The ISC Int'l Journal of Information Security
ISeCure

July 2012, Volume 4, Number 2 (p. 167)
http://www.isecure-journal.org

Persian Abstract

تحلیل سیستم‌های پنهان‌سازی با استفاده از مقادیر ویژه

فرشید فرحت[۲،۱]، ابوالفضل دیانت[۲،۱]، شاهرخ قائم‌مقامی[۱]، و محمدرضا عارف[۲]

[۱]پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

[۲]آزمایشگاه تئوری اطلاعات و مخابرات امن، دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران

روش‌های نهان‌کاوی عکس‌ها کلاً می‌توانند به دو صورت باشند. روش‌های نهان‌کاوی بینا که به منظور تحلیل الگوریتم پنهان‌سازی خاصی بکار می‌روند و یا روش‌های نهان‌کاوی کور که بیشتر بر مبنای روش‌های آماری، دسته‌ای از الگوریتم‌های پنهان‌سازی را تحلیل می‌کنند. روش‌های کور از این جهت که قابلیت آشکارسازی تغییرات اعمال شده به مشخصات آماری سیگنال پوشش را دارند، بیشتر مورد پسند هستند. به هر صورت اطلاعاتی درباره مواد مورد نیاز سیستم پنهان‌ساز مانند نوع الگوریتم پنهان‌سازی، خصوصیات سیگنال پوشش، الگوی مکان‌های جاسازی و غیره، می‌تواند تحلیلگر را برای بدست آوردن نتایج تشخیص بهتر کمک کند. بسیاری از مؤلفه‌های خصوصیات عکس‌ها مانند تابع مشخصه هیستوگرام، توزیع رنگ‌های مجاور و تحلیل جفت نمونه برای نهان‌کاوی مورد استفاده قرار گرفته است، اگرچه روش‌های نهان‌سازی معینی پیشنهاد شده است که قادر است این‌گونه تحلیل‌ها را با مدیریت جاسازی خنثی کند.

در این مقاله روش جدید تحلیلی برای تشخیص عکس نهان‌نگاری شده مطرح می‌شود که در مقابل بسیاری از الگوهای جاسازی مختلف که در صدد فریب تحلیلگران هستند، مقاوم است. روش اخیر بر مبنای تحلیل مقادیر ویژه ماتریس همبستگی پوشش است و برای اولین بار مورد استفاده قرارگرفته است. تجزیه عکس، محاسبه تابع همبستگی، چیدمان داده‌های همبسته و آزمایش مقادیر ویژه، از موضوعات چالش برانگیز روش تحلیلی اخیر محسوب می‌شود. روش پیشنهادی از سطح کم ارزش‌ترین بیت عکس در دامنه فضایی برای تشخیص نرخ‌های پنهان‌سازی کم که نگرانی اصلی حوزه‌ی پنهان‌سازی در کم ارزش‌ترین بیت است، بهره می‌برد و قابل گسترش به حوزه‌های تبدیل دیگر نیز می‌باشد. نتایج شبیه‌سازی نشان می‌دهد که روش پیشنهادی جدید در نرخ‌های کم از برخی روش‌های مشهور دیگر در این حوزه بهتر عمل می‌کند.

واژه‌های کلیدی: ماتریس همبستگی، تحلیل مقادیر ویژه، تخمین نرخ، نهان‌کاوی اطلاعات، جاسازی در کم‌ارزش‌ترین بیت.

The ISC Int'l Journal of Information Security
ISeCure

July 2012, Volume 4, Number 2 (p. 168)
http://www.isecure-journal.org

Persian Abstract

تحلیل الگوریتم رمز A5/1 در شبکه GSM

وحید امین غفاری[۱،۲]، علی ورداسبی[۳]، و جواد مهاجری[۳]

