

تحلیل و اولویت بندی چالش های امنیتی وُپ

سعید بختیاری*

اسماعیل زارع**

چکیده

معماری شبکه آی پی از نقطه نظر امنیتی شکننده است و وُپ نیز که از استانداردهای این شبکه استفاده می کند با حملات متعدد مورد آسیب قرار می گیرد، حملاتی که کاهش کیفیت و در مواردی قطع خدمات و اتلاف منابع وُپ را به دنبال دارد. در این راستا تأمین امنیت وُپ امری ضروری است و به طور معمول اعمال راهکارهای امنیتی در سامانه ها از جمله وُپ موجب کندی و کاهش کیفیت عملکرد و افزایش هزینه های راه اندازی و نگهداشت می شود؛ بنابراین مدیران فناوری اطلاعات می بایست راهکارهای امنیتی با درجه ای اولویت بالا را مدنظر قرار دهند. برای این کار با مرور ادبیات تحقیق، ماتریس جامع امنیت وُپ مشتمل بر فهرست جامعی از چالش های امنیتی وُپ و راهکارهای مقابله استخراج گردید که کمک بسزایی در هوشمندی و مدیریت ریسک سازمان ها می نماید. نتایج به دست آمده در این مقاله نشان داد که انجام سه راهکار «جداسازی VLAN های ترافیک صوت و داده»، «احراز هویت سیگنالینگ» و «احراز هویت در گاه» بیشترین تأثیر مثبت را بر امنیت وُپ دانشگاه علوم انتظامی خواهد داشت. نتایج حاصل با توصیه ها و راهکارهای مقابله امنیتی ذکر شده توسط تحقیقات قبلی و مؤسسات معتبر امنیتی کاملاً مطابق و هم راستا است و فقط اولویت های پیشنهادی جابجا شده است. لذا در برنامه های راهبردی فناوری اطلاعات سازمان و تصمیم گیری و نظارت مدیران فناوری اطلاعات سه راهکار مذکور می بایست در اولویت به کارگیری وُپ لحاظ گردد.

واژگان کلیدی: وُپ، 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 پذیرش: ۱۳۹۷/۰۸/۲۸

تاریخ دریافت: ۱۳۹۷/۰۵/۰۶

مقدمه

با توسعه‌ی شبکه‌ی مراکز تلفن آنالوگ و بعد از آن دیجیتال شهری، رفته‌رفته «شبکه‌ی مراکز تلفن عمومی»^۱ شکل گرفت. با توسعه‌ی «شبکه‌های داده مبتنی بر پروتکل اینترنت»^۲، 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. از آنجا که فناوری وُیپ از زیرساخت شبکه‌ی آی.پی استفاده می‌کند، چالش‌های ذاتی آن نظیر تأخیر^۳، جیتِر^۴، گم شدن بسته‌های داده^۵، کاهش قابلیت اطمینان و در دسترس بودن سرویس را به ارث می‌برد (حسین‌پور و همکاران^۶، ۲۰۱۶؛ فیتاکیتنوکان و همکاران^۷، 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^۸، ۱۹۹۵). تحقیقات فراوانی در رابطه با امنیت شبکه‌های وُیپ انجام گرفته 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 امنیتی 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 وُپ بارها به «آسیب‌پذیری»^۱ و «سوءاستفاده»^۲ دچار می‌شوند (کرومیتیس^۳، ۲۰۱۲). چون معماری شبکه‌های مبتنی بر پروتکل اینترنت شکننده است و وُپ از استانداردهای باز مانند سیپ^۴ 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 وُپ می‌شود (ونیلا و مانیکاندان^۵، ۲۰۱۶). شرکت امنیتی نتتیود^۶ تعداد حملات علیه خدمات وُپ 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 وُپ 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^۷ پروتکل خاص وُپ 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 وُپ بر اثر 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 وُپ دانشگاه علوم انتظامی مورد تجزیه و تحلیل قرار گرفته و در نهایت چالش‌های امنیتی خدمات وُپ 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

ویپ پهنای باند در دسترس شبکه‌ی آی.پی را به اشتراک گذاشته و در مصرف آن صرفه‌جویی می‌کند. چون ویپ روی شبکه‌های اینترنت و اینترنت کار می‌کند هزینه‌های عملیاتی آن پائین است. تلفن‌های ویپ نرم‌افزاری، سخت‌افزاری و قابل جابجایی است. ویپ 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 هم‌گرایی شبکه‌های صوت و داده که در هزینه‌های راه‌اندازی و نگهداری ویپ صرفه‌جویی 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^۱، ۲۰۰۹).

