بسم الله الرحمن الرحيم

دانشگاه یزد

دانشکده‌ی مهندسی برق و کامپیوتر

گروه مهندسی کامپیوتر

پایان‌نامه

برای دریافت درجه‌ی کارشناسی‌ارشد

مهندسی فناوری اطلاعات - شبکه‌های کامپیوتری

ارزیابی کمی و کیفی حملات DNS flooding به SIP VoIP و روش‌های مقابله با آن

استاد راهنما: دکتر فضل‌اله ادیب‌نیا

استاد مشاور: دکتر محمدحسن شیرعلی شهرضا

پژوهش و نگارش: احمد اخلاقی ظفری

مهرگان ۱۳۸۷

به پاس تعبیر عظیم و انسانی‌شان از کلمه‌ی ایثار و از خود گذشتگی

به پاس عاطفه‌ی سرشار و گرمای امیدبخش وجودشان که در این سردترین روزگاران، بهترین پشتیبان است

به پاس قلب‌های بزرگشان که فریادرس است و سرگردانی و ترس در پناهشان به شجاعت می‌گراید

و به پاس محبت‌های بی‌دریغشان که هرگز فروکش نمی‌کند

این مجموعه را به پدر و مادر عزیزم تقدیم می‌کنم.

شکر و سپاس خداوند یکتا را که توفیق کسب علم و معرفت عطا فرمود و قطره‌هایی از دریای علم و دانش را در کویر تشنه‌ی دل، فرو بارانید. وی را می‌ستایم که مرا مشمول عنایت بی‌انتهایش قرار داد تا بتوانم این مجموعه را به پایان رسانم.

بی‌تردید نگارش این پایان‌نامه مرهون زحمات بی‌شائبه‌ی استادان ارجمندی است که از ابتدای تحصیل، مرا مورد لطف و محبت خود قرار داده‌اند. لذا بر خود وظیفه می‌دانم که از یکایک این بزرگواران به خصوص آقای دکتر فضل‌اله ادیب‌نیا و همچنین آقای دکتر محمدحسن شیرعلی شهرضا به خاطر راهنمایی‌های ارزشمند در مراحل انجام کار و تصحیح پایان‌نامه سپاس‌گزاری نمایم.

از تمامی دوستان و عزیزانی که مرا به هر نوعی در ارائه هر چه بهتر این پایان‌نامه یاری کرده‌اند نیز تشکر و قدردانی می‌کنم.

این پایان‌نامه با حمایت‌های مالی

مرکز تحقیقات مخابرات ایران

به انجام رسیده است.

مدیریت تحصیلات تکمیلی	**صورتجلسه دفاعیه پایان نامه دانشجوی** **دوره کارشناسی ارشد**	شناسه: ب/ک/۳ شماره: تاریخ: پیوست:

جلسه دفاعیه پایان نامه تحصیلی آقای: *احمد اخلاقی*

دانشجوی کارشناسی ارشد رشته / گرایش: *مهندسی فناوری اطلاعات گرایش شبکه‌های کامپیوتری*

تحت عنوان: *ارزیابی کیفی و کمی حملات DNS Flooding به SIP VOIP و روشهای مقابله با آن*

و تعداد واحد: ۶ در تاریخ ۱۳۸۷/۷/۱۸ با حضور اعضای هیأت داوران (به شرح ذیل) تشکیل گردید.

پس از ارزیابی توسط هیأت داوران، پایان نامه با نمره: به عدد ۱۹/۷۵ **به حروف** نوزده و هفتاد و پنج صدم **و درجه** عالی **مورد تصویب قرار گرفت.**

عنوان	نام و نام خانوادگی	امضاء
استاد / استادان راهنما	دکتر فضل ا... ادیب‌نیا	
استاد / استادان مشاور	دکتر محمدحسن شیرعلی	
متخصص و صاحبنظر داخلی	دکتر مهدی‌آقا صرام	
متخصص و صاحبنظر خارجی	دکتر سیدمرتضی بابامیر (از دانشگاه کاشان)	

نماینده تحصیلات تکمیلی دانشگاه (ناظر)

نام و نام خانوادگی: علی دهقانی

امضاء:

چکیده:

یک حمله‌ی ساده و در عین حال موثر DoS (اخلال در سرویس‌دهی) علیه سرویس‌دهنده‌های SIP (قرارداد آغاز نشست) غرق کردن سرویس‌دهنده توسط درخواست‌های برقراری تماس با آدرس‌هایی است که وجود خارجی نداشته و غیر قابل ترجمه می‌باشند.

