دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۰، جلد ۱۹، شماره ۱ (۶۲-۷۱)
https://monadi.isc.org.ir

ارائه‌شده در شانزدهمین کنفرانس بین المللی انجمن رمز ایران در دانشگاه فردوسی مشهد، ۶ و ۷ شهریور ۱۳۹۸

ارزیابی مجموعه حملات نشأت گرفته شده از حمله مرد میانی در شبکه‌های کنترل صنعتی با نگاه ویژه به پروتکل DNP3★

محمد نوروززادگان*[۱]، فاطمه بابایی[۲] و سعدان زکایی[۱]

[۱]دانشکده برق و کامپیوتر، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران
[۲]دانشکده ریاضیات، دانشگاه صنعتی امیرکبیر، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
شبکه‌های کنترل صنعتی
حمله‌ی مرد میانی
DNP3
تأخیر

dor: 10.0000/000000000

نوع مقاله: پژوهشی

چکیده

شبکه‌های کنترل صنعتی همواره بخش اصلی زیرساخت یک کشور محسوب می‌شوند و هرگونه آسیب رساندن به آنها می‌تواند آثار فاجعه باری را به همراه داشته باشد. تأمین امنیت این نوع از شبکه‌ها که امروزه به چالشی برای کشورها تبدیل شده است، از زمانی اهمیت پیدا کرد که نیروگاه اتمی نطنز قربانی این نوع از حملات شد. پس از آن شاهد افزایش این نوع از حملات بودیم چنانکه در سال ۲۰۱۵ حمله‌ای دیگر به زیرساخت برق کشور ترکیه صورت گرفت. بنابراین ما در این مقاله سعی کرده‌ایم مجموعه حملاتی که در یک شبکه‌ی کنترل صنعتی بعد از حمله‌ی مرد میانی قابلیت اجرا دارند را پیاده‌سازی کرده و سپس بر اساس عامل زمان، حداقل تأخیری که این حملات می‌توانند بر اساس پروتکل DNP3 در یک شبکه‌ی کنترل صنعتی ایجاد کنند را به صورت تئوری بررسی کرده و نشان خواهیم داد که حملاتی که در شبکه‌های کامپیوتری مهم تلقی نمی‌شوند، در شبکه‌های کنترل صنعتی نقشی اساسی را ایفا می‌کنند.

۱ مقدمه

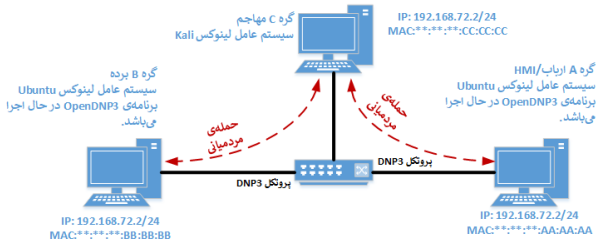
در گذشته شبکه‌های کنترل صنعتی همواره در محیط‌های ایزوله قرار داشته‌اند که به همین علت، نگرانی کمتری برای تأمین امنیت آنها وجود داشت، ولی امروزه شبکه‌های صنعتی از لحاظ گستردگی و تعداد، با سرعت غیر قابل باوری در حال رشد هستند به طوریکه اتوماتیک کردن کلیه فرآیندهای سیستم‌های صنعتی در رأس سیاست‌های کشورها قرار گرفته است. شبکه‌های صنعتی جزو زیرساخت‌های حیاتی یک کشور محسوب می‌شوند و هرگونه تأخیر و یا قطعی در ارائه‌ی خدمات، می‌تواند آثار جبران ناپذیری را به همراه داشته باشد. بر اساس گزارشاتی که در سال ۲۰۱۸ در سایت کسپرسکی منتشر شد از لحاظ تعداد حملات انجام شده به شبکه‌های زیرساخت کشورهای مختلف، کشور ایران رتبه‌ی هشتم را به خود اختصاص داده است.

استانداردهای امنیتی متعددی در سطح بین‌الملل مطرح است که هدفشان تامین امنیت برای شبکه‌های صنعتی است ولی امروزه با رعایت این استانداردهای امنیتی شاهد وقوع حملات سایبری به شبکه‌های صنعتی و آثار مخرب آنها هستیم، به طور مثال می‌توان به حملات سایبری انجام شده بر روی تجهیزات آزمایش موشکی کره شمالی در آوریل سال ۲۰۱۷ اشاره کرد که در نتیجه آن حملات آزمایش موشکی با شکست مواجه شد[۱].

★از کمیته علمی شانزدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.

*نویسنده مسئول
آدرس‌های رایانامه: norouzzadegan@email.kntu.ac.ir (محمد نوروززادگان)، fm.babaee@aut.ac.ir (فاطمه بابایی)، szokaie@eetd.kntu.ac.ir (سعدان زکایی)

[1] www.businessinsider.com/us-hack-north-korea-missile-system-2017-4



شکل ۱. معماری ارتباطی گره‌ها در محیط شبیه‌ساز

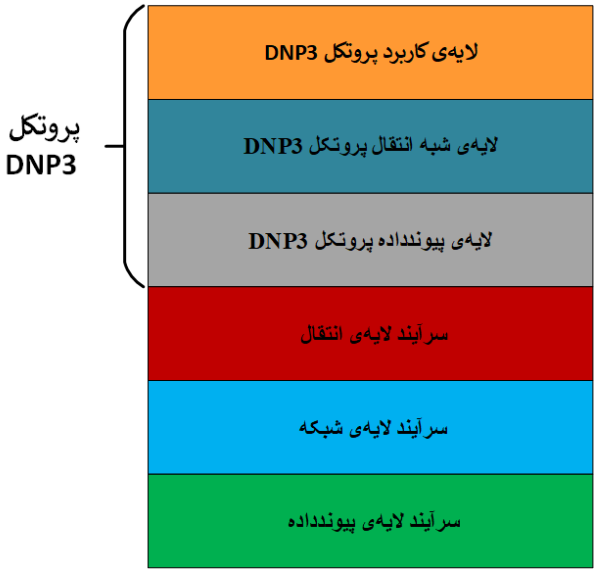
در این مقاله مجموعه حملات نشأت گرفته شده از حمله‌ی مرد میانی را در یک شبکه‌ی شبیه‌ساز صنعتی با توجه به پروتکل DNP3 [۱] پیاده‌سازی خواهیم کرد و سپس به بررسی و ارزیابی نتایج آنها از نظر حداقل تأخیر تزریقی به شبکه خواهیم پرداخت. برای این منظور در محیط شبیه‌ساز Virtual Box سه نود قرار دادیم که معماری ارتباطی آنها در شکل ۱ نشان‌داده شده است. در دو گره A و B برنامه شبیه‌ساز پروتکل DNP3، Opendnp3 را در سیستم عامل لینوکس Ubuntu اجرا کرده‌ایم که یکی نقش ارباب و دیگری نقش برده را ایفا می‌کنند و برای گره C که نقش مهاجم را دارد، از سیستم عامل لینوکس Kali استفاده می‌کنیم. به علت آنکه تمام سناریوهای انجام شده برروی پروتکل DNP3 اجرا می‌شود، در بخش دوم پروتکل DNP3 را به همراه سرآیندهای آن به طور کامل بررسی می‌کنیم. در بخش سوم حمله‌ی مرد میانی و حملاتی که از آن سرچشمه گرفته‌اند را معرفی می‌کنیم و در بخش آخر حملات پیاده‌سازی شده را از لحاظ عامل تأخیر تزریق شده به شبکه مورد بررسی و ارزیابی قرار خواهیم داد که بر اساس نتایج آن می‌توان IDS را پیشنهاد داد که جلوی اجرای این‌گونه از حملات گرفته شود.

