گزارش آسیب پذیری

Security Vulnerability Report

CVE-2018-4833

سطح مخاطره : زیاد

محصول تحت تأثیر: Scalance X زینمس و ...

نسخه سند: ۲,۱,۰

تاریخ انتشارعمومی سند: ۹۷/۴/۱۸

در این گزارش می خوانیم:

بررسی اجمالی آسیب‌پذیری سوئیچ‌های صنعتی زیمنس
سوء برداشتی در بین برخی مدیران صنایع و زیرساخت‌های حیاتی
معیارهای گزینش دوره‌های پیشرفته امنیت کنترل و اتوماسیون صنعتی
معرفی مجموعه فیلم حوادث و حملات سایبر-فیزیکی به سامانه‌های صنعتی

@MohammadMehdiAhmadian
www.mmAhmadian.ir
@mmAhmadian

تهیه گزارش : محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

فهرست عناوین

صفحه

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

۱. مقدمه

سامانه‌های کنترل صنعتی که در صنعت و زیرساخت‌های حیاتی کشورها مورداستفاده قرار دارند، اغلب توسط شرکت‌های محدود و انحصاری تولید می‌گردند. این سامانه‌ها درگذشته به‌صورت جدا از سایر سامانه‌های دیگر به کار گرفته می‌شدند و این امر روشی در امن سازی این سامانه‌ها قلمداد می‌گردید. اتکا فراوان به این ممیزه، تولیدکنندگان و مصرف‌کنندگان این سامانه‌ها را از پرداختن به سایر لایه‌های امنیتی غافل کرده بود. استفاده از معماری و پروتکل‌های غیر امن و واسطهای غیراستاندارد را می‌توان از نتایج این رویکرد دانست [۱].به دلیل نیازمندی‌های جدید و توسعه فناوری امروزه این قبیل سامانه‌های صنعتی، به‌تدریج با انواع جدیدتر جایگزین و یا به‌روزرسانی می‌گردند. در سامانه‌های جدید از پروتکل‌ها و نقاط دسترسی ارتباطی مشترک در شبکه‌ها استفاده می‌گردد [۱]. به علت تفاوت‌های متعدد میان امنیت در فضای فناوری اطلاعات (IT) و امنیت در فضای فناوری عملیاتی (OT[1]) لزوماً نمی‌توان راهکارهای عمومی حوزه‌ی سایبری را به حوزه‌ی سایبر-فیزیکی منتقل کرد[۱].

در غالب صنایع و زیرساخت‌های حیاتی شاهد به‌کارگیری انواع تجهیزات ارتباطی شبکه نظیر سوییچ‌های لایه دو و لایه سه، هاب‌ها، بریج‌ها، تقویت‌کننده‌های ارتباطی کارت‌های شبکه و حتی مسیریاب‌ها هستیم. به دلیل اینکه این تجهیزات به شکل کاملاً فعال در شبکه‌ها به کار گرفته می‌شوند در صورت حمله یا گسترش آلودگی سایبری به این تجهیزات قطعاً شاهد اختلال در صنایع و زیرساخت‌های حیاتی کشور خواهیم بود. ازاین‌رو توجه به امنیت سایبر-فیزیکی این تجهیزات باید در دستور کار مدیران صنعت و حراست، مسئولان و سرپرستان، کارشناسان فناوری اطلاعات و شبکه‌های کنترل صنعتی(واحدهای بهره بردار و نگه‌داری) قرار گیرد. در این سند در بخش دوم به بررسی اجمالی آسیب‌پذیری سوئیچ‌های صنعتی زیمنس (CVE-2018-4833) می‌پردازیم، در بخش سوم در راستای پاسخ به سوال یکی از مخاطبان گرامی به گزینش دوره‌های پیشرفته امنیت کنترل و اتوماسیون صنعتی درکشور خواهیم پرداخت .در بخش چهارم مجموعه فیلم حوادث و حملات سایبر-فیزیکی به سامانه‌های کنترل صنعتی را معرفی خواهیم کرد و نهایتا در بخش پنجم به سوء برداشتی که در بین برخی مدیران صنایع و زیرساخت‌های حیاتی وجود دارد خواهیم پرداخت.

[1] Operational Technology

۲. گزارش بررسی اجمالی آسیب‌پذیری سوئیچ‌های صنعتی زیمنس (CVE-2018-4833)

۲-۱- مشخصات آسیب‌پذیری

جدول ۱: مشخصات آسیب‌پذیری اخیر سوئیچ‌های صنعتی زیمنس

شناسه آسیب‌پذیری:	CVE-2018-4833
محصول تحت تأثیر:	• Siemens SCALANCE X • Siemens SIMATIC • Siemens RUGGEDCOM WiMAX • Siemens RFID
تاریخ گزارش آسیب‌پذیری	۲۰۱۸۰۶۱۲
نوع حمله و آسیب‌پذیری:	افشاء اطلاعات و بالابردن سطح دسترسی در اثر اعتبارسنجی ناصحیح ورودی‌ها (آسیب پذیری سرریز هیپ)
نقطه ورودی[1]	داخل شبکه
سطح مخاطره:	زیاد
نمره CVSS:	۷,۵ AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

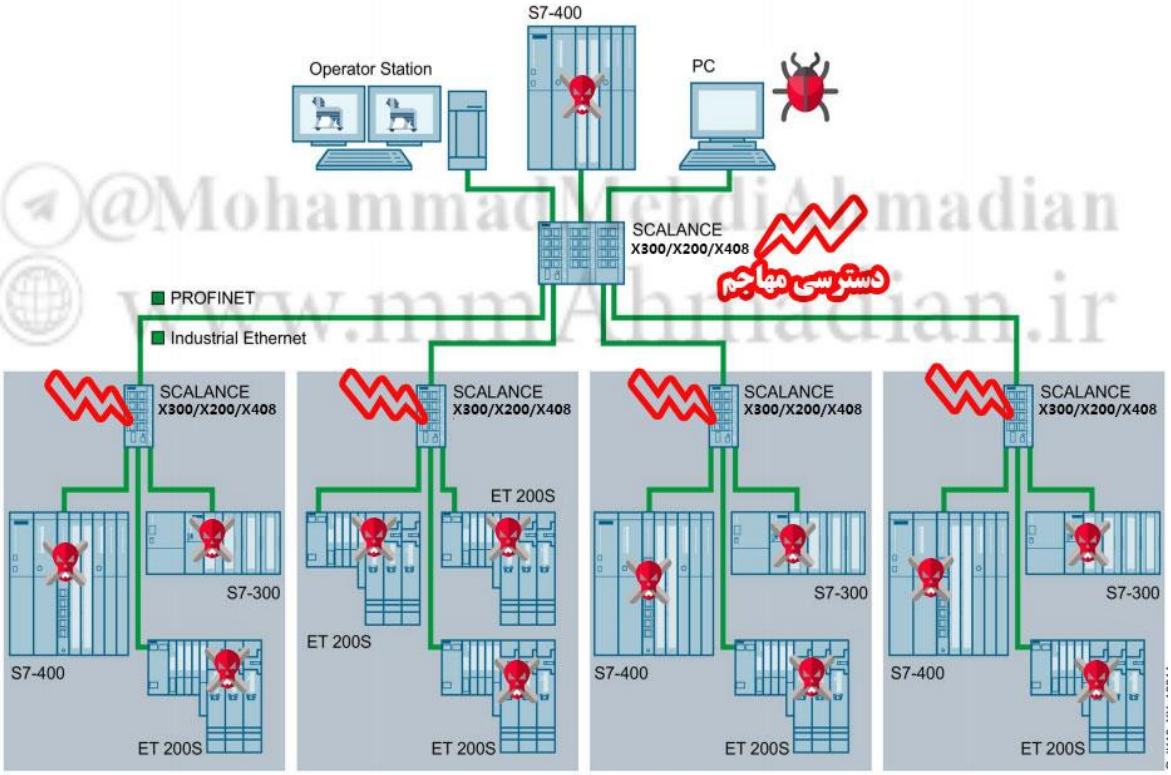
* شایان ذکر است برای سوییچ‌های SCALANCE X آسیب‌پذیری CVE-2018-4842 نیز اخیرا گزارش شده است.

۲-۲- گزاش فنی آسیب‌پذیری

سوییچ‌های صنعتی SCALANCE X جهت اتصال تجهیزات کنترل صنعتی نظیر PLCها و HMIها مورد استفاده قرار می‌گیرند.

[1] Entry Point

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



این حمله در محدوده میزبان‌های یک شبکه (لایه دوم OSI) با ارسال بسته دستکاری شده پاسخ DHCP به سیستمی انجام می گیرد که بسته درخواست DHCP را ارسال کرده است و در صورت موفقیت در بهرداری به مهاجم امکان اجرای کدهای دلخواه را می دهد.

