The ISC Int'l Journal of Information Security
ISeCure

January 2014, Volume 4, Number 1 (p. 87)
http://www.isecure-journal.org

Persian Abstract

بهبود سامانه رمزنگاری کلید مخفی رائو-نام با استفاده از کدهای EDF-QC-LDPC منظم

رضا هوشمند[۲،۱]، ترانه اقلیدس[۳] و محمدرضا عارف[۲]

[۱] دانشگاه آزاد اسلامی واحد علوم و تحقیقات، دانشکده مهندسی، تهران، ایران

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

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

در این مقاله، یک سامانه توأم رمزنگاری کلید مخفی–کدگذاری کانال با استفاده از کدهای بررسی توازن کم‌چگال شبه‌دوری منظم مبتنی بر خانواده های تفاضلی گسترش یافته (EDF-QC-LDPC) ارائه شده است. طول کلید سامانه توأم پیشنهادی با استفاده از یک الگوریتم فشرده‌سازی پیشنهادی کارا تا ۸۵ درصد کاهش یافته است. تحلیل‌های رمزنگاری نشان می‌دهند که سامانه پیشنهادی به دلیل بهبود در ساختار سامانه توأم رمزنگاری رائو-نام و انتخاب مناسب پارامترهای کد، از مقاومت بیشتری نسبت به سامانه اصلی در مقابل حمله متن آشکار انتخابی برخوردار است. همچنین سامانه پیشنهادی در مقایسه با سامانه‌های توأم رمزنگاری ارائه شده پیشین دارای بیشترین نرخ کد و عملکرد تصحیح خطای مناسبی است.

واژه‌های کلیدی: سامانه رمزنگاری کلید مخفی رائو-نام، کدهای بررسی توازن کم‌چگال، خانواده‌های تفاضلی.

The ISC Int'l Journal of Information Security
ISeCure

January 2014, Volume 4, Number 1 (p. 88)
http://www.isecure-journal.org

Persian Abstract

آزمون‌های مربع کای چندبخشی و پیچیدگی داده در آن‌ها

علی ورداسبی، محمود سلماسی‌زاده و جواد مهاجری

پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

آزمون‌های مربع کای (χ^2) عموماً برای تمایز مورد استفاده قرار می‌گیرند؛ با این حال، ترکیب این آزمون‌ها به‌منظور آزمودن همزمان چندین متغیر مستقل، نیازمند توجه ویژه‌ای است. در این مقاله، نشان داده می‌شود که آمارگان مربع کای در برخی از کارهای گذشته، نصف مقدار واقعی محاسبه شده‌است. بنابراین برای اجتناب از اشتباهات احتمالی آتی، مفهوم آزمون‌های مربع کای چندبخشی معرفی می‌شود. به منظور نشان دادن کاربرد آزمون‌های مربع کای چندبخشی، دو آزمون جدید معرفی و به Trivium با دورهای کاسته‌شده اعمال می‌شوند. این آزمون‌ها، نسخه‌های اصلاح‌شده‌ای از آزمون تک‌جمله‌ای صورت نرمال جبری (ANF) هستند، و با اعمال آن‌ها به Trivium با تعداد دورهای یکسان، پیچیدگی داده آن‌ها در حدود 2^4 برابر کم‌تر از آزمون‌های تک‌جمله‌ای ANF پیشین می‌باشد.

درجه آزادی بحرانی در یک آزمون مربع کای چندبخشی، برابر حداقل مقدار برای درجه آزادی تعریف می‌شود که به ازای آن آزمون در تمایز مجموعه نمونه‌ها از نمونه‌های تصادفی موفق باشد. این مقاله به بررسی رابطه بین این مقدار بحرانی و آمارگان مربع کای در یک آزمون مربع کای چندبخشی می‌پردازد. در نهایت، با بهره‌گیری از این رابطه، شیوه‌ای برای تخمین پیچیدگی داده در یک آزمون مربع کای چندبخشی تمایزگر معرفی می‌شود و برای حالت خاص Trivium با دورهای کاسته شده نشان داده‌می‌شود که این شیوه به درستی عمل می‌کند.

واژه‌های کلیدی: آزمون مربع کای چندبخشی، حملات تمایز، درجه آزادی بحرانی، Trivium.