۲ پروتکل DNP3

پروتکل DNP3 استاندارد IEEE-1815 است که یک پروتکل متن‌باز[1] سیستم‌های اتوماسیون صنعتی بوده که برای اولین بار در سال ۱۹۹۳ توسط شرکت GE-HARRIS ارائه شد [۲]. این پروتکل در حال حاضر یکی از مهمترین پروتکل‌های ارتباطی در شبکه‌ی توزیع هوشمند برق در ایالات متحده محسوب می‌شود. پروتکل DNP3 در واقع برای ارتباط بین دستگاه‌های ارتباط از راه دور[2] و جمع‌کننده‌ی اطلاعات ارائه شد و یکی از کاربردهای اصلی آن در سیستم‌های SCADA، برای ایجاد برقراری ارتباط بین مرکز کنترل و زیربخش‌های دیگر شبکه، مانند بخش مانیتورینگ می‌باشد [۳].

انتقال اطلاعات در پروتکل DNP3 مبتنی بر معماری ارباب و برده بوده و این پروتکل در برگیرنده‌ی چهار لایه، از مدل هفت لایه‌ای اصلی استاندارد OSI است. لایه‌های مختلف این پروتکل عبارتند از: لایه فیزیکی، لایه پیوند داده، لایه شبه‌انتقال و لایه کاربرد. این پروتکل در شبکه‌هایی با ساختار مختلف مانند بی‌سیم، طیف گسترده و ... قابلیت پیاده‌سازی دارد. این پروتکل بر بستر TCP/IP بر روی لایه انتقال بسته بندی شده و به طور

[1]open source [2]RTU



شکل ۲. پروتکل DNP3 بر بستر TCP/IP [۱]

متداول روی پورت ۲۰۰۰۰ فرستاده می‌شود. شکل ۲ نحوه‌ی بسته‌بندی یک بسته‌ی DNP3 را بر بستر TCP/IP نشان می‌دهد. در ادامه سرآیند[3] هرکدام از لایه‌های مختلف پروتکل DNP3 را به تفصیل معرفی خواهیم کرد.

۱.۲ بسته‌ی پروتکل DNP3

شکل ۳ یک بسته‌ی کامل پروتکل DNP3 را به همراه سرآیند لایه‌های مختلف نشان می‌دهد. همانطور که نشان داده شده است این بسته از تعدادی بلاک[4] مختلف تشکیل شده که بلاک صفر نشان دهنده‌ی سرآیند لایه‌ی پیوند داده است که ۴ بایت اول آن برای سنکرون کردن اطلاعات همواره برابر 0x0564 می‌باشد، یک بایت بعدی نشان دهنده‌ی طول بسته بر حسب بایت می‌باشد که در واقع طول اطلاعات رسیده از لایه شبه انتقال به همراه طول آدرس گیرنده و فرستنده و به همراه طول توابع کد را نشان می‌دهد که در نتیجه کمترین میزانی که نشان داده می‌شود برابر 0x05 می‌باشد. یک بایت بعدی نشان‌دهنده‌ی دستورات کنترلی مختلف پروتکل DNP3 است که هرکدام برای حالت خاصی از ارسال اطلاعات طراحی شده‌اند. هر کدام از دو بایت بعدی به ترتیب نشان‌دهنده‌ی آدرس‌های گیرنده و فرستنده پیام هستند که این یک ویژگی بارز پروتکل DNP3 است که می‌تواند بر روی یک لینک ارتباطی، بیش از ۶۵۰۰ دستگاه را آدرس‌دهی کند. اگر در بسته‌ای آدرس گیرنده برابر 0XFFFF باشد به معنای همه‌پخشی[5] آن پیام است. دو بایت انتهایی بلاک صفر، کد تصحیح‌خطا سرآیند لایه پیونداده را نشان می‌دهد. بایت اول بلاک، یک نشان‌دهنده‌ی سرآیند لایه شبه‌انتقال است که بیت اول و دوم آن به ترتیب مشخص‌کننده‌ی اول و یا آخر بودن بسته‌ی مورد نظر می‌باشد و شش بیت بعدی آن مشخص‌کننده‌ی شماره ترتیب بسته‌های این پروتکل می‌باشد. در واقع عملکرد پروتکل DNP3 به این صورت است که در ابتدا حجم

[3]header [4]block [5]broadcasting

وسیعی از اطلاعات از قسمت کاربری به لایه کاربرد می‌رسد و سپس این لایه اطلاعات را به اندازه‌هایی به طول حداکثر ۲۰۴۸ بایت می‌شکند، سپس با قراردادن سرآیند لایه کاربرد به صورت یک قالب آن را برای لایه شبه‌انتقال می‌فرستد. لایه شبه‌انتقال هم بسته‌های رسیده از لایه کاربرد را به حداکثر طول ۲۴۹ بایت شکانده و با چسباندن سرآیند لایه شبه‌انتقال آن را برای لایه پیونده‌داده می‌فرستد. در این لایه ابتدا اطلاعات رسیده از لایه بالاتر به قالب‌های ۱۶ بایتی تقسیم‌بندی می‌شوند و در انتهای هرکدام ۲ بایت کد تصحیح خطا قرار داده می‌شود، که هرکدام از این ۱۶ بایتی‌ها نشان‌دهنده‌ی بلاک یک تا n هستند. با چسباندن بلاک‌ها به یکدیگر و افزوده شدن سرآیند لایه‌ی پیونده‌داده به ابتدای آن، بسته ساخته شده و بعد از ارسال به لایه‌ی فیزیکی در شبکه مخابره می‌شود. در زیربخش بعدی امنیت در این پروتکل را بررسی خواهیم کرد.