۲-۳- محصولات تحت تأثیر

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

نسخه‌های ذیل از تجهیزات زینمس در برابر آسیب‌پذیری معرفی‌شده آسیب‌پذیرند:

- Siemens SIMATIC RF182C 0
- Siemens SCALANCE X414 0
- Siemens Scalance X408 0
- Siemens Scalance X-300 0
- Siemens SCALANCE X-200 IRT 0
- Siemens SCALANCE X-200 0
- Siemens RUGGEDCOM WiMAX 4.5
- Siemens RUGGEDCOM WiMAX 4.4
- Siemens RFID 181-EIP 0

تجهیزات ذیل آسیب پذیر نیستند:

- Siemens SCALANCE X-200 IRT 5.4.1
- Siemens SCALANCE X-200 5.2.3

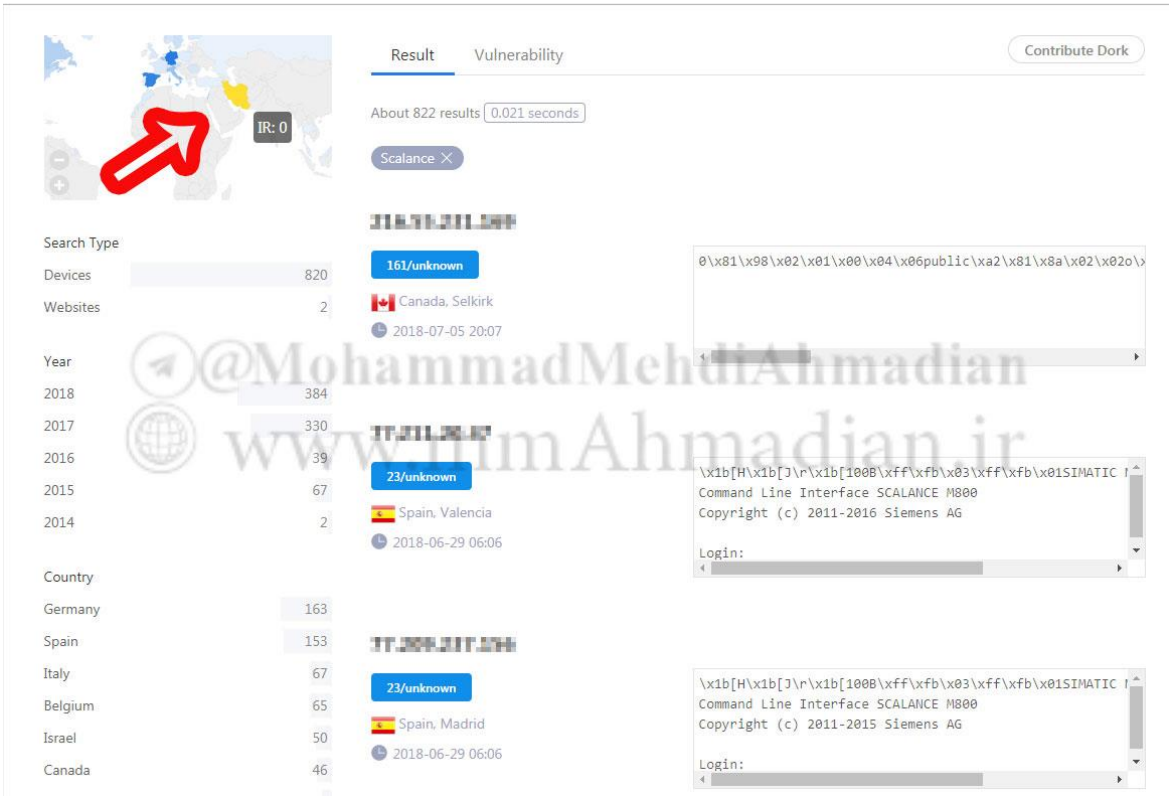
- اطلاعیه رسمی شرکت زیمنس[۲] محصولات تحت تأثیر را به شکل ذیل دسته‌بندی نموده است:

Affected Product and Versions
RFID 181-EIP: All versions
RUGGEDCOM WiMAX: V4.4 and V4.5
SCALANCE X-200: All versions < V5.2.3
SCALANCE X-200 IRT: All versions < V5.4.1
SCALANCE X-204RNA: All versions
SCALANCE X-300: All versions
SCALANCE X408: All versions
SCALANCE X414: All versions
SIMATIC RF182C: All versions

۲-۴- کدهای بهره‌جویی[1] منتشرشده

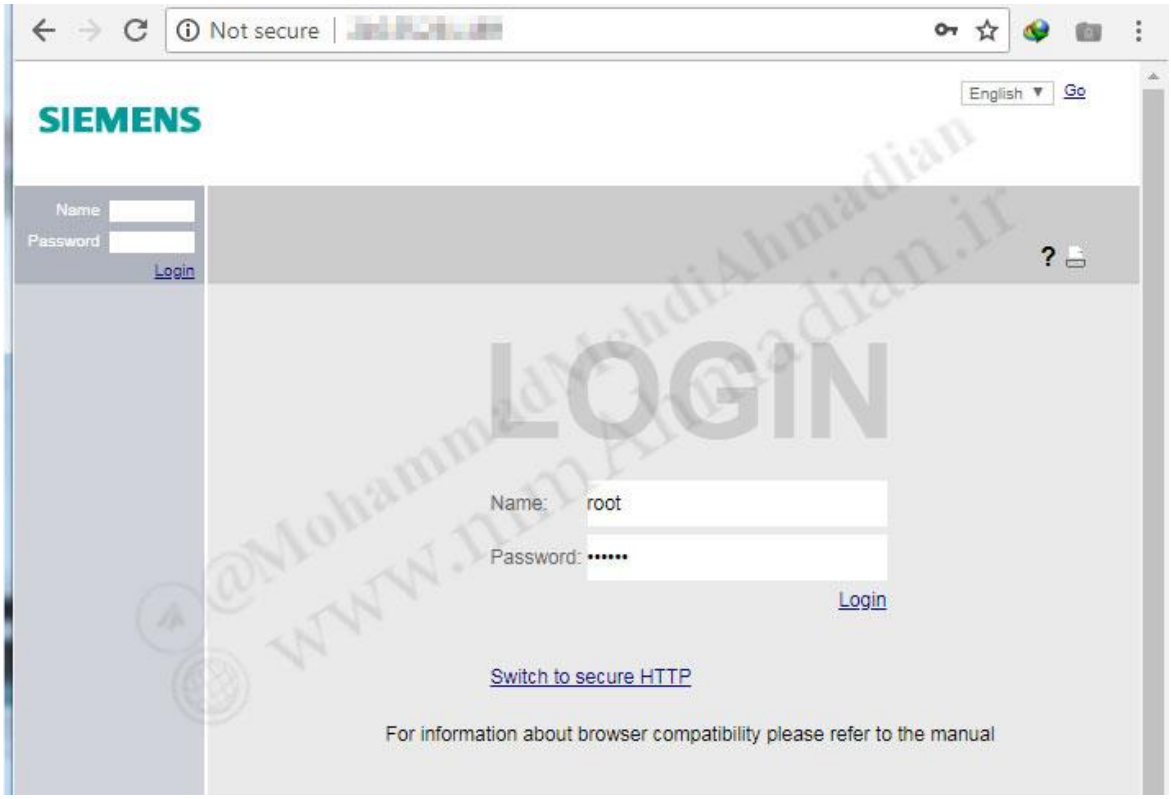
تازمان انتشار این گزارش کد بهره‌جویی عمومی برای این آسیب پذیری منتشر نشده است.

طبق بررسی‌های اندک ما، در زمان انتشار این گزارش هیچ تجهیز Scalance X (با بنردستکاری نشده) در داخل کشور به اینترنت متصل نبود.

