Journal of Crisis Management and Emergency Situations

3

Vol. 15
Autumn 2023
P.P:37-60

Research Paper

Received:
25 August 2023
Accepted:
06 November 2023

Investigating cyberspace security and safety engineering in rail transport network systems and subsystems (case study: Italian regional railways)

Mehran Khalaj [1] | Daud Jafari [2] | Pejman Salehi [3]

Abstract

Studying the history of cyber attacks on computer networks and rail transportation systems shows the vulnerability of these systems and related subsystems against the possible threats of intruders and attackers. In recent years, various implementation methods and guidelines have been designed and documented to improve the security level of railway systems against the risks in cyberspace. The large number and wide variety in the scope of these documents shows the importance and necessity of safety and security against the current increasing and complex attacks in the cyber fields. In this regard, the market of new technologies and innovative industrial services in this field shows a considerable growth. However, the risks of information exchange space in the computer networks of the rail transport industry are still considered one of the most important challenges in this field. Therefore, in this study, in addition to presenting a conceptual model, an attempt has been made to identify environmental threats and gain awareness about the vulnerability of rail transportation systems against cyber attacks, using a case example that includes the violation of the safety structures of critical facilities in the rail transportation industry. to be In this study, it has tried to investigate the existing vulnerabilities in the railway industry through the RAMS risk analysis model. Therefore, for the case study of the current research, an attack tree was used, which can provide the possibility of analyzing security and safety risks using systemic approaches in the rail network in an integrated manner. Some findings of the current research show that security risks in the rail network have the same importance as safety risks, and therefore, coherent integration between cyber security and rail transportation safety can increase the effectiveness of security measures in the rail network.

Keywords: Cyber security, safety engineering, rail transportation, resilience, penetration, RAMS analysis.

1. Corresponding Author: Associate Professor, Faculty of Industrial Engineering, Islamic Azad University, Parand Branch, Iran. pejmansalehi.metro@gmail.com
2. Department of Educational Industrial Engineering, Faculty of Industrial Engineering, Azad University, Parand branch.
3. Faculty of Industrial Engineering, Islamic Azad University, Parand branch.

نشریه علمی مدیریت بحران و وضعیت‌های اضطراری

۳

سال پانزدهم
پاییز ۱۴۰۲
صص: ۶۰-۳۷

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۲/۰۳/۰۸
تاریخ پذیرش:
۱۴۰۲/۰۶/۱۸

بررسی امنیت فضای سایبری و مهندسی ایمنی در سیستم ها و زیرسیستم های شبکه حمل و نقل ریلی (مطالعه موردی: راه آهن منطقه ای ایتالیا)

مهران خلج [۱] | داود جعفری [۲] | پژمان صالحی [۳]

چکیده

مطالعه پیشینه حملات سایبری به شبکه‌های رایانه‌ای و سامانه‌های حمل‌ونقل ریلی، آسیب‌پذیری این سیستم‌ها و زیرسیستم های مرتبط را در مقابل تهدیدهای احتمالی نفوذگران و مهاجمان نشان می‌دهد. طی سال‌های اخیر روش‌های اجرایی و دستورالعمل‌های متنوعی برای ارتقای سطح امنیت سامانه‌های ریلی در برابر ریسک‌های موجود در فضای مجازی طراحی و مستندسازی شده است. تعدد فراوان و تنوع وسیع در دامنه شمول این اسناد، اهمیت و ضرورت ایمنی و امنیت را در برابر حملات فزاینده و پیچیده‌ی کنونیِ حوزه های سایبری نشان می‌دهد. در این راستا بازار فن‌آوری‌های جدید و خدمات نوآورانه‌ی صنعتی در این حوزه، رشد قابل‌ملاحظه‌ای را نشان می‌دهد. بااین‌حال مخاطرات فضای تبادل اطلاعات در شبکه‌های رایانه‌ای صنعت حمل‌ونقل ریلی همچنان یکی از مهم‌ترین چالش‌های این حوزه محسوب می‌شود. لذا در این مطالعه ضمن ارائه یک مدل مفهومی کوشیده شده است به‌منظور شناسایی تهدیدهای محیطی و کسب آگاهی در خصوص نقاط آسیب‌پذیری سیستم‌های حمل‌ونقل ریلی در برابر حملات سایبری از یک نمونه موردی که شامل نقض ساختارهای ایمنی تسهیلات حیاتی در صنعت حمل و نقل ریلی است، استفاده شود. در این مطالعه کوشیده است آسیب‌پذیری های موجود در صنعت ریلی از طریق مدل تحلیل ریسک RAMS[۴] بررسی نماید. ازاین‌رو برای مطالعه موردی تحقیق حاضر از یک درخت حمله استفاده‌شده که می‌تواند امکان تحلیل ریسک‌های امنیتی و ایمنی را با استفاده از رهیافت های سیستمی در شبکه ریلی به‌صورت یکپارچه فراهم نماید. برخی یافته‌های تحقیق حاضر نشان می‌دهد که مخاطرات امنیتی در شبکه ریلی دارای اهمیتی برابر با ریسک‌های ایمنی است و لذا یکپارچگی منسجم میان امنیت سایبری و ایمنی حمل‌ونقل ریلی می‌تواند اثرگذاری اقدامات تأمینی را در شبکه ریلی افزایش می‌دهد.

کلیدواژه‌ها: امنیت سایبری، مهندسی ایمنی، حمل‌ونقل ریلی، تاب‌آوری، نفوذ گری، تحلیل RAMS.

۱. نویسنده مسئول: دانشیار دانشکده مهندسی صنایع، دانشگاه آزاد اسلامی واحد پرند، ایران.
pejmansalehi.metro@gmail.com

۲. دانشیار دانشکده مهندسی صنایع، دانشگاه آزاد اسلامی واحد پرند، ایران.

۳. دکتری مهندسی صنایع، دانشگاه آزاد اسلامی واحد پرند، ایران.

۴. قابلیت اطمینان (Reliability)؛ قابلیت دسترسی (Availability)؛ قابلیت تعمیر و تعویض (Maintainability)؛ ایمنی (Safety)

مقدمه و بیان مسئله

در ادبیات صنعت حمل‌ونقل ریلی، سامانه‌های نرم‌افزاری و سخت‌افزاری بهره‌برداری و عملیاتی از نظر ساختاری و کارکردی دارای وجوه تمایز متعددی هستند (اَمبروس[1] و همکاران، ۲۰۱۸). سامانه‌های بهره‌برداری اصطلاحاً به بخش‌هایی اطلاق می‌گردد که مستقیماً با مسافران در ارتباط بوده و خدمات جابجای شهری و بین‌شهری را به ایشان عرضه می‌کنند. از سوی دیگر سامانه‌های عملیاتی به‌طور مستقیم، عملکرد ایمن تسهیلات و تجهیزات ثابت و متحرک در شبکه ریلی را تضمین می‌نمایند. به‌این‌ترتیب ازآنجایی‌که سامانه‌های فن‌آوری اطلاعات و ارتباطات برای ارسال و دریافت داده‌ها در سیستم‌ها و زیرسیستم‌های کنترلی ناوگان قطارها و تجهیزات کنار خط مورداستفاده قرار می‌گیرند لذا امنیت فضای تبادل اطلاعات در محیط تعاملی ماشین و کاربران مراکز ناوبری عملیات و کنترل کننده های سایبرنتیک با عنوان «مهندسی حفاظت اطلاعات و نرم‌افزارهای ریلی» در نظر گرفته می‌شود (زلوسکی[2] و همکاران، ۲۰۱۹). از سوی دیگر فرآیند امنیت سایبری به‌عنوان «مهندسی حفاظت از عملکرد ایمن سامانه‌های کنترلی قطار» در نظر گرفته می‌شود که می‌تواند امنیت سایبری شبکه ریلی را از طریق دسترس‌پذیری، یکپارچگی و محرمانگی برآورده نماید (باریل[3] و همکاران، ۲۰۱۶). استقرار الگوی عمومی RAMS در شبکه‌های ریلی، چارچوب تحصیل قابلیت اطمینان تجهیزات و سامانه‌ها، نگهداری و تعمیر پذیری تسهیلات و ایمنی زیرسیستم‌های کنترل قطار را تضمین می‌نماید (یامپولسکی[4]، ۲۰۱۷). امنیت سایبری در صنعت حمل‌ونقل ریلی یک مسئله پیچیده و چندوجهی است که لازم است آلترناتیوهای مرتبط با آن توأم با رویکردهای ایمنی ارائه گردد. استانداردهای امنیت سایبری که توسط اتحادیه بین‌المللی راه‌آهن‌ها[5] و اتحادیه اروپا ارائه‌شده است یکپارچگی کارکردهای ایمنی و امنیت سایبری را ترویج می‌نماید (بارنا[6]، ۲۰۲۲). درهم تنیدگی ایمنی و امنیت در صنعت حمل و نقل ریلی، همانندی ضرورت و اهمیت این دو مؤلفه را در کنترل سیر و حرکت قطارها نشان