زیرساخت ویپ

چون ویپ 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^۲ عموماً تلفن‌ها، گره‌های کنترل تماس^۱ 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 در مجموع زیرساخت اساسی وُیپ را تشکیل می‌دهد (باچر و همکاران^۴، ۲۰۰۷).

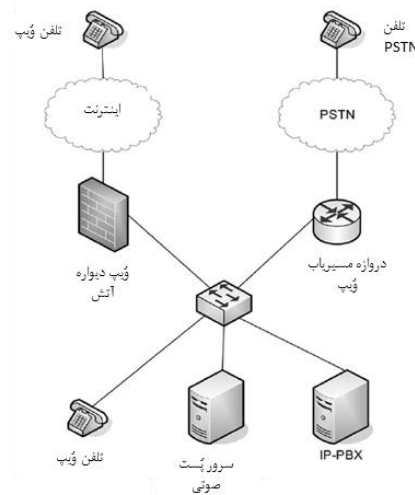
پردازش وُیپ

پردازش داده‌های وُیپ یا پیام‌های سیگنالینگ و صوتی آن شامل چهار مرحله است؛ سیگنالینگ^۵، کُدگذاری/کُدگشایی^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 به صورت «کپسول»هایی درآمده‌اند، به عنوان «محموله»^{۱۱} توسط پروتکل یو دی پی^{۱۲} همراه با جریان عادی انتقال داده، حمل می‌شود. در مقصد عملیات معکوس انجام می‌گیرد؛ بسته‌ها بازگشایی 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»^۱ دستگاهی است که مکالمات بین شبکه‌ی پی.اس.تی.ان با سامانه‌های مختلف چندرسانه‌ای 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»^۲ 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^۱ در سامانه جلوگیری کند.

حملات وُپ

چون وُپ از سیگنالینگ سیپ و پروتکل انتقال آر.تی.پی استفاده می‌کند تا پیام‌ها و بسته‌های حاوی اطلاعات مدیریت و هماهنگی تماس همچنین انتقال صوت مکالمه را روی رسانه‌های باسیم و بی‌سیم شبکه‌ی آی.پی به صورت بی‌درنگ^۲ منتقل نماید، دامنه‌ی وسیعی از حملات روی دو حوزه‌ی سیگنالینگ و رسانه متمرکز شده‌اند. دسته‌ی دیگری از حملات با هدف از کار انداختن وُپ طراحی و اجرا می‌شود بنابراین از منظر دامنه‌ی تأثیرگذاری و عملیات، حملات وُپ 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 وُپ

کد	عنوان حمله	توضیح	منبع
C01	عدم سرویس (علیه سیگنالینگ)	اتلاف منابع موجود سیستم وُپ از قبیل حافظه، پهنای باند و پردازنده با هدف از کار انداختن آن (با هدف از کار انداختن، سبلی از پیام‌های ساختگی سیگنالینگ به سمت سرور یا پایانه‌ی وُپ ارسال می‌شود)	(بوچرو همکاران، ۲۰۰۷)، (کولیالی 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)، (فیتاکینو کون و همکاران، ۲۰۰۸)، (هان و جیانگ، ۲۰۰۹)، (سیات سیکاس و همکاران، ۲۰۱۵)، (زین،

1. Challenge
2. Real-Time

منبع	توضیح	عنوان حمله	کد
(۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)			
(بوچرو همکاران، ۲۰۰۷)، (کولیالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)	برخی برنامه‌های کاربردی بانکی بر اساس شماره تلفن تماس گیرنده به او خدمات می‌دهد مهاجم با جعل شماره تلفن قربانی می‌تواند به اطلاعات بانکی و کارت اعتباری او دست پیدا کند	جعل شماره تلفن	C02
(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیالی 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)	در حمله‌ی «ربایش ثبت‌نام»، مهاجم هویت یک کاربر مجاز در سرور ثبت را جعل کرده و آدرس خود را به عوض او معرفی می‌کند، با این کار تماس‌های کاربر مجاز به سمت کاربر جعلی (مهاجم) ارسال می‌شود. سپس با استفاده از یک سرور «تغییر مسیر» به مشترک وبپ 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.	مرد میانی (ربایش اطلاعات ثبت‌نام و تغییر مسیر تماس)	C03
(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیالی 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)	با اجرای یکی از حملات «مرد میانی» مهاجم پیام‌های سیگنالینگ را رهگیری کرده و متن آن‌ها حتی بخشی یا همه صفاتشان را تغییر می‌دهد.	تغییر متن پیام‌ها	C04