[۱]پژوهشکده پردازش علائم هوشمند، تهران، ایران

[۲]مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران، ایران

[۳]پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

الگوریتم A5/1 یکی از مشهورترین الگوریتم‌های رمز جریانی است که برای حفظ محرمانگی اطلاعات در فاصله هوایی بین گوشی و ایستگاه پایه در شبکه‌ی GSM بکار می‌رود. در این مقاله الگوریتم رمز A5/1 مورد تحلیل و بررسی قرار می‌گیرد. Biham و Dunkelman حمله‌ای با پیچیدگی زمانی و داده‌ای $2^{39.91}$ و $2^{21.1}$ ارائه کردند. در این مقاله به منظور بهبود حمله‌ی مزبور، روشی برای شناسایی و حذف حالت‌های بدون استفاده از جداول پیش‌فرض محاسبه و همچنین روشی نو برای دسترسی به جدول‌ها در مرحله‌ی برخط حمله پیشنهاد می‌شود که باعث کاهش پیچیدگی زمانی به $2^{37.89}$ و کاهش حافظه‌ی مورد نیاز به نصف می‌شود. علاوه بر این، یکی دیگر از ضعف‌های الگوریتم A5/1 با بررسی انتقال حالت داخلی و دوره تناوب دنباله کلید اجرایی آن مورد بحث قرار می‌گیرد و مدلی برای دسته‌بندی حالت‌های داخلی به دو دسته‌ی «سرانجام متناوب» و «ابتدائاً متناوب» ارائه می‌شود. سازگاری این مدل با نتایج حاصل از شبیه‌سازی، صحت مدل ارائه شده را تأیید می‌کند.

واژه‌های کلیدی: A5/1، جدول پیش‌محاسبه، حالات بدون استفاده، انتقال حالت داخلی، سرانجام متناوب

The ISC Int'l Journal of Information Security
ISeCure

July 2012, Volume 4, Number 2 (p. 169)
http://www.isecure-journal.org

Persian Abstract

بهبود امنیت روش جفت فاز تصادفی با استفاده از نظریه آشوب و تصویر فرکتالی

مطهره طاهری و سعید مظفری

دانشکده مهندسی برق و کامپیوتر دانشگاه سمنان، ایران

در این مقاله از روش رمزنگاری جفت فاز تصادفی استفاده شده است. کلیدهای رمزنگاری و رمزگشایی تصویر رمز شده که هم اندازه با تصویر ورودی هستند با کمک نظریه‌ی آشوب و تصویر فرکتالی تولید شده است و بدین ترتیب نیازی به ارسال خود کلیدها از طریق کانال امن نیست بلکه پارامترهای تولید کلید ارسال میگردد. همچنین برای واترمارکینگ تصویر رمز شده، قسمت‌های حقیقی و موهومی آن در تصویر میزبان بزرگ و نرمالیزه شده قرار می‌گیرد و ارسال می‌شود. بدین ترتیب امنیت رمزنگاری تصویر با روش جفت فاز تصادفی را بالا می‌بریم، که نتایج تجربی در انتهای مقاله گواه بر این امر است.

واژه‌های کلیدی: رمزنگاری جفت فاز تصادفی، روش تولید تصویر فرکتالی، روش مندلبروت و ژولیا، نظریه آشوب، دنباله‌ی لجستیک دو بعدی.

The ISC Int'l Journal of Information Security
ISeCure

July 2012, Volume 4, Number 2 (p. 170)
http://www.isecure-journal.org

Persian Abstract

همبسته‌سازی بلادرنگ هشدارهای سیستم تشخیص نفوذ و استخراج سناریوی حمله مبتنی بر روش پیشنیاز-پیامد

زینب زالی، مسعودرضا هاشمی، و حسین سعیدی

دانشکده برق و کامپیوتر، دانشگاه صنعتی اصفهان، ایران

سیستم‌های همبسته‌سازی هشدار سعی می‌کنند روابط بین هشدارهای تولیدشده توسط یک یا چند سیستم تشخیص نفوذ را به منظور کشف سناریوهای حمله تشخیص دهند. در این مقاله، یک روش جدید همبسته‌سازی هشدارهای سیستم تشخیص نفوذ ارائه می‌گردد که قادر به استخراج سناریوهای حمله به صورت بلادرنگ می‌باشد. روش پیشنهادی، با توجه به نکات قوت روش‌های سببی در عمل، مبتنی بر یک روش سببی است. جهت تعیین موقعیت امنیتی شبکه از نظر تلاش‌های نفوذ به شبکه، به یک روش بلادرنگ نیاز است. اکثر روش‌های سببی، به صورت برون‌خط قابل استفاده هستند و در کاربردهای بلادرنگ به دلیل محدودیت‌های حافظه و زمان قابل پیاده‌سازی نمی‌باشند. در روش پیشنهادی، پایگاه دانش الگوهای حمله در گرافی با نام گراف روابط سببی یا CRG مدل می‌شود. در حالت برون‌خط، قبل از شروع به کار سیستم، درخت‌های صف با توجه به همبستگی‌های احتمالی هشدارها براساس پایگاه دانش الگوهای حمله، ساخته می‌شوند. در حالت بلادرنگ، با دریافت هر هشدار جدید، می‌توان همبستگی آن هشدار را با هشدارهای دریافت‌شده قبلی تنها از طریق جستجو در درخت صف مربوطه به دست آورد. بنابراین با جستجو در یک درخت به جای جستجو در کل پایگاه دانش، زمان پردازش هشدار به صورت قابل توجهی کاهش پیدا می‌کند. علاوه بر این، روش ارائه‌شده در مقابل حملات آرام نیز مقاوم است. روش پیشنهادی با زبان C++ پیاده‌سازی شده و با استفاده از مجموعه داده‌های DARPA2000 تست شده است. نتایج آزمایشات انجام شده، صحت عملکرد و کارآیی روش را از نظر زمان تأیید می‌کند.