۲.۲ امنیت در پروتکل DNP3

در سال ۲۰۰۹ پژوهشگران پروتکل DNP3 را مورد ارزیابی امنیتی قرار دادند و در نتیجه‌ی این ارزیابی، مجموعاً ۱۲۸ آسیب‌پذیری برای این پروتکل شناسایی شد که بسیاری از این آسیب‌پذیری‌ها در واقع تنها از لحاظ تئوری قابل بررسی بوده و در عمل قابلیت پیاده‌سازی نداشتند [۲]. ولی در سال ۲۰۱۵ بررسی دقیق‌تری بر روی حملاتی که به صورت عملی قابلیت پیاده‌سازی در پروتکل DNP3 را داشتند صورت گرفت [۴]. پروتکل DNP3 درواقع ناشی از رقابت شرکت‌های آمریکایی با همتایان اروپایی خود بود که نتیجه‌ی آن فقدان ملاحظات امنیتی در طراحی این پروتکل بود. البته طی چند سال گذشته طرح‌هایی برای افزایش امن‌سازی این پروتکل انجام شده که می‌توان به مدل امن تبادل اطلاعات پروتکل DNP3 [۵، ۶] اشاره کرد که در آن مدل، معماری SSL برای این پروتکل طراحی کرده‌اند و یا DNP3_SECURE [۷] برای افزایش امنیت در پروتکل DNP3 معرفی گردیده است ولی با این حال هنوز تحقیقات در این زمینه ادامه داشته و در حال حاضر نمی‌توانند به صورت بلادرنگ [۱] در شبکه‌های صنعتی که نیازمند کمترین تأخیر هستند، پیاده‌سازی شوند. این نکته مورد اهمیت است که بسیاری از تجهیزات IED دارای نام کاربری و رمز عبور پیش فرض کارخانه‌ای هستند و معمولاً هیچ‌وقت توسط اپراتور تغییر نمی‌کنند و مهاجم می‌تواند با نفوذ به آنها و استفاده از آسیب‌پذیری‌های موجود در پروتکل DNP3 برای شبکه‌ی مورد نظر تهدیدهای جدی ایجاد کند.

۳ حملات پیاده‌سازی شده

در طی چندین سال اخیر شاهد حملات متنوعی به شبکه‌های کنترل صنعتی هستیم که هر روز به پیچیدگی آنها افزوده می‌شود. این نوع از شبکه‌ها در بیش از یک دهه‌ی قبل در یک سیستم ایزوله قرار داشتند که نفوذ و ایجاد خرابکاری در آنها صرفاً به صورت فیزیکی امکان‌پذیر بود، ولی با وصل شدن این نوع از شبکه‌ها به یکدیگر و عبور ترافیک آنها از شبکه‌های LAN و حتی در مواردی اتصال آنها به شبکه‌ی پهناور اینترنت برای بالا بردن بهره‌وری و مدیریت آسان‌تر، باعث بروز آسیب‌پذیری‌های زیادی شده است. در حال حاضر سرویس‌هایی مانند شودان [۲] وجود دارد که شبکه‌های کنترل صنعتی را که به اینترنت متصل هستند را بر اساس پارامترهای مختلف شناسایی کرده و با برچسب ICS در وب‌سرویس‌شان قرار می‌دهند. در سال ۲۰۱۳ دو محقق امنیت سیستم‌های کنترل صنعتی توانستند بیش از هفت هزار تجهیزات کنترل صنعتی که به صورت آنلاین به اینترنت متصل بودند را بوسیله‌ی شودان، شناسایی کنند.

در مقاله‌ی [۸] برای پیشگیری از شناخت تجهیزات و نوع شبکه توسط شودان راه‌هایی ارائه شده‌است.

شکل ۱ نشان‌دهنده‌ی شبکه‌ی مورد آزمایش ما می‌باشد که در آن حمله‌ی مرد میانی رخ می‌دهد. گره A نشان‌دهنده‌ی ارباب بوده که با استفاده از پروتکل DNP3 دستورات کنترلی را به سمت گره B که نقش برده را دارد، ارسال می‌کند. گره C نشان‌دهنده مهاجمی است که یا توانسته به شبکه نفوذ کند و یا نود مشروعی بوده که توسط مهاجم به یک نود مخرب تبدیل شده است. به علت آنکه حملات بعد از حمله‌ی مرد میانی پیاده‌سازی می‌شوند در ادامه به ارائه توضیحی می‌پردازیم تا درک صحیحی از حمله‌ی مرد میانی داشته باشیم.

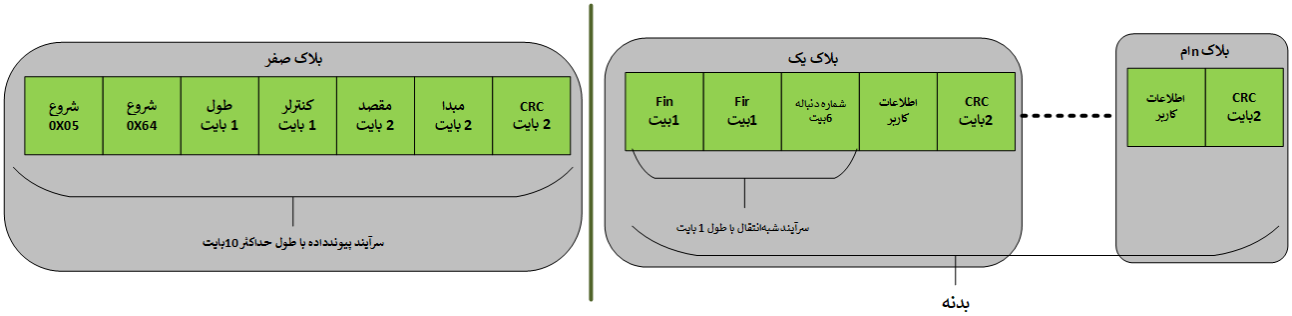
۱.۳ حمله‌ی مرد میانی در شبکه‌های کنترل صنعتی

حمله‌ی مرد میانی یکی از شناخته‌شده‌ترین حملات در شبکه‌های کامپیوتری است که قابلیت پیاده‌سازی در شبکه‌های صنعتی را هم دارد [۹]، برای مثال ویروس استاکسنت از اثرگذاری این نوع حمله بر روی سیستم‌های مانیتورینگ نیروگاه نطنز، سواستفاده کرد تا با کمک حمله‌ی بازپخش، اطلاعات غلط برای HMIها نمایش داده شود. بنابراین این حمله می‌تواند آغازگر دیگر حملاتی باشد که تنها در شبکه‌های کنترل صنعتی مهم تلقی می‌شوند. اسم حمله مرد میانی در واقع از سناریوی بازی بسکتبال گرفته شده است جایی که دو بازیکن در تلاش هستند توپی را به یکدیگر پاس دهند در حالی که فرد بین آنها مانع این کار می‌شود. بر اساس [۹] حمله‌ی مرد میانی در کل به چهار روش مختلف قابل پیاده‌سازی است. مبتنی بر جعل هویت (ARP, IP, DNS Poisoning)، مبتنی بر SSL/TLS، مبتنی بر مسیر یابی BGP و مبتنی بر ایستگاه پایه [۳].

موارد ذکر شده در قابلیت پیاده‌سازی در هر شبکه‌ی دلخواه را ندارند. ولی روش مبتنی بر جعل هویت پروتکل ARP که ما نیز هم در این مقاله برای پیاده‌سازی حملات در محیط شبیه‌ساز از آن استفاده کرده‌ایم، این قابلیت را دارد که در تقریباً تمام شبکه‌ها اجرا شود. ما در این مقاله در ابتدا فرض می‌کنیم که حمله‌ی مرد میانی در شبکه انجام شده است. برای پیاده‌سازی عملی این حمله در محیط شبیه‌ساز از ابزار Ettercap [۱۰] استفاده کرده‌ایم که در نتیجه آن مهاجم در وسط ارتباط بین ارباب و برده قرار می‌گیرد. حال در ادامه به ترتیب حملاتی که می‌توانند از این نوع

[1] realtime

[2] www.shodan.io [3] base station



شکل ۳. یک بسته‌ی کامل پروتکل DNP3 به همراه سرآیندهای آن [۱]

حمله نشأت بگیرند را معرفی و پیاده‌سازی خواهیم کرد.