The ISC Int'l Journal of Information Security
ISeCure

January 2014, Volume 4, Number 1 (p. 89)
http://www.isecure-journal.org

Persian Abstract

رویکردی ترکیبی مبتنی بر الگوریتم‌های کلونی زنبورهای مصنوعی و انتخاب منفی برای تشخیص نفوذ به شبکه‌های اقتضایی متحرک با پروتکل مسیریابی AODV

فاطمه بارانی و مهدی آبادی

گروه مهندسی کامپیوتر، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران

هر شبکه اقتضایی متحرک شامل مجموعه‌ای از گره‌های متحرک و بی‌سیم است که در آن هیچ‌گونه زیرساخت ثابتی وجود ندارد. شبکه‌های اقتضایی متحرک به دلیل ویژگی‌های ذاتی خود در برابر حمله‌های مسیریابی آسیب‌پذیر بوده و گره‌های بدخواه به آسانی می‌توانند فرآیند مسیریابی را در این شبکه‌ها مختل کنند. در رویکردهای متداول برای تشخیص چنین فعالیت‌های بدخواهانه‌ای، ابتدا یک نما از ترافیک عادی شبکه ایجاد شده و سپس هر فعالیتی که از این نما انحراف داشته باشد به عنوان یک فعالیت مشکوک شناسایی می‌شود. اما با توجه به تغییر سریع همبندی در شبکه‌های اقتضایی متحرک، استفاده از یک نمای ایستا برای تشخیص نفوذ به این شبکه‌ها کارا نیست.

در این مقاله، رویکردی ترکیبی و پویا مبتنی بر الگوریتم‌های کلونی زنبورهای مصنوعی و انتخاب منفی، به نام BeeID، برای تشخیص نفوذ به شبکه‌های اقتضایی متحرک با پروتکل مسیریابی AODV ارائه می‌شود. رویکرد پیشنهادی شامل سه مرحله آموزش، تشخیص و به‌روزرسانی است. در مرحله آموزش، یک الگوریتم انتخاب منفی چندین بار اجرا شده و مجموعه‌ای از شناساگرهای منفی بالغ برای پوشش حداکثری فضای غیرعادی تولید می‌شود. در مرحله تشخیص، از شناساگرهای منفی بالغ تولید شده برای جداسازی فعالیت‌های عادی از فعالیت‌های بدخواهانه استفاده می‌شود. در مرحله به‌روزرسانی، مجموعه شناساگرهای منفی بالغ با استفاده از یکی از دو روش به‌روزرسانی جزیی یا به‌روزرسانی کلی به‌روز می‌شود. برای تخمین میزان فضای غیرعادی پوشانده شده توسط شناساگرهای منفی بالغ و تعیین بازه‌های زمانی مناسب برای انجام فرآیند به‌روزرسانی کلی از روش انتگرال‌گیری مونت کارلو استفاده می‌شود. با استفاده از شبیه‌ساز NS2 تعدادی از حمله‌های مسیریابی بر روی شبکه‌های اقتضایی متحرک با پروتکل مسیریابی AODV شبیه‌سازی شده و کارآیی رویکرد پیشنهادی برای تشخیص این حمله‌ها مورد ارزیابی قرار می‌گیرد. نتایج آزمایش‌ها نشان می‌دهند که رویکرد پیشنهادی در مقایسه با سایر رویکردهای پویای قبلی قادر است توازن بهتری بین نرخ تشخیص و نرخ هشدار نادرست برقرار کند.

واژه‌های کلیدی: شبکه اقتضایی متحرک، حمله مسیریابی، تشخیص نفوذ، کلونی زنبورهای مصنوعی، انتخاب منفی، انتگرال‌گیری مونت کارلو.

The ISC Int'l Journal of Information Security
ISeCure

January 2014, Volume 4, Number 1 (p. 90)
http://www.isecure-journal.org

Persian Abstract

پرس‌وجوی مبتنی بر کلید خصوصی در داده‌های رمز شده

حماد افضلی[۱]، حامد نعمتی[۲] و رضا عزمی[۳]

[۱] آزمایشگاه امنیت سیستم‌عامل، دانشگاه الزهرا، تهران، ایران

[۲] دانشکده ارتباطات و علوم کامپیوتر، دانشگاه KTH، استکهلم، سوئد

[۳] دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران

امروزه کاربران سیستم‌های اطلاعاتی برای کاهش هزینه نگهداری و حمل اطلاعات از یک ماشین خدمت‌گزار مرکزی استفاده می‌کنند. از آنجا که این ماشین قابل اعتماد نیست، داده‌های محرمانه کاربران عموما به صورت رمزشده نگهداری می‌شود. از طرفی رمزنگاری به تنهایی نمی‌تواند امنیت اطلاعات را تضمین نماید، چرا که روش‌های ناامن جستجو در داده‌های رمزشده می‌تواند امنیت اطلاعات را به خطر اندازد.

