
ST Engineering
TRANSMISSION SECURITY (TRANSEC)
EVOLUTION DEFENSE
iDIRECT

مقدمه

ما در ST Engineering iDirect اهمیت حیاتی حفاظت از جریان ارتباطات را در هر جایی که نیروهای نظامی و سازمان‌های دولتی فعالیت می‌کنند، درک می‌کنیم. در هر نقطه‌ای که این فعالیت‌ها انجام شوند، عوامل تهدید آماده‌اند تا ارتباطات را رصد، سوءاستفاده یا شنود کنند و مقاصد مخرب خود را پیش ببرند. برای کاهش این تهدید، ما از اولین نسخه نرم‌افزار Evolution قابلیت‌های امنیت انتقال (TRANSEC) را ارائه داده‌ایم. با انتشار نسخه 4.2، این قابلیت‌ها را ارتقا داده و پوشش امنیتی را برای شبکه‌های یک‌طرفه و دوطرفه گسترش داده‌ایم.

در شرایط رزمی، حتی یک «افزایش کوچک» در حجم ترافیک می‌تواند به‌عنوان یک سرنخ اطلاعاتی حیاتی در نظر گرفته شود. بنابراین، نیاز به مخفی کردن هرگونه فعالیت ارتباطی کاملاً آشکار می‌شود. آژانس امنیت ملی ایالات متحده (NSA) آسیب‌پذیری‌های ذاتی زیر را در انتقال TDMA مبتنی بر IP شناسایی کرده که برای دستیابی به امنیت واقعی TRANSEC باید برطرف شوند:

- **فعالیت کانال** –توانایی ایمن‌سازی انرژی انتقال برای پنهان کردن حجم ترافیک.
- **اطلاعات کانال کنترل** – استتار حجم ترافیک برای حفاظت از منبع و مقصد ترافیک.
- **اعتبارسنجی هاب و واحدهای ریموت** –اطمینان از اینکه ترمینال‌های ریموت متصل به شبکه کاربران مجاز هستند.

TRANSECچیست؟

TRANSEC(امنیت انتقال) مانع از این می‌شود که یک دشمن بتواند از اطلاعات موجود در یک کانال ارتباطی سوءاستفاده کند، حتی اگر نتوانسته باشد رمزگذاری را بشکند.

TRANSEC مستلزم آن است که تمام کانال‌های کنترل شبکه و داده‌های مدیریت و کنترل (M&C) رمزگذاری شوند و هرگونه اطلاعات مربوط به مهندسی ترافیک از دید دشمن پنهان بماند. به عنوان مثال، TRANSEC ایجاب می‌کند که یک کانال ارتباطی از دید دشمن همیشه کاملاً پر به نظر برسد، حتی اگر داده‌ی کمی یا اصلاً داده‌ای منتقل نشود.

این ویژگی در تضاد با امنیت ارتباطات (COMSEC) است. درCOMSEC ، محتوای واقعی ارتباط (مثل صدا، ویدئو یا جریان داده) رمزگذاری می‌شود، اما برخی اطلاعات هدر به‌صورت آشکار ارسال می‌شوند. در حالی که رمزگذاری تقریباً غیرقابل نفوذ است، اطلاعات موجود در هدر IP از جمله آدرس مبدأ، آدرس مقصد و مهم‌تر از همه فیلد نوع سرویس (ToS) به‌صورت آشکار باقی می‌مانند. با دسترسی به هدر IP یک بسته رمزگذاری‌شده، دشمن می‌تواند تشخیص دهد چه بخشی از ترافیک مربوط به صدا، ویدئو یا داده است. حتی مهم‌تر از آن، دشمن می‌تواند متوجه شود که چه زمانی ترافیک با اولویت بسیار بالا آغاز شده و این ترافیک از چه موقعیتی منشأ می‌گیرد.

در توپولوژی سنتی شبکه‌های ماهواره‌ای (SCPCیک کانال به ازای هر حامل)، دستیابی به انطباق با TRANSEC نسبتاً ساده است. در اتصال‌های SCPC از یک Bulk Encryptor برای رمزگذاری تمام داده‌ها و اطلاعات کنترلی عبوری از شبکه استفاده می‌شود. هدر IP بسته پیش از ارسال به ماهواره توسط Bulk Encryptor رمزگذاری می‌شود. علاوه بر این، از آنجا که لینک SCPCثابت و همیشه فعال است و هیچ اطلاعات کنترلی بین مودم‌های SCPC رد و بدل نمی‌شود، تمام الزامات TRANSEC برآورده می‌شوند.

اما در یک شبکه TDMA، انطباق با TRANSEC دشوارتر است. شبکه TDMA پهنای باند را به‌صورت پویا بین ریموت‌ها تخصیص می‌دهد، بنابراین لازم است نوعی اطلاعات کنترلی به هر دستگاه در شبکه ارسال شود. این داده‌های کنترلی که حاوی اطلاعات مهندسی ترافیک هستند، به‌همراه اطلاعات قابل استخراج از هدر بسته‌های رمزگذاری‌شدهIP ، می‌توانند توسط دشمن مورد سوءاستفاده قرار گیرند. برای مثال، حجم غیرعادی ترافیک به یک ریموت خاص می‌تواند نشان‌دهنده آغاز فعالیت جدید در آن منطقه باشد، یا نسبت‌های متفاوت ترافیک صدا به داده می‌تواند نشان دهد چه میزان داده (اطلاعات حساس) نسبت به ترافیک کم‌اهمیت‌تر صوت منتقل می‌شود.

راهکارهای ST Engineering iDirect برای رفع آسیب‌پذیری‌های امنیتی شبکه VSAT مبتنی برTDMA

پنهان‌سازی فعالیت کانال

چالش

اولین آسیب‌پذیری در شبکه TDMA در دسترس بودن اطلاعات مهندسی ترافیک است. در شبکه SCPC لینک ثابت بوده و ویژگی‌های انتقال با ارتباط کاربر نهایی تغییر نمی‌کند. بنابراین دشمنی که از یک آنالایزر طیف برای مشاهده ترانسپوندر ماهواره استفاده می‌کند، تنها یک سیگنال RF ثابت می‌بیند.

اما در شبکهTDMA ، حامل in-route (مسیر بازگشت) با شروع و توقف ترافیک، روشن و خاموش می‌شود. این ماهیت روشن/خاموش بودن، نتیجه طبیعی تخصیص پهنای باند به ریموت‌هایی است که نیاز موقتی دارند. در حالی که این ویژگی TDMA را بسیار کارآمدتر از نظر استفاده از پهنای باند می‌کند، به دشمن امکان می‌دهد زمان اوج فعالیت‌ها، رویدادهای غیرمنتظره و حتی مکان ریموت‌هایی که مدتی خاموش بوده‌اند و ناگهان فعال شده‌اند را شناسایی کند. در اختیار داشتن چنین اطلاعاتی می‌تواند به دشمن امکان دهد زمان‌بندی، موقعیت و مقیاس یک فعالیت استراتژیک را تخمین بزند.

راه‌حل

ما الگوریتم توزیع پهنای باند TDMA خود را به گونه‌ای طراحی کرده‌ایم که اختصاص شکاف آزاد(Free Slot Allocation) را پیاده‌سازی کند. با این روش، دشمنی که انرژی ترانسپوندر ماهواره را رصد می‌کند، یک «دیوار داده» پیوسته مشاهده می‌کند، فارغ از اینکه ترافیک واقعی چقدر است.

همان‌طور که از نامش پیداست، اختصاص شکاف آزاد باعث می‌شود حامل‌های in-route فعال باقی بمانند، حتی زمانی که هیچ ترافیکی جریان ندارد. این روش ضمن حفظ بهره‌وری شبکهTDMA ، حجم واقعی ترافیک را پنهان کرده و ریسک استفاده از فعالیت انتقال به‌عنوان یک ابزار جمع‌آوری اطلاعات را از بین می‌برد.

پنهان‌سازی فعالیت اتصال(Acquisition Activity)

چالش

نرخ اتصال ریموت‌ها به شبکه می‌تواند اطلاعات حیاتی درباره فعالیت‌های نیروهای نظامی در اختیار دشمن قرار دهد. تمام شبکه‌های TDMAیک کانال اختصاصی برای فعالیت اتصال ریموت‌ها فراهم می‌کنند. اگر دشمن این کانال را رصد کند، با مشاهده موج اتصال‌های جدید متوجه جابجایی نیروها خواهد شد.

راه‌حل

ما با پرداختن به این آسیب‌پذیری فراتر از الزامات TRANSEC عمل کرده‌ایم. الگوریتم اتصال ST Engineering iDirect بسته‌های ساختگی (Dummy Bursts) را از ریموت‌های موجود در شبکه ارسال می‌کند و در زمان‌هایی که فعالیت اتصال زیاد است، برخی از بسته‌های واقعی را عمداً حذف می‌کند. این کار باعث می‌شود دشمن تنها یک الگوی تصادفی از فعالیت اتصال ببیند.

علاوه بر این، الگوریتم اتصال ما فراتر رفته و فرکانس، زمان‌بندی و توان بسته‌های ساختگی را به‌صورت تصادفی تغییر می‌دهد. این تصادفی‌سازی تضمین می‌کند که دشمن قادر به تشخیص تفاوت بین بسته ساختگی و فعالیت واقعی اتصال نباشد.

اطلاعات کانال کنترل(Control Channel Information)

چالش

حجم زیادی از اطلاعات مربوط به حجم و اولویت‌بندی ترافیک را می‌توان با بررسی اطلاعات کنترل درون‌باند یا برون‌باند در یک شبکه TDMA رمزگذاری‌شده استخراج کرد. همانطور که پیش‌تر گفته شد، هدر IP شامل اطلاعات مبدأ، مقصد و اولویت است. برای اینکه شبکه TDMA کیفیت خدمات (QoS) لازم جهت پشتیبانی از ترافیک بی‌درنگ مانند صدا و ویدیو را فراهم کند، لازم است اطلاعات حجم داده‌ها و اولویت‌بندی جمع‌آوری شود.

این اطلاعات حتی می‌تواند برای دشمن مفیدتر از داده‌های فعالیت کانال باشد، زیرا به اندازه کافی دقیق است تا بتواند بین ارتباطات عمومی مانند ایمیل و وب‌گردی، و ارتباطات تاکتیکی مانند صدا و ویدئو تمایز قائل شود.

راه‌حل

تنها راه‌حل این آسیب‌پذیری، رمزگذاری کامل تمام اطلاعات لایه ۲ و همچنین هرگونه اطلاعات کنترلی ارسال‌شده به ریموت‌هاست. روش رمزگذاری باید به‌اندازه‌ای امن باشد که دشمن نتواند اطلاعات را به‌موقع رمزگشایی کند و داده‌ها بی‌ارزش شوند.

ما از استاندارد فدرال پردازش اطلاعات 140-2 (FIPS) با الگوریتم AESبا کلید 256 بیتی برای رمزگذاری تمام داده‌های لایه ۲ و اطلاعات کنترلی استفاده کرده‌ایم. رمزگذاری فریم‌های لایه ۲ مزیت جانبی دیگری دارد: بار داده (Payload) دوباره رمزگذاری می‌شود. در نتیجه، حتی هدر IP ارسالی نیز با AES رمزگذاری می‌شود.

علاوه بر این، شکاف‌های TDMA در TRANSEC ما دارای اندازه ثابت هستند تا ویژگی‌های ترافیک پنهان بمانند. این راهکار رمزگذاری لایه ۲ تمام آسیب‌پذیری‌های کانال کنترل را برطرف می‌کند.

روش رمزگذاری ما حتی فراتر رفته و شامل موارد زیر است:

- به‌روزرسانی کلیدها از طریق هوا(OTA Key Updates)
- فرمت منحصربه‌فرد فریم لایه ۲ شامل بردار اولیه‌سازی (Initialization Vector) که باعث تصادفی‌سازی جریان‌های داده تکراری می‌شود .

نتیجه نهایی این است که دشمن قادر به تشخیص هیچ الگوی تکراری نخواهد بود، موضوعی که می‌تواند در رمزگشایی الگوریتم‌های رمزگذاری به او کمک کند.

اعتبارسنجی هاب و ریموت(Hub and Remote Authentication)

چالش

یکی دیگر از آسیب‌پذیری‌های سیستم VSAT مبتنی برTDMA ، موضوع اعتبارسنجی هاب و ریموت است. در معماری‌های سنتی SCPC، لینک پس از برقراری برای مدت‌های طولانی فعال باقی می‌ماند. از آنجایی که این اتصالات ثابت هستند و سطح بالایی از هماهنگی بین پرسنل در زمان راه‌اندازی لینک وجود دارد، اعتماد زیادی وجود دارد که دشمن سعی نمی‌کند هویت یک نهاد مورد اعتماد را جعل کند.

اما در شبکه‌هایTDMA ، ریموت‌ها به‌طور مرتب وارد شبکه می‌شوند و از آن خارج می‌شوند. این موضوع به‌خصوص در شبکه‌هایی با ترمینال‌های متحرک یا سیار (مثل خودروهای در حال حرکت، هواپیماها یا کشتی‌ها) رایج است. چنین محیط پویایی به دشمن فرصت بیشتری می‌دهد تا از طریق روش‌های قانونی یا غیرقانونی به یک ترمینال VSAT دسترسی پیدا کند، شناسه دستگاه

(Device ID)را جعل کرده و یک ریموت مخرب را وارد شبکه امن کند. همچنین امکان دارد دشمن به ترمینال هاب دسترسی پیدا کرده و یک ریموت نیروهای خودی را به شبکه دشمن جذب کند.

راه‌حل

برای کاهش این ریسک، ما از گواهی‌های دیجیتال X.509 در ریموت‌های TRANSEC استفاده کرده‌ایم. گواهی X.509 از سیستم رمزنگاری کلید عمومی RSAبهره می‌برد. در این سیستم دو کلید مرتبط تولید می‌شود: یک کلید خصوصی و یک کلید عمومی. عملکرد این کلیدها به این صورت است که هر چیزی که با کلید عمومی رمزگذاری شود، تنها با کلید خصوصی قابل رمزگشایی است و بالعکس.

در سیستمST Engineering iDirect ، گواهی‌های X.509 از طریق سرور NMSتولید می‌شوند. این گواهی‌ها روی تمام کارت‌های خطTRANSEC ، پردازنده‌های پروتکل و همچنین روی ریموت‌ها قرار می‌گیرند. سیستم هاب کلید عمومی هر ریموتی را که برای کار روی هاب پیکربندی شده، ذخیره می‌کند و ریموت‌ها نیز کلید عمومی هر دستگاه هاب را دارند. در فرآیند اتصال به شبکه، ریموت گواهی X.509 خود را با کلید خصوصی‌اش رمزگذاری می‌کند و هاب با کلید عمومی آن را رمزگشایی و اعتبارسنجی می‌کند (و برعکس). این فرآیند تضمین می‌کند که ریموت مجاز به کار در شبکه است و هاب نیز یک موجودیت مورد اعتماد است.

پیاده‌سازی عملیاتی(Operational Implementation)

چالش

پیاده‌سازی امنیت و اطمینان از رعایت همه سیاست‌های امنیتی می‌تواند برای سرباز حاضر در میدان سخت و زمان‌بر باشد. اجرای TRANSECو مدیریت کلید نیز از این قاعده مستثنی نیست. چالش‌هایی که در راه‌اندازی یک شبکه TRANSEC وجود دارد شامل موارد زیر است:

- ایجاد، توزیع و ابطال گواهی‌هایX.509
- تولید، توزیع و مدیریت کلیدهای کانال اتصال (ACQ) و کانال داده(DCC)
- صفر کردن مودم‌ها(Zeroizing)

یک شبکه TRANSEC قدرتمند به حداقل دو کلید سراسری نیاز دارد :کلید ACC برای فرآیند اتصال و کلید DCC برای کانال داده. یک عبارت عبور طولانی و تولیدشده توسط کاربر برای محافظت از این کلیدها در زمان راه‌اندازی اولیه استفاده می‌شود. وارد کردن این عبارت عبور از طریق پنل جلویی مودم یا مکانیزم‌های فیزیکی بارگذاری کلید (Key Fill) هم برای نیروها بار اضافی ایجاد می‌کند و هم آسیب‌پذیری‌های امنیتی جدیدی به وجود می‌آورد.

اقدامات امنیتی تکمیلی(Additional Security Measures)

FIPS 140-2

استاندارد FIPS 140-2یک استاندارد امنیتی دولت ایالات متحده برای اعتبارسنجی ماژول‌های رمزنگاری است. این استاندارد توسط مؤسسه ملی استاندارد و فناوری (NIST) منتشر شده است.

FIPS 140-2یک اطمینان شخص ثالث و بسیار سخت‌گیرانه از ادعاهای امنیتی هر محصولی که شامل رمزنگاری باشد و ممکن است توسط سازمان‌های دولتی مورد استفاده قرار گیرد، فراهم می‌کند. این استاندارد برنامه‌ای به نام Cryptographic Module Validation Program (CMVP)ایجاد کرده که یک تلاش مشترک بین NIST و سازمان امنیت ارتباطات کانادا (CSE) است.

FIPS 140-2چهار سطح امنیتی را برای طراحی و پیاده‌سازی ماژول‌های رمزنگاری مشخص می‌کند. طبق توضیحاتNIST ، خلاصه‌ای از این سطوح به شرح زیر است:

- **سطح امنیتی 1 :**پایه‌ای‌ترین سطح امنیت است. هیچ ویژگی فیزیکی خاصی برای امنیت لازم نیست و تنها یک الگوریتم امنیتی مورد تأیید کافی است.
- **سطح امنیتی 2 :**نیازمند پوشش‌ها یا پلمب‌های ضد دستکاری است که برای دسترسی به کلیدهای رمزنگاری و پارامترهای امنیتی حیاتی باید شکسته شوند.
- **سطح امنیتی 3 :**علاوه بر الزامات سطح 2، مکانیزم‌های امنیت فیزیکی برای شناسایی و پاسخ به تلاش‌های دسترسی فیزیکی یا تغییر ماژول رمزنگاری مورد نیاز است.
- **سطح امنیتی 4 :**نیازمند یک لایه محافظتی کامل در اطراف ماژول رمزنگاری است که بتواند تمام تلاش‌های غیرمجاز برای دسترسی را شناسایی و پاسخ دهد.

علاوه بر نیازمندی‌های سخت‌افزاری، اعتبارسنجی FIPS شامل کل راهکار رمزنگاری می‌شود، از جمله سیستم‌عامل و نرم‌افزار.

ارتقای TRANSEC و امنیت با سری 9 و کارت‌هایDLC

با عرضه روترهای ماهواره‌ای سری 9 و کارت‌های Defense Line Cards (DLCs)، ما سطح تأییدیه FIPS 140-2 محصولاتمان را از سطح 2 به سطح 3 ارتقا داده‌ایم.

در این فرآیند، ما یک ماژول TRANSEC توسعه دادیم که با الزامات سخت‌گیرانه FIPS 140-2 سطح 3 مطابق است. این ماژول که در محصولات سری 9 وDLC ها به‌صورت تعبیه‌شده و مستقل وجود دارد، از یک مسیر جداگانه و قابل اعتماد نسبت به سایر رابط‌های دستگاه عمل می‌کند.

این ماژول همچنین دارای مکانیزم‌های امنیت فیزیکی قوی برای جلوگیری از دستکاری بوده و قابلیت صفر کردن (Zeroize) کلیدهای امنیتی یا پارامترهای حیاتی امنیتی (CSPs) ذخیره‌شده در ماژول را دارد. در صورت نیاز، ابطال یا صفرسازی کلیدها می‌تواند به‌صورت OTAتوسط اپراتور هاب یا به‌صورت محلی روی ریموت توسط افراد مجاز انجام شود.

شبکه‌های یک‌طرفه(One-Way Networks)

ما قابلیت‌های TRANSEC خود را با ایمن‌سازی ارتباطات پخش یک‌طرفه نیز گسترش داده‌ایم. بر اساس روش کپسوله‌سازی LEGS، پلتفرم ST Engineering iDirect می‌تواند همان سطح امنیتی که برای شبکه‌های دوطرفه فراهم می‌کند را برای شبکه‌های یک‌طرفه نیز ارائه دهد.

مدل‌های 900و 9350با پشتیبانی از دمدولاتور دوگانه (Dual-Demodulator) قادر به اجرای TRANSECدو دامنه‌ای (Dual-Domain TRANSEC)هستند. به این معنی که می‌توانند دو زنجیره اعتماد مستقل(مجموعه‌ای از گواهی‌های X.509)بین دو مرجع صدور گواهی (CA) متفاوت برقرار کنند.

یک نمونه کاربرد این قابلیت می‌تواند این باشد که یک دمدولاتور در یک شبکه دوطرفه TRANSEC فعال باشد، در حالی که دمدولاتور دوم یک پخش یک‌طرفه امن TRANSEC را دریافت کند. برای تولید کلید از رمزنگاری منحنی بیضوی (ECC) استفاده می‌شود و در هر دامنه امنیتی از گواهی‌های X.509برای احراز هویت بهره گرفته می‌شود.

تماس با ما:

شرکت عصر ارتباطات بین الملل پارس کار (ایکاست)

آدرس : تهران، سعادت آباد، میدان بهرود، خیابان عابدی، پلاک 15 ساختمان صبا، طبقه سوم واحد 8 - کد پستی : 1981863695

تلفن : 982175229229+ فکس : 982175229239+

وبگاه : www.icasat.net پست الکترونیک : **cmo@icasat.net**