هجدهمین کنفرانس حفاظت و اتوماسیون در سیستم‌های قدرت
دانشگاه صنعتی شاهرود
۱۹ و ۲۰ دی ماه ۱۴۰۲

اصول امنیت مخابرات در سیستم‌های اسکادا و اتوماسیون پست

پدیده نوبخت، محمد لاری، رحیم غلامی، مهدی ساجدی

شرکت برق منطقه ای خراسان، مشهد،
Padideh.nobakht@gmail.com

چکیده

فن‌آوری همواره در حال پیشرفت است. شرکت‌هایی موفق هستند که در تغییر مدل‌های کاری سازمان خود برای پذیرفتن فن‌آوری روز تلاش می‌کنند. سازمان‌هایی که تغییرات را نادیده گرفته و به وضع موجود پایبند باشند، منسوخ می‌شوند. زیرساخت‌های اصلی نیازمند ارائه خدمات با کیفیت و امنیت بالا به مشتریان هستند. صنعت برق یکی از زیرساخت‌های اصلی است که باید با پیشرفت تکنولوژی همگام باشد. همچنین صنعت برق از زیرساخت های مخابراتی استفاده می کند که در صورت عدم رعایت الزامات امنیتی، با خسارات جبران ناپذیری مانند خاموشی کلی و یا از بین رفتن شبکه مواجه خواهند شد. در این مقاله اصول امنیت مخابرات و معیارهای امنیتی سیستم‌های اسکادا و اتوماسیون پست‌ها معرفی شده‌است. عدم توجه به این اصول در طراحی و پیاده سازی این سیستم‌ها باعث خواهد شد تا شبکه به لحاظ امنیتی بسیار آسیب‌پذیر باشد.

کلمات کلیدی

امنیت مخابرات، پروتکل‌های ارتباطی، انواع حملات، استراتژی معماری امنیت، امنیت پروتکل‌های صنعتی.

۱- مقدمه

در اصطلاحات مربوط به امنیت اطلاعات سیستم، سیستمی ناامن است که در آن آسیب پذیری و تهدید وجود داشته باشد. آسیب پذیری یک سیستم اطلاعاتی ممکن است بر اثر نقص طراحی منطقی، نقص پیاده سازی یا یک ضعف اساسی باشد. یک مهاجم همواره در تلاش برای یافتن قسمت های آسیب پذیر و بهره برداری از آسیب در جهت تحمیل خسارت می باشد. همچنین ممکن است خسارت اتفاقی و بر اساس خطاها و اشتباهات ایجاد شود. امروزه سیستم های ارتباطی صنعتی تا حد زیادی مبتنی بر سیستم عامل‌های تجاری، پیاده سازی پروتکل و برنامه های کاربردی ارتباطی با آسیب پذیریی بالا هستند. با اتصال به اینترنت یا دیگر شبکه های عمومی، سیستم در معرض حمله بالقوه قرار می گیرد. از طرفی، حمله نیاز به تخصص و انگیزه دارد. با فن آوری های اینترنت باز، تخصص به راحتی در دسترس همگان است. انگیزه های سیاسی و اقتصادی می تواند دلیلی برای حمله صنعتی به سیستم های ارتباطی و زیرساخت های حیاتی که به وسیله کامپیوتر کنترل می شوند، باشد. به عنوان مثال در ژانویه ۲۰۰۳، کرم غیرفعال کامپیوتری اسلمر بر سیستم نظارت ایمنی نیروگاه هسته ای دیویس در اوهایو تاثیر گذاشت و باعث خاموشی نیروگاه در آن زمان شد. مدیران مسئول این نیروگاه دیوار آتش را برای محافظت اتصال به خارج از شبکه خود در نظر گرفته بودند. این کرم به وسیله یک پیمانکار وارد شبکه نیروگاه شد. به طوری که کامپیوتر آلوده متصل شده از طریق شماره گیری تلفن به طور مستقیم به شبکه های نیروگاه متصل شده، در نتیجه دیوار آتش را بی تأثیر کرد[۱] . یکی دیگر از کرم های مشهور کامپیوتری استاکس نت است که توانست کنترل سیستم نظارتی نیروگاه هسته ای در ایران را مختل سازد[۳].

اهمیت زیرساخت های حیاطی صنعت آب و برق سبب شده است که IEEE تشویق های مالی برای نفوذ مخرب به کامپیوتر و ارتباطات سیستم های صنعت برق و بازار شرکت کنندگان را ایجاد کند. بنابراین، امنیت به یک مسئله مهم تبدیل شده است.

۲- اصول امنیت مخابرات

شبکه هوشمند دارای تعابیر متفاوتی از جمله مدرنیزه ساختن، ایجاد واکنش سریع و مدیریت بهینه شبکه قدرت با استفاده از سیستم مخابرات و فن آوری است. سیستم های هوشمند شامل بخش های تولید، انتقال، توزیع، مشترکین، بهره بردار، بازار برق و ارائه دهنده سرویس است. در ادامه به بررسی اصول امنیت مخابرات پرداخته شده است [۵].

۲-۱- اهداف امنیتی

نحوه دسترسی مهاجم به سیستم، اصول امنیتی در برابر تهدیدها و سطوح اطمینان یک سیستم برای رسیدن به اهداف امنیتی مربوطه از دیدگاه های عمده در تعریف امنیت است. محرمانه بودن اطلاعات، صحت اطلاعات، دسترس پذیری اطلاعات، تصدیق هویت، مجوز، قابلیت ممیزی و بازرسی، عدم انکار و حفاظت در مقابل شخص ثالث به عنوان هدف های امنیتی قابل استفاده در سیستم هستند.

۲-۲- انواع حملات

بسته به توابع خاص و شرایط محیط در هر شبکه صنعتی زیر مجموعه ای از اهداف امنیتی تعریف می شود که نقض عمدی این اهداف امنیتی حمله نام دارد. ممکن است حملات توسط افراد خارج یا داخل سازمان انجام گردد. حملات به دو دسته ی هدفمند و بی هدف دسته بندی می شوند. بالا بودن آسیب پذیری سیستم باعث می‌شود تا حملات بی هدف خسارت های بیشتری به سیستم تحمیل نماید. در حملات هدفمند مقصود آسیب رساندن به یک سیستم ارتباطی خاص با اهداف مشخص نظیر جاسوسی صنعتی، جنگ یا تروریسم است که به طور معمول یک مرحله از آن جمع آوری اطلاعات در مورد هدف است. حمله DOS2، استراق سمع، حمله مردی در میانه راه، شکاف در سیستم، ویروس و کرم های اسمر و استاکس‌نت از جمله ی حملات به سیستم هستند.

اسلمر: کرم اسلمر که بعضی از اوقات با نام سافایر از آن یاد می شود به عنوان یکی از سریع ترین کرم های کامپیوتری در تاریخ شناخته می شود. به محض انتشار در اینترنت بیش از ۹۰ درصد میزبان‌های آسیب پذیر را آلوده ساخته و با ایجاد مانع در پاسخ گویی انسانی باعث ایجاد اختلالات قابل توجهی در مؤسسات مالی، حمل و نقل و مؤسسات دولتی می‌شود[۲].

استاکس نت: اصطلاح کرم کامپیوتری استاکس نت توسط فرِد کوهن در سال ۱۹۸۵ ابداع شد که با گذشت زمان و تکمیل نسخه های قدیمی آن نسل جدیدی مخصوص حمله به سیستم های فیزیکی سایبری طراحی شد. نسل جدید رفتارهای کاملا متفاوتی نسبت به تعاریف کلاسیک دارد. پنهان شدن تا انتهای مأموریت از استراتژی‌های مشخص و همیشگی استاکس نت و ویروس و کرم های مشابه است. به این معنا که تا پایان مأموریت، از هرگونه رفتار مخرب فیزیکی پرهیز می کند. این کرم به عنوان اولین کرمی شناخته می‌شود که به سیستم های کنترل نظارت و جمع آوری داده ها SCADA حمله کرده است. این کرم ها قدرت انتشار سریع بدون ردیابی توسط سیستم ها از طریق فلش مموری و انواع شبکه ها را دارند. ویروس و کرم هایی نظیر استاکس نت، Duqu و Flame به نحوی طراحی شده اند که دستگاه های برنامه ریز کنترل منطقی را آلوده می‌سازند تا به اهداف طراح خود برسند، که این اهداف شامل سرقت اطلاعات صنعتی یا ایجاد تغییرات رفتاری در سیستم های کنترل و تخریب تجهیز است. در نتیجه با توجه به حضور گسترده دستگاه های کنترلی در صنعت همواره این خطر امنیتی صنعت را تهدید می‌کند.

در دهه اخیر کمیسیون‌های بین المللی نظیر CIGRÉ و IEC سازوکارهای متعددی برای ارتقاء امنیت سایبری در سیستم های قدرت ارائه کرده اند. استاندارد IEC62351، برای امنیت سیستم های قدرت و IECTC57 برای امنیت مخابراتی استفاده می شوند [۳,۴].

۲-۳- روش‌های رمزنگاری

الگوریتم‌های رمزنگاری به منظور ذخیره‌سازی و انتقال امن داده ها استفاده می شوند. اهداف امنیتی نظیر محرمانگی، درستی، احراز هویت و عدم انکار با استفاده از روش های رمزنگاری محقق می شوند. قبل از اختراع تکنیک‌های رمزنگاری امروزی، رمزنگاری با تکیه برنگه داشتن راز الگوریتم انجام می شد. با این حال، در رمزنگاری مدرن و مطابق اصل کرک هاف، باید الگوریتم رمزنگاری آشکار و فقط کلید محرمانه باشد. همچنین یک الگوریتم رمزنگاری باید در مقابل آسیب ها و حملات کشف شده مقاوم باشد و با مشاهده حملات جدید به روزرسانی گردد. الگوریتم های رمزنگاری به دو دسته متقارن و نامتقارن تقسیم می شوند، که به ترکیب رمزنگاری متقارن و نامتقارن رمزنگاری ترکیبی گویند.

یکی از روش های مدرن رمزگذاری ساختار چندلایه بر پایه تکنولوژی بلاک چین است. که برای استفاده از آن می‌توان به رویکرد خوشه بندی هوشمند و یادگیری ماشینی مبتنی بر الگوریتم های SI و محاسبات تکاملی به منظور رمزگذاری ساختار چند لایه اشاره نمود. پیاده سازی بلاک چین به طور بالقوه می تولند منجر به مشکلات اضافی و مقیاس پذیری شود. یکی از کاربردهای این روش در اینترنت اشیاء است [۸].

۲-۴- امنیت در شبکه و پروتکل های ارتباطی

در شبکه‌های ارتباطی، اهداف امنیتی توسط پروتکل‌های امنیتی در لایه‌های مختلف شبکه ارتباطی فراهم می‌گردد. تاکید این پروتکل‌های امنیتی به محافظت در برابر حملات مبتنی بر شبکه بر روی لینک‌های ارتباطی است. سرویس‌های امنیتی ارائه شده توسط یک لایه خاص ارتباط بین نقاط ابتدایی و انتهایی مربوط به آن لایه را حفظ می کنند. در حال حاضر پروتکل‌های امنیت در شبکه و لایه انتقال به ترتیب IPSec و SSL هستند. رایج ترین پروتکل‌های امنیتی و خدمات آنها در جدول(۱) ارائه شده است.

- **امنیت لایه لینک:** برای تعمیم امنیت پروتکل های PPP، PAP و CHAP به کاربران ارائه شده است. در گذشته از رمز عبور و

مکانیسم چالش/پاسخ استفاده مش شد. همچنین پروتکل EAP یک چهارچوب کلی برای احراز هویت تعریف می کند. لینک های بی سیم طیف کوتاه مانند بلوتوث یا شبکه های محلی بی سیم IEEE 802.11 بسیارآسیب پذیر هستند. حملات DOS به راحتی پارازیت رادیویی ایجاد می کنند و امکان محافظت در برابر چنین حملاتی وجود ندارد، اما این حملات قابل شناسایی می باشند. اقدامات حفاظتی در برابر حملات استراق سمع و حملات فعال موجود برای ارتباطات بی سیم برد کوتاه مدرن به شرح ذیل است:

- ✓ استاندارد IEEE802.11 ، امنیتی اختیاری و معادل حریم خصوصی بی سیم است که سرویس رمزنگاری آن مبتنی بر رمزنگاری RC4 می باشد.
- ✓ پروتکل IEEE 802.1X بر اساس کنترل دسترسی به شبکه LAN وi IEEE 802.11 برای استفاده WLAN طراحی شده است.
- ✓ یک جایگزین برای تضمین عملیات WLAN، به کارگیری راه حل-های IPsec / VPN می باشد.

جدول (۱): رایج ترین پروتکل های امنیتی [۵]

Layer	Protocol	Security Protocol	Confidentiality	Integrity	Authentication	to be secured
Applications	SOAP	WS-Security	yes	yes	data origin	document parts
	SMTP	PGP/GnuPG	yes	yes	message	mail content
		S/MIME	yes	yes	message	
	HTTP	HTTP Digest Authentication	no	no[a]	user[b]	user-to-server
Transport layer	TCP	SSH Transport Layer Protocol	yes	yes	server[c]	client(user)-to-server
		SSL/TLS	yes	yes	server[d]	client-to-server
Internet layer	IP	IPSec	yes[e]	yes	host /	host-to-host
	PPP	CHAP/PAP	no	no	client	end-point of link
Link layer	Bluetooth	Bluetooth Security	yes	yes	device	air interface
	WLAN IEEE802.11	WEP/WPA/802.1X	yes	yes	device	

[a] optional, but usually not implemented
[b] server (or mutual) authentication optional
[c] user authentication provided by SSH User Authentication Protocol
[d] client authentication optional
[e] optional, only in Encapsulated Security Payload (ESP)-mode
[f] data origin authentication optional, only in Authentication Header (AH)-mode

• **امنیت لایه اینترنت:** برایی ایجاد امنیت در لایه اینترنت پروتکل IPSec پیشنهاد شده است. این روش برای محافظت در لایه IP و برای حفاظت از تمام برنامه های کاربردی UDP و TCP استفاده می شود. برای ایجاد امنیت در لایه اینترنت IPSec پیشنهاد شده است و اهداف امنیتی زیر را برای ارتباطات میزبان به میزبان پشتیبانی می کند:

- ✓ محرمانه بودن داده (فقط در ESP)
- ✓ احراز هویت مبدا داده ها (تنها درحالتAH)
- ✓ درستی داده ها (در حالت ESP و AH)
- ✓ کنترل دسترسی، با توجه به میزبان فردی (در ESP و AH)

دو حلت برای IPSec با نام های ESP و AH وجود دارد که هر دو حالت را می توان با هم یا به تنهایی استفاده کرد. بعلاوه، تبادل کلید IPSec چهارچوبی برای مدیریت کلید وامنیت جلسه (به عنوان مثال، کلید جلسه برای رمزنگاری متقارن) فراهم می کند. روش IPSec برای تصدیق هویت کاربران شخصی کاربرد ندارد. بنابراین، IPSec اغلب برای ایجاد شبکه های خصوصی مجازی (VPN ها) و تامین امنیت بین میزبانان نهایی استفاده می شود. از آنجا که امنیت IPSec توسط آدرس IP مبدا و مقصد ایجاد می گردد، ممکن است در صورت بروز برخی تغییرات در ترجمه آدرس شبکه یا ویرایش آدرس های IP و پورت ها، تنظیمات IPSec از بین برود.

• **امنیت لایه انتقال:** برای تأمین امنیت برنامه های در حال اجرا در بالای TCP از SSL و یا TLS استفاده می شود. لازم به ذکر است که این حالت شامل UDP نمی شود. همچنین برنامه های کاربردی HTTP و FTP از SSL استفاده می‌کنند.

ویژگی های اصلی SSL به شرح ذیل است:

- ✓ مدیریت کلید جلسه و انجام الگوریتم رمزنگاری
- ✓ تأیید هویت سرور با استفاده از گواهی نامه
- ✓ محرمانه بودن داده
- ✓ حفاظت از درستی داده ها
- ✓ احراز هویت مشتری و ارائه گواهی (به ندرت اجرا می گردد).

پروتکل لایه انتقال SSH -TRANS امکان محرمانه بودن، تأیید هویت سرور، تبادل کلید جلسه و حفاظت از درستی داده را فراهم می کند. پروتکل SSH-TRANS از پروتکل های تصدیق(SSH-AUTH)و پروتکل اتصال (SSH-CONN) پشتیبانی می کند که SSH-AUTH وظیفه تائید هویت کاربرها و SSH-CONN وظیفه شماره سرویس های شبکه ، ورود امن از راه دور و ارسال امن TCP را به عهده دارد.

• **امنیت لایه کاربردی:** تصور برآورده شدن اهداف امنیتی با استفاده از پروتکل های امنیتی مطرح شده اشتباه است، بنابراین نیاز است تا لایه های بالاتر نیز ایمن گردد. به منظور تأمین امنیت پروتکل های HTTP ،DA، PGP و سرویس XML معرفی می شود.

دیوار آتش: برای کنترل دسترسی شبکه و محافظت از استفاده های غیرمجاز کامپیوترها، مورد استفاده قرار می گیرد. دیوارهای آتش وظیفه صدور مجوز عبور ترافیک شبکه را به عهده دارند و دارای ویژگی های زیر هستند [۵-۷]:

- •کنترل دسترسی ها برای محافظت از شبکه
- •کنترل دسترسی به تجهیزات برای محافظت از شبکه
- •پیشگیری از ورود بسته های ناخواسته به شبکه های حفاظت شده
- •حفاظت از بخش های شبکه و حفاظت از میزبان در برابر کاربران بیرونی
- •کنترل ترافیک صادره در شبکه های ناامن
- •ضبط اطلاعات مفید نظارت ترافیک و آشکارسازی ورودی های غیرمجاز

سیستم های تشخیص نفوذ: هدف این سیستم‌ها، کشف حملات براساس پروفایل تهاجمی شناخته شده و یا رفتار غیرمعمول سیستم است. اطلاعات مورد نیاز سیستم های تشخیص نفوذ تحت شبکه از ترافیک مشاهده شده در بخش شبکه به دست می آید. این اطلاعات شامل نوع،

محتوا، فرکانس و مسیر انتقال پیام است. تشخیص نفوذ، مبتنی بر میزبان، از اطلاعات محلی میزبان برای کشف حملات استفاده می کند. میزبان‌های مرتبط با امنیت مانند دیوارهای آتش و سرورهای تشخیص نفوذ شبکه باید توسط یک سیستم تحت نفوذ مبتنی بر میزبان محافظت گردند.

۲-۵- بهترین استراتژی های معماری امنیت

ایجاد سیستم های امنیتی که مانع از طیف گسترده ای از حملات گردد و با گستره عملکرد و بودجه سازمان تطبیق داشته باشد بسیار دشوار است. به همین سبب، بررسی اصول و استراتژی‌های مختلف سیستم های امنیتی از اهمیت بالایی برخوردار است.

• **سیاست های امنیتی:** بدون وجود سیاست صریح امنیتی قبل از شروع طراحی، احتمال به هدر رفتن تلاش های انجام شده در تأمین امنیت سیستم زیاد است.

• **نگاه فرآیندی به امنیت:** با توجه به تغییر شرایط محیطی و وجود حملات جدید، هیچ سیستم امنیتی قادر به انجام هدف خود برای همیشه نیست و نیازمند بررسی منظم قوانین، تعمیر، نگهداری، رشد و ارتقاء خواهد بود. در این بررسی باید سیستم با سیاست های امنیتی تطبیق داده شود و تنظیمات و تغییرات مورد نیاز به سیستم اعمال گردد.

• **اهمیت دادن به ضعیف ترین لینک:** برای جلوگیری از حمله مهاجمین باید اهداف مختلف امنیتی مورد نیاز یک سیستم متعادل گردد. به عنوان مثال انتخاب یک الگوریتم رمزنگاری قوی با طول کلید بزرگ، با رمز عبور ساده آسیب پذیری سیستم را به همراه دارد.

• **تفکر امنیت توسط گمنامی:** فروشندگان و سازندگان ادعا می کنند که مهاجمین به دانش فنی دقیق و لازم برای بهره برداری از پروتکل های اختصاصی دسترسی ندارند، در نتیجه سیستم های اتوماسیون در برابر حملات الکترونیکی ایمن می باشند. در صورتی که این تصور کاملا نادرست است و با توجه به گسترش اتوماسیون و آشنایی تعداد زیادی از کارشناسان با دانش این سیستم ها و دسترس‌پذیری اطلاعات در استانداردها و سایت های اینترنتی، ابهامی وجود ندارد و سیستم ها به راحتی تحت حمله قرار می گیرند.

- **حداقل امتیاز:** لازم است هر کاربر حداقل مجوز لازم برای انجام کار خود را داشته باشد و باید از ارائه مجوزهای بیشتر از حدود محدوده کار کاربر جلوگیری گردد.

• **حفاظت از کلید و داده ها:** بسیاری از سیستم های اتوماسیون حاوی اطلاعاتی هستند که نباید توسط کاربران قابل مشاهده یا اصلاح باشد. برای حصول اطمینان از حفاظت داده ها می توان از رمزگذاری، توابع یک طرفه، سخت افزار و سرور امن استفاده کرد.

• **امنیت ابتدا تا انتها:** در ساختار امنیتی نباید فقط فاز انتقال مورد توجه قرار گیرد. در بسیاری از موارد، خراب کاری در نقاط انتهایی یا ابتدایی انجام می شود. بنابراین باید در مکانیزم های امنیتی حفاظت از داده از محل تولید تا مقصد در نظر گرفته شود.

• **دفاع عمیق:** دو دیدگاه اصلی برای امنیت فیزیکی و اطلاعاتی به نام های محیط سخت و دفاع عمیق وجود دارد. ایده اصلی در محیط سخت ایجاد دیوار غیر قابل رسوخ اطراف سیستم و عدم رعایت امنیت در داخل سیستم است. در این دیدگاه مشکلاتی مانند کاهش واکنش برای دفاع صحیح و عدم وجود حفاظت از بدخواهی های داخلی وجود دارد. در دیدگاه دفاع عمیق چندین ناحیه در اطراف کلیدید مورد حفاظت قرار می گیرند که مکانیزم‌های متفاوتی برای حفاظت همزمان درون و اطراف ناحیه مذکور دارند. بخش بیرونی ناحیه از ارزش امنیتی کمتری برخوردار است و سیستم های اتوماسیون مهم در داخلی ترین بخش ناحیه قرار می گیرند.

• **الگوریتم های استاندارد رمزنگاری:** در حال حاضر الگوریتم‌های رمزنگاری بسیار متنوعی وجود دارد و دلیل منطقی برای ایجاد الگوریتم های اختصاصی جدید وجود ندارد و بهتر است یکی از الگوریتم های رمزنگاری موجود که با نیازهای سازمان تطبیق دارد انتخاب گردد.

۳- امنیت برای پروتکل های صنعتی

به دلیل وجود برخی تفاوت‌ها بین پروتکل‌های صنعتی و پروتکل‌های موجود، نیاز به بررسی الزامات پروتکل‌های صنعتی و استانداردهای خاص این پروتکل‌ها است. در این بخش به بررسی تفاوت‌های بین سیستم‌های اتوماسیون صنعتی و اداری می‌پردازیم و استانداردهای تعریف شده مربوط به پروتکل‌های صنعتی معرفی می‌شوند.

۳-۱- امنیت مربوط به سیستم های مخابرات صنعتی

تفاوت های محسوسی بین سیستم های مخابرات صنعتی با سیستم های اداری، بازرگانی وجود دارد. این تفاوت ها و جدید بودن سیستم های اتوماسیون پست سبب می شود تا نتوان از امکانات امنیتی اداری تعریف شده، برای اتوماسیون پست ها استفاده کرد.

• **الزامات:** الزامات امنیتی سیستم های کنترل و اتوماسیون صنعتی با شبکه های IT سازمان ها و شرکت ها متفاوت است. در شبکه های صنعتی الزام ایمنی کارکنان و لزوم دسترس پذیری (کار مداوم و عدم امکان خاموشی) وجود دارد. این الزام گاهی اوقات برای به کارگیری شیوه مدیریت استاندارد IT (مانند راه اندازی مجدد سیستم جهت رفع عیب) به عنوان مانع محسوب می شود. برای تمرکز روی امنیت سیستم های اتوماسیون پست ها باید تجهیزات اتوماسیون که تجهیزات مرزی (بیرونی ترین تجهیزات) سیستم محسوب می شوند (مانند PLC) از حملات محافظت گردند و برای دسترسی به آن ها باید تصدیق مشتری صورت

پذیرد. در مقایسه با سیستم های اداری و بازرگانی که حفاظت از سرورهای مرکزی بسیار مهم است در سیستم های اتوماسیون حفاظت از تجهیزات مرزی اهمیت دارد.

• **محیط عملیاتی:** سیستم ها اتوماسیون توسط یک تیم تخصصی متشکل از مجموعه ای از مهندسین و تکنسین ها در حال بهره برداری است. این گروه معمولا کوچک و محدود می باشند که برای هر نفر یک نقش تعریف شده است. حذف و اضافه کردن اعضاء یا تغییر در نقش ها و دسترسی ها محدود می باشد و نیاز به سیستم مدیرتی ندارد. بنابراین این سیستم ها در مقایسه با شبکه های بزرگ IT یا شبکه های Web، مدیریت نقش ها اهمیت کمتری دارد و نیاز به روش های مدیریتی اتوماتیک نمی باشد. پیکربندی و توپولوژی، سخت افزار و نرم افزار سیستم اتوماسیون دارای مشخصات خاص هستند. در نتیجه باید مکانیزم های حفاظت و آشکارسازی مناسب با سیستم باشد.

• **چالش ها:** تجهیزات اتوماسیون نسبت به کامپیوترهای رومیزی دارای قدرت پردازش پایین تری هستند ولی باید الزامات پاسخ به موقع (خیلی از مواقع در محدوده میلی یا چند ده میکرو ثانیه)را فراهم سازند. این الزامات کاربردی پروتکل های رمزنگاری را محدود می کنند. از طرفی دیگر با توجه به طول عمر زیاد سیستم های اتوماسیون (سیستم های قدیمی در شبکه که بر پایه امنیت توسط ابهام بنا شده اند و امکان استفاده از الگوریتم‌های حفاظتی را ندارند) باید راه حل امنیتی برای آن ها تدبیر کرد، که در نهایت اپراتورهای سیستم اتوماسیون و تکنسین های پست ها در بسیاری مواقع با ایجاد سیستم های جدید امنیتی و تغییرات مخالف هستند.

۳-۲- امنیت گذرگاه در سطح تجهیز

همان طور که می دانید پایین ترین لایه شبکه های مخابرات صنعتی شامل تجهیزات کاربردی مانند سنسورها، اندازه گیرها و سیستم های محرک می باشند و تعداد زیادی از سیستم های مخابراتی و پروتکل ها در این سطح قرار دارند. زمانی که نیاز به اتصال تعداد زیادی از تجهیزات اتوماسیون به کنترل کننده باشد، از گذرگاه استفاده می شود. ارسال دادها با استفاده از سیم مسی، کابل کواکسیال و فیبرنوری انجام می‌گردد.

۳-۳- امنیت سیستم‌های PLC

یکی از کانال های مخابراتی صنعت برق خطوط انتقال هستند. با استفاده از خاصیت عدم تقارن و تطبیق امپدانس می توان سیگنال‌های مخابراتی جعلی در خطوط قدرت ایجاد کرد. بنابراین امکان استراق سمع با یک گیرنده رادیویی ساده که در مجاورت خط انتقال قرار دارد وجود دارد. سیستم های پیشرفته مخابرات روی خطوط قدرت باید از اقدامات امنیتی مشابه سیستم های مخابرات رادیویی استفاده کنند. جهت افزایش امنیت در سیستم های PLC استفاده از کارت های هوشمند و رمزنگاری پیشنهاد شده است.

۳-۴- امنیت مراکز کنترل و مخابرات صنعتی

الزامات زمان واقعی: وظیفه اصلی تجهیزات اتوماسیون صنعتی اندازه گیری و کنترل به صورت ادواری و در تاریخ های مشخص شده می باشد. ممکن است حمله کنندگان خارجی از واسط های مخابراتی برای حملات DOS استفاده کنند و با ایجاد ترافیک سنگین نرخ بالای وقفه در پردازش ترافیک داده را ایجاد کنند. از اینرو در طراحی ها باید انتخاب اولویت پیام ها برای کاهش آسیب پذیری حملات DOS در نظر گرفته شود.

محدودیت های پردازش و حافظه: محدودیت های پردازش و حافظه از جمله مشخصه های اصلی سیستم های تعبیه شده در مخابرات صنعتی است. در انتخاب ابزار رمز نگاری و پروتکل های امنیتی نظیر SSL و HTTP DA باید محدودیت های تجهیزات نصب شده در نظر گرفته شود. استفاده از رمزنگاری ECC به لحاظ کاهش حجم پردازش و زمان پردازش از رمزنگاری RSA مناسب تر می باشد.

انعطاف‌نلپذیری: کنترل کننده های اتوماسیون باید اغلب به صورت خودگردان عمل کنند و به صورت ویژه انعطاف ناپذیر باشند. همچنین باید در برابر حملات مقاوم و دارای قابلیت تصدیق برای فرامین و پیام های دریافتی، باشند. از طرفی ممکن است باتری این سیستم ها به وسیله انجام پردازش های غیر ضروری خراب یا تخلیه گردد که برای این منظور باید تدابیر امنیتی لحاظ شود.

۴- پیشنهادات امنیتی

در این بخش به معرفی استانداردهایی با کاربردهای عمومی، زیرساختی، سخت افزاری و نرم افزاری و پروتکل های ارتباطی پرداخته شده است. استانداردهای عمومی امنیتی که قابل اجرا نیز هستند مانند استاندارد CC و ISO/IEC 17799 از استانداردهای عمومی امنیت هستند. استانداردهای IEEE1402، PCSRF، ISA SP99، AGA، IEC TC65، NERC 1200، FDA، IAONA و CIGRE برای سیستم های مخابرات صنعتی کاربرد دارند.

تمرکز اصلی استانداردهای امنیتی در جدول ۲ نمایش داده شده-است.

از آنجایی که پروتکل ها در سیستم های اسکادا و اتوماسیون پست ها از اهمیت خاصی برخوردار هستند، الزامات امنیتی در این پروتکل ها به شرح ذیل پیشنهاد می شود:

امنیت پروتکل Profibus :برای ایجاد امنیت در این پروتکل پیشنهادات زیر ارائه شده است:

- ✓ استفاده از دیوار آتش
- ✓ ایجاد مرکز کنترل صحت اسناد و مجوز ها
- ✓ استفاده از شبکه های خصوصی مجازی(VPNs)
- ✓ ارزیابی امنیت
- ✓ حفاظت از ویروس
- ✓ ایجاد سیستم ثبت وقایع
- ✓ شناسایی ریسک ها، اهداف حمله کننده و ارائه راهکار های لازم

جدول (۲): تمرکز اصلی استاندارد های امنیتی [۹]

نام استاندارد	تمرکز اصلی
NIST SGIP-CSWG	شبکه هوشمند – حملات سایبری
NERC CIP	مقررات حملات سایبری تجهیزات قدرت آمریکای شمالی
IEC 62351	امنیت داده و امنیت در مخابرات
IEEE PSRC/H13 & SUB/C10	الزامات امنیت سایبری برای اتوماسیون پست‌ها، سیستم-های کنترل و حفاظت
IEEE 1686	استاندارد برای امنیت سایبری تجهیزات هوشمند الکترونیکی پست‌ها
ISA S99	اتوماسیون صنعتی و امنیت سیستم کنترل

- **امنیت پروتکل Modbus**: برای ایجاد امنیت در این پروتکل پیشنهادات زیر ارائه شده است:

- ✓ گسترش آشکار سازی ورود های بدون اجازه، به واسطه تجهیزات IDS ، تراکنش ثبت وقایع یا نظارت ترافیک
- ✓ اعلام وضعیت نا امن برای تمام ارتباطات SCADA بیرونی که با سیستم های فیزیکی محافظت نمی شوند و در صورت امکان رمز نگاری اطلاعات
- ✓ ایجاد ارتباطات مطمئن وحفاظت به وسیله دیوار آتش یا VPN ها
- ✓ استفاده از رمز نگاری برای جلوگیری از کشف داده ها
- ✓ شناسایی ریسک ها، اهداف حمله کننده و ارائه راهکار های لازم
- ✓ محافظت فیزیکی از تمام تجهیزات گذرگاه ارتباطی که دارای تجهیز بیرونی هستند(جهت جلوگیری از حمله های مستقیم) و ایزوله کردن این تجهیزات از سایر تجهیزات سیستم کنترل اسکادا
- ✓ استفاده از ارتباط IPsec VPN برای حفاظت از ترافیک هایی که از مدیای ارتباطی با آسیب پذیری متوسط عبور می کنند
- ✓ استفاده از IPsec برای ایجاد تصدیق متقابل بین عوامل شروع کننده جلسه وانتقال کلید های رمز نگاری جلسه

- **امنیت پروتکل IEC 61850**: با توجه به استفاده روز افزون از این پروتکل در هوشمند سازی شبکه های قدرت در آینده نزدیک و وجود الزامات زمانی در شبکه های قدرت و الزامات امنیتی، امنیت این پروتکل باید به صورت ویژه مورد توجه قرار گیرد. بر اساس بررسی های انجام شده پیشنهادات ارائه شده به شرح ذیل می باشد:

- ✓ دقت و توجه به هشدار ها
- ✓ پاک کردن نرم افزار های بلا استفاده از سرور و سیستم کامپیوتری
- ✓ غیر فعال کردن سرویس های بلا استفاده
- ✓ پاک کردن دسترسی های بلا استفاده
- ✓ تغییر مرتب کلمه های عبور و کلمه عبور پیش فرض سیستم
- ✓ بررسی تنظیمات سیستم در زمان تست و راه اندازی
- ✓ استفاده از دیوار های آتش میزبان محور
- ✓ به روز رسانی مرتب نرم افزار ویروس یاب
- ✓ استفاده از فرآیند مدیریت و پشتیبانی پیوسته امنیت
- ✓ استفاده از رمز نگاری در پیام ها با شرط رعایت الزام زمانی
- ✓ مدیریت کلید
- ✓ استفاده از الگوریتم های امنیتی
- ✓ استفاده از VPN
- ✓ عدم اجازه اتصال به شبکه یا استفاده از حافظه های جانبی
- ✓ مدیریت و کنترل بیشتر پیمانکاران

یک نگرانی در رمزنگاری داده ها در پروتکل ۶۱۸۵۰ رعایت الزاما زمانی شبکه است. با توجه به الزام زمان ۳ میلی ثانیه برای پیام های GOOSE و ۸۳ میکرو ثانیه برای اندازه گیری SV در این پروتکل روش های رمز نگاری متفاوتی بررسی شده است و پیشنهادات نهایی بر اساس نتایج مشاهده شده به شرح ذیل می باشد:

روش اول:استفاده از کلید های درهم (HMAC) است. در این روش ابتدا فرستنده Aکد همگام C را به پیام اصلی A و کلید تصدیق KAB الحاق می کند. سپس MAC توسط تابع hash یک طرفه محاسبه می شودو H نامیده می شود. لازم به ذکر است که کد همگام عددی غیر نزولی است. سپس MAC جایگزین کلید تصدیق شده و پیام ارسال می شود. روش تکمیل پیام از A به B به شرح ذیل است:

$A \rightarrow B: <C \mid MA \mid MAC$ و $MAC = H(C \mid MA \mid KAB)$

روش دوم: از تابع hash با طول ثابت مقدار hash وبا طول رشته بیت ورودی اختیاری استفاده شده است. تابع Hash اختصاصی فقط برای انجام عملیات Hash پردازش های بهینه مورد استفاده قرار می گیرد و هرگز برای اجزاء سیستم موجود مانند بهره برداری مدولار توصیه نمی شود. تابع MD-4 برای نرم افزار CPU 32 بیت مورد استفاده قرار می گیرد. توابع

اختصاصی مانند MD-5،SHA-1وRIPEMD برپایه MD-4 طراحی شده اند. طول خروجی MD-5 و SHA-1 به ترتیب ۱۲۸ و۱۶۰ بیت است. الگوریتم رمز نگاری کلید عمومی RSA بر مبنای تجزیه اعداد اول کار می کند و باالگوریتم های کلید رمزی مانند DES به دلیل وجود طول کلید وplaintext متغیر متفاوت است. جدول ۳ سخت افزارهای استفاده شده در این دو روش و جدول ۴ زمان ارسال را ارائه کرده است

جدول ۳: مقایسه سخت افزارهای مورد استفاده

عنوان روش	CPU	Memory	HDD	OS
روش ۱	Intel Pentium 4 , 3 G Hz	1 G	80 G	Windows XP , SP2
روش ۲	Pentium III 700 MHz, 256KB cache	256MB	Linux kernel version 2.4.34,GCC version 3.2.2	Development Environment

جدول ۴: مقایسه زمان انجام کار

روش	طول پیام/ زمان			
	۹۶ بایت	۱۳۲ بایت	۶۲۰ بایت	۱۰۲۴ بایت
MD-5 hash	.....	407.7 usec	580.9 usec	742.41 usec
SHA-1 hash	.....	436.0 usec	644.0 usec	816.6 usec
RSA	.....	15212 usec	15518.2 usec	15704.3 usec
MD-5 & RSA	.....	15500.3 usec	15693.5 usec	15889.7 usec
SHA-1&RSA	.....	15714.9 usec	15969.7 usec	17450.6 usec
AES 256, MAC: …	5.38400 ms	....	....	....
AES 256, MAC: SEED	11.79450 ms	....	....	....
AES 256, MAC: MD5	7.23000 ms	....	....	....
AES 256, MAC: HMAC-MD5	9.15900 ms	....	....	....
SEED, MAC: …	5.36000 ms	....	....	....
SEED, MAC: AES 256	10.13950 ms	....	....	....
SEED, MAC: MDS	8.54600 ms	....	....	....
SEED, MAC: HMAC-MDS	11.66550 ms	....	....	....
…, MAC: MDS	2.82750 ms		....	....
…, MAC:HMAC-MDS	4.68950 ms	....	....	....

- **امنیت پروتکل IEC 60870**: در این پروتکل باید با از روش های امنیتی ارائه شده در IEC 62351 استفاده گردد. مستندات کمی در رابطه با امنیت سیستم های اسکادا وجود دارد. این مستندها تهدیدها و آسیب‌پذیری های سیستم ها را شناسایی و اقدامات امنیتی برای کاهش ریسک ها را پیشنهاد می کند. می توان الزامات NERC CIP را با الزامات تجهیزات مخابراتی ESP نگاشت داد که موارد اصلی آن به شرح ذیل می‌باشد:
  - ✓ ثبت وقایع و صدور اخطار برای امنیت سایبری
  - ✓ ممیزی امنیت
  - ✓ کنترل های تکنیکی قوی در نقاط تعامل برای اعتبار سنجی اطلاعات و مجوز دسترسی
  - ✓ نرم افزار های ویروس یاب، IDS و سایر ابزارهای پیش گیری و به روزرسانی آنها
  - ✓ سرویس ها و پورت های وضعیت نرمال و اورژانسی با قابلیت فعال وغیر فعال برای حالات خاص
  - ✓ به روز رسانی و اصلاح اقدامات امنیتی
  - ✓ استفاده از کلمه های عبور با تنوع کارکتر بالا و اجبار در استفاده از طول خاص برای کلمه عبور
  - ✓ لزوم دسترسی منابع برای هر روش امنیتی (بنابراین سطح بالای دسترسی برای تمام منابع الزامی است)
  - ✓ پاک کردن نرم افزارهای بلا استفاده از سرور و سیستم کامپیوتری
  - ✓ مدیریت پست LAN
  - ✓ مجوز سرور برای کنترل دسترسی
  - ✓ مدیریت کلید جلسه
  - ✓ مدیریت سیاست های امنیتی سرور
  - ✓ ممیزی سرور برای بررسی امنیت رخدادها
  - ✓ غیر فعال کردن سرویس های بلا استفاده
  - ✓ پاک کردن دسترسی های بلا استفاده
  - ✓ مدیریت IPSec VPN
  - ✓ تغییر مرتب کلمه های عبور
  - ✓ تغییر کلمه عبور پیش فرض سیستم ها
  - ✓ بررسی تنظیمات سیستم در زمان تست و راه اندازی
  - ✓ استفاده از فرآیند مدیریت و پشتیبانی پیوسته امنیت
  - ✓ عدم اجازه اتصال به شبکه یا استفاده از حافظه های جانبی
  - ✓ مدیریت و کنترل بیشتر پیمانکاران
  - ✓ حق دسترسی SSH و HTTPS
  - ✓ مدیریت SNMPV3
  - ✓ مدیریت لایه های انتقال و لینک
  - ✓ استفاده از رمزنگاری در پیام ها با شرط رعایت الزام زمانی
- **امنیت زیر ساخت‌های مخابراتی**: نیاز است امنیت را در زیر ساخت های مخابراتی پیاده سازی کرد. در این رابطه لازم است موارد ذیل رعایت شود:
  - ✓ استفاده از VPN
  - ✓ استفاده از دیوارهای آتش میزبان محور
  - ✓ استفاده از رمزنگاری در کانال‌های ارتباطی(مثل PLC)

- ✓ حفاظت فیزیکی از پست‌ها و مراکز اسکادا
- ✓ سنکرون‌سازی زمان سرو

۴- نتیجه گیری

برای طراحی سیستم‌های اسکادا و اتوماسیون پست نیاز است کلیه استانداردهای امنیتی که به صورت عمومی و تخصصی در بخش امنیت مخابرات تعریف شده‌اند لحاظ شود. برای لحاظ کردن این استانداردها نیاز است اصول امنیتی که در این مقاله به آن اشاره شده‌است لحاظ شود. همچنین باید برخی تفکراتی که در این مقاله به آن بعنوان تفکر اشتباه اشاره شده‌است، را در طراحی‌ها لحاظ نمائیم. اهداف امنیتی را تدوین کرده و در موارد خاص از رمزنگاری داده‌ها استفاده شود. همچنین باید راهکارهایی برای تشخیص نفوذ سیستم اندیشید. برای شناسایی این راهکارها نیاز است تست‌های تشخیص نفوذ را قبل از پیاده‌سازی و اجرای سیستم‌های مخابراتی انجام داد. باید لیست کامل از دارایی های سازمانی تهیه و ریسک‌های مربوط آن با تعیین اولویت هر ریسک مشخص گردد. در نهایت برای دارایی‌های ریسک‌پذیر روش‌های امنیتی ارائه شده در استانداردهای ذکر شده در این مقاله را اجرا کرد.

مراجع

[1] U.S. Nuclear Regulatory Commission. (2003) “NRC Information Notice 2003-14”,2003, http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/in200 314.pdf.
[2] Moore D, Paxson V, Savage S, Shannon C, Staniford S, Weaver N, “Inside the slammer worm. IEEE Security & Privacy”, Jul 2003.
[3] Moreira N, Molina E, Lázaro J, Jacob E, Astarloa A, “Cyber-security in substation automation systems”. Renewable and Sustainable Energy Reviews, Feb 2016.
[4] Homay A, Chrysoulas C, El Boudani B, de Sousa M, Wollschlaeger M. “A security and authentication layer for SCADA/DCS applications”, Microprocessors and Microsystems, Nov 2020.
[5] Dzung D, Naedele M, Von Hoff TP, Crevatin M, “Security for industrial communication systems”, Proceedings of the IEEE, May 2005.
[6] PROFINET Security Guideline, March 2005, www.profibus.com
[7] Sampaio D, Bernardino J. “Evaluation of Firewall Open Source Software”,WEBIST, Apr 2017 25 .
[8] Honar Pajooh H, Rashid M, Alam F, Demidenko S, “Multi-layer blockchain-based security architecture for internet of things”, Sensors, Jan 2021.
[9] “Cyber security for substation automation systems by ABB”, December 2010.