

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

فن آوری همواره در حال پیشرفت است. شرکت‌هایی موفق هستند که در تغییر مدل‌های کاری سازمان خود برای پذیرفتن فن آوری روز تلاش می‌کنند. سازمان‌هایی که تغییرات را نادیده گرفته و به وضع موجود پایبند باشند، منسوخ می‌شوند. زیر ساخت‌های 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 زیر ساخت‌های مخابراتی استفاده می‌کند 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 شده است. 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.

1- مقدمه

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 [1]. یکی دیگر از کرم های مشهور کامپیوتری استاکس نت است که توانست کنترل سیستم نظارتی نیروگاه هسته ای در ایران را مختل سازد [3].

اهمیت زیرساخت های حیاتی 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.

2- 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 [5].

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 عامل های تجاری، پیاده سازی پروتکل و برنامه های کاربردی ارتباطی با آسیب پذیری 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 2003، کرم غیرفعال کامپیوتری اسلمر بر سیستم نظارت ایمنی نیروگاه هسته ای دیویس در اوهایو تأثیر گذاشت و باعث خاموشی نیروگاه

1-2- 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.

2-2- 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 می شود تا حملات بی هدف خسارت های بیشتری به سیستم اعمال سازند. 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 استاکس نت 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 90 درصد میزبان های آسیب پذیر را آلوده ساخته و با ایجاد مانع در پاسخ گویی از سانی باعث ایجاد اختلالات قابل توجهی در مؤسسات مالی، حمل و نقل و مؤسسات دولتی می شود [2].

استاکس نت: اصطلاح کرم کامپیوتری استاکس نت توسط فرد کوهن در سال 1985 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 کاملاً متفاوتی نسبت به تعاریف کلاسیک دارد. پنهان شدن تا انتهای مأموریت از استراتژی های 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 می شود 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

می سازند 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 می کند. در دهه اخیر کمیسیون های 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 [3,4].

2-3- روش های رمزنگاری

الگوریتم های رمزنگاری به منظور ذخیره سازی 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 تکنیک های رمزنگاری امروزی، رمزنگاری با تکیه بر نگه 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 می توان 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 تواند منجر به مشکلات اضافی و مقیاس پذیری شود. یکی از کاربردهای این روش در اینترنت اشیا است [8].

2-4- امنیت در شبکه و پروتکل های ارتباطی

در شبکه های ارتباطی، اهداف امنیتی توسط پروتکل های امنیتی در لایه های مختلف شبکه ارتباطی فراهم می گردد. تاکید این پروتکل های امنیتی به محافظت در برابر حملات مبتنی بر شبکه بر روی لینک های ارتباطی است. سرویس های امنیتی ارائه شده توسط یک لایه خاص ارتباط بین نقاط ابتدایی و انتهایی مربوط به آن لایه را حفظ می کنند. در حال حاضر پروتکل های امنیت در شبکه و لایه انتقال به ترتیب IPsec¹ و SSL² هستند. رایج ترین پروتکل های امنیتی و خدمات آنها در جدول (1) ارائه شده است.

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

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 می کنند.

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 تأیید 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 [5-7]:

- 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 نامن
- ضبط اطلاعات مفید نظارت ترافیک و آشکارسازی ورودی های غیرمجاز
- **سیستم های تشخیص نفوذ:** هدف این سیستم ها، کشف حملات براساس پروفایل تهاجمی شناخته شده و یا رفتار غیرمعمول سیستم است. اطلاعات مورد نیاز سیستم های تشخیص نفوذ تحت شبکه از ترافیک

چالش/پاسخ استفاده می شد. همچنین پروتکل EAP یک چارچوب کلی برای احراز هویت تعریف می کند. لینک های بی سیم طیف کوتاه مانند بلوتوث یا شبکه های محلی بی سیم IEEE 802.11 بسیار آسیب 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 و IEEE 802.11i برای استفاده WLAN طراحی شده است.
- ✓ یک جایگزین برای تضمین عملیات WLAN، به کارگیری راه حل- های IPsec / VPN می باشد.

جدول (1): رایج ترین پروتکل های امنیتی [5]

| 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 | |
| Transport layer | HTTP | HTTP Digest Authentication | no | no ^a | user ^b | user-to-server |
| | TCP | SSH Transport Layer Protocol | yes | yes | server ^c | client(user)-to-server |
| Internet layer | IP | SSL/TLS | yes | yes | server ^d | client-to-server |
| | | IPsec | yes ^e | yes | host / host-to-host | host-to-host |
| Link layer | PPP | CHAP/PAP | no | no | client | end-point of link |
| | WLAN | Bluetooth Security | yes | yes | device | air interface |
| | | WEP/WPA/802.1X | yes | yes | device | |
| | IEEE802.11 | | | | | |

^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:** برای 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 در حالت AH)
 - ✓ درستی داده ها (در حالت ESP و AH)
 - ✓ کنترل دسترسی، با توجه به میزبان فردی (در ESP و AH)
- دو حالت برای IPsec با نام های AH و ESP وجود دارد که هر دو حالت را می توان با هم یا به تنهایی استفاده کرد. علاوه، تبادل کلید IPsec چارچوبی برای مدیریت کلید و امنیت جلسه (به عنوان مثال، کلید جلسه برای رمزنگاری متقارن) فراهم می کند. روش IPsec برای تصدیق هویت کاربران شخصی کاربرد ندارد. بنابراین، اغلب برای ایجاد شبکه های خصوصی مجازی (VPN ها) و تأمین امنیت بین میزبانان

• **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 می‌شود. بنابراین باید در مکانیزم‌های امنیتی حفاظت از داده از محل تولید تا مقصد در نظر گرفته شود.

• **دفاع عمیق:** دو دیدگاه اصلی برای امنیت فیزیکی و اطلاعاتی به نام‌های 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 بدخواهی‌های داخلی وجود دارد. در دیدگاه دفاع عمیق چندین ناحیه در اطراف کاندید مورد حفاظت قرار می‌گیرند که مکانیزم‌های متفاوتی برای حفاظت همزمان درون و اطراف ناحیه مذکور دارند. بخش بیرونی ناحیه از ارزش امنیتی کمتری برخوردار است و سیستم‌های اتوماسیون مهم در داخلی‌ترین بخش ناحیه قرار می‌گیرند.

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

3- امنیت برای پروتکل‌های 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.

3-1- امنیت مربوط به سیستم‌های مخابرات صنعتی

تفاوت‌های محسوسی بین سیستم‌های مخابرات صنعتی با سیستم‌های اداری، بازرگانی وجود دارد. این تفاوت‌ها و جدید بودن سیستم‌های اتوماسیون پست سبب می‌شود تا نتوان از امکانات امنیتی اداری تعریف شده، برای اتوماسیون پست‌ها استفاده کرد.

• **الزامات:** الزامات امنیتی سیستم‌های کنترل و اتوماسیون صنعتی با شبکه‌های IT سازمان‌ها و شرکت‌ها متفاوت است. در شبکه‌های صنعتی الزام ایمنی کارکنان و لزوم دسترسی پذیری (کار مداوم و عدم امکان خاموشی) وجود دارد. این الزام گاهی اوقات برای به کارگیری شیوه مدیریت استاندارد IT (مانند راه‌اندازی مجدد سیستم جهت رفع عیب) به عنوان مانع محسوب می‌شود. برای تمرکز روی امنیت سیستم‌های اتوماسیون پست‌ها باید تجهیزات اتوماسیون که تجهیزات مرزی (بیرونی ترین تجهیزات) سیستم محسوب می‌شوند (مانند PLC) از حملات

مشاهده شده در بخش شبکه به دست می‌آید. این اطلاعات شامل نوع، محتوا، فرکانس و مسیر انتقال پیام است. تشخیص نفوذ، مبتنی بر میزبان، از اطلاعات محلی میزبان برای کشف حملات استفاده می‌کند. میزبان‌های مرتبط با امنیت مانند دیوارهای آتش و سرورهای تشخیص نفوذ شبکه باید توسط یک سیستم تحت نفوذ مبتنی بر میزبان محافظت گردند.

5-2- بهترین استراتژی‌های معماری امنیت

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

• **سیاست‌های امنیتی:** بدون وجود سیاست صریح امنیتی قبل از شروع طراحی، احتمال به هدر رفتن تلاش‌های 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 سیاست‌های امنیتی تطبیق داده شود و تنظیمات و تغییرات مورد نیاز به سیستم اعمال گردد.

• **اهمیت دادن به ضعیف‌ترین 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 آسیب‌پذیری سیستم را به همراه دارد.

• **تفکر امنیت توسط گمنامی:** فروشنده‌گان و سازندگان ادعا می‌کنند که مهاجمین به دانش فنی دقیق و لازم برای بهره‌برداری از پروتکل‌های اختصاصی دسترسی ندارند، در نتیجه سیستم‌های اتوماسیون در برابر حملات الکترونیکی ایمن می‌باشند. در صورتی که این تصور کاملاً نادرست است و با توجه به گسترش اتوماسیون و آشنایی تعداد زیادی از کارشناسان با دانش این سیستم‌ها و دسترسی‌پذیری اطلاعات در استانداردها و سایت‌های اینترنتی، ابهامی وجود ندارد و سیستم‌ها به راحتی تحت حمله قرار می‌گیرند.

• **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 داده‌ها:** بسیاری از سیستم‌های اتوماسیون حاوی اطلاعاتی هستند که نباید توسط کاربران قابل مشاهده یا اصلاح باشد. برای حصول اطمینان از حفاظت داده‌ها می‌توان از رمزگذاری، توابع یک طرفه، سخت افزار و سرور امن استفاده کرد.

مشابه سیستم‌های مخابرات رادیویی استفاده کنند. جهت افزایش امنیت در سیستم‌های PLC استفاده از کارت‌های هوشمند و رمزنگاری پیشنهاد شده است.

3-4- امنیت مراکز کنترل و مخابرات صنعتی

الزامات زمان واقعی: وظیفه اصلی تجهیزات اتوماسیون صنعتی اندازه‌گیری و کنترل به صورت ادواری و در تاریخ‌های مشخص شده می‌باشد. ممکن است حمله‌کنندگان خارجی از واسط‌های مخابراتی برای حملات DOS استفاده کنند و با ایجاد ترافیک سنگین نرخ بالای وقفه در پردازش ترافیک داده را ایجاد کنند. از اینرو در طراحی‌ها باید انتخاب اولویت پیام‌ها برای کاهش آسیب‌پذیری حملات DOS در نظر گرفته شود.

محدودیت‌های پردازش و حافظه: محدودیت‌های پردازش و حافظه از جمله مشخصه‌های اصلی سیستم‌های تعبیه شده در مخابرات صنعتی است. در انتخاب ابزار رمزنگاری و پروتکل‌های امنیتی نظیر SSL و HTTP DA باید محدودیت‌های تجهیزات نصب شده در نظر گرفته شود. استفاده از رمزنگاری ECC به لحاظ کاهش حجم پردازش و زمان پردازش از رمزنگاری RSA مناسب‌تر می‌باشد.

انعطاف‌ناپذیری: کنترل‌کننده‌های اتوماسیون باید اغلب به صورت خودگردان عمل کنند و به صورت ویژه انعطاف‌ناپذیر باشند. همچنین باید در برابر حملات مقاوم و دارای قابلیت تصدیق برای فرامین و پیام‌های دریافتی، باشند. از طرفی ممکن است باتری این سیستم‌ها به وسیله انجام پردازش‌های غیر ضروری خراب یا تخلیه گردد که برای این منظور باید تدابیر امنیتی لحاظ شود.

4-4- پیشنهادات امنیتی

در این بخش به معرفی استانداردهایی با کاربردهای عمومی، زیرساختی، سخت‌افزاری و نرم‌افزاری و پروتکل‌های 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، IEC 60855، PCSRF، ISA SP99، AGA، IEC TC65، NERC 1200، FDA، IAONA و CIGRE برای سیستم‌های مخابرات صنعتی کاربرد دارند. تمرکز اصلی استانداردهای امنیتی در جدول 2 نمایش داده شده است.

محافظت کردند و برای دسترسی به آن‌ها باید تصدیق مشتری صورت پذیرد. در مقایسه با سیستم‌های اداری و بازرگانی که حفاظت از سرورهای مرکزی بسیار مهم است در سیستم‌های اتوماسیون حفاظت از تجهیزات مرزی اهمیت دارد.

• محیط عملیاتی: سیستم‌های اتوماسیون توسط یک تیم تخصصی متشکل از مجموعه‌ای از مهندسين و تکنسین‌ها در حال بهره‌برداری است. این گروه معمولاً کوچک و محدود می‌باشند که برای هر نفر یک نقش تعریف شده است. حذف و اضافه کردن اعضا یا تغییر در نقش‌ها و دسترسی‌ها محدود می‌باشد و نیاز به سیستم مدیریتی ندارد. بنابراین این سیستم‌ها در مقایسه با شبکه‌های بزرگ IT یا شبکه‌های Web، مدیریت نقش‌ها اهمیت کمتری دارد و نیاز به روش‌های مدیریتی اتوماتیک نمی‌باشد. پیکربندی و توپولوژی، سخت‌افزار و نرم‌افزار سیستم اتوماسیون دارای مشخصات خاص هستند. در نتیجه باید مکانیزم‌های حفاظت و آشکارسازی مناسب با سیستم باشد.

• چالش‌ها: تجهیزات اتوماسیون نسبت به کامپیوترهای رومیزی دارای قدرت پردازش پایین‌تری هستند ولی باید الزامات پاسخ به موقع (خیلی از مواقع در محدوده میلی یا چند ده میکروثانیه) را فراهم سازند. این الزامات کاربردی پروتکل‌های رمزنگاری را محدود می‌کنند. از طرفی دیگر با توجه به طول عمر زیاد سیستم‌های اتوماسیون (سیستم‌های قدیمی در شبکه که بر پایه امنیت توسط ابهام بنا شده‌اند و امکان استفاده از الگوریتم‌های حفاظتی را ندارند) باید راه حل امنیتی برای آن‌ها تدبیر کرد، که در نهایت اپراتورهای سیستم اتوماسیون و تکنسین‌های پست‌ها در بسیاری مواقع با ایجاد سیستم‌های جدید امنیتی و تغییرات مخالف هستند.

3-2- امنیت گذرگاه در سطح تجهیز

همان‌طور که می‌دانید پایین‌ترین لایه شبکه‌های مخابرات صنعتی شامل تجهیزات کاربردی مانند سنسورها، اندازه‌گیرها و سیستم‌های محرک می‌باشند و تعداد زیادی از سیستم‌های مخابراتی و پروتکل‌ها در این سطح قرار دارند. زمانی که نیاز به اتصال تعداد زیادی از تجهیزات اتوماسیون به کنترل‌کننده باشد، از گذرگاه استفاده می‌شود. ارسال داده‌ها با استفاده از سیم مسی، کابل کواکسیال و فیبرنوری انجام می‌گردد.

3-3- امنیت سیستم‌های PLC

یکی از کانال‌های مخابراتی صنعت برق خطوط انتقال هستند. با استفاده از خاصیت عدم تقارن و تطبیق امپدانس می‌توان سیگنال‌های مخابراتی جعلی در خطوط قدرت ایجاد کرد. بنابراین امکان استراق‌سمع با یک گیرنده رادیویی ساده که در مجاورت خط انتقال قرار دارد وجود دارد. سیستم‌های پیشرفته مخابرات روی خطوط قدرت باید از اقدامات امنیتی

جدول (2): تمرکز اصلی استاندارد های امنیتی [9]

| 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، سیستم‌های کنترل و حفاظت |
| IEEE 1686 | استاندارد برای امنیت سایبری تجهیزات هوشمند الکترونیکی پست‌ها |
| ISA S99 | اتوماسیون صنعتی و امنیت سیستم کنترل |

از آنجایی که پروتکل‌ها در سیستم‌های اسکادا و اتوماسیون پست‌ها از اهمیت خاصی برخوردار هستند، الزامات امنیتی در این پروتکل‌ها به شرح ذیل پیشنهاد می‌شود:

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

- ✓ استفاده از دیوار آتش
 - ✓ ایجاد مرکز کنترل صحت اسناد و مجوزها
 - ✓ استفاده از شبکه‌های خصوصی مجازی (VPNs)
 - ✓ ارزیابی امنیت
 - ✓ حفاظت از ویروس
 - ✓ ایجاد سیستم ثبت وقایع
 - ✓ شناسایی ریسک‌ها، اهداف حمله‌کننده و ارائه راهکارهای لازم
- 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 سیستم‌های فیزیکی محافظت نمی‌شوند و در صورت امکان رمز نگاری اطلاعات
- ✓ ایجاد ارتباطات مطمئن و حفاظت به وسیله دیوار آتش یا VPN ها
- ✓ استفاده از رمز نگاری برای جلوگیری از کشف داده‌ها
- ✓ شناسایی ریسک‌ها، اهداف حمله‌کننده و ارائه راهکارهای لازم
- ✓ محافظت فیزیکی از تمام تجهیزات گذرگاه ارتباطی که دارای تجهیز بیرونی هستند (جهت جلوگیری از حمله‌های مستقیم) و ایزوله کردن این تجهیزات از سایر تجهیزات سیستم کنترل اسکادا

- ✓ استفاده از ارتباط IPsec VPN برای حفاظت از ترافیک‌هایی که از مدیای ارتباطی با آسیب پذیری متوسط عبور می‌کنند
- ✓ 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 شبکه‌های قدرت در آینده نزدیک و وجود الزامات زمانی در شبکه‌های قدرت و الزامات امنیتی، امنیت این پروتکل باید به صورت ویژه مورد توجه قرار گیرد. بر اساس بررسی‌های انجام شده پیشنهادات ارائه شده به شرح ذیل می‌باشد:

- ✓ دقت و توجه به هشدارها
- ✓ 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 و ویروس یاب
- ✓ استفاده از فرآیند مدیریت و پشتیبانی پیوسته امنیت
- ✓ استفاده از رمز نگاری در پیام‌ها 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 اده‌ها در پروتکل 61850 رعایت الزامات زمانی شبکه است. با توجه به الزام زمان 3 میلی ثانیه برای پیام های GOOSE و 83 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 می‌باشد:

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

$$MAC = H(C | MA | KAB) \text{ و } A \rightarrow B: \langle C | MA | MAC$$

آسیب‌پذیری‌های سیستم‌ها را شناسایی و اقدامات امنیتی برای کاهش ریسک‌ها را پیشنهاد می‌کند. می‌توان 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
- ✓ کنترل‌های تکنیکی قوی در نقاط تعامل برای اعتبار سنجی اطلاعات و مجوز دسترسی
- ✓ نرم‌افزارهای ویروس یاب، IDS و سایر ابزارهای پیش‌گیری و به‌روزرسانی آنها
- ✓ سرویس‌ها و پورت‌های وضعیت نرمال و اورژانسی با قابلیت فعال و غیرفعال برای حالات خاص
- ✓ به‌روزرسانی و اصلاح اقدامات امنیتی
- ✓ استفاده از کلمه‌های 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 نرم‌افزارهای بلا استفاده از سرور و سیستم کامپیوتری
- ✓ مدیریت پست LAN
- ✓ مجوز سرور برای کنترل دسترسی
- ✓ مدیریت کلید جلسه
- ✓ مدیریت سیاست‌های امنیتی سرور
- ✓ ممیزی سرور برای بررسی امنیت رخدادها
- ✓ غیرفعال کردن سرویس‌های بلا استفاده
- ✓ پاک کردن دسترسی‌های بلا استفاده
- ✓ مدیریت IPsec VPN
- ✓ تغییر مرتب کلمه‌های عبور
- ✓ تغییر کلمه عبور پیش‌فرض سیستم‌ها
- ✓ بررسی تنظیمات سیستم در زمان تست و راه‌اندازی
- ✓ استفاده از فرآیند مدیریت و پشتیبانی پیوسته امنیت
- ✓ عدم اجازه اتصال به شبکه یا استفاده از حافظه‌های جانبی
- ✓ مدیریت و کنترل بیشتر پیمانکاران
- ✓ حق دسترسی SSH و HTTPS
- ✓ مدیریت SNMPv3
- ✓ مدیریت لایه‌های انتقال و لینک
- ✓ استفاده از رمزنگاری در پیام‌ها با شرط رعایت الزام زمانی

روش دوم: از تابع hash با طول ثابت مقدار hash و با طول رشته بیت ورودی اختیاری استفاده شده است. تابع Hash اختصاصی فقط برای انجام عملیات Hash پردازش‌های بهینه مورد استفاده قرار می‌گیرد و هرگز برای اجزاء سیستم موجود مانند بهره‌برداری مدولار توصیه نمی‌شود. تابع MD-4 برای نرم‌افزار 32 CPU بیت مورد استفاده قرار می‌گیرد. توابع اختصاصی مانند MD-5، SHA-1، RIPEMD بر پایه MD-4 طراحی شده‌اند. طول خروجی MD-5 و SHA-1 به ترتیب 128 و 160 بیت است. الگوریتم رمزنگاری کلید عمومی RSA بر مبنای تجزیه اعداد اول کار می‌کند و با الگوریتم‌های کلید رمزی مانند DES به دلیل وجود طول کلید و plaintext متغیر متفاوت است. جدول 3 سخت‌افزارهای استفاده شده در این دو روش و جدول 4 زمان ارسال را ارائه کرده است

جدول 3: مقایسه سخت‌افزارهای مورد استفاده

| عنوان روش | CPU | Memory | HDD | OS |
|-----------|----------------------------------|--------|--|-------------------------|
| روش 1 | Intel Pentium 4 , 3 G Hz | 1 G | 80 G | Windows XP , SP2 |
| روش 2 | Pentium III 700 MHz, 256KB cache | 256MB | Linux kernel version 2.4.34, GCC version 3.2.2 | Development Environment |

جدول 2: مقایسه زمان انجام کار

| روش | طول پیام/زمان | | | |
|------------------------|---------------|--------------|--------------|-------------|
| | 1024 بایت | 620 بایت | 132 بایت | 96 بایت |
| MD-5 hash | 742.41 usec | 580.9 usec | 407.7 usec | |
| SHA-1 hash | 816.6 usec | 644.0 usec | 436.0 usec | |
| RSA | 15704.3 usec | 15518.2 usec | 15212 usec | |
| MD-5 & RSA | 15889.7 usec | 15693.5 usec | 15500.3 usec | |
| SHA-1&RSA | 17450.6 usec | 15969.7 usec | 15714.9 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 روش‌های امنیتی ارائه شده در IEC 62351 استفاده گردد. مستندات کمی در رابطه با امنیت سیستم‌های اسکادا وجود دارد. این مستندات تهدیدها و

مراجع

- [1] U.S. Nuclear Regulatory Commission. (2003) NRC Information Notice 2003-14. [Online]. Available: <http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2003/in200314.pdf>
- [2] Moore D, Paxson V, Savage S, Shannon C, Staniford S, Weaver N. *Inside the slammer worm*. *IEEE Security & Privacy*. 2003 Jul;1(4):33-9.
- [3] Moreira N, Molina E, Lázaro J, Jacob E, Astarloa A. *Cyber-security in substation automation systems*. *Renewable and Sustainable Energy Reviews*. 2016 Feb 1;54:1552-62.
- [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*. 2020 Nov 15:103479.
- [5] Dzung D, Naedele M, Von Hoff TP, Crevatin M. *Security for industrial communication systems*. *Proceedings of the IEEE*. 2005 May 31;93(6):1152-77.
- [6] PROFINET Security Guideline, Order No: 7.002, March 2005, www.profibus.com
- [7] Sampaio D, Bernardino J. *Evaluation of Firewall Open Source Software*. In *WEBIST 2017* Apr 25 (pp. 356-362).
- [8] Honar Pajooh H, Rashid M, Alam F, Demidenko S. *Multi-layer blockchain-based security architecture for internet of things*. *Sensors*. 2021 Jan;21(3):772.
- [9] *Cyber security for substation automation systems by ABB*, December 2010.

امنیت زیر ساخت‌های مخابراتی: نیاز است امنیت را در زیر ساخت‌های 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 PLC³)
- ✓ حفاظت فیزیکی از پست‌ها و مراکز اسکادا
- ✓ سنکرون‌سازی زمان سرو

5- 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 شده است لحاظ شود. همچنین باید برخی تفکراتی که در این مقاله به آن بعنوان تفکر اشتباه اشاره شده است، 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 پیاده سازی و اجرای سیستم‌های مخابراتی انجام داد. باید لیست کامل از دارایی‌های سازمانی تهیه و ریسک‌های مربوط آن با تعیین اولویت هر ریسک مشخص گردد. در نهایت برای دارایی‌های ریسک پذیر روش‌های امنیتی ارائه شده در استانداردهای ذکر شده در این مقاله را اجرا کرد.

3 - Power line carrier

1 - Internet Protocol Security

2 - secure sockets layer