اغلب روش‌های مدیریت و جستجو در داده‌های رمزشده با مشکلات اساسی از جمله سربار عملیات رمزنگاری و حملات تحلیل رمز مواجه‌اند. ما در این نوشتار یک مدل اولیه از جستجوی مبتنی بر کلید خصوصی در داده‌های متنی رمزشده ارائه می‌کنیم و سپس با بهبود تهدیدات مشکلات امنیتی و کارایی آن به یک مدل نهایی می‌رسیم. هدف اصلی ما، ارائه یک مدل عملی برای جستجوی کلمات در متون رمز شده با حداقل محدوده اعتماد است. همچنین ما یک مدل برقراری توازن بین کارایی و امنیت براساس نیازهای کاربر ارائه می‌کنیم. در مقایسه با روش‌های مشابه زمان پرس‌وجوی کلمات و حملات آماری کاهش یافته است.

واژه‌های کلیدی: داده‌های رمزشده، پرس‌وجو در داده‌های رمزشده، جستجوی مبتنی بر کلید خصوصی، حفاظت از حریم خصوصی.

The ISC Int'l Journal of Information Security
ISeCure

January 2014, Volume 4, Number 1 (p. 91)
http://www.isecure-journal.org

Persian Abstract

روشی غیرنظارتی و برخط برای تشخیص بات‌نت‌ها

موسی یحیی‌زاده و مهدی آبادی

گروه مهندسی کامپیوتر، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران

امروزه بات‌نت‌ها به عنوان یکی از خطرناک‌ترین تهدیدات در برابر زیرساخت اینترنت محسوب شده و برای فعالیت‌های بدخواهانه‌ای از قبیل انجام حملات جلوگیری از سرویس توزیع‌شده، ارسال هرزنامه و نشت اطلاعات شخصی مورد استفاده قرار می‌گیرند. روش‌های موجود برای تشخیص بات‌نت‌ها با وجود این که ایده‌های خوبی را ارائه می‌کنند، اما هنوز تا کامل‌شدن فاصله زیادی دارند. به دلیل این که بسیاری از این روش‌ها قادر به تشخیص بات‌نت‌ها در مراحل آغازین از چرخه‌حیات آن‌ها نبوده و یا به یک پروتکل فرمان و کنترل خاص وابسته هستند.

در این مقاله، برای حل مشکلات فوق یک روش غیرنظارتی و برخط با نام BotOnus پیشنهاد می‌شود که برای تشخیص بات‌نت‌ها نیازی به دانش پیشین ندارد. در این روش، ابتدا مجموعه‌ای از بردارهای جریان در انتهای هر دوره زمانی از ترافیک شبکه استخراج می‌شود. سپس این بردارهای جریان با استفاده از یک الگوریتم خوشه‌بندی با شعاع ثابت برخط به تعدادی خوشه گروه‌بندی می‌شوند. خوشه‌هایی که دارای حداقل دو عضو بوده و شباهت درون خوشه‌ای آن‌ها از یک آستانه شباهت بیش‌تر باشد، به عنوان خوشه‌های مشکوک به بات‌نت شناسایی شده و همه میزبان‌ها در این خوشه‌ها آلوده به بات تشخیص داده می‌شوند. نتایج آزمایش‌های انجام شده برای تشخیص بات‌نت‌های مبتنی بر HTTP، IRC و P2P نشان می‌دهد که روش پیشنهادی می‌تواند بات‌نت‌های مختلف را با متوسط نرخ تشخیص ۹۴٫۳۳٪ و متوسط نرخ هشدار نادرست ۳٫۷۴٪ شناسایی کند.

واژه‌های کلیدی: تشخیص بات‌نت، چرخه‌حیات بات‌نت، کانال فرمان و کنترل، خوشه‌بندی برخط.