در اکثر تحقیقاتی که در زمینه‌ی امنیت شبکه‌های کامپیوتری انجام شده، جنبه‌های مختلف امنیتی و روش‌های متفاوت حمله از دید کیفی بررسی گردیده و تحلیل کمی معیارهای امنیتی شبکه، کمتر مورد توجه قرار گرفته است. در این پایان‌نامه، یک مدل صف‌بندی برای ارزیابی حملات DoS تحلیل گردیده و شبکه‌ای که مورد حمله‌ی DoS واقع شده، با یک زنجیره‌ی مارکوف دوبعدی نمایش داده می‌شود. به کمک این مدل، می‌توان یک الگوریتم کارآ برای محاسبه‌ی توزیع احتمال ثابت پیاده‌سازی نمود که برای تعیین سایر معیارهای کارآیی، مانند درصد اشغال حافظه‌ی درخواست‌های با آدرس عادی و درخواست‌های با آدرس غیر قابل ترجمه، به کار برده می‌شود.

در اینجا ما نوع خاصی از حملات DoS را بررسی نموده که هدف آنها، سرویس‌دهنده‌های VoIP (صدا بر روی IP) است که از SIP استفاده می‌کنند. این حملات از DNS (سرویس نام ناحیه) استفاده می‌نمایند. با ارسال سیل‌آسای درخواست‌های برقراری تماس با آدرس‌هایی که وجود خارجی نداشته و غیر قابل ترجمه می‌باشند به سوی یک سرویس‌دهنده‌ی SIP، می‌توان آن را برای مدت قابل توجهی از سرویس‌دهی بازداشت. ما روش‌های متفاوت کاهش اینگونه مشکلات را بررسی کرده و نشان می‌دهیم که افزایش منابع برای کنترل این نوع حملات کافی نیست. به عنوان یک راه حل موثرتر، ما روش حافظه‌ی نهان DNS را تحلیل نموده که بر اساس کاربرد غیرانسدادی حافظه‌ی نهان DNS عمل می‌کند. سپس کارآیی این روش را بر اساس اطلاعات مختلفی که جمع آوری شده، نشان داده و راندمان سیاست‌های گوناگون جایگزینی حافظه‌ی نهان را مقایسه می‌نماییم. در نهایت می‌بینیم روش جایگزینی LFU (کمترین تعداد مراجعات) بهترین نتیجه را برای کاهش آثار این حمله فراهم می‌کند.

فهرست مطالب

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فصل اول

مقدمه

برخلاف PSTN (شبکه‌ی تلفن عمومی[1]) ارائه‌دهندگان VoIP (صدا بر روی IP[2]) به دلیل مزیت ارزان بودن آن، رشد بسیار زیادی دارند. اما در این میان، برای استفاده کنندگان از VoIP مشکلات ارتباطی جدیدی مانند گم شدن بسته و QoS (کیفیت سرویس[3]) نیز وجود دارد. شبکه‌های سوییچ مداری[4] موجود، تهدیدات امنیتی چندانی نداشته چون از یک محیط ارتباطی محصور اختصاصی تک منظوره استفاده می‌نمایند. اما در مورد سرویس‌های VoIP که بر پایه‌ی یک محیط ارتباطی باز همچون اینترنت بنا نهاده شده‌اند، سیستم‌ها کاملا در معرض تهدیدات مهاجمان قرار دارند. به خاطر فراهم نمودن یک سرویس فراگیر، هر کاربر با هر سرعت ارتباطی دلخواه به سرویس‌دهنده‌های VoIP دسترسی دارد. بنابراین یک مهاجم می‌تواند با هزینه‌ی اندکی، یک حمله‌ی DoS (اخلال در سرویس‌دهی[5]) را علیه سرویس‌دهنده‌های VoIP انجام دهد.

