوذ مبتنی بر وضعیت می‌توان بسته‌های سرویس‌دهنده‌ی TFTP را فیلتر کرد و دریافت این

[33] Trivial File Transfer Protocol

بسته‌ها را فقط از سرویس‌دهنده‌ی قانونی مجاز در نظر گرفت. سازمان‌هایی که به دنبال راه‌اندازی سیستم‌های VoIP هستند باید به دنبال ابزارهایی برای تلفن IP خود باشند که بتوانند فایل‌های دودویی امضا شده را دانلود کنند.

در سناریوهای VoIP، آسیب رساندن به صحت داده‌ها روی سرویس‌دهنده موجب حملاتی نظیر جلوگیری از سرویس می‌شود.

4-2-3 دسترس‌پذیری و جلوگیری از سرویس

دسترس‌پذیری به این مفهوم است که سرویس‌ها، اطلاعات و منابع همیشه به هنگام نیاز کاربران مجاز، در دسترس باشند. دسترس‌پذیری بزرگترین خطر آشکار برای یک سوئیچ است. حملاتی که از آسیب‌پذیری‌های نرم‌افزاری سوئیچ یا پروتکل‌ها استفاده می‌کنند ممکن است منجر به کاهش کارایی سوئیچ و یا حتی جلوگیری از سرویس شوند. به عنوان مثال اگر یک دسترسی غیرمجاز به هر شاخه از کانال ارتباطی (مانند لینک CCS یا لینک TCP/IP)، صورت پذیرد، ممکن است که لینک با پیام‌های جعلی موردحمله‌ی سیل‌آسا قرار گرفته و منجر به خرابی یا قطع سرویس شود. یک سیستم VoIP ممکن است آسیب‌پذیری‌های بیشتری از طریق ارتباطات اینترنت داشته باشد. از آنجایی که سیستم‌های تشخیص نفوذ از رهگیری درصد قابل توجهی از حملات مبتنی بر اینترنت ناتوان هستند، مهاجمین قادر خواهند بودند که با بهره‌گیری از ضعف‌های موجود در پروتکل‌ها و سرویس‌های اینترنت، سیستم‌های VoIP را از کار بیاندازند.

هر شبکه‌ای ممکن است با سرریز شدن حافظه‌ی سیستم، نسبت به حملات جلوگیری از سرویس آسیب‌پذیر باشد. از آنجایی که VoIP نسبت به از بین رفتن بسته و تأخیر بسیار حساس است، این حمله در آن به مراتب شدیدتر است.

4-2-3-1 حمله‌ی مصرف منابع CPU بدون اطلاعات حساب

یک مهاجم با دسترسی از راه دور به سرویس‌دهنده، ممکن است قادر به شروع مجدد سیستم شود. این کار را می‌توان با تأمین حداکثر تعداد کاراکترهای لازم برای پر شدن بافر نام کاربری و کلمه عبور، به صورت متوالی، انجام داد. در نتیجه‌ی این حمله ممکن است تلفن‌های IP راه‌اندازی مجدد شوند.

شروع مجدد نیز مانند قطع برق سیستم ممکن است منجر به تغییرات غیرقابل بازیابی و یا بازیابی کلمات عبور پیش‌فرض

شود و در نهایت آسیب‌پذیری‌های نفوذ را در پی داشته باشد. با استقرار یک دیوار آتش می‌توان مانع از ارتباطات غیرضروری و یا ارتباطات از موجودیت‌های ناشناخته شد و تا حد امکان بر این مشکل غلبه کرد. هرچند هنوز این امکان برای مهاجم وجود دارد که با کلاه‌برداری آدرس MAC و IP، حفاظت‌های انجام شده توسط دیوار آتش را دور بزند.

