امنیت سامانه‌های نهفته

«بررسی تهدیدات رایج بر علیه سامانه‌های حیاتی»

تاریخ تالیف: شنبه – ۲۱ فروردین ۱۴۰۰

تهیه شده توسط میلاد کهساری الهادی

مقدمه‌ای بر امنیت سامانه‌های نهفته[1]

سامانه‌های نهفته در بسیاری از فناوری‌های امروزی از جمله سامانه‌های هوافضایی و نظامی در حال استفاده هستند. از همین روی، سامانه‌های نهفته هدف جذابی برای هکرها به شمار می‌روند، چون به آن‌ها دسترسی کامل به داده‌های تولید شده، پردازش شده و حتی در حال انتقال ارائه می‌دهند.

محافظت از سامانه‌های نهفته به دلیل محدودیت‌هایی که این تجهیزات دارند، کاملا چالش بر انگیز است. برای ایجاد یک نرم‌افزار کاربردی و همچنین ایمن برای سامانه‌های نهفته، توسعه‌دهندگان به دانش عمیق و تجربه گسترده نسبت به برنامه‌نویسی ایمن و شناخت تهدیدات سامانه‌های نهفته نیاز دارند، تا با توجه به محدودیت‌های این سامانه‌ها بتوانند نرم‌افزارهای ایمن در مقابل تهدیدات سایبری پیاده‌سازی کنند.

در این مقاله، برخی از تهدیدات رایج بر علیه سامانه‌های نهفته برای مطالعات آتی را معرفی خواهیم کرد..

[1] Embedded Systems

کلیدواژه:

امنیت سامانه‌های صنعتی، امنیت سامانه‌های نهفته، امنیت سامانه‌های نظامی، مدارگردها، امنیت تجهیزات فضایی، امنیت سامانه‌های هوانوردی