منبع	توضیح	عنوان حمله	کد
(۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)			
(بوچرو همکاران، ۲۰۰۷)، (کولیالی 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 چنداوار کار، ۲۰۱۳)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)	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.	حمله لغو/خداحافظ	C05
(بوچرو همکاران، ۲۰۰۷)، (کولیالی 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 چنداوار کار، ۲۰۱۳)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)	مهاجم بسته‌های سیپ را با دستورات ناقص تغییر شکل داده و برای گره‌های حساس وُپ می‌فرستد، این امر موجب کاهش کارایی و یا خارج از دسترس شدن گره‌های ذکر شده می‌شود.	دستورات ناقص	C06
(بوچرو همکاران، ۲۰۰۷)، (کولیالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (ژانگ و همکاران، ۲۰۱۶)	در ارتباطات وُپِ 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 گذاشته شده از سوی خودش مجبور کرده و آن‌ها را فریب می‌دهد.	مرد میانی (کلاه‌برداری با جعل کلید تبادل)	C07
(بوچرو همکاران، ۲۰۰۷)،	مهاجم، قربانی را به برقراری تماس با پروکسی	جعل پروکسی	C08

کد	عنوان حمله	توضیح	منبع
		جعلی خود وادار کرده و کنترل تماس‌های او را در اختیار می‌گیرد و حتی مکالماتش را ضبط می‌کند.	(کولیالی 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)، (کولیالی 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، به صورت برخط و نابرخط، رمز عبور کاربر را حدس می‌زند.	(بوچرو همکاران، ۲۰۰۷)، (کولیالی 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)، (کولیالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوار کار، 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)، (کولیالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (فیتا کیتو کون و همکاران،

منبع	توضیح	عنوان حمله	کد
(هان و جیانگ، ۲۰۰۸)، (سان وین و چنداوارکار، ۲۰۱۳)، (ونیلا و منیکاندان، ۲۰۱۶)، (زین، ۲۰۰۷)			
(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیالی 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)	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 تلفن بانک برای به دست آوردن رمز عبور کارت‌های اعتباری و اطلاعات بانکی نیز می‌شود.	شنود (استراق سمع)	C13
(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیالی 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)	در واقع 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.	تغییر جریان صدا	C14
(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیالی 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)	بعد از انجام یک حمله «مرد میانی» و دسترسی به جریان رسانه‌ی آر تی پی بین دو گره وُپ، 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.	تغییر محموله‌ی آر تی پی	C15

کد	عنوان حمله	توضیح	منبع
			(۲۰۰۷)
C16	دست کاری سرآیند آر تی پی	با دست کاری شماره توالی و برجسب 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)، (کولیالی و لی یو، ۲۰۱۰)، (پرز بوترو و دونوسو، ۲۰۱۱)، (زین، ۲۰۰۷)
C17	تأخیر رسانه و آر تی 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 سیستم عامل 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 غیرقابل تحمل 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)، (کولیالی و لی یو، ۲۰۱۰)،

منبع	توضیح	عنوان حمله	کد
(مانونزا و همکاران، ۲۰۱۷)، (هان و جیانگ، ۲۰۰۹)	تحمیل می‌کند و یا با دست‌کاری و حذف موارد ثبتی در پایگاه اطلاعات تماس‌ها در هزینه‌های خود تقلب می‌کند.		
(پرز بوترو و دونوسو، ۲۰۱۱)، (فیتا کیتنوکون و همکاران، ۲۰۰۸)	ارسال میلیون‌ها درخواست از طریق پست الکترونیکی، پدیده‌ای به نام اسپم نامیده می‌شود. بازاریاب تلفنی می‌تواند از تلفن وُپ برای ارسال اسپم روی اینترنت (اس پی آی تی) استفاده کند. مهاجم سرورهای متعددی که فهرست‌هایی از شماره تلفن‌های وُپ را در اختیار دارند راه‌اندازی کرده و سپس این سرورها به شماره تلفن‌های مذکور متصل شده و در حجم بالایی پیام می‌فرستند این پیام‌ها از طریق تلفن قربانی‌ها پخش شده و یا صندوق پست صوتی آن‌ها را انباشته می‌کند.	پیام‌ها و تماس‌های ناخواسته (اس پی آی تی)	C38
(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (حسین پور و همکاران، ۲۰۱۶)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (سان وین و چنداوار کار، ۲۰۱۳)	در شبکه وُپ 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 به راحتی مورد حمله 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 پی را می‌دهند که قابل بو کشیدن توسط مهاجمین است.	دسترسی غیرمجاز به منابع شبکه	C39