2-3-2-4 سوء استفاده از معایب نرم افزاری

مانند سایر نرم افزارها، سیستم های VoIP نیز به دلیل سرریزی بافر و مدیریت نادرست سرآیند بسته دارای آسیب‌پذیری‌هایی هستند. این معایب به صورت عمده به این دلیل به وجود می‌آید که نرم افزار اطلاعات حساس را به صورت صحیح پیکربندی نمی‌کند. به عنوان مثال ممکن است یک عدد صحیح کوتاه به عنوان شاخص جدول انتخاب شود بدون بررسی این‌که آیا پارامتر ارسال شده به تابع از 32767 بیشتر می‌شود یا خیر. در نتیجه یک دسترسی نامعتبر به حافظه یا متوقف شدن سیستم اتفاق می افتد.

در حالت کلی، سوء استفاده از معایب نرم‌افزاری می‌تواند منجر به دو نوع آسیب‌پذیری شود: جلوگیری از سرویس یا افشای پارامترهای حساس سیستم. جلوگیری از سرویس اغلب از راه دور پیاده‌سازی می‌شود. این کار با ارسال بسته‌هایی با سرآیندهای ایجاد شده‌ی خاص انجام می‌شود که می‌تواند منجر به سقوط سیستم شود. در برخی موارد وقتی که یک سیستم سقوط می‌کند، یک memory dump ایجاد می‌شود و نفوذگر می‌تواند آدرس‌های IP گره‌های حساس سیستم، کلمات عبور و یا اطلاعات امنیتی سیستم را به دست آورد. علاوه بر این، مانند دیگر برنامه‌های کاربردی، سرریزی بافر ممکن است منجر به پیدا شدن کدهای مخرب در نرم افزار VoIP شود.

این مشکلات نیاز به اقداماتی توسط فروشنده نرم افزار و توزیع وصله[34] ها به مدیران دارد. نفوذگران بر اعلان آسیب‌پذیری‌ها نظارت می‌کنند و می‌دانند که اغلب سازمان‌ها به روزها یا هفته‌ها برای به‌روزرسانی نرم افزارشان نیاز دارند. بررسی منظم برای به‌روز رسانی‌های نرم افزاری و نیز

[34] Patch

وصله‌ها، به منظور کاهش این آسیب‌پذیری‌ها الزامی است. بررسی خودکار وصله‌ها می‌تواند به کاهش فرصت نفوذگر برای بهره‌برداری از آسیب‌پذیری نرم‌افزاری شناخته شده کمک کند.

4-2-3-3 آسیب‌پذیری قفل شدن حساب

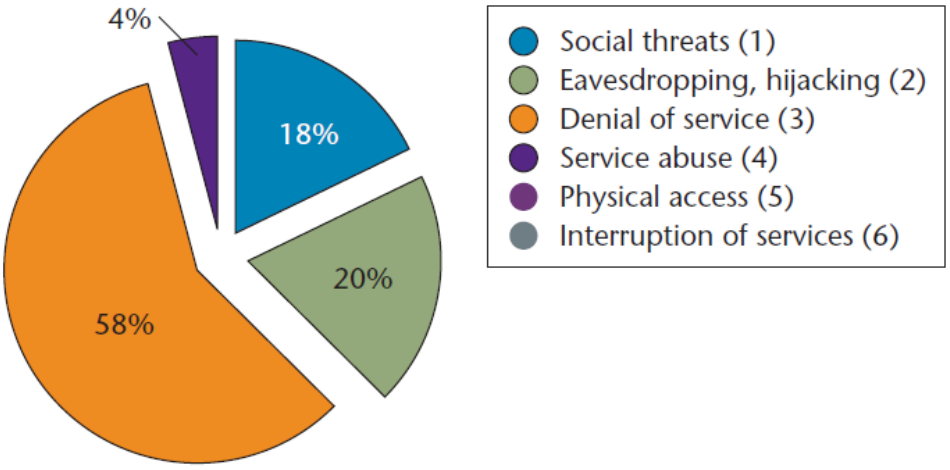
یک مهاجم قادر خواهد بود که با چندین بار تلاش ناموفق برای ورود، موجب قفل شدن حساب گردد. (این مشکل در اغلب سیستم‌هایی که با کلمه‌عبور محافظت می‌شوند متداول است. چون موجب می‌شود که از تکرار تلاش‌های مهاجم جلوگیری به عمل آید و نتواند با بررسی همه‌ی حالت‌های ممکن برای کلمه‌عبور، مقدار صحیح آن را بیابد). در نتیجه در زمان قفل شدن این حساب قادر به اتصال نخواهد بود. اگر دسترسی از راه دور امکان‌پذیر نباشد این مشکل را می‌توان با کنترل دسترسی فیزیکی حل کرد.