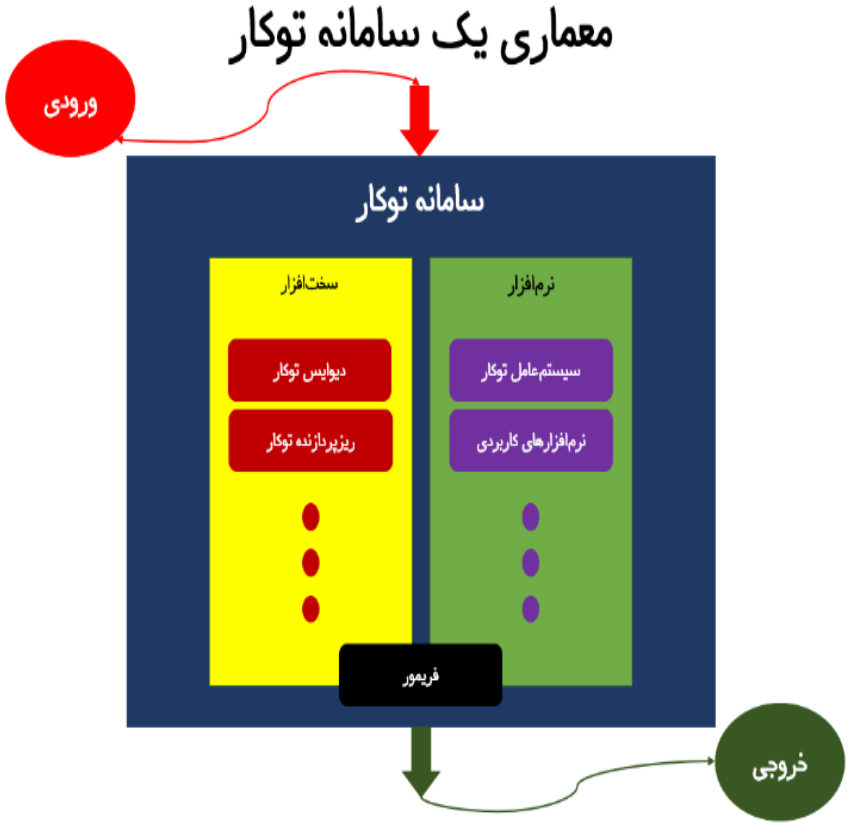
سامانه نهفته چیست؟

یک سامانه نهفته ترکیبی از تجهیزات است که تحت لقای یک مکانیزم بزرگ‌تر با هم کار می‌کنند. چنین سامانه‌هایی طراحی می‌شوند تا یک عمل مشخص را انجام بدهند. عموما، یک سامانه نهفته شامل یک پردازنده، حافظه، و یک دستگاه جانبی می‌شود.

در سامانه‌های مدرن، این مولفه‌ها در یک میکروکنترلر (هر سه مولفه بر روی یک تراشه واحد قرار دارند) یا یک ریزپردازنده (که از یک حافظه خارجی و یک دیوایس جانبی مجزا برای کاهش هزینه و مصرف برق استفاده می‌کند) تجمیع می‌شوند. در هر صورت، ترکیب و ظرفیت این نوع دستگاه‌ها بسته به هدف هر سامانه متفاوت است.

شایان ذکر است، یک سامانه نهفته توسط یک نرم‌افزار یکپارچه مدیریت و کنترل می‌شود که رفتار تجهیزات نهفته را مشخص می‌کنند. معمولا، توسعه‌دهندگان می‌توانند با نرم‌افزار نهفته از طریق یک رابط کاربری تعامل برقرار کنند اما

سامانه‌هایی که دارای محدودیت‌های شدید هستند، ممکن است این امکان را به توسعه‌دهندگان ندهند.



تصویر ۱: معماری سامانه‌های نهفته

مزئیت اصلی استفاده از سامانه‌های نهفته توانایی آن‌ها در کار به صورت بلادرنگ[1]، توانایی انجام کارها بدون یا حداقل تاخیر است. چنین عملکردی با بهینه‌سازی منابع سامانه و سخت‌افزار با محوریت انجام فقط یک کار مشخص صورت می‌گیرد. به دلیل چنین بهینه‌سازی، استفاده از یک سامانه نهفته ارزان‌تر و کم مصرف‌تر از ساخت یک دستگاه پیچیده است.

با پیاده‌سازی نرم‌افزارهای نهفته به صورت درست و صحیح، سامانه‌های نهفته می‌توانند قابل پیش‌بینی و همچنین در هر محیطی بدون هیچ مشکلی عمل کنند. ولی به هر صورت، نقطعه ضعف سامانه‌های نهفته از کوچک بودن و تک وظیفگی آن‌ها نشات می‌گیرد.

اول اینکه محدودیت مصرف توان و همچنین محدودیت حافظه همواره توسعه‌دهندگان را در یک وضعیت چالش بر انگیز قرار می‌دهد. آن‌ها نیازمند توانایی‌های مشخص و تجربه فراوان هستند تا بتوانند نرم‌افزارهایی ایجاد کنند که عملکرد سامانه‌های نهفته را پایدار و ایمن نگهدارند.

نکته بعدی این است که سامانه‌های نهفته به دلیل داشتن توان پردازش برای یک میزان مشخص از بار محاسباتی قابل مقیاس‌پذیری[2] نیستند. نکته نهایی این است که محدودیت توان، یک تاکید دیگر بر روی عملکرد است. این محدودیت خود می‌تواند موجب شکل‌گیری آسیب‌پذیری‌های جدی بر روی سامانه‌های نهفته شود چون نمی‌توان از راه‌حل‌های امنیتی پیچیده استفاده کرد.

[1] Realtime

[2] Scalability

نکات مثبت منفی سامانه‌های توکار

تصویر ۲: نکات مثبت منفی سامانه‌های نهفته

چالش‌های امنیتی سامانه‌های نهفته

یک آسیب‌پذیری در سامانه‌های نهفته این شانس را به یک هکر می‌دهد که به اطلاعات محرمانه دسترسی بگیرد، و همچنین از سامانه نهفته برای انجام حملات بعدی استفاده کند و حتی در برخی شرایط به دیوایس‌ها خصارت فیزیکی وارد کنند.