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

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

منبع	توضیح	عنوان حمله	کد
بوترو و دونوسو، (۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)	و دریافت اطلاعات موردنظر خود دست می‌زند.	IP	
(بوچرو همکاران، ۲۰۰۷)، (کولیالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)	مهاجم با ارسال بسته‌هایی (دارای نقص در پشتی پروتکل شبکه) به سمت گره‌های شبکه منجر به کاهش عملکرد و حتی غیرفعال شدن آن‌ها می‌شود	بسته‌های ناقص	C22
(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (هان و جیانگ، ۲۰۰۹)	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.	سیل بسته‌های تی سی پی (با تنظیم پرچم SYN)	C23
(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیالی و لی یو، ۲۰۱۰)، (پکوری و ولتری، ۲۰۱۶)، (بوز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)، (ژانگ و همکاران، ۲۰۱۶)	مهاجم با ارسال سیلی از بسته‌های یکسان، شبکه را آسیب‌پذیر می‌کند.	بازپخش بسته‌های تی سی پی و یو دی پی	C24
(عزیز و همکاران، ۲۰۱۴)، (بوچرو همکاران، ۲۰۰۷)، (کولیالی و لی یو، ۲۰۱۰)، (حسین پور و همکاران، ۲۰۱۶)	تلفن‌های وُپ 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	ایجاد سرور تی اف تی پی ساختگی	C25

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 چنداوار کار، ۲۰۱۳)، (زین، ۲۰۰۷)
C26	تخلیه‌ی مخزن IP سرور دی اچ سی پی	با ارسال سیل درخواست به سوی دی اچ سی پی برای تولید مک آدرس‌های اتفاقی، مهاجم می‌تواند استخر آدرس‌های آی پی موجود در دی اچ سی پی را خالی کند. این حمله گره را از دریافت آدرس آی پی و متعاقباً امکان ارتباط با سایر سرورهای ویپ محروم می‌کند.	(بوچرو همکاران، ۲۰۰۷)، (کولیالی 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)، (کولیالی 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 تعیین شده ذخیره کنند، بدین ترتیب بافر سرریز شده و کدها برای سوءاستفاده مهاجم ر بوده می‌شود.	(بوچرو همکاران، ۲۰۰۷)، (کولیالی و لی یو، ۲۰۱۰)، (پرز بوترو و دونوسو، ۲۰۱۱)، (هان و جیانگ، ۲۰۰۹)، (زین، ۲۰۰۷)
C29	سیستم عامل	سیستم‌عامل‌هایی که گره‌های کنترلی و دروازه‌های شبکه ویپ روی آن‌ها کار می‌کنند مورد حملات شناخته‌شده و ناشناخته قرار می‌گیرند. مثل حملات به تلفن نرم‌افزاری ویپ که بر روی رایانه نصب می‌شود.	(زین، ۲۰۰۷)
C30	ویروس‌ها و	آلوده شدن سیستم‌عامل گره‌های شبکه به	(زین، ۲۰۰۷)

منبع	توضیح	عنوان حمله	کد
	ویروس‌ها و نرم‌افزارهای مخرب، موجب تخریب و تنزل سطح توانائی آن در رسیدگی به ترافیک وُپ می‌شود.	نرم‌افزارهای مخرب	
کتاب آموزشی	تجمع بیش از حد بسته‌های داده در صف انتظار و در نتیجه از بین رفتن آن‌ها	تراکم در شبکه‌ی داده	C31
کتاب آموزشی	شامل تأخیر سرریالی‌بیشن، تأخیر انتشار، تأخیر بسته‌بندی، تأخیر صف، تأخیر پردازش و تأخیر شبکه است که در مجموع نباید از محدوده ۳۰۰ تا ۴۰۰ میلی‌ثانیه (رفت و برگشت) تجاوز نماید.	تأخیرات انتقال (زیرساخت)	C32
کتاب آموزشی	تفاوت میان کمترین تأخیر و بیشترین تأخیر در دریافت بسته‌های داده را جیت‌ر می‌گویند، این زمان بایستی کمتر از ۴۰ میلی‌ثانیه باشد.	جیت‌ر	C33
(زین، ۲۰۰۷)	جلوگیری از عبور یا گم شدن پیام‌های سیگنالینگ و بسته‌های صوتی به دلیل استفاده از دیواره‌ی آتش و نت بین طرفین تماس وُپ	دیواره‌ی آتش و نت	C34