3-4 گزارش خلاصه‌ای از تهدیدات امنیتی VoIP

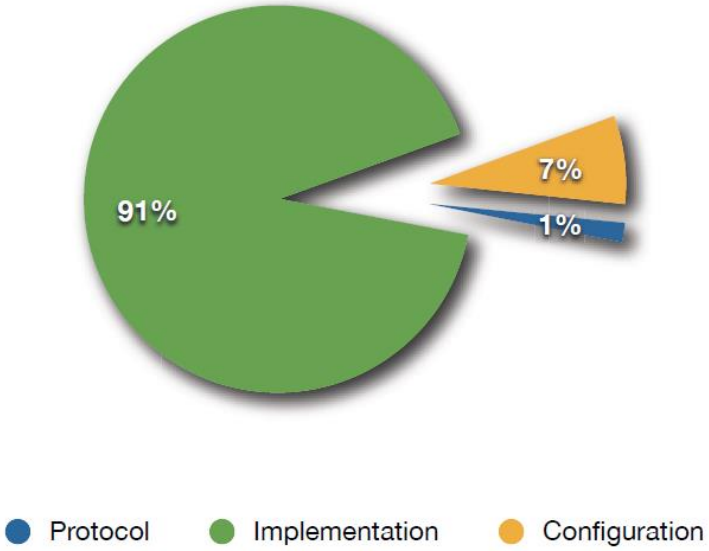
در این قسمت خلاصه‌ای از آسیب‌پذیری‌ها بر اساس آسیب‌پذیری‌های منتشر شده در پایگاه داده‌ی CVE [35] و نیز دو پیش‌نویس اینترنت IETF RFC ارائه می‌شود. در مجموع از 221 مشکل از سال 1999 تا 2009 کشف شده است. شکل 13 درصد آسیب‌پذیری‌ها را بر اساس نوع آن‌ها، با استفاده از طبقه‌بندی VoIPSA، نشان می‌دهد. بیشتر این مشکلات از طریق سقوط سرویس‌دهنده یا تجهیزات، منجر به حملات DoS می‌شوند. نکته جالب توجه این نمودار این است که استراق سمع و ربودن ترافیک تقریباً یک پنجم این آسیب‌پذیری‌ها را تشکیل می‌دهد. به بیان دقیق‌تر، بیشتر این مشکلات تحلیل ترافیک را از طریق دسترسی به وسیله‌ی کاربر یا لاگ‌های تماس سرویس‌دهنده انجام می‌دهند و به صورت مستقیم اجازه‌ی استراق سمع مکالمات صوتی را به مهاجم نمی‌دهند. شکل 14 درصد این آسیب‌پذیری‌ها را بر اساس منبع آن‌ها نشان می‌دهد. نکته‌ی عجیب این است که بیشتر مشکلات مربوط به پیاده‌سازی می‌باشند. هرچند که درصد قابل توجهی از مشکلات نیز مربوط به پیکربندی‌های نادرست می‌باشند. این پیکربندی‌های نادرست می‌توانند شامل اطلاعات محرمانه‌ی پیش‌فرض مدیر، اجرای سرویس‌های ناامن و مستند

[35] Common Vulnerabilities and Exposures

نشده روی وسیله (مانند اجرای ابزارهای اشکال‌زدایی از راه دور روی گوشی VoIP بدون احرازهویت)، و دسترسی به دیگر سرویس‌های محدود شده از طریق واسطهای جایگزین، باشد. در نهایت تعداد بسیار کمی از آسیب‌پذیری‌های پروتکل‌ها منجر به حملات DoS یا کلاهبرداری می‌شوند.