با در نظر گرفتن اینکه سامانه‌های نهفته اجزای تجهیزات بسیار گران و ارزشمند هستند، امکان هک این سامانه‌ها نظر بسیاری از هکرها را به خود جلب می‌کند.

به همین دلیل ایمن‌سازی سامانه‌های نهفته بسیار مهم است. با این حال پیاده‌سازی راه‌حل‌های امنیتی در سامانه‌های نهفته دارای چالش‌های متعدد است. از قبیل موارد زیر:

۱. محدودیت در توان و حافظه موجب می‌شود تعداد محدودی از برنامه‌های محافظتی و پیشگیری تهدیدات سایبری بر روی سامانه نهفته قابل نصب و راه‌اندازی باشند.
۲. ایجاد نرم‌افزارهای نهفته و طراحی سخت‌افزار با محوریت امنیت به تخصص توسعه بالایی نیاز است.
۳. اتصالات تحت شبکه و کنترل سطح دسترسی ضعیف در سامانه‌های نهفته یک مسئله رایج است.
۴. امکان استفاده از پروتکل‌های رمزنگاری در تمامی شرایط و سناریوهای عملیاتی وجود ندارد.

در ادامه به حملات بر علیه سامانه‌های نهفته خواهیم پرداخت.

پیامدهای اکسپلویت آسیب‌پذیری بر روی سامانه‌های نهفته؟

رایج‌ترین بحث اکسپلویت سامانه‌های نهفته هک لوازم الکترونیکی مصرفی از قبیل تجهیزات مبتنی بر GPS، مسیریاب‌های رادیویی و کنترلرهای پرواز و ... هستند. این حملات ممکن است، زیرا تولیدکنندگان تجهیزات سخت‌افزاری فریمور دستگاه‌های خود را در مقابل آسیب‌پذیری‌های گوناگون ایمن نمی‌کنند.

در سال ۲۰۱۸، هکرها دو آسیب‌پذیری با عنوان Meltdown و Spectre شناسایی کردند که تمامی پردازنده‌های AMD و Intel را تحت تاثیر قرار می‌دادند. هر دو آسیب‌پذیری باعث از بین رفتن فضای ایزوله بین برنامه‌های کاربر

می‌شدند و این امکان را فراهم می‌کردند که برنامه‌های کاربردی به داده‌های حساس دسترسی بگیرند و سطح حمله خود را گسترش بدهند. توسعه‌دهندگان ویندوز و لینوکس وصله‌های امنیتی برای رفع این آسیب‌پذیری‌ها ارائه کردند که به صورت جزیی جلوی انجام این حمله را می‌گرفتند. با این حال، بسیاری از تجهیزات مخصوصا قدیمی‌ها دارای این آسیب‌پذیری‌ها هستند [1].

همانطور که در بالا ذکر شد، ماشین‌ها در هر اندازه‌ای و پیچیدگی ممکن است به دلیل وجود سامانه‌های نهفته دارای آسیب‌پذیری باشند. به عنوان مثال، فریمور سامانه نگهداری / سامانه اطلاعات خدمه پرواز و سامانه شبکه آنبورد بوئینگ ۷۸۷ به سرریز بافر، تخریب حافظه، سرریز پشته و حملات منع سرویس آسیب پذیر بود [2]. یک هکر با انجام یک حمله موفق، می توانست اطلاعات خلبانان را به دست بیاورد و حتی شبکه هوانوردی را مورد نفوذ قرار بدهد.

