فصلنامه علمی-پژوهشی مطالعات مدیریت کسب و کار هوشمند- سال هفتم ـ شماره ۲۵ـ پاییز ۱۳۹۷
صفحات ۲۱۸-۱۸۳

تحلیل و اولویت‌بندی چالش‌های امنیتی وُیپ

سعید بختیاری
اسماعیل زارع

چکیده

معماری شبکه آی‌پی ازنقطه‌نظر امنیتی شکننده است و وُیپ نیز که از استانداردهای این شبکه استفاده می‌کند با حملات متعدد مورد آسیب قرار می‌گیرد، حملاتی که کاهش کیفیت و در مواردی قطع خدمات و اتلاف منابع وُیپ را به دنبال دارد. در این راستا تأمین امنیت وُیپ امری ضروری است و به‌طورمعمول اعمال راهکارهای امنیتی در سامانه‌ها ازجمله وُیپ موجب کندی و کاهش کیفیت عملکرد و افزایش هزینه‌های راه‌اندازی و نگهداشت می‌شود؛ بنابراین مدیران فناوری اطلاعات می‌بایست راهکارهای امنیتی با درجه‌ی اولویت بالا را مدنظر قرار دهند. برای این کار با مرور ادبیات تحقیق، ماتریس جامع امنیت وُیپ مشتمل بر فهرست جامعی از چالش‌های امنیتی وُیپ و راهکارهای مقابله استخراج گردید که کمک بسزایی در هوشمندی و مدیریت ریسک سازمان‌ها می‌نماید. نتایج به‌دست‌آمده در این مقاله نشان داد که انجام سه راهکار «جداسازی VLANهای ترافیک صوت و داده»، «احراز هویت سیگنالینگ» و «احراز هویت درگاه» بیشترین تأثیر مثبت را بر امنیت وُیپ دانشگاه علوم انتظامی خواهد داشت. نتایج حاصل با توصیه‌ها و راهکارهای مقابله امنیتی ذکرشده توسط تحقیقات قبلی و مؤسسات معتبر امنیتی کاملاً مطابق و هم‌راستا است و فقط اولویت‌های پیشنهادی جابجا شده است. لذا در برنامه‌های راهبردی فناوری اطلاعات سازمان و تصمیم‌گیری و نظارت مدیران فناوری اطلاعات سه راهکار مذکور می‌بایست در اولویت به‌کارگیری وُیپ لحاظ گردد.

واژگان کلیدی: وُیپ، امنیت، چالش، راهکار مقابله.

عضو هیئت علمی، گروه فناوری اطلاعات، دانشگاه علوم انتظامی امین، تهران.
کارشناس ارشد مدیریت فناوری اطلاعات، دانشگاه علوم انتظامی امین. (نویسنده مسئول)،
ezaree1354@chmail.ir

تاریخ دریافت:۱۳۹۷/۰۵/۰۶ **تاریخ پذیرش:۱۳۹۷/۰۸/۲۸**

مقدمه

با توسعه‌ی شبکه‌ی مراکز تلفن آنالوگ و بعدازآن دیجیتال شهری، رفته‌رفته «شبکه‌ی مراکز تلفن عمومی»[1] شکل گرفت. با توسعه‌ی «شبکه‌های داده مبتنی بر پروتکل اینترنت»[2]، فناوری «انتقال صدا بر روی بستر اینترنت» یا وُیپ معرفی شد که صوت و تصویر را در قالب جریانی از بسته‌های داده از طریق بستر شبکه‌ی آی.پی حمل و بین طرفین تماس مبادله می‌کند. ازآنجاکه فناوری وُیپ از زیرساخت شبکه‌ی آی.پی استفاده می‌کند، چالش‌های ذاتی آن نظیر تأخیر[3]، جیتر[4]، گم‌شدن بسته‌های داده[5]، کاهش قابلیت اطمینان و در دسترس بودن سرویس را به ارث می‌برد (حسین‌پور و همکاران[6]، ۲۰۱۶؛ فیتاکیتنوکان و همکاران[7]، ۲۰۰۸).

بیان مسئله

برقراری امنیت در شبکه‌های آی.پی مهم است، اما امنیت در ارتباطات وُیپ با چالش‌های به‌مراتب بیشتری مواجه است، چراکه به‌کارگیری راهکارهای امنیتی، معمولاً باعث کاهش سرعت و کیفیت صدا و تصویر تماس تلفنی می‌شود (دینگ و هورستر[8]، ۱۹۹۵). تحقیقات فراوانی در رابطه با امنیت شبکه‌های وُیپ انجام‌گرفته اما همچنان پرداختن به چالش‌های امنیتی وُیپ جزء مسائل روز دنیای فناوری اطلاعات و ارتباطات است. تحقیقات قبلی سعی کرده‌اند، حملات وُیپ و راهکارهای مقابله با آن‌ها را دسته‌بندی و معرفی نمایند اما ضمن آنکه از جامعیت کافی برخوردار نیستند، بر اساس مأموریت و ویژگی‌های ساختار شبکه و تجهیزات وُیپ دانشگاه علوم انتظامی و حساسیتی که برقراری ارتباطات صوتی و تصویری امن در سطح سازمان مذکور دارد از چالش‌ها و راهکارهای امنیتیِ وُیپ اولویت‌بندی ارائه نکرده‌اند.

1. Public Switched Telephone Network(PSTN)
2. IP-Based Packet Networks
3. Delay
4. Jitter
5. Packet loss
6 .Hosseinpour et al.
7 .Phithakkitnukoon et al.
8 .Ding & Horster

به دلیل لزوم یکپارچگی با زیرساخت تلفنی موجود، ارائه‌ی قابلیت‌های جدید و سرعت زیاد در توسعه و استقرار، استانداردها و تجهیزات وُیپ بارها به «آسیب‌پذیری»[1] و «سوءاستفاده»[2] دچار می‌شوند (کرومیتیس[3]، ۲۰۱۲). چون معماری شبکه‌های مبتنی بر پروتکل اینترنت شکننده است و وُیپ از استانداردهای باز مانند سیپ[4] در چنین شبکه‌هایی استفاده می‌کند، با حملات متعدد مورد آسیب قرار می‌گیرد، حملاتی که منجر به کاهش کیفیت و حتی قطع خدمات و اتلاف منابع سیستم وُیپ می‌شود (ونیلا و مانیکاندان[5]، ۲۰۱۶). شرکت امنیتی نتتیود[6] تعداد حملات علیه خدمات وُیپ در طی سه‌ماهه اول سال ۲۰۱۵ را ۶۷٪ از تمام حملات ثبت‌شده علیه سرورهای خود در بریتانیا اعلام کرد. به گزارش سرویس‌های امنیتی شرکت آی.بی.ام، پروتکل سیپ با ثبت ۵۱ درصد رویداد امنیتی، هدف اصلی حملات علیه وُیپ بوده و از اکتبر ۲۰۱۵ تا همین تاریخ در سال ۲۰۱۶ تعداد رویدادهای امنیتی مرتبط با پروتکل مذکور، از کمتر ۱ میلیون مورد به حدود ۵ میلیون رویداد افزایش یافته است. در این آمار SCCP[7] پروتکل خاص وُیپ مربوط به شرکت سیسکو با ۴۸ درصد و H225 که بخشی از پروتکل H.323 است، یک درصد رویدادهای امنیتی را بنام خود ثبت کرده‌اند.

کاهش کیفیت و قطع خدمات وُیپ براثر سوءاستفاده و اجرای حملات عدیده، ارائه‌دهنده و بهره‌بردار آن را با چالش‌های جدی مواجه می‌کند. محور دیگر تحقیق، معرفی راهکارهای پیشگیری و مقابله با حملات فوق است، سپس نتایج حاصل متناسب با وضعیت خدمات وُیپ دانشگاه علوم انتظامی مورد تجزیه‌وتحلیل قرارگرفته و درنهایت چالش‌های امنیتی خدمات وُیپ در سازمان مذکور به همراه راهکارهای مقابله، اولویت‌بندی و به‌عنوان یک سند جامع فنی و راهبردی برای بهره‌برداری پیشنهاد می‌گردد.

1. Vulnerability
2. Abuse
3. Keromytis
4. Session Initiation Protocol (SIP)
5. Vennila, G. & Manikandan
6. Nettitude
7. Skinny Client Control Protocol (SCCP)

با توجه به بهینه‌سازی و توسعه و تکمیل روزافزون تجهیزات و فناوری‌های زیرساخت شبکه‌ی IP و ضرورت‌های استفاده از فناوری ویپ در دانشگاه علوم انتظامی، باهدف تأمین ارتباطات تلفنی موردنیاز، پیش‌بینی و اعمال خط‌مشی‌های اساسی و منسجم امنیتی، برای تضمین کیفیت، محرمانگی، یکپارچگی و دسترسی فراگیر، سریع و مستمر به ارتباطات تلفنی، امری ضروری و لازم‌الاجرا است.

ادبیات تحقیق

وُیپ پهنای باند در دسترس شبکه‌ی آی.پی را به اشتراک گذاشته و در مصرف آن صرفه‌جوئی می‌کند. چون وُیپ روی شبکه‌های اینترنت و اینترانت کار می‌کند هزینه‌های عملیاتی آن پائین است. تلفن‌های وُیپ نرم‌افزاری، سخت‌افزاری و قابل جابجایی است. وُیپ مجموعه‌ای از قابلیت‌ها مانند «پست صوتی» و «تلفن گویای تعاملی» را ارائه می‌دهد و چون پیاده‌سازی و نگهداری آن ساده است به‌طور وسیع بهره‌برداری می‌شود. جدا از حذف هزینه‌های تماس و هم‌گرائی شبکه‌های صوت و داده که در هزینه‌های راه‌اندازی و نگهداری وُیپ صرفه‌جوئی به دنبال دارد امکاناتی مانند انعطاف‌پذیری و ارائه پلتفرم واحد در تحویل سرویس‌های چندرسانه‌ای، مراکز تماس مجازی و اینترنت از طریق تلفن، به سازمان‌های بهره‌بردار در انجام مأموریت و جلب رضایت و وفاداری مخاطبین مزیت رقابتی می‌بخشد (والاس[1]، ۲۰۰۹).