واژه‌های کلیدی: حمله، نفوذ، سناریوی حمله، سیستم تشخیص نفوذ، هشدار، همبسته‌سازی هشدار، گراف.

The ISC Int'l Journal of Information Security
ISeCure

July 2012, Volume 4, Number 2 (p. 171)
http://www.isecure-journal.org

Persian Abstract

تحلیل رجیستری، فایل‌های لاگ، و فایل‌های پری‌فِچ به منظور یافتن مدارک دیجیتال در برنامه‌های طراحی گرافیکی

اِنوس کِی. مابوتو و هِین اس. وِنتِر

دانشکده‌ی علوم کامپیوتر، دانشگاه پرتوریا، پرتوریا، آفریقای جنوبی

خروجی برنامه‌های طراحی گرافیکی، ردپاهایی از اطلاعات دیجیتال به جا می‌گذارند که می‌تواند در بررسی صحنه‌ی جرم دیجیتال، و به ویژه در مواردی که اسناد جعلی تولید شده است، مورد استفاده قرار گیرد. این مقاله به تحلیل فرایند بررسی صحنه‌ی جرم دیجیتال می‌پردازد که در آن تولید اسناد جعلی رخ داده است. این هدف، ابتدا با تشخیص مصنوعات صحنه‌ی جرم که پس از استفاده از برنامه‌های طراحی گرافیکی بر جای مانده‌اند، و سپس با تحلیل فایل‌های منتسب به این برنامه‌ها حاصل می‌شود. وقتی به تحلیل مصنوعات صحنه‌ی جرم که توسط برنامه‌ای تولید شده است پرداخته می‌شود، توجه خاص روی تعیین این موارد ضروری است که آیا برنامه طراحی گرافیکی نصب شده است؛ آیا برنامه استفاده شده است؛ و آیا می‌توان رابطه‌ای میان فعالیت‌های برنامه و جرم دیجیتالی برقرار کرد. پاسخ به این سؤالات، با یافتن اطلاعاتی در این خصوص در رجیستری، فایل‌های لاگ و فایل‌های پری‌فِچ انجام می‌شود. تحلیل فایل نیز شامل بررسی فایل‌های منتسب به این برنامه‌ها به منظور یافتن امضاهای فایل و فراداده می‌باشد. در انتها می‌توان تعیین کرد که آیا یک سیستم برای ساختن اسناد جعلی مورد استفاده قرارگرفته است یا خیر.

واژه‌های کلیدی: مدرک دیجیتال، بررسی صحنه‌ی جرم دیجیتال، مصنوعات صحنه‌ی جرم، برنامه‌های طراحی گرافیکی.

The ISC Int'l Journal of Information Security
ISeCure

July 2012, Volume 4, Number 2 (p. 172)
http://www.isecure-journal.org

Persian Abstract

ارائه یک مدل اعتماد آگاه از اطمینان مبتنی بر بازه

حسن شاکری و عباس قائمی بافقی
گروه کامپیوتر دانشگاه فردوسی مشهد

این مقاله یک چارچوب برای بازنمایی مجتمع اعتماد و اطمینان با استفاده از بازه‌ها ارائه می‌کند که شامل دو عملگر ضرب و جمع بازه‌های اعتماد است. این دو عملگر به ترتیب انتشار و تجمیع نظرهای اعتماد را نشان می‌دهند. خواص این عملگرها در مقاله مورد بررسی قرار گرفته است. همچنین روشی مبتنی بر چهار معیار برای تخمین اطمینان پیشنهاد شده است. نتایج آزمایش‌های انجام‌شده نشان می‌دهد که راهکار ارائه‌شده دقت استنتاج اعتماد را در مقایسه با راه‌حل‌های موجود افزایش می‌دهد.

واژه‌های کلیدی: اعتماد، اطمینان، بازه اعتماد، تجمیع اعتماد، انتشار اعتماد، تخمین اطمینان.