The ISC Int'l Journal of Information Security
ISeCure

January 2013, Volume 5, Number 1 (p. 111)
http://www.isecure-journal.org

Persian Abstract

بررسی اصول، روش‌ها و کاربردهای سیستم‌های پنهان‌سازی اطلاعات

محمدعلی اخایی[۱] و فرخ مروستی[۲]

[۱] عضو هیأت علمی دانشکده برق و کامپیوتر، پردیس دانشکده‌های فنی دانشگاه تهران

[۲] عضو هیأت علمی دانشکده برق و مدیر پژوهشکده مخابرات نظری، دانشگاه صنعتی شریف

با گسترش روزافزون دنیای رقمی و راه‌های آسان تبادل این گونه اطلاعات، پنهان‌نگاری رقمی مورد توجه بسیاری قرار گرفته است. در این مقاله سعی شده موضوع نهان‌نگاری و نشان‌گذاری مورد تحلیل و بررسی قرار گیرد. در این راستا ابتدا مفاهیم اولیه در پنهان‌سازی بیان گردیده و در ادامه نیازمندی‌ها و کاربردهای آن ارائه می‌شود. برای طراحی یک سیستم نهان‌نگاری کارا دانستن مفاهیم پایه‌ای از درج و استخراج نهان‌نگاره لازم و ضروری است. داشتن اطلاعات کافی از سیگنال میزبان (نظیر صحبت، صوت، تصویر و ویدئو) و آشنا بودن با ساختار گیرنده نهایی آن که چشم و گوش انسان است به طراح کمک می‌کند که عمل درج را به بهترین نحو انجام دهد. در این حالت نهان‌نگاره‌ی بیشتر با اثرات ظاهری/آماری کمتر در سیگنال میزبان جاسازی می‌گردد. در این خصوص روش‌های بسیاری معرفی و پیاده‌سازی شده است. البته شایان ذکر است که اگرچه الگوریتم‌های بسیار زیادی تاکنون ارائه گردیده اما به سادگی می‌توان این روش‌ها را در چند گروه کلی طبقه‌بندی کرد. در این مقاله پس از معرفی اجمالی سیستم بینایی و شنوایی انسان، روش‌های نخستین به همراه نسخه‌های پیشرفته و بهبودیافته آن‌ها معرفی می‌گردد. سپس یک مقایسه جامع بین این الگوریتم‌ها صورت پذیرفته تا یک طراح بتواند برحسب نیازها و امکاناتی که در اختیار دارد در مورد انتخاب الگوریتم و تنظیم پارامترهای آن تصمیم‌گیری کند. در ادامه با در نظر گرفتن مساله زندانی و زندانبان و سوء نیت زندانبان برای کشف یا خراب کردن ارتباط بین زندانیان، حملات به دو صورت عمدی و غیرعمدی تقسیم‌بندی شده است. این حملات که همانند یک سنگ محک برای ارزیابی کیفیت و عملکرد روش‌ها در نظر گرفته می‌شود در این‌جا معرفی و دسته‌بندی شده است.

واژه‌های کلیدی: امنیت، نهان‌نگاری، نشان‌گذاری، نهان‌کاوی، پایداری.

The ISC Int'l Journal of Information Security
ISeCure

January 2013, Volume 5, Number 1 (p. 112)
http://www.isecure-journal.org

Persian Abstract

طراحی و ارزیابی صوری پروتکل اصلاح شده رمزنگاری همه‌پخشی DZMBE+

مهدی سودخواه محمدی [1] و عباس قائمی بافقی [1]

[1] آزمایشگاه امنیت داده‌ها و ارتباطات، دانشکده کامپیوتر، دانشگاه فردوسی مشهد، خراسان رضوی، ایران

در این مقاله، یک طرح رمزنگاری همه‌پخشی براساس اشتراک سرآستانه‌ای و محاسبات چندطرفه امن ارائه می‌شود. این طرح عادلانه و پویا است و در نتیجه یک فرستنده می‌تواند اطلاعات را به هر زیرمجموعه دلخواه از کاربران سیستم به صورت همه‌پخشی ارسال کند و هیچ فرد متخلفی نمی‌تواند برتری اطلاعاتی نسبت به سایرین پیدا کند. ویژگی مهم دیگر این طرح مقاومت در برابر تبانی متخلفین است. به علت استفاده از محاسبات چندطرفه امن، یک متخلف نیاز به k همکار دارد تا بتواند طرح را با شکست مواجه کند که مقدار این پارامتر براساس انتخابی تعادلی بین ارتباطات بیشتر و امنیت بالاتر توسط مدیر سیستم انتخاب می‌شود. مقایسه با سایر طرح‌ها نشان‌دهنده بهبود در کارآیی و پیچیدگی طرح ارائه شده (از نظر هزینه محاسباتی رمز و ترجمه رمز پیام، طول متن رمز شده و طول کلید) است. این طرح توسط حساب کاربردی پی به‌صورت صوری مدل شده و توسط یک ابزار ارزیابی خودکار بنام ProVerif امنیت آن مورد بررسی قرار گرفته است.

