حملات MitM (مرد میانی)

با Session Theft (سرقت نشست)

تهدیدات، مکانیزم‌ها و دفاع‌ها

Session Hijacking

Session Fixation

Man-in-the-Middle Attacks

ط . شکری

استاد دکتر علی فریدی

موسسه آموزش عالی باختر ایلام

آذر ۱۴۰۴

چکیده

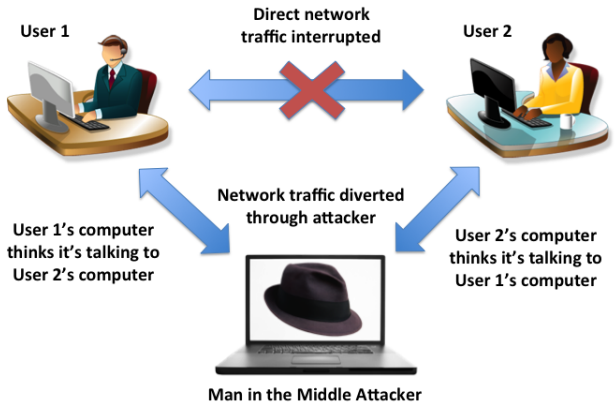
این مقاله حملات مرد میانی (MitM) با تمرکز بر سرقت نشست (Session Theft) را بررسی می‌کند که یک تهدید امنیتی جدی در برنامه‌های وب، شبکه‌های IoT و 5G است. حملات MitM به مهاجم امکان رهگیری، تغییر یا تزریق داده بین طرفین در حال ارتباط را می‌دهد. سرقت نشست، زیرمجموعه‌ای ازMitM ، شامل دزدیدن توکن‌های نشست معتبر برای جعل هویت کاربران است که منجر به دسترسی غیرمجاز و دستکاری داده می‌شود. ما وکتورهای حمله مانندXSS ، CSRF، استراق‌سمع بسته‌ها و تثبیت نشست را بررسی کرده و تأثیرات واقعی از جمله آسیب‌پذیری‌های Session Lingering (SLV) در برنامه‌های وب جاوا و ربودن دستگاه‌های IoT را تحلیل می‌کنیم. در نهایت، راهکارهای کاهش مانند رمزنگاری، مدیریت نشست امن، کوکی‌های HttpOnly و تشخیص مبتنی بر یادگیری ماشین در شبکه‌های ۵ Gرا بحث می‌کنیم. مقاله نتیجه می‌گیرد که دفاع چندلایه‌ای ترکیب‌کننده فناوری، سیاست و آگاهی کاربری برای مقابله با این تهدیدات در حال تحول ضروری است.

کلمات کلیدی:

حملات مرد میانی، MitM Attacks ، سرقت نشست، Session Theft ،

ربایش نشست، Session Hijacking ، امنیت وب، امنیت IoT، امنیت 5G

مقدمه



حمله مرد میانی (MitM) نوعی حمله on-path است که در آن مهاجم بین دو طرف مشروع در حال ارتباط قرار می‌گیرد و امکان رهگیری، تغییر یا تزریق داده به کانال ارتباطی را فراهم می‌کند[۱]. برخلاف مهاجمان off-path که فقط می‌توانند بسته‌ها را جعل کنند بدون اینکه ترافیک را مشاهده کنند، مهاجمان MitM قابلیت مشاهده و دستکاری کامل را دارند[۲]. یک نوع به خصوص شدیدMitM ، سرقت نشست (که Session Hijacking نیز نامیده می‌شود) است که در آن مهاجم توکن نشست فعال کاربر - مانند کوکی - را می‌دزدد تا قربانی را جعل هویت کند. در زمینهIoT ، « ربایش نشست یک حمله سایبری است که در آن مهاجم کنترل یک نشست معتبر بین یک دستگاه IoT و برنامه یا سرور متصل به آن را به دست می‌آورد، که به او اجازه می‌دهد داده‌ها یا اقدامات انجام‌شده توسط دستگاه IoT را دستکاری کند»[۳].

گسترش دستگاه‌های IoT و شبکه‌های 5G سطح حمله برای حملات MitM را افزایش داده است، در حالی که برنامه‌های وب سنتی همچنان از آسیب‌پذیری‌های مدیریت نشست رنج می‌برند. این مقاله یافته‌های مطالعات اخیر را ترکیب می‌کند تا توضیح دهد سرقت نشست چگونه کار می‌کند، تأثیر واقعی آن در حوزه‌های مختلف چگونه و راهکارهای مؤثر مقابله آن چیست.

مکانیزم‌های سرقت نشست

سرقت نشست می‌تواند از طریق وکتورهای متعدد رخ دهد که اغلب نقاط ضعف مدیریت نشست و ارتباط شبکه را اکسپلویت می‌کنند. مکانیزم‌های اصلی شامل موارد زیر هستند:

۱- حملات مبتنی بر وب

در برنامه‌های وب، توکن نشست (اغلب در کوکی ذخیره می‌شود) به عنوان رمز عبور برای درخواست‌های بعدی عمل می‌کند؛ دزدیدن این توکن اجازه جعل هویت کامل را بدون به خطر انداختن اتصال شبکه یا سرور می‌دهد[۴]. تکنیک‌های رایج شامل:

اسکریپت‌نویسی بین‌سایتی (XSS): مهاجمان اسکریپت‌های مخرب تزریق می‌کنند تا کوکی‌ها را بدزدند[۵].

جعل درخواست بین‌سایتی (CSRF): کاربران را فریب می‌دهد تا درخواست‌های احراز هویت شده ارسال کنند[۶].

تثبیت نشست: مهاجم قبل از ورود قربانی یک توکن نشست تنظیم می‌کند، سپس پس از احراز هویت از آن استفاده می‌کند[۵].

۲- حملات مبتنی بر شبکه

استراق‌سمع بسته‌ها روی ترافیک HTTP رمزنگاری‌نشده همچنان رایج است. یک بررسی در سال ۲۰۱۰ نشان داد که استراق‌سمع بسته‌های HTTP به دلیل عدم استفاده از HTTPS رایج‌ترین روش سرقت نشست بود[۵].

۳- آسیب‌پذیری‌های Session Lingering (SLV)

SLV ها زمانی رخ می‌دهند که نشست‌ها پس از عملیات حساس مانند تغییر رمز عبور باقی می‌مانند. همان‌طور که در تحقیق SLVHound ذکر شده است: «وقتی قربانی فعالیت‌های مشکوک را متوجه شده و رمز عبور خود را به عنوان یک اقدام احتیاطی تغییر می‌دهد، نشست ربوده شده باید بلافاصله منقضی شود؛ در غیر این صورت، مهاجم علیرغم تغییر رمز عبور به دسترسی غیرمجاز خود ادامه می‌دهد»[۶].

٤- حملات خاص IoT

در محیط‌های IoT، ابزارهایی مانند Bettercap ربایش نشست را تسهیل می‌کنند و به مهاجمان امکان کنترل از راه دور دستگاه‌ها را می‌دهند[۱]. ناهمگنی و محدودیت منابع دستگاه‌های IoT این خطرات را تشدید می‌کند.

تأثیرات واقعی و مطالعات موردی

۱- برنامه‌های وب

یک مطالعه در سال ۲۰۲۵ روی سیستم‌های جاوا ابزار SLVHound را معرفی کرد، یک ابزار تحلیل استاتیک که ۴۴ آسیب‌پذیری Session Lingering واقعی را در ۱۵ برنامه محبوب، از جمله ۳۰ مورد قبلاً گزارش‌نشده، کشف کرد[۶]. این نشان می‌دهد که نقص‌های انقضای نشست گسترده و اغلب نادیده گرفته شده‌اند.

۲- سیستم‌های IoT

ربایش نشست به نقض‌های دنیای واقعی مانند دوربین‌های Eufy و حادثه Verkada مرتبط شده است، جایی که مهاجمان به صورت غیرمجاز به فیلم‌ها و داده‌های حساس دسترسی پیدا کردند[۱].

۳- شبکه‌های 5G

حملات MitM لایه فیزیکی شبکه‌های 5G را تهدید می‌کنند، جایی که دفاع‌های رمزنگاری سنتی ممکن است کافی نباشند. با این حال، رویکردهای یادگیری ماشین با استفاده از ویژگی‌هایی مانند تأخیر جهتی فاصله-زمان به دقت تشخیص نزدیک به ۱۰۰درصد در سناریوهای نقطه داغ داخلی دست یافته‌اند[۷].

٤- شیوع تاریخی

داده‌های یک بررسی در سال ۲۰۱۰ از ۴۰ برنامه وب ایتالیایی نشان داد که فقط ۱۵درصد از HTTPS استفاده می‌کردند و استراق‌سمع بسته‌های HTTP رایج‌ترین وکتور حمله بود[۵].

۴ .راهکارهای پیشگیری و کاهش

وکتور حمله	راهکار کاهش	منابع کلیدی
استراق‌سمع بسته	رمزنگاریHTTPS/TLS	[۵] و [۸]
سرقت کوکیXSS	پرچم‌های HttpOnly, Secure, SameSite	[۴] و [۶]
تثبیت نشست	تولید مجدد شناسه‌های نشست پس از احراز هویت	[۵]
Session Lingering	انقضای فوری نشست پس از عملیات حساس	[۶]
حملات لایه فیزیکی	تشخیص مبتنی بر یادگیری ماشین	[۷]
حملاتOff-path	محافظت‌های رمزنگاری(TLS, DNSSEC, IPsec)	[۲]

دفاع مؤثر نیازمند یک رویکرد چندلایه است[۱]:

۱- رمزنگاری: تمام ترافیک باید از HTTPS/TLS استفاده کند[۸].

۲- مدیریت نشست امن: نشست‌ها باید بلافاصله پس از عملیات حساس باطل شوند[۶].

۳- امنیت کوکی: کوکی‌های HttpOnly سرقت از طریق XSS را جلوگیری می‌کنند[۴].

٤- ابزارهای توسعه‌دهنده: ابزارهای تحلیل استاتیک مانند SLVHound آسیب‌پذیری‌ها را در حین توسعه کشف می‌کنند[۶].

٥- تشخیص پیشرفته: یادگیری ماشین برای احراز هویت لایه فیزیکی 5G [۷].

٦- آگاهی کاربری: چرخش منظم رمز عبور و نظارت[۳].

نتیجه‌گیری و جهت‌گیری‌های آینده

سرقت نشست در حملات مرد میانی همچنان یک تهدید حیاتی و در حال تحول برای برنامه‌های وب، اکوسیستم‌های IoT و شبکه‌های نسل بعدی است. مهاجمان از تکنیک‌هایی ranging از XSS و استراق‌سمع بسته تا تثبیت نشست استفاده می‌کنند و انقضای ناکافی نشست و رمزنگاری ضعیف را اکسپلویت می‌کنند. گسترش دستگاه‌های IoT و شبکه‌های ۵ Gسطوح حمله جدیدی را معرفی می‌کند، در حالی که برنامه‌های وب قدیمی همچنان آسیب‌پذیری‌هایی مانندSLV ها را در خود جای داده‌اند.

دفاع مؤثر نیازمند یک استراتژی جامع است: اجرای رمزنگاری، پیاده‌سازی مدیریت چرخه حیات نشست امن، اتخاذ ویژگی‌های امنیتی کوکی و بهره‌گیری از روش‌های تشخیص پیشرفته مانند یادگیری ماشین در لایه‌های فیزیکی 5G. تحقیقات آینده باید چالش‌هایی مانند ناهمگنی دستگاه‌هایIoT ، عدم استانداردسازی و نیاز به پروتکل‌های امنیتی سبک‌وزن اما قوی را مورد توجه قرار دهد.

همان‌طور که در ادبیات اخیر تأکید شده است، امن‌سازی ارتباطات مدرن نیازمند «یک رویکرد چندلایه ترکیب‌کننده فناوری، سیاست و آموزش کاربری» است[۱]. با ادغام این اقدامات، سازمان‌ها می‌توانند بهتر در برابر مهاجمان off-path و on-path محافظت کنند.

مراجع

[1] H. Fereidouni, O. Fadeitcheva, M. Zalai

IoT and Man-in-the-Middle Attacks (2023)

[2] Y. Gilad, A. Herzberg, H. Shulman

Off-Path Hacking: The Illusion of Challenge-Response Authentication (2013)

[3] H. Fereidouni, O. Fadeitcheva, M. Zalai

IoT and Man-in-the-Middle Attacks (2025)

[4] S. Calzavara, M. Squarcina, R. Focardi, M. Tempesta

Surviving the Web: A Journey into Web Session Security (2018)

[5] C.A. Visaggio, L.C. Blasio

Session Management Vulnerabilities in Today's Web (2010)

[6] H. Meng, Y. Huang, Jie Lu, Lian Li

SLVHound: Static Detection of Session Lingering Vulnerabilities in Modern Java Web Applications (2025)

[7] A. Qasem, A. Tahat

Machine learning-based detection of the man-in-the-middle attack in the physical layer of 5G networks (2024)

[8] MD. IMTAZ HABIB, A. Al Maruf, MD. JOBAIR AHMAD NABIL

An Exploration into Web Session Security: A Systematic Literature Review (2018)

[9] C. De Alwis, P. Porambage, K. Dev, T.R. Gadekallu, M. Liyanage

A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions (2023)