1 - Ambrose
2- Zalewski
3- Bar-El
4- Yampolskiy
5 - UIC
6- Barna

می‌دهد (تالبی[1]، ۲۰۱۷). دراین‌بین حفاظت فیزیکی به‌عنوان یکی از مؤلفه‌های تأثیرگذار بر امنیت سایبری، می‌تواند نخستین مرحله از یک نفوذ مخرب باشد لذا علاوه بر بُعد ایمنی لازم است حفاظت فیزیکی نیز به‌صورت یکپارچه با ایمنی و امنیت لحاظ گردد (فِرگ[2] و همکاران، ۲۰۱۸). به‌عنوان یک مورد عملی، پروژه ریل سایبری[3] در اتحادیه اروپا به ارائه راهکردهایی برای ارتقای امنیت سایبری در سیستم‌های سیگنالینگ شبکه ریلی با استفاده از شناسایی و ارزیابی ریسک‌های سایبری می‌پردازد و لزوم پیاده‌سازی مدل RAMS را توصیه می‌نماید. در این الگو با استفاده از سیستم‌های تشخیص نفوذ (IDS)، سامانه‌های مبتنی بر فن‌آوری اطلاعات و سایر زیرسیستم‌های عملیاتی نظیر پکیج‌های علائم و ارتباطات به‌صورت انعطاف‌پذیر پیاده‌سازی شده‌اند (شاکلا[4]، ۲۰۱۹). در این راستا توسعه فن‌آوری‌های مرتبط با امنیت سایبری در صنعت حمل‌ونقل ریلی نظیر استقرار سیستم‌های پیشرفته تشخیص نفوذ در سوئیچ‌ها و فایروال‌های شبکه ریلی برای حفاظت از سامانه‌های عملیاتی حمل‌ونقل ریلی به‌ویژه بخش‌های ناوبری، کنترل و سیگنالینگ از آن جمله است. بااین‌حال بهره‌بردارهای حمل‌ونقل ریلی در به‌کارگیری این سیستم‌ها با چالش مواجه هستند (لاکشمینارایانا[5]، ۲۰۱۹). برنامه‌های امنیتی کاربردی در صنعت حمل و نقل ریلی به سیستم‌های تعبیه‌شده‌ای اطلاق می‌شود که دارای ساختار محاسباتی بوده و با سازوکارهای ساخت‌یافته برای یک محیط پیچیده و کارکردی طراحی‌شده‌اند و می‌توانند رفتارهای عناصر فعال در شبکه ریلی را از طریق سامانه‌های ریلی پیش‌بینی و کنترل نمایند. سیستم‌های عملیاتی در صنعت حمل و نقل ریلی، به تعبیری زیرسیستم‌های الکترونیکی توسعه‌یافته‌ای هستند که در سامانه‌های کنترلی استقراریافته و ارزیابی امنیتی سامانه‌ها را راهبری و سازمان‌دهی می‌کنند (کارای[6]، ۲۰۲۱). اختلاف میان سیستم‌های امنیتی در محیط فن‌آوری اطلاعات به تفاوت کاربری‌های عملیاتی این سامانه‌ها بازمی‌گردد لذا در وهله نخست لازم است مسائل مرتبط با امنیت فیزیکی در بخش سخت‌افزاری سامانه‌ها شناسایی گردد و سپس در صورت شناسایی نفوذ؛ ردگیری حمله و آثار مهاجمان انجام گیرد. علاوه بر این در چرخه حیات این قبیل برنامه‌ها، ارزیابی و به‌روزرسانی ساختارها می‌تواند به

1- Talebi
2- Ferrag
3 - CyberRil
4- Shukla
5- Lakshminarayana
6- Karray

شناسایی نقاط ضعف و آسیب‌پذیری‌های شبکه بر اساس اطلاعات به‌روز منتج شود (کومار و استولینگا[1]، ۲۰۲۰). وجود حفرهای امنیتی و آسیب‌پذیری های سیستم‌های اطلاعات مدیریتی در شبکه ریلی، زمینه‌ساز بروز نفوذ در سیستم‌های داخلی می‌گردد. این در حالی است که نقاط ضعف سامانه‌های مرتبط با خدمات مسافری می‌تواند موجبات بروز اختلال در روند بهره‌برداری از شبکه ریلی و ایجاد خسارت‌های گسترده برای ذی‌نفعان گردد. سیستم‌های طراحی‌شده در یک زیرساخت (پلتفرم) یکپارچه که با سایر شبکه‌های محلی در ارتباط است، اصطلاحاً یک ساختار شبه مجازی از عناصر سخت‌افزاری فیزیکی را به وجود می‌آورند که در صنایع تولیدی نظیر نفت و گاز مورداستفاده قرار می‌گیرد بنابراین نکته قابل‌توجه وجود مخاطرات و تهدیدهای سایبری برای این سیستم‌هاست، که گاه تبعات جبران‌ناپذیری را در پی دارد(شکری[2] و همکاران، ۲۰۱۹). برخی از این خطاها دارای پیامدهای ایمنی است که درنتیجه سبب خرابی تجهیزات متحرک و سیستم‌های کنترل صنعتی می‌گردد در این میان یک رویکرد «سخت‌افزاری (فیزیکی) –سایبری» با شتابی مضاعف توسعه‌یافته و عوامل دیگر صنعت حمل‌ونقل ریلی را متأثر می‌سازد.

۲- پیشینه تحقیق

در یک مطالعه، پکیک[3] (۲۰۲۱) با مرور تهدیدها و آسیب‌های مترتب بر سامانه‌های سخت‌افزاری و نرم‌افزاری در صنعت حمل‌ونقل ریلی، به طبقه‌بندی انواع حملات سایبری در شبکه ریلی پرداخته و یک چشم‌انداز کلی از تهدیدهای تأثیرگذار بر سامانه‌های کنترل خودکار تعبیه‌شده قطار و تجهیزات کنار خط آهن ارائه داد. نتیجه این تحقیق از طریق تجزیه‌وتحلیل ریسک‌های امنیتی به ارائه یک مدل برای استقرار و توسعه سیستم‌های امن و ایمن برای مقابله با نفوذگری منتهی شده است.

در مطالعه دیگری که توسط اُکا[4] (۲۰۱۷) انجام‌شده است، محقق ضمن طبقه‌بندی انواع حملات فیزیکال و سایبری به پیشنهاد توصیه‌هایی برای تقویت کمی و کیفی زیرساخت‌ها به‌منظور ارتقای تاب‌آوری در برابر حملات سایبری پرداخته است. در مطالعه مزبور محقق ضمن تبیین

1- Kumar &Stoelinga
2- Shoukry
3- Rekik
4- Oka

سناریوهای مختلف حملات سایبری در شبکه ریلی؛ شیوه‌های شناسایی آسیب‌های نرم‌افزاری و سخت‌افزاری در ناوگان قطارها را بیان نموده است. تمرکز اصلی تحقیق مزبور مطالعه رفتارهای غیرخطی واحدهای برنامه پذیر الکترونیکی در سیستم‌های مدیریت و کنترل ترافیک قطارها و سایر زیرسیستم‌های مشابه است.

در مطالعه‌ای که توسط پاپ و بوتیان[1] (۲۰۱۸) انجام‌شده است، محققان به بررسی نقش واحدهای کنترل الکترونیکی[2] در وسایل نقلیه ریلی از طریق بررسی معماری توزیع‌شده پردازنده‌ها و به‌طور خاص میکروکنترلرهای سری TC1797 پرداخته و از طریق تحلیل نتایج شبیه‌سازی تحت شرایط خاص از قبیل تغییر جریان خروجی‌های برنامه از قبیل تزریق کدهای SQL مخرب و تأثیرات آن بر واحدهای کنترلی پرداخته‌اند. این مطالعه هرچند آسیب‌پذیری‌های ECUهای بازرگانی مورداستفاده در TCMS را تبیین نکرده اما در نتیجه‌گیری تحقیق ضمن تأیید یافته‌های مطالعه اسکینیر (۲۰۰۹) یک حمله فرضی را برای یک نمونه واحدهای کنترل الکترونیکی شبیه‌سازی نموده و بر اساس یافته‌های میدانی نتیجه گرفته است که مکانیسم‌های حفاظت از حافظه و پردازشگر در برابر حملات سایبری در واحدهای کنترل الکترونیکی های قطارهای مسافری از استحکام کافی برخوردار نیستند. پژوهش یادشده همچنین چگونگی مواجه با آسیب‌پذیری‌های نرم‌افزاری را در میکروکنترلرهای قطار مورد آنالیز قرار داده و آورده است که پردازنده‌های قطار در برابر برخی حملات نظیر تزریق کدهای مخرب زبان جستجوی ساختار یافته[3] دچار خطای سخت‌افزاری شده و باعث بروز مشکلاتی در ولتاژ و کلاک پالس پردازنده می‌شوند. نتایج مطالعه مزبور با بیانی دیگر توسط پونسارد[4] و همکاران (۲۰۲۲) تأییدشده است.