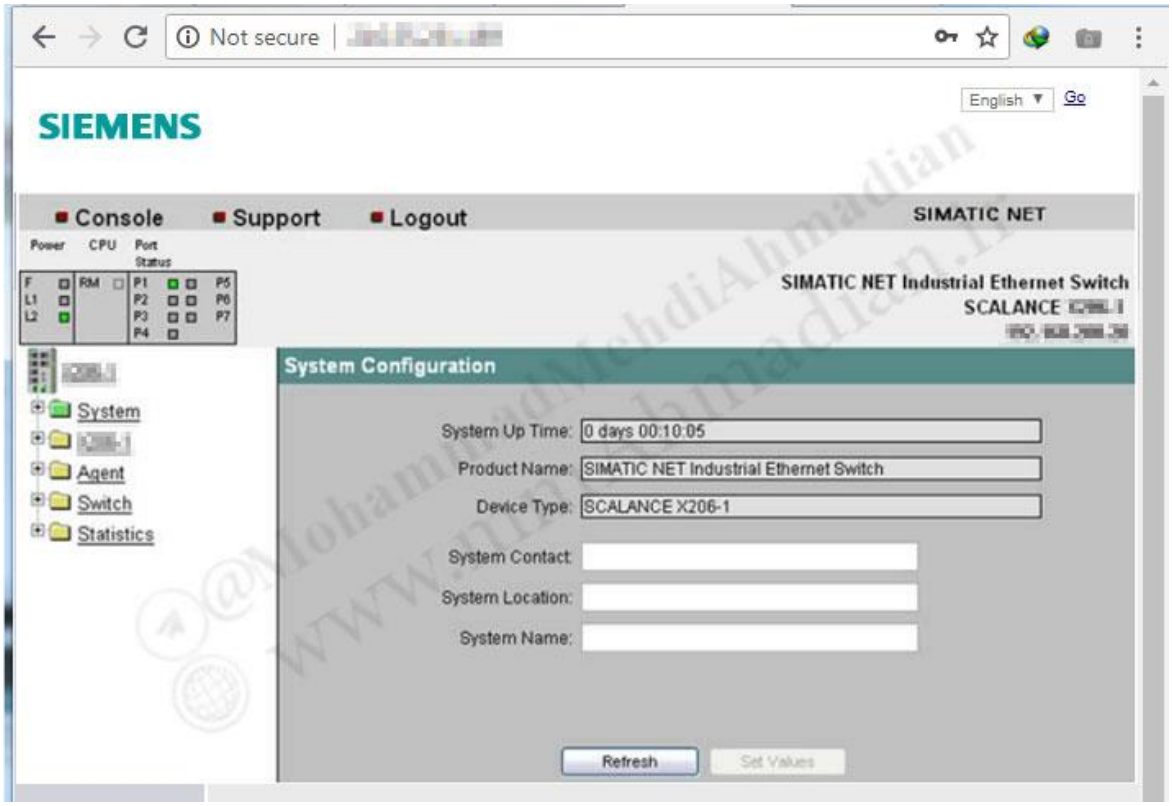


[1] Exploit

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



دسترسی به سوییچ قربانی بعد از بهره برداری موفق:



۲-۵- توصیه‌ها و راه‌حل‌های امنیتی

- شرکت زیمنس این آسیب‌پذیری‌ها را تائید کرده است و برای آن وصله‌های امنیتی ارائه کرده است؛ لذا به کلیه مدیران شبکه‌های کنترل صنعتی که محصولات تحت تأثیر را در اختیاردارند و بتوانند نسخه به‌روزرسانی را دریافت نمایند، توصیه می‌شود در اسرع وقت وصله موردنظر را نصب نمایند (در مورد نصب وصله‌های حتماً «ضمیمه ب» این سند را مطالعه فرمایید).
  - لینک به‌روزرسانی‌های SCALANCE X-200 برای ارتقاء به v5.2.3

https://support.industry.siemens.com/cs/cn/en/view/109758142

  - لینک به‌روزرسانی‌های SCALANCE X-200 IRT برای ارتقاء به v5.4.1

https://support.industry.siemens.com/cs/de/en/view/109758144

در صورت مشکل در ارتقاء تجهیزات جهت مدیریت مخاطرات، به شکل موقت می‌توانید از اختصاص IPهای ایستا[1] جهت برقراری ارتباط استفاده نمایید.

توصیه‌های عمومی:

- به مدیران شبکه‌های کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که دسترسی به محصولات تحت تأثیر و سامانه مدیریت و نظارت[2] بر آن را محدود کنند؛ این محدودسازی می‌تواند از طریق دیواره‌های آتش کنترل صنعتی (برای شبکه‌های غیرصنعتی از دیواره‌های آتش عمومی)، لیست سفید، DMZ و غیره انجام شود. در صورت عدم به‌روزرسانی محصولات تحت تأثیر حتماً دسترسی آن‌ها به شبکه عمومی (به‌ویژه اینترنت یا VPN های پیمانکاران) را قطع نمایید.
  - تا جایی که امکان دارد باید نمای حمله[3] مهاجمین جهت دسترسی به دارایی‌های سایبر-فیزیکی(تجهیزات و سیستم‌ها) شما به حداقل برسد؛ اتصال این تجهیزات را به شبکه‌های غیرامن به حداقل برسانید.
- به مدیران شبکه‌های کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که به کمک راهکارهای کنترل دسترسی تنها به کاربران مجاز امکان دسترسی به شبکه را بدهند(ترجیحا این دسترسی مبتنی بر نقش اعمال شود).

---

[1] Static

[2] Monitoring

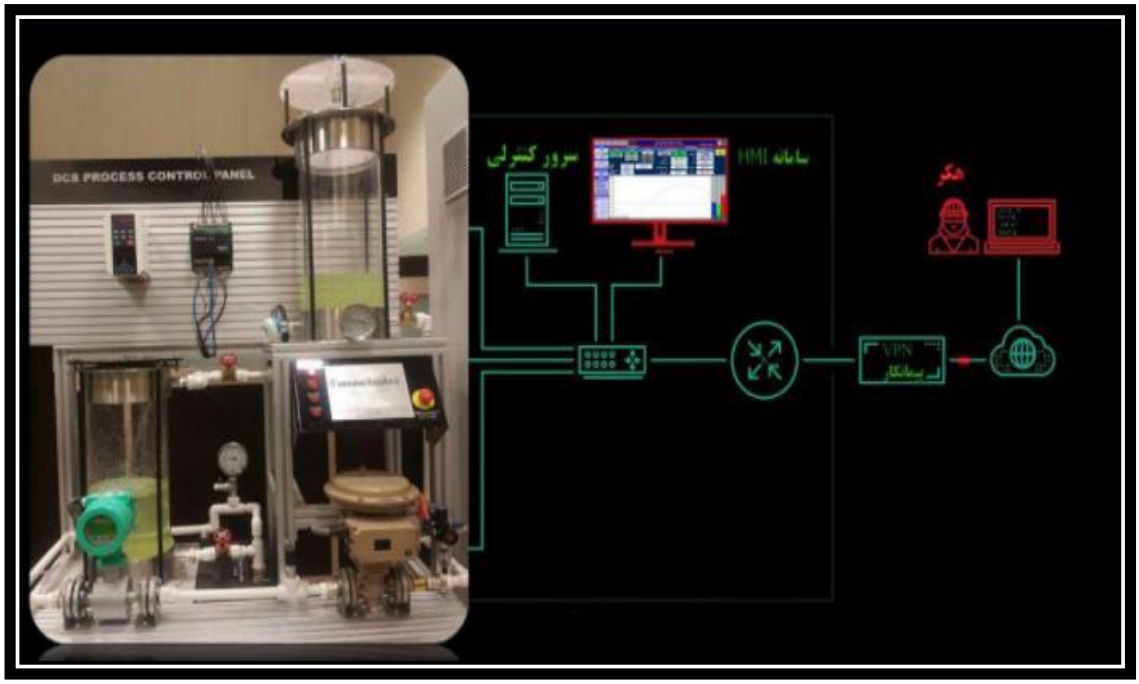
[3] Attack Surface

- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که در صورت اتصال شبکه‌ی کنترل صنعتی به شبکه‌های دیگر حتماً از دیواره آتش کنترل صنعتی یا یک‌سوساز[1] کنترل صنعتی استفاده نمایند؛ در صورت نیاز ما می‌توانیم در ارائه محصولات کنترل صنعتی به شما مشاوره دهیم به‌عنوان مثال تجربه‌های موفقی در نصب تجهیزات یک‌سوساز کنترل صنعتی در صنایع کشور داشته‌ایم.
- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک محصولاتی مانند SIEM کنترل صنعتی و سامانه تشخیص نفوذ صنعتی (IDS) به شکل مستمر کلیه تجهیزات سامانه و ترافیک عبوری را پایش نمایند.
- به مدیران شبکه‌های کنترل صنعتی دارای محصولات تحت تأثیر توصیه می‌شود که در صورت محدودیت در شبکه یا پلنت صنعتی و جهت اتخاذ رویکرد کاهش مخاطره، سامانه‌های تحت تأثیر را در یک زیرشبکه[2] ایزوله یا محدوده‌ی امن قرار دهند.
- درصورتی‌که در شبکه یا واحد صنعتی شما نیاز به اتصال از راه دور دارید حتماً از راهکارهای اتصال راه دور امن نظیر VPN استفاده کنید؛ توجه شود که خود راهکار VPN داری آسیب‌پذیری نباشد و پاشنه آشیل نباشد؛ در شکل ۱ نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر را مشاهده می‌کنید ما در قالب دوره آموزشی پیشرفته می‌توانیم این تهدیدات و راهکارهای امن سازی آن‌ها را به شما ارائه نماییم.

[1] Data Diode

[2] Subnet

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



شکل ۱: نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر

- همانند غالب آسیب‌پذیری‌ها و حملات به سامانه‌های فناوری اطلاعات و کنترل صنعتی و زیرساخت‌های حساس (حساس، حیاتی و مهم) پیاده‌سازی دفاع در عمق و سایر راهبردهای امنیتی نظیر تنوع در دفاع، موضع ایمنی در برابر خرابی، نقطه وارسی و غیره به شما توصیه می‌شود.

* درصورتی‌که هر یک از موارد بالا برای شما مبهم است، می‌توانیم با شما و صنعت شما جلسه‌ی مشترک گذاشته و راهکارهای امنیتی خود را، همراه با مجموعه خدمات و محصولات امنیتی، به شما معرفی نماییم (به‌ضمیمه د، جهت مشاهده خدمات و راه ارتباطی مراجعه نمایید.)

