طراحی چارچوب امنیت سایبری در شبکه‌های بی‌سیم فضاپایه

سیده فاطمه ملک

کارشناس ارشد مهندسی فناوری اطلاعات- شبکه های کامپیوتری، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر، تهران

سیاوش خرسندی

دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر، تهران

چکیده

امروزه با استقرار تدریجی شبکه‌های بی‌سیم فضاپایه، که در نتیجه یکپارچگی و همگرایی ارتباطات ماهواره‌ای، اینترنت و شبکه‌های بی‌سیم موبایل و تلفن همراه می‌باشد، شاهد افزایش امکان ارائه اطلاعات و خدمات جامع و جهانی در هر زمان و هر مکان می‌باشیم، اما از منظر امنیتی، این یکپارچگی منجر به افزایش آسیب‌پذیری آنها در برابر حملات سایبری می‌شود. سوء استفاده از ویژگی پیکربندی راه دور مبتنی بر اینترنت، شنود یا مختل نمودن ارتباطات اینترنت ماهواره‌ای، جعل سیگنال‌ها، ایجاد اختلال در شبکه‌های تلفن همراه، از جمله حملات سایبری امکان‌پذیر در این نوع شبکه‌ها می باشند.

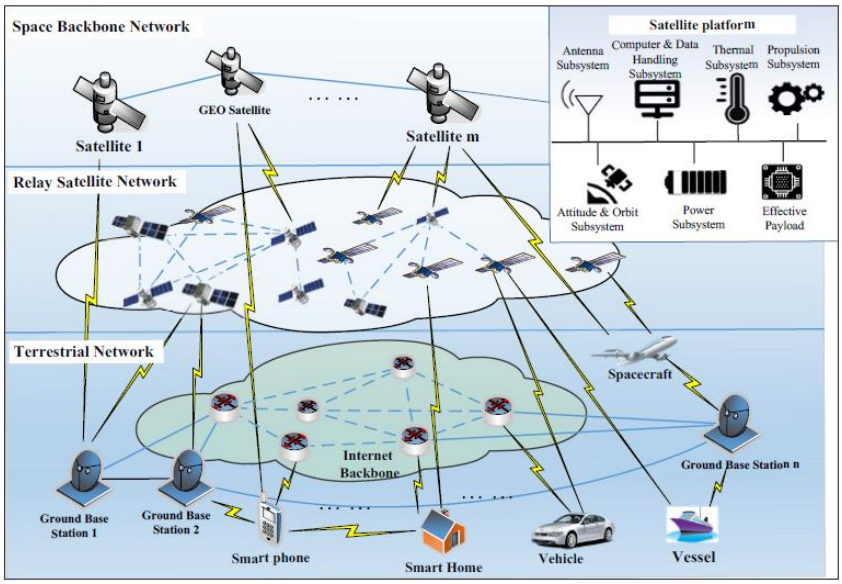
تاکنون اقدامات فنی زیادی در مورد ساختار، معماری و پروتکل های این نوع شبکه ها صورت گرفته و اکثر تحقیقات در حوزه بهبود کارایی و قابلیت اطمینان شبکه‌های بی‌سیم فضاپایه می باشند، در مقالات مربوط به حوزه تهدیدات و راهکارهای امنیتی نیز تنها بخشی از تهدیدات سایبری این نوع شبکه‌ها ارائه گردیده و دید جامعی از انواع تهدیدات سایبری شبکه‌های بی‌سیم فضاپایه و راهکارهای امنیتی موردنیاز مبتنی بر معماری آنها وجود ندارد. بر این اساس، در این مقاله، ضمن شناسایی معماری و احصاء دارایی‌های سایبری این نوع شبکه‌ها و تحلیل و طبقه بندی تهدیدات سایبری بر اساس تلفیقی از طبقه‌بندی تهدیدات انیسا و مدل تهدید استرید، به ارائه یک چارچوب جامع امنیت سایبری مبتنی بر استراتژی دفاع در عمق در شبکه‌های بی‌سیم فضاپایه پرداخته‌ایم.

واژگان کلیدی: تهدید سایبری، عوامل تهدید، حملات سایبری، ماهواره، آسیب پذیری

مقدمه

معماری کلی شبکه‌های بی‌سیم فضاپایه متشکل از شبکه ستون فقرات فضایی، شبکه ماهواره‌ای رله و شبکه زمینی می‌باشد (شکل ۱). شبکه ستون فقرات فضایی معمولاً شامل چندین ماهواره در مدار زمین است. شبکه ماهواره‌ای رله به ایجاد ارتباطات بین شبکه ستون فقرات فضایی و شبکه زمینی کمک می‌کند زیرا هر یک از ماهواره‌های آن امکان دسترسی به شبکه ستون فقرات فضایی را دارند (Daojing et al., 2019).

هر ماهواره دارای پیلود، تجهیزاتی برای انجام ماموریت‌ها و یک باس جهت نگهداری پیلود و بقیه سیستم‌های آن می‌باشد. سنجش از دور، ردیابی و فرماندهی، مدیریت دستورات و داده‌ها و کنترل و تعیین جهت، سه سیستم اصلی ماهواره‌ها هستند. این سیستم‌ها به ترتیب وظیفه دریافت و پردازش سیگنال‌های تبادلی بین ماهواره و زمین، اعتبارسنجی، دیکدینگ، ارسال دستورات به زیر سیستم‌های دیگر و ایجاد موازنه و کنترل جهت‌گیری ماهواره را بر عهده دارند. ارتباط با ماهواره‌ها از طریق امواج رادیویی و معمولاً در محدوده فرکانس مگاهرتز و گیگاهرتز برقرار می‌گردد (Ruan et al, 2018)



شکل ۱: معماری کلی شبکه‌های بی‌سیم فضاپایه

شبکه زمینی شامل ایستگاه‌های زمینی، ستون فقرات اینترنت و پایانه‌های کاربری مانند تلفن‌های هوشمند، وسایل نقلیه و کشتی‌ها است (Daojing et al., 2019). ایستگاه‌های زمینی با قابلیت‌هایی مانند سنجش از دور، ردیابی و فرماندهی، کنترل پیلود، اتصال سیستم‌های مختلف زمینی به یکدیگر و توزیع داده‌های جمع‌آوری شده، به عنوان عنصر اصلی شبکه زمین محسوب می‌شوند (Ruan et al, 2018).

پایانه‌های کاربری می‌توانند دستگاه یا رابطی باشند که از طریق دریافت مستقیم سیگنال‌های ماهواره یا تعامل با سایر سیستم‌ها یا برنامه‌های شبکه زمین، سرویس‌های مبتنی بر ماهواره را برای کاربران نهایی فراهم می‌نمایند. به عنوان نمونه، خدماتی از قبیل تلویزیون خانگی ماهواره‌ای و سیستم ناوبری ماهواره‌ای جهانی نیازمند دستگاه گیرنده اختصاصی (دیش ماهواره/گیرنده جی‌پی‌اس)، جهت دریافت سیگنال‌های پخش‌شده می‌باشند. در حالتی دیگر، کاربران نیازی به تجهیزات اختصاصی جهت دریافت سیگنال‌های

ماهواره‌ای ندارند، زیرا اپراتورهای ماهواره از طریق قابلیت‌های شبکه زمینی داده‌ها را برای کاربران خود منتشر می‌کنند. در واقع داده‌ها بعد از دریافت از طریق ایستگاه زمینی، به صورت متمرکز توسط سیستم‌های زیرساخت ابری، پردازش و از طریق ای‌پی‌آی‌ها و برنامه‌های مبتنی بر وب توزیع می‌شوند (Ruan et al, 2018).

در مقالات (Manulis et al, 2021)، (Jiao et al, 2017)، (Yao et al, 2019)، (Jin, Zhang, 2016) معماری شبکه‌های بی‌سیم فضاپایه، از نقطه نظر بهبود بازدهی و قابلیت اطمینان پروتکل‌های انتقال داده‌ها یا الگوریتم‌های مورد بررسی قرار گرفته‌اند، اما تهدیدات امنیت سایبری این نوع شبکه‌ها به طور جامع و سیستماتیک تجزیه و تحلیل نشده‌اند. در مقاله (Daojing et al., 2019)، ابتدا خلاصه‌ای از الزامات امنیتی شبکه‌های بی‌سیم فضاپایه ارائه و سپس سه روش حمله منع سرویس، مردمیانی و تغییر اطلاعات برای ماهواره‌های مبتنی بر گذرگاه MIL-STD-1553 شرح و در نهایت نیز برخی از مکانیسم‌های امنیتی پیشنهاد گردیده است.

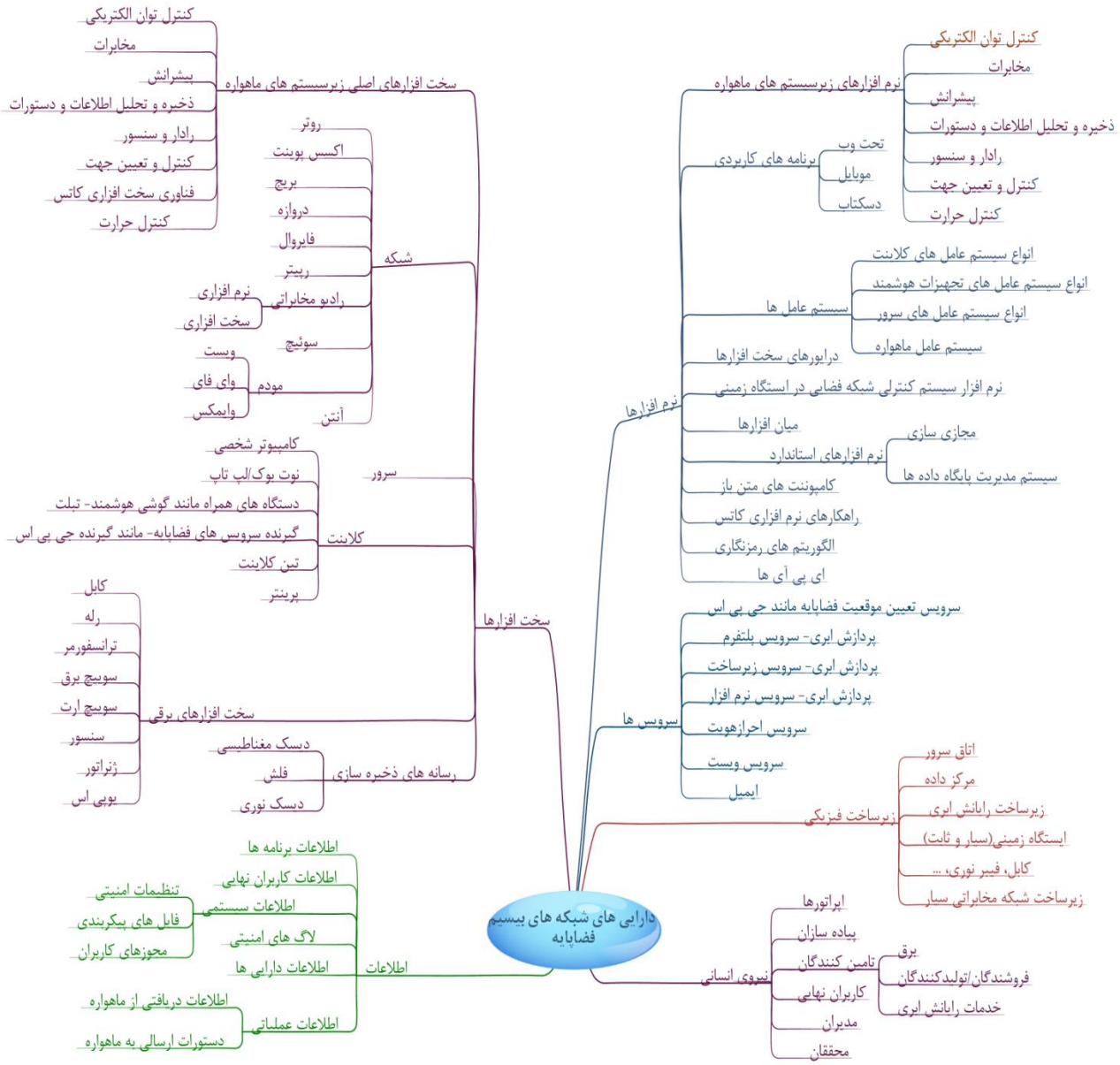
در مقاله (She1 et al, 2017)، یک روش بهبود یافته تشخیص کد مخرب بر اساس درخت هدف و سازگار با ویژگی‌ها و نیازهای امنیتی شبکه اطلاعات فضایی ارائه گردیده است. نتایج شبیه‌سازی حاکی از نرخ تشخیص بالا و مصرف کم منابع ماهواره است. از جمله نقاط ضعف این روش عدم تشخیص کدهای مخرب ایمپلنت در زیرسیستم ماهواره‌ها می‌باشد. در مقاله (Jiang et al, 2015) چالش‌ها، تهدیدات و راهکارهای امنیتی در شبکه‌های اطلاعاتی فضایی، تنها از چهار منظر انتقال امن، کنترل انتقال امن، مدیریت کلید و مسیریابی امن، بر اساس بررسی و مقایسه کارهای موجود، مورد بحث قرار گرفته است. در مقاله (Bradbury, et al, 2019) با ترسیم بلوک دیاگرام و ارتباطات داخلی و خارجی ماهواره‌ها با یکدیگر و با ایستگاه زمینی از دیدگاه عملیاتی، سطوح حمله استخراج و بر اساس مدل تهدید استرید، نمونه‌ای از درخت حمله منع سرویس ارائه شده است. اما در این پژوهش استخراج تهدیدات و سطوح حمله تنها در حوزه ماهواره و ایستگاه زمینی بوده و چالش‌های امنیتی در کل این نوع شبکه‌ها، نظیر تهدیدات در ارتباطات شبکه‌های زمینی، زیرساخت ابری، اینترنت اشیاء لحاظ نشده است. در مقاله (Bodeau, et al, 2018) طبقه‌بندی تهدیدات مبتنی بر مدل تهدید استرید، ارائه شده است که موید غلبه نگاه سیستمی بر دید جامع شبکه‌ای در این حوزه می‌باشد.

در ادامه این مقاله، بعد از ارائه نتایج بررسی معماری شبکه و طبقه‌بندی جامع از تهدیدات سایبری در شبکه‌های بی‌سیم فضاپایه، چارچوب امنیت سایبری مبتنی بر استراتژی دفاع در عمق ارائه می‌شود و در بخش آخر به ارائه نتایج و پیشنهادات می‌پردازیم.

احصاء دارایی های سایبری در شبکه های بی‌سیم فضاپایه

با توجه به بررسی‌های صورت گرفته بر روی معماری شبکه فضاپایه می توان این نوع شبکه ها را به سه لایه ایستگاه زمینی، زیرساخت‌های شبکه ارتباطی و ارائه سرویس (از جمله مراکز داده، زیرساخت ابری، اینترنت اشیاء و تلفن همراه) و لایه ماهواره تقسیم نمود.

بر اساس نتایج بررسی جزئیات معماری و احصاء دارائی‌های سایبری این نوع شبکه‌ها در شش دسته کلی نرم‌افزار، سخت‌افزار، زیرساخت فیزیکی، اطلاعات، سرویس‌ها و کاربران طبقه‌بندی و در شکل ۱ ارائه شده است.



شکل ۲: طبقه بندی و احصاء دارایی های سایبری شبکه های بی سیم فضاپایه

تحلیل و طبقه بندی تهدیدات سایبری در شبکه های بی سیم فضاپایه

در این بخش بر اساس تلفیقی از مدل طبقه‌بندی تهدیدات انیسا و مدل تهدید استرید و نگاشت آنها بر معماری و دارایی‌های سایبری شبکه‌های بی‌سیم فضاپایه، در شش حوزه اقدامات بدخواهانه، استراق سمع، خسارات غیرعمدی، تهدیدات فیزیکی، تهدیدات طبیعی و خرابی/اختلال صورت گرفته است، که در ادامه به تشریح آنها می‌پردازیم.

۱. اقدامات بدخواهانه/ سوءاستفاده از دارایی‌ها:

در این دسته از تهدیدات، عامل تهدید سیستم‌ها، زیرساخت‌ها و شبکه‌ها را با انجام اقدامات بدخواهانه و با هدف سرقت، اختلال، تغییر یا تخریب مورد حمله قرار می‌دهد. در ادامه به تشریح مهمترین موارد این نوع تهدیدات در شبکه‌های فضاپایه می‌پردازیم.

۱-۱- بهره‌برداری از آسیب‌پذیری‌ها

عامل تهدید می‌تواند با بهره‌برداری از آسیب‌پذیری‌های شناخته‌شده یا روز صفر موجود در دارایی‌های شبکه فضایی، زمینی یا کاربر نهایی حملات سایبری گسترده‌ای را انجام دهد، تخریب/ از دست دادن داده‌ها، از دست دادن کنترل یا کنترل غیرمجاز ماهواره، عدم موفقیت در ارسال و دریافت نتایج دستورات و داده‌ها می‌تواند از جمله پیامدهای آن باشد. به عنوان نمونه عامل تهدید با بهره‌برداری از آسیب‌پذیری سیستم کنترل‌کننده ماهواره در ایستگاه زمینی، می‌تواند فرماندهی و کنترل ماهواره را بدست آورد. مدارها را تغییر داده و حسگرهای ماهواره را کور یا داده‌ها را تغییر دهد.

شبکه زمینی آسیب‌پذیرترین نقاط شبکه‌های بی‌سیم فضاپایه را در بر دارد. عامل تهدید می‌تواند مشابه حمله به شبکه‌های سازمانی، با بهرگیری از تکنیک‌های مهندسی اجتماعی نظیر فیشینگ هدف‌دار، سوء استفاده از پیکربندی‌های اشتباه یا آسیب‌پذیری‌های فناوری‌ها، پروتکل‌ها، الگوریتم‌ها و سیستم‌ها به شبکه‌های زمینی نفوذ نماید(Manulis et al, 2021).

آسیب‌پذیری‌های برنامه‌های مبتنی بر وب که دسترسی از راه دور به ماهواره را تسهیل می‌کنند، یکی از نقاط ورودی اصلی عوامل تهدید در شبکه زمینی می‌باشند. در اکثر موارد عوامل تهدید از آسیب‌پذیری‌هایی نظیر عدم اعتبارسنجی ورودی/خروجی‌ها، عدم وجود مکانیزم‌های کنترل دسترسی، احراز هویت یا کنترل خطای امن و جامع، با هدف کسب اعتبارنامه کاربر، بهره‌برداری می‌نمایند. از جمله مزایای بدست آوردن اعتبارنامه کاربر مجاز، دستیابی به کنترل ماهواره و امکان ماندگاری در شبکه فضاپایه می‌باشد. تزریق اس‌کیوال و فیشینگ هدف‌دار از جمله حملات این حوزه می‌باشند.

استفاده از رایانش ابری، محاسبات لبه و اتصال به اینترنت، دسترسی به شبکه تلفن همراه، در زیرساخت شبکه‌های فضاپایه علیرغم افزایش مزیت‌های عملیاتی، منجر به افزایش آسیب‌پذیری در برابر حملات سایبری شده است(Khalil, et al. 2014) به عنوان مثال، عامل تهدید می‌تواند از ویژگی پیکربندی راه دور مبتنی بر اینترنت سوءاستفاده نماید تا کنترل ماهواره را بدست آورده و منجر به انجام اقدامی غیرعادی یا حتی انهدام ماهواره شود (Livingstone,2016)

شواهد موجود مبنی بر وجود آسیب‌پذیری در دارایی‌های شبکه فضایی نیز در سراسر جهان غیرقابل انکار است. عدم به‌روزرسانی یا وصله ناسازگار نرم‌افزاری، الگوریتم رمزنگاری و مدیریت کلید ضعیف، استفاده از پروتکل‌های ناامن، نرم‌افزارها و تجهیزات قدیمی از آسیب‌پذیری‌های کلیدی سیستم‌ها و شبکه‌های ماهواره‌ای می‌باشند. به عنوان نمونه، در بررسی امنیتی آی‌اواکتیو (Hudaib, 2016) رمزعبور ثبت شده در کد منبع، انتخاب رمزعبور ضعیف، وجود درپشتی‌ها، استفاده از پروتکل‌های ناامن، رایج‌ترین آسیب‌پذیری‌های میان‌افزاری در بسیاری از رادیوهای ستکام برآورد شده‌اند. هک ماهواره ایریدیوم نیز اهمیت توجه به این آسیب‌پذیری‌ها و تلاش در رفع آنها را نشان می‌دهد. این آسیب‌پذیری‌ها به راحتی اصلاح می‌شوند اما در صورت عدم کنترل، عامل تهدید می‌تواند با هزینه اندکی، حملات سایبری ویرانگری را انجام دهد.

بسیاری از سیستم‌های فضایی قبل از افزایش حملات سایبری طراحی شده‌اند. از این رو زیرسیستم‌های آنها به ویژه در برابر روش‌های جدید و پیچیده حملات سایبری آسیب‌پذیر هستند(Hudaib, 2016). سیستم‌های قدیمی ماهواره‌ها به راحتی به‌روزرسانی نمی‌شوند و باید آزمایش‌های قابل توجهی صورت پذیرد تا از عدم تداخل به‌روزرسانی‌ها با سایر عملکردهای حیاتی سیستم اطمینان حاصل شود. همچنین، به علت بعد مسافت و عدم دسترسی فیزیکی به دارایی‌های شبکه فضایی، انجام به‌روزرسانی میان‌افزارهای زیرسیستم‌های ماهواره، به دسترسی از راه دور نیاز دارد که باعث افزایش آسیب‌پذیری می‌گردد. در مجموع سیستم‌های فضایی همیشه آسیب‌پذیری‌هایی دارند که باید برطرف شوند(Hudaib, 2016)، (Manulis et al, 2020).

بهره‌برداری از آسیب‌پذیری‌های ماهواره‌های کوچک و کم‌هزینه که با استفاده از فناوری کاتس ساخته شده‌اند از دیگر نقاط ورودی عوامل تهدید در شبکه‌های فضاپایه می‌باشد. به عنوان نمونه عامل تهدید می‌تواند با بهره‌برداری از آسیب‌پذیری‌ها و بدست آوردن کنترل این نوع ماهواره‌ها، آنها را جهت برخورد با ماهواره‌های دیگر، هدایت نماید.

در واقع روند گسترش پرتاب این نوع ماهواره‌ها در مدار، به دلایل ذیل باعث افزایش سطح حمله دارایی‌های مستقر در مدار و زیرساخت‌های پشتیبانی زمینی شده است (Falco, 2018):

- با توزیع گسترده محصولات کاتس و افزایش دسترسی به اینگونه دستگاه‌ها، امکان استخراج آسیب‌پذیری‌های آنها توسط عامل تهدید، فراهم می‌گردد.
- محصولات کاتس باید به طور فعال نگهداری و به‌روزرسانی گردند، که اغلب توسط کاربران اعمال نمی‌شود.
- امکان مشارکت در ارتقاء کد و قراردادن درپشتی در آن توسط عامل تهدید، با توجه به ماهیت متن باز بودن کد و ای‌پی‌آی‌ها وجود دارد. این موضوع امکان دسترسی مخفیانه را فراهم می‌نماید.

تلفیق پیامدهای مربوط به آسیب‌پذیری‌های الکترومغناطیسی و سایبری در زمان عملیات نیز بسیار مهم است. به عنوان مثال عدم بررسی‌های کافی در پردازش فریم رادیو و ارسال بسته‌های داده نامناسب در زمان استفاده از رادیوی نرم‌افزاری و نرم افزار پردازش سیگنال دیجیتال، می‌تواند منجر به موفقیت در حمله سرریز بافر و مسدودی ارتباطات گردد. این نوع انسداد بسیار مخفیانه است زیرا تنها با ارسال تعداد کمی بسته تحریک می‌شود و نیازی به ارسال مداوم سیگنال رادیویی نیست. در واقع رادیوی نرم‌افزاری، علیرغم داشتن مزایایی نسبت به تکنیک‌های سخت‌افزاری، منشاء آسیب‌پذیری‌های نرم‌افزاری می‌باشد(Manulis et al, 2021).

۱-۲- دستکاری

عامل تهدید با دستکاری انواع سخت‌افزارها، ابزارها و اطلاعات می‌تواند یکپارچگی شبکه را به خطر بیندازد. دستکاری داده‌ها به معنای تخریب یا تغییر داده‌ها می‌باشد، که می‌تواند در حالت ذخیره، انتقال بین ایستگاه فضایی و زمینی یا انتقال در بین شبکه‌های زمینی یا در ماهواره و ایستگاه فضایی صورت پذیرد. تغییر یا تخریب فایل‌های رویدادنگاری، اطلاعات هویتی، دستورات ارسالی، اطلاعات دریافتی از ماهواره‌ها مانند اطلاعات موقعیتی و ایجاد داده‌های متناقض و انبوه، از جمله مصادیق دستکاری داده‌ها می‌باشند. به عنوان مثال، عامل تهدید می‌تواند با تغییر دستور ارسالی به ماهواره، باعث خارج شدن آن از مدار موردنظر، برخورد با اشیای فضایی و انهدام ماهواره گردد. در سال ۲۰۱۱، هکرها با سرقت ۱۵۰ اعتبارنامه کارمندان ناسا، کنترل عملیاتی کاملی بر آزمایشگاه پیشرانه جت آن بدست آوردند. آنها امکان اصلاح، کپی یا حذف پرونده‌های حساس، حساب‌های کاربری، بارگزاری ابزارهای هک و تغییر فایل‌های رویدادنگاری را داشته‌اند(Falco, 2018).

تغییر تنظیمات یا پنهان نمودن سخت‌افزار، برنامه‌های مخرب یا رخنه امنیتی در دستگاه، از مصادیق دستکاری سخت‌افزار و نرم‌افزار، می‌باشند، که در اکثر موارد با نفوذ عامل تهدید در زنجیره تامین صورت می‌پذیرد و در کلیه مراحل چرخه حیات محصول از مرحله پیاده‌سازی با انجام اقداماتی نظیر گنجاندن توابعی جهت دورزدن مکانیزم‌های رویدادنگاری، قرار دادن درپشتی تا مرحله نصب و نگهداری با استفاده از به‌روزرسانی‌های کنترل‌نشده، امکان‌پذیر می‌گردد.

به عنوان مثال، امکان استفاده از نرم‌افزارها یا سیستم‌عامل‌های شخص ثالث و/یا متن باز حاوی کد مخرب یا ایمپلنت ناشناخته، در ماهواره‌ها و فضاپیماها وجود دارد. با پیچیده‌تر شدن ماهواره‌ها و کاهش زمان‌بندی توسعه، ممکن است بررسی کمتری بر روی زنجیره تأمین نرم‌افزار اعمال شود.

زنجیره تأمین سخت‌افزاری یکی دیگر از نقاط ورود عامل تهدید می‌باشد. قرار دادن درب‌پشتی یا ایمپلنت در قطعات، تهدید قابل‌توجهی برای شبکه‌های فضایی است. در بهترین حالت، عامل تهدید اطلاعی از محل استفاده قطعه در سیستم نهایی ندارد و در بدترین حالت، ممکن است به زنجیره تأمین دسترسی داشته و با دانستن جزئیات روابط، قطعه‌ای از یک سیستم حیاتی را مورد هدف قرار دهد (Bailey et al, 2018)

مهندسی معکوس سخت‌افزارها و نرم‌افزارها جهت استخراج کدها، کلیدها و داده‌های برنامه، تغییر تنظیمات و بارگذاری مجدد آنها، از دیگر روش‌های دستکاری می‌باشد. دستکاری تنظیمات شبکه زمینی مانند دستکاری جداول مسیریابی، جعل داده‌های پیکربندی،

دستکاری دی‌ان‌اس، که در نتیجه سیاست‌های ناکافی در مدیریت و محافظت از داده‌های مهم پیکربندی صورت می‌پذیرد، بر محرمانگی و یکپارچگی آن تأثیر می‌گذارد و ممکن است منجر به رفتار غیرقابل پیش‌بینی و ایجاد دسترسی غیرمجاز به سیستم‌های مهم گردد. لذا کلیه زیرسیستم‌های ماهواره، تجهیزات کاربران نهایی و به خصوص دستگاه‌های موجود در اینترنت اشیا، مراکز پردازش داده، زیرساخت‌ها و سرویس‌های ابری و شبکه ایستگاه زمینی در معرض تهدید دستکاری می‌باشند.

۱-۳- کد/نرم‌افزار مخرب

تروجان‌ها، کرم‌ها، ویروس‌ها، جاسوس‌افزارها، روت‌کیت‌ها نمونه‌هایی از نرم‌افزارهای مخرب می‌باشند. کدهای مخرب امکان انجام اقدام غیرمجاز در زمان بهره‌برداری از آنها را برای عامل تهدید فراهم می‌نمایند. عامل تهدید می‌تواند سیستم‌ها، دستگاه‌ها و شبکه‌های سیستم‌های زمینی یا کامپیوتر ماهواره را به بدافزار یا کد مخرب آلوده نماید(Mazzolin, 2020), (Cohen, et al, 2014)

به منظور آلوده‌سازی سیستم‌ها معمولا از تکنیک‌های مهندسی اجتماعی مانند فیشینگ (ایمیل، پیامک، وب‌سایت)، انتشار فایل مخرب در اینترنت و شبکه‌های اجتماعی استفاده می‌شود (Manulis et al ,2021) به عنوان نمونه، دریافت به‌روزرسانی‌های رادیوی نرم‌افزاری از اینترنت، این فرصت را برای عامل تهدید فراهم می‌نماید که با استفاده از تکنیک‌های مهندسی اجتماعی، نرم‌افزارهای مخرب خود را به عنوان فایل اصلی، به کاربر ارائه نماید. متن باز بودن کد در فناوری کاتس و ای‌پی‌آی‌ها. امکان انتشار کد مخرب را برای عامل تهدید فراهم می‌نماید. استفاده از راهکارهای ابری و اینترنت اشیا نیز ضریب موفقیت عوامل تهدید در آلوده‌سازی سیستم‌های زمینی و اجرای حملات مبتنی بر باتها را افزایش داده است(Falco, 2018).

۱-۴- حملات منع سرویس

در حمله منع سرویس، امکان دسترسی کاربران مجاز به منابع و خدمات موجود با اختلال مواجه می‌شود. اتلاف منابع (مانند پهنای باند ارتباطی، ظرفیت پردازنده، فضای دیسک، حافظه)، اختلال در اجزای سیستم یا انسداد/اختلال در مسیرهای ارتباطی از مهمترین روش‌های این نوع حملات می‌باشند(Shah, et al, 2014). ناتوانی در فرماندهی و کنترل ماهواره، عدم امکان دستیابی به اطلاعات، تاخیر در انجام فعالیت‌ها در شبکه زمین و فضا به علت فقدان یا کمبود منابع سیستمی، از جمله پیامدهای حملات انکار سرویس می‌باشند. در ادامه به بیان نمونه‌هایی از امکان انجام منع سرویس در سیستم‌های شبکه فضایی، زمینی و لینک‌های ارتباطی می‌پردازیم.

عامل تهدید می‌تواند از جمینگ یا تداخل، به منظور ایجاد اختلال در لینک‌های ارتباطی بین ایستگاه زمینی و ماهواره یا برعکس، استفاده نماید(Ibrahim, et al, 2016). کلیه سیستم‌های ارتباطی بی‌سیم در معرض تداخل الکترومغناطیسی یا جمینگ هستند. تنها نکته مهم در رابطه با این آسیب‌پذیری، درجه حفاظت طراحی‌شده در سیستم ارتباطی برای مقابله با سناریوهای خاص تداخل یا جمینگ است. البته در سرویس‌های ماهواره‌ای، مسدود نمودن ارتباطات به سمت ماهواره، منجر به مختل شدن خدمات برای کلیه کاربران منطقه تحت پوشش ماهواره می‌گردد، اما مسدود کردن ارتباطات به سمت زمین یک اثر محلی برای کاربران خاص آن ارتباط را دارد، مانند جمینگ جی‌پی‌اس.

در حوزه منع سرویس در زیرسیستم‌های شبکه فضایی، می‌توان به سنسورها اشاره نمود که یکی از کامپوننت‌های اصلی ماهواره‌ها در جهت جمع‌آوری اطلاعات مربوط به ماهواره، محیط و سایر اطلاعات مورد نظر می‌باشند. این اطلاعات معمولاً قبل از انتقال به زمین برای تحلیل بیشتر، به صورت محلی ذخیره می‌شوند. سیستم فضایی آینده ممکن است از این اطلاعات برای هدایت و تصمیم‌گیری مستقل استفاده نماید. این بخش مستعد منع سرویس از طریق کور کردن موقت یا دائمی سنسورها می‌باشد.

در سال ۱۹۹۸، هکرها با بدست آوردن کنترل ماهواره نجومی ROSAT، صفحات خورشیدی آن را مستقیماً به سمت خورشید قرار داده و باتری را بیش از حد شارژ نمودند که باعث گردید سرویس‌دهی ماهواره مختل شود (Kallender, 2014).

زیرساخت محاسباتی در شبکه زمینی، از ذخیره‌سازی تا پردازش داده‌ها، بر اساس راهکارهای ابری صورت می‌پذیرد. اختلال در

زیرساخت‌های ابری، می‌تواند تاثیرات فاجعه‌باری در ایستگاه زمین مانند منع سرویس برای گیرنده ماهواره یا اختلال در عملکرد صحیح سیستم‌های بلادرنگ مبتنی بر ماهواره را به همراه داشته باشد(Masdari, et al., 2016). از طرفی عامل تهدید می‌تواند از منابع محاسباتی زیرساخت ابری در راستای اجرای حملات منع سرویس استفاده نماید.

۱-۵- جعل

عامل تهدید می‌تواند با استفاده از تکنیک‌های مختلف، کاربر، دستگاه یا برنامه‌ای غیرمجاز را در قالب یک کاربر، دستگاه یا سرویس مجاز در شبکه استتار و معرفی نماید تا یک مزیت غیرمجاز را بدست آورد. به عنوان مثال، عامل تهدید می‌تواند از آدرس آی‌پی جعلی برای رسیدن به اهداف خود کمک بگیرد. ایمیل‌های جعلی ارسال نماید یا اقدام به راه‌اندازی وب‌سایت‌های جعلی به منظور جذب کاربران و سرقت اطلاعات حساب کاربران کند. از جعل می‌توان برای دستیابی به اطلاعات شخصی یک هدف، گسترش بدافزار از طریق لینک‌ها یا پیوست‌های آلوده، دور زدن کنترل‌های دسترسی یا توزیع مجدد ترافیک جهت منع سرویس استفاده نمود.

گروه جاسوسی سایبری تورلا، با نفوذ به مراکز ارائه‌دهنده اینترنت ماهواره‌ای و استفاده از آنتن زمینی، آدرس آی‌پی کاربران اینترنت ماهواره‌ای را شناسایی و ارتباطات خودرا از آن آدرس آغاز می‌نمودند. در واقع با جعل آدرس آی‌پی کاربر اینترنت ماهواره‌ای، عملیات خود را پنهان کردند(Falco, 2018).

جعل سیگنال به عنوان یکی از انواع جعل در شبکه‌های فضاپایه مطرح می‌باشد. در این حمله، که فراتر از جمینگ بوده، گیرنده باید به عملکرد صحیح خود ادامه دهد و از طرفی سیگنال‌های جعلی باید علاوه بر مسدود نمودن سیگنال موردنظر، غیرقابل تمایز از آن نیز باشند (Jasani, 2016). جعل جی‌پی‌اس یکی از نمونه‌های جعل سیگنال بوده و یکی از روش‌های انجام آن استفاده از جعل‌کننده نرم افزاری است، به این صورت که با وارد نمودن یک سیگنال جعلی و به سختی قابل تمایز، در پشت سیگنال واقعی، حمله آغاز می‌شود و به تدریج قدرت سیگنال جعلی افزایش می‌یابد تا جاییکه گیرنده، سیگنال جعلی را به عنوان سیگنال واقعی می‌پذیرد.

یکی از وظایف مهم ایستگاه زمین به عنوان مرکز اصلی وی‌ست، اطمینان از مجاز بودن کاربران متصل به ترمینال‌های شبکه زمینی می‌باشد. لذا قبل از تخصیص پهنای باند پویا به ترمینال‌های این نوع شبکه‌ها، داده‌های کنترلی به ترمینال‌ها ارسال می‌گردد. چنانچه عوامل تهدید بتوانند اطلاعات ترمینال وی‌ست را بدست آورده و شناسه دستگاه را جعل نمایند، می‌توانند دستگاه جعلی خود را وارد شبکه کنند.

۲- استراق سمع/رهگیری

این گروه از تهدیدات به عنوان اقداماتی با هدف شنود، قطع یا کنترل ارتباط شخص ثالث بدون رضایت و اطلاع وی، تعریف می‌شوند. اطلاعات ارسالی در ارتباطات بین شبکه فضایی و زمینی یا بین شبکه‌های زمینی مستعد شنود، رهگیری، ضبط و پخش مجدد می‌باشند. به عنوان نمونه اگر داده‌های ارسالی، فرمان تغییر جهت ماهواره باشد و مجددا نیز ارسال شود، می‌تواند منجر به انجام عملیات تکراری گردد که نتیجه آن قرار گرفتن آنتن ماهواره در جهت اشتباه است.

اکثر پروتکل‌های ارتباطی ماهواره‌ای در راستای کاهش مصرف منابع و افزایش سرعت انتقال، سبک طراحی شده‌اند. حتی در مواردی که از رمزگذاری استفاده می‌شود، در شرایط اضطراری، حفظ ارتباط بدون رمزنگاری ارجحیت دارد (Manulis et al, 2021). به عنوان نمونه، در اکثر موارد ترافیک اینترنت ماهواره‌ای به‌منظور تسریع در انتقال داده‌ها رمزگذاری نمی‌شود و لذا سرقت اطلاعات را برای هکرها تسهیل می‌کند. محققان دانشگاه آکسفورد، از یک دیش و گیرنده‌ای که برای دریافت تصاویر ویدئویی شبکه‌های ماهواره‌ای به‌کار می‌رود، برای دسترسی به اطلاعات اینترنت ماهواره‌ای استفاده کردند. آن‌ها بعد از جستجو در وب و یافتن موقعیت ماهواره هدف، با قرار دادن دیش در جهت مناسب و اعمال تنظیمات موردنیاز در نرم‌افزار ضبط سیگنال‌های ماهواره‌ای، ذخیره‌سازی ترافیک اینترنت ماهواره‌ای را آغاز و سپس بر روی یک تلویزیون مشاهده نمودند.

انواع شبکه‌های موجود در ایستگاه زمین و بخش کاربر از جمله شبکه‌های سیمی، سلولار، وای‌فای، وی‌ست، ویپ[1]، زیرساخت‌های ابری نیز مستعد شنود ترافیک، تحلیل ترافیک، سرقت نشست، حمله مردمیانی، پخش مجدد و تغییر مسیر ترافیک، می‌باشند. به عنوان نمونه، گروهی از هکرهای رومانیایی داده‌های حساس شبکه ناسا و آژانس فضایی اروپا را به منظور فروش داده‌ها در بازار سیاه سرقت و سرانجام اکثر آنها را در اینترنت منتشر نمودند(Falco, 2018).

۳- تهدیدات فیزیکی

اقداماتی با هدف تخریب، افشاء، تغییر، غیرفعال نمودن، سرقت یا دستیابی غیرمجاز به دارایی‌های فیزیکی مانند زیرساخت‌ها، سخت‌افزار یا لینک‌های ارتباطی، در این گروه از تهدیدات قرار می‌گیرند. این نوع اقدامات از نوع سایبری نمی‌باشند، اما می‌توانند باعث قطع یا اختلال در سیستم‌ها و خدمات سایبری یا نقض محرمانگی اطلاعات شبکه‌های فضاپایه گردند.

۳-۱- سرقت/ دسترسی فیزیکی غیرمجاز به تجهیزات

سرقت یا دسترسی فیزیکی غیرمجاز به ایستگاه زمینی و سایر دارایی‌ها، می‌تواند ایستگاه زمینی را از کار بیندازد و مستقیماً بر ماموریت و خدمات شبکه‌های فضاپایه تأثیر بگذارد. به عنوان نمونه، هکرها با سرقت نوت‌بوک ناسا و دستیابی به الگوریتم‌های کنترلی توانستند کنترل ایستگاه فضایی بین‌المللی را بدست آورند.

۳-۲- ورود تجهیزات غیرمجاز

ورود تجهیزاتی غیرمجاز مانند رسانه‌های ذخیره‌ساز در زیرساخت‌های ایستگاه زمینی می‌تواند منشا حملات بدافزاری باشد. این ضعف امنیتی در مورد بدافزار استاکس‌نت استفاده شده است(Kallender, 2014).

۳-۳- تخریب زیرساخت‌ها و تجهیزات زمینی

ایستگاه‌های زمینی در معرض حملات فیزیکی می‌باشند، اقداماتی که عوامل تهدید داخلی یا خارجی با هدف تخریب و از کارانداختن سیستم‌ها و زیرساخت‌ها انجام می‌دهند و باعث ایجاد اختلال و عدم دسترسی به خدمات در شبکه‌های فضاپایه می‌شوند. آنتن‌های ایستگاه زمین مشهودترین و آسیب‌پذیرترین اجزای ایستگاه‌های زمین در برابر حمله فیزیکی هستند. تخریب زیرساخت‌های پشتیبان سیستم‌های این نوع شبکه‌ها مانند شبکه برق نیز دارای پیامدهای مشابه در وضعیت کنترل سیستم‌ها و اطلاعات این نوع شبکه‌ها می‌باشد.

۳-۳- برخورد ماهواره‌ها در فضا

هر ماهواره‌ای با توانایی تغییر مدار، می‌تواند یک سلاح فضایی محسوب شود. در صورت تغییر مدار یک برخورد رخ می‌دهد، یکی از ماهواره‌ها منهدم و بقایای فضایی ایجاد می‌گردد که در آینده، تهدیدهای زیادی برای ماهواره‌های دیگر ایجاد می‌کند. با توجه به روند افزایشی تعداد ماهواره‌ها، احتمال برخورد آنها با زباله‌های فضایی بیشتر و با افزایش تراکم زباله‌های فضایی به صورت آبشاری، افزایش برخوردها را خواهیم داشت (Oakley, 2020)

۳-۴- استفاده از تسلیحات ضدماهواره‌ای

در حوزه حملات فیزیکی به شبکه فضایی، که عمدتا توسط عوامل تهدید دولتی و یا تروریست‌ها قابل انجام می‌باشد، تسلیحات انرژی مستقیم، موشک‌های ضدماهواره، انفجار هسته‌ای در فضا و تهدیدات مداری، در راستای قطع ارتباط، تخریب یا آسیب رساندن به ماهواره‌ها و حسگرهای آنها مورد استفاده قرار می‌گیرند.

۴- خسارات غیرعمدی

سوءاستفاده عامل تهدید از اقدامات و خطاهای غیرعمدی عامل انسانی، که دارای پیامدهایی مانند نشت اطلاعات، از دست دادن کنترل ماهواره، شکست ماموریت می‌باشد، در این دسته از تهدیدات قرار می‌گیرد مانند:

[1] VOIP

- نشت/اشتراک اطلاعات به دلیل خطای انسانی
- از دست دادن داده‌ها در اثر حذف ناخواسته
- سوء استفاده از طراحی و برنامه‌ریزی ناکافی یا عدم تطابق: سطح پیچیدگی سیستم‌های فضایی، دستیابی به معماری بهینه، رویه‌های امنیتی و عملیاتی کافی را دشوار نموده و می‌تواند منجر به طراحی، اجرا و پیاده‌سازی ضعیف گردد. سیستم یا شبکه منسوخ‌شده ناشی از عدم به‌روزرسانی یا مدیریت وصله، خطاهای ناشی از عدم مدیریت تغییر پیکربندی، نقص طراحی شبکه و معماری سیستم فرصت‌هایی را برای بهره‌برداری عوامل تهدید فراهم می‌آورد. به عنوان مثال، در آوریل ۲۰۰۸، هکرها با قرار دادن تروجانی در رایانه‌های مرکز فضایی جانسون، به لینک اتصال به ایستگاه فضایی بین‌المللی دسترسی یافتند و برخی از عملیات‌های داخل هواپیما مانند ایمیل را مختل کردند. علت موفقیت عدم به‌روزرسانی سیستم‌عامل بوده است (Fritiz BS, 2013)
- سوءاستفاده از پیکربندی اشتباه یا ضعیف سیستم‌ها/شبکه‌ها: در صورت عدم پیکربندی صحیح زیرسیستم‌ها و تجهیزات شبکه، فرصتی برای عامل تهدید فراهم می‌گردد، تا به دارایی‌های حیاتی دسترسی یافته یا حمله‌ای را انجام دهد. این تهدید در اکثر موارد، دلیل اصلی وقایع امنیتی بوده است.
- سوءاستفاده از مدیریت اشتباه شبکه، سیستم‌ها و دستگاه‌ها: خطاهای ناشی از مدیریت ضعیف و اشتباه در زیرسیستم‌های فضایی می‌تواند منجر به نقض محرمانگی، یکپارچگی یا دسترس‌پذیری گردد. فقدان فرآیندها و رویه‌های عملیاتی، فقدان لاگ‌های ممیزی جهت انجام کنترل‌های موردنیاز از مصادیق مدیریت اشتباه هستند.

۵- تهدیدات طبیعی

پدیده‌های طبیعی مانند زلزله، سیل، طوفان، به علت ماهیت و تاثیرات تخریبی و قطع‌کنندگی، می‌توانند سبب بروز حوادثی به ویژه در امکانات و تسهیلات زیرساخت‌های شبکه زمینی و ترمینال‌های کاربران گردند.

در شبکه فضایی نیز آنتن‌ها به علت برجستگی از سطح ماهواره، یکی از آسیب‌پذیرترین اجزای آن هستند. به عنوان نمونه، برخورد شهاب سنگ‌ها یا ذرات پرانرژی ناشی از انفجارهای شدید خورشیدی، منجر به آسیب آنتن‌ها می‌گردند (Oakley, 2020)

البته ممکن است در شرایطی که زیرساخت شبکه فضاپایه مستقیما آسیبی ندیده باشد، تأمین خدمات شبکه فضاپایه تحت تأثیر قرار گیرند (مانند قطع برق به علت زلزله)، در نمونه‌ای دیگر، در ارتباطات دریایی جهت همگام‌سازی زمان از جی‌پی‌اس استفاده می‌شود. اما زمانبندی جی‌پی‌اس در شرایط بد آب و هوایی آسیب‌پذیر بوده و ممکن است در طوفان‌های شدید مختل شود.

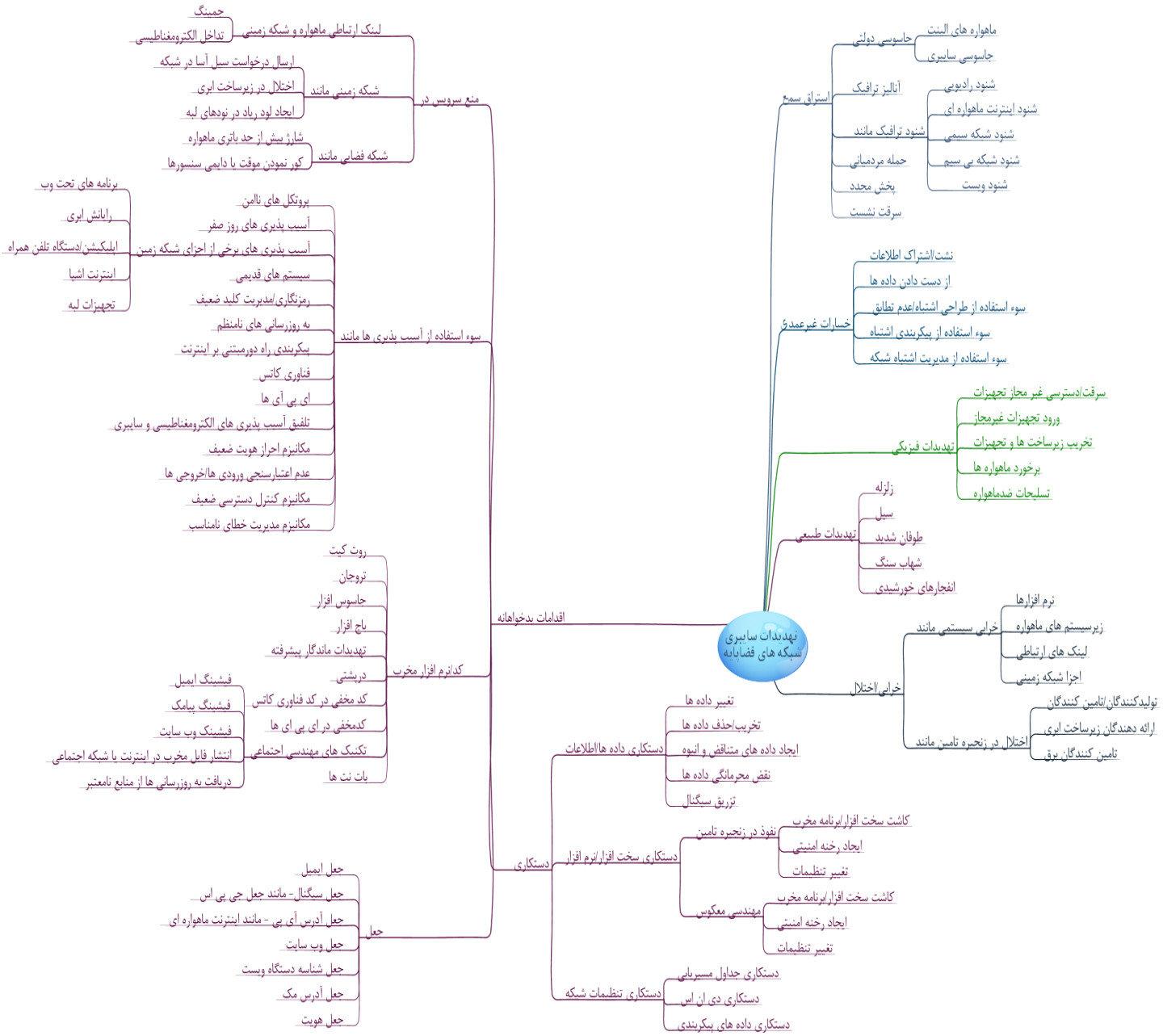
۶- خرابی یا اختلال

خرابی جزئی یا کامل در عملکرد اصلی دارائی‌ها، در این دسته از تهدیدها تعریف می‌گردد، که شامل دو زیربخش اختلال سیستمی و اختلال زنجیره تامین می باشد.

خرابی در بخش‌های مختلف شبکه‌های فضاپایه می‌تواند منجر به عدم دریافت خدمات موردنظر گردد.

خرابی/اختلال در نرم‌افزار مانند نرم‌افزار پردازش اطلاعات دریافتی از ماهواره، در زیرسیستم‌های ماهواره مانند ذخیره‌ساز اطلاعات در ماهواره، در لینک‌های ارتباطی مانند اختلال در آنتن‌های گیرنده و فرستنده، کابل‌های ارتباطی یا در اجزاء شبکه زمینی مانند روتر، سرورها، مراکز ذخیره داده، نمونه‌هایی از خرابی‌های سیستمی می باشند.

اختلال در زنجیره تأمین دارایی‌های شبکه فضایی به دلیل پیچیدگی در توسعه، مدیریت، استفاده و مالکیت آنها، خارج از کنترل مستقیم بهره‌بردار می‌باشد. از آنجائیکه قطعات تخصصی موردنیاز دارایی‌های فضایی توسط یک تولیدکننده ساخته نمی‌شود، اینکه چه کسی باید از نظر عملیاتی و مالی مسئول امنیت سایبری یک سیستم در چرخه حیات دارایی فضایی باشد، چالش برانگیز است. همچنین افزایش ارتباطات در زنجیره تامین باعث افزایش آسیب‌پذیری این حوزه شده است (Falco, 2018). علاوه بر تأمین‌کنندگان



زیرسیستم‌های شبکه فضایی، ارائه‌دهندگان خدمات ابری، خدمات شبکه، تأمین‌کنندگان برق از جمله عناصر موثر در زنجیره تامین هستند.

در شکل ۳، شمای کلی از طبقه بندی تهدیدات سایبری شبکه های بیسیم فضاپایه ارائه شده است:

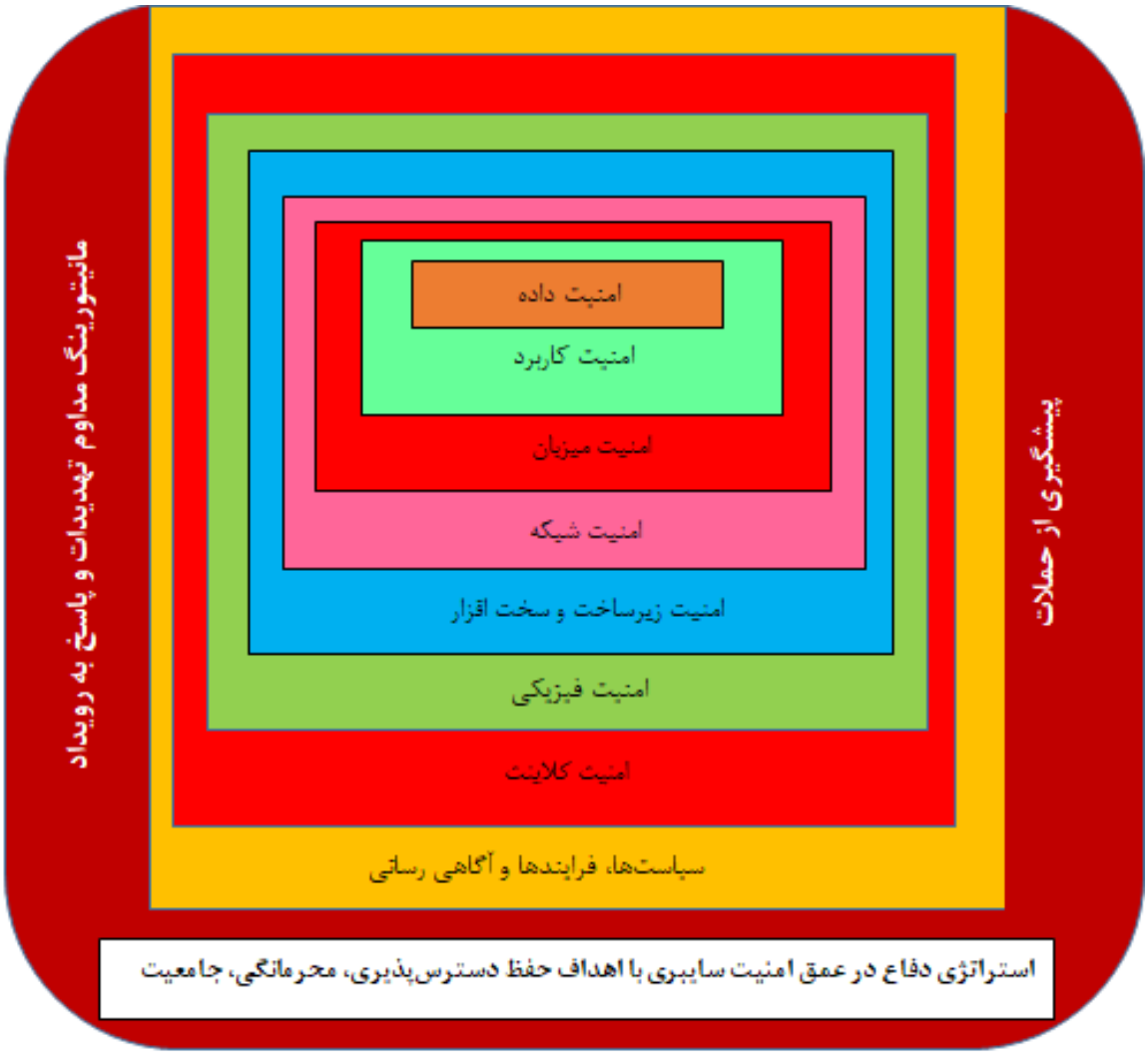
شکل ۳: طبقه بندی تهدیدات سایبری شبکه های بی سیم فضاپایه

طراحی چارچوب جامع امنیت سایبری در شبکه های بی‌سیم فضاپایه

با توجه به بررسی‌های صورت گرفته بر روی معماری و احصاء دارایی‌های سایبری، معماری شبکه فضاپایه به سه لایه ایستگاه

زمینی، زیرساخت‌های شبکه ارتباطی و ارائه سرویس (از جمله مراکز داده، زیرساخت ابری، اینترنت اشیاء و تلفن همراه) و لایه ماهواره تقسیم گردید. هر یک از لایه های مذکور دارای دارایی‌های سایبری داده/اطلاعات، نرم افزار/میان افزار، سخت افزار، شبکه و ارتباطات، نیروی انسانی می باشند.

با تلفیق نتایج احصاء دارایی‌ها و تحلیل تهدیدات سایبری شبکه‌های فضاپایه، این نتیجه حاصل گردید که یک محصول، فناوری یا راه حل امنیتی نمی‌تواند به تنهایی از این نوع شبکه محافظت نماید و اتخاذ استراتژی دفاع در عمق و چند لایه شامل دو (یا بیشتر) مکانیزم امنیتی همپوشان متفاوت، روشی که به آن عمق دفاع نیز گفته می‌شود، جهت کاهش تأثیر شکست هر مکانیزم امنیتی در طراحی چارچوب جامع امنیت سایبری ضروری می باشد. بر این اساس لایه‌های امنیتی مورد نظر مبتنی بر دارایی‌های سایبری این نوع شبکه ها، در شکل ۴ مشخص شده‌اند.



شکل ۲: لایه های امنیتی چارچوب امنیت سایبری شبکه های فضاپایه

در نهایت با نگاشت لایه‌های امنیتی به هر از دارایی‌های سایبری لایه‌های اصلی شبکه، راهکارها و اقدامات امنیتی هر بخش مبتنی بر تحلیل تهدیدات سایبری استخراج و ارائه گردیده است (جدول ۱)

جدول ۱: چارچوب جامع امنیت سایبری شبکه های بی‌سیم فضاپایه

لایه امنیتی	راهکارها و اقدامات امنیتی	لایه های شبکه بی‌سیم فضاپایه		
		ایستگاه زمینی	زیرساخت و شبکه سرویس‌دهی	ماهواره
امنیت داده	تحلیل امنیتی و مقاوم‌سازی سیستم مدیریت پایگاه داده	✓	✓	
	رمزنگاری (مکانیزم‌های مدیریت امن کلید، امضای دیجیتال، هشینگ، گواهینامه معتبر و ...)	✓	✓	✓
	استفاده از پروتکل‌های امن در تبادل اطلاعات (احراز هویت، برچسب زمانی، ...)	✓	✓	✓
	مکانیزم‌های ذخیره سازی امن داده های ذخیره شده راه دور نظیر زیرساخت ابری	✓	✓	
	ذخیره‌سازی امن اطلاعات حساس در هنگام ذخیره در دستگاه	✓	✓	✓
	مکانیزم پشتیبان‌گیری امن از اطلاعات و تست دوره‌ای نسخ پشتیبان	✓	✓	
	طبقه‌بندی اطلاعات و به کارگیری مکانیزم‌های کنترل‌دسترسی و احراز هویت	✓	✓	✓
	رویدادنگاری	✓	✓	
امنیت نرم افزار	نیازسنجی امنیتی و مدل سازی تهدیدات	✓	✓	✓
	معماری و طراحی امن	✓	✓	✓
	احراز هویت قوی (احراز هویت چندعاملی- پسورد یکبار مصرف، ...)	✓	✓	
	کدنویسی امن	✓	✓	✓
	احرازهویت APIهای مورداستفاده	✓	✓	
	اجرا در حالت کیوسک مد	✓		✓
	مدیریت امن شرایط خطا و استثناء	✓	✓	✓
	اعتبارسنجی ورودی ها و خروجی ها	✓	✓	✓

لایه امنیتی	راهکارها و اقدامات امنیتی	لایه های شبکه بی‌سیم فضاپایه		
		ایستگاه زمینی	زیرساخت و شبکه سرویس‌دهی	ماهواره
	مدیریت حساب ها و کنترل دسترسی	✓	✓	✓
	رویدادنگاری در سطح نرم افزار	✓	✓	
	امنیت زنجیره تامین نرم افزار (کد منبع باز، COTS، API، ...)	✓	✓	✓
	ارزیابی های امنیتی (جعبه سفید و سیاه)	✓	✓	✓
	استقرار امن نرم‌افزار	✓	✓	
	تست نفوذ دوره ای	✓	✓	
امنیت میزبان	تحلیل امنیتی و مقاوم‌سازی سرویس ها	✓	✓	
	مدیریت امن به روزرسانی وصله ها	✓	✓	✓
	نرم‌افزار کنترل لیست سفید	✓		✓
	ضدبدافزار	✓	✓	
	پیکربندی امن سرورها (فیزیکی /مجازی)	✓	✓	
	مقاوم سازی و پیکربندی امن سیستم‌عامل/ میان افزار	✓	✓	✓
	نرم افزار تشخیص بدافزار مبتنی بر موتور چندضدبدافزار	✓	✓	
امنیت شبکه	سامانه تشخیص و پیشگیری از نفوذ شبکه	✓	✓	
	فایروال نسل آینده	✓	✓	
	سامانه انتقال امن فایل	✓	✓	
	ارتباطات امن- رمزکننده شبکه سیمی	✓	✓	
	رمزنگاری ارتباطات بی‌سیم	✓	✓	✓
	مخابرات طیف گسترده	✓	✓	✓
	طراحی امن شبکه/مرکز داده مبتنی بر معماری اعتماد صفر	✓	✓	
	راهکار گسترده شناسایی و پاسخ (XDR)	✓	✓	
امنیت	مکانیزم های تشخیص دستکاری سخت افزار	✓	✓	✓

لایه امنیتی	راهکارها و اقدامات امنیتی	لایه های شبکه بی‌سیم فضاپایه		
		ایستگاه زمینی	زیرساخت و شبکه سرویس‌دهی	ماهواره
زیرساخت و سخت‌افزار	ذخیره سازی میان افزار در رسانه‌های فقط خواندنی		✓	✓
	کدنویسی امن و ایمن در میان افزار			✓
	طراحی پروتکل های امن جهت ارتباطات بین زیرسیستم‌ها			✓
	پیکربندی و مقاوم‌سازی تجهیزات شبکه (سوییچ، روتر، ...)	✓	✓	
	به کارگیری چندین نقطه دسترسی در ارتباطات بی‌سیم	✓	✓	✓
	به کارگیری چندین مسیر uplink و downlink	✓		✓
	استفاده از مکانیزم های احراز هویت و کنترل دسترسی	✓	✓	✓
	طراحی امن بردها	✓		✓
	ارزیابی امنیتی تجهیزات سخت افزاری	✓	✓	✓
	کنترل کننده درگاه ها و اینترفیس های دستگاه	✓	✓	✓
	ارتقای تجهیزات سخت‌افزاری	✓	✓	✓
امنیت فیزیکی	امنیت فیزیکی ساختمان‌ها و مراکز باارزش و حساس (اتاق سرور، مراکز داده، ایستگاه زمینی و ...)	✓	✓	
	تجهیزات نظارتی (دوربین- کنترل دسترسی بیومتریک)	✓	✓	✓
	کنترل دسترسی فیزیکی (گیت شناسایی- احراز هویت – کنترل دسترسی)	✓	✓	✓
	رصد، سرشماری و کنترل دارایی‌های فیزیکی	✓	✓	
	رویدادنگاری دسترسی‌ها و مانیتورینگ دسترسی‌های غیرمجاز	✓	✓	✓
	شیلدینگ	✓	✓	✓
امنیت دستگاه‌های موبایل و کلاینت‌ها	تحلیل امنیتی و مقاوم‌سازی کلاینت‌ها	✓	✓	
	ضدبدافزار سیستم های کامپیوتری/ لپ تاپ	✓	✓	
	ضدبدافزار تلفن همراه	✓	✓	
	فایروال سیستم های کامپیوتری/ لپ تاپ	✓	✓	
	تشخیص و پاسخ نقطه پایانی (EDR)	✓	✓	
سیاست‌ها،	امنیت نیروی انسانی (آموزش و آگاهی رسانی)	✓	✓	

لایه امنیتی	راهکارها و اقدامات امنیتی	لایه های شبکه بی‌سیم فضاپایه		
		ایستگاه زمینی	زیرساخت و شبکه سرویس‌دهی	ماهواره
فرایندها و آگاهی رسانی	تدوین سیاست‌ها، رویه‌ها و روش‌های اجرایی و الزامات امنیت سایبری از جمله مدیریت پیکربندی امن، مدیریت وصله‌ها، فرایند شناسایی، احرازهویت و کنترل دسترسی، فرایند شناسایی اطلاعات حساس، تهیه و تست نسخ پشتیبان، مانیتورینگ و رویدادنگاری و ...	✓	✓	✓
	امنیت زنجیره تامین و ارتباطات افراد/شرکت‌های همکار/پشتیبان شبکه	✓	✓	✓
مانیتورینگ تهدیدات و پاسخ به رویدادها	تنظیم مانیتورینگ در سطح تجهیزات شبکه (سوییچ، روتر،..)	✓	✓	
	مدیریت پاسخ به رویدادها	✓	✓	✓
	تحلیل فارنزیکی رویدادها	✓	✓	✓
	راه‌اندازی آزمایشگاه تحلیل حملات و فارنزیک	✓	✓	
	توسعه و نصب ایجنت های جمع آوری لاگ‌های امنیتی/ممیزی بر روی تجهیزات و سخت افزار	✓	✓	✓
	راه‌اندازی مرکز عملیات امنیت (SOC)	✓	✓	
پیشگیری از حملات	طراحی پایگاه دانش آسیب‌پذیری‌های امنیتی	✓	✓	✓
	مدیریت آسیب پذیری های امنیتی	✓	✓	✓
	طراحی و پیاده سازی الزامات امنیت سایبری	✓	✓	✓
	مدیریت و ارزیابی ریسک امنیتی	✓	✓	✓
	دفاع سایبری فعال مانند هانی‌پات	✓	✓	
	برآورد اطلاعات تهدیدات سایبری و مدل‌سازی تهدید	✓	✓	✓

بحث و نتیجه‌گیری

شبکه‌های بی‌سیم فضاپایه، به طور بالقوه در معرض طیف وسیعی از حملات سایبری هستند و با توجه به افزایش کاربرد این نوع شبکه‌ها در زیرساخت‌های حیاتی نمی‌توان تنها به قابلیت اطمینان و در دسترس بودن به عنوان الزامات این نوع شبکه‌ها اکتفا نمود و لحاظ نمودن امنیت سایبری در چرخه حیات شبکه‌های فضاپایه و ایجاد سازوکارهای حفاظتی موثر امنیتی برای مقاوم‌سازی آنها ضروری است.

در این راستا اولین اقدام شناسایی دارایی‌ها و استخراج همه‌جانبه تهدیدات سایبری متصور برای این نوع شبکه می‌باشد. لذا در این مقاله، بر اساس تلفیقی از طبقه‌بندی تهدیدات انیسا و مدل تهدید استرید طبقه‌بندی جامعی از تهدیدات سایبری در شش حوزه اقدامات بدخواهانه، استراق سمع، خسارات غیرعمدی، تهدیدات فیزیکی، تهدیدات طبیعی و خرابی/اختلال ارائه گردید و سپس با نگاشت لایه های امنیت سایبری مبتنی بر استراتژی دفاع در عمق به دارایی های سایبری لایه های شبکه موردنظر، چارچوب جامع امنیت سایبری شبکه های فضاپایه طراحی گردید.

در مقالات مربوط به حوزه تهدیدات و راهکارهای امنیتی تنها بخشی از تهدیدات سایبری این نوع شبکه‌ها ارائه گردیده و دید جامعی از انواع تهدیدات سایبری شبکه‌های بی‌سیم فضاپایه و راهکارهای امنیتی موردنیاز مبتنی بر معماری آنها وجود ندارد و از این رو مقاله حاضر با ارائه ایده استفاده از استراتژی دفاع در عمق و ایجاد چارچوب جامعی از راهکارهای امنیتی در لایه های دارایی‌های سایبری این نوع شبکه ها، بستر را جهت طراحی دقیق تر راهکارها و افزایش ضریب امنیت سایبری شبکه های بی‌سیم فضاپایه فراهم نموده است.

منابع

[1] Daojing He, et al. Security Analysis of a Space-Based Wireless Network, IEEE Network, January 2019
[2] Yuhan Ruan et al. Energy Efficient Adaptive Transmissions in Integrated Satellite-Terrestrial Networks With SER Constraints, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, Vol.17, No.1, 2018.
[3] M.Manulis et al. Cyber security in New Space: Analysis of threats, key enabling technologies and challenges, International Journal of Information SecurityVolume 20 Issue 3 Jun 2021
[4] Jian Jiao et al. Performance Analysis of Space Information Networks with Backbone Satellite Relaying for Vehicular Networks, Hindawi Wireless Communications and Mobile Computing Volume 2017.
[5] H. Yao et al. The Space-Terrestrial Integrated Network: An Overview, IEEE Wireless Communication, 2019.
[6] X. Jin, P. Zhang. "A Communication Framework Between Backbone Satellites and Ground Stations," Proc. Int'l. Symp. Commun. and Info. Technologies, 2016.
[7] Chundong She1 et al. An improved malicious code intrusion detection method based on target tree for space information network, International Journal of Distributed Sensor Networks, Vol. 13(12), 2017.
[8] Chunxiao Jiang et al. Security in Space Information Networks, IEEE Communications Magazine, 2015.
[9] Bradbury, et al. Identifying attack surfaces in the evolving space industry using reference architectures. IEEE Aerospace Conference, 2019.
[10] Deborah J. Bodeau, et al. Cyber threat modeling: Survey, Assessment and Representative Framework, The Homeland Security Systems Engineering and Development Institute (HSSEDI), 2018.
[11] Issa M. Khalil, et al. Cloud Computing Security: A Survey, licensee MDPI, Basel, Switzerland, 2014.
[12] David Livingstone, Patricia Lewis, Space, the Final Frontier for Cybersecurity، The Royal Institute of international Affairs, 2016.
[13] Adam Ali Zare Hudaib, Satellite Network Hacking & Security Analysis, International Journal of Computer Science and Security (IJCSS), Vol (10): Issue (1): 2016.
[14] Gregory Falco, Cybersecurity Principles for Space Systems, JOURNAL OF AEROSPACE INFORMATION SYSTEMS, 2018.
[15] Brandon Bailey et al. Defending Spacecraft in the cyber domain, Center for space Policy and Strategy, 2019.
[16] Nicholas Cohen, Spacecraft Embedded Cyber Defense- Prototypes & Experimentation, SPACE Conferences and Exposition, Long Beach, California, 2016.
[17] Robert Mazzolin, A Perspective on Cyber in Space for National Security, International Journal of Cyber Diplomacy, Volume 1, Issue 1, 2020.
[18] Muhammad Jamil Shah, et al. A Survey Paper on Security Issues in Satellite Communication Network infrastructure. International Journal of Engineering Research and General Science, 2014.
[19] Maged Hamada Ibrahim, et al. Jamming resistant non-interactive anonymous and unlinkable authentication scheme for mobile satellite networks, security and communication networks. 2016
[20] Paul Kyle Kallender, Waking Up to a New Threat: Cyber Threats and Space, Trans. JSASS Aerospace Tech, Vol.12, No. 29, 2014.
[21] Mohammad Masdari, et al. A survey and taxonomy of DoS attacks in cloud computing, Security Comm. Networks; in Wiley Online Library, 2016.
[22] Bhupendra Jasani, Space assets and emerging threats, Department of War Studies, King's College London UK. 2016.
[23] Jacob G. Oakley, Cybersecurity for Space: Protecting the Final Frontier, Owens Cross Roads, AL, USA, 2020,
[24] Jason Fritz BS, SATELLITE HACKING: A Guide for the Perplexed, Bulletin of the Centre for East-West Cultural and Economic Studies, Vol. 10, No. 1, 2013

Cyber Security Framework Design in Space-Based Wireless Networks

Seyyedeh Fatemeh Malek

Senior Expert in Information Technology Engineering - Computer Networks, Faculty of Computer Engineering, Amirkabir University of Technology, Tehran

Siavash Khorsandi

Associate Professor, Faculty of Computer Engineering, Amirkabir University of Technology, Tehran

Abstract

Today, with the gradual establishment of space-based wireless networks, which is a result of the integration and convergence of satellite communications, the Internet, and mobile wireless networks, we are witnessing an increase in the possibility of providing comprehensive information and services at any time and in any place, but from a security perspective, this integration leads to an increase in their vulnerability to cyber attacks. Abusing the Internet-based remote configuration feature, eavesdropping or disrupting satellite Internet communications, falsifying signals, disrupting mobile phone networks, are among the possible cyber attacks in these types of networks.

So far, many technical measures have been taken regarding the structure, architecture, and protocols of this type of networks, and most of the research are in the field of improving the efficiency and reliability of space-based wireless networks. In the articles related to threats and security solutions, only a part of the cyber threats of this type of networks is presented, and there is no comprehensive view of the types of cyber threats of space-based wireless networks and the required security solutions based on their architecture. Based on this, in this article, while identification and valuation of cyber assets and the understanding of the overall architecture of these types of networks and analyzing and classifying cyber threats based on a combination of ENISA threat classification and STRIDE threat model, we have designed a comprehensive cyber security framework based on defense-in-depth strategy in space-based wireless networks.

Keywords: Cyber threat, Threat Agents, Cyber Attacks, Satellite, Vulnerability