در مطالعه دیگری پیکین[5](۲۰۲۱) به بررسی امنیت شبکه‌های ارتباطی برای انتقال داده‌ها میان وسایل نقلیه ریلی و بخش‌های کنترل ترافیک قطار در قالب توپولوژی (همبندی) CAN پرداخته است. در این مطالعه محقق ضمن تأکید بر ضعف‌های موجود در استانداردهای بین‌المللی و مرتبط در عدم تدقیق جامع ویژگی‌های درونی امنیت شبکه‌های رایانه‌ای ریلی، در نتایج مطالعه خود

1- Papp &Buttyan
2- ECU
3 - SQL
4- Ponsard
5- Pekin

آورده است که گذرگاه انتقال داده در شبکه‌های CAN برای ارتباطات شبکه‌های ریلی از امنیت کافی برخوردار نیست زیرا در این همبندی اصول محرمانگی، یکپارچگی، دسترس‌پذیری و همچنین احراز اصالت تضمین نشده و انواع مختلف حملات نظیر جعل، شخص ثالث، ردگیری و غیره... پشتیبانی نمی‌شود. اهمیت این امر تا بدان جا است که در صنایعی نظیر خودروسازی یا واگن سازی، برخی از تولیدکنندگان در سامانه‌های مبتنی بر سخت‌افزارهای توزیع‌شده برای فرستنده و گیرنده پیام در واحدهای کنترل صنعتی الکترونیکی به‌منظور ایجاد استحکام سامانه‌ها در برابر تهاجمات هکرها از سامانه‌های IPS و IDS برای تشخیص و مقابله با نفوذ و همچنین پروتکل‌های رمزنگاری استفاده می‌شود. بااین‌وجود تعاملات شبکه‌ای و پیام‌های رمزنگاری‌شده در معرض تهدیدهای دیگری هستند ازاین‌رو با استفاده از تحلیل‌های قدرتمند یا سایر تکنیک‌های مکمل برای دریافت پیام رمز شده در مقصد سیستم‌های تعبیه‌شده در قطار و کنار خط آهن استفاده می‌شود.

نتایج یک مطالعه که توسط اَمبروس و همکاران (۲۰۱۸) انجام‌شده، نشان می‌دهد که هدف برخی از تکنیک‌های حمله در شبکه ریلی، تهاجم به ارتباطات میان سنسورهای فیزیکی نصب‌شده در قطار و تجهیزات کنار خط آهن با واحدهای مختلف کنترل علائم و سیگنالینگ است. یافته‌های این مطالعه نشان می‌دهد که در این قبیل حملات مهاجمان از طریق تزریق داده‌های نادرست به پایگاه‌های اطلاعات، به دست‌کاری داده‌های صحیح و نرمال حسگرها پرداخته و مقادیر ولتاژ یا جریان را از طریق تداخل‌های الکترومغناطیسی تغییر می‌دهند.

نتایج مطالعه زلوسکی و همکاران (۲۰۱۹) نشان می‌دهد که برخی خبرگان امنیت فن‌آوری اطلاعات و ارتباطات ریلی، قطار را به‌عنوان یک مجموعه جامع از مراکز جمع‌آوری داده‌های حیاتی برای کنترل فرآیندهای حساس سیر و حرکت قطار در نظر می‌گیرند که می‌تواند توسط نفوذ گران فضای سایبری موردحمله قرار گیرد. در مطالعه فوق‌الذکر محققان تجهیزات کلیدی قطار شامل را به چندین واحد الکترونیکی کنترل تسهیلات سیر و حرکت تقسیم کرده‌اند که بر روی قطار نصب بوده اما در فرایند سیر ایمن قطار نقش به سزایی دارد و هر یک دارای عملکرد وظیفه‌ای خاصی در کنترل قطار است. برخی از تجهیزات کلیدی از این قرار است: واحد کنترل

قطار (VCU[1])، واحد کنترل درب‌های قطار (DCU[2])، واحد کنترل سیستم ترمز قطار (BCU[3]) و واحد کنترل نیروی رانش قطار (TCU[4]). در بخشی از یافته‌های پژوهش مزبور آمده است که سیستم‌های یادشده، بر روی قطار نصب‌شده‌اند و رفتارهای حرکتی قطار را کنترل و در نتیجه ایمنی آن را در طول مسیر حرکت تضمین می‌نمایند. در همین راستا مطالعه (باریل و همکاران (۲۰۱۶) ضمن تأیید نتایج مطالعه قبلی با بررسی نقاط آسیب‌پذیری و ریسک‌های قطار آورده است که مقصد جذاب و صریح برخی نفوذ گران برای رخنه و حمله به سامانه‌های کنترل درب‌های قطار، سیستم کنترل الکتروموتورها و غیره ... است. در تحقیق یادشده محققان ضمن بیان آسیب‌های سیستم کنترل تراکشن قطار به آنالیز برخی حملات سایبری این بخش پرداخته‌اند. در یک مطالعه دیگر ری کیک و همکاران (۲۰۱۶) به ارزیابی و تحلیل آن دسته از حملات خارجی پرداخته‌اند که می‌تواند به‌صورت از راه دور و با استفاده از ابزارهای موجود در سیستم مدیریت کنترل ترافیک، ضمن نقض اصول مثلث امنیت (CIA) بر عملکرد سامانه‌های ارتباطی و ناوبری قطار متمرکزشده و رفتار نظام‌مند آن را مختل نماید. همچنین در مستندات استاندارد IEEE ISNCC (۲۰۱۹) ضمن تبیین ابعاد محرمانگی، یکپارچگی و دسترس‌پذیری در زیرسامانه‌های کنترلی قطار و مرکز فرمان، مراحل و تکنیک‌های ارزیابی نفوذ گری و حملات سایبری در این سامانه‌ها از طریق تست نفوذ و ارزیابی امنیتی تشریح شده است.

در مطالعه دیگری که توسط اوکا و همکاران (۲۰۱۹) انجام‌شده است، محققان ضمن تبیین ابعاد مرتبط با تهدیدها و ریسک‌های سیستم کنترل درب‌های قطار به برخی تبعات ناشی از حملات سایبری به این واحد کنترلی پرداخته و یکی از مهم‌ترین آثار تهاجم را بروز خطاهای پیکره‌بندی ذکر کرده‌اند. لازم به ذکر است که ارزیابی و تحلیل ریسک‌های امنیتی و ایمنی در شبکه ریلی با استفاده از ماتریس ارزیابی ریسک به روش FMEA (نظیر تساوی شدت ریسک در احتمال بروز) و به دست آوردن عدد تحلیل ریسک انجام می‌شود و در مورد ارزیابی‌های امنیتی ناشی از حملات سایبری در قطارها از طریق تکنیک‌های ارزیابی‌های امنیتی برای برآورد پتانسیل‌های احتمال بروز نفوذ استفاده می‌شود (تالبی، ۲۰۱۷). در برخی تحقیقات دیگر نظیر

1- vehicle control unit
2- Doors control unit
3 - Break control unit
4 - Traction control unit

یامپولسکی (۲۰۱۷) و بارنا (۲۰۲۲) به تبعات ادامه سیر قطار پس از ارزیابی امنیتی و وجود ریسک‌های غیرقابل‌قبول اشاره نموده‌اند و در یافته‌های مطالعه خود آورده‌اند که برخی آسیب‌پذیری‌های شبکه ریلی ناشی از طراحی ناایمن نرم‌افزارهای کنترلی قطار، عدم وجود حفاظت‌های مستحکم فیزیکی برای تجهیزات رایانه‌ای و ناآگاهی کارکنان شبکه ریلی نسبت به ماهیت مخاطرات امنیتی است و برخی از تبعات مهم تهاجمات سایبری نظیر شنود شخص ثالث، دستبرد، ویروسی شدن ناشی از بدافزار، انکار، ربایش جلسات ارتباطی میان تجهیزات و غیره ... را ذکر نموده و توصیه کرده‌اند که برای اتخاذ اقدامات مؤثر متقابل از سیستم‌های تشخیص نفوذ پیشرفته استفاده شود.

