The ISC Int'l Journal of Information Security
ISeCure

January 2015, Volume 7, Number 1 (p. 83)
http://www.isecure-journal.org

Persian Abstract

یک پروتکل تبادل منصفانه خوشبینانه قابل ردیابی در مدل استاندارد

رامین گنجوی[۱]، مریم رجب‌زاده عصار[۱] و محمود سلماسی‌زاده[۲]

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

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

پروتکل تبادل منصفانه خوشبینانه روشی است که به دو طرف درگیر در پروتکل کمک می‌کند تا کالاهای دیجیتالی خود را به شکل منصفانه مبادله کنند به طوری که در پایان اجرای پروتکل، هر دو طرف به کالای مورد نظر خود دسترسی پیدا کنند یا هیچکدام از طرفین موفقیتی به دست نیاورند. در یک پروتکل تبادل منصفانه خوشبینانه نیاز به یک شخص سوم بین دو طرف مبادله است که به عنوان داور عمل کند. داور از منظر امضاکننده و وارسی‌کننده نیمه امین است و تنها هنگام بروز اختلاف بین طرفین، وارد عمل می‌شود. مشکل امنیتی که در این پروتکل‌ها وجود دارد بدین صورت است که اگر داور بدخواه عمل کرده و با وارسی کننده تبانی کند، امکان کامل کردن مبادله، بدون مجوز امضا کننده وجود دارد. هوانگ و همکارانش در سال ۲۰۱۱ با رسمی کردن ویژگی پاسخگویی این مشکل را پاسخ دادند. اما امنیت طرح هوانگ و همکارانش در مدل پیشگوی تصادفی اثبات می‌شود که یک مدل ایده‌آل است و در دنیای واقعی وجود ندارد. در این مقاله اولین طرح عام تبادل منصفانه خوشبینانه در مدل استاندارد ارائه می‌شود. امنیت پروتکل ارائه شده در مدل کلید منتخب و چندکاربره اثبات می‌شود.

واژه‌های کلیدی: تبادل منصفانه خوشبینانه، پاسخگویی، امضای حلقوی قابل ردیابی، مدل استاندارد.

The ISC Int'l Journal of Information Security
ISeCure

January 2015, Volume 7, Number 1 (p. 84)
http://www.isecure-journal.org

Persian Abstract

یک روش جستجوی محلی برای مسئله‌ی ریزتجمیعی

رضا مرتضوی [۱] و سعید جلیلی [۲]

[۱] دانشکده فنی و مهندسی، دانشگاه دامغان، دامغان، ایران

[۲] دانشکده برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، ایران

یکی از مکانیزم‌های قابل‌استفاده برای انتشار داده‌های آماری با حفظ حریم‌خصوصی ریزتجمیع است. از این مکانیزم برای پیاده‌سازی مدل حریم‌خصوصی k-بی‌نامی استفاده می‌شود. نشان داده شده است که در حالت کلی مسئله‌ی ریزتجمیع یک مسئله‌ی NP- سخت است. در این مقاله روشی مبتنی بر ارضای قیود در قالب یک الگوریتم جستجوی محلی ارائه می‌شود که می‌تواند به ازای سطح حریم‌خصوصی تعیین‌شده توسط k، داده‌های بی‌نام‌سازی‌شده و سودمند را تولید کند. مقایسه‌ی نتایج روش پیشنهادی با سایر الگوریتم‌های ریزتجمیع اخیر نشان از برتری روش ارائه‌شده دارد.

واژه‌های کلیدی: ریزتجمیع، انتشار داده‌ها با حفظ حریم‌خصوصی، k-بی‌نامی، خوشه‌بندی.

The ISC Int'l Journal of Information Security
ISeCure

January 2015, Volume 7, Number 1 (p. 85)
http://www.isecure-journal.org

Persian Abstract

ترکیبی از مدلهای کنترل دسترسی معنایی و خصوصیت-مبنا برای سازمان‌های مجازی

مرتضی امینی[1] و مجید آراسته[1]

[1]آزمایشگاه امنیت داده و شبکه، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران

یک سازمان مجازی شامل تعدادی سازمان واقعی با علایق مشترک است که امکان اشتراک منابع و تعامل بین سازمان‌ها را به منظور دستیابی به تعدادی هدف مشترک فراهم می‌نماید. یکی از نیازهای اساسی در سازمان‌های مجازی فراهم‌سازی مکانیزم‌های امنیتی و به خصوص مکانیزم کنترل دسترسی است. از آنجایی که یک سازمان مجازی محیطی پیچیده با تعداد زیادی کاربر و منبع است، استفاده از مدل‌های کنترل دسترسی سنتی نمی‌تواند پاسخگوی نیازهای امنیتی این محیط‌ها باشد. بسیاری از پیشنهادهای ارایه شده کنونی برای کنترل دسترسی در این محیط‌ها مبتنی بر خصوصیات کاربران و منابع است. در این مقاله، ترکیبی از مدل کنترل دسترسی معنایی SBAC و مدل کنترل دسترسی خصوصیت-مبنا ABAC بر مبنای یک هست‌شناسی مشترک از خصوصیت عامل‌ها در سازمان‌های مجازی پیشنهاد شده است. در این مدل هر سازمان عضو سازمان مجازی دسترسی به منابع خود را بر اساس یک مدل ارتقاءیافته از ABAC در سطح خود کنترل می‌کند. این در حالی است که در سطح سازمان مجازی، کنترل دسترسی در سطحی انتزاعی‌تر و بر اساس مدل ارتقاءیافته SBAC صورت می‌پذیرد. استفاده از هست‌شناسی عامل‌ها و منابع در این مدل ترکیبی، امکان مدیریت کنترل دسترسی را در سازمان‌های مجازی بزرگ با تعداد قابل توجهی سازمان تسهیل می‌نماید. با ترکیب مدل‌های SBAC و ABAC در دو سطح سازمان‌های واقعی و سازمان مجازی، ضمن برخورداری از مزایای هر دو مدل، معایب و مشکلات آن‌ها پوشش داده می‌شود. به منظور اثبات کاربردپذیری مدل پیشنهادی و ارزیابی زمان پاسخ یک سیستم کنترل دسترسی بر اساس مدل پیشنهادی در زبان جاوا و با استفاده از APIهای موجود از جمله Sun's XACML API، Jena، Pallet و Protégé پیاده‌سازی گردید.

واژه‌های کلیدی: سازمان مجازی، وب معنایی، کنترل دسترسی، مدل SBAC، مدل ABAC.

The ISC Int'l Journal of Information Security
ISeCure

January 2015, Volume 7, Number 1 (p. 86)
http://www.isecure-journal.org

Persian Abstract

بهینه‌سازی نهان‌نگاری تصویر با ترکیب الگوریتم ژنتیک و الگوریتم رقابت استعماری

فرامرز صادقی[1]، فاطمه زریسفی کرمانی[1] و مرجان کوچکی رفسنجانی[1]

[1]گروه علوم کامپیوتر، دانشکده ریاضی و کامپیوتر، دانشگاه شهید باهنر کرمان، کرمان، ایران

در این مقاله، یک روش جدید حاصل ترکیب رمزنگاری و نهان‌نگاری به منظور پنهان‌کردن اطلاعات محرمانه در تصاویر دیجیتال ارائه شده است. در این فرآیند، ابتدا داده محرمانه با روش جایگزینی تک‌حرفی، رمزنگاری شده و سپس با استفاده از الگوریتم پیشنهادی در تصویر میزبان جاسازی می‌شود. در الگوریتم جاسازی پیشنهادی، از الگوهای تصادفی مبتنی بر منحنی‌های فضاپرکن به منظور یافتن بهترین پیمایش بلوک‌های تصویر میزبان استفاده می‌شود. سپس روش انطباق زوج پیکسل بهینه شده به کمک الگوریتم رقابت استعماری گسسته براي جاسازی داده محرمانه رمزشده به‌کاربرده می‌شود. از آنجا که یافتن لیست جانشینی شبه بهینه در روش انطباق زوج پیکسل یک مسئله گسسته است، بنابراین از عملگرهای وراثتی به منظور اصلاح الگوریتم رقابت استعماری و ارائه نسخه گسسته آن استفاده شده‌است. در نهایت با محاسبه میانگین مربع خطا (MSE) و حدبالای سیگنال نسبت به نویز (PSNR) که دو معیار اندازه‌گیری کیفیت بصری تصاویر محسوب می‌شوند کارایی روش پیشنهادی در مقایسه با سایر روش‌ها نشان داده می‌شود.