تقلب در هزینه‌های تماس^۱

تقلب در هزینه‌ی تماس توسط کاربر، یکی از موارد نقض یکپارچگی و صحت اطلاعات در ارتباطات وُپ محسوب می‌شود. عزیز و همکاران^۲ (۲۰۱۴) یک معماری کنترل توزیع‌شده برای تشخیص حمله به شبکه‌های سیپ پیشنهاد دادند، آن‌ها تقلب در هزینه‌ی تماس را به‌عنوان نمونه‌ای برجسته از این دست حملات معرفی کردند. معماری «کربروس»^۳ روش جدیدی است که تقلب‌ها را از طریق تحلیل مستقیم رویدادهای اُسی اس^۴ 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^۱، ۲۰۱۷).

ناسازگاری عملکرد و امنیت

معمولاً استفاده از راهکارهای امنیتی موجب کاهش سرعت عملیات و در نتیجه کاهش کیفیت خدمات بی‌درنگ وُپ می‌شود، به عبارت دیگر 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 باین حال با توجه به هزینه‌ها و فواید هر روش، سازمان‌های مختلف می‌توانند از روش‌های مختلف امنیتی بنا به نیاز خود استفاده نمایند (حسین و همکاران^۲، ۲۰۱۶).

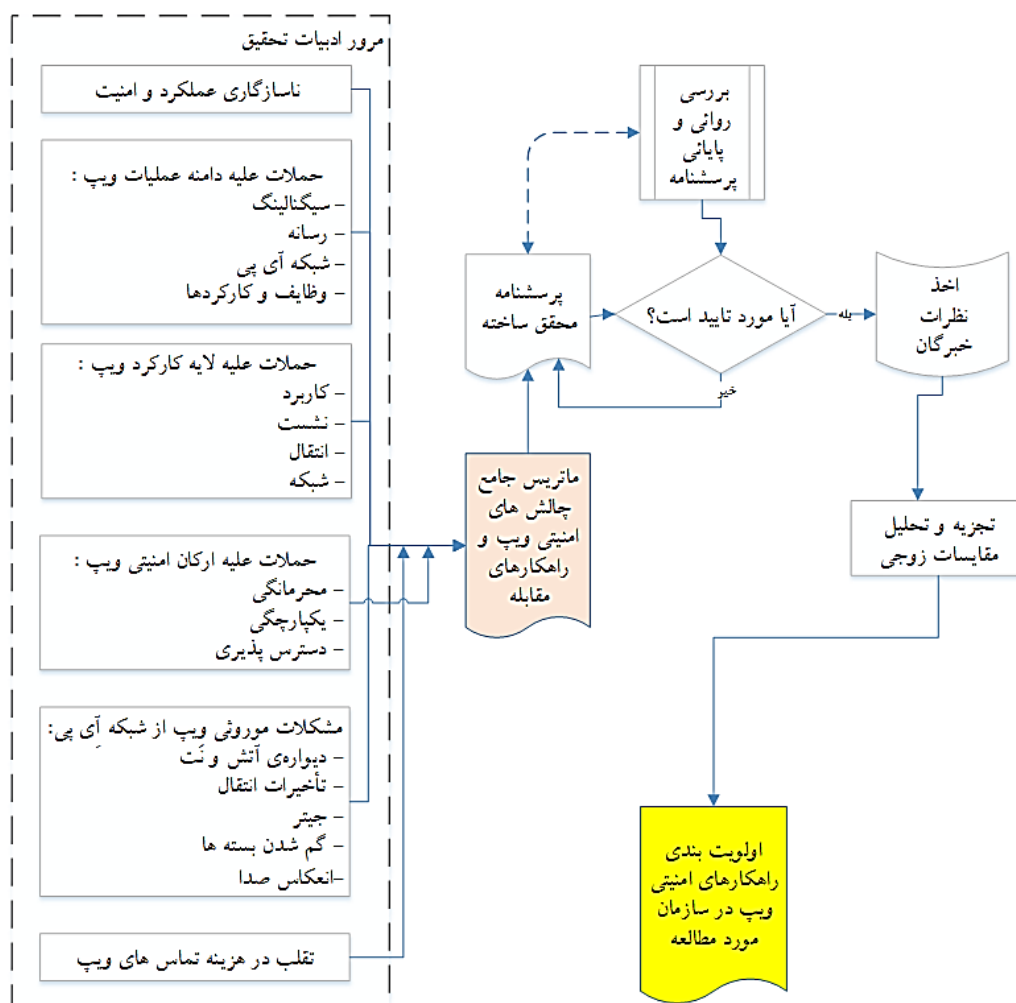
شمای جامع از چالش‌ها و راهکارها

طیف حملات صورت گرفته روی سیستم وُپ 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 وُپ 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 شناسایی شده با توجه به ساختار شبکه‌ی آی.پی و تجهیزات وُپ 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.

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 استفاده شده 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 گردآوری شده مورد تحلیل قرار گرفته 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، جامعه آماری شامل خبرگان، صاحب نظران و کارشناسان ارشد مراکز تلفن و امنیت فناوری اطلاعات و ارتباطات «ناجا» و «نیروهای مسلح» است که مدارک تحصیلی ۸۰ درصد آن ها فوق لیسانس و دکترا است. طبق نظرسنجی تحقیق، جامعیت چالش های امنیتی شناسایی شده با ۷۴ درصد نظر موافق به تأیید خبرگان رسید بنابراین پرسشنامه ی تحقیق از

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

جدول ۴: بخشی از پرسشنامه در حوزه سیگنالینگ ویپ

حوزه	چالش	سؤالات	مقیاس			
