The ISC Int'l Journal of Information Security
ISeCure

July 2014, Volume 6, Number 2 (p. 193)
http://www.isecure-journal.org

Persian Abstract

یک مدل مخاطره برای فرآیندها در محیط ابر

ارنستو دامیانی[1]، استلویو چیماتو[1] و گابریل جیانینی[1]

[1]دانشکده علوم کامپیوتر، دانشگاه مطالعاتی میلان، ایتالیا

به‌طور سنتی، ارزیابی مخاطره شامل ارزیابی احتمال رخداد حوادث ناشی از تهدیدات و حملات شناخته شده و همچنین شدت این حملات بر اساس میزان تأثیر آن‌ها می‌باشد. بررسی مخاطره‌ی فرآیندهای محیط ابر به علت نبود تاریخچه‌ای از حملات اعمال شده بر آن‌ها امری دشوار است. هم‌چنین خاصیت پویا و چندعاملی پردازش ابری، ارزیابی میزان شدت این حملات را به‌طور چشمگیری به مجموعه عوامل دخیل در اجرای یک فرآیند ابری وابسته می‌سازد. در این مقاله، با پرداختن به این مشکلات، اسلوبی نوین، کمی، و فرآیندگرا برای ارزیابی مخاطره با تمرکز بر مخاطرات ناشی از افشای اطلاعات در بستر رایانش ابری ارائه شده است. مزیت‌های کلیدی روش ارائه شده عبارتند از: ۱) رهیافتی کاملاً کمی و تکرارشونده که باعث می‌شود عوامل دخیل در اجرای فرآیند بتوانند نسخه‌های مختلفی از فرآیندهای ابری را باهم مقایسه نمایند (مثلاً انتخاب یک فرآیند با یا بدون کنترل‌های امنیتی). ۲) تخمین‌های احتمالی غیرمبتنی بر میزان تکرار تهدید که امکان تحلیل تهدیدهایی که تاریخچه مناسبی از آن‌ها در دسترس نیست را فراهم می‌آورد. ۳) پشتیبانی از مقایسه‌ی سریع بصری برای نمایه مخاطره مرتبط با فرآیندهای مختلف حتی در مواقعی که میزان تأثیر مخاطره را نتوان به‌طور دقیق اندازه گرفت.

واژه‌های کلیدی: پردازش ابری، ارزش داده، ارزیابی مخاطره، محسبات امن.

The ISC Int'l Journal of Information Security
ISeCure

July 2014, Volume 6, Number 2 (p. 194)
http://www.isecure-journal.org

Persian Abstract

آرتمیا: یک خانواده از طرح‌های رمزگذاری احراز اصالت شده با امنیت اثبات‌پذیر

جواد علیزاده[۱،۲]، محمدرضا عارف[۲] و نصور باقری[۳]

[۱]آزمایشگاه تئوری اطلاعات و مخابرات امن (ISSL)، دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران
[۲]مرکز تحقیقات فتح، دانشکده و پژوهشکده مهندسی فاوا، دانشگاه جامع امام حسین (ع)، تهران، ایران
[۳]دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران

در سال‌های اخیر، شبکه‌های اجتماعی برخط رشد قابل توجهی از نظر تعداد کاربران و محبوبیت داشته‌اند. در شبکه‌های اجتماعی، کاربران از طریق طرح‌های رمزگذاری احراز اصالت شده، محرمانگی و احراز اصالت پیام را همراه باهم برآورده می‌کنند. در این مقاله خانواده‌ای از طرح‌های رمزگذاری احراز اصالت شده اختصاصی به نام آرتمیا توضیح داده می‌شود. آرتمیا یک طرح رمزگذاری احراز اصالت شده برخط است که از داده وابسته نیز پشتیبانی می‌کند. در این طرح از یک سبک عمل مبتنی بر جایگشت به نام JHAE استفاده شده است که در مدل جایگشت ایده‌آل، امنیت اثبات‌پذیر دارد. برای رمزگشایی با استفاده از آرتمیا، نیازی به معکوس جایگشت مورد استفاده نیست. این امر باعث کارایی پیاده‌سازی می‌شود. جایگشت‌های آرتمیا ساختار ساده و کارایی دارند و در برابر تحلیل‌های خطی و تفاضلی دارای امنیت اثبات‌پذیر هستند. در این جایگشت‌ها از لایه‌های MDS بازگشتی استفاده شده است که به راحتی در نرم‌افزار و سخت‌افزار قابل پیاده‌سازی می‌باشند.