SIP (قرارداد آغاز نشست[6]) استانداردی برای ایجاد[7]، نگهداری[8] و خاتمه‌ی[9] یک نشست ارتباطی متقابل است که می‌تواند شامل اجزاء چند رسانه‌ای نیز باشد. SIP بسیار به DNS (سرویس نام ناحیه[10]) وابسته بوده و مهاجمان با توجه به این موضوع، حمله‌ی DoS را با سیل آدرس‌های غیر قابل ترجمه[11] به راه می‌اندازند.

منظور از حملات DoS ممانعت یا کاهش دسترسی کاربران مجاز به یک سرویس یا منبعی از شبکه و یا از کار انداختن سرویس‌دهنده‌هایی است که این خدمات را ارائه می‌دهند [2-1]. یک مهاجم به روش‌های متفاوتی می‌تواند به یک ساختار VoIP حمله‌ی DoS انجام دهد [3]. مهاجمان می‌توانند علاوه بر برقراری تعداد زیادی تماس بیهوده، از برخی مشخصه‌های قرارداد به کار رفته در VoIP نیز برای ایجاد بار اضافه بر روی سرویس‌دهنده‌ها استفاده نمایند. همچنین ممکن است

---

[1] Public Switched Telephone Network
[2] Voice over Internet Protocol
[3] Quality of Service
[4] Circuit switch
[5] Denial of Service
[6] Session Initiation Protocol
[7] Initiating
[8] Modifying
[9] Terminating
[10] Domain Name Service
[11] Irresolvable

ساختار VoIP بر اثر حملات DoS به اجزاء آن یا به قراردادها و لایه‌هایی که در بالای آن قرار دارند در هم شکسته شود (مانند قراردادهای مسیریابی یا TCP[1]).

در این پایان‌نامه، ما به نوع خاصی از حمله‌ی DoS می‌پردازیم که از DNS استفاده نموده و می‌دانیم که SIP بسیار به سرویس نام ناحیه وابسته است و به همین دلیل آن را حمله‌ی SIP DNS می‌نامند. ما نشان می‌دهیم که راه اندازی این حمله ساده بوده و پردازش پیام‌ها و درخواست‌های برقرای تماس را به میزان قابل توجهی کند می‌کند.

تاکنون و با استفاده از شبیه‌ساز (ارزیابی کیفی[2])، بررسی‌های مختلفی در این زمینه صورت گرفته و نشان داده شده است که افزایش منابع به تنهایی برای مقابله با این مشکل، کافی نیست. روش‌های گوناگونی نیز برای کاهش اثرات این حمله ارائه شده است، از جمله راه حلی که بر اساس کاربرد غیرانسدادی[3] حافظه‌ی نهان عمل می‌کند. در اینجا ما ضمن بررسی نتایج تست این روش و همچنین سیاست‌های جایگزینی مختلف در حافظه‌ی نهان، خواهیم دید الگوریتم LFU (کمترین تعداد مراجعات[4]) بهترین نتیجه را برای کاهش آثار این حمله فراهم می‌کند.

می‌دانیم در ارزیابی عملکرد شبکه‌ها بر کاربردترین روش، شبیه‌سازی است. مهم‌ترین دلیل آن هم سادگی استفاده از شبیه‌ساز در مقایسه با سایر روش‌هاست، اما انتقاد وارد به آن این است که محدود به فرضیات می‌باشد.