۱.۱.۳ حمله‌ی شنود اطلاعات

مهاجم پس از اجرای حمله‌ی مرد میانی قادر است اطلاعاتی که بین ارباب و برده در حال تبادل می‌باشد را شنود کرده و با تجزیه و تحلیل این اطلاعات می‌تواند به نوع معماری شبکه صنعتی مورد نظر، نوع دستگاه‌های موجود، محصول شبکه‌ی صنعتی مورد نظر، نوع پروتکل‌های مورد استفاده در آن شبکه و ... پی ببرد، که از نظر مهاجم این اطلاعات بسیار مهم تلقی می‌شوند. برای پیاده‌سازی عملی این حمله ما در ابتدا برنامه‌ی شبیه‌ساز پروتکل DNP3، Opendnp3 را در دو گره برده و ارباب اجرا کردیم سپس مهاجم با اجرای اسکریپت زیر که مبتنی بر ماژول Scapy [۱۱] است، اقدام به شنود و ذخیره اطلاعات با فرمت Pcap می‌کند تا بعداً به بررسی آنها بپردازد.

```
Sniff_DNP3=sniff(filter = 'dst port 20000',
        prn = lambda x:x.summary(),
        count =10, timeout = 200)
wrpcap("/root/Desktop/sniffdnp3.pcap",
        Sniff_DNP3)
```

۲.۱.۳ حمله‌ی تکرار

این حمله همانطور که از نامش مشخص است مربوط به تکرار بسته و یا پیام‌های کنترلی است و در حالت کلی می‌تواند به دو صورت مختلف پیاده‌سازی شود. در حالت اول مهاجم مانند یک تکرارکننده عمل می‌کند به این معنی که وقتی بسته‌های عبوری بین ارباب و برده را شنود کرد، اقدام به ارسال دو و یا چندباره بسته‌های رد و بدل شده بین ارباب و برده می‌پردازد ولی در حالت دوم مهاجم بعد از شنود، بسته‌هایی را که شامل دستورات کنترلی خاصی هستند را انتخاب کرده و سپس بدون تغییر و یا دستکاری، آنها را در لحظه‌ای خاص به سمت هدف (ارباب یا برده) ارسال می‌کند. این نوع از حمله‌ی تکرار با نام حمله‌ی بازپخش [1] نیز شناخته می‌شود با این‌حال قابلیت پیاده‌سازی را در تمام پروتکل‌های صنعتی ندارد و علت آن هم می‌تواند در نظر گرفتن شماره ترتیب بسته‌ها در بعضی از پروتکل‌های صنعتی باشد، برای مثال در پروتکل DNP3 شماره‌ی ترتیب بسته‌ها را هم در لایه شبه‌انتقال مشاهده می‌کنیم و هم در لایه کاربرد. برای پیاده‌سازی عملی این حمله بعد از حمله‌ی مرد میانی هر بسته‌ای که از نود مهاجم عبور می‌کند توسط ماژول Scapy از آن کپی گرفته شده و دو عدد از آن‌ها به سمت مقصد به صورت بی‌درنگ ارسال می‌شود.

۳.۱.۳ حمله‌ی حفره‌ی سیاه

در این حمله مهاجمی که در میان ارتباط ارباب و برده قرار گرفته است، بسته‌ای را که دارای پیام کنترلی خاصی است را انتخاب کرده و آن را دور می‌اندازد و پاسخ پیام دور ریخته شده را بعد از سرهم کردن به سمت فرستنده ارسال می‌کند تا فرستنده متوجه دور ریخته شدن آن نشود. این حمله در یک شبکه‌ی صنعتی می‌تواند آثارجبران ناپذیری را به همراه داشته باشد، به این دلیل که یک پیام کنترلی در شبکه‌ی کنترل صنعتی تنها یک بار به سمت گیرنده ارسال می‌شود و در صورت عدم پاسخ گیرنده به پیام ارسالی در بازه‌ی زمانی مشخص، فرستنده مجدداً اقدام به ارسال بسته‌ی کنترلی مورد نظر می‌کند.

برای درک بهتر و ملموس‌تر این حمله و آثار مخرب آن، سناریوی زیر را در نظر بگیرید. در یک سناریو واقعی فرض کنید که در یک شبکه‌ی صنعتی در حوزه‌ی نفت و گاز درحالی که یک پیام کنترلی حاوی این مضمون که شیرتخلیه باید باز شود، از طرف ارباب به سمت برده فرستاده شود. اگر بسته‌ی مورد نظر توسط مهاجم دور ریخته شود و همزمان مهاجم پاسخ پیام دور ریخته شده را برای ارباب ارسال کند، ارباب متوجه نمی‌شود که برده آن را دریافت نکرده است. بنابراین احتمال انفجار به دلیل عدم باز شدن شیر تخلیه، افزایش می‌یابد.

برای پیاده‌سازی این حمله ما از ماژول Scapy زبان برنامه‌نویسی پایتون استفاده خواهد شد و در ابتدا نوع ترافیکی را که قرار است دور ریخته شود و همچنین پاسخ آن، توسط Scapy ساخته می‌شود. زمانی که بسته‌ی مورد نظر از IP-table نود مهاجم عبور می‌کند توسط nfqueue در سطح کرنل نود شناسایی شده و دور ریخته می‌شود و سپس پاسخ آن به سمت فرستنده (ارباب) ارسال می‌شود.

[1] replay

۴.۱.۳ حمله‌ی دستکاری

در این حمله مهاجم به صورت بلادرنگ وقتی بسته‌های رد و بدل شده بین ارباب و برده را شنود کرد، هم زمان بعضی از اطلاعاتی را که داخل بسته قرار دارد را به نفع خود تغییر داده و با محاسبه‌ی دوباره کد تصحیح خطا، اطلاعات جدید را بسته‌بندی کرده و آن را به سمت گیرنده مورد نظر ارسال می‌کند. این حمله یکی از مهمترین حملاتی است که بعد از اجرایی شدن حمله‌ی مرد میانی می‌تواند تأثیرات مخربی را بر شبکه‌ی کنترل صنعتی ما داشته باشد. سناریوی زیر را برای این حمله در نظر بگیرید. بر اساس این سناریو که در لایه‌ی پیونداده پروتکل DNP3 اتفاق خواهد افتاد، در ابتدا ارباب از برده درخواست اطلاعاتی می‌کند، سپس برده بسته‌ای را به ارباب خود ارسال می‌کند با مضمون اینکه لینک ارتباطی برده‌ی زیر دستش خواهان بازآوری[1] است. در همین زمان مهاجم بسته را انتخاب و سپس با دستکاری پرچم DFC در بخش کنترلر سرآیند لایه پیوند داده و قرار دادن مقدار یک در این پرچم به ارباب اینطور القا می‌کند که برده در حال حاظر مشغول است و ارباب باید درخواست‌های دیگرش را بعداً برای برده ارسال کند.