واژه‌های کلیدی: محرمانگی، احراز اصالت، امنیت اثبات‌پذیر، رمزگذاری احراز اصالت شده، آرتمیا.

The ISC Int'l Journal of Information Security
ISeCure

July 2014, Volume 6, Number 2 (p. 195)
http://www.isecure-journal.org

Persian Abstract

یک پروتکل صورت‌حساب انکارناپذیر در شبکه‌های نامتجانس 3G-WLAN

علی فانیان[1]، فریبا اعلمی‌فر[1] و مهدی برنجکوب[1]

[1]دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی اصفهان، اصفهان، ایران

در چند سال اخیر ارتباطات بی‌سیم با ارائه خدمات متنوع به کاربران به سرعت رو به گسترش است. در این ارتباط، شبکه‌های سلولي نسل سوم و شبکه‌های بی‌سیم محلی دو نمونه مهم از فناوری بی‌سیم هستند که به شکل گسترده مورد استفاده قرار گرفته‌اند. شبکه‌های سلولی نسل سوم (3G) می‌توانند سرویس خود را در نواحی تحت پوشش گسترده ارائه کنند. در مقابل، شبکه‌های بی‌سیم محلی (WLAN) امکان برقراری ارتباط بی‌سیم را با نرخ بالا اما در محدوده فضایی کوچک، حدود چند صد متر، فراهم می‌کنند. با توجه به ویژگی‌های این دو شبکه می‌توان خدمات آن‌ها را مکمل یکدیگر دانست. از این رو، اجتماع این دو نوع شبکه و تشکیل شبکه‌ای نامتجانس نوید بخش دستیابی به شبکه‌ای بی‌سیم با قابلیت استفاده از مزایای هر دو شبکه قبلی است. در شبکه نامتجانس مورد نظر، خدماتی هم چون احراز اصالت، هزینه استفاده، و کیفیت خدمات از موارد مهمی هستند که باید برای دستیابی به آن‌ها راه‌کارهایی اندیشیده شود. در این مقاله، پروتکل احراز اصالت دوطرفه و صورت‌حساب انکارناپذیری با نام NRBP ارائه شده است که در آن کاربر شبکه نسل سوم ابتدا خود را به شبکه محلی بی‌سیم احراز اصالت می‌نماید تا از طریق آن به شبکه اینترنت دسترسی پیدا کند. شبکه محلی نیز خود را به کاربر احراز اصالت می‌نماید تا کاربر با اطمینان کامل، از خدمات شبکه بی‌سیم محلی استفاده کند. پروتکل NRBP مبتنی بر پروتکل‌های توسعه‌پذیر است و در آن سعی شده است احراز اصالت کاربر به شبکه محلی بی‌سیم با هزینه پردازشی کم و با استفاده از عملیات رمزنگاری متقارن انجام شود. نتایج ارزیابی‌های انجام‌گرفته گویای کارآمدی پروتکل NRBP است.

واژه‌های کلیدی: شبکه محلی بی‌سیم، شبکه سلولی، احراز اصالت، شبکه نامتجانس، رمزنگاری متقارن، رمزنگاری نامتقارن، سرویس انکارناپذیری.

The ISC Int'l Journal of Information Security
ISeCure

July 2014, Volume 6, Number 2 (p. 196)
http://www.isecure-journal.org

Persian Abstract

یک رویکرد ترکیبی برای تشخیص نفوذ پایگاه‌داده در سطوح تراکنش و میان‌تراکنش

مصطفی دورودیان[1] و حمیدرضا شهریاری[1]