زیرساخت وُیپ

چون وُیپ از شبکه‌ی آی.پی استفاده می‌کند بخش عمده‌ای از زیرساخت موردنیاز خود را عاریه گرفته است اما تجهیزات خاصی را برای جابجایی صدا و تصویر بر روی زیرساخت فوق و تماس با «شبکه‌های مراکز تلفن عمومی» اضافه کرده است. مطابق شکل ۱ این تجهیزات شامل پایانه‌ها[2] عموماً تلفن‌ها، گره‌های کنترل تماس[1] شامل سرورهای مدیریت

1. Wallace
2. Endpoints

تماس و خدمات چندرسانه‌ای تلفنی و گره‌ی «دروازه‌بان»[۲]، گره‌های دروازه[۳] یا واسط اتصال و وفق دهنده‌ی وُیپ با «شبکه‌های مراکز تلفن عمومی» است که در کنار شبکه‌ی آی.پی درمجموع زیرساخت اساسی وُیپ را تشکیل می‌دهد (باچر و همکاران[۴]، ۲۰۰۷).

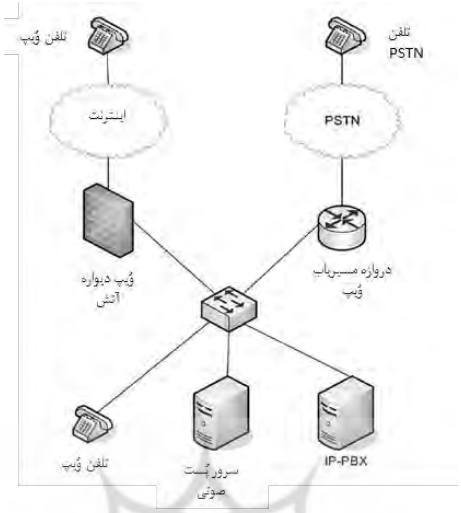
پردازش وُیپ

پردازش داده‌های وُیپ یا پیام‌های سیگنالینگی و صوتی آن شامل چهار مرحله است؛ سیگنالینگ[۵]، کُدگذاری/کدگشایی[۶]، انتقال[۷] و کنترل دروازه[۸].

سیگنالینگ: وظیفه‌ی راه‌اندازی و مدیریت تماس بین پایانه‌های شبکه‌ی وُیپ را به عهده دارد. دو سیگنالینگ استاندارد و پرکاربرد وُیپ H.323 و SIP است.

کُدگذاری/کُدگشایی و انتقال: با راه‌اندازی یک تماس تلفنی، صدای آنالوگ به دیجیتال تبدیل و فشرده می‌شود سپس نمونه‌های صوت، با استفاده از پروتکل آر تی پی[۹] داخل بسته‌های داده قرار گرفته و بر روی شبکه آی.پی حمل می‌شود. بسته‌های آر.تی.پی دارای قسمتی بنام «سرآیند»[۱۰] هستند که اطلاعات موردنیاز برای بازسازی سیگنال صوت در سمت گیرنده را نگهداری می‌کنند، درنهایت بسته‌های صوتی که به‌صورت «کپسول»هایی درآمده‌اند، به‌عنوان «محموله»[۱۱] توسط پروتکل یو دی پی[۱۲] همراه با جریان عادی انتقال داده، حمل می‌شود. در مقصد عملیات معکوس انجام می‌گیرد؛ بسته‌ها بازگشائی و سپس صوت دیجیتال برای پخش از طریق گوشی تلفن مقصد به آنالوگ تبدیل می‌شود.

1. Control Nodes
2. Gatekeeper Node
3. Gateway Nodes
4. Butcher
5.Signaling
6. Coding&Decoding(CODEC)
7. Transport
8. Gateway Control
9. Real-Time Transport Protocol
10. Heder
11. Payload
12. User Datagram Protocol



شکل ۱. زیرساخت معمول شبکه‌ی وُیپ (باچر و همکاران ، ۲۰۰۷)

کنترل دروازه: «دروازه»[1] دستگاهی است که مکالمات بین شبکه‌ی پی.اس.تی.ان با سامانه‌های مختلف چندرسانه‌ایِ مبتنی بر آی.پی و بالعکس را، از پروتکلی به پروتکل دیگر تبدیل و ترجمه می‌کند. همچنین برای تجهیزات صوتی آنالوگ و دیجیتال مانند تلفن‌ها، ماشین‌های دورنگار و مراکز تلفن، امکان دسترسی فیزیکی به شبکه‌ی آی.پی را فراهم می‌کند.

مرور متون تحقیق

اگرچه وُیپ دارای مزایایی مانند انعطاف‌پذیری در استفاده و مقرون‌به‌صرفه بودن برای ارائه‌دهنده و کاربر است اما این مزایا اشکالاتی را نیز به همراه دارد وُیپ «تهدیدات»[2] امنیتی شبکه‌های آی.پی را به ارث می‌برد و هدف جذابی برای مهاجمان است خصوصاً اگر بر روی شبکه‌ی اینترنت راه‌اندازی گردد. بدیهی است که پیش‌بینی تهدیدات و نقاط آسیب‌پذیر و اجرای تمهیدات پیشگیرانه در جلوگیری از حملات به سیستم وُیپ مؤثر خواهد بود اما در

1. Gateway
2. Threats

صورت بروز حمله نیز باید بلافاصله روش‌های دفاعی وارد عمل شده و از بروز چالش[1] در سامانه جلوگیری کند.

حملات وُیپ

چون وُیپ از سیگنالینگ سیپ و پروتکل انتقال آر.تی.پی استفاده می‌کند تا پیام‌ها و بسته‌های حاوی اطلاعاتِ مدیریت و هماهنگی تماس همچنین انتقال صوت مکالمه را روی رسانه‌های باسیم و بی‌سیم شبکه‌ی آ.پی به‌صورت بی‌درنگ[2] منتقل نماید، دامنه‌ی وسیعی از حملات روی دو حوزه‌ی سیگنالینگ و رسانه متمرکزشده‌اند. دسته‌ی دیگری از حملات با هدف از کار انداختن وُیپ طراحی و اجرا می‌شود بنابراین از منظر دامنه‌ی تأثیرگذاری و عملیات، حملات وُیپ به چهار حوزه‌ی شبکه‌ی آی.پی، سیگنالینگ، رسانه و وظایف تقسیم‌بندی می‌شود. جدا از حملات شبکه‌ی آی.پی که در بخش قبل معرفی گردید با مرور متون تحقیقات گذشته، حملات سایر حوزه‌ها مطابق جدول ۱ شناسایی و جمع‌بندی گردید.

جدول ۱. حملات وُیپ

کد	عنوان حمله	توضیح	منبع
C01	عدم سرویس (علیه سیگنالینگ)	اتلاف منابع موجود سیستم وُیپ از قبیل حافظه، پهنای باند و پردازنده با هدف از کار انداختن آن (با هدف از کار انداختن، سیلی از پیام‌های ساختگی سیگنالینگ به سمت سرور یا پایانه‌ی وُیپ ارسال می‌شود)	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (دینگ و هوستر، ۱۹۹۵)، (فارلی و ونگ، ۲۰۱۴)، (حسین پور و همکاران، ۲۰۱۶)، (پکوری و ولتری، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (فیتاکیتنوکون و همکاران، ۲۰۰۸)، (هان و جیانگ، ۲۰۰۹)، (سیات سیکاس و همکاران، ۲۰۱۵)، (زین،

1. Challenge
2. Real-Time

کد	عنوان حمله	توضیح	منبع
			۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)
C02	جعل شماره تلفن	برخی برنامه‌های کاربردی بانکی بر اساس شماره تلفن تماس‌گیرنده به او خدمات می‌دهد مهاجم با جعل شماره تلفن قربانی می‌تواند به اطلاعات بانکی و کارت اعتباری او دست پیدا کند	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)
C03	مرد میانی (ربایش اطلاعات ثبت‌نام و تغییر مسیر تماس)	در حمله‌ی «ربایش ثبت‌نام»، مهاجم هویت یک کاربر مجاز در سرور ثبات را جعل کرده و آدرس خود را به‌عوض او معرفی می‌کند، با این کار تماس‌های کاربر مجاز به سمت کاربر جعلی (مهاجم) ارسال می‌شود. سیپ با استفاده از یک سرور «تغییر مسیر» به مشترک وُیپ اجازه می‌دهد مسیر تماس (زنگ خوری) خود را به محل تلفن دیگری تغییر دهد، با حمله به سرور مذکور و سلطه بر آن، مهاجم، تماس‌های فرد قربانی را به سمت شماره‌ی تلفن دلخواه یا پوچ تغییر می‌دهد.	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پکوری و ولتری، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)
C04	تغییر متن پیام‌ها	با اجرای یکی از حملات «مرد میانی» مهاجم پیام‌های سیگنالینگی را رهگیری کرده و متن آن‌ها حتی بخشی یا همه صفاتشان را تغییر می‌دهد.	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پکوری و ولتری، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین،

کد	عنوان حمله	توضیح	منبع
			۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)
C05	حمله لغو/خداحافظ	مهاجم پیام‌های سیپ حاوی دستورات لغو یا خداحافظی ساخته و آن را برای خاتمه مکالمه جاری یک تلفن برای او می‌فرستد. با تکرار این کار، تلفن مذکور قادر به دریافت یا برقراری تماس نخواهد بود.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پکوری و ولتری، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)
C06	دستورات ناقص	مهاجم بسته‌های سیپ را با دستورات ناقص تغییر شکل داده و برای گره‌های حساس وُیپ می‌فرستد، این امر موجب کاهش کارایی و یا خارج از دسترس شدن گره‌های ذکرشده می‌شود.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پکوری و ولتری، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)
C07	مرد میانی (کلاه‌برداری با جعل کلید تبادل)	در ارتباطات وُیپ همتا-به-همتا، از پروتکل‌های تبادل کلید برای ایجاد یک ارتباط امن استفاده می‌شود، در این حمله شخص ثالث (مهاجم)، طرفین تماس را به پذیرش دو کلید متفاوت به اشتراک گذاشته‌شده از سوی خودش مجبور کرده و آن‌ها را فریب می‌دهد.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (ژانگ و همکاران، ۲۰۱۶)
C08	جعل پروکسی	مهاجم، قربانی را به برقراری تماس با پروکسی	(بوچرو همکاران، ۲۰۰۷)،