برای پیاده‌سازی عملی آن بعد از اجرای حمله مرد میانی یک کپی از بسته‌ی مورد نظر توسط Scapy گرفته می‌شود. به علت آنکه عملکرد Scapy به صورت منفعل[2] است احتیاج است که بسته توسط nfqueue با فرمتی خاص شناسایی شده و سپس دور ریخته شود. تغییرات مورد نظر در بسته‌ی کپی شده، توسط Scapy انجام می‌شود و سپس توسط تابع crcmod.predefined.mkCrcFun میزان کد تصحیح خطای آن را دوباره محاسبه کرده و به سمت گیرنده ارسال می‌شود.

۵.۱.۳ حمله‌ی ارسال اطلاعات تصادفی

مهاجم در این حمله پس از شنود بسته‌های عبوری بین ارباب و برده، به انتهای بسته‌هایی را که طول آنها کمتر از حداکثر طول یک بسته (برای مثال در پروتکل DNP3 حداکثر طول بسته ۲۹۲ بایت است) باشد، به صورت تصادفی اطلاعاتی را اضافه کرده و سپس بسته را به سمت گیرنده آن ارسال می‌کند. این نوع از حمله را می‌توان در زمره‌ی حملاتی به نام فازینگ نیز قرار داد که عموماً در تست‌های نرم‌افزاری و حتی سخت‌افزاری استفاده می‌شود. این نوع از حمله دو بخش مهم را تحت تأثیر قرار می‌دهد. بخش اول زمانی که بسته به گیرنده برسد به علت عدم درست بودن در کدهای تشخیص‌خطا، بسته دور ریخته می‌شود و درخواست مجدد برای دریافت بسته مورد نظر، ارسال خواهد شد. در بخش دوم بر اساس سازندگان مختلف این حمله می‌تواند آثار جداگانه‌ای داشته باشد که آن هم به خاطر سرریز بافری است که اتفاق می‌افتد. در بعضی موارد احتمال آن وجود دارد که بخشی از بسته خوانده شود و یا اطلاعات اضافه شده باعث تغییر یافتن ماهیت بسته‌ی کنترلی مورد نظر شود که با خواندن توسط گیرنده نتایج نامشخصی را به همراه داشته باشد.

همانطور که مشخص است برای پیاده‌سازی عملی این حمله، مراحل همانند حمله‌ی دستکاری اطلاعات است با این تفاوت که بسته‌های مورد نظر، بسته‌هایی هستند که طول آنها کمتر از ۲۹۲ بایت است و اطلاعات اضافی تصادفی توسط تابع os.urandom تولید و سپس توسط Scapy به بسته‌های مورد نظر تزریق شده و بسته‌ها ارسال می‌شوند.

۶.۱.۳ حمله‌ی تزریق بسته

در این حمله مهاجم بسته یا بسته‌های تولید شده‌اش را با توجه به شماره ترتیب بسته‌هایی که قبلا در شبکه عبور کرده‌اند، را به شبکه تزریق می‌کند که می‌تواند حاوی آسیب‌پذیری‌هایی برای شبکه مورد نظر باشد. مهاجم باید دقت کند که زمانیکه پاسخ بسته‌ی ارسال شده‌اش را از طرف گیرنده دریافت کرد آن را دور ریخته و سپس می‌تواند به حمله‌ی مرد میانی را پایان دهد. برای مثال سناریوی زیر را در نظر بگیرید.

مهاجم (گره C) با سرهم کردن یک بسته با کد تابع 0X0F در سرآیند لایه کاربرد و فرستادن آن به سمت برده مورد نظر به آن اعلام می‌دارد که باید اطلاعات ذخیره شده‌اش را به اندازه‌های اولیه خود تغییر دهد که باعث می‌شود که تنظیمات برده‌ی مورد نظر به مقادیر اولیه‌ی خود تبدیل شود و در نتیجه باعث از دسترس خارج شدن برده می‌شود. مهاجم باید پاسخی را که از طرف برده به طرف ارباب ارسال می‌شود را دور ریخته تا سیستم‌های تشخیص نفوذ متوجه اجرای چنین حمله‌ای نشوند.

برای پیاده‌سازی عملی این حمله، بسته‌ی مورد نظر توسط Scapy ساخته شده و در زمانی خاص، آن را به سمت برده ارسال می‌کنیم و برای دورانداختن پاسخ بسته‌ای که به شبکه تزریق شده است روند اجرا به مانند حمله‌ی حفره سیاه است تا بسته‌ی پاسخ دور انداخته شود.

۷.۱.۳ حمله‌ی قطعه قطعه کردن بسته

در یک شبکه‌ی صنعتی با توجه به نوع پروتکل و لینک ارتباطی استفاده شده، بسته‌ها با نرخ و اندازه‌های متفاوتی ارسال می‌شوند. برای مثال در پروتکل DNP3 حداکثر طول یک بسته‌ی آن برابر ۲۹۲ بایت می‌باشد که با توجه به شرایط محیطی مانند نویز و نوع کانال ارتباطی و ... طول بسته‌ها می‌توانند کمتر از ۲۹۲ بایت باشند. در این حمله مهاجم بر اساس الگوریتمی خاص اقدام به قطعه قطعه کردن بسته‌هایی می‌کند که بین ارباب و برده در حال عبور هستند. این حمله می‌تواند باعث افزایش ترافیک و توان پردازشی شبکه شده که قادر است تأخیر زیادی را به شبکه تحمیل کند و یا در مواردی باعث اشباع حافظه‌ی دستگاه‌هایی باشد که از آن پروتکل استفاده می‌کنند. سناریوی زیر را برای این حمله در نظر بگیرید.

بر اساس معماری شکل ۱ ارباب که نقش یک جمع‌کننده‌ی اطلاعات را ایفا می‌کند، به صورت دوره‌ای اطلاعاتی را از برده‌های زیر دستش به صورت نمونه‌برداری دریافت می‌کند. مهاجم بسته‌هایی که تنها به صورت یک بسته مستقل هستند را به این معنی که هم پرچم Fin و هم پرچم Fir

[1] reset [2] passive

آنها یک باشد را انتخاب کرده و سپس مبتنی بر معماری بسته هر کدام از بخش‌هایی را که دارای دو بایت کد تصحیح خطا هستند را به صورت یک بسته دنباله‌دار درآورده و سپس به سمت گیرنده‌ی مورد نظر ارسال می‌کند که این عمل می‌تواند ترافیک شبکه را در پروتکل DNP3 تا حدود ۶۰ درصد افزایش دهد. برای پیاده‌سازی عملی این حمله، بعد از اجرای حمله‌ی مرد میانی ابتدا بسته‌های مستقلی که طول آنها ۲۹۲ بایت است را شناسایی کرده و سپس توسط Scapy یک کپی از بسته‌ی مورد نظر گرفته می‌شود و بعد از آن بسته توسط nfqueue دور ریخته می‌شود. سپس با جدا کردن سرآیند لایه‌های پیونده‌داده و شبه‌انتقال و حفظ آنها، با توجه به نوع قطعه‌بندی بسته‌ها در حالت قبلی که هر ۱۶ بایت دارای دو بایت کد تصحیح خطا بوده‌اند را به یک بسته تبدیل می‌کنیم و با قراردادن سرآیندهای مورد نظر و محاسبه‌ی کد تصحیح خطا، بسته‌های قطعه قطعه شده را به سمت گیرنده ارسال می‌کنیم. در بخش بعدی نتایج این حملات را از نظر عامل تأخیر مورد ارزیابی قرار می‌دهیم.