۳. معیارهای گزینش دوره‌های پیشرفته امنیت کنترل و اتوماسیون صنعتی در کشور

اخیراً جناب کاظم زاده،یکی از مخاطبین گرامی سمینارها، در این پست پرسش ذیل را مطرح نمودند:

بخش‌هایی از این نظر که با * مشخص شده، حذف شده است

سلام جناب دکتر احمدیان

از مقالات آموزشی شما بسیار ممنونم. بنده و همکاران در سمینار اخیر شما حضور داشتیم و استفاده فراوان بردیم. سوالی در مورد دوره آموزشی امنیت کنترل صنعتی sans داشتم، در پروپوزال دوره آموزشی شما سرفصل های sans پوشش داده نشده است، می خواستم بدانم چرا؟ در دوره های دیگر موجود در اینترنت نظیر دوره های ***** ***** ***** ***** ***** ***** ***** ***** این سرفصل ها پوشش داده شده است. آیا شما نیز این دوره ها را ارائه می کنید؟ شما کدام دوره را توصیه می کنید؟

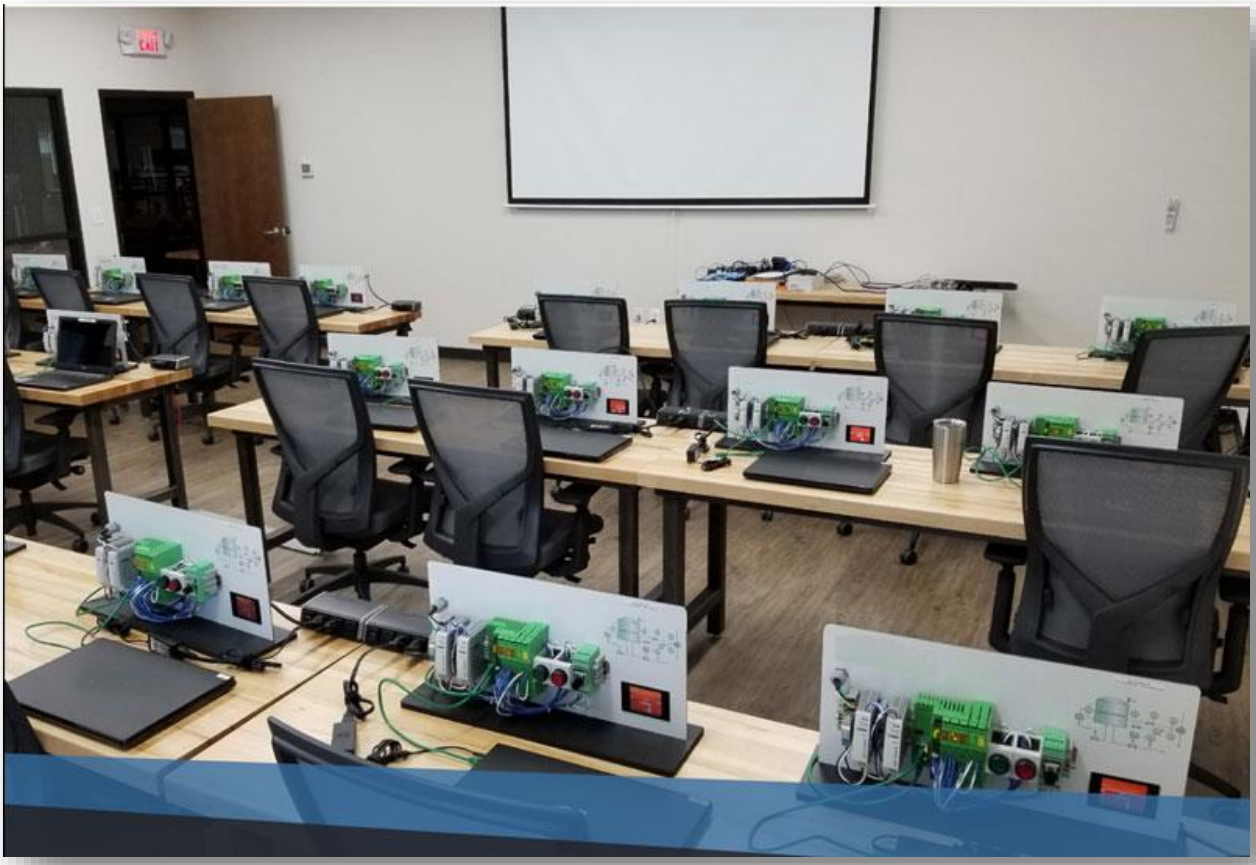
در مورد این سؤال به‌تفصیل پاسخ می‌دهم چون این مسئله چند ماهی است در چندین جلسه و محفل دیگر نیز مطرح‌شده است و خالی از لطف نیست که یک‌بار به شکل مفصل به آن پاسخ دهم.نخست باید به این نکته اشاره‌کنم که دوره‌های امنیت کنترل صنعتی غالباً در دو سطح برگزار می‌شوند؛ سطح نخست عمومی (دوره‌های مقدماتی) است که این دوره غالباً به شکل کاملاً نظری برگزار می‌شود، سطح دوم دوره‌های پیشرفته است که این دوره‌های باید به شکل نظری و عملی برگزار شوند.

آنچه در ادامه مطرح می‌کنم معیارها و نیازمندی‌هایی است که یک دوره پیشرفته (مانند دوره‌های مشابه SANS) باید داشته باشد و شما چنانچه نیاز به برگزاری این دوره‌های تخصصی دارید فارغ از اینکه چه مدرس یا مدرسینی آن را ارائه می نمایند شرایط ذیل را برای انتخاب دوره و مدرس بررسی نمایید و در نظر بگیرید.

۱. **نیاز به تخصص چندساله امنیتی و کنترلی:** در سایر حوزه‌های امنیت اطلاعات داشتن مدارک معتبر بین‌المللی یا دانشگاهی می‌تواند شاخصی برای سنجش مهارت مدرس (مدرسین) باشد اما در این حوزه متأسفانه مدارک بین‌المللی چندان فراگیر نیستند و چند سالی است که دوره‌های بین‌المللی توسط SCADAHacker،DHS،SANS و غیره برگزار می‌شود. لذا معیار دقیق علمی برای سنجش مهارت علمی مدرسین و مراکز برگزار کننده در داخل کشور وجود ندارد اما آنچه کاملاً مشهود است و صنایع و سازمان‌ها باید در چنین شرایطی در انتخاب دوره و مدرس به آن توجه نمایند این است که حداقل مدرسین آن‌ها ضمن داشتن رزومه قوی در پژوهش و تدریس، سابقه درخشانی در پروژه‌های ارزیابی و امن سازی داشته باشند و تجربه عملیاتی از کار در صنایع و زیرساخت‌های حیاتی یا آزمایشگاه‌های مرتبط داشته باشند (این تجربه حداقل ۵ سال زمان برای کار تخصصی در این حوزه است) وگرنه حاصل برگزاری دوره صرفاً ارائه محفوظاتی خواهد بود که با جست‌وجوی اندک در کتاب‌های این حوزه و مقالات عمومی قابل‌دسترسی است. قابل‌توجه است که در حوزه امنیت کنترل صنعتی بالغبر ۱۲ کتاب رسمی مرجع کاربردی (انگلیسی) و بالغبر ۶۰۰ مقاله معتبر (انگلیسی) قابل‌دسترس وجود دارد که طبیعتاً گروه مدرسین باید حداقل بر ۵۰٪ این منابع اشراف کامل داشته باشند که خود این مسئله نیاز به زمانی بالغبر ۳ سال مطالعه تخصصی و کاربردی دارد.

۲. **نیاز به تجهیزات آزمایشگاهی:** برگزاری دوره‌های تخصصی امنیت اتوماسیون صنعتی نیاز به ارائه کارگاهی همراه با اجرای زنده حملات و راهکاری‌های امنیتی بر روی بسترهای آزمایشگاهی (Test Bed) دارد که مدرس(مدرسین) یا موسسه برگزارکننده این دوره‌ها باید توان تهیه این بسترهای آزمایشگاهی را داشته باشد و در کنار آن در سطحی از دانش و مهارت باشند که بتوانند حملات و راهکارهای امنیتی را بر روی سامانه‌های کنترل صنعتی پیاده‌سازی نمایند و دوره به سمت ارائه تنها نظری مطالب پیش نرود تا دوره اثربخش باشد. ذیلاً نمونه محل برگزاری یکی از این دوره‌های تخصصی را مشاهده می‌کنیم(به پلنت های کوچک صنعتی روی میزهای آموزش دقت بفرمایید) :

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



به‌عنوان‌مثال یکی مصادیق بلوغ یک دوره‌این است که مدرسین در عمل مشخص کنند کدام‌یک از حملات لایه فناوری اطلاعات در لایه تجهیزات کنترل محلی تا سطح فیلد (دیجیتال و آنالوگ) قابل انجام است و صرفاً انبوهی از حملات فناوری اطلاعات که حتی بسیاری از آن‌ها در لایه‌های صنعتی امکان اجرا ندارند را به مخاطبین بی‌اطلاع منتقل نکنند.

