
بسم الله الرحمن الرحيم

سمینار

عنوان
روش‌های تشخیص برخط تزریق اشکال

نگارنده:

فهرست مطالب

عنوان | **صفحه**

فهرست اشکال

فهرست جداول

چکیده

رمزنگاری فرآیندی است که در آن یک پیام، تنها توسط دریافت کننده مجاز آن قابل شناسایی باشد؛ بنابراین برای تامین امنیت باید اطلاعات در برابر استراق سمع و یا دست کاری ایمن باشند. با پیشرفت دانش انسان، هنر رمزنگاری به منظور ایجاد هرچه بیشتر امنیت اطلاعات بسیار پیچیده تر شده است. حملات مختلفی که بخش‌های گوناگونی از امنیت سامانه نهفته رمزنگاری را تهدید می‌کنند. مهاجم به وسیله حملات اشکال می‌تواند محرمانگی، تمامیت و دسترس‌پذیری سامانه را به خطر بی‌اندازد. بنابراین مقابله با این حملات برای حفظ امنیت کامل یک سامانه رمزنگاری از اهمیت بالایی برخوردار است. حملات تزریق خطا دسته از حملات تحلیل رمز هستند که توانایی کشف کلید مخفی بسیاری از پیاده‌سازی‌های الگوریتم‌های رمزنگاری را دارا می باشند. در نتیجه روش‌های بسیاری برای مقابله با این دسته از حملات کانال جانبی تاکنون ارایه شده است. از طرفی دیگر تکنیک‌های فراوانی برای تشخیص خطا در الگوریتم‌های رمزنگاری متقارن و نامتقارن پیشنهاد شده است. مهاجم به وسیله حملات خطا می‌تواند محرمانگی، تمامیت و دسترس‌پذیری سیستم‌های رمزنگاری را به خطر بیاندازد. بنابراین مقابله با این حملات برای حفظ امنیت کامل یک سامانه رمزنگاری از اهمیت بالایی برخوردار است. در این سمینار به مطالعه و ارزیابی روش‌های تشخیص برخط تزریق اشکال در سامانه‌های رمزنگاری پرداخته می‌شود. همچنین هر کدام از این روش‌های مقابله دارای مزایا و معایبی هستند که مورد بررسی قرار گرفت. بنابراین می‌توان نتیجه گرفت بهترین روش مقابله ترکیبی از روش‌های مختلف با توجه به عمل مورد نظر است.

کلمات کلیدی: رمزنگاری، حملات، تشخیص خطا، کلید.

فصل اول

مقدمه

۱-۱- مقدمه

همزمان با پیشرفت و فراگیری روزافزون مخابرات دیجیتال و افزایش حجم مبادله‌ی اطلاعات از طریق شبکه‌های متنوع مخابره‌ی داده نیاز به استانداردها و الگوریتم‌های مخابراتی با کارآیی بالا از جمله ضروریات دنیای امروز محسوب می‌شود. یکی از وظایف مهم صاحبنظران امروز دنیای ارتباطات طراحی الگوریتم‌هایی با قابلیت و انعطاف‌پذیری بالاست که بتواند پاسخگوی تقاضا برای شبکه‌های مخابراتی پرسرعت، پرظرفیت، کم حجم، کم هزینه و در عین حال امن باشد. بدون شک امنیت داده‌های مبادله شده و رمزکردن آنها از مهمترین مسائل در این حوزه به‌شمار می‌آید. تأمین امنیت در مبادلات مالی و بانکی و نیز ارتباطات نظامی نمونه‌هایی از اهمیت موضوع است. رمزشکنها همیشه و همه جا در کمین اطلاعات مالی یا نظامی هستند که فاش شدن آنها ممکن است عواقب جبران ناپذیر و وخیمی به دنبال داشته باشد. معمولاً شخص کنجکاو یا رمزشکن گاه سعی می‌کند اطلاعات مبادله‌شده را به دست بیاورد و محرمانگی آن را از بین ببرد. گاهی سعی در تغییر محتوای اطلاعات و خدشه دار کردن اصالت آن دارد و بعضاً سعی می‌کند تا خود را به جای شخص دیگری معرفی کند و به مطالب مورد علاقه‌اش پی ببرد. رمزنگاری، شیوه باستانی حفاظت از اطلاعات است که سابقه آن به حدود ٤٠٠٠ سال پیش از میلاد باز می گردد. امروزه رمزنگاری در دنیای مدرن از اهمیت ویژه ای برخوردار است، به طوری که رمزنگاری به عنوان یک روش مؤثربرای حفاظت از اطلاعات حساس به کار می رود. بنابراین، رمزنگاری از دیر بازبه عنوان یک ضرورت برای حفاظت از اطلاعات خصوصی در مقابل دسترسی‌های غیر مجاز در تجارت و سیاست و مسایل نظامی وجود داشته است به طور مثال تلاش برای ارسال یک پیام سری بین دو هم پیمان به گونه‌ای که حتی اگر توسط دشمن دریافت شود قابل درک نباشد، در رم قدیم نیز دیده شده است (رمز سزار). در سالیان اخیر رمزنگاری وتحلیل رمز از یک هنر پا را فراترگذاشته و یک علم مستقل شده است و در واقع به عنوان یک وسیله عملی برای ارسال اطلاعات محرمانه روی کانال‌های غیر امن همانند تلفن، ماکرویو و ماهواره‌ها شناخته می‌شود. پیشرفت علم رمزنگاری موجب به وجود آمدن روش‌های تحلیل مختلفی شده است به گونه ای که به طور متناوب سیستم‌های رمز مختلف شکسته شده‌اند. معروف‌ترین نمونه این نوع سیستم‌ها ماشین« انیگما » بوده است. انیگما ماشین رمز گذار و کد گذار وکد کننده‌ای بوده است که حزب نازی در زمان جنگ جهانی دوم برای ارسال پیام‌ها یشان از طریق رادیو به سایر نقاط استفاده می‌کردند. رمزنگاری که به طور عمده به دو بخش رمزنگاری متقارن یا رمزنگاری با کلید خصوصی و رمزنگاری نامتقارن یا رمزنگاری با کلید عمومی صورت می‌گیرد، تلاش می-