در تحقیق دیگری شاکلا (۲۰۱۹) به بررسی مخاطرات امنیتی مرتبط با سامانه رانش قطار پرداخته است. در مطالعه مزبور محقق ضمن ارزیابی ریسک‌های سایبری مرتبط با واحد کنترل الکتروموتورهای قطار، برخی تهدیدهای امنیتی مرتبط را ذکر نموده و در یک کار میدانی با اندازه‌گیری پارامترهای ترمز الکترودینامیکی؛ در نتایج مطالعه خود آورده است که حملات سایبری در این حوزه می‌تواند در بستر میدان‌های الکترومغناطیسی مدارهای خط آهن، با استفاده از سیگنال‌های جعلی یا تروجان‌های سخت‌افزاری و نرم‌افزاری، سیگنال‌های الکتریکی را متأثر نموده و با نقض محدودیت‌های ایمنی مرتبط با ولتاژ، کارایی سیستم را دچار اختلال نماید.

در یک تحقیق که توسط پانسردیتال[1] و همکاران (۲۰۱۵) در خصوص امنیت سامانه‌های کنترل ترمز قطار انجام‌شده است، محققان ضمن ترسیم درخت حمله این سامانه کلیدی، از طریق شیوه‌های مرسوم و یکپارچه‌ی ارزیابی مهندسی امنیت و ایمنی صنعت ریلی نشان داده‌اند که چگونه کارکردهای وظیفه‌ای سیستم ترمز، می‌تواند در یک حمله خاص سایبری توسط نفوذ گران به مخاطره افتاده و راهکارهای متقابل تا چه اندازه از اثربخشی برخوردارند.

در یک جمعبندی اجمالی از پیشینه پژوهش مشاهده می‌شود که خلأ تحقیقاتی وسیعی در خصوص یکپارچگی امنیت فضای سایبری و مهندسی ایمنی وجود دارد که در صورت تحقق می‌تواند سبب ارتقای سطح استحکام سامانه‌های عملیاتی و مسافری در مقابل حملات نرم‌افزاری و

1- Ponsardetal

سخت‌افزاری سیستم‌ها و زیرسیستم‌های شبکه حمل‌ونقل ریلی گردد و از این منظر پژوهش حاضر می‌تواند یک کار جدید و تازه باشد.

۳- روش انجام پژوهش

همان‌گونه که پیش‌تر نیز گفته شد هدف از تحقیق حاضر در یک سطح مفهومی بررسی قابلیت اطمینان، دسترس‌پذیری و یکپارچگی سامانه‌های ایمنی شبکه ریلی است بنابراین روش انجام پژوهش حاضر مبتنی بر تحلیل ایمنی عملیات ریلی از طریق روش‌های کمی و شبیه‌سازی بوده و به پیشنهاد یک رهیافت مبتنی بر قابلیت اطمینان از طریق مدل‌سازی فرکانس و احتمال بروز سانحه با توجه به توپولوژی شبکه ریلی پرداخته است. از سوی دیگر با استفاده از روش‌های کمی به مطالعه امکان‌پذیری حفظ و نگهداشت شبکه ریلی در برابر حملات سایبری از منظر زمان بازیابی سیستم‌ها پرداخته شده و به‌منظور شناسایی ایستگاه‌ها و بخش‌های مهم ریلی از منظر امنیتی از رویکرد K-means استفاده شده است. به‌منظور بررسی اثربخشی خروجی‌های به دست آمده در این مدل، رفتارهای یک سیستم موردی در شرایط واقعی مورد آزمون قرار گرفته است. همچنین از یافته‌های مطالعه موردی به‌منظور مشخص نمودن کارآمدی مدل پیشنهادی در شناسایی ایستگاه‌ها و بخش‌های مهم شبکه ریلی با لحاظ کارایی و ظرفیت شبکه یاری گرفته می‌شود. همچنین در این مطالعه در نهایت شاخص‌هایی برای سنجش ایمنی شبکه راه‌آهن ارائه می‌گردد.

۳-۱- آنالیز توصیفی شبکه ریلی

سیستم ریلی یک شبکه گسترده است که با استفاده از گراف $G=(N,E)$ توصیف می‌شود. در این شبکه $n = N$ نشان‌دهنده ایستگاه‌ها و $e= E$ ناظر بر خطوط ریلی است که ایستگاه‌های مجاور i و j را به هم متصل می‌نماید.

۳-۲- تجزیه‌وتحلیل قابلیت اطمینان در شبکه ریلی

قابلیت اطمینان شبکه ریلی به عملیات سیر و حرکت قطارها با احتمال عددی وقوع صفر حادثه در زمان بهره‌برداری اطلاق می‌گردد. با توجه به نتایج به دست آمده از مطالعات پیشین می‌توان

احتمال بروز سانحه‌های عمدی (انسان‌ساز) یا غیرعمدی در شبکه ریلی را با توجه کران‌های بـالا و پایین احتمال بروز سوانح که به‌صورت P_{ij}^{up} و P_{ij}^{down} نشان داده می‌شود میان ایستگاه‌هـای i و j را با استفاده از رابطه زیر به دست آورد:

$$P_{ij}^{up} = \frac{N_{ij}^{up}}{T} , P_{ij}^{down} = \frac{N_{ij}^{down}}{T}$$ رابطه شماره (۱)

در رابطه شماره یک N_{ij}^{up} و N_{ij}^{down} به ترتیب حدود بالا و پایین برای احتمال بروز وقایع برنامه‌ریزی‌شده در شبکه ریلی هستند و T یک مقدار آماری است که احتمال شکست شبکه ریلی در برابر حملات سایبری را نشان می‌دهد. این مسئله می‌تواند از طریق رابطه زیر توصیف شود:

$$P_{ij} = P_{ij}^{up} P_{ij}^{down}$$ رابطه شماره (۲)

در یک شبکه ریلی تعداد زیادی اعزام برای قطارها در نظر گرفته می‌شود. بنابراین فرض کنیم Pik نشان‌دهنده احتمال بروز سوانح و حملات برنامه‌ریزی‌شده در مسیر k و ایستگاه ریلی i باشد در این صورت احتمال بروز نفوذ در سیستم‌های ایستگاه ریلی i به‌صورت رابطه شماره سه نشان داده می‌شود:

$$P_i = \prod_{k=1}^{K} P_i^k$$ رابطه شماره (۳)

بنابراین قابلیت اطمینان شبکه ریلی در برابر حملات سایبری با استفاده از رابطه شماره چهـار بـه دست می‌آید:

$$R_G = \prod_{ij \in N}(1 - P_{ij}) \prod_{i \in N}(1 - P_i)$$ رابطه شماره (۴)

۳-۳- مدل مفهومی کارایی شبکه ریلی در برابر تهاجمات سایبری و فیزیکی

با در نظر گرفتن جریان ترافیـک میـان ایسـتگاه‌هـای شـبکه ریلـی، کـارایی شـبکه ریلـی G را می‌توان با استفاده از رابطه شماره ۵ به‌صورت زیر محاسبه نمود:

$$E = \sum_{mn} \frac{u_{mn}}{d_{mn}}$$ رابطه شماره (۵)

در رابطه فوق u_{mn} تعداد قطارهای عبوری در مسافت میان ایستگاه m تا ایستگاه n را نشان می‌دهد و d_{mn} حداقل فاصله زمانی میان این دو ایستگاه است و 'E نشان‌دهنده کارایی زمانی شبکه ریلی برای حالتی است که یک ایستگاه خاص در معرض تهاجم نفوذگران قرار بگیرید در این صورت میزان کارایی شبکه پس از بروز حادثه است که مقدار آن با استفاده از رابطه شماره ۶ به دست می‌آید:

$$\Delta E = \frac{E-E'}{E}$$ رابطه شماره (۶)

حال فرض کنیم X_j^i تعداد قطارهای عبوری بین ایستگاه‌های ریلی مجاور i و j باشد در این صورت چنانچه X_j نشانگر تعداد قطارهای ورودی از سایر ایستگاه‌ها به ایستگاه i باشد. در این صورت خواهیم داشت:

$$F_j^i = \frac{x_j^i}{X_j}$$ رابطه شماره (۷)

همچنین تعداد قطارهای ورودی به ایستگاه j با استفاده از رابطه زیر به دست می‌آید:

$$X_j = \sum_{i=1}^{N-1} F_j^i X_i + \sum_{s=1}^{S} x_j^s = \sum_{i=1}^{N-1} F_j^i X_i + U_j$$ رابطه شماره (۸)

برای به دست آوردن مجموع قطارهایی که به‌تمامی ایستگاه‌های شبکه ریلی اعزام می‌شوند می‌توان از رابطه شماره ۹ استفاده نمود:

$$X = F^{(-i)}X + U$$ رابطه شماره (۹)