واژه‌های کلیدی: بهینه‌سازی ترکیبی، الگوریتم رقابت استعماری گسسته، الگوریتم وراثتی، نهان‌نگاری، روش انطباق زوج پیکسل و منحنی‌های فضاپرکن.

The ISC Int'l Journal of Information Security
ISeCure

January 2015, Volume 7, Number 1 (p. 87)
http://www.isecure-journal.org

Persian Abstract

الگوریتم تجمیع شهرت مبتنی بر شایعه‌ی گروه‌محور

صفیه قاسمی فلاورجانی[۱]، بهروز ترک لادانی[۱] و سیمین قاسمی[۲]

[۱]دانشکده‌ی مهندسی کامپیوتر، دانشگاه اصفهان، ایران
[۲]دانشکده‌ی مهندسی کامپیوتر، دانشگاه پیام‌نور، ایران

یکی از موضوعات مهم در شبکه‌های نظیر به نظیر وجود گره‌های بدخواه هستند که کارایی چنین شبکه‌هایی را کاهش می‌دهد. یکی از راه‌حل‌های پیشنهادی برای تشخیص و جداسازی گره‌های بدخواه، سیستم شهرتی است که گره‌ها را براساس رفتار آن‌ها رتبه‌بندی می‌کند. GossipTrust یکی از الگوریتم‌های پیشنهاد شده‌ی قبلی برای تجمیع شهرت در شبکه‌های نظیر به نظیر براساس مفهوم شایعه می‌باشد. علی‌رغم اهمیت و برتری این الگوریتم، تعداد زیاد گره‌ها در شبکه، منجر به افزایش زمان اجرا و نیز کاهش صحت نتایج نهایی می‌شود.

در این مقاله، الگوریتم تجمیع شهرت گروه‌محوری براساس شایعه (GGRA) پیشنهاد شده است. در GGRA، GossipTrust میان اعضای هر گروه و مابین گروه‌ها اجرا می‌گردد. به دلیل کاهش در تعداد گره‌ها و استفاده از گراف با اتصالات قوی به جای گراف ضعیف، الگوریتم شایعه در GGRA با سرعت بیشتری اجرا می‌گردد. با استفاده از گروه‌بندی، نه تنها تجمیع شهرت مقیاس‌پذیرتر میگردد، بلکه به دلیل کاهش در تعداد خطاهای ارتباط شایعه، نتایج شایعه‌پراکنی صحت بیشتری دارند. ارزیابی الگوریتم پیشنهادی و مقایسه‌ی آن با GossipTrust، نتایج مورد انتظار را تایید می‌کند.

واژه‌های کلیدی: شبکه‌ی نظیر به نظیر، الگوریتم شایعه، تجمیع شهرت، شبکه‌ی نظیر به نظیر گروهی، شهرت گروه‌محور.

The ISC Int'l Journal of Information Security
ISeCure

January 2015, Volume 7, Number 1 (p. 88)
http://www.isecure-journal.org

Persian Abstract

جایابی امن ثبات‌ها به منظور جلوگیری از درج مدارهای تهدیدآمیز و بهبود تشخیص تروجان سخت‌افزاری

مهرشاد وثوقی[1] و علی جهانیان[2]

[1]دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد قزوین، قزوین، ایران
[2]دانشکده علوم و مهندسی کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران

امروزه پروسه ساخت تراشه‌های الکترونیکی بدلیل محدودیت‌هایی از قبیل هزینه ساخت و زمان ارائه به بازار به شرکت‌های شخص ثالث سپرده می‌شود. در این شرایط آسیب‌پذیری طرح اصلی یکی از دغدغه‌های بزرگ طراحان سیستم‌های سخت افزاری خواهد بود. در این مقاله تکنیکی جدید برای جایابی سلول‌ها ارائه کرده‌ایم که درج مدارات اضافی تهدیدآمیز تحت عنوان تروجان‌های سخت‌افزاری را مشکل کرده و یا تشخیص وجود آن‌های تسهیل خواهد کرد. نتایج شبیه‌سازی بر روی مدارهای آزمون نشان می‌دهند که الگوریتم جایابی ارائه شده با هزینه سربار و تاخیر بسیار مناسب تشخیص تروجان‌های سخت‌افزاری را تا ۲۰ درصد ارتقاء می‌بخشد.

واژه‌های کلیدی: امنیت سخت افزار، جایابی سلول‌ها، ساختار درخت ساعت.