در این راستا، پیشنهاد ما استفاده از روش‌های تحلیلی، مانند نظریه‌ی صف است. ما یک مدل صف‌بندی را برای ارزیابی این حمله پیشنهاد نموده (تحلیل صف سرویس‌دهنده‌ی تحت حمله با استفاده از زنجیره‌ی مارکوف دوبعدی) و به ارزیابی کمی[5] این حمله می‌پردازیم.

---

[1] Transmission Control Protocol
[2] Qualitative
[3] Non blocking
[4] Least Frequently Used
[5] Quantitative

فصل دوم

تعریف موضوع

به خاطر فراگیر شدن شبکه‌های ارتباطی و کامپیوتری گسترده، اینترنت در سراسر جهان نفوذ سریعی نمود و اکنون به یکی از اجزاء ضروری زندگی روزمره‌ی ما تبدیل شده است.

اما اینترنت به دلیل دسترسیهای غیرمجاز به آن، باعث مشکلات امنیتی و زیانهای مالی بسیاری نیز گردیده و به همین علت، امنیت شبکه در دهه‌های اخیر مورد توجه زیادی قرار گرفته است. اولین مورد امنیتی شبکه‌ی آرپانت که به اعلام عموم رسید را کلیف استول[1] در ۱۹۸۶ کشف نمود [4]. بعدها آرپانت در ۱۹۸۸ کرم موریس[2] یعنی اولین حمله‌ی خودکار بر علیه امنیت شبکه را تجربه کرد [4]. هرچه شبکه‌های کامپیوتری سریعتر و بزرگ‌تر شده و امکانات آنها افزایش پیدا می‌کند، امنیت شبکه چه از نظر تئوری و چه از دید برنامه‌های مهندسی نیز بیشتر مورد توجه قرار می‌گیرد.

امروزه حمله به شبکه، امری عادی شده است. اخلال در سرویس‌دهی، کرم، اسب تروا[3] و ویروس، انواع حمله‌های مهم می‌باشند که هر کدام از اینها مشکلات جدی را به وجود می‌آورند.

در شبکه‌های سوییچ مداری موجود، تهدیدات امنیتی اندکی وجود دارد زیرا از یک محیط ارتباطی محصور اختصاصی برای یک کاربرد مشخص به نام صدا استفاده می‌شود. اما در یک محیط ارتباطی باز همچون اینترنت، راه اندازی یک حمله علیه سرویس‌دهنده‌ی ارتباط تلفنی بسیار ساده است چون سرویس‌های VoIP بر اساس فناوریهای استاندارد شده و مشخص (مانند SIP یا H.323)، استفاده از سرویس‌دهنده‌هایی که از سراسر اینترنت قابل دسترسی است، پیاده‌سازی به کمک نرم‌افزار و به کار بردن تجهیزات سخت‌افزاری همه منظوره، عمل می‌کنند [5]. یکی از تهدیدات امنیتی بزرگ، ارسال سیل‌آسای پیام‌های بیهوده یا غیر قابل استفاده است که می‌تواند مقدار قابل توجهی از منابع سرویس‌دهنده‌ی SIP را هدر دهد. مهاجم می‌تواند به راحتی به جای برقراری تعداد زیادی تماس تلفنی پر هزینه، هزاران درخواست جعلی برقراری ارتباط VoIP را ارسال نماید. به راه انداختن اینگونه حملات، ساده است و با وجود یک ارتباط اینترنتی پرسرعت، هزینه‌ی چندانی هم برای مهاجم ندارد.