حال چنانچه قطعه میان ایستگاه‌های U و V نتواند به هر علتی ظرفیت شبکه ریلی را پوشش دهد در این صورت می‌توان شبکه از رابطه زیر برای محاسبه ظرفیت جدید استفاده نمود:

$$X^{-(u,v)} = \left(1 - F^{(-i-(u,v))}\right)^{-1} U$$ رابطه شماره (۱۰)

با لحاظ آنچه در فوق گفته شد ظرفیت شبکه ریلی پس از بروز حملات سایبری با استفاده از رابطه زیر به دست می‌آید:

$$\Delta C = \frac{\sum X - \sum X^{-(u,v)}}{\sum X}$$ رابطه شماره (۱۱)

زمان بازیابی شبکه ریلی بر اساس تعداد حملات ثبت‌شده با توجه به زمان شروع و پایان حمله که با t_s و t_e نشان داده می‌شود با استفاده از رابطه شماره ۱۲ به دست می‌آید:

$$M = 1 - \frac{t_r}{t_o}$$ رابطه شماره (۱۲)

۳-۵- تجزیه‌وتحلیل امنیت و ایمنی

ارزیابی امنیت و ایمنی شبکه ریلی با لحاظ ریسک بروز حمله و از دست رفتن قابلیت دسترس‌پذیری و نگهداری سیستم (M) و تبعات بروز حمله (S) از رابطه شماره ۱۳ محاسبه می‌شود:

$$S = (1 - R)\Delta A(1 - M)$$ رابطه شماره (۱۳)

در رابطه شماره ۱۳ S تبعات حمله را نشان می‌دهد و R نشان‌دهنده احتمال بروز نفوذ در شبکه ریلی است. حال چنانچه در حالت بروز حمله به شبکه ریلی قطعات موردحمله قرار گرفته فرموله شوند مقدار ریسک را می‌توان از رابطه زیر محاسبه نمود:

$$EL_{ij} = p_{ij}\Delta E(1 - M), CL_{ij} = p_{ij}\Delta C(1 - M)$$ رابطه شماره (۱۴)

در رابطه شماره ۱۴ EL_{ij} نشان‌دهنده مقدار اتلافات شبکه پس از بروز تهاجم و CL_{ij} نشان‌دهنده اتلاف رخ‌داده در ظرفیت شبکه در اثر تهاجم نفوذگران است. بنابراین در خصوص عدد ریسک می‌توان از رابطه شماره ۱۵ استفاده نمود:

$$EL_i = p_{ij}\Delta E(1 - M), CL_i = p_{ij}\Delta C(1 - M)$$ رابطه شماره (۱۵)

در رابطه فوق EL_i نشان‌دهنده مقدار کارایی ازدست‌رفته شبکه در اثر تهاجم سایبری و CL_i نشان‌دهنده میزان ظرفیت ازدست‌رفته شبکه در اثر حملات رخ‌داده شده است. برای ارزیابی سطح امنیت و ایمنی قطعات ریلی و یا ایستگاه‌ها با توجه به افت کارایی شبکه ناشی از حملات سایبری

از روش K-means استفاده می‌شود. رویکرد K-means یک روش خوشه‌بندی است که می‌تواند داده‌ها را در کلاس‌های مختلف طبقه‌بندی نماید. بنابراین رویکرد K-means می‌تواند به یافتن بخش‌های بحرانی شبکه ریلی و ایستگاه‌ها از منظر امنیت و ایمنی کمک نماید.

٤- مطالعه موردی: بررسی حادثه حمله‌ی سایبری به راه‌آهن منطقه‌ای ایتالیا (٢٠١٤)

در مورد کاوی این پژوهش ابعاد حمله سایبری به راه‌آهن منطقه‌ای ایتالیا در بخش‌هایی نظیر سامانه کنترل ترمز و سیستم ضد لغزش قطار (WSP[1]) و غیره ... مورد تحلیل قرارگرفته و از طریق بررسی سناریوهای احتمالی حملات سایبری به ارائه یک تحلیل یکپارچه از فضای تهاجم پرداخته‌شده است.

٤-١- شرح کلیت سانحه

در راه‌آهن منطقه‌ای ایتالیا، قطاری که با سرعت ٨٠ کیلومتر بر ساعت در حال طی مسیر ریلی تعیین‌شده در جدول زمان‌بندی بود با تأخیری در حدود ٣٠ ثانیه در اعمال ترمز در چرخ‌ها، پس از ارسال پالس سیگنال ترمز گیری توسط راهبری قطار مواجه گردید. تحقیقات میدانی کمیسیون عالی سوانح ریلی ایتالیا نشان از بروز اختلال ارتباطی در واحد ضد لغزش چرخ‌ها در سیستم ترمز قطار داشت.

هرچند در پی اقدامات صورت گرفته توسط تیم نگهداری و تعمیرات به‌وسیله پیکره‌بندی مجدد دریچه‌های WSP با استفاده از استاندارد مرتبط در اتحادیه بین‌المللی راه‌آهن‌ها (سند شماره UIC 541-05) و به‌روزرسانی نرم‌افزار واحد کنترل ترمز به رفع اختلال امکان‌پذیر گردید اما ردگیری سیستم حاکی از نفوذ گری گسترده در این ابزار حیاتی قطار بود.

دپارتمان واکنش اضطراری حملات سایبری راه‌آهن سرتاسری ایتالیا، پس از آنالیز داده‌های ضبط‌شده در بانک اطلاعاتی تشخیص خطاهای قطار، علت سانحه را عملکرد غیرعادی زیرسیستم WSP در سامانه ترمز اعلام نمود و در گزارش نهایی خود این‌گونه توضیح داد: "واحد کنترل WSP در آغاز فرایند ترمز گیری، سیگنال غلط دریافت نموده است که درنتیجه به‌عکس العمل

1- Wheel slide protection

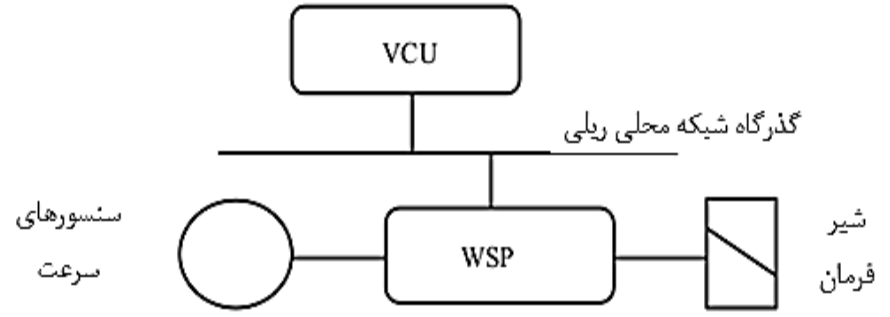
نادرست بخش اجرایی ترمز منتهی شده و این به دلیل پاک شدن داده‌های صحیح در بانک اطلاعاتی بوده و در ادامه، ایجاد اختلال در ارتباط بخش مقایسه کننده‌ی واحد کنترل WPSبا مقادیر برنامه‌ریزی‌شده جدید و اشتباه که در حافظه دیتابیس جایگزین داده‌های درست و ذخیره‌شده در حافظه به‌عنوان مقادیر مبنا بوده است و همچنین عدم امکان به‌روزرسانی جداول متناسب با مختصات خط ریلی بوده که درنهایت به‌فرمان نادرست برای بخش اجرایی سیستم ترمز منجر شده است". لازم به توضیح است در وسایل نقلیه ریلی، سامانه WSP یک سیستم کنترلی محسوب می‌شود که بر اساس گشتاور قطار در سامانه سیستم ترمز از طریق تنظیم فشار هوا در سیلندرهای ترمز، فرمان‌های الکتریکی متناسب را برای سوپاپ‌های تخلیه ارسال می‌نماید که ضمن حفظ چسبندگی میان چرخ و ریل، از قفل شدن چرخ‌ها در هنگام ترمز گیری جلوگیری نموده و درنتیجه از خرابی خط و صاف شدن چرخ پیشگیری می‌نماید. بنابراین WSP یک سیستم حیاتی برای ایمنی سیر و حرکت قطارها محسوب می‌شود که بروز اشکال یا خرابی آن می‌تواند اشکالات زیر را در شبکه ریلی ایجاد نماید:

نخست: گشتاور ناکافی نیروی ترمزی و عدم اعمال به هنگام آن‌که مسافت ترمزی را به‌صورت غیر نرمال افزایش می‌دهد.

دوم: نیروی گشتاور بیش‌ازحد ترمزی که درنتیجه منجر به لغزش چرخ‌ها در امتداد ریل حرکتی شده که علاوه بر صاف شدن چرخ می‌تواند در موارد حاد باعث خروج قطار از خط شود (لاکشمینارایانا، ۲۰۱۹).