کد	عنوان حمله	توضیح	منبع
		جعلی خود وادار کرده و کنترل تماس‌های او را در اختیار می‌گیرد و حتی مکالماتش را ضبط می‌کند.	(کولیبالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)
C09	اطلاعات تصدیق به سرقت رفته	در جریان جلسات احراز هویت (مبتنی بر رمز عبور)، مهاجم اطلاعات موردنیاز برای تأیید توسط سرور را دزدیده و هویت یک کاربر مجاز را برای جلسات احراز هویت بعدی جعل می‌کند.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (ژانگ و همکاران، ۲۰۱۶)
C10	حدس زنی نابرخط و برخط رمز کاربر	در جریان جلسات احراز هویت (مبتنی بر رمز عبور)، مهاجم برای ورود به سیستم، به‌صورت برخط و نابرخط، رمز عبور کاربر را حدس می‌زند.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (ژانگ و همکاران، ۲۰۱۶)
C11	تأخیر سیگنالینگ	زمانی که طول می‌کشد، سیگنالینگ، تماس وُیپ بین دو تلفن را برقرار کند.	(عزیز و همکاران، ۲۰۱۴)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین، ۲۰۰۷)
C12	عدم سرویس (علیه رسانه)	اتلاف منابع موجود سیستم وُیپ از قبیل حافظه، پهنای باند و پردازنده با هدف از کار انداختن آن (اتلاف شدید پهنای باند با ارسال سیل بسته‌های آر تی پی بین مهاجم و قربانی)	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (فیتاکیتنوکون و همکاران،

کد	عنوان حمله	توضیح	منبع
			۲۰۰۸)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (ونیلا و منیکاندان، ۲۰۱۶)، (زین، ۲۰۰۷)
C13	شنود (استراق سمع)	مهاجم، داده‌های صوتی طرفین تماس را مخفیانه شنود کرده و برای مقاصد غیرمجاز بازپخش می‌کند، این داده‌ها شامل نسخه‌برداری از اسناد دورنگار و شنود دی تی ام اف تون‌ها در ارتباط با تلفن‌بانک برای به دست آوردن رمز عبور کارت‌های اعتباری و اطلاعات بانکی نیز می‌شود.	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین، ۲۰۰۷)
C14	تغییر جریان صدا	درواقع ترکیب حملات «جایگزینی» و «مرد میانی» است. مهاجم صدای مکالمه را شنود کرده و نتایج ارتباط را تغییر می‌دهد، مثل تغییر پیام «نه» به «بله» و یا «فروش» به «خرید» در مکالمه با یک مشاور مالی یا به دست آوردن رمز مالی قربانی و تخلیه حساب او هنگام تعامل او با سامانه تلفن گویا.	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین، ۲۰۰۷)
C15	تغییر محموله‌ی آر تی پی	بعد از انجام یک حمله «مرد میانی» و دسترسی به جریان رسانه‌ی آر تی پی بین دو گره وُیپ، مهاجم، محموله پیام را بازرسی و تغییر می‌دهد، با این کار او نویزی را به پیام تزریق کرده و یا پیام خودش را داخل بسته می‌گذارد و باعث اختلال یا تغییر معنی مکالمه می‌شود.	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین،

کد	عنوان حمله	توضیح	منبع
			(۲۰۰۷
C16	دست‌کاری سرآیند آر تی پی	با دست‌کاری شماره توالی و برچسب زمانی سرآیند بسته‌های آر تی پی، می‌توان توالی بسته‌ها را به هم ریخت یا آن‌ها را غیرقابل استفاده کرد، این حمله مفهوم گفتگو را بر هم زده یا گره دریافت‌کننده‌ی بسته‌ها را از کار می‌اندازد.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پرز بوترو و دونوسو، ۲۰۱۱)، (زین، ۲۰۰۷)
C17	تأخیر رسانه و آرتی پی	زمانی که بعد از برقراری نشست طول می‌کشد تا اولین صدا شنیده شود و تأخیر آر تی پی بیشترین تأخیر بین دو بسته‌ی آر تی پی است.	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین، ۲۰۰۷)
C18-34	نوع و مشخصات این دسته از حملات در بخش ۲-۲-۲ توصیف گردیده است.		
C35	علیه رایانه‌ی میزبان تلفن نرم‌افزاری وُیپ	مهاجم از طریق آسیب‌پذیری‌های ذاتی تلفن نرم‌افزاری وُیپ، حافظه‌ی سیستم‌عامل رایانه‌ی میزبان تلفن را اتلاف کرده و رایانه را مجبور به راه‌اندازی مجدد می‌کند.	(دینگ و هوستر، ۱۹۹۵)، (پرز بوترو و دونوسو، ۲۰۱۱)، (زین، ۲۰۰۷)
C36	علیه حافظه و پردازنده	مهاجم سیلی از پیام‌های «دعوت» را برای پروکسی سرور می‌فرستد، اگر دریافت‌کنندگان پاسخ سرور را ندهند، پروکسی مجبور می‌شود اطلاعات اوضاع را برای بیش از ۳۰ ثانیه در حافظه‌ی خود حفظ کند که ادامه‌ی این روند پروکسی را از کار می‌اندازد. در حمله دیگر مهاجم با افزایش غیرقابل‌تحمل بار پردازش پروکسی سرور آن را از سیستم خارج می‌کند.	(فارلی و ونگ، ۲۰۱۴)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)
C37	تقلب در هزینه‌ی تماس	مهاجم با جعل هویت یک کاربر مجاز تماس‌هایی برقرار کرده و هزینه‌های آن را به او	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)،

کد	عنوان حمله	توضیح	منبع
		تحمیل می‌کند و یا با دست‌کاری و حذف موارد ثبتی در پایگاه اطلاعات تماس‌ها در هزینه‌های خود تقلب می‌کند.	(مانونزا و همکاران، ۲۰۱۷)، (هان و جیانگ، ۲۰۰۹)
C38	پیام‌ها و تماس های ناخواسته (اس پی آی تی)	ارسال میلیون‌ها درخواست از طریق پست الکترونیکی، پدیده‌ای به نام اِسپَم نامیده می‌شود. بازاریاب تلفنی می‌تواند از تلفن وُیپ برای ارسال اِسپَم روی اینترنت (اس پی آی تی) استفاده کند. مهاجم سرورهای متعددی که فهرست‌هایی از شماره تلفن‌های وُیپ را در اختیار دارند راه‌اندازی کرده و سپس این سرورها به شماره تلفن‌های مذکور متصل شده و در حجم بالائی پیام می‌فرستند این پیام‌ها از طریق تلفن قربانی‌ها پخش شده و یا صندوق پست صوتی آن‌ها را انباشته می‌کند.	(پرز بوترو و دونوسو، ۲۰۱۱)، (فیتاکیتنوکون و همکاران، ۲۰۰۸)
C39	دسترسی غیرمجاز به منابع شبکه	در شبکه وُیپ واحدهای متعددی مثل گره‌های کنترلی و صدور صورتحساب هزینه وجود دارد که حاوی رمز و شماره تلفن و اطلاعات شخصی کاربران است، خیلی از دروازه‌ها و سوئیچ‌ها با رمز پیش‌فرض در حال کار هستند که اگر تغییر داده نشود به‌راحتی موردحمله قرار می‌گیرند. برخی از تجهیزات از تِلنِت برای دسترسی از راه دور پشتیبانی می‌کنند که به مهاجم اجازه بو کشیدن ترافیک شبکه را می‌دهد. برخی تجهیزات (مثل دروازه‌ها) نیز امکان دسترسی راه دور از طریق اچ تی تی پی را می‌دهند که قابل بو کشیدن توسط مهاجمین است.	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)

حملات شبکه‌ی آی.پی

بر اساس مرور متون تحقیقات، حملات مرسوم در شبکه‌های آی.پی و تأثیرگذار بر عملکرد وُیپ به شرح جدول ۲ شناسایی و جمع‌بندی گردید.

جدول ۲. حملات شبکه‌ی آی.پی

کد	عنوان حمله	توضیح	منبع
C18	حمله فیزیکی	دسترسی فیزیکی غیرمجاز به لینک‌های اصلی، تلفن‌ها، سرورهای وُیپ، سوئیچ‌های داده و غیره برای انجام اقدامات خرابکارانه	(زین، ۲۰۰۷)
C19	حمله به پایگاه ثبت اطلاعات تماس‌ها	مهاجم با دسترسی به پایگاه اطلاعات ثبتی تماس‌ها الگوهای تماس را استخراج و با تحلیل آن‌ها به مسائل محرمانه دست پیدا می‌کند سپس با دست‌کاری یا حذف آن‌ها در هزینه تماس‌ها تقلب می‌کند. ازآنجاکه اطلاعات تماس‌ها در پایگاه‌های داده تجاری ذخیره می‌شود، آسیب‌های شناخته‌شده برای این دست نرم‌افزارها مانند **SQL** می‌تواند منجر به آن شود که اطلاعات ذکرشده مورد استثمار قرار گیرند.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پرز بوترو و دونوسو، ۲۰۱۱)، (زین، ۲۰۰۷)
C20	مسومیت حافظه آرپ	عبور ترافیک شبکه از ماشین (گره) شخص مهاجم برای دستیابی غیرمجاز به اطلاعات	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)
C21	مرد میانی (کلاه‌برداری با جعل آدرس **MAC** یا	مهاجم با جعل مَک آدرس و خارج کردن یک گره/کاربر مجاز از شبکه، گره ساختگی خود را در سیستم وُیپ مشروع جلوه داده و به ارسال	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (پرز