---

[1] Cliff Stoll
[2] Morris worm
[3] Trojan horse

تاکنون برای مقابله با حملات DoS روش‌های زیادی پیشنهاد شده است [6-10]. در این روش‌ها محققان معمولا به کشف حملات و انجام واکنشی علیه آنها پرداخته‌اند. شیوه‌های کشف حالت غیرعادی[1] و یا پویش امضای حمله[2] می‌توانند برای تشخیص شروع یک حمله به کار روند. برای کاهش آثار حمله، واکنش‌ها نیز می‌تواند حالت پیشگیری و یا مقابله‌ای داشته باشند. این روش‌ها برای کاهش تبعات حمله، بسته‌های مهاجم را بلوکه کرده، برای کشف منبع حمله، بسته‌ها را ردیابی نموده و روش‌های پیشگیری را برای فیلتر نمودن بسته‌های مهاجم به کار می‌برند [6]. به کمک شیوه‌های موثر تشخیص و فیلتر کردن، می‌توان رفتار حملات DoS را تشخیص داده و آثار آنها را به صورت کمی ارزیابی نمود. روشی به نام تحلیل Backscatter ترافیک عبوری شبکه‌ی اینترنت را نظارت[3] کرده و اطلاعاتی در مورد شیوع فعالیتهای بدخواهانه[4] از نوع DoS فراهم می‌کند [11]. رویه‌ای نیز طراحی شده که حملات DoS را بر اساس محتویات سرآیند بسته‌ها دسته بندی نموده، تغییرات انفجاری را در طیف رفتار بسته‌ها بررسی کرده و یک تحلیل آماری از اینگونه حمله‌ها به دست می‌آورد که می‌تواند در مطالعه کمی این نوع حملات و تهیه سیستم‌های دفاعی به کار رود [8].

تا به حال از مدل‌های ریاضی، کمتر برای تحلیل حملات DoS استفاده شده است. این موضوع ما را بر آن داشت تا با ارائه‌ی مدل‌های ریاضی عمومی‌تر (مانند مدل‌های صف‌بندی) به تجزیه و تحلیل حملات DoS بپردازیم. در این رابطه، یک مدل صف‌بندی ساده برای حمله‌ی SYN Flood که یکی از حملات معروف DoS می‌باشد ارائه شده است [6]. دو مدل صف‌بندی دیگر نیز برای محاسبه‌ی تغییر در تاخیر[5] و احتمال گم شدن بسته در حملات DoS پیشنهاد شده است [9]. آثار حملات DoS بر متغیرهایی که در تشخیص حمله به کار می‌روند مانند نرخ ورود بسته[6]، نرخ رشد صف[7] و زمان پاسخ[8] نیز بررسی شده‌اند [10]. اما با استفاده از یک مدل صف‌بندی

---

[1] Anomaly detection
[2] Signature scan
[3] Monitor
[4] Malicious
[5] Jitter
[6] Arrival rate
[7] Queue growth rate
[8] Response time

عمومی‌تر مانند زنجیره‌ی مارکوف دوبعدی[1]، با دقت بیشتری می‌توان حملات DoS واقعی را بررسی نمود.

بنابراین با توجه به کمبود نتایج حاصل از تحلیلهای کمی حملات DoS، یک مدل تئوری برای مطالعه‌ی آنها ارائه گردیده و یک مدل صف‌بندی دوبعدی برای ارزیابی کارآیی شبکه‌ای که تحت حمله‌ی DoS قرار دارد استفاده می‌شود. مدل صف‌بندی مذکور از این جهت تازگی دارد که در آن برای درخواست‌های ترجمه‌ی آدرس عادی و درخواست‌های ترجمه‌ی آدرس مهاجم، دو صف مجزا با توزیع زمان سرویس[2] مختلف در نظر گرفته می‌شود. در این مدل، تمام درخواست‌های ترجمه‌ی آدرس، از یک فضای حافظه استفاده نموده و به محض ورود یک درخواست ترجمه‌ی آدرس، در صورت وجود، یک فضای خالی به آن اختصاص داده شده و در غیر این صورت بلوکه می‌شود. درخواست‌های ترجمه‌ی آدرس عادی و مهاجم رفتار متفاوتی دارند (مثلا زمان اشغال حافظه‌ی[3] آنها دارای توزیع احتمال متفاوتی است) بنابراین برای تحلیل حملات DoS فقط می‌توان از زنجیره‌ی مارکوف دوبعدی (نه کمتر و نه بیشتر) استفاده نمود. همچنین توزیع احتمال ثابت[4] زنجیره‌ی مارکوف محاسبه می‌شود که به کمک آن می‌توان برخی از معیارهای امنیتی مهم را به دست آورد و این معیارهای امنیتی نیز به نوبه‌ی خود در تنظیم گزینه‌های مهمی مانند اندازه‌ی حافظه و مدت زمان نگهداری درخواست‌های ترجمه‌ی آدرس به کار می‌روند تا حداکثر میزان سرویس‌دهی تحت حملات مشخص، تضمین شود.