۴ ارزیابی حملات بر اساس عامل تأخیر

در این بخش مجموعه حملاتی را که در بخش گذشته معرفی و پیاده‌سازی شده‌اند را از لحاظ حداقل تأخیری که می‌توانند به شبکه تزریق کنند، مورد ارزیابی قرار می‌دهیم. به همین دلیل ابتدا مسأله‌ی تأخیر را در شبکه‌های کنترل صنعتی بررسی خواهیم کرد و سپس نتایج هرکدام از حملات را بر اساس عامل تأخیر وارده به شبکه تجزیه و تحلیل می‌کنیم.

۱.۴ مساله‌ی تأخیر در پروتکل DNP3

مهمترین عامل در شبکه‌های کنترل صنعتی نسبت به شبکه‌های کامپیوتری دسترس‌پذیری شبکه است که میزان تأخیر بخش عمده‌ای از آن را در برمی‌گیرد. تأخیر بیش از حد به این معنی که یا بعضی از اطلاعات به سیستم گیرنده نمی‌رسد و یا در صورت رسیدن، آن اطلاعات دریافت شده دیگر قابلیت استفاده را نداشته باشند که می‌تواند نتایج مخربی به همراه داشته باشد. در شبکه‌های کنترل صنعتی نیز به مانند شبکه‌های کامپیوتری بین هر دو گره‌ای که می‌خواهند با هم ارتباط برقرار کنند سوکت زده می‌شود ولی در شبکه‌های کنترل صنعتی این عمل چون از قبل پیش‌بینی شده و عمل سوکت زدن انجام می‌شود می‌توان از تأخیر TCP 3-Way Handshake آن صرف‌نظر کرد. بر اساس مقاله [۱۲] حداقل تأخیر کلی در یک شبکه‌ی کنترل صنعتی، با توجه به استفاده از تجهیزاتی که از پروتکل DNP3 پشتیبانی می‌کنند، به صورت زیر بدست می‌آید:

$$\text{delay}_{\text{total}} = T_T + T_X + T_R \qquad (۱)$$

هر کدام از بخش‌های موجود در رابطه (۱) عبارتند از:

T_T: نشان‌دهنده‌ی تأخیر در فرستنده است که در واقع برابر مدت زمانی است که اطلاعات در لایه‌ی کابرد فرستنده آماده‌ی ارسال است تا زمانی که از پورت خروجی خارج می‌شود.

جدول ۱. میزان تأخیر برای بسته‌های پروتکل DNP3برحسب میلی‌ثانیه [۱۲]

دستگاه	ارسال بسته		دریافت بسته	
	$T_{\text{T\_DNP3}}$	$T_{\text{T\_TCP}}$	$T_{\text{R\_DNP3}}$	$T_{\text{R\_TCP}}$
رله	۱۱٫۸۵۶	۳٫۰۸۷	۱۰٫۸۲۸	۱٫۸۷۱
مرکز کنترل	۰٫۵۰۱	۰٫۳۵۷	۰٫۴۸۹	۰٫۲۷۱

T_X: نشان‌دهنده‌ی تأخیر در کانال ارتباطی است و در صورت یکسان بودن طول بسته‌ها و عدم وجود ترافیک و عوامل وابسته به آن، اندازه‌ی آن ثابت می‌ماند.

T_R: نشان‌دهنده‌ی آن است که وقتی اطلاعات توسط پورت گیرنده دریافت شد چقدر طول می‌کشد تا به لایه کاربرد گیرنده برسد.

البته T_R و T_T عموماً بستگی زیادی به نوع دستگاه‌هایی دارد که از آنها استفاده می‌شود و عموماً با هم تفاوت دارند و خود آن ها نیز از دو جز دیگر تشکیل می‌شوند که عبارتند از:

$$T_T = T_{\text{T\_DNP3}} + T_{\text{T\_TCP}} \qquad (۲)$$

$$T_R = T_{\text{R\_DNP3}} + T_{\text{R\_TCP}} \qquad (۳)$$

بر اساس مقاله [۱۲] میانگین تأخیر بر حسب میلی‌ثانیه در تجهیزات مختلف برای بسته‌بندی و ارسال بسته پروتکل DNP3 به شبکه و سپس دریافت آنها به صورت جدول ۱ می‌باشد.

همانطور که از جدول مشخص است DNP3 بیشتر از TCP تأخیر را به ازای هر بسته افزایش می‌دهد و علت آن است که پروتکل DNP3 در اصل برای ارتباط سریال طراحی شده بود و به مانند TCP دارای مکانیزم‌هایی برای تشخیص خطا می‌باشد که این مکانیزم‌ها با هم تداخل داشته و ۵۰ تا ۸۰ درصد تأخیرهای به وجود آمده به همین علت است. لازم به ذکر است که میزان تأخیر برای پروتکل‌های مختلف متفاوت است، ولی نتایجی که ما در این مقاله بدست آورده‌ایم مبتنی بر پروتکل DNP3 است. در ادامه حملات را بر اساس عامل تأخیر به صورت تئوری بر اساس مقاله‌ی [۱۲] بررسی خواهیم کرد.

۱.۱.۴ حمله شنود اطلاعات

حمله‌ی شنود متداول‌ترین حمله بعد از اجرای حمله‌ی مرد میانی است به دلیل آنکه اطلاعات از گره مخرب که عبور می‌کند، مهاجم می‌تواند هر زمان که خواست اطلاعات را شنود کند. در بخش قبل این حمله را شبیه‌سازی کردیم و مشاهده نمودیم که هدف این حمله آن است که اطلاعات مهمی را از شبکه بدست آورد. از نظر معماری امنیت، دسترسی به چنین اطلاعاتی، محرمانگی شبکه را نقض می‌کند. از لحاظ میزان تأخیر، این حمله تأخیری مشخص را به تنهایی به شبکه وارد نمی‌کند بلکه این تأخیر حمله‌ی مرد میانی است که به شبکه وارد می‌شود و دلیل اصلی آن هم خواندن و فرستادن بسته‌ها توسط گره مخرب است. بر اساس [۱۲] حداقل تأخیر کلی که این حمله به شبکه وارد می‌کند به صورت رابطه (۴) بدست می‌آید. تأخیر تولید شده توسط حمله‌ی شنود اطلاعات هیچ

وابستگی به نرخ شبکه ندارد. در معادله (۴) n برابر با تعداد بسته‌هایی است که از گره مخرب عبور می‌کنند.

$$\text{delay}_{\text{T\_sniff}} = n(T_{\text{R\_attacker}} + T_{\text{T\_attacker}}) \quad (۴)$$