کد	عنوان حمله	توضیح	منبع
	(IP	و دریافت اطلاعات موردنظر خود دست می‌زند.	بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)
C22	بسته‌های ناقص	مهاجم با ارسال بسته‌هایی (دارای نقص در پشته‌ی پروتکل شبکه) به سمت گره‌های شبکه منجر به کاهش عملکرد و حتی غیرفعال شدن آن‌ها می‌شود	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)
C23	سیل بسته‌های تی سی پی (با تنظیم پرچم SYN)	مهاجم سیلی از بسته‌های تی سی پی با آدرس‌های مبدأ اتفاقی و مقدار «۱» پرچم SYN تولید کرده و از گره قربانی درخواست تخصیص بافر می‌کند وقتی تمام فضای بافر گره مذکور اتلاف شد، بقیه کاربران مشروع نمی‌توانند با آن ارتباط برقرار کنند.	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (هان و جیانگ، ۲۰۰۹)
C24	بازپخش بسته‌های تی سی پی و یو دی پی	مهاجم با ارسال سیلی از بسته‌های یکسان، شبکه را آسیب‌پذیر می‌کند.	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)
C25	ایجاد سرور تی اف تی پی ساختگی	تلفن‌های وُیپ با مراجعه به یک تی اف تی پی سرور پیکربندی و بروز رسانی می‌شوند اگر مهاجم چنین سروری را در شبکه ایجاد کند به‌طور بالقوه باعث می‌شود تلفن‌ها، پیکربندی	(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران،

کد	عنوان حمله	توضیح	منبع
		جعلی (مثل شماره تلفن دیگری یا صورتحساب هزینه تقلبی) دریافت کنند.	۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوارکار، ۲۰۱۳)، (زین، ۲۰۰۷)
C26	تخلیه‌ی مخزن IP سرور دی اچ سی پی	با ارسال سیل درخواست به‌سوی دی اچ سی پی برای تولید مَک آدرس‌های اتفاقی، مهاجم می‌تواند استخر آدرس‌های آی پی موجود در دی اپ سی پی را خالی کند. این حمله گره را از دریافت آدرس آی پی و متعاقباً امکان ارتباط با سایر سرورهای وُیپ محروم می‌کند.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)
C27	سیل بسته‌های آی سی ام پی	مهاجم با ارسال سیلی از بسته‌های آی سی ام پی، کارائی گره موردحمله را کم یا تخریب می‌کند.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)
C28	سرریز بافر	این حملات، از نقص نرم‌افزارها سوءاستفاده کرده تا اطلاعات بیشتری در فضای بافر تعیین‌شده ذخیره کنند، بدین ترتیب بافر سرریز شده و کدها برای سوءاستفاده مهاجم ربوده می‌شود.	(بوچرو همکاران، ۲۰۰۷)، (کولیبالی و لی یو، ۲۰۱۰)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)
C29	سیستم‌عامل	سیستم‌عامل‌هایی که گره‌های کنترلی و دروازه‌های شبکه وُیپ روی آن‌ها کار می‌کنند مورد حملات شناخته‌شده و ناشناخته قرار می‌گیرند. مثل حملات به تلفن نرم‌افزاری وُیپ که بر روی رایانه نصب می‌شود.	(زین، ۲۰۰۷)
C30	ویروس‌ها و	آلوده شدن سیستم‌عامل گره‌های شبکه به	(زین، ۲۰۰۷)

کد	عنوان حمله	توضیح	منبع
	نرم‌افزارهای مخرب	ویروس‌ها و نرم‌افزارهای مخرب، موجب تخریب و تنزل سطح توانائی آن در رسیدگی به ترافیک ویپ می‌شود.	
C31	تراکم در شبکه‌ی داده	تجمع بیش‌ازحد بسته‌های داده در صف انتظار و درنتیجه از بین رفتن آن‌ها	کتب آموزشی
C32	تأخیرات انتقال (زیرساخت)	شامل تأخیر سِریالیزِیشِن، تأخیر انتشار، تأخیر بسته‌بندی، تأخیر صف، تأخیر پردازش و تأخیر شبکه است که درمجموع نباید از محدوده ۳۰۰ تا ۴۰۰ میلی‌ثانیه (رفت‌وبرگشت) تجاوز نماید.	کتب آموزشی
C33	جیتر	تفاوت میان کمترین تأخیر و بیشترین تأخیر در دریافت بسته‌های داده را جیتر می‌گویند، این زمان بایستی کمتر از ۴۰ میلی‌ثانیه باشد.	کتب آموزشی
C34	دیواره‌ی آتش و نَت	جلوگیری از عبور یا گم‌شدن پیام‌های سیگنالینگ و بسته‌های صوتی به دلیل استفاده از دیواره ی آتش و نَت بین طرفین تماس وُیپ	(زین، ۲۰۰۷)

تقلب در هزینه‌های تماس[1]

تقلب در هزینه‌ی تماس توسط کاربر، یکی از موارد نقض یکپارچگی و صحت اطلاعات در ارتباطات وُیپ محسوب می‌شود. عزیز و همکاران[2] (۲۰۱۴) یک معماری کنترل توزیع‌شده برای تشخیص حمله به شبکه‌های سیپ پیشنهاد دادند، آن‌ها تقلب در هزینه‌ی تماس را به‌عنوان نمونه‌ای برجسته ازاین‌دست حملات معرفی کردند. معماری «کربروس[3]» روش جدیدی است که تقلب‌ها را از طریق تحلیل مستقیم رویدادهای اُ سی اس[4] تشخیص داده و

1. Toll-Fraud
2. Aziz
3. Kerberos
4. On-line Charging System

به اپراتور این امکان را می‌دهد که در لحظه‌ی وقوع تقلب، اقدام مناسب (مثل قطع تماس یا انتقال آن به بخش مدیریت تقلب) را اتخاذ نماید (مانونزا و همکاران[1]، ۲۰۱۷).

ناسازگاری عملکرد و امنیت

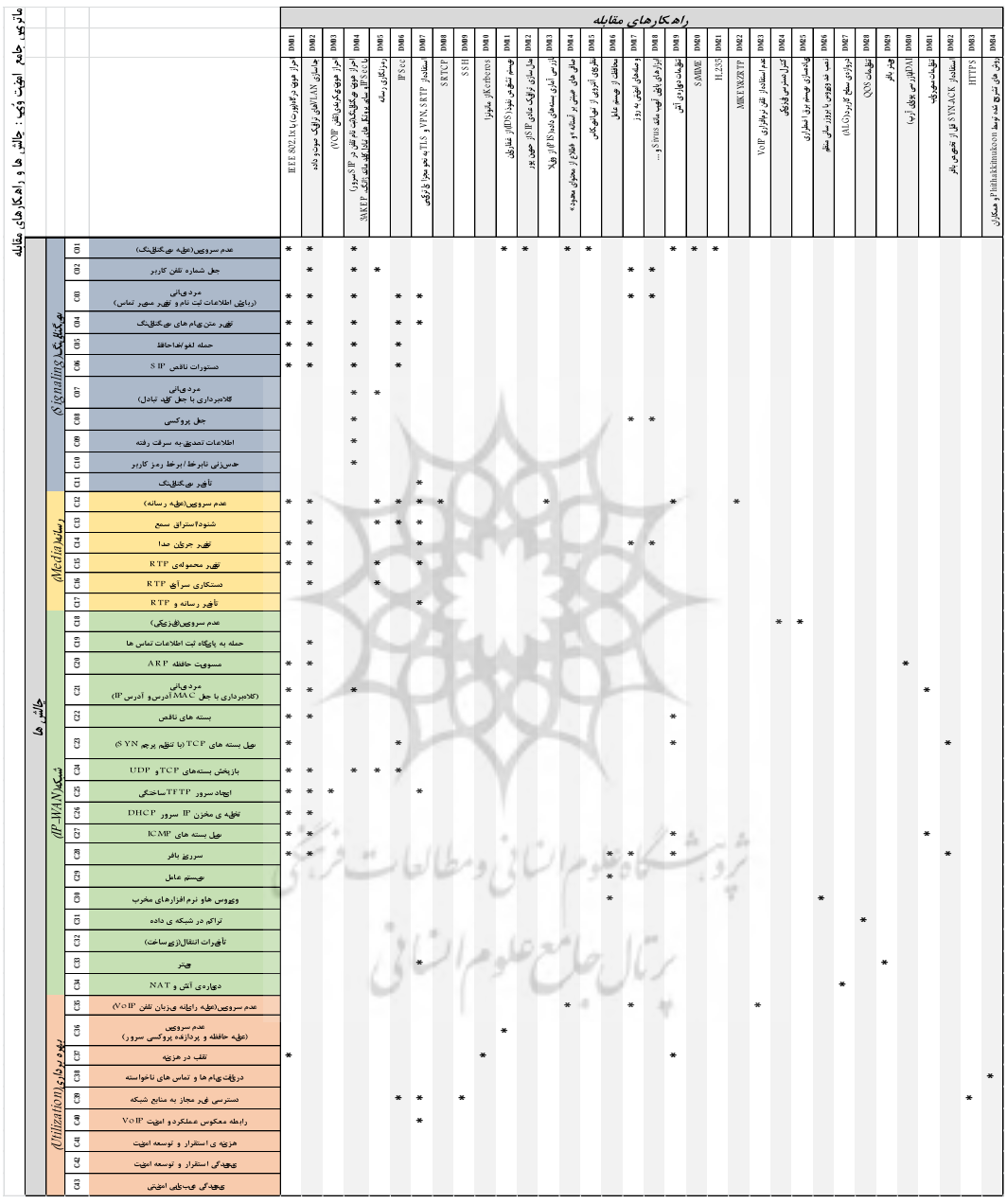
معمولاً استفاده از راهکارهای امنیتی موجب کاهش سرعت عملیات و درنتیجه کاهش کیفیت خدمات بی‌درنگ وُیپ می‌شود، به‌عبارت‌دیگر عملکرد خوب با امنیت مطلوب ناسازگار است. در تمام انواع شبکه‌های کامپیوتری، وی پی ان، اس آر تی پی یا ترکیب آن‌ها سریع‌ترین روش‌های امنیتی هستند بااین‌حال با توجه به هزینه‌ها و فواید هر روش، سازمان‌های مختلف می‌توانند از روش‌های مختلف امنیتی بنا به نیاز خود استفاده نمایند (حسین و همکاران[2]، ۲۰۱۶).

