The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 183)
http://www.isecure-journal.org

Persian Abstract

بررسی پیچیدگی محاسباتی پیدا کردن پایه مینیمال برای حمله حدس و تعیین

شهرام خزایی[1] و فرخ‌لقا معظمی[2]

[1]دانشکده علوم ریاضی، دانشگاه صنعتی شریف، تهران، ایران
[2]پژوهشکده فضای مجازی دانشگاه شهید بهشتی، تهران، ایران

حمله حدس و تعیین یکی از حملات اساسی در رمزهای جریانی است و ابزار تحلیلی مشترکی برای اندازه‌گیری امنیت رمزهای جریانی است. اثربخشی این حمله به تعداد بیت‌های نامعلومی که باید توسط حمله‌کننده حدس زده شود تا سیستم رمزنگاری شکسته شود، وابسته است. در این مقاله رابطه‌ای بین مینم تعداد بیت‌هایی که در این حمله باید حدس زده شود و اندازه یک تطابق یکتای محدود شده مینیمم از یک گراف ارائه می‌دهیم. با استفاده از این رابطه نتیجه می‌گیریم که پیدا کردن مینیمم تعداد بیت‌های حدس زده شده مساله‌ای در کلاس پیچیدگی NP–کامل است. اگرچه بررسی مهارشدنی با پارامتر ثابت بودن این مساله بر اساس مینیمم تعداد بیتهای حدس زده شده یک مساله باز باقی مانده است ولی توانستیم نتایج مرتبطی در رابطه با آن پیدا کنیم. به‌علاوه مفاهیم گرافی که با مساله پیدا کردن مینیمم تعداد بیت‌های حدس زده شده ارتباط خیلی نزدیکی دارند را معرفی کردیم از جمله تطابق بدون دور، اعداد پرشی و عدد تعیین کننده یک تطابق کامل.

واژه‌های کلیدی: حمله حدس و تعیین، پیچیدگی محاسباتی، NP–کامل، مهارشدنی با پارامتر ثابت، تطابق یکتای محدود شده، تطابق بدون دور متناوب، تطابق کامل، عدد پرشی و عدد تعیین کننده.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 184)
http://www.isecure-journal.org

Persian Abstract

کدگذاری کانال به‌صورت امن و کارا مبتنی بر کدهای قطبی

بهنام مفاخری[1]، ترانه اقلیدس[2] و حسین پیل‌آرام[1]

[1]دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران
[2]پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

در این مقاله، چهارچوب جدیدی را برای کدگذاری توأم مبتنی بر کدهای قطبی ارائه می‌کنیم، به این صورت که یک ساختار جدید کدگذاری، یعنی کدهای قطبی، در طرحهای شبه Rao-Nam مورد بررسی قرار می‌گیرد. نتایج تحلیل رمز نشان می‌دهد که طرح ارائه شده دارای سطح امنیتی قابل قبول و همچنین طول کلید کمتری در مقایسه با طرح‌های پیشین است، همچنین طرح پیشنهادی در مقابل خطای کانال به صورت بهینه عمل می‌کند و دارای نرخ کدگذاری بیشتری است که می‌تواند به ازای ابعاد کد به اندازه کافی بزرگ، به ظرفیت کانال میل کند. مهمترین ویژگی طرح ارائه شده آن است که با افزایش طول کد، می‌توان به نرخ کد بیشتری دست یافت و همچنین سطح امنیت طرح نیز، بدون تغییرات زیادی در طول کلید، بهبود می‌یابد. و ویژگی‌های منتج شده از طرح آن را برای انتقال اطلاعات با سرعت زیاد مانند مخابرات ماهواره‌ای مناسب می‌سازد.

واژه‌های کلیدی: رمزنگاری کدمبنا، سیستم رمز Rao-Nam، کدگذاری کانال، ظرفیت شانون.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 185)
http://www.isecure-journal.org

Persian Abstract

یک پیاده‌سازی جدید نرم‌افزاری مقاوم در برابر حمله تحلیل همبستگی توان برای رمزهای متقارن با کمک هموارسازی توان مصرفی: بررسی موردی رمز SIMON

مرتضی صفائی پور[1] و محمود سلماسی‌زاده[2]

[1] دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران
[2] پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