در این راستا (بارنا، ۲۰۲۲) شرح جامعی از استانداردهای مرتبط با ایمنی سیر و حرکت از طریق WSPرا ارائه نموده است. در این استاندارد شباهت‌های فراوانی میان سیستم WSP و سیستم ضد قفل خودروها (ABS) ازنظر معماری و عملکردی ذکرشده است. لذا می‌توان تهدیدها و آسیب‌های مکانیکال مترتب بر ABS را به‌طور مشابه برای WSP نیز لحاظ نمود و این بدان معناست که سنسورهایWSP از همان فن‌آوری‌های ساختاری مشابه استفاده می‌کنند. در مطالعه انجام‌شده توسط زلوسکی و همکاران (۲۰۱۹) عکس‌العمل‌های سیستم در قبال تزریق کدهای مخرب به پایگاه اطلاعات این سامانه موردبررسی قرارگرفته است. در مطالعه دیگری که توسط شکری و همکاران (۲۰۱۹) در خصوص این فن‌آوری انجام‌گرفته، محققان به توصیف

تکنیک‌های حمله به زیرسیستمWSP پرداخته و از نتایج آن برای تجزیه‌وتحلیل آسیب‌های احتمالی سامانه نرم‌افزاری WSP در صنعت حمل‌ونقل ریلی استفاده کرده‌اند. ازنظر عملکردی واحد کنترل قطار (VCU) به‌عنوان یک مرجع اصلی، به اندازه‌گیری سرعت واگن‌های قطار می‌پردازد و اطلاعات به‌دست‌آمده را برای واحد کنترلر WSP ارسال می‌نماید. واحد کنترل WSP داده‌های گردآوری‌شده از سنسورهای سرعت هریک از محورهای بوژی قطار را با سرعت برنامه‌ریزی‌شده در ماژول مربوطه مورد مقایسه قرار داده و با استفاده از آن از طریق شیر تخلیه فشار هوای فشرده پشت سیلندر ترمز را تنظیم نموده و قدرت ترمزی را هماهنگ می‌سازد. در تصویر شماره یک، ضمن ترسیم معماری زیرسیستم WSP نصب‌شده در قطار حادثه راه‌آهن منطقه‌ای ایتالیا به تجزیه‌وتحلیل عملکرد سیستم پرداخته‌شده است.



تصویر شماره ۱) معماری ساختار WSP به بیان ساده

طبق معماری ترسیمی در تصویر شماره یک می‌توان توابعی عملکردی هر یک از بخش‌ها به شرح ادامه تبیین نمود:

- سنسورهای سرعت: بر اساس استانداردهای تولید قطار، سنسورهای سرعت که بر روی قطار نصب‌شده‌اند از نوع مغناطیسی است.
- VCU (واحد کنترل قطار): نقش کنترلر را در معماریWSP بر عهده داشته و لذا بر اساس معماری میکروکنترلر تعبیه‌شده در آن، می‌توان نوع کامپایلر مورداستفاده در نرم‌افزار تشکیل‌دهنده WSP را استنباط نمود.

- گذرگاه انتقال داده محلی قطار که به‌عنوان ابزار مخابراتی و ارتباطی در شبکه تجهیزات سخت‌افزاری قطار مورداستفاده قرار می‌گیرد.

بر اساس نتایج برخی مطالعات نظیر مطالعه کارای (۲۰۲۱) تجهیزات شبکه گذرگاه انتقال داده‌های قطار از چندین بُعد مختلف دارای نقاط آسیب‌پذیری است که از آن جمله می‌توان به موارد زیر اشاره نمود:

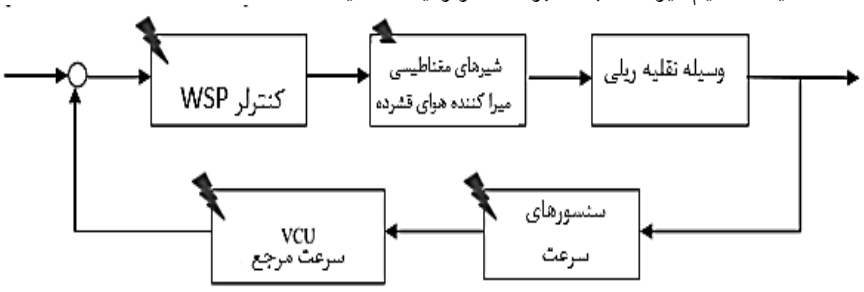
نخست: سطح و طیف حمله به سیستمWSP قطار؛ که در تصویر شماره دو بلوک دیاگرام ساده‌شده WSP برای شناسایی نقاط آسیب‌پذیری و تهاجم به WSP قطار ترسیم‌شده است. بر این اساس واحدهای مختلف WSP قطار برحسب شدت آسیب‌پذیری به شرح زیر است:

۱- واحد کنترلر سخت‌افزاری و نرم‌افزاری WSP قطار

۲- گذرگاه ارتباطی میان سنسورهای سرعت و واحد پردازش و مقایسه سرعت جاری با سرعت مرجع که در میان گزینه‌های متعدد تجهیزات قطار برای نفوذگران از جذابیت بالایی برخوردار می‌باشد زیرا مهاجمان می‌توانند از طریق تزریق کدهای مخرب به پایگاه داده به ثبت اختلاف غیرواقعی میان سرعت مرجع و سرعت واقعی قطار منجر شده و درنتیجه فرایند اعمال هوای فشرده برای ترمز گیری را دچار خطا نمایند.

۳- گذرگاه ارتباطی میان واحد کنترل WSP و شیرهای مغناطیسی تخلیه و تنظیم فشار باد سیلندر ترمزهای سیستم ترمز قطار

۴- کنترلر شیرهای مغناطیسی تخلیه هوای فشرده که از طریق تزریق داده‌های اشتباه می‌تواند زمینه تصمیم‌گیری اشتباه را برای کنترلر ایجاد نماید.



تصویر شماره ۲) WSP قطار به‌عنوان یک سیستم کنترل‌کننده

۵- بحث

امروزه حمل و نقل ریلی به یک شیوه محبوب برای جابجایی در شهرها بدل شده است. بااین‌حال حملات سایبری می‌توانند عملیات معمول شبکه ریلی را دچار اختلال نمایند. بنابراین قابلیت اطمینان و دسترس‌پذیری شبکه ریلی از منظر کارکردی لازم است مورد تجزیه‌وتحلیل قرار گیرد تا میزان آسیب‌پذیری شبکه در برابر شکست‌های امنیتی در تسهیلات ریلی تعیین گردد. قابلیت اطمینان شبکه ریلی یک جنبه مهم است که می‌تواند از حملات سایبری متأثر گردد.

در سانحه حمله سایبری به‌قطار منطقه‌ای ایتالیا با توجه به نتایج تحلیل بردار حمله، نفوذ گران از تکنیک‌های رسوخ به حفره‌های امنیتی، دو بخش کلیدی را موردتهاجم قرار داده بودند که به شرح زیر بیان می‌شود:

نخست: حمله به واحد کنترل الکترونیکی WSP قطار با هدف تخریب حافظه داخلی از طریق تزریق کدهای غلط و بهره‌گیری از تکنیک نفوذگری سرریز بافر در WSP قطار

دوم: حمله نفوذ گران به گذرگاه انتقال داده و شبکه ارتباطی میان سنسورهای سرعت و واحد کنترل الکترونیکی WSP که از طریق تزریق اطلاعات نادرست، سبب ایجاد تفاوت غیرواقعی میان سرعت واقعی و سرعت مرجع در خط منطقه‌ای ایتالیا گردید و درنتیجه به رفتار غیر نرمال واحد کنترل WSP منجر شد. هرچند بر اساس اعلام شرکت سازنده‌ی قطار، بروز این رخداد از شرایط بسیار نادر در سامانه‌ی ترمز قطارها بوده، اما بااین‌حال بر اساس گزارش دپارتمان امنیت و ایمنی وقوع این سانحه ناشی از درک نادرست شرکت سازنده از رفتار واقعی سامانه ترمز قطارها در مناطق بین‌شهری بوده است، هرچند بر اساس شواهد به‌دست‌آمده، تمامی اجزا و ارکان سیستم کنترل WSPدر ناوگان قطارهای راه‌آهن ایتالیا با استانداردهای خاص تدوین‌شده توسط اتحادیه بین‌المللی راه‌آهن‌ها (UIC) انطباق داشته است، لیکن تنظیم نامناسب شیرهای مغناطیسی تخلیه هوای فشرده در سری‌های زمانی غلط بر اساس حمله سایبری، سبب عملکرد نادرست واحد کنترل در تنظیم WSP برای پیکره‌بندی صحیح خروجی سنسورهای سرعت قطار گردید. در این سانحه