شمای جامع از چالش‌ها و راهکارها

طیف حملات صورت گرفته روی سیستم وُیپ عدیده است. مرور ادبیات تحقیق نشان داد که تحقیقات گذشته به یک یا موارد معدودی از حملات و راهکارهای مقابله پرداخته‌اند، جدول ۳ ماتریس جامعی از انواع چالش‌های امنیتی وُیپ و راهکارهای متناسب برای مقابله را نمایش می‌دهد. جنبه‌ی تمایز این تحقیق نسبت به بقیه در دو چیز است اول جامعیت حملات و راهکارها و دوم اولویت‌بندی راهکارهای امنیتی شناسایی‌شده با توجه به ساختار شبکه‌ی آی.پی و تجهیزت وُیپ در دانشگاه علوم انتظامی که مشخص می‌کند کدام راهکارهای امنیتی در توقف حملات بیشتری، مؤثر واقع می‌شوند، کاری که تحقیقات قبلی به آن نپرداخته یا به‌طور ناقص پرداخته‌اند.

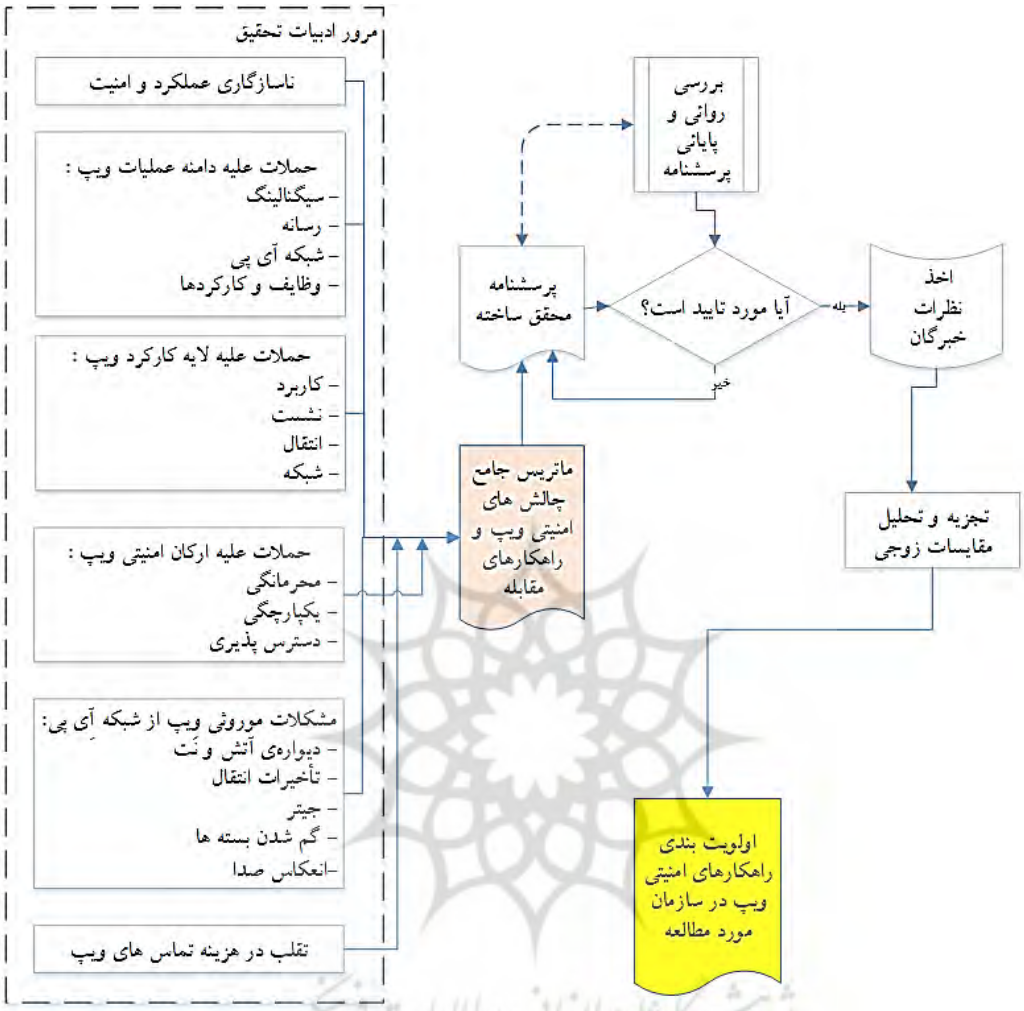
1. Manunza et al.
2. Hussain et al.

جدول ۳. ماتریس جامع امنیت وُیپ: چالش‌ها و راهکارهای مقابله



روش‌شناسی تحقیق

در این پژوهش با رویکردی کاربردی با هدف ارائه سندی جامع از چالش‌های امنیتی وُیپ و اولویت راهکارهای مقابله در دانشگاه علوم انتظامی، از روش توصیفی-پیمایشی استفاده‌شده به این نحو که ابتدا بامطالعه‌ی مقالات علمی معتبر، فهرست جامعی از چالش‌ها و راهکارهای امنیتی در قالب ماتریس جامع امنیت وُیپ (جدول ۳) شناسایی و گردآوری گردید. سپس بر اساس چالش‌های مذکور پرسشنامه‌ای محقق ساخته طراحی و در اختیار ده تن از خبرگان مسلط به ساختار و تجهیزات شبکه و وُیپ دانشگاه علوم انتظامی قرار گرفت. در مرحله‌ی آخر، نتایج گردآوری‌شده مورد تحلیل قرارگرفته و اولویت‌بندی راهکارها (مؤثرترین اقدامات امنیتی) استخراج و معرفی می‌شود. مراحل انجام تحقیق مطابق شکل ۲ است.



شکل ۲. مراحل انجام تحقیق

در این تحقیق، جامعه‌ی آماری شامل خبرگان، صاحب‌نظران و کارشناسان ارشد مراکز تلفن و امنیت فناوری اطلاعات و ارتباطات «ناجا» و «نیروهای مسلح» است که مدارک تحصیلی ۸۰ درصد آن‌ها فوق‌لیسانس و دکترا است. طبق نظرسنجی تحقیق، جامعیت چالش‌های امنیتی شناسایی‌شده با ۷۴ درصد نظر موافق به تأیید خبرگان رسید بنابراین پرسشنامه‌ی تحقیق از

روایی محتوایی و صوری کافی برخوردار بود. به‌علاوه با استفاده از نرم‌افزار **SPSS** مقدار ضریب آلفای کرونباخ ۰/۸۶ به دست آمد که حاکی از پایایی مطلوب پرسشنامه‌ی مذکور بود.

جدول ٤: بخشی از پرسشنامه در حوزه سیگنالینگ ویپ

حوزه	چالش	سؤالات	مقیاس				
			خیلی زیاد	زیاد	متوسط	کم	خیلی کم
سیگنالینگ	**C01**	ارسال سیلی از پیام‌های ساختگی سیگنالینگ به سمت سرورها یا پایانه‌های ویپ خطرناک است					
	C02	نباید به مهاجمین اجازه داد با جعل یک شماره تلفن معتبر در شبکه تماس برقرار کرده و خود را به سامانه‌های تلفنی عملیاتی عنصری قانونی معرفی کنند					
	C03	حفظ اطلاعات پایه برای ثبت‌نام در سیپ سرورها و جلوگیری از هرگونه تغییر مسیر تماس ویپ به نقطه‌ی دلخواه مهاجم ضروری است					
	C04	باید از رهگیری پیام‌های سیگنالینگی و تغییر متن آن‌ها ممانعت به عمل آورد					
	C05	نباید از پیام‌های سیپ حاوی دستورات لغو یا خداحافظی ساختگی که ممکن است مکرر برای تلفن‌های ویپ ارسال شود غافل شد					
	C06	با استفاده از پروتکل‌های تبادل کلید باید فرآیند احراز هویت کاربران و تبادل داده‌های صوتی را رمزنگاری کرد					
	C07	در ارتباطات سیپ احتمال جعل پروکسی سرور وجود دارد					
	C08	حفاظت از اطلاعات موردنیاز برای					

	تصدیق/تأیید شدن از سوی سرور ویپ، حین عملیات احراز هویت الزامی است						
C09	ارسال سیلی از پیام‌های ساختگی سیگنالینگ به سمت سرورها یا پایانه‌های ویپ خطرناک است						
C10	نباید به مهاجمین اجازه داد با جعل یک شماره تلفن معتبر در شبکه تماس برقرار کرده و خود را به سامانه‌های تلفنی عملیاتی عنصری قانونی معرفی کنند						

همان‌طور که اشاره شد، از منظر دامنه‌ی تأثیرگذاری و عملیات، حملات وُیپ به چهار حوزه‌ی شبکه‌ی آی.پی، سیگنالینگ، رسانه و وظایف تقسیم‌بندی شدند که جدول ۴ نمونه‌ای از سؤالات پرسشنامه را در حوزه‌ی سیگنالینگ ویپ نمایش می‌دهد.

تجزیه‌وتحلیل داده‌ها

در این تحقیق، برای تجزیه‌وتحلیل اطلاعات و تعیین وزن چالش‌های مورد شناسایی از روش میانگین حسابی مبتنی بر ماتریس مقایسات زوجی استفاده شده است بنابراین در ادامه به تشریح تعاریف و نحوه‌ی اجرا پرداخته می‌شود.

تعیین وزن چالش‌ها

برای تعیین اهمیت نسبی چالش‌های امنیتی وُیپ آن‌ها دوبه‌دو باهم مقایسه می‌شوند. مقایسه‌های زوجی از طریق پر کردن ماتریسی به نام ماتریس مقایسات زوجی انجام می‌گیرد. برای بیان ارجحیت بین دو عامل مقایسه شونده از جدول مقیاس ۵ استفاده می‌شود.