در این مقاله، روشی جدید برای اعمال مقاوم‌سازی به طریق پنهان‌سازی در برابر حملات تحلیل همبستگی توان ارائه شده است. این روش برای پیاده‌سازی نرمافزاری بر اساس هموارسازی توان مصرفی دستگاه است. اگرچه روش پیشنهادی به هیچ‌یک از خصوصیات ساختاری الگوریتم رمز SIMON وابسته نیست، به عنوان یک مطالعه موردی، روش مذکور برای ارزیابی عملکرد روی این رمز پیاده‌سازی شده است. روش جدید پیشنهادی، تنها شامل عملگرهای AND معادل و XOR معادل است، زیرا هر الگوریتم رمزنگاری را می‌توان با دو عملگر پایه مانند AND و XOR پیاده‌سازی نمود. به کمک عملگرهای معادل تعریف شده، وزن همینگ و فاصله همینگ در هر زمان دارای مقادیر ثابتی هستند که این امر به کاهش وابستگی بین مقادیر پردازش‌شده و توان مصرفی می‌انجامد. به منظور ارزیابی عملی سربارهای پیاده‌سازی و همچنین میزان بهبود امنیت در برابر حملات تحلیل همبستگی توان، الگوی کدگذاری پیشنهادی بر روی یک رمز متقارن سبک به نام SIMON روی یک کارت هوشمند با پردازنده ATmega163 پیاده شده است. در این مقاله، امنیت به عنوان تعداد نمودارهای توانی تعریف شده است، که برای کمتر از آن تعداد، تمیز دادن کلید صحیح از دیگر کلیدهای فرضی بر اساس ضریب همبستگی آن‌ها در هیچ لحظه‌ای از زمان امکان‌پذیر نباشد. نتایج این پیاده‌سازی، بهبود ۳۵۰ برابری امنیت در برابر حملات تحلیل همبستگی توان را نشان می‌دهند.

واژه‌های کلیدی: حملات کانال جانبی، حملات تحلیل تحلیل توان تفاضلی، مقاوم‌سازی نرم‌افزاری، هموارسازی توان.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 186)
http://www.isecure-journal.org

Persian Abstract

حمله متن رمز شده معلوم به اسکرمبلرهای زمانی صوت، با استفاده از تصحیح اسپکتروگرام

حمزه قاسم‌زاده[۱،۲]، مهدی تاجیک‌خاص[۳] و حامد مهرآرا[۴]

[۱]گروه علوم ارتباطی و ناهنجاری‌های آن، دانشگاه ایالتی میشیگان، میشیگان، آمریکا
[۲]گروه ریاضیات محاسباتی، مهندسی و علم، دانشگاه ایالتی میشیگان، میشیگان، آمریکا
[۳]گروه برق و کامپیوتر، دانشگاه تبریز، تبریز، ایران
[۴]گروه مهندسی برق، دانشگاه خواجه نصیرالدین طوسی، تهران، ایران

بررسی‌های اخیر نشان داده‌اند که رمزهای جابجایی حوزه مولتی‌مدیا با استفاده از حمله متن پاک انتخابی به صورت کامل شکسته می‌شوند. از طرف دیگر حمله متن پاک انتخابی مدل بسیار قدرتمندی از دشمن بوده و در بسیاری از شرایط برقرار نمی‌باشد. به منظور نشان دادن ضعف امنیتی شدید در رمزهای جابجایی حوزه مولتی‌مدیا، این مقاله یک حمله متن رمز شده معلوم را پیشنهاد می‌دهد. به این منظور رمزهای جابجایی صوت بررسی شده و نشان می‌دهیم که افزونگی‌های ذاتی موجود در صوت امکان یک حمله موفق متن رمز شده معلوم را فراهم می‌کنند. به این منظور صوت با استفاده از تبدیل زمان کوتاه فوریه به حوزه زمان–فرکانس تبدیل می‌شود. پس از آن نشان می‌دهیم اسپکتروگرام صوت رمز شده رفتاری همانند یک پازل به هم ریخته دارد. پس از آن تکنیک‌های مختلفی هم‌چون پردازش تصویر، شاخه‌سازی و کران‌گذاری و تئوری گراف با یکدیگر ترکیب شده تا پازل‌های حاصله به بهترین شیوه حل گردند. در نهایت کلید از پازل حل شده استخراج شده و با استفاده از آن صوت رمزگشایی می‌گردد. بررسی‌های انجام شده نشان می‌دهند که دقت و قابلیت فهم صوت‌های بازگشایی شده به این روش به ترتیب ٪۸۷٫۸ و ٪۹۲٫۹ می‌باشند. درمقایسه با روش موجود، روش پیشنهادی این اعداد را به ترتیب ٪۵۰٫۹ و ٪۳۴٫۶ بهبود می‌بخشد. در نهایت با استفاده از تحلیل فاصله بین پنجره‌های لغزان اسپکتروگرام نشان می‌دهیم که می‌توان تخمین دقیقی از پارامترهای سیستم رمزگذار به‌دست آورد.

واژه‌های کلیدی: رمزشکنی، حمله متن رمز شده معلوم، سیستم‌های اسکرمبلینگ صوت، رمزهای مولتی‌مدیا، پازل، اسپکتروگرام.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 187)
http://www.isecure-journal.org

Persian Abstract

آشکارسازی وب‌سایت‌های تله با استفاده از جاسازی خط ویژگی وزن‌دار

مریم ایمانی[۱] و غلامعلی منتظر[۲]

[۱] دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران
[۲] دانشکده مهندسی فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران

هدف تله به دست آوردن اطلاعات شخصی کابران بدون اجازه آن‌ها و با استفاده از طراحی یک وب‌سایت جدید است که به تقلید از وب‌سایت حقیقی ایجاد شده است. متخصصان فناوری اطلاعات بر روی تعریف ویژگی‌های ممیزی که مشخص‌کننده‌ی وب‌سایت‌های تله باشند، توافق ندارند. بنابراین، تعداد نمونه‌های آموزشی قابل اطمینان در مسائل آشکارسازی تله محدود است. به علاوه، در میان نمونه‌های آموزشی در دسترس، نمونه‌های غیرنرمالی وجود دارند که سبب ایجاد خطا در طبقه‌بندی می‌شوند. برای مثال، ممکن است نمونه‌های تله‌ای وجود داشته باشند که دارای ویژگی‌های مشابه با نمونه‌های قانونی باشند و برعکس. یک روش استخراج ویژگی نظارت شده به نام جاسازی خط ویژگی وزن‌دار (WFLE) در این مقاله پیشنهاد شده است که مسائل اشاره شده را حل می‌کند. روش WFLE با استفاده از معیار خط ویژگی به طور مجازی نمونه‌های آموزشی تولید می‌کند. بنابراین می‌تواند مسئله‌ی اندازه‌ی نمونه کوچک را حل کند. به علاوه، WFLE به هر جفت از نقاط ویژگی، وزن‌های مناسبی را نسبت می‌دهد که کیفیت نامطلوب نمونه‌های غیرنرمال را تصحیح می‌کند. ویژگی‌های استخراج شده کارایی آشکارسازی وب‌سایت‌های تله را به خصوص با استفاده از مجموعه‌های آموزشی کوچک بهبود می‌بخشند.

واژه‌های کلیدی: آشکارسازی تله، استخراج ویژگی، خط ویژگی، نمونه آموزشی مجازی.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 2 (p. 188)
http://www.isecure-journal.org

Persian Abstract

بررسی ویژگی های جدید محتوای آلوده وب برای شناسای صفحات مخرب وب

جواد حاجیان‌نژاد[۱]، مجید وفایی جهان[۲]، محمد حسین طیرانی[۳] و زهره صدرنژاد[۴]

[۱]دانشکده مهندسی برق و کامپیوتر، دانشگاه امام رضا (ع)، مشهد، ایران
[۲]دانشکده مهندسی کامپیوتر، دانشگاه آزاد مشهد، مشهد، ایران
[۳]دانشکده مهندسی برق و کامپیوتر، دانشگاه گلاسکو، انگلستان
[۴]دانشکده مهندسی کامپیوتر، دانشگاه آزاد مشهد، مشهد، ایران

امروزه گسترش ابزار و استانداردهای طراحی و توسعه صفحات وب باعث شده است تا حملات مبتنی بر کدهای مخرب وب افزایش یابد. این کدهای مخرب می‌توانند با اهداف مختلفی از جمله نصب بد افزارها در کامپیوتر کاربران یا سرقت اطلاعات حساس مرورگر کاربر، در یک صفحه وب جایگذاری شوند. توسعه‌های اخیر در استانداردهای وب باعث شده است که مهاجمان این کدهای مخرب را به روش‌های جدیدتری به کار ببرند و آن‌ها را به شکلی مخفی یا مبهم سازی کنند که بتوانند از فیلتر های امنیتی شناسایی کدهای مخرب، فرار کنند. در این پژوهش به شناسایی صفحات مخرب با استفاده از روش‌های یادگیری ماشین می‌پردازیم. اکثر روش‌های ارائه‌شده براي شناسايي محتوایی صفحات مخرب وب بر پایه روش‌های یادگیری ماشین، بازه‌ی محدودي از حملات و ویژگی‌های صفحات مخرب را بررسي می‌کنند و یا ویژگی‌های ارائه‌شده توسط آن‌ها با آخرین ابزار موجود در طراحی و توسعه صفحات وب سازگار نمی‌باشد و باعث می‌شود که روش‌های آن‌ها ناقص باشد. در این پژوهش سعي کرده‌ایم که مجموعه کاملی از ویژگی‌های تاثیر گذار برای شناسایی صفحات مخرب وب شامل ویژگی های HTML (شامل ویژگی‌های HTML5)، JavaScript (شامل کتابخانه غنی Jquery)، VBScript و ویژگی‌های حملات XSS را شناسایی کنیم، که برای شناسایی بهتر فایل CSS حاوی اطلاعات صفحه وب را نیز مورد بررسی قرار داده‌ایم. در همین راستا فیلتر های زیادی برای شناسایی این ویژگی‌ها و استخراج آن‌ها از صفحات وب، طراحی کرده‌ایم. نتایج به دست آمده از پیاده‌سازی و شبیه‌سازی بر روی مجموعه داده جمع‌آوری شده توسط خزنده از لیست نام، دامنه و IP صفحات مخرب وب، نشان می‌دهد که صفحات مخرب وب، با افزودن ویژگی‌های پیشنهادشده در این پژوهش، با بیشترین مقدار صحت ۹۷٫۶۱ درصد و بیشترین مقدار F1-Measure برابر ۹۶٫۷۵ درصد با استفاده از الگوریتم C4.5-Tree، شناسایی می شوند. در پایان رتبه‌بندی از مهم‌ترین ویژگی‌های تأثیرگذار برای شناسایی یک صفحه مخرب وب، بیان گردیده است.

واژه‌های کلیدی: صفحات مخرب وب، ویژگی، یادگیری ماشین، محتوا، مبهم سازی، مهاجم.