کند برای ایجاد یک ارتباط سری از طریق سیستم‌های مخابراتی و شبکه‌های کامپیوتری مباحث مربوط به محرمانگی و احراز هویت، را تحت فرض‌های مشخص به درستی اثبات نماید.

حملات علیه سیستم مخابراتی به دو نوع غیرفعال و فعال تقسیم می‌شوند. در حمله غیر فعال دشمن بصورت یک گیرنده غیر مجاز عمل می‌کند و در کانال غیر امن بین فرستنده و گیرنده استراق سمع می‌نماید. هدف در این نوع تهدید آن است که داده‌های ارسالی ضبط شوند و بعدا محتوای آنها کشف شود. در حمله فعال دشمن علاوه بر گیرنده غیرمجاز، فرستنده غیرمجاز نیز می‌باشد. یعنی توسط دستگاه‌ی داده‌های ارسالی یا سیگنال‌های کنترلی را عوض می‌کند و یا داده‌ها و سیگنال‌های کنترلی جعلی تولید می‌کند. هدف دشمن در این حمله، دادن اطلاعات اشتباه به گیرنده و یا جلوگیری از ارسال اطلاعات به آن است. تحلیگر رمز ممکن است خودی یا دشمن باشد که هدف خودی از تحلیل الگوریتم، بررسی نقاط ضعف الگوریتم به منظور اصلاح آن می‌باشد در صورتی که هدف دشمن دستیابی به کلید است. اعمالی که دشمن برای دستیابی به کلید یا متن اصلی انجام می‌دهد نام حمله بخود می‌گیرد. البته در بسیاری موارد رمزشکنی و حمله بصورت مترداف بکار می‌روند. حملات به سیستم‌های رمزنگاری به سه نوع کلی تقسیم می‌شود:

۱- حمله نوع اول (یا حمله فقط براساس متن رمز شده): در این نوع حمله دشمن الگوریتم رمزنگاری و رمزگشایی را می‌داند (ولی کلید را نمی شناسد) و متن رمز شده را نیز در اختیار دارد.

۲- حمله نوع دوم (یا حمله براساس متن اصلی معلوم): دشمن در این نوع حمله علاوه بر شناخت الگوریتم قسمتی از متن اصلی و متن رمز شده متناظر با آنرا در اختیار دارد.

۳- حمله نوع سوم (یا حمله براساس متن اصلی انتخاب شده): دشمن در این نوع حمله علاوه بر شناخت الگوریتم، برای هر متن اصلی دلخواه خود، متن رمز شده متناظر با آنرا در اختیار خواهد داشت. بعبارت دیگر فرض بر این است که دشمن کلیه اطلاعات لازم برای شکستن سیستم را در اختیار دارد و فقط کلید را نمی‌داند.