۳. **گروه مدرسین با تخصص‌های امنیت، شبکه، کنترل و ابزار دقیق:** با توجه به بین‌رشته‌ای بودن امنیت کنترل و اتوماسیون صنعتی (گرایش‌های شبکه، امنیت اطلاعات، مهندسی نرم‌افزار از مهندسی کامپیوتر و گرایش‌های کنترل، ابزار دقیق و مخابرات از رشته مهندسی برق) توقع می‌رود گروه مدرسین دوره دارای تحصیلات و تخصص‌های متفاوت در هر یک از این گرایش‌ها باشند؛ طبیعتاً این کار در کشور ما از عهده یک نفر خارج است (به دلیل سابقه کم افراد متخصص این حوزه) و نیاز به چند مدرس برای ارائه دوره است. تاکید می کنم سابقه‌ی تدریس صرف در حوزه امنیت اطلاعات و شبکه یا در حوزه‌های کنترل و ابزاردقیق نمی‌تواند به معنای صلاحیت در تدریس دوره‌های امنیت سامانه‌های کنترل صنعتی باشد.

۴. **هزینه بالای دوره‌های تخصصی:** تاکنون چندین بار در یک سال گذشته از ما خواسته‌شده است که دوره‌های منطبق با SANS را ارائه نماییم و برای آن سیلابس معرفی نمایم؛ همیشه به مدیران محترم صنایع گفته‌ایم که صرف ارائه سیلابس کپی شده از دوره‌های SANS و مؤسسات دیگر امر منطقی نیست، چراکه این سیلابس در وب‌سایت‌های این مؤسسات خیلی شفاف و کامل معرفی‌شده است (نمونه۱) مهم توانمندی در ارائه محتوا و تضمین کیفیت دوره است. برگزاری دوره‌های پیشرفته امنیت کنترل صنعتی در این سطح باید برای مدرسین مقرون‌به‌صرفه باشد چراکه به‌عنوان‌مثال خود دوره‌های SANS ICS 410و 515 به‌طور میانگین برای هر نفر تقریباً ۵هزاردلار هزینه مطالبه می‌نمایند. بنابراین اگر قرار باشد ما دوره‌ای باکیفیت حداقل ۶۰٪ دوره‌های مشابه هم ارائه نماییم باید هزینه‌ای متناسب با این کیفیت از صنایع دریافت نماییم که متأسفانه بسیاری از صنایع کشور در حال حاضر به چنین بلوغی نرسیده‌اند. لذا برگزاری این دوره‌ها با هزینه‌های بسیار پایین نمی‌تواند نشان از تطبیق با دوره با دوره‌های بین‌المللی باشد و مدیران محترم صنایع باید قبل از برگزاری دوره، این مسئله را در نظر داشته باشند.

۵. **چالش عدم رعایت کپی‌رایت در ایران و طرح سیلابس و جزئیات:** این‌که ما تاکنون سرفصل جزئی دوره‌های مقدماتی و پیشرفته را به شکل عمومی منتشر نکرده‌ایم به دو دلیل است: نخست اینکه اگر قرار به کپی از دوره‌های خارجی باشد که نیاز به ارائه سرفصل نیست چراکه این سیلابس در وب‌سایت‌های این مؤسسات خیلی شفاف و کامل معرفی‌شده است (نمونه۲) ، دوم اینکه جزئیات دوره‌های ما با توجه به نیاز کشور و شرایط صنایع کشور (بر اساس تجربه بالغبر ۴ سال کار با صنایع و آزمایشگاه‌های مرتبط) طراحی‌شده است و به دلیل عدم رعایت قوانین کپی رایت در کشور هرگز قصد انتشار عمومی آن‌ها را نداریم.

۶. **تجربه‌های موفق برگزاری:** یکی دیگر از معیارهای سنجش دوره‌های آموزشی، تجربه‌های موفق برگزاری دوره‌ها توسط مدرس (مدرسین) است که می‌توانید با مراجعه به صنعت مربوطه اثربخشی دوره را به شکل ملموس مورد ارزیابی قرار دهید.

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

۴. مجموعه فیلم حوادث و حملات سایبر–فیزیکی به سامانه های کنترل صنعتی

ذیلا به معرفی ویدئوهای مختلف در حوزه حوادث و حمله های سایبر-فیزیکی به سامانه های کنترل صنعتی رامعرفی نمایم (با کلیک بر روی لینک هر عنوان فیلم مربوطه را مشاهده خواهید کرد):

- **فیلم راف لنگنر در مورد استاکس نت و تشخیص آن از طریق صدای سانتریفیوژ(لینک)**
  - 

در این فیلم لاف لنگنر پژوهشگر برجسته حوزه امنیت سامانه های کنترل صنعتی بر اساس فیلم های جدید منتشر شده از سایت های هسته ای کشور به مسئله احتمال تشخیص استاکس نت از طریق نویز شدید ایجاد شده می پردازد. راف به‌صراحت به صدای بلند نویزی اشاره دارد که واضح است که تیم مستقر در سایت هسته‌ای می‌دانست که سرعت چرخش در صفحه‌نمایش آن‌ها دقیق نیست. اخیراً مستندی چند قسمتی در کشور با عنوان آفتاب نهان توسط شبکه مستند تولیدشده که اطلاعات بسیاری از صنایع هسته‌ای کشور را منتشر کرده است که علیرغم اینکه در این فیلم تصاویر مانیتورها و برخی تجهیزات محو شده است اما بازهم حجم زیادی اطلاعات از دارایی‌هایی فیزیکی سایت های اتمی منتشر شده است که ما بارها این مسئله را تذکر داده‌ایم و در کنفرانس PetroICT اخیر نیز یک سخنرانی با همین موضوع و اهمیت اطلاعات میدانی در سایت های صنعتی ارائه کردم .

- **آزمایش و انفجار ناشی از افزایش فشار بخار حاصل از جوشیدن مایع از دنیای فیزیکی تا دنیای سایبری(لینک)**
  - 
در این فیلم در بخش اول شاهد آزمایش انفجار ناشی از افزایش فشار بخار حاصل از جوشیدن مایع (BLEVE[1])هستیم که عمده ترین انفجار مخازن در صنایع مختلف بوده که سبب دو یا چند تکه شدن مخزن مایع در کسری از ثانیه می شود و بسیار خطرناک است. انفجار این مخازن زمانی صورت می گیرد که درجه حرارت مایع داخل مخزن به بالاتر از نقطه جوش خود (در فشار اتمسفر) برسد. در بخش دوم فیلم نمونه واقعی این نوع انفجار را خواهیم دید.

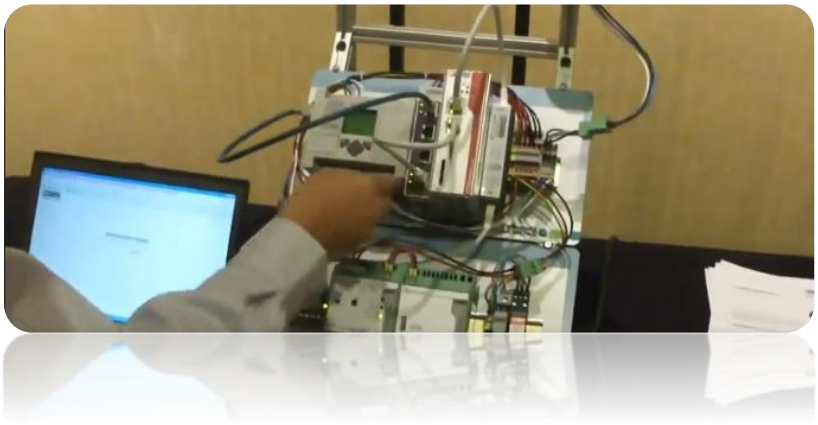
[1] Boiling Liquid Expanding Vapor Explosion

- با توسعه فناوری اطلاعات (IT) و نسل چهارم سامانه های اتوماسیون ، اسکادا و فناوری های عملیاتی (OT)و همگرا شدن آنها شاهد هوشمند شدن بیشتر تجهیزات مختلف تا لایه فیلد (Field)خواهیم بود؛ آنگاه حوداث فیزیکی نظیر انفجارها در صنایع نفت، گاز، پالایش، پتروشیمی، نیروگاه ها، فولاد، مس و غیره کی در برخی موارد تا چند کیلومتر می تواند به محیط اطراف آسیب جبران ناپذیری وارد کند می تواند از بستر کانالهای سایبری و توسط مهاجمین انجام شود؛ به مرور بحث ایمنی (Safety)و امنیت (Security)به همدیگر نزدیک تر می شوند همانطور که بدافزار Triton این مسئله را نشان داد .