همچنین سامانه های نظامی می توانند تحت تاثیر حملات بر علیه سامانه های نهفته قرار بگیرند. به عنوان مثال، هکرها در یک حمله توانستند ایستگاه دانلود اطلاعات هوایی قابل اعتماد متعلق به جنگنده F15 را خاموش کنند [3]. این دیوایس نهفته اطلاعات را از دوربین‌ها و سنسورها در طول پرواز جمع‌آوری می‌کرد و به خلبان اطلاعات راهبری را ارائه می‌داد.

تهدیدات سایبری بر علیه سامانه‌های نهفته

به هر صورت، امروزه سامانه‌های نهفته در بسیاری از زمینه‌ها و صنایع راه خود را باز کرده‌اند، از این میان می‌توان به خودروسازی، ابزار دقیق و موارد مرتبط با اندازه‌گیری، جنگنده‌ها، ماهواره‌ها، موشک و موارد متعدد دیگری اشاره کرد.

حال که اثر این سامانه‌ها بر جنبه‌های متعدد زندگی ما روز به روز در حال گسترش است، نگاهی دقیق به مسئله امنیت آنها ضروری است. در ادامه این مقاله به معرفی برخی از رایج‌ترین تهدیدهای سایبری و نقاط ضعف این سامانه‌ها پرداخته‌ایم. با توجه به این موضوع، به صورت خلاصه، رایج‌ترین حملات نرم‌افزاری، تحت شبکه و سخت‌افزاری بر علیه دستگاه‌های نهفته شامل موارد ذکر شده در تصویر ۳ می‌شوند.

تصویر ۳: حملات بر علیه سامانه‌های نهفته

در این مقاله دید کلی از این تهدیدات موجود برای سامانه‌های نهفته و آسیب‌پذیری آن‌ها به دست خواهیم آورد.

حملات مبتنی بر نرم‌افزار

حملات مبتنی بر نرم‌افزار مغز یک سامانه را هدف قرار می‌دهند، یعنی نرم‌افزاری و سامانه عامل که تجهیزات را کنترل می‌کند. یک حمله موفق بر علیه نرم‌افزاری که روی تجهیزات است، به هکرها اجازه خواهد داد به داده‌های حیاتی دسترسی بگیرند یا کنترل کامل تجهیزات را به دست آورند.

جستجوی آسیب‌پذیری‌ها در طراحی نرم‌افزار و کدها بردار حمله رایجی است، زیرا انجام حملات را برای هکرها به صورت راه دور و محلی فراهم می‌کنند. گسترده‌ترین حملات نرم‌افزاری بر علیه سامانه‌های نهفته شامل موارد زیر می‌شوند:

۱. بدافزارها
۲. حملات جستجوی فراگیر
۳. سرریز بافر و تخریب حافظه
۴. اسیب‌پذیری سرویس‌های نرم‌افزاری و سامانه عامل

به هر صورت، حملات بدافزاری بر علیه سامانه‌های نهفته بسیار رایج‌تر است. یک هکر می‌تواند با استقرار یک بدافزار در سامانه‌های نهفته کنترل آن‌ها را کامل به دست آورد. هکرها عموما برای انجام این کار از به‌روزرسانی تقلبی فریمور، درایورها، و حتی وصله‌های امنیتی استفاده می‌کنند تا بدافزار خود را در سامانه های هدف مستقر کنند.

حملات مبتنی بر شبکه

حملات مبتنی بر شبکه مبتنی بر آسیب‌پذیری‌هایی صورت می‌گیرند که در زیرساخت ارتباطات تحت شبکه وجود دارند. با استفاده از این آسیب‌پذیری‌ها هکرها می‌توانند ترافیک شبکه بین سامانه‌های نهفته را شنود، بررسی و حتی دستکاری کنند. برخی از این حملات در تصویر ۳ ذکر شدند.

به عنوان مثال، برخی از تجهیزات نهفته از سامانه‌عامل VxWorks استفاده می‌کند. VxWorks یک سامانه‌عامل بلادرنگ است که توسط Wind River Systems ایجاد و در نهایت توسط Intel خریداری شد. هم اکنون حدود ۳۰۰ میلیون دستگاه وجود دارد که از VxWorks به عنوان سامانه‌عامل خودشان استفاده می‌کنند.