تجزیه‌وتحلیل واحد کنترل الکترونیکی WSPنشان داد که پیامدهای ناشی از عدم شناسایی ریسک‌ها و تهدیدهای بالقوه، ترکیبی از علل بروز خطا را به وجود آورد که در اثر آن زمینه مناسبی برای تهاجم نفوذ گران را به وجود آورد که سامانه‌ی ترمز قطار را دچار اختلال نمود. آموزه‌های این حادثه به پیشنهادهای جدید برای طبقه‌بندی حملات تأثیرگذار بر سیستم ترمز قطار منتهی گردید که می‌تواند در یکی از دسته‌های زیر قرار گرفته و یا ترکیبی از آن‌ها باشد:

- حملات فیزیکی که در آن مهاجمان معماری سیستم‌های کنترل قطار را با هدف طراحی دلخواه برای نفوذ از طریق نصب سیستم‌های مخرب تغییر می‌دهند.
- حملات غیرفعال از طریق کانال‌های جانبی قطار که در آن مهاجمان با مشاهده و شنود سیگنال‌های ارتباطات بیرونی سیستم و تجزیه‌وتحلیل توان دفاعی، زمان اجرای یک برنامه را بر اساس نشت مغناطیسی داده‌ها برای به دست آوردن کلیدهای رمزنگاری مورداستفاده قرار می‌دهند.
- حملات منطقی به شبکه‌های ارتباطی و نرم‌افزارهای نصب‌شده در قطار
- استفاده نفوذ گران از تکنیک درب‌های پشتی[1] بر اساس بهر گیری از آسیب‌پذیری‌های نرم‌افزارهایی که پیش‌تر از طریق بدافزارها و کدهای مخرب در قطار نصب‌شده‌اند. به‌عنوان‌مثال استفاده از سرریز بافر که برای تغییر روند اجرای برنامه‌های سیر و حرکت قطارها از طریق کُدهای مخرب به حافظه سخت‌افزار تزریق‌شده‌اند.
- استفاده از ضعف‌های موجود در رمزنگاری و پروتکل‌های مربوطه به‌منظور رمزگشایی از پیام‌های ارسال‌شده بر روی شبکه‌های مخابراتی قطارها و اجرای حملاتی نظیر جعل، تغییر، تزریق پیام، ایجاد ترافیک کاذب، MITM و غیره در سامانه سیر و حرکت قطارها

در حادثه قطار منطقه‌ای ایتالیا، داده‌های تغیر یافته که از طریق شبکه ارتباطی قطار برای تنظیم سرعت ارسال شدند دارای تبعاتی چندگانه بودند. حملات در این سانحه در یک سری زمانی

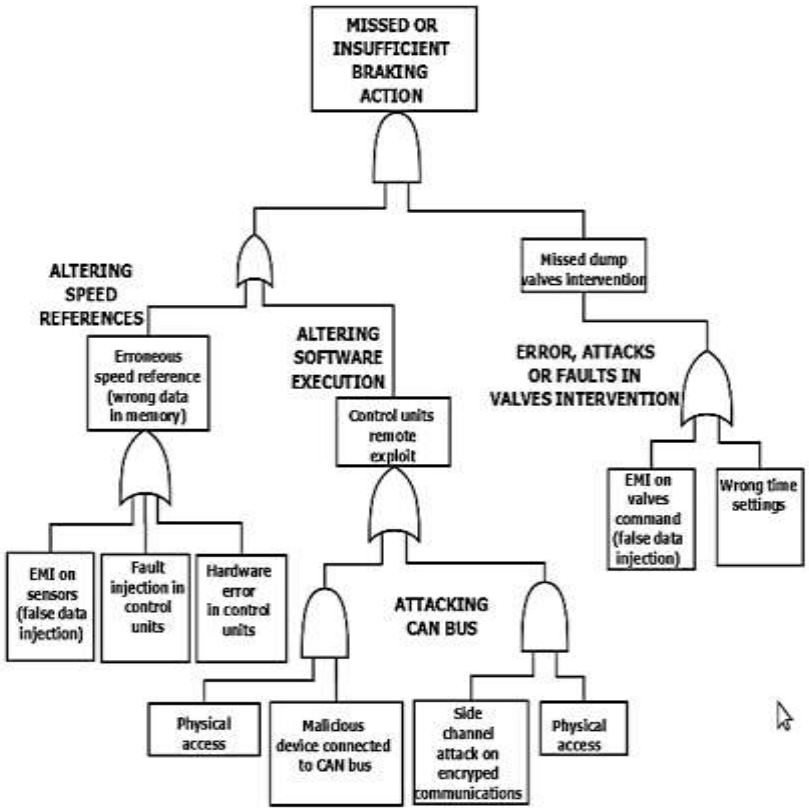
1- backdoor

متوالی و متناسب و بر اساس طرح قبلی با هم ترکیب شدند تا اهداف مدنظر مهاجمان برآورده شود. آثار این تهاجم نشان می‌دهد که خطاها می‌توانند که خود می‌توانند ناشی از خرابی تجهیزات و یا نقص فنی باشد و در زمره آسیب‌پذیری‌های شبکه ریلی به شمار می‌آیند. خطاهای سیستم توسط حملات فعال مورداستفاده قرار می‌گیرد و آسیب‌پذیری‌ها توسط تهدیدهای محیطی شبکه ریلی استفاده می‌شوند و این در حالی است که اشتباهات کاربران شبکه ریلی می‌تواند منشأ حملات فعال و بالفعل نمودن تهدیدها شود.

ملاحظات فوق در سانحه ریلی قطار منطقه‌ای فرانسه برای محققان دو دستاورد مهم به همراه داشت که عبارت بودند از نخست: اهمیت تحلیل کلی ریسک‌های سیستم و دوم: ضرورت یکپارچه‌سازی تجزیه‌وتحلیل خطاها و آسیب‌پذیری‌های سیستم

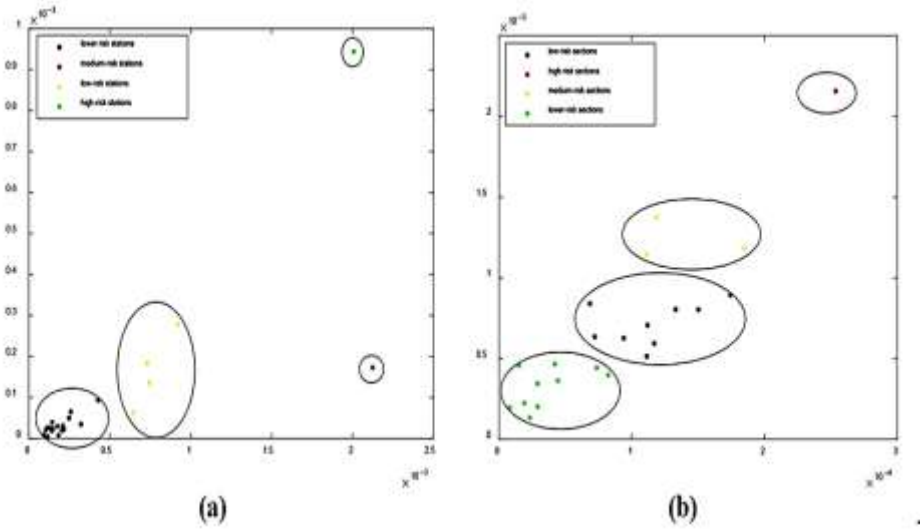
برای نیل به دستاوردهای فوق می‌توان از تکنیک توأمان درخت حمله و خطا استفاده نمود. بر اساس استانداردهای EN 50126 و IEC 61025 درخت تجزیه‌وتحلیل خطا و درخت حمله می‌توانند برای آنالیز شکست‌ها و شناسایی ریسک‌ها در شبکه ریلی مورداستفاده قرارگرفته و نشان‌دهنده تعامل و رابطه علی میان خرابی‌های سیستم، زیرسیستم‌ها و قطعات باشد که به‌طور مشابه در درخت حمله و خطا به‌عنوان یک تکنیک مؤثر شناسایی و نمایش حملات سایبری از طریق ساختارهای درختی، هم برای حملات مجزا به تجهیزات و یا کل وسیله نقلیه ریلی مورداستفاده قرارگرفته، و برای برآورد ریسک مخاطرات سایبری در ناوگان قطارها و زیرساخت‌های شبکه ریلی استفاده گردد.

با در نظر گرفتن جمیع جهات فوق می‌توان چنین اذعان نمود که برای مواجهه با حوادث مشابه، لازم است درخت حمله و درخت خطا به‌صورت یکپارچه برای تجزیه‌وتحلیل مخاطرات و شناسایی تهدیدها در شبکه ریلی مورداستفاده قرار گیرد که این خود ناظر بر مهندسی ایمنی و امنیت سایبری به‌صورت مشترک است که برای موردمطالعه در تحقیق حاضر به‌صورت تصویر شماره سه نشان داده می‌شود.