جدول ۵. مقیاس مورداستفاده در مقایسات زوجی

عدد	توضیح
۱	وقتی دو شاخص نسبت به هم ارجحیتی نداشته باشند
۳	وقتی یک عامل نسبت به عامل دیگر به‌طور متوسط ارجحیت داشته باشد
۵	وقتی یک عامل نسبت به عامل دیگر به‌طور قابل‌توجهی ارجحیت داشته باشد

۷	وقتی ارجحیت یک عامل نسبت به عامل دیگر بسیار قابل‌توجه باشد
۹	وقتی ارجحیت یک عامل نسبت به عامل دیگر بسیار بسیار قابل‌توجه باشد

برای تعیین وزن چالش‌ها از طریق میانگین حسابی، ابتدا مجموع اعداد هر ستون ماتریس مقایسه‌ی زوجی به دست می‌آید سپس اعداد واقع در یک ستون ماتریس بر مجموع اعداد همان ستون تقسیم می‌شود تا تمام درایه‌های ماتریس مقایسه‌ی زوجی نرمال شوند. در مرحله‌ی بعد میانگین سطرها که درواقع همان وزن مربوط به هر شاخص است به دست می‌آید.

تشخیص سازگاری و ناسازگاری ماتریس مقایسات زوجی

نرخ ناسازگاری نشان می‌دهد تا چه اندازه می‌توان به داده‌های گردآوری‌شده اعتماد کرد. تجربه نشان داده که اگر نرخ سازگاری کمتر از ۰/۱۰ باشد سازگاری مقایسه‌ها قابل‌قبول و در غیر این صورت تجدیدنظر لازم است. بر اساس محاسبات الگوریتم تشخیص سازگاری و ناسازگاری ماتریس مقایسات زوجی، سازگاری کامل مقایسات زوجی این تحقیق اثبات گردید.

نحوه‌ی تجزیه‌وتحلیل داده‌های تحقیق

۱) طبق جدول ۶ شاخص‌های به‌دست‌آمده در هفت گروه قرار داده شد. مبنای دسته‌بندی چالش‌ها دامنه‌ی حملات و تأثیرات ناشی از آن‌ها است. برای هر گروه عنوانی در نظر گرفته شد. اسامی گروه‌ها حتی‌الامکان معنادار انتخاب گردید و تا حد امکان سعی شد تعداد شاخص‌های مربوط به هر گروه نزدیک به هم باشد.

جدول ٦. گروه‌بندی چالش‌های امنیتی وُیپ بر اساس دامنه‌ی حملات

شماره گروه	عنوان گروه چالش	شامل چالش‌های زیر (از جدول ۳)
گروه ۱	اختلال در راه‌اندازی و مدیریت تماس‌های وُیپ	۱ و ۵و۶و۸و۱۱
گروه ۲	کلاه‌برداری از سیستم وُیپ از طریق جعل	۲و۳و۴و۷و۹و۱۰

	اطلاعات	
گروه ۳	اختلال در تبادل بسته‌های صوتی وُیپ	۱۲و۱۳و۱۴و۱۵و۱۶و۱۷
گروه ۴	سوءاستفاده از اطلاعات سیستم وُیپ	۱۹و ۲۰و ۲۱و۲۵و۲۸و۳۷
گروه ۵	اختلال در عملکرد شبکه و زیرساخت وُیپ	۱۸و۲۲و۲۳و۲۴و۲۶و۲۷و۳۶و۳۹
گروه ۶	اختلال در کیفیت شبکه و خدمات وُیپ	۲۹و ۳۰و ۳۱و۳۲و۳۳و۳۴
گروه ۷	موانع بهره‌برداری از وُیپ	۳۵و۳۸و ۴۰و ۴۱و ۴۲و ۴۳

۲) یک‌بار ماتریس مقایسات زوجی تشکیل و هفت گروه به‌دست‌آمده دوبه‌دو مقایسه و وزن (رتبه‌بندی) گروه‌ها به دست آمد. برای این کار و بر اساس نمرات نظرسنجی ابتدا می‌بایست اهمیت هر گروه با یک عدد مشخص می‌شد بنابراین میانگین حسابی پاسخ‌های مربوط به هر شاخص در هر گروه محاسبه و سپس میانگین حسابی مقادیر مذکور استخراج گردید که عدد نهائی به‌دست‌آمده نمایانگر میزان اهمیت هر گروه چالش از دیدگاه پاسخ‌دهندگان به پرسشنامه است. نتایج نهائی مطابق جدول ۷ به دست آمد.

در یک نگاه ساده مشخص است که به ترتیب گروه‌های دوم، پنجم و سوم چالش‌ها دارای عدد اهمیت بیشتری نسبت به بقیه هستند اما این نتیجه‌گیری باید با تشکیل ماتریس مقایسات زوجی گروه‌های چالش به دست آید. برای این کار ماتریس مقایسات زوجی گروه‌های چالش با استفاده از اعداد اهمیت فوق تشکیل و نرمال‌سازی انجام گرفت سپس میانگین سطرها که درواقع وزن مربوط به هر گروه است محاسبه و از بزرگ به کوچک مرتب گردید نتیجه مطابق جدول ۸ است. چنانچه قبلاً نیز پیش‌بینی شده بود گروه دوم داری بالاترین عدد اهمیت است این موضوع مؤید این نکته است که گروه چالش‌ها تحت عنوان «کلاه‌برداری از سیستم وُیپ از طریق جعل اطلاعات» از بالاترین میزان اهمیت برخوردار است و البته گروه ۶ با عنوان «اختلال در کیفیت شبکه و خدمات وُیپ» نیز دارای کمترین وزن یا میزان اهمیت نسبت به سایر گروه‌ها است.

برای شاخص‌های مربوط به هر گروه یک ماتریس مقایسات زوجی جداگانه تشکیل و وزن (رتبه) شاخص‌ها محاسبه می‌گردد. در مقایسات مذکور از عدد میانگین حسابی نظرات برای هر چالش استفاده می‌شود. نتایج نهائی به شرح جدول ۹ به دست آمد.

جدول شماره ۷. نمایش اعداد اهمیت گروه‌های هفت‌گانه چالش‌ها

شماره گروه چالش	۱	۲	۳	٤	٥	٦	۷
عدد اهمیت	۳/۹٦	٤/۱۸	٤/۰٥	٤/۰۳	٤/۱۳	۳/۸۲	۳/۹۷

جدول شماره ۸. رتبه‌بندی گروه‌های چالش

گروه	وزن گروه	رتبه
گروه۲	۰/۱۴۸۵	۱
گروه۵	۰/۱۴۶۸	۲
گروه۳	۰/۱۴۳۹	۳
گروه۴	۰/۱۴۳۲	۴
گروه۷	۰/۱۴۱۱	۵
گروه۱	۰/۱۴۰۷	۶
گروه۶	۰/۱۳۵۷	۷

۳) وزن هر چالش حاصل از مرحله‌ی (۳) در وزن گروهی که بدان تعلق دارد و در مرحله‌ی (۲) محاسبه گردید ضرب تا وزن نهایی شاخص‌های هر گروه به دست آید سپس با مرتب‌سازی آن‌ها از زیاد به کم ۱۰ رتبه‌ی اول معلوم و راهکارهای مقابله با هرکدام از روی نگاشت ماتریس جامع امنیت وُیپ ۷ معرفی و نتایج تفسیر می‌گردد. نتایج حاصل از اقدامات فوق طبق جدول ۱۰ قابل‌مشاهده است. دقت کنید که به دلیل یکسان بودن رتبه‌ی تعدادی از چالش‌های مندرج در جدول مذکور تعداد چالش‌های مطرح در ۱۰ رتبه نخست بیشتر و شامل ۲۲ عنوان است برای مثال چالش‌های ۱۷، ۲۵،

۲۹، ۳۰ و ۴۱ همگی هم‌سطح و در رتبه ۸ قرارگرفته‌اند بنابراین تمامی راهکارهای دفاعی شناسایی‌شده در قالب ماتریس جامع امنیت وُیپ که در مقابله با چالش‌های مذکور مؤثر باشند در اولویت‌بندی نهائی راهکارهای دفاعی مدنظر قرار می‌گیرند.

با مراجعه به ماتریس جامع امنیت وُیپ، اولویت‌بندی راهکارهای مقابله با چالش امنیتی واقع در ۱۰ رتبه‌ی اول با در نظر گرفتن فراوانی و تکرار آن‌ها در تقابل با تعداد چالش‌های بیشتر مطابق ترتیب مندرج در جدول ۱۱ به دست آمد.

جدول ۹. رتبه‌بندی چالش‌های هر گروه

شماره گروه	چالش‌ها	وزن	رتبه	شماره گروه	چالش‌ها	وزن	رتبه
۱	۱	۰/۲۱۲۱	۱	۵	۱۸	۰/۱۴۸۵	۱
	۵	۰/۲۰۲	۲		۳۹	۰/۱۳۰۳	۲
	۱۱	۰/۲۰۲			۲۶	۰/۱۲۷۳	۳
	۶	۰/۱۹۱۹	۳		۲۳	۰/۱۲۴۲	۴
	۸	۰/۱۹۱۹			۲۷	۰/۱۲۴۲	
۲	۲	۰/۱۷۵۳	۱		۲۴	۰/۱۱۸۲	۵
	۳	۰/۱۶۷۳	۲		۲۲	۰/۱۱۵۲	۶
	۹	۰/۱۶۷۳			۳۶	۰/۱۱۲۱	۷
	۱۰	۰/۱۶۷۳		۶	۲۹	۰/۱۸۳۴	۱
	۷	۰/۱۶۳۳	۳		۳۰	۰/۱۸۳۴	
	۴	۰/۱۵۹۴	۴		۳۱	۰/۱۷۹	۲
۳	۱۳	۰/۱۸۱۱	۱		۳۲	۰/۱۷۰۳	۳
	۱۴	۰/۱۸۱۱			۳۳	۰/۱۶۵۹	۴
	۱۷	۰/۱۷۲۸	۲		۳۴	۰/۱۱۷۹	۵
	۱۲	۰/۱۶۰۵	۳	۷	۴۰	۰/۱۸۹۱	۱
	۱۵	۰/۱۵۶۴	۴		۴۱	۰/۱۷۶۵	۲
	۱۶	۰/۱۴۸۱	۵		۴۳	۰/۱۶۸۱	۳
۴	۲۰	۰/۱۷۷۷	۱		۳۵	۰/۱۵۹۷	۴
	۲۵	۰/۱۷۳۶	۲		۴۲	۰/۱۵۵۵	۵
	۱۹	۰/۱۶۹۴	۳		۳۸	۰/۱۵۱۳	۶
	۲۱	۰/۱۶۹۴					
	۲۸	۰/۱۵۷	۴				
	۳۷	۰/۱۵۲۹	۵				