میزان مقاومتی را که سیستم رمزنگاری در مقابل حملات دشمن از خود نشان می‌دهد، امنیت سیستم گویند. سیستمی را که از لحاظ تئوری و عملی، قابل شکست نباشد، سیستم با امنیت کامل نامند و سیستمی را که از لحاظ تئوری قابل شکستن باشد، ولی از لحاظ عملی نیاز به زمان یا هزینه شکستن بسیار بالایی داشته باشد، سیستم با امنیت عملی گویند. گروه‌های تحقیقاتی زیادی تلاش می‌کنند که سیستم‌های رمزنگاری ایمن طراحی کنند. اما یک پیاده‌سازی بد می‌تواند تمامی این تلاش‌ها را بیهوده سازد. به همین دلیل در کنار

طراحی و تحلیل امنیت سیستم‌های رمزنگاری، بحث پیاده‌سازی آن‌ها در دستور کار گروه‌های تحقیقاتی قرار می‌گیرد. بنابراین، امنیت هر الگوریتم رمزنگاری مستقیماً به پیچیده بودن اصولی مربوط است که الگوریتم بر اساس آن بنا شده است.، اما اساساً امنیت رمزنگاری بر اساس پنهان ماندن کلید و نه الگوریتم مورد استفاده است. در حقیقت، با فرض اینکه که الگوریتم از قدرت کافی برخوردار باشد (یعنی اینکه ضعف شناخته‌شده‌ای که بتوان برای نفوذ به الگوریتم از آن استفاده کرد، وجود نداشته باشد) تنها روش درک متن اصلی برای یک استراق سمع کننده، کشف کلید است. در بیشتر انواع حمله، حمله‌کننده تمام کلیدهای ممکن را تولید و روی متن رمزشده اعمال می‌کند تا در نهایت یکی از آنها نتیجه درستی دهد. تمام الگوریتمهای رمزنگاری در برابر این نوع حمله آسیب‌پذیر هستند، اما با استفاده از کلیدهای طولانی‌تر، می‌توان کار را برای حمله‌کننده مشکل‌تر کرد. هزینه امتحان کردن تمام کلیدهای ممکن با تعداد بیتهای استفاده شده در کلید بصورت نمایی اضافه می‌شود، و این در حالیست که انجام عملیات رمزنگاری و رمزگشایی بسیار کمتر افزایش می‌یابد.

حمله تزریق خطا یک حمله فیزیکی جهت کسب اطلاعات رمزی داخلی برای نمونه‌های رمزگشایی با ایجاد یک نقص در واحدهای عملیاتی یا منطق ترتیبی بوده و با استفاده از تزریق نویز الکتریکی به منبع توان یا سیگنال ساعت یا با روشن کردن مدل توسط تابش الکترونیکی بوجود می‌آید. وقتی که توصیف ریاضی الگوریتم رمزنگاری یکسان است، مستقل از تکنولوژی هدف که در آن پیاده‌سازی شده است (برای مثال، یک برنامه میکروپردازنده، یک نوشته پایتون یا یک پیاده‌سازی سخت‌افزاری VHDL)، جزئیات پیاده‌سازی خاص به نشت اطلاعات یا نقاط حمله حساس فعلی/کنونی برای عامل بد منجر شود. بویژه، حمله کنندگان خطا بر فاسد شدن عناصر حافظه داخلیِ یک وسیله رمزنگاری استوار هستند. در پیاده‌سازی سخت افزاری، این معمولاً به معنای فاسد شدن محتوای رجیسترهای (فیلیپ-فلاپ‌ها) مدار، وقتی خود مدار عمل می‌کند، است. این خطاها معمولاً توسط پروژکت کردن نور لیزری در قالب سیلیکون القا می‌شوند، اما احتمال استفاده از تابش یونیزه برای القای خطاها نیز وجود دارد که می‌تواند یک انتخاب برای حمله کنندگان با بودجه کافی باشد. برای اینکه حمله معتبر باشد، خطاها بایستی در طول یک زمان خاص (چرخه زمان سنج) در جریان عمل اتفاق بیفتد. معمولاً حمله کننده می‌تواند با دقت، زمان اجرای القا را با نظارت کردن مصرف توان مدار تعیین کند، و اگر کافی نباشد، وی می‌تواند همچنین شبیه‌سازی‌های ورودی و زمان سنجی دستگاه را کنترل کند.