ویژگی اصلی VxWorks که مهاجمین را محدود می‌سازد، برنامه کاربردی مُد کاربر است. بدین معنا که این سامانه‌عامل می‌تواند فرآیند بلادرنگ را از برنامه‌های کاربردی مُد کاربر مجزاسازی کند. همچنین هسته از طریقه مکانیزم محافظتی از حافظه هرگونه آزمایش نفوذی را محدود می‌کند. این سامانه عامل می‌تواند بر روی معماری x86، MIPS، PowerPC، ARM اجرا شود. معروفترین سامانه‌های زیرساختی که بر روی آنها VxWorks در حال اجرا است در لیست زیر آورده شده‌اند.

1. Airbus A400M Atlas military transport aircraft
2. C-130 Hercules aircraft
3. Boeing AH-64 Apache attack helicopter
4. Mars Reconnaissance Orbiter spacecraft
5. Curiosity Mars Rover

6. The ALR-67(V)3 Radar Warning Receiver used in the F/A-18E/F Super Hornet

این سامانه‌عامل با اینکه در محصولات حیاتی استفاده شده است، و بالاترین سطح امنیت را در بین سامانه‌های‌عامل دارد، اما در پژوهشی مشخص شد که هسته آن در تولید PRNG دارای آسیب‌پذیری است. در نتیجه، هکرها می‌توانستند ترافیک ارتباطی بین تجهیزاتی که از این سامانه‌عامل استفاده می‌کردند، شنود و دستکاری کنند [4].

حملات کانال جانبی

در انجام حملات کانال جانبی از آسیب‌پذیری‌های سخت‌افزاری در سامانه‌های نهفته استفاده می‌شود. انجام این حملات هزینه بر و بسیار دشوار است، زیرا به دانش عمیق سخت افزاری و همچنین دسترسی فیزیکی به دستگاه نیاز است. به منظور انجام حملات کانال جانبی شخص هکر نیازمند اطلاعات از توان مصرفی، نشت الکترومغناطیسی، زمان عملیات و ... است. در تصویر ۳، برخی از حملات مهم کانال جانبی بر علیه سامانه های نهفته لیست شده است.

نتیجه‌گیری

در انجام حملات سایبری بر علیه سامانه‌های نهفته رویکردها و تکنیک‌های گوناگونی وجود دارد که در این مقاله ۱۲ حمله در سه خانواده از تهدیدات معرفی شدند. هر کدام از این تهدیدات ممکن است در سطوح گوناگون سامانه‌های نهفته رخ بدهند، و عملیاتی که قرار است انجام بدهند را دچار شکست کنند. در این مقاله، صرفا به معرفی پرداخت شد. در سری مقالات بعدی، به جزئیات این تهدیدات پرداخته خواهد شد.

مراجع

[1] "Computer security: Spectre and Meltdown, just the beginning?," [Online]. Available: https://home.cern/news/news/computing/computer-security-spectre-and-meltdown-just-beginning.

[2] DarkReading, "Boeing 787 On-Board Network Vulnerable to Remote Hacking," [Online]. Available: https://www.darkreading.com/vulnerabilities---threats/boeing-787-on-board-network-vulnerable-to-remote-hacking-researcher-says/d/d-id/1335463.

[3] newsweek, "Ethical Hackers Sabotage F-15 Fighter Jet, Expose Serious Vulnerabilities," [Online]. Available: https://www.newsweek.com/cybersecurity-vulnerability-fighter-jet-f15-defcon-hacking-tads-flight-system-hack-pentagon-1454491.

[4] 33C3, "Analyzing Embedded Operating System Random Number Generators," [Online]. Available: https://samvartaka.github.io/cryptanalysis/2017/01/03/33c3-embedded-rngs.