- **یک حادثه در مجتمع مس شهربابک (کارخانه ذوب خاتون آباد)(لینک)**
  - به گزارش باشگاه خبرنگاران جوان در این ویدئو به عنوان یک حادثه غیرامنیتی شاهد پاره شدن سیم جرثقیل سقفی در سالن ذوب مس و چپ شدن پاتیل مواد مذاب هستیم. در این حادثه خوشبختانه به کسی آسیب نرسیده است. هرچه فناوری اطلاعات (IT)و نسل چهارم سامانه های اتوماسیون و اسکادا توسعه پیدا کنند و با فناوری های عملیاتی (OT)همگرا شوند شاهد هوشمند شدن بیشتر تجهیزات مختلف تا لایه فیلد (Field)خواهیم بود؛ تصور کنید در آن زمان (که چندان دور هم نخواهد بود) مهاجمین می توانند در صورت ضعف در امنیت صنایع و زیرساخت های حیاتی به راحتی این گونه حوادث فیزیکی را از طریق کانال های سایبری تحقق بخشند؛ مانند اتفاقی که در سال ۲۰۱۴ در صنعت فولاد آلمان افتاد. در حمله سایبری به صنعت فولاد آلمان مهاجمین با تکنیک های مهندسی اجتماعی و فیشینگ بدافزاری را از لایه مالی-تجاری صنعت به لایه کنترل محلی رساندند و با شناخت بسیار زیادی که از صنعت هدف داشتند و این صنعت را در سطح عالی می شناختند(شناخت در سطح فرایندها، دارایی ها، ارتباطات و غیره) تخریب شدید فیزیکی را در این صنعت رقم زدند! مدیران عزیز و سرپرستان گرامی! قبل از اینکه دیر شود و اینترنت اشیاء صنعتی و نسل چهارم اتوماسیون فراگیر شوند به فکر امنیت صنایع و زیرساخت های حیاتی وابسته به اتوماسیون صنعتی باشیم !

- **دموی حمله DoS به PLC** (لینک)
  - در این ویدئو دموی حمله ممانعت از خدمات (DoS)با سناریو بسیار ساده ای را مشاهده می کنیم.

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی



- **دموی حمله دستکاری مقادیر کنترلی ژنراتور (لینک)**
  - در این ویدئو نمونه حمله سایبر-فیزیکی (زیررنظر آزمایشگاه آیداهو) را مشاهده می کنید که بعد از انجام نفوذ به سامانه کنترلی آسیب پذیر کنترل ژنراتور به دست گرفته می شود و منجر به بروز چنین رخدادی می شود. بسیار قابل توجه است که بسیاری از صنایع در برابر چنین حملاتی آسیب پذیر هستند و متولیان صنایع باید هرچه سریعتر به فکر امن سازی سامانه های عملیاتی و فرایندی خود باشند.

- **نمونه یک مسیر از درخت حمله سایبری به سامانه های کنترل صنعتی (لینک)**
  - نمونه صنعت: پلنت نیروگاه برق
  - نکات:
    - اهمیت فاز شناسایی در حملات هدفمند به زیرساخت های حیاتی و سامانه های کنترل صنعتی
    - متاسفانه این مرحله از شناسایی برای مهاجمین در کشور ما تسهیل شده است، چرا که بسیاری از اطلاعات پلنت های صنعتی ما در اینترنت، کانال های فضای مجازی، مقالات و ویدئوهای تبلیغاتی و غیره بدون رعایت اصول امنیتی افشاء می شود!

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

- مهاجمین حرفه ای سازمان دهی شده زمان و هزینه زیادی برای شناسایی و حمله به پلنت هدف اختصاص می دهند.
- بهره گیری از تکنیک های مهندسی اجتماعی اهمیت ویژه ای دارد.

- **یک حادثه یا یک حمله سایبر-فیزیکی، مسئله این است(لینک)**
  - در این ویدئو در کمترین زمان ممکن، یک انفجار مهیب در یک سایت صنعتی به وقوع می‌پیوندد و حجم عظیمی از خاکستر و دود به هوا بر می خیزد، حادثه ای که تلفات جانی و مالی بسیاری را به همراه دارد.گاهی مرز میان حوادث در صنایع و حملات سایبر-فیزیکی به آنها، آنقدر به هم نزدیک می شود و از سویی با فقدان شواهد فورنزیکی در اثر خلاء زیرساخت ایمنی و امنیتی در صنایع روبه رو می شویم که واقعا مسئله تیم ارزیابی این می شود که با یک حادثه رو به رو هستیم یا یک حمله سایبر-فیزیکی! به راستی چقدر به فکر حملات سایبر-فیزیکی ممکن برای صنعت خود بوده ایم و به چه میزان برای کاهش خسارات و تلفات آن برنامه ریزی کرده ایم؟ آیا برای بعد از حملات و حوادث برنامه های ایمنی و امنیتی تدوین کرده ایم و مکانیزم های لازم را اعمال نموده ایم؟

- **فیلم راف لنگنر و دیل پترسون در مورد استاکسنت (لینک)**
  - در این فیلم لاف لنگنر و دیل پترسون از پژوهشگران برجسته حوزه امنیت سامانه های کنترل صنعتی به تحلیل اولیه بر روی استاکسنت می پردازند.

۵. سوء برداشتی در بین برخی مدیران صنایع و زیرساخت‌های حیاتی(اصل کرکهُفس)

در جلسات و محافل مختلف امنیتی زیادی به این موضوع برخورد کرده‌ام که افرادی که آگاهی عمیقی از امنیت سایبری ندارند (مدیران، سرپرستان تا کارشناسان) ، تصور می‌کنند که امنیت یک سامانه باید بسیار متکی باشد به پنهان نگاه‌داشتن ساختار و جزییات طراحی و یا پیاده‌سازی آن و زمانی که اشتباه بودن این تصور و ضعف‌های آن صحبت می‌کنیم و به اصل کرکهُفس(Kerckhoffs's principle)-که در قرن ۱۹ میلادی در حوزه رمزنگاری مطرح شد- اشاره می‌کنیم تصور می‌کنند که چه حرف غریبی می‌گوییم. اگرچه متخصصین حوزه امنیت به این اصل اشراف کامل دارند اما هدف بنده از نوشتن این بخش صرفاً ترویج و آگاهی بخشی در مورد این اصل ساده امنیتی است تا در آینده کمتر شاهد این سوءبرداشت باشیم.

البته اگر بخواهیم اندکی به کالبدشکافی این موضوع بپردازیم به این نکته پی می‌بریم که این تصور اشتباه در این‌گونه افراد -که عموماً تحصیلات دانشگاهی تخصصی در گرایش امنیت اطلاعات ندارند- می‌تواند حاصل سوءبرداشت آن‌ها از راهبرد امنیتی امنیت از طریق ایجاد ابهام (Security through Obscurity strategy) باشد.اگرچه ایجاد ابهام و مبهم کردن غالب سامانه‌ها می‌تواند به تقویت امنیت در آن‌ها کمک کند اما قراردادن این راهبرد، به‌عنوان اصل اساسی امنیتی در طراحی و پیاده‌سازی یک اشتباه قطعی و مسلم است و تهدیدات امنیتی پرخطری را برای سامانه موردنظر رقم خواهد زد.

اگرچه تأکید می‌کنم راهبرد امنیتی امنیت از طریق ایجاد ابهام یکی از راهبردهای اولیه امنیتی است و باید در زیرساخت‌های حیاتی به آن توجه کرد اما نباید آن را مبنای امن سازی قرارداد. در مورد اهمیت این راهبرد به‌کرات صحبت کرده‌ام و مطلب نوشته‌ام؛ به‌عنوان‌مثال در سخنرانی اجلاس PetroICT سال گذشته(لینک به محتوای سخنرانی) در این مورد به‌تفصیل صحبت کردم و در اردیبهشت‌ماه سال جاری نیز ارائه‌ای در این حوزه با موضوع افشاء اطلاعات زیرساخت‌های حیاتی از طریق مستند تلویزیونی آفتاب نهان را منتشر کردم(لینک به محتوای این ارائه).

در ادامه به بیان اصل کرکهُفس (برخی آن را کرهافس نیز تلفظ می‌کنند) که برگرفته از ویکی‌پدیا است می‌پردازم:

اصل کرکهُفس(Kerckhoffs) اصلی مهم درزمینه‌ی سامانه‌های رمزنگاری است که بیان می‌دارد در ارزیابی امنیت این سامانه‌ها همواره باید فرض کرد که نفوذ گران روش‌های به‌کاررفته در سامانه را می‌دانند و با آن آشنایند. بنابراین اصل، امنیت سامانه نباید به پنهانی و محرمانه بودن الگوریتم‌های آن وابسته باشد، بلکه تنها باید به محرمانه بودن کلیدهای رمز متکی باشد.