۲-۱. اخلال در سرویس‌دهی

حملات DoS معمولا مزاحمتهای زیادی را برای شبکه‌های کامپیوتری ایجاد می‌کنند. حمله‌ی DoS را می‌توان اینگونه تعریف نمود: تلاش مهاجمان برای جلوگیری از دسترسی کاربران

---

[1] Two-dimensional Markov chain
[2] Service time distribution
[3] Buffer occupancy time
[4] Stationary probability distribution

مجاز به سرویس‌های شبکه. به خاطر مشکلات زیادی که حملات DoS ایجاد کرده‌اند، تحقیقات زیادی در این زمینه انجام شده است. حملات DoS انواع مختلفی دارد که متداول‌ترین آنها، حمله به روش ارسال سیل‌آسای بسته‌های اطلاعاتی است. مهاجمان می‌توانند شبکه ای را با ارسال تعداد زیادی از بسته‌های اطلاعاتی غرق کنند تا به این ترتیب، منابع اصلی و محدود سیستم، تلف شود. برخی حملات DoS عملکرد طبیعی تجهیزات ارتباطی شبکه را مختل کرده و یا حتی اطلاعات رمزنگاری شده را در حین انتقال، دستکاری می‌نمایند [12]. همچنین ممکن است تعدادی از دیگر کامپیوترهای متصل به شبکه برای مشارکت در حمله به خدمت گرفته شده تا هدف را با سیل بسته‌های مهاجم، غرق نمایند که این روش به حمله‌ی DDoS (DoS توزیع شده[1]) معروف است. حمله‌ی بازتابی[2] که نوع خاصی از حملات DDoS است کامپیوترهای به خدمت گرفته شده را به عنوان بازتابنده به کار می‌گیرد تا هویت مهاجمان، مخفی مانده و یا قدرت حمله چند برابر شود. بنابراین، حملات بازتابی می‌توانند آسیبهای شدیدتری را به شبکه‌ها وارد نمایند.

انگیزه‌ی حمله‌ی DoS چیزی جز خراب‌کاری نیست و انواع آن به صورت زیر می‌باشد:

الف- جلوگیری از دسترسی به اطلاعات. چنانچه حمله‌ی DoS روی اطلاعات سیستم انجام شود اطلاعات سیستم غیر قابل دسترسی می‌گردد. این نوع حمله به وسیله‌ی نابود کردن اطلاعات یا تغییر اطلاعات به فرمی که غیر قابل استفاده گردد انجام می‌گیرد. روش دیگر این حمله آن است که اطلاعات همچنان بدون تغییر می‌ماند اما در مکانی غیر قابل دسترسی قرار داده می‌شود.

ب- جلوگیری از سرویس‌دهی سیستم‌های نرم‌افزاری. نوع دیگر حمله‌ی DoS آن است که سیستم‌های نرم‌افزاری که اطلاعات را نمایش داده یا آنها را تغییر می‌دهند، هدف حمله قرار می‌گیرد. این حمله معمولا به کامپیوتری انجام می‌گیرد که آن سیستم را اجرا می‌کند. چنانچه این سیستم غیر قابل استفاده گردد سازمان مذبور قادر به انجام وظایف خود از آن طریق نخواهد بود.

ج- جلوگیری از دسترسی به سیستم. یکی از انواع حمله‌ی DoS آن است که سیستم کامپیوتری از کار انداخته شود. این نوع حمله باعث خواهد شد سیستم به همراه تمام نرم‌افزارهای

---

[1] Distributed Denial of Service
[2] Reflective