The ISC Int'l Journal of Information Security
ISeCure

January 2014, Volume 4, Number 1 (p. 92)
http://www.isecure-journal.org

Persian Abstract

SEIMCHA: آزمون تصویری معنایی بازشناسی انسان از ماشین با استفاده از تبدیلات هندسی

مریم مهرنژاد[۱]، عباس قائمی بافقی[۱]، احد هراتی[۲]، احسان تورینی[۳]

[۱] آزمایشگاه امنیت اطلاعات و ارتباطات، گروه کامپیوتر، دانشگاه فردوسی مشهد، ایران

[۲] آزمایشگاه بینایی ماشین، گروه کامپیوتر، دانشگاه فردوسی مشهد، ایران

[۳] گروه کامپیوتر، دانشکده مهندسی، دانشگاه آزاد اسلامی واحد مشهد، ایران

از آنجایی که محافظت از برنامه های تحت وب روز به روز اهمیت بیشتری پیدا می کند، کپچاها (CAPTCHAs)، که از آن ها به عنوان آزمون بازشناسی انسان از ماشین نیز یاد می کنیم، بیشتر از قبل مورد توجه کاربران و طراحان امنیت قرار می گیرند. استفاده از مفاهیم بصری، امنیت و قابلیت استفاده را در آزمون های بازشناسی افزایش می دهد. چندین ایده اصلی در طراحی آزمون های بازشناسی مبتنی بر تصویر وجود دارد. در برخی از این روش‌ها برای امن‌تر کردن آزمون، یک نسخه تغییر یافته از عکسِ انتخاب شده از پایگاه داده (مثل عکس چرخیده شده) به کاربر نمایش داده می شود. در این مقاله دو روش متفاوت برای طراحی یک آزمون بازشناسی انسان از ماشین مبتنی بر تصویر ارائه می شود. روش اول (که آزمون بازشناسی مبتنی بر برچسب نامیده می‌شود) مبتنی بر عکس‌های از قبل برچسب خورده است و از تبدیلات هندسی برای افزایش امنیت استفاده می‌کند. روش دوم SEIMCHA یا آزمون تصویری معنایی بازشناسی انسان از ماشین با استفاده از تبدیلات هندسی، با حذف برچسب‌های عکس‌ها و و به کار بردن مفاهیم بصری معنایی به جای آن‌ها سعی در بهبود روش اول دارد. در واقع در روش دوم، مفهوم سمت بالای عکس به عنوان یک معنای بصری به کار برده شده است. راهکارهای ارائه شده توسط کاربران انسانی آزمایش و قابلیت استفاده هر روش ارزیابی شده است. امنیت سیستم نیز در قالب حملات مختلف تحلیل و بحث شده است. از طرفی مجموعه‌ای از مطالعات و آزمایش‌های اولیه بر روی میزان تغییرات لازم توسط تبدیلات هندسی و مناسب بودن خود عکس‌های اصلی نیز برای استفاده در این آزمون انجام شده است. نتایج آزمایش‌ها نشان می‌دهد که مجموعه راهکارهای ارائه شده برای استفاده در یک آزمون تصویری معنایی بازشناسی انسان از ماشین مناسب بوده و کار ارائه شده نسبت به کارهای مشابه امن‌تر و قابل استفاده‌تر است.

واژه‌های کلیدی: SEIMCHA، آزمون تصویری معنایی بازشناسی انسان از ماشین، تبدیلات هندسی، اشیا سه بعدی، سمت بالای عکس، آزمون بازشناسی مبتنی بر برچسب، پایگاه داده عکس‌های برچسب خورده، یادگیری ماشین، حمله حدس تصادفی، تطابق مستقیم.

The ISC Int'l Journal of Information Security
ISeCure

January 2014, Volume 4, Number 1 (p. 93)
http://www.isecure-journal.org

Persian Abstract

یک الگوریتم واترمارکینگ ویدئو مبتنی بر دنباله های آشوب

سمیه محمدی و احمد حکیمی

دانشکدهٔ مهندسی برق، دانشگاه شهید باهنر کرمان، ایران

خواص جالب دنباله های آشوبناک، محققین را ترغیب به استفاده از این دنباله ها در سیستم های واترمارکینگ در جهت برخورداری از یک روش کارا کرده است. ما در این مقاله برای دستیابی به یک سیگنال واترمارک شبه نویز، تصویر واترمارک باینری را در یک دنباله Tent Map پوشیده و مخفی میکنیم. که این عملکرد استخراج سیگنال واترمارک را توسط حمله کننده دشوار میسازد. موقعیت های واترمارکینگ بر طبق یک اصل مشخص انتخاب میشوند. نتایج تجربی نشاندهنده برتری روش پیشنهادی ما نسبت به روشهای مورد مقایسه در این مقاله میباشند. روش پیشنهادی این مقاله در یک سطح مطلوب از نظر مقاومت و امنیت قرار دارد.

واژه‌های کلیدی: دنباله های اشوبناک، مقاومت، امنیت، واترمارکینگ.