این اصل به نام آگوست کرکهُفس نام‌گذاری شده است. سامانه‌های رمزنگاری نوین عموماً بر پایه‌ی اصل کرکهُفس بنا می‌شوند. هرچند امروزه استفاده از سامانه‌هایی که محرمانه بودن روش‌ها را

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

اصل قرار می‌دهند همچنان رایج است، اما رمز چنین سامانه‌هایی معمولاً خیلی زود شکسته می‌شود و در دنیای اطلاعات امروزی محرمانه نگاه‌داشتن جزئیات فنی یک سامانه بسیار دشوار است؛ همچنین با پیشرفت روزافزون فناوری‌ها مدت‌زمان لازم برای شکستن رمزها روزبه‌روز کاهش می‌یابد و به علت نامعلوم بودن میزان این پیشرفت‌ها نمی‌توان آن‌ها در طراحی سامانه دخیل کرد؛ ولی می‌توان محرمانه نگاه‌داشتن روش‌ها را به‌عنوان یک سطح امنیتی بیشتر و به‌صورت ترکیبی با اصل کرکهُفس استفاده نمود.او در دو مقاله‌ای که در سال ۱۸۸۳ در مجله علوم نظامی فرانسه[1] چاپ کرد. این مقاله‌ها که با عنوان رمزنگاری نظامی منتشر شدند شامل شش اصل اساسی بودند که اصل دوم آن به‌عنوان یکی از قوانین اساسی در رمزنگاری مدرن مورد تأیید دانشمندان و زیربنای فعالیت و پژوهش قرار گرفت. در زیر اصول دوم و ششم کرکهُفس که مرتبط با بحث ما است را آورده‌ام:

۲) سیستم رمزنگار باید هیچ نکته پنهان و محرمانه‌ای نداشته باشد بلکه تنها چیزی که باید سری نگاه داشت شود کلید رمز است. (اصل اساسی کرکهُفس) طراح سامانه نباید فرض را بر این بگذارد که جزئیات سامانه خود را حتی از دشمنان مخفی نگاه دارد؛ این اصل به این نکته اشاره دارد که چنانچه امنیت سامانه ما صرفاً متکی به محرمانه نگه‌داشتن اطلاعات طراحی باشد در صورت افشاء این اطلاعات(به هر نحوی) امنیت کل سامانه مختل می‌شود. منظور این است که اگرچه راهبرد امنیتی امنیت از طریق ایجاد ابهام می‌تواند به امنیت سامانه‌ها کمک کند و ما نیز آن را به شما در امن سازی صنایع توصیه می‌کنیم اما نباید صرفاً متکی به پنهان کردن و محرمانه نگه‌داشتن دارایی‌ها و اطلاعات آن‌ها باشیم بلکه باید به نحوی امن سازی را انجام دهیم که چنانچه حتی مهاجمین توانستن این اطلاعات را به دست آوردند باز نتوانند امنیت کل سامانه(سایت صنعتی) را مختل نمایند؛ این یعنی رسیدن به سطح بالاتری از بلوغ امنیتی.

۶) سامانه رمزنگاری باید به سهولت قابل‌راه‌اندازی و کاربری باشند. چنین سامانه‌ای نباید به آموزش‌های مفصل و رعایت فهرست بزرگی از قواعد و دستورالعمل‌ها نیاز داشته باشد.

به امید افزایش دانش امنیتی همه تصمیم گیران و متصدیان حوزه امنیت فناوری اطلاعات و امنیت فناوری‌های عملیاتی ، به‌ویژه مدیران محترم صنایع و زیرساخت‌های حیاتی.

[1] Le Journal des Sciences Militaires


گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

ضمیمه الف: آسیب‌پذیری و انواع آن

بر اساس مرجع [۱]، به‌طور عمومی آسیب‌پذیری امنیتی مجموعه‌ای از ویژگی‌ها در سامانه است که به مهاجمین اجازه نقض خط‌مشی امنیتی تعریف‌شده را می‌دهد. آسیب‌پذیری از اموری ناشی می‌شود که در زیر به برخی از آن‌ها می‌پردازیم.

- طراحی/مشخصات[۱]: زمانی که یک فرآیند یا مؤلفه دارای معایب مربوط به طراحی است، از این نقایص برای به دست آوردن دسترسی به سامانه استفاده می‌شود. این نوع آسیب‌پذیری‌ها حاصل از مرحله طراحی سامانه سرچشمه می‌گیرند و اصلاح آن‌ها در غالب موارد نیاز به بازطراحی دارد.
- پیاده‌سازی[۲]: حتی زمانی که طراحی سخت‌افزاری یا نرم‌افزاری یک سامانه درست باشد، پیاده‌سازی سامانه ممکن است نادرست باشد. این مسئله می‌تواند منجر به ایجاد ضعف‌های امنیتی یا عدم استحکام منجر به خرابی شود. این آسیب‌پذیری‌ها غالباً همان ایرادهای امنیتی فنی در زمان توسعه و پیاده‌سازی یک سامانه هستند.
- پیکربندی[۳] یا عملیاتی: زمانی که یک منبع به طرز نادرستی پیکربندی شود می‌تواند زمینه این را فراهم کند که علیرغم مطلوب بودن مراحل طراحی و پیاده‌سازی مهاجم بتواند برخی خاصیت‌های[۴] امنیتی مورد اهمیت سامانه را نقض کند. این دسته از آسیب‌پذیری‌ها مواردی هستند که به علت پیکربندی و گسترش نادرست یک سامانه در محیطی خاص به وجود می‌آیند. آسیب‌پذیری‌های عملیاتی به دلایل مختلف ازجمله ناقص بودن، نامناسب بودن یا نبود مدارک امنیتی ازجمله دستورالعمل‌ها و راهنماهای عملیاتی به سامانه وارد می‌شوند. مدارک امنیتی، به همراه پشتیبانی مدیریت، اساس کار همه برنامه‌های امنیتی محسوب می‌شوند. در جدول ۲ نمونه‌هایی از آسیب‌پذیری‌های امنیتی ذکرشده است:

---

[۱] Design/Specification

[۲] Implementation

[3] Configuration

[4] Properties

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

جدول ۲: نمونه‌هایی از آسیب‌پذیری سه مرحله مختلف [۱]

مرحله	برخی نمونه آسیب‌پذیری‌ها
طراحی/مشخصات	• طراحی ارتباطات بدون رمزنگاری • عدم تبیین جزئیات و نوع احراز اصالت موجودیت‌ها در مرحله طراحی • در نظر نگرفتن روش‌هایی برای تضمین صحت داده‌ها
پیاده‌سازی	• اتخاذ روش‌های برنامه‌نویسی غیر امن • پیاده‌سازی احراز اصالت با سطح امنیتی پایین • ضعف در واسط برنامه‌نویسی امن • بکار گیری تجهیزات دست‌کاری شده و غیر امن • نظارت و رویدادنگاری ضعیف
پیکربندی	• ضعف در مدیریت حساب کاربران با توجه به خط‌مشی‌های سازمان • ضعف در مدیریت سرویس‌های بدون استفاده با توجه به خط‌مشی‌های سازمان • ضعف در مدیریت وصله‌ها با توجه به خط‌مشی سازمان • ضعف در تغییر مقادیر پیش‌فرض تنظیمات

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

ضمیمه ب: توصیه‌های در مورد به‌روزرسانی تجهیزات و وصله‌های امنیتی

- حتماً جهت دانلود به‌روزرسانی‌ها یا وصله‌های امنیتی از وبگاه معتبر سازنده استفاده نمایید.
- بعد از دانلود به‌روزرسانی‌ها یا وصله‌های امنیتی و قبل از اجرا در صورت وجود کد درهم‌ساز[1] در وبگاه سازنده، حتماً این کد را با کد به‌روزرسانی یا وصله‌ی امنیتی دانلود شده مقایسه نمایید و از صحت آن اطمینان حاصل نمایید.
- قبل از نصب به‌روزرسانی یا وصله‌ی امنیتی دانلود شده گواهی رقمی[2] آن‌ها را بررسی کرده و از صحت آن اطمینان حاصل نمایید
- در صورت امکان ابتدا به‌روزرسانی یا وصله‌ی امنیتی را بر روی سامانه‌ی تست یا محیط دارای افزونگی[3] امتحان کرده بعدازآن بر روی تجهیزات اصلی اجرا نمایید.

* درصورتی‌که هر یک از موارد بالا برای شما مبهم است ما این مفاهیم را همراه با مجموعه‌ای از اصول امنیتی دیگر در قالب دوره‌های آموزشی مقدماتی و پیشرفته به شما آموزش می‌دهیم.

[1] Hash Code

[2] Digital Certificate

[3] Redundancy

ضمیمه ج: اصول سه‌گانه‌ی امنیت

در فضای سایبر-فیزیکی هر سامانه دارای ضعف‌های ذاتی و اجرایی است که هدف امنیت اطلاعات پیشنهاد راه‌هایی برای جلوگیری از سوءاستفاده و بهره‌جویی از این ضعف‌ها هست. به‌طورکلی امنیت اطلاعات مبتنی بر تحقق سه ویژگی محرمانگی[۱]، صحت اطلاعات[۲] و دسترس‌پذیری[۳] است که از این سه ویژگی در برخی منابع با عنوان سه‌تایی CIA یاد می‌شود که در شکل ۲ نمایش داده‌شده‌اند. در ادامه این سه ویژگی را تعریف می‌کنیم [۱]:

شکل ۲: مثلث سه‌تایی CIA

در جدول ۳ اصول سه‌گانه‌ی امنیتی به همراه تعریف اختصاری آن‌ها و رخدادهای ناقض هرکدام از ویژگی‌ها آورده شده است. شرح تفصیلی هر یک از این سه ویژگی در ادامه این بخش آورد شده است.