[1]دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران

امروزه اطلاعات نقش مهمی در سازمان‌ها ایفا می‌کند. اطلاعات حساس اغلب در پایگاه‌های داده ذخیره می‌شوند. مکانیزم‌های سنتی از قبیل رمزنگاری، کنترل دسترسی و تصدیق اصالت سطح بالایی از اطمینان را فراهم نمی‌کنند. بنابراین وجود سامانه‌های تشخیص نفوذ در پایگاه‌داده امری ضروری به‌نظر می‌رسد. در این مقاله یک سامانه تشخیص نفوذ پایگاه‌داده به‌منظور تشخیص حملات در سطوح تراکنش و میان‌تراکنش (وظیفه کاربر) ارائه می‌شود. برای این منظور ابتدا یک روش تشخیص در سطح تراکنش ارائه می‌شود که مبتنی بر توصیف تراکنش‌های مورد انتظار در سطح برنامه‌های کاربردی پایگاه‌داده می‌باشد. سپس در سطح میان-تراکنش یک روش تشخیص ناهنجاری پیشنهاد می‌شود و از رویکرد داده‌کاوی برای یافتن قوانین وابستگی و دنباله میان‌تراکنشی استفاده می‌شود. از مزایای این سامانه نسبت به سامانه‌های تشخیص نفوذ پایگاه‌داده پیشین، توانایی تشخیص رفتارهای مخرب در هر دو سطح تراکنش و میان‌تراکنش می‌باشد. همچنین این سامانه با بهره‌گیری از مزایای ترکیب رویکردهای تشخیص مبتنی بر توصیف و تشخیص مبتنی بر ناهنجاری موجب به حداقل رساندن هشدارهای مثبت کاذب و منفی کاذب می‌شود. آزمایش‌هایی به‌منظور ارزیابی درستی عملکرد سامانه پیشنهادی انجام شده است. نتایج ارزیابی‌های عملی حاکی از بالا بودن میزان درستی عملکرد و سودمندی سامانه پیشنهادی می‌باشد.

واژه‌های کلیدی: تشخیص نفوذ، امنیت پایگاه‌داده، ماشین وضعیت، وابستگی میان‌تراکنشی، دنباله میان‌تراکنشی.

The ISC Int'l Journal of Information Security
ISeCure

July 2014, Volume 6, Number 2 (p. 197)
http://www.isecure-journal.org

Persian Abstract

یک روش نهان‌کاوی کور تصویر در حوزه کانتورلت برمبنای یک مجموعه ویژگی‌های توسعه داده شده

احسان شاکری[1] و شاهرخ قائم‌مقامی[1]

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

هدف اصلی نهان‌کاوی تصویر کشف وجود اطلاعات مخفی در تصویر نهانه است. در این مقاله یک روش نهان‌کاوی کور تصویر در حوزه کانتورلت معرفی می‌کنیم و سپس نشان می‌دهیم که عمل درج، آماره‌های ضرایب کانتورلت تصویر را تغییر می‌دهد. تصویر مشکوک به حوزه کانتورلت انتقال داده شده و سپس آماره‌های ضرایب کانتورلت تصویر به عنوان خصوصیات کشف نهان‌کاوی استفاده می‌شوند. قدرمطلق ممان‌های زرنایک و ممان‌های تابع مشخصه‌ی ضرایب زیرباندهای کانتورلت برای تشخیص تصویر نهانه به‌کار می‌رود. قدرمطلق ممان‌های زرنایک برای بررسی میزان تصادفی بودن تصویر مورد تست و ممان‌های تابع مشخصه‌ی ضرایب زیرباندهای کانتورلت برای بررسی میزان تغییرات در هیستوگرام ضرایب زیرباندهای کانتورلت بکار گرفته شده‌است. سپس، این مجموعه خصوصیات به یک SVM غیرخطی با هسته‌ی RBF اعمال شده تا تصویر مشکوک شناسایی گردد. نشان می‌دهیم که عمل درج آماره‌های ضرایب کانتورلت تصویر را تغییر می‌دهد که این نکته می‌تواند به عنوان کلیدی برای شناسایی تصویر نهانه باشد. نتایج شبیه‌سازی تایید می‌کند که خصوصیات معرفی شده نسبت به تغییرات ناشی از عمل درج بسیار حساس هستند. همچنین، نتایج شبیه‌سازی بیانگر برتری روش پیشنهادی بر روش‌های نهان‌کاوی مورد مقایسه در مقابل ۵ روش نهان‌نگاری معروف در حوزه JPG است. بهبود حاصل شده در نتایج عمدتاً به‌دلیل حساسیت بالای ممان‌های زرنایک به نویز درج است که بطور متوسط حدود ۴ درصد بهبود در عمل تشخیص نهانه داریم.

واژه‌های کلیدی: نهