سیستم تشخیص نفوذ در شبکه سیار موردی

رضا امیری

۱۳۹٤

سرشناسه: امیری، رضا، ۱۳۶۰ -
عنوان و نام پدیدآور: سیستم تشخیص نفوذ در شبکه سیار موردی/ رضا امیری.
مشخصات نشر: شخصیت و شادمانی / مهتاب ضیائیان.
مشخصات ظاهری: اصفهان: نشر دارخوین، ۱۳۹۴.
شابک: ۱۲۲ ص
وضعیت فهرست نویسی: ۹۷۸-۶۰۰-۳۸۰-۲۲۹-۲
موضوع: شبکه‌های موردی
موضوع: شبکه‌های موردی -- تدابیر ایمنی
موضوع: شبکه‌های محلی بی‌سیم
موضوع: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع: [illegible]طات بی‌سیم
رده بندی کنگره: ۱۳۹۴ ۹س۱۸الف/TK۵۱۰۵/۷۷
رده بندی دیویی: ۳۸
شماره کتابشناسی ملی: ۳۸۹[illegible]۱۶

سیستم تشخیص نفوذ در شبکه سیار موردی

رضا امیری

ناشر: دارخوین
نوبت چاپ: اول ۱۳۹۴
شمارگان: ۱۰۰۰
شابک: ۹۷۸-۶۰۰-۳۸۰-۲۲۹-۲
طرح جلد: حامد شاهمرادی
صفحه‌آرا: حامد شاهمرادی

www. ndarkhovain. ir

۰۳۱ ۹۵۰ ۲۰۷۷۲

پیشگفتار

شبکه‌های کامپیوتری جزء اساسی جوامع امروزی محسوب می‌شوند. امنیت سیستم‌های کامپیوتری شامل محرمانگی[1]، جامعیت[2] و قابلیت دسترسی[3] است. این اصطلاحات در زیر توضیح داده شده‌اند.

قابلیت دسترسی: قابلیت دسترسی ضمانت می‌کند که سرویس‌ها و منابع شبکه در تمامی مواقع برای کاربران قانونی در دسترس باشد. و این مساله از قابلیت نجات شبکه در مقابل درخواستهای بدخواهانه اطمینان می‌دهد.

احرازهویت: احراز هویت به گره در شبکه قابلیت شناسایی گره یا کاربر مقابل خود که با آن ارتباط برقرار می‌کند را می‌دهد، و برای جلوگیری از جعل هویت است. یک گره در شبکه می‌تواند خود را به جای گره دیگر معرفی کند و از این طریق به شبکه نفوذ کند. در شبکه‌های سیمی و شبکه‌های بی‌سیم زیرساخت‌محور، ممکن است که یک قدرت مرکزی مانند روتر، ایستگاه اصلی یا نقطه دسترسی ایجاد کرد، ولی در شبکه سیار موردی هیچ قدرت مرکزی وجود ندارد و احراز هویت دشوارتر است. معتبرشناسی می‌تواند از طریقیک کد معتبرشناسی پیام بدست آید.

جامعیت: جامعیت ضمانت می‌کند که پیام‌ها از تغییر یا تخریب غیر قانونی حین انتقال حفظ می‌شوند. تغییر در بسته‌ها می‌تواند به علت یک حمله یا خطای انتشار رخ دهند. زمانی که داده‌ها ازطریق رسانه بی‌سیم ارسال می‌شوند، ممکن است توسط

1. Confidentiality
2. Integrity
3. Availability

حمله کننده‌ها تغییر پیدا کنند یا حذف شوند. جامعیت می‌تواند از طریق توابع در همسازی بدست آید.

محرمانگی: معنای محرمانگی این است که اطلاعات فرستاده شده غیر قابل خواندن برای کاربران یا گره‌های غیر مجاز شود. این خصیصه در مورد اطلاعات حساس بسیار مهم می‌باشد. شبکه سیار موردی از یک رسانه باز استفاده می‌کند، بنابراین معمولاً تمام گره‌ها در یک برد در یک انتقال مستقیم می‌توانند داده‌ها را بگیرند. یک راه برای محرمانه نگه داشتن اطلاعات رمزنگاری آن‌هاست و تکنیک دیگر استفاده از آنتن‌های جهت‌دار می‌باشد.

انکارناپذیری: هدف از انکارناپذیری این است که اگر یک موجودیت یک پیام را بفرستد نباید بتواند این کار را انکار کند. توسط ایجاد امضا برای پیام، آن موجودیت نمی‌تواند بعداً فرستادن آن را انکار کند. در رمزنگاری کلید عمومی، یک گره A نامه‌ها را توسط کلید خصوصیش امضا می‌کند. تمام گره‌های دیگر می‌توانند این پیام امضا شده را با کلید عمومیA باز کنند و A نمی‌تواند انکار کند چرا که امضایش به نامه متصل است.

تلاش برای نفوذ در یک شبکه کامپیوتری حداقل یکی از پارامترهای امنیت را به خطر می‌اندازد. این تلاش می‌تواند با هدف دسترسی غیرمجاز به اطلاعات، تغییر اطلاعات با دسترسی غیر مجاز و یا از کار انداختن سیستم (تبدیل سیستم به یک سیستم غیر قابل اعتماد یا غیر قابل استفاده) صورت گیرد. عموما این تلاش‌ها به دلیل وجود آسیب‌پذیری‌هایی در سیستم شانس موفقیت دارند.

یک آسیب‌پذیری، ایرادی در طراحی نرم افزار، سخت افزار و یا عملکرد سیستم است که سیستم را در مقابل تلاش‌های نفوذ، ناامن می‌کند. اشتباهات و یا ضعف‌هایی در پروتکل‌ها و پیاده سازی، نصب و یا تنظیمات سرویس‌ها و ابزارهای مختلف شبکه منجر به این آسیب‌پذیری‌ها می‌شود. مدیر امنیتی باید تا حد امکان سیستم را در برابر نفوذ مقاوم کند. یک حمله، اجرای یک برنامه‌ی طرح‌ریزی شده با هدف نفوذ در شبکه است. این حمله ممکن است موفقیت آمیز باشد و یا با شکست مواجه شود.

با گسترش شبکه‌های کامپیوتری تعداد حملات گزارش شده از سال ۲۰۰۰ با سرعت زیادی رو به افزایش بوده است. بنابراین روز به روز اهمیت امنیت در شبکه‌ها بیشتر شده است. امروزه جهت تامین امنیت در شبکه، از سیستم‌ها و ابزارهای امنیتی متفاوتی از جمله سیستم‌های جلوگیری از نفوذ و سیستم‌های تشخیص نفوذ استفاده می‌گردد.

در سال‌های اخیر، شبکه سیار موردی (MANET)، به یک تکنولوژی مهم و در حال توسعه تبدیل شده است. این شبکه‌ها به عنوان شبکه بی‌سیم پویا شناخته می‌شوند که می‌توانند بدون هیچ زیرساخت ثابتی و درحالی که هر گره به عنوان یک مسیریاب عمل می‌کند، شکل بگیرند. این شبکه‌ها شامل مجموعه‌ای از گره‌های همکار هستند که توانایی‌های بی‌سیم خود را با گره‌های مشابه دیگر به اشتراک می‌گذارند تا بدین طریق با گره‌هایی که در محدوده رادیوییشان قرار ندارند ارتباط برقرار کرده و بطور موثر پیغام‌ها را بر روی گره‌های میانی باز پخش کنند. گره‌ها می‌توانند بهراحتی در شبکه‌های موردی حرکت کنند. این مشخصه، شبکه‌های موردی را برای کاربردهای متفاوت مناسب می‌کند. این شبکه‌ها بطورگسترده درکاربردهای نظامی و عملیات نجات در جاهایی که زیرساخت ارتباطی آسیب دیده و یا در دسترس نیستند، استفاده می‌شوند؛ محیطهایی مانند زلزله و یا در میدان جنگ.

شبکه‌های سیار موردی گروهی از گره‌های متحرک بی‌سیم و خودسازمانده هستند که فاقد یک ساختار شبکه ثابت می‌باشند. انعطاف پذیری و آزادی در شبکه‌های سیار موردی، آن‌ها را برای جمع‌آوری اطلاعات بسیار مناسب کرده است. اما همین انعطاف‌پذیری و آزادی باعث بروز نقاط ضعف امنیتی در آن‌ها شده است. در شبکه موردی سیار اگر یک گره نفوذی وارد شبکه شده و تشخیص داده نشود، می‌تواند کارایی شبکه را بسیار پایین آورد. البته پیشنهادهای زیادی برای سیستم‌های تشخیص نفوذ در شبکه‌های سیمی ارائه و پیاده‌سازی شده است، اما به علت ساختار متفاوت شبکه‌های سیار موردی با شبکه‌های سیمی، سیستم‌های تشخیص نفوذ پیشنهاد شده در شبکه‌های سیمی، برای شبکه‌های سیار موردی مناسب نمی‌باشند. بنابراین،

یا بایستی این روش‌ها بر اساس ویژگی‌های شبکه سیار موردی تغییر کنند و یا اینکه روش‌های جدیدی برای برقراری امنیت در این شبکه‌ها ارائه شوند.

به علت متحرک بودن ساختار گره‌ها در شبکه سیار موردی، امکان زیادی برای اسیر شدن و مصالحه کردن گره‌ها (به ویژه در مناطق جنگی) وجود دارد. اگر گره‌های نفوذی تشخیص داده نشوند، این گره‌ها می‌توانند به سادگی در شبکه حرکت کرده و کارایی شبکه را تا حد چشمگیری کاهش دهند. به علت محدودیت منابع در شبکه‌های سیار موردی، نمی‌توان از تکنیک‌های رمزنگاری برای ارسال اطلاعات استفاده کرد. به همین دلیل گره‌های نفوذی به سادگی می‌توانند اطلاعات لازم را به دست آورده و شبکه را دچار مشکل کنند. برای مقابله با گره‌های نفوذی، از سیستم‌های تشخیص نفوذ استفاده شد

در شبکه‌های سیار موردی، معمولا بر روی هر گره، یک سیستم تشخیص نفوذ نصب می‌شود. برای بالا بردن سرعت تشخیص، سیستم‌های تشخیص نفوذ نصب شده بر روی هر گره، اطلاعاتی را که در مورد نفوذ به دست آوردهاند، برای دیگر گره‌های موجود در شبکه ارسال می‌کنند؛ به عبارت دیگر، گره‌ها از اطلاعات همدیگر برای تشخیص نفوذ استفاده می‌کنند.

شبکه‌های سیار موردی در معرض انواع حملات مخربکارانه قرار دارند. بنابراین مسئله امنیت به عنوان یک مفهوم مهم و کانون توجه از انواع تحقیق‌ها قرار گرفته است. در اکثر پروتکل‌های مسیریابی در شبکه‌های سیار موردی هیچ معیار امنیتی برای محافظت از فرایند مسیریابی وجود ندارد. مهاجمین می‌توانند به سادگی با اعلام یک مسیر جعلی، خود را در مسیر قرار داده و سپس با حذف بسته‌ها در شبکه، کارایی شبکه را تا اندازه چشمگیری کاهش دهند.

یکی از مهمترین حملاتی که بر روی شبکه‌های سیار موردی وجود دارد، حمله سیاه چاله می‌باشد. در این حمله، حمله کننده یک مسیر دروغین را به مبدا اعلام کرده و سپس مبادرت به حذف بسته‌ها می‌کند. روش‌های زیادی برای تشخیص اینگونه حملات در شبکه‌های سیار موردی پیشنهاد شده است، اما در بیشتر روش‌ها،

با کمی تغییر در حمله یا با همکاری چند گره نفوذی حمله کننده می‌تواند از سد سیستم‌های تشخیص نفوذ گذشته و کارایی شبکه را تا حد چشمگیری کاهش دهد.

کتاب حاضر با هدف ارائه یک سیستم تشخیص نفوذ برای جلوگیری از حمله سیاه چاله در شبکه سیار موردی تدوین شده است. امید است مطالب ارزشمند این اثر که به منظور توسعه دانش و بینش مدیران، دانشجویان و علاقه مندان نگاشته شده است به عنوان یک منبع مناسب مورد استفاده جامعه علمی قرار بگیرد. جا دارد پس از حمد و سپاس خداوند منان از کلیه کسانی که به نحوی از انحاء در شکل گیری این اثر سهم داشتند تشکر و قدردانی گردد. از ایزد متعال برای دانشجویان و جوانان عزیز ایران اسلامی آرزوی موفقیت و برای خود طلب مغفرت می‌نمایم.