جدول ۱۰. محاسبه وزن و اولویت‌بندی نهائی چالش‌ها و تعیین ۱۰ چالش برتر

رتبه	چالش	وزن نهائی	رتبه	چالش	وزن نهائی	رتبه	چالش	وزن نهائی
۱	۱	۰/۰۲۹۸	۹	۳	۰/۰۲۴۸	۱۴	۳۷	۰/۰۲۱۹
۲	۵	۰/۰۲۸۴		۹	۰/۰۲۴۸		۴۲	۰/۰۲۱۹
	۱۱	۰/۰۲۸۴		۱۰	۰/۰۲۴۸	۱۵	۱۸	۰/۰۲۱۸
۳	۶	۰/۰۲۷	۱۰	۷	۰/۰۲۴۳	۱۶	۱۶	۰/۰۲۱۳
	۸	۰/۰۲۷		۱۹	۰/۰۲۴۳		۳۸	۰/۰۲۱۳
۴	۴۰	۰/۰۲۶۷		۲۱	۰/۰۲۴۳	۱۷	۳۹	۰/۰۱۹۱
۵	۱۳	۰/۰۲۶۱		۳۱	۰/۰۲۴۳	۱۸	۲۶	۰/۰۱۸۷
	۱۴	۰/۰۲۶۱	۱۱	۴	۰/۰۲۳۷	۱۹	۲۳	۰/۰۱۸۲
۶	۲	۰/۰۲۶		۴۳	۰/۰۲۳۷		۲۷	۰/۰۱۸۲
۷	۲۰	۰/۰۲۵۴	۱۲	۱۲	۰/۰۲۳۱	۲۰	۲۴	۰/۰۱۷۳
۸	۱۷	۰/۰۲۴۹		۳۲	۰/۰۲۳۱	۲۱	۲۲	۰/۰۱۶۹
	۲۵	۰/۰۲۴۹	۱۳	۱۵	۰/۰۲۲۵	۲۲	۳۶	۰/۰۱۶۵
	۲۹	۰/۰۲۴۹		۲۸	۰/۰۲۲۵	۲۳	۳۴	۰/۰۱۶
	۳۰	۰/۰۲۴۹		۳۳	۰/۰۲۲۵			
	۴۱	۰/۰۲۴۹		۳۵	۰/۰۲۲۵			

جدول ۱۱. اولویت نهائی راهکارهای دفاعی امنیتی در شبکه‌ی وُیپ دانشگاه علوم انتظامی

اولویت	راهکار دفاعی
۱	جداسازی **VLAN**های ترافیک صوت و داده
۲	احراز هویت سیگنالینگ (ثبت‌نام تلفن در سیپ سرور) با **IPSec** و سایر پروتکل‌های تبادل کلید مانند ژانگ، **AKEP3**
۳	احراز هویت درگاه (پورت) با **IEEE 802.1x**
۴	استفاده از سیستم تشخیص نفوذ (**IDS**)
۵	مدل‌سازی ترافیک عادی سیپ
۶	استفاده از صافی‌های «مبتنی بر آستانه» و «اطلاع از محتوای محدود»
۷	استفاده از نظریه‌ی آنتروپی برای تشخیص حملات عدم سرویس بر اساس ترافیک ثبت‌شده

اولویت	راهکار دفاعی
	استفاده از سیستم تشخیص حملات انکار سرویس توزیع‌شده با استفاده از سیستم خبره {سعدآبادی، ۲۰۱۶ #۲۹}
۸	اجرای تنظیمات دیواره‌ی آتش
۹	استفاده از پروتکل **S/MIME**
۱۰	استفاده از پروتکل **H.235**
۱۱	استفاده از **VPN**، **SRTP** و **TLS** به نحو مجزا یا ترکیبی
۱۲	استفاده از پروتکل **IPSec**
۱۳	نصب وصله‌های امنیتی به‌روز
۱۴	ابزارهای پایش آسیب مانند **Sivus** و ...
۱۵	اجرای رمزنگاری رسانه
۱۶	بازرسی پویای آرپ (**DAI**)
۱۷	محافظت از سیستم‌عامل
۱۸	نصب ضدویروس با به‌روزرسانی منظم
۱۹	اولویت‌دهی به راهکارهای مقابله با تأثیر امنیتی بیشتر
۲۰	تنظیمات مسیریاب
۲۱	تنظیمات **QOS**

جمع‌بندی و نتیجه‌گیری

چنانچه نتایج این تحقق نشان می‌دهد به ترتیب سه راهکار «جداسازی **VLAN** های ترافیک صوت و داده»، «احراز هویت سیگنالینگ» و «احراز هویت درگاه» مهم‌ترین و مؤثرترین راهکارهای تضمین‌کننده امنیت سامانه‌های وُیپ در دانشگاه علوم انتظامی هستند.

نتایج فوق با توصیه‌ها و راهکارهای امنیتی ذکرشده در تحقیقات گذشته و مؤسسات معتبر امنیتی کاملاً مطابق و هم‌راستا است و فقط در برخی موارد اولویت‌های پیشنهادی کمی جابجا

شده است. گروه امنیتی سیسکو تالوس[1] در سال ۲۰۱۶، تکنیک‌های زیر را برای کاهش حملات امنیتی وُیپ پیشنهاد داده است:

- رمزگذاری توسط دستگاه یا کاربر که بدون تردید می‌تواند تأخیر بیش‌ازحد در شبکه یا سربار و پیچیدگی عملیاتی به وجود آورد.
- رمزگذاری سیگنالینگ در دروازه‌های اتصال به اینترنت، به‌وسیله‌ی سیپ و تی اِل اِس روی لایه حمل‌ونقل.
- استفاده از وی پی اِن برای ارتباط تلفن‌های راه دور با شبکه، خصوصاً هنگامی‌که HTTPS یا اِس آر تی پی در دسترس نباشد.
- استفاده از رمزهای عبور قوی، برای دسترسی به صندوق پست صوتی.
- حذف پیام‌های حساس پست‌های صوتی، به‌محض این‌که کاربر به آن‌ها گوش داد.

چنانچه ملاحظه می‌شود پیشنهادهای فوق، راهکارهای دوم و سوم پیشنهادی همچنین چالش اشاره‌شده در فصل دوم یعنی ناسازگاری امنیت و عملکرد وُیپ را تصدیق می‌کند اما استفاده از وی.پی.ان که توسط اکثریت تحقیقات مرور شده و مؤسسات امنیتی به‌منظور برقراری ارتباط امن تلفن‌های راه دور با سرورهای وُیپ سازمان‌ها مورد تأکید و توصیه قرارگرفته در اولویت‌بندی ما در سطح پائین تری قرارگرفته که دلیل آن واضح و ناشی از استفاده‌ی تجهیزات وُیپ دانشگاه علوم انتظامی از شبکه‌ی اینترانت اختصاصی و بسته است که امکان هرگونه دسترسی غیرمجاز و بدون کنترل به اینترنت از طریق سرویس وی.پی.آن را سلب کرده است. به‌علاوه در صورت نیاز به استفاده از وی.پی.ان برای ارتباطات وُیپ این کار توسط مدیریت شبکه قابل‌اعمال و در صورت انجام برای ارتقای امنیت بسیار مؤثر خواهد بود. چنانچه ماتریس جامع امنیت وُیپ نشان می‌دهد اجرای راهکار اول پیشنهادی یا همان جداسازی **VLAN**های ترافیک صوت و داده، هم‌زمان باعث توقف حجم بسیاری از حملات و تهدیدات امنیتی وُیپ می‌شود، با اعمال این راهکار مهاجمان نمی‌توانند از رایانه‌ها و ایستگاه‌های کاری مستقر روی شبکه‌ی داده برای رخنه به سامانه‌های وُیپ مستقر روی

1.Cisco Talos

شبکه صوت استفاده کنند. اجرای دو شبکه‌ی فیزیکی مجزا با استفاده از فناوری VLAN انجام می‌شود. سوئیچ‌های شبکه VLAN ها را پیاده‌سازی کرده و تنها بین دستگاه‌هایی که در یک VLAN پیکربندی‌شده‌اند اجازه مسیریابی خواهند داد. تلفن‌های وُیپ پورت دومی برای اتصال رایانه دارند. فناوری VLAN(802.1q) این امکان را می‌دهد که رایانه متصل شده به تلفن وُیپ در شبکه داده قرار بگیرد و نه در شبکه صوت. به‌هرحال برخی اتصالات بین شبکه صوت و داده نیز الزامی است، به‌عنوان‌مثال سرورهای پست صوتی معمولاً روی شبکه‌های داده قرار می‌گیرند. سرورهای کنترل تماس وُیپ به اتصال نظارت‌شده با سرورهای پست صوتی احتیاج دارند. برای پیاده‌سازی این اتصال بین دو بخش صوت و داده در شبکه LAN، بین آن‌ها «دیواره‌ی آتش» نصب می‌شود. درمجموع به‌کارگیری این راهکار دفاعی در شبکه WAN دانشگاه علوم انتظامی برای تضمین امنیت ارتباطات وُیپ الزامی و بر اساس نتایج این تحقیق مؤثرترین راهکار از سبد راهکارهای مؤثر امنیتی وُیپ است.