واژه‌های کلیدی: رمزنگاری همه‌پخشی، محاسبات چندطرفه امن، اشتراک سرآستانه‌ای، روش‌های صوری، حساب پی کاربردی.

The ISC Int'l Journal of Information Security
ISeCure

January 2013, Volume 5, Number 1 (p. 113)
http://www.isecure-journal.org

Persian Abstract

یک پروتکل توافق کلید مبتنی بر شناسه برای محیط‌های دارای مراکز تولید کلید مستقل با امنیت قابل اثبات

محمد سبزی‌نژاد فراش[۱] و محمود احمدیان عطاری[۲]

[۱]دانشکده علوم ریاضی و کامپیوتر، دانشگاه خوارزمی، تهران، ایران

[۲]دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی خواجه نصیر الدین طوسی، تهران، ایران

پروتکل‌های توافق کلید به منظور برقراری ارتباط امن در شبکه‌های ارتباطی توزیع شده و ناامن مورد استفاده قرار می‌گیرند. پروتکل‌های توافق کلید مبتنی بر شناسه دسته‌ای از پروتکل‌های توافق کلید هستند که به دلیل سهولت در مدیریت کلید عمومی اخیرا بیشتر مورد توجه قرار گرفته‌اند. ایده اصلی رمزنگاری مبتنی بر شناسه بر این اساس است که شناسه کاربر به عنوان کلید عمومی وی در نظر گرفته می‌شود و کلید خصوصی متناظر توسط یک مرجع تولید کلید خصوصی (PKG) تولید می‌شود. با این وجود، در نظر گرفتن یک PKG برای تعداد زیادی از کاربران یا کاربران متعلق به سازمان‌های مختلف در عمل با چالش‌هایی مواجه است. بنابراین، در چنین شرایطی به‌کارگیری چندین PKG لازم و ضروری به نظر می‌رسد. به همین دلیل، در این مقاله یک پروتکل توافق کلید مبتنی بر شناسه برای محیط‌های چند PKG ارائه می‌دهیم که مبتنی بر رمزنگاری خم بیضوی (ECC) می‌باشد. ما همچنین امنیت پروتکل پیشنهادی را در مدل سروش تصادفی اثبات کرده و نشان می‌دهیم که تمام ویژگی‌های امنیتی شناخته شده را دارا می‌باشد. در مقایسه با پروتکل‌های مشابه، زمان اجرای پروتکل پیشنهادی ۱۰ درصد و هزینه‌های ارتباطی آن ۵۰ درصد پروتکل‌های مشابه می‌باشد.

واژه‌های کلیدی: رمزنگاری مبتنی بر شناسه، پروتکل توافق کلید، رمزنگاری مبتنی بر خم بیضوی، مدل سروش تصادفی.

The ISC Int'l Journal of Information Security
ISeCure

January 2013, Volume 5, Number 1 (p. 114)
http://www.isecure-journal.org

Persian Abstract

شناسایی پویای بدافزارها براساس استخراج الگوهای مجموعه مقادیر ثبات‌ها

محبوبه غیاثی [۱]، اشکان سامی [۱] و زهرا صالحی [۱]

[۱]دانشکده مهندسی برق و کامپیوتر، گروه مهندسی و علوم کامپیوتر و فناوری اطلاعات، دانشگاه شیراز، ایران

امروزه تحلیلگران امنیت برای این‌که بتوانند رشد نمایی بدافزارها را کنترل نمایند، از روش‌های پویا برای شناسایی اتوماتیک و تحلیل نمونه‌های مخرب استفاده می‌کنند. با توجه به اینکه شناسایی بدافزارهایی که از روش‌های مبهم‌سازی و چند ریختی استفاده می‌کنند توسط روش‌های ایستا، دشوار می‌باشد تحلیل پویای رفتارها در زمان اجرا می‌تواند تکنیک بهتری را برای شناسایی بدافزارها فراهم نماید. در این مقاله، از روش پویا برای استخراج خصیصه‌های فایل‌های باینری استفاده شده است. رفتارهای زمان اجرای باینری‌ها در یک محیط کنترل شده توسط ابزار تهیه شده به‌وسیله نگارندگان، ضبط و ثبت می‌گردد. در این مقاله از ایده‌ی DyVSoR استفاده شده است. در این ایده فرض می‌شود که رفتار زمان اجرای هر باینری، می‌تواند توسط مجموعه مقادیر رجیسترها منعکس گردد. بنابراین مقادیر رجیسترها قبل و بعد از فراخوانی هر API ثبت می‌گردد و به بردارهایی نگاشت می‌شود. برای شناسایی یک فایل ناشناخته کافیست که فایل ناشناخته با باینرهای موجود در مجموعه داده‌های آموزش مقایسه گردد. برای این منظور فاصله شباهت بین رجیسترهای فایل ناشناخته و تمام فایل‌های مجموعه داده محاسبه می‌شود. نتایج نشان می‌دهد که روش پیشنهادی توانسته است، نمونه‌های مخرب را با دقت ۹۶/۱% و نرخ مثبت کاذب ۴% شناسایی کند. مجموعه داده‌ها و جریانات اجرایی باینری‌ها در آدرس `http://home.shirazu.ac.ir/~sami/malware` قابل دسترسی می‌باشد.