۲.۱.۴ حمله‌ی تکرار

در حمله‌ی تکرار همانطور که قبلا گفته شد، گره مخرب همانند یک تکرارکننده در مسیر ترافیک عمل می‌کند. این حمله می‌تواند باعث افزایش تأخیر در شبکه‌ی ارتباطی و یا سرریز بافر در گیرنده شود. عامل تأخیر این حمله از دو مورد نشأت می‌گیرد که عبارتند از افزایش ترافیک ایجاد شده به علت تکرار تعداد بسته‌های ارسالی (مبتنی بر تعداد تکرار توسط مهاجم) و افزایش تعداد بسته‌های خوانده شده توسط گیرنده. بنابراین حداقل تأخیر ایجاد شده در شبکه به صورت زیر بدست می‌آید:

$$\begin{aligned}\text{delay}_{\text{T\_repeat}} &= n(T_{\text{R\_attacker}} + mT_{\text{T\_attacker}}) \\ &+ n(m-۱)\left(\frac{۱}{۲}T_{\text{x\_channel}} + T_{\text{R\_master}}\right)\end{aligned} \quad (۵)$$

در رابطه‌ی (۵) مقدار n برابر با تعداد کل بسته‌هایی است که از گره مخرب عبور می‌کنند و مقدار m برابر با تعداد کل تکراری است که توسط گره مخرب انجام می‌شود. اگر تعداد تکرارها زیاد باشد این حمله باعث از دسترس خارج شدن سرویس می‌شود به همین دلیل، این حمله از لحاظ معماری امنیت متناقض با دسترس پذیری شبکه است.

۳.۱.۴ حمله‌ی حفره‌ی سیاه

سناریو این حمله را بر اساس پروتکل DNP3 در زیر بخش قبلی پیاده‌سازی کرده‌ایم همانطور که گفته شد، بسته‌هایی از پروتکل DNP3 مورد هدف قرار می‌گیرند که حتما باید پرچم Fin و Fir آنها یک باشد، به این معنی که در امتداد سری دیگر از بسته‌ها نباشد تا در صورت دور ریخته شدن آنها، سیستم‌های تشخیص‌نفود نتوانند متوجه اجرای چنین حمله‌ای شوند. این حمله با توجه به تعداد بسته‌هایی که توسط گره مخرب دور ریخته می‌شود تأخیری که به شبکه تحمیل می‌کند از تأخیر حمله مرد میانی کمتر است ولی صفر نیست. رابطه‌ی زیر حداقل تأخیر تزریق شده توسط این حمله را نشان می‌دهد.

$$\begin{aligned}\text{delay}_{\text{T\_blackhole}} &= n(T_{\text{R\_attacker}} + (n-m)T_{\text{R\_attacker}}) \\ &- m\left(\frac{۱}{۲}\right)T_{\text{x\_channel}}\end{aligned} \quad (۶)$$

در رابطه‌ی (۶)، n برابر تعداد بسته‌های عبوری از گره مخرب و مقدار m برابر تعداد بسته‌های دور ریخته شده توسط مهاجم است. از لحاظ معماری امنیت، حمله حفره‌سیاه به علت دور ریختن بسته‌ها جامعیت اطلاعات را نقض خواهد کرد.

۴.۱.۴ حمله‌ی دستکاری

همانطور که در بخش قبل توضیح کاملی در مورد آن داده شد، حمله‌ی دستکاری قابلیت پیاده‌سازی را در لایه‌های مختلف یک پروتکل شبکه‌ی صنعتی را دارا می‌باشد، در بررسی این حمله از لحاظ عامل تأخیر، اگر از تأخیر ناشی از پردازش در گره مهاجم صرف‌نظر کنیم حداقل تأخیر ایجاد شده در شبکه مربوط به تأخیر حمله‌ی مرد میانی است به دلیل آنکه بسته‌های پروتکل DNP3 در گره مهاجم باید در ابتدا خوانده شده و سپس ارسال شوند. بنابراین این تأخیر بر اساس رابطه (۷) بدست می‌آید:

$$\text{delay}_{\text{T\_manipulate}} = n\left(T_{\text{R\_attacker}} + T_{\text{T\_attacker}}\right) \quad (۷)$$

در رابطه (۷) مقدار n برابر با تعداد بسته‌های عبوری از گره مخرب است. این حمله از لحاظ معماری امنیت، به علت دستکاری بسته‌ها جامعیت اطلاعات را نقض می‌کند.

۵.۱.۴ حمله‌ی اطلاعات اضافی تصادفی

حمله‌ی اطلاعات اضافی تصادفی در بخش گذشته معرفی و پیاده‌سازی شد. بعضی از شرکت‌های سازنده قبل از آن که محصولات خود را به بازار عرضه کنند این نوع از حمله را به عنوان آزمایش برای محصولاتشان امتحان می‌کنند تا با پیش‌بینی شرایط، از وقوع اتفاقاتی به مانند ایست سریع [۱] دستگاه جلوگیری کنند و البته این حمله می‌تواند برای محصولات از شرکت‌های مختلف نتایج متفاوتی را به همراه داشته باشد ولی عاملی که ما در این بخش آن را بررسی خواهیم کرد میزان تأخیری است که این حمله به شبکه وارد خواهد کرد تا با اندازه‌گیری این نوع از الگوهای تأخیری و استفاده‌ی آنها در الگوریتم‌های یادگیری ماشین از وقوع چنین حملاتی جلوگیری کنیم. حداقل تأخیری که به شبکه تحمیل می‌شود برابر است با:

$$\begin{aligned}\text{delay}_{\text{T\_random}} &= n\left(T_{\text{R\_attacker}} + T_{\text{T\_attacker}}\right) \\ &+ m'T_{\text{x\_channel}}\end{aligned} \quad (۸)$$

مقدار m' در واقع برابر با میزان اطلاعاتی است که توسط مهاجم به بسته‌های مورد نظر تزریق می‌شود. از نظر معماری امنیت این حمله می‌تواند باعث از دسترس خارج شدن شبکه شود و از طرفی دیگر به علت دستکاری بسته‌های پروتکل DNP3 جامعیت اطلاعات را نیز نقض می‌کند.

۶.۱.۴ حمله‌ی تزریق بسته

حمله‌ی تولید و تزریق بسته یکی از حملاتی است که گره مخرب در زمانی خاص آن را انجام می‌دهد و سپس می‌تواند به حمله‌ی مرد میانی پایان دهد. در این حمله مهاجم با ساخت انواع بسته و سرهم کردنشان، آن‌ها را در لحظه‌ای خاص به شبکه تزریق می‌کند که هرکدام از این تزریق‌ها می‌تواند بر اساس نوع بسته‌ی مورد نظر، آثار جداگانه‌ای را به همراه داشته باشد. البته میزان تأخیر ایجاد شده در شبکه نشأت گرفته شده از دو عامل

[1] crash

مهم است که عبارتند از تعداد بسته‌های تزریق شده به شبکه که در صف انتظار پاسخگویی قرار گرفته‌اند و میزان تأخیر مربوط به افزایش ترافیک اطلاعات تزریقی توسط هر بسته که به شبکه تحمیل می‌شود، بنابراین میزان تأخیر تولیدی برابر است با:

$$\begin{aligned}\text{delay}_{\text{T\_injection}} &= n\left(T_{\text{R\_attacker}} + T_{\text{T\_attacker}}\right) \\ &+ m\left(\left(\frac{۱}{۲}\right)T_{\text{x\_channel}} + T_{\text{R\_slave}}\right) \qquad (۹)\end{aligned}$$

در رابطه (۹) مقدار n برابر با تعداد بسته‌های عبوری از گره مخرب و مقدار m برابر با تعداد بسته‌های تزریق شده به شبکه است. هدف دیگر این حمله می‌تواند سریز در بافر برده مورد نظر باشد. در مقاله [۱۳] این نوع از حمله را با توجه به اینکه بسته‌های تزریقی از نوع پاسخ‌های نابهنگام است مورد بررسی و ارزیابی قرار داده است.