جدول ۳: اصول سه‌گانه‌ی امنیتی [۱]

ویژگی	تعریف مختصر	رخداد ناقض ویژگی
محرمانگی	عدم افشای غیرمجاز داده‌ها	• نشت اطلاعات محرمانه • دسترسی غیرمجاز به داده‌ها • سرقت داده‌ها • تعرض به حریم خصوصی

[1] Confidentiality

[2] Integrity

[3] Availability

صحت	عدم دست‌کاری داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز	• تغیر مخفیانه در داده‌ها • جعل داده‌ها
دسترس‌پذیری	دسترسی به داده‌ها توسط افراد مجاز در هر مکان و در هرزمان	• از دسترس خارج شدن خدمات یک کارگزار • نابودی داده‌ها • اختلال در عملکرد تجهیزات

محرمانگی

محرمانگی به معنای عدم افشای غیرمجاز داده‌ها است. ازاین‌رو هدف امنیت اطلاعات، ارائه مجموعه مکانیزم‌ها و رویه‌هایی[1] است که از دسترسی افراد، فرآیندها و موجودیت‌های غیرمجاز به اطلاعات طبقه‌بندی‌شده جلوگیری کند. محرمانگی می‌تواند گستره وسیعی از عدم افشاء محتوای داده‌ها تا عدم افشای نام‌ها[2] را در بربگیرد [۱].

صحت

صحت اطلاعات به معنای حفظ یکپارچگی و عدم امکان تحریف و دست‌کاری عمدی یا غیرعمدی اطلاعات است. ازاین‌رو هدف امنیت اطلاعات، ارائه مجموعه مکانیزم‌ها و رویه‌هایی است که از هرگونه تحریف، دست‌کاری و حذف اطلاعات توسط افراد یا موجودیت‌های غیرمجاز جلوگیری کند. صحت داده‌ها شامل اصالت داده‌ها (عدم حذف، اضافه و تکرار)، اصالت مبدأ داده‌ها[3] و انکارناپذیری[4] است [۱].

[1] Procedures

[2] Anonymity

[3] Data Origin Authentication

[4] Non-Repudiation

دسترس‌پذیری

دسترس‌پذیری به معنای امکان دسترسی به داده‌ها (به‌طور عام منابع) توسط افراد یا موجودیت‌های مجاز است. ازاین‌رو هدف امنیت اطلاعات، ارائه مجموعه مکانیزم‌ها و رویه‌هایی است که افراد و موجودیت‌های مجاز امکان دسترسی به داده‌ها یا سایر منابع مجاز را در زمان مناسب و مکان مناسب داشته باشند [۱].

ضمیمه د: خدمات ما و راه ارتباطی

خدمات ما ذیلاً فهرست شده است:

- تدریس دوره‌های مقدماتی و پیشرفته امنیت سامانه‌های کنترل صنعتی و سمینارها و کارگاه‌های مرتبط
- مشاوره و اجرای طرح‌های جامع امن سازی سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- طراحی و راه‌اندازی آزمایشگاه‌های ارزیابی امنیتی سامانه‌های کنترل صنعتی
- طراحی نقشه راه امن سازی سایبری سامانه‌های سایبری و سایبر-فیزیکی
- ارزیابی امنیتی سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی
- تحلیل جریان اطلاعات در سامانه‌های سایبر-فیزیکی
- مدل‌سازی امنیتی سامانه‌های سایبر- فیزیکی

راه ارتباطی:

تماس جهت عقد قرارداد مشاوره، طراحی و اجرا، برگزاری دوره‌های آموزشی یا سخنرانی:

✉ mm.Ahmadian[aatt]aut[dot]ac[dot]ir

www.mmAhmadian.ir

عزیزانی که تمایل دارند نامه یا پیام ارسالی خود را با یک‌لایه امنیتی (رمزنگاری) برای بنده ارسال کنند می‌توانند از کلید عمومی PGP بنده (لینک) برای ارسال رمز شده نامه خود استفاده کنند. قبل از استفاده از کلید عمومی بنده می‌توانید برای اطمینان بیشتر از صحت این کلید، کد درهم‌ساز فایل مربوط به کلید بنده را با کد درهم‌ساز ذیل مقایسه کنید.

MD5 checksum of PGP_PublicKey_MMAhmadian.zip:
5818bc4225bdd6354b07a5a9ed3bf0af

برخی سوابق آموزشی مرتبط:

عنوان	عنوان انگلیسی	محل ارائه	زمان	اسلاید
سخنرانی چالش‌های امنیتی در سامانه‌های سایبر-فیزیکی (با محوریت تحلیل جریان اطلاعات در خطوط لوله نفت و گاز)	*Cyber–Physical Systems Security Challenges (Case study: Information Flow Security Analysis in Natural Gas and Oil Pipeline System)*	ششمین کنفرانس فناوری اطلاعات و ارتباطات در نفت، گاز، پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی	دی ماه ۱۳۹۶	لینک
شناسایی تهدیدات و آسیب‌پذیری‌های امنیتی پروتکل کنترل صنعتی IEC 60870-5-104	*Towards the Identification of IEC 60870-5-104 Protocol Security Vulnerabilities and Threats*	چهاردهمین کنفرانس بین‌المللی انجمن رمز، شیراز، دانشگاه شیراز	۱۶ شهریور ۱۳۹۶	لینک آگهی
کارگاه آموزشی امنیت اطلاعات در سامانه‌های کنترل صنعتی: چالش‌ها و راهکارها	*Information Security in Industrial Control Systems: Challenges and Solutions*	چهاردهمین کنفرانس بین‌المللی انجمن رمز شیراز، دانشگاه شیراز	۱۴ شهریور ۱۳۹۶	لینک آگهی
ارائه علمی تحلیل و وارسی صوری امنیت جریان اطلاعات در سامانه‌های سایبری-فیزیکی، مطالعه موردی: سامانه انتقال (خطوط لوله) گاز	*Formal Analysis and Verification of information flow security in cyber–physical systems, Case study: natural gas pipeline system*	دانشگاه صنعتی امیرکبیر	مرداد ۱۳۹۵	
ارائه علمی درآمدی بر سامانه‌های سایبری-فیزیکی و چالش‌های امنیتی آن‌ها، حوزه محوری: سامانه‌های کنترل صنعتی	*Introduction to cyber–physical systems and their security challenges, Case study: ICSs*	دانشگاه صنعتی امیرکبیر	شهریور ۱۳۹۵	
سخنرانی چالش‌ها و راهکارهای امنیتی در سامانه‌های کنترل صنعتی	*security challenges and solutions in ICSs*	-	آبان ۱۳۹۵	
کارگاه آموزشی امنیت سایبری در سامانه‌های کنترل صنعتی	*Cyber Security in Industrial control systems*	شرکت ملی گاز ایران، تهران	اسفند ۱۳۹۴	لینک
سخنرانی امنیت سایبری سامانه‌های کنترل صنعتی در صنایع نفت، گاز، پالایش و پتروشیمی		سومین کنفرانس و نمایشگاه فناوری اطلاعات و ارتباطات در صنایع نفت، گاز، پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی	دی ۱۳۹۳	لینک

گرداورنده و مولف گزارش :محمد مهدی احمدیان
کاندیدای دکتری تخصصی امنیت اطلاعات از دانشگاه صنعتی امیرکبیر
پژوهشگر، مدرس و مشاور امنیت سامانه های کنترل و اتوماسیون صنعتی

مراجع

۱. احمدیان، محمدمهدی؛ رضازاده، بابک. پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری، انستیتو ایزایران، ۱۳۹۶

2. https://cert-portal.siemens.com/productcert/pdf/ssa-181018.pdf
3. https://www.securityfocus.com/bid/104482
4. https://nvd.nist.gov/vuln/detail/CVE-2018-4833
5. https://ics-cert.us-cert.gov/advisories/ICSA-18-165-01
6. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4833
7. https://exchange.xforce.ibmcloud.com/vulnerabilities/144827
8. https://vulners.com/cve/CVE-2018-4833
9. https://www.siemens.com/cert/operational-guidelines-industrial-security
10. https://www.siemens.com/cert/operational-guidelines-industrial-security
11. https://support.industry.siemens.com/cs/document/109758142/firmware-update-version-5-2-3-for-scalance-x-200-?dti=0&lc=en-CN

*کلیه معادل‌سازی‌های این گزارش بر اساس فرهنگ واژگان موجود در آدرس ذیل:

- http://www.mmahmadian.ir/mysecglossary/infosecgloss/