واژه‌های کلیدی: شناسایی بدافزارها، فراخوانی API، تحلیل پویا، مقادیر رجیسترهای پردازنده، رجیسترهای x86.

The ISC Int'l Journal of Information Security
ISeCure

January 2013, Volume 5, Number 1 (p. 115)
http://www.isecure-journal.org

Persian Abstract

نشان‌گذاری مقاوم ضربی ویدئو با استفاده از مدل‌سازی آماری

ابوالفضل دیانت[۱]، محمدعلی اخایی[۱] ، و شاهرخ قائم مقامی [۳،۲]

[۱] دانشکده برق و کامپیوتر، پردیس دانشکده های فنی دانشگاه تهران، تهران، ایران

[۲]دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران

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

در این مقاله یک روش نشان‌گذاری مقاوم ضربی برای ویدئو ارائه شده است. در این روش، در گام نخست، سیگنال ویدئویی را به قالب‌های سه‌بعدی مکعبی تقسیم‌بندی می‌کنیم. سپس به هر قالب، تبدیل موجک سه‌بعدی اعمال می‌شود. در گام بعدی، در ضرایب فرکانس پایین تبدیل موجک به‌دست آمده، عملیات نشان‌گذاری را انجام می‌دهیم. مقاومت در برابر حملات عمدی و رخدادهای غیرعمدی را شاید بتوان مهم‌ترین علت انتخاب این ضرایب دانست. پنهان‌سازی پیام، با ضرب و یا تقسیم بر آن‌ها بر یک پارامتر ثابت که کنترل‌کننده توان عملیات نشان‌گذاری است، انجام می‌گردد. عملیات استخراج نشانه نیز توسط رویه بیشینه شباهت با یاری جستن از توزیع ضرایب تبدیل موجک، انجام می‌پذیرد. کارایی روش پیشنهادی توسط شبیه‌سازی مورد ارزیابی قرار گرفته است و نشان داده شده است که این روش دربرابر حملات و اثرات شناخته شده، مقاوم خواهد بود.

واژه‌های کلیدی: نشان‌گذاری ضربی ویدئو، کدگشایی با بیشینه شباهت، تبدیل موجک سه‌بعدی.

The ISC Int'l Journal of Information Security
ISeCure

January 2013, Volume 5, Number 1 (p. 116)
http://www.isecure-journal.org

Persian Abstract

رمزنگاری تصویر براساس تابع آشوبناک خیمه در حوزه‌های فرکانس و زمان

الهام حسنی[۱] و محمد عشقی[۲]

[۱]مرکز آموزش سازمان فناوری اطلاعات و ارتباطات شهرداری تهران

[۲]عضو هیأت علمی دانشکده برق و کامپیوتر دانشگاه شهید بهشتی

در این مقاله، به ارائه‌ی یک الگوریتم رمزنگاری تصویر با استفاده از تابع آشوبناک خیمه و یک تصویر کلیدی دلخواه پرداخته‌ایم. این الگوریتم از دو بخش تشکیل شده است. بخش اول الگوریتم در حوزه‌ی فرکانس و بخش دوم، در حوزه‌ی زمان کار می‌کند. در حوزه‌ی فرکانس از یک تصویر کلیدی دلخواه و یک عدد تصادفی که توسط نگاشت آشوبناک خیمه تولید شده است برای ایجاد تغییر در فاز تصویر اصلی استفاده می‌شود که نتیجه‌ی آن در حوزه‌ی زمان باعث تغییر و به هم ریختن مکان پیکسل‌ها می‌شود. در پایان در حوزه‌ی زمان از یک تصویر شبه تصادفی که توسط نگاشت آشوبناک خیمه تولید شده است برای ترکیب آن با تصویر حاصل از حوزه فرکانس و رمزنگاری استفاده می‌شود. از شبیه‌سازی کامپیوتری برای ارزیابی کارایی و امنیت الگوریتم و مقایسه نتایج حاصل از تصاویر رمزشده با دیگر کارهاي صورت گرفته استفاده‌شده‌است. معیارهای ارزیابی کارایی عبارتند از تست‌چی‌دو از هیستوگرام، ضریب همبستگی پیکسل‌ها، ضریب تعداد تغییر پیکسل‌ها، میانگین تفاوت سطح خاکستری پیکسل‌ها، میانگین مجذور اختلاف سطح خاکستری تصویر اصلی و رمز شده، میانگین قدر مطلق اختلاف سطح خاکستری تصویر اصلی و رمز شده، فضای کلید و حساسیت به مقادیر اولیه. نتایج مقایسات حاکی از کارایی و امنیت بالاتر الگوریتم رمزنگاری تصویر ارائه شده است.

واژه‌های کلیدی: رمزنگاری تصویر، نگاشت آشوبناک خیمه، تصویر کلیدی، حوزه فرکانس، حوزه زمان.