ازآنجاکه اتصال بین تلفن‌ها و سروهای وُیپ با استفاده از پروتکل سیپ انجام می‌گیرد هنگامی‌که تلفن در سرور سیپ ثبت می‌شود شناسه‌هایی از خود نظیر MAC و آی.پی آدرس را به سرور معرفی می‌کند. مهاجمان همواره سعی دارند با جعل اطلاعات مذکور خود را به‌عنوان تلفن یا یک گره معتبر در شبکه‌ی وُیپ جا بزنند. لذا احراز هویت کاربران و گره‌های کنترلی ضرورتی امنیتی است. با استفاده از پروتکل‌های مختلفی می‌توان در لایه سیگنالینگ به احراز هویت پرداخت. استفاده از پروتکل IPSec روش مؤثری است، با این روش عملیات احراز هویت به شکل قدرتمند انجام می‌گیرد. هنگام درخواست پیکربندی، دستگاه تلفن مجموعه‌ای از کلیدها را از سرور دریافت می‌کند. IPSec چنین وظیفه‌ای را بر عهده می‌گیرد. IPSec درواقع ترکیبی از سه پروتکل AH، ESP و IKE است که در دو حالت تونل[1] و انتقال[2] و در لایه‌ی شبکه اجرا می‌شود. IPSec سه عملیات احراز هویت، رمزنگاری و محرمانگی در تبادلات سیگنالینگ بین تلفن و سرور کنترل وُیپ را انجام داده و

1. Tunnel
2. Transport

برای این کار ترکیبی از توابع ریاضی مثل DES، 3DES، AES، کلیدهای RSA و PSK همچنین الگوریتم‌های دیفن-هلمن، MD5 و SHA را بکار می‌گیرد. استفاده از IPSec در شبکه‌های وُیپ بزرگ‌مقیاس راحت نخواهد بود. روش‌هایی همچون استفاده از «مراکز صدور گواهی»[1] و «پروتکل‌های امنیتی سیستم نام دامنه»[2] انتخاب‌های دیگری برای احراز هویت در لایه سیگنالینگ است که در جای خود بایستی برای استفاده از آن‌ها نیز برنامه‌ریزی لازم را انجام داد.

احراز هویت درگاه از استانداردهای 802.1x استفاده می‌کند تا دستگاه‌های باسیم و بی‌سیمی را که قصد اتصال به شبکه دارند قبل از دسترسی به شبکه مورد شناسایی دقیق قرار دهد. البته تأثیر این تمهید امنیتی زمانی که محدوده ترافیک وُیپ از شبکه محافظت‌شده سازمانی خارج و به اینترنت گسترده می‌شود کاهش می‌یابد.

مشکل اصلی مدیران امنیت، تضمین سطح قابل قبولی از امنیت در سطح سامانه‌های گسترده است. یافته‌های این تحقیق، شاخص‌های اصلی برای برقراری امنیت سرویس ویپ را معرفی می‌کند و برای هرکدام مؤثرترین مکانیسم‌های پیش‌گیری و مقابله را با لحاظ چالش‌های ارتباط معکوس عملکرد و امنیت و همچنین هزینه‌های نسبتاً بالای برقراری و حفظ امنیت، ارائه می‌دهد.

داشبورد امنیتی که وضعیت شاخص‌های کلیدی تجمیع شده توسط این تحقیق را به مدیران فناوری اطلاعات سازمان‌ها نمایش می‌دهد امکان مدیریت هوشمندانه کسب‌وکار خدمات ویپ را فراهم می‌کند؛ و به جرأت می‌توان گفت الگوی مناسب و جامعی از حیث دانش شناخت آسیب‌ها و اقدامات امنیتی ویپ به ایشان ارائه می‌دهد.

بنابراین، استفاده از جدول جامع ارائه‌شده (جدول ۳)، علاوه بر نمایش مجموعه راهکارهایی که یک مدیر امنیت ویپ می‌بایست روی آن‌ها متمرکز گردد؛ در برنامه‌های راهبردی فناوری اطلاعات و مدیریت ریسک سازمان‌ها به چابکی و عکس‌العمل سریع در پاسخ به حملات و تهدیدات سیستم‌های مبتنی بر وُیپ می‌تواند کمک بسزایی نماید. همچنین مدیران فناوری

1. Cetification Authority(CA)
2. Domain Name System Security(DNSSec)

اطلاعات در تصمیم‌گیری و نظارت خود جهت به‌کارگیری وُیپ می‌بایست سه راهکار پیشنهادی را در اولویت نظارت بر پیاده سازی ویپ لحاظ نمایند.

حفظ محرمانگی، یکپارچگی و دسترس‌پذیری ارتباطات متنوع ویپ در سازمان‌های نظامی-امنیتی از اهمیت به‌مراتب بالاتری برخوردار است. لاجرم باید شناخت روزآمد، کامل و مستمر از تهدیدات و چالش‌های امنیتی برای انتخاب، بهره‌برداری و توسعه سامانه‌های ویپ در دست داشت که این موضوع عین هوشمندی در مدیریت این حوزه از فناوری اطلاعات و ارتباطات است.

امید است نتایج حاصل از این پژوهش، برای برقراری و تضمین امنیت سامانه‌های کنونی همچنین اتخاذ سیاست‌ها و انتخاب سامانه‌های آتی وُیپ در دانشگاه علوم انتظامی و سایر سازمان‌ها، به‌عنوان مرجعی جامع و کاربردی مورد بهره‌برداری و استناد مدیران، متصدیان و همچنین محققان علاقه‌مند قرار گیرد.

پیشنهادها

به‌منظور تکمیل این پژوهش، انجام مطالعات مشابه در زمینه‌های زیر پیشنهاد می‌شود:

حتی‌المقدور از راهکارهای پیشنهادی این تحقیق استفاده شود. هم‌زمان خط‌مشی‌های امنیتی مذکور در همه سطوح و اجزای شبکه وُیپ سازمانی اعمال و عملیاتی گردد.

وضعیت فعلی کاربست راهکارهای پیشنهادی و نقاط ضعف و تهدید استخراج و مبنای اقدامات پیشگیرانه قرار گیرد.

هزینه و تأثیر راهکارهای امنیتی پیشنهادی بر عملکرد سامانه‌های وُیپ سازمان‌ها مورد تحقیق بیشتری قرار گیرد.

حتی‌المقدور از سامانه‌های جامع، بومی و یکسان وُیپ استفاده تا آموزش متخصصین، نگهداشت و از همه مهم‌تر اعمال سیاست‌های امنیتی ساده شود.

در مورد تأثیرات کاربرد دستگاه‌های «کنترل‌کننده‌ی ارتباطات وُیپ در لبه‌ی شبکه» یا **SBC**[1] ها که راهکارهای جامعی در رفع چالش‌های امنیتی وُیپ ارائه می‌کنند تحقیق شود.

1. Session Border Controller

منابع

سعدآبادی. ع، امیرشاهی. ب، (۱۳۹۵)، تشخیص حملات انکار سرویس توزیع‌شده با استفاده از سیستم خبره، *فصلنامه مطالعات مدیریت فناوری اطلاعات*، سال پنجم، شماره ۱۷، ۹۲-۶۳

Aziz, A. Hoffstadt, D. Rathgeb, E. & Dreibholz, T. (2014, 2-4 June 2014). A distributed infrastructure to analyse SIP attacks in the Internet. *Paper presented at the 2014 IFIP Networking Conference*.

Butcher, D. Li, X. & Guo, J. (2007). *Security Challenge and Defense in VoIP Infrastructures. IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*.

Chiappetta, S. Mazzariello, C. Presta, R. & Romano, S. P. (2013). An anomaly-based approach to the analysis of the social behavior of VoIP users. *Computer Networks*, 57(6), 1545-1559.

Coulibaly, E. & Liu, L. H. (2010). *Security Of VoIP Networks*.

Ding, Y. & Horster, P. (1995). *Undetectable On-line Password Guessing Attacks*.

Farley, R. & Wang, X. (2014). Exploiting VoIP softphone vulnerabilities to disable host computers: Attacks and mitigation. *International Journal of Critical Infrastructure Protection*.

Ghafarian, A. Seno, S. A. H. & Dehghani, M. (2016). *An Empirical Study of Security of VoIP System*.

Hosseinpour, M. Hosseini Seno, S. A .Yaghmaee Moghaddam, M. H. & Khosravi roshkhari, H. (2016). *Modeling SIP Normal Traffic to Detect and Prevent SIP-VoIP Flooding Attacks Using Fuzzy Logic*.

Hussain, M. Gupta, P. Bano, S. & Kulkarni, V. (2016). *High-Performance and Cost-Effective VoIP Security Techniques for Operations on IPv4, IPv6, and IPv4IPv6 Networks*.

Keromytis, A. D. (2012). A Comprehensive Survey of Voice over IP Security Research. *IEEE Communications Surveys & Tutorials*.

Lutiis, P. D. & Lombardo, D. (2009, 26-29 Oct. 20 .(۰۹An innovative way to analyze large ISP data for IMS security and monitoring. *Paper presented at the 2009 13th International Conference on Intelligence in Next Generation Networks*.

Manunza, L. Marseglia, S. & Romano, S. P. (2017). Kerberos: A real-time fraud detection system for IMS-enabled VoIP networks. *Journal of Network and Computer Applications*.

Pecori, R. & Veltri, L. (2016). 3AKEP: Triple-authenticated key exchange protocol for peer-to-peer VoIP applications. *Computer Communications*.

Perez-Botero, D. & Donoso, Y. (2011). *VoIP Eavesdropping: A Comprehensive Evaluation of Cryptographic Countermeasures*.

Phithakkitnukoon, S. Dantu, R. & Baatarjav, E.A. (2008). VoIP Security — Attacks and Solutions. *Information Security Journal: A Global Perspective*.

Shan, L. & Jiang, N. (2009). Research on Security Mechanisms of SIP-Based VoIP System. *Paper presented at the 2009 Ninth International Conference on Hybrid Intelligent Systems*.

Sonwane, G. D. & Chandavarkar, B. R. (2013). Security Analysis of Session Initiation Protocol in IPv4 and IPv6 Based VoIP Network. *Paper presented at the 2013 2nd International Conference on Advanced Computing, Networking and Security*.

Tsiatsikas, Z. Geneiatakis, D. Kambourakis, G. & Keromytis, A. D. (2015). An efficient and easily deployable method for dealing with DoS in SIP services. *Computer Communications*.

Vennila, G. & Manikandan, M. (2016). A Scalable Detection Technique for Real-time Transport Protocol (RTP) Flooding Attacks in VoIP Network. *Procedia Computer Science*.

Wallace, K. (2009). *Cisco-Voice-over-IP-CVOICE*.

Xin, J. (2007). *Security Issues and Countermeasure for VoIP*.

Zhang, L. Tang, S. & Zhu, S. (2016). An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks. *Journal of Network and Computer Applications*.