تصویر شماره ۳) یکپارچگی درخت حمله و درخت خطا برای ارتقای امنیت سایبری و ایمنی شبکه ریلی در مطالعه موردی راه‌آهن منطقه‌ای ایتالیا

درخت حمله به‌عنوان یک ابزار تحلیلی می‌تواند به‌منظور دستیابی به مسیر «خطا – حمله» مورداستفاده قرار گیرد. از طرفی تکنیک‌های تحلیلی لازم است در یک رویکرد یکپارچه و تشکیل‌شده از موارد ایمنی و امنیتی برای توسعه دستورالعمل‌ها و استانداردها مورداستفاده قرار گیرد. در این مطالعه نتایج تجزیه‌وتحلیل RAMS در تصویر شماره ۴ ترسیم شده است. در این شکل قسمت a از دست رفتن کارآمدی شبکه ریلی در اثر تهاجمات سایبری متناسب با کاهش ظرفیت شبکه را نشان می‌دهد در قسمت b از تصویر شماره ۴ ظرفیت ازدست‌رفته شبکه ریلی در اثر تهاجم سایبری به تصویر کشیده شده است.



تصویر شماره ۴) میزان کارایی و ظرفیت ازدست‌رفته شبکه ریلی در اثر حملات سایبری

نتیجه‌گیری

در این تحقیق پس از بررسی ابعاد مختلف ایمنی و امنیت در صنعت حمل‌ونقل ریلی، ضرورت همراستائی توأمان آن‌ها مورد بررسی قرار گرفت. در این پژوهش همچنین به‌عنوان یک مطالعه موردی سانحه حمله سایبری به‌قطار منطقه‌ای ایتالیا بررسی گردید. چنانکه در قسمت یافته‌های پژوهش بحث گردید، گراف حمله سایبری به قطار با نقایص ایمنی عملیات، یک فراگرد سازگار است. در مورد کاوی این تحقیق هرچند هر یک از بخش‌های زیرسیستم سامانه ضد لغزش چرخ ها (WSP) با الزامات و استانداردهای مدون در صنعت حمل‌ونقل ریلی انطباق دارند ولی بااین‌حال فقدان یک رویکرد یکپارچه برای ایمنی و امنیت سایبری، می‌تواند به نتایج غافلگیرکننده‌ای در شبکه ریلی منتهی گردد. از طرفی هنگامی‌که سخن از سیستم‌های عملیاتی در صنعت حمل‌ونقل ریلی می‌شود، امنیت سایبری علاوه بر موارد مرتبط با آسیب‌پذیری‌های نرم‌افزارهای کاربردی سیر و حرکت قطار، سامانه‌های خدمات مسافری و سیستم‌های اطلاعاتی ریلی را نیز در برمی‌گیرد زیرا نقاط ضعف، آسیب‌پذیری‌های نرم‌افزاری و تهدیدهای ناشی از

نشت سیگنال‌های الکترومغناطیسی می‌تواند به‌صورت مستقل یا وابسته هر یک از تجهیزات و یا مجموعه‌ای از اجزاء مرتبط در ترافیک سیر و حرکت قطارها را از طریق کدهای مخرب یا بدافزارهای نصب شده؛ به‌صورت حملات منفرد و یا ترکیبی از تکنیک‌های نفوذگری متأثر سازد. ازاین‌رو به‌عنوان یک نوآوری در این تحقیق، در بررسی سانحه نفوذ راه‌آهن منطقه‌ای ایتالیا؛ ریسک‌های ترکیبی (امنیتی و ایمنی) بر اساس درخت حمله برای سیستم‌ها و زیرسیستم‌های «فیزیکی –سایبری» شبکه ریلی آنالیز شدند. استفاده از این تکنیک برای تجزیه‌وتحلیل مدیریت اختلال و کنترل قطارها می‌تواند ابعاد متنوع و جدیدی را اضافه و مورد بررسی قرار دهد و از این راه بینش مناسبی را برای ارزیابی ریسک‌های امنیتی با لحاظ مهندسی ایمنی عملیات در شبکه حمل‌ونقل ریلی فراهم آورد.

فهرست منابع

Ambrose, J.; Ragel, R.; Jayasinghe, D.;Li, T.; Parameswaran, S. (2018). Side channel attacks in embedded systems: A tale of hostilities and deterrence. 452-459.

Bar-El, H.; Choukri, H.; Naccache, D.; Tunstall, L.; Whelan, L. (2016). “The Sorcerer's Apprentice Guide to Fault Attacks”, in Proc. of IEEE, vol. 94, issue 2, pp:370-382.

Barna, G. (2022).; Control system of wheel slide protection devices for rail vehicles meeting the requirements of European normative documents -CzasopismoTechniczne, MechanikaZeszyt 7-M/2022.

Ferrag M. A.; Chekkai N.; Nafa M. (2018). - Securing Embedded Systems: Cyberattacks, Countermeasures and Challenges in Securing Cyber-PhysicalSystems - CRC Press.

Lakshminarayana, S.; Teo, Z.; Tan, R.; Yau, D.K.Y.; Arboleya, P. (2019) "On False Data Injection Attacks Against Railway Traction PowerSystems," 2019 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse, 2019, pp. 383-394.

Karray, K.; Danger, J; Guilley, S; El Aabid, M. A. (2021). Attack tree construction: an application to the connected vehicle - Cyber-physical securityeducation workshop - Paris, France — July 17-19, 2020 or Cyber-Physical Systems Security - Springer .

Kumar, R.; Stoelinga, M. (2020). Quantitative Security and Safety Analysis with Attack-Fault Trees. 10.1109/HASE.2020.12.

Rekik, M.; Gransart, C.; Berbineau, M. (2021). - Cyber-Physical Security Risk Assessment for Train Control and Monitoring Systems. SSV, 1stInternational Workshop on System Security and Vulnerability, IEEE CNS Conference on Communications and Network Security, May 2021.

Pekin, China. SSV 2021, 1st International Workshop on System Security and Vulnerability, IEEE CNS Conference on Communications andNetwork Security, 9p, 2021.

Rekik, M.; Gransart, C.; Berbineau, M. (2020) - Cyber-physical Threats and Vulnerabilities Analysis for Train Control and Monitoring Systems.

IEEEISNCC 2019, International Symposium on Networks, Computers and Communications, Jun 2019, Rome, Italy.

IEEE ISNCC 2021,International Symposium on Networks, Computers and Communications, 6p, 2021.

Oka, D.; Matsuki, T. (2017). A security assessment study and trial of Tricore-powered automotive ECU.

Oka, D., Langenhop, L., Marie-Louise, M. &Waguri, N. &Matsuki, T. (2019). Investigation of How to Exploit Software Vulnerabilities on anAutomotive Microcontroller and Corresponding Security Measures.

Papp, D.; Ma, Z.; Buttyan, L. (2018) - Embedded Systems Security: Threats, Vulnerabilities, and Attack Taxonomy - 2015 Thirteenth AnnualConference on Privacy, Security and Trust (PST)

Ponsard, C.; Massonet; P., Dallons; G. 2022- Co-engineering Security and Safety Requirements for Cyber-Physical Systems - The European ResearchConsortium for Informatics and Mathematics ERCIM News 106, Special theme: Cybersecurity.

Schneier, B. - Attack Trees - Dr. Dobb's Journal, December 2009 - https://www.schneier.com/academic/archives/2009/12/attack_trees.html

Shoukry, Y.; Paul Martin, P.; Paulo Tabuada, P. (2019). Srivastava, M - Non-invasive Spoofing Attacks for Anti-lock Braking Systems – InternationalWorkshop on Cryptographic Hardware and Embedded Systems, pp. 55-72.

Shukla, S. (2019). - Embedded Security for Vehicles, ECU Hacking - Uppsala Universitet - Department of Information Technology.

Talebi, S. (2017). A Security Evaluation and Internal Penetration Testing Of the CAN-bus - Chalmers University of Technology Department ofComputer Science and Engineering - Göteborg, Sweden, October 2017.

Yampolskiy, M.; Horvath, P.; Koutsoukos, X.D.; Xue, Y.; Sztipanovits, J. (2017)- Taxonomy for description of cross-domain attacks on CPS –HiCoNS'13 Proceedings of the 2nd ACM international conference on High confidence networked systems

Zalewski, J.; Buckley, I.A.; Czejdo, B.; Drager, S.; Kornecki, A.J. (2019). Subramanian, N. A Framework for Measuring Security as a System Property.