			خیلی زیاد	زیاد	متوسط	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 ثبت نام در سیپ سرورها و جلوگیری از هرگونه تغییر مسیر تماس ویپ به نقطه‌ی دلخواه مهاجم ضروری است				
	C04	باید از رهگیری پیام‌های سیگنالینگ 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 وُپ، حین عملیات احراز هویت الزامی است	
					ارسال سیلی از پیام‌های ساختگی سیگنالینگ به سمت سرورها یا پایانه‌های وُپ خطرناک است	C09
					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	C10

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

تجزیه و تحلیل داده‌ها

در این تحقیق، برای تجزیه و تحلیل 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 وُپ آن‌ها دوه‌دو 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 مورد استفاده در مقایسات زوجی

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

وقتی ارجحیت یک عامل نسبت به عامل دیگر بسیار قابل توجه باشد	۷
وقتی ارجحیت یک عامل نسبت به عامل دیگر بسیار بسیار قابل توجه باشد	۹

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 در واقع 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 گردآوری شده اعتماد کرد. تجربه نشان داده که اگر نرخ سازگاری کمتر از $0/10$ باشد سازگاری مقایسه‌ها قابل قبول 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 تجزیه و تحلیل داده‌های تحقیق

۱) طبق جدول ۶ شاخص‌های به دست آمده 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 ۶. گروه‌بندی چالش‌های امنیتی وُپ بر اساس دامنه‌ی حملات

شماره گروه	عنوان گروه چالش	شامل چالش‌های زیر (از جدول ۳)
گروه ۱	اختلال در راه‌اندازی و مدیریت تماس‌های وُپ	۱ و ۵ و ۶ و ۸ و ۱۱
گروه ۲	کلاهبرداری از سیستم وُپ از طریق جعل	۲ و ۳ و ۴ و ۷ و ۹ و ۱۰

اطلاعات		
اختلال در تبادل بسته‌های صوتی وُپ	۱۷ و ۱۶ و ۱۵ و ۱۴ و ۱۳ و ۱۲	گروه ۳
سوءاستفاده از اطلاعات سیستم وُپ	۳۷ و ۲۸ و ۲۵ و ۲۱ و ۲۰ و ۱۹	گروه ۴
اختلال در عملکرد شبکه و زیرساخت وُپ	۳۹ و ۳۶ و ۲۷ و ۲۶ و ۲۴ و ۲۳ و ۲۲ و ۱۸	گروه ۵
اختلال در کیفیت شبکه و خدمات وُپ	۳۴ و ۳۳ و ۳۲ و ۳۱ و ۳۰ و ۲۹	گروه ۶
موانع بهره‌برداری از وُپ	۴۳ و ۴۲ و ۴۱ و ۴۰ و ۳۸ و ۳۵	گروه ۷

۲) یک‌بار ماتریس مقایسات زوجی تشکیل و هفت گروه به دست آمده 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 به دست آمده 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 در واقع 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 دارای بالاترین عدد اهمیت است این موضوع مؤید این نکته است که گروه چالش‌ها تحت عنوان «کلاه‌برداری از سیستم وُپ از طریق جعل اطلاعات» از بالاترین میزان اهمیت برخوردار است و البته گروه ۶ با عنوان «اختلال در کیفیت شبکه و خدمات وُپ» 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	۴	۵	۶	۷
عدد اهمیت	۳/۹۶	۴/۱۸	۴/۰۵	۴/۰۳	۴/۱۳	۳/۸۲	۳/۹۷

جدول شماره ۸. رتبه‌بندی گروه‌های چالش

رتبه	وزن گروه	گروه
۱	۰/۱۴۸۵	گروه ۲
۲	۰/۱۴۶۸	گروه ۵
۳	۰/۱۴۳۹	گروه ۳
۴	۰/۱۴۳۲	گروه ۴
۵	۰/۱۴۱۱	گروه ۷
۶	۰/۱۴۰۷	گروه ۱
۷	۰/۱۳۵۷	گروه ۶

(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 هر کدام از روی نگاشت ماتریس جامع امنیت و پ ۷ معرفی و نتایج تفسیر می‌گردد. نتایج حاصل از اقدامات فوق طبق جدول ۱۰ قابل مشاهده 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 قرار گرفته‌اند بنابراین تمامی راهکارهای دفاعی شناسایی شده در قالب ماتریس جامع امنیت وُپ که در مقابله با چالش‌های مذکور مؤثر باشند در اولویت‌بندی نهائی راهکارهای دفاعی مدنظر قرار می‌گیرند.

با مراجعه به ماتریس جامع امنیت وُپ، 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

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

جدول ۱۰. محاسبه وزن و اولویت بندی نهائی چالش ها و تعیین ۱۰ چالش برتر

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

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

اولویت	راهکار دفاعی
۱	جداسازی VLAN های ترافیک صوت و داده
۲	احراز هویت سیگنالینگ (ثبت نام تلفن در سیپ سرور) با IPsec و سایر پروتکل های تبادل کلید مانند ژانگ، AKEP3
۳	احراز هویت در گاه (پورت) با IEEE 802.1x
۴	استفاده از سیستم تشخیص نفوذ (IDS)
۵	مدل سازی ترافیک عادی سیپ
۶	استفاده از صافی های «مبتنی بر آستانه» و «اطلاع از محتوای محدود»
۷	استفاده از نظریه‌ی آنتروپی برای تشخیص حملات عدم سرویس بر اساس ترافیک ثبت شده

اولویت	راهکار دفاعی
	استفاده از سیستم تشخیص حملات انکار سرویس توزیع شده با استفاده از سیستم خیره (سعدآبادی، {۲۹#۲۰۱۶}
۸	اجرای تنظیمات دیوارهی آتش
۹	استفاده از پروتکل S/MIME
۱۰	استفاده از پروتکل H.235
۱۱	استفاده از VPN، SRTP، TLS و 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 وُپ 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^۱ در سال ۲۰۱۶، تکنیک‌های زیر را برای کاهش حملات امنیتی وُپ پیشنهاد داده است:

- رمزگذاری توسط دستگاه یا کاربر که بدون تردید می‌تواند تأخیر بیش از حد در شبکه یا سربار و پیچیدگی عملیاتی به وجود آورد.
 - رمزگذاری سیگنالینگ در دروازه‌های اتصال به اینترنت، به وسیله‌ی سیپ و تی ال اس روی لایه حمل و نقل.
 - استفاده از وی پی ان برای ارتباط تلفن‌های راه دور با شبکه، خصوصاً هنگامی که HTTPS یا اس آر تی پی در دسترس نباشد.
 - استفاده از رمزهای عبور قوی، برای دسترسی به صندوق پست صوتی.
 - حذف پیام‌های حساس پست‌های صوتی، به محض این که کاربر به آن‌ها گوش داد.
- چنانچه ملاحظه می‌شود پیشنهادهای فوق، راهکارهای دوم و سوم پیشنهادی همچنین چالش اشاره شده در فصل دوم یعنی ناسازگاری امنیت و عملکرد وُپ را تصدیق می‌کند اما استفاده از وی.پی.ان که توسط اکثریت تحقیقات مرور شده و مؤسسات امنیتی به منظور برقراری ارتباط امن تلفن‌های راه دور با سرورهای وُپ سازمان‌ها مورد تأکید و توصیه قرار گرفته در اولویت‌بندی ما در سطح پائین تری قرار گرفته که دلیل آن واضح و ناشی از استفاده‌ی تجهیزات وُپ دانشگاه علوم انتظامی از شبکه‌ی اینترنت اختصاصی و بسته است که امکان هرگونه دسترسی غیرمجاز و بدون کنترل به اینترنت از طریق سرویس وی.پی.ان را سلب کرده است. به علاوه در صورت نیاز به استفاده از وی.پی.ان برای ارتباطات وُپ این کار توسط مدیریت شبکه قابل اعمال و در صورت انجام برای ارتقای امنیت بسیار مؤثر خواهد بود. چنانچه ماتریس جامع امنیت وُپ نشان می‌دهد اجرای راهکار اول پیشنهادی یا همان جداسازی VLAN‌های ترافیک صوت و داده، هم‌زمان باعث توقف حجم بسیاری از حملات و تهدیدات امنیتی وُپ می‌شود، با اعمال این راهکار مهاجمان نمی‌توانند از رایانه‌ها و ایستگاه‌های کاری مستقر روی شبکه‌ی داده برای رخنه به سامانه‌های وُپ 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 پیکربندی شده‌اند اجازه مسیریابی خواهند داد. تلفن‌های وُیپ پورت دومی برای اتصال رایانه دارند. فناوری (802.1q) VLAN 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، به‌عنوان مثال 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. در مجموع 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.

از آنجاکه اتصال بین تلفن‌ها و سرورهای وُیپ با استفاده از پروتکل سیپ انجام می‌گیرد هنگامی که 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 در واقع ترکیبی از سه پروتکل AH، ESP و IKE است که در دو حالت تونل^۱ و انتقال^۲ 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 وُپ بزرگ مقیاس راحت نخواهد بود. روش‌هایی همچون استفاده از «مراکز صدور گواهی»^۱ و «پروتکل‌های امنیتی سیستم نام دامنه»^۲ 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 در گاه از استانداردهای 802.1x استفاده می‌کند تا دستگاه‌های باسیم و بی‌سیم 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 وُپ 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 وُپ را معرفی می‌کند و برای هر کدام 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 وُپ را فراهم می‌کند؛ و به جرأت می‌توان گفت الگوی مناسب و جامعی از حیث دانش شناخت آسیب‌ها و اقدامات امنیتی وُپ به ایشان ارائه می‌دهد.

بنابراین، استفاده از جدول جامع ارائه‌شده (جدول ۳)، علاوه بر نمایش مجموعه راهکارهایی که یک مدیر امنیت وُپ 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 وُپ می‌تواند کمک بسزایی نماید. همچنین مدیران فناوری

1. Certification Authority(CA)

2. Domain Name System Security(DNSSec)

اطلاعات در تصمیم‌گیری و نظارت خود جهت به‌کارگیری وُپ می‌بایست سه راهکار پیشنهادی را در اولویت نظارت بر پیاده‌سازی وُپ لحاظ نمایند.

حفظ محرمانگی، یکپارچگی و دسترس‌پذیری ارتباطات متنوع وُپ 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 وُپ 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 وُپ 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 وُپ 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 وُپ سازمان‌ها مورد تحقیق بیشتری قرار گیرد.
 - حتی‌المقدور از سامانه‌های جامع، بومی و یکسان وُپ استفاده تا آموزش متخصصین، نگهداشت و از همه مهم‌تر اعمال سیاست‌های امنیتی ساده شود.
 - در مورد تأثیرات کاربرد دستگاه‌های «کنترل‌کننده‌ی ارتباطات وُپ در لبه‌ی شبکه» یا **SBC**^۱ ها که راهکارهای جامعی در رفع چالش‌های امنیتی وُپ ارائه می‌کنند تحقیق شود.

منابع

سعدآبادی. ع، امیرشاهی. ب، (۱۳۹۵)، تشخیص حملات انکار سرویس توزیع شده 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). An 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*.