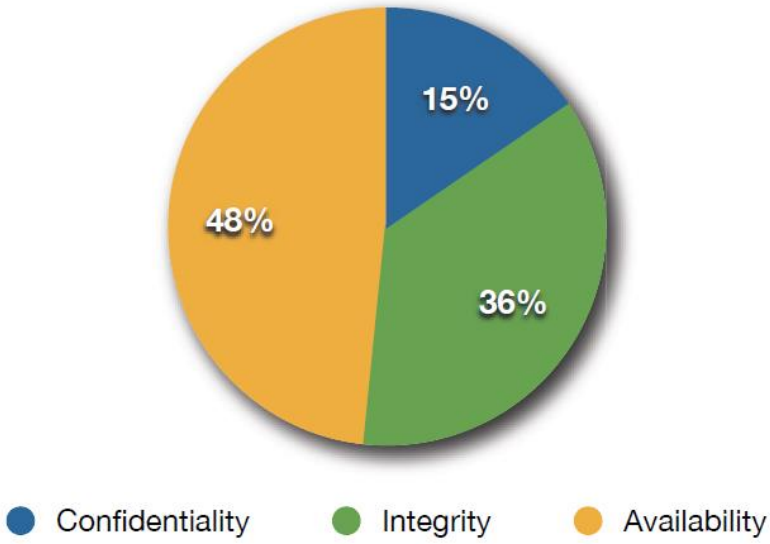


شکل 13 درصد آسیب‌پذیری‌ها بر اساس طبقه‌بندی VoIPSA



شکل 14 طبقه‌بندی آسیب‌پذیری‌ها بر اساس موقعیت‌ها و دلایل آسیب‌پذیری

شکل 15 آسیب‌پذیری‌های VoIP را بر اساس تقسیم‌بندی NIST (محرمانگی، صحت و دسترس‌پذیری) نشان می‌دهد. همان‌طور که در این شکل هم مشهود است حملات جلوگیری از سرویس بیشترین نگرانی را به وجود می‌آورند. همچنین مشاهده می‌شود که تخلفات صحت بخش قابل توجهی از فضای تهدیدات را به خود اختصاص می‌دهند در حالی که تخلفات محرمانگی 15٪ از آسیب‌پذیری‌های کشف شده را تشکیل می‌دهند.



شکل 15 درصد آسیب‌پذیری‌ها بر اساس طبقه‌بندی NIST (محرمانگی، صحت و دسترس‌پذیری)

5 مراجع

[1] Keromytis, Angelos D. "Voice-over-IP security: Research and practice", *Security & Privacy, IEEE* 8.2 (2010): 76-78.

[2] Ferdous, R. Analysis and Protection of SIP based Services (Doctoral dissertation, University of Trento), 2014.

[3] Kuhn, D. Richard, Thomas J. Walsh, and Steffen Fries. "Security considerations for voice over IP systems", *NIST Special Publication* (2005): 800-58.

[4] Sadiwala, Ritesh, and Manisha Sharma. "Security threats of VoIP", *J Innov Trends Sci Pharm Technol* 1 (2014): 7-18.

[5] Keromytis, Angelos D. "Voice over ip: Risks, threats and vulnerabilities", *Cyber Infrastructure Protection* (2011).

[6] Ambre, Amruta, and Narendra Shekokar. "Detection and Prevention Mechanism on Call Hijacking in VoIP System", *International Journal of Computer Applications* 90.6 (2014).

[7] Hussain, Intesab, et al. "A Comprehensive Study of Flooding Attack Consequences and Countermeasures in Session Initiation Protocol (SIP)", *Security Comm. Networks* (2014).