۷.۱.۴ حمله‌ی قطعه قطعه کردن بسته‌ها

حمله‌ی قطعه قطعه کردن بسته‌ها مبتنی بر معماری خاص، در شبکه‌های صنعتی نسبت به شبکه‌های کامپیوتری از اهمیت به سزایی برخوردار است، برای مثال این حمله بر اساس پروتکل DNP3 مبتنی بر الگوریتمی که در اینجا پیاده‌سازی کرده‌ایم، ترافیک شبکه را در حدود ۶۰ درصد افزایش می‌دهد. از طرف دیگر به علت افزایش تعداد بسته‌های رسیده به گیرنده، بر اساس جدول ۱ شاهد افزایش تأخیر هستیم. از طرفی دیگر به علت اینکه هر بسته می‌تواند نشان‌دهنده‌ی یک رویداد باشد، بنابراین زمانی که یک بسته به چندین بسته شکسته می‌شود یک رویداد [1] به چندین رویداد تبدیل می‌شود که نتیجه آن به سرریز شدن بافر [۱۳] در گیرنده می‌باشد. از لحاظ عامل تأخیر، کل تأخیری که این حمله به شبکه وارد می‌کند برابر است با:

$$\begin{aligned}\text{delay}_{\text{T\_splitting}} &= nT_{\text{R\_attacker}} + mT_{\text{T\_attacker}} \\ &+ (m-۱)\left(\frac{۱}{۲}\right)T_{\text{x\_channel}} \\ &+ (m-۱)T_{\text{R\_master}} \qquad (۱۰)\end{aligned}$$

در رابطه‌ی (۱۰) تعداد بسته‌هایی که در ابتدا به گره مخرب می‌رسند برابر n است و مقدار m برابر تعداد کل بسته‌هایی است که بعد از قطعه قطعه شدن از پورت گره مخرب خارج می‌شوند. اگر تمام بسته‌ها طول یکسانی داشته باشند و می‌توان مقدار m را به صورت $m'n$ نیز نوشت. این حمله به علت قطعه قطعه کردن بسته‌ها جامعیت اطلاعات را نقض می‌کند.

۵ نتیجه

در این مقاله ارزیابی‌ها بر اساس پروتکل DNP3 انجام شده و مجموعه حملاتی که در یک شبکه‌ی کنترل صنعتی بعد از حمله‌ی مرد میانی قابلیت اجرا دارند با توجه به عامل تأخیر مورد بحث و بررسی قرار گرفتند. برای این منظور ابتدا لایه‌های مختلف این پروتکل را بررسی کرده و به اهمیت مطالعات بیشتر در این گونه از پروتکل‌های صنعتی اشاره کردیم. در ادامه با معرفی و پیاده‌سازی مجموعه حملات قابل اجرا بعد از حمله‌ی مرد میانی (حمله‌ی شنوداطلاعات، حمله‌ی تکرار، حمله‌ی حفره‌ی سیاه، حمله‌ی دستکاری، حمله‌ی ارسال اطلاعات تصادفی، حمله‌ی تزریق بسته و حمله‌ی قطعه قطعه کردن)، بر اساس حداقل تأخیری که این حملات می‌توانند به شبکه تزریق کنند آنها را مورد ارزیابی قرار دادیم که می‌توان از نتایج آن در طراحی سیستم‌های تشخیص‌نفوذ استفاده کرد. در نتیجه‌ی ارزیابی‌ها نشان داده شد که در بین این حملات، حمله‌ی قطعه قطعه کردن به علت آنکه یک بسته را به چندین بسته تبدیل می‌کند، می‌تواند بیشترین تأخیر را به شبکه تحمیل کند. لازم به ذکر است که در شبکه‌های صنعتی عامل تأخیر نقش به‌سزایی را ایفا می‌کند و تأخیر هرچند کوچک می‌تواند برای شبکه آثار مخربی را به بار آورد.

[1] event

مراجع

[1] K Curtis. Dnp3 application note an2013-004b validation of incoming dnp3 data. www.dnp.org. DNP3 Users Group, Calgary, Canada.

[2] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. A taxonomy of attacks on the dnp3 protocol. In *International Conference on Critical Infrastructure Protection*, pages 67–81. Springer, 2009.

[3] Zhuo Lu, Xiang Lu, Wenye Wang, and Cliff Wang. Review and evaluation of security threats on the communication networks in the smart grid. In *2010-Milcom 2010 Military Communications Conference*, pages 1830–1835. IEEE, 2010.

[4] Zakarya Drias, Ahmed Serhrouchni, and Olivier Vogel. Taxonomy of attacks on industrial control protocols. In *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, pages 1–6. IEEE, 2015.

[5] Raphael Amoah, Seyit Camtepe, and Ernest Foo. Securing dnp3 broadcast communications in scada systems. *IEEE Transactions on Industrial Informatics*, 12(4):1474–1485, 2016.

[6] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. A taxonomy of attacks on the dnp3 protocol, in 'critical infrastructure protection iii', ICCIP 2009. IFIP Advances in Information and Communication Technol-

ogy.

[7] Jin Bai, Salim Hariri, and Youssif Al-Nashif. A network protection framework for dnp3 over tcp/ip protocol. In *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, pages 9–15. IEEE, 2014.

[8] Roland Bodenheim, Jonathan Butts, Stephen Dunlap, and Barry Mullins. Evaluation of the ability of the shodan search engine to identify internet-facing industrial control devices. *International Journal of Critical Infrastructure Protection*, 7(2):114–123, 2014.

[9] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, 18(3):2027–2051, 2016.

[10] www.ettercap.github.io/ettercap/.

[11] http://www.secdev.org/projects/scapy/.

[12] Xiang Lu, Zhuo Lu, Wenye Wang, and Jianfeng Ma. On network performance evaluation toward the smart grid: A case study of dnp3 over tcp/ip. In *2011 IEEE Global Telecommunications Conference-GLOBECOM 2011*, pages 1–6. IEEE, 2011.

[13] Dong Jin, David M Nicol, and Guanhua Yan. An event buffer flooding attack in dnp3 controlled scada systems. In *Proceedings of the 2011 Winter Simulation Conference (WSC)*, pages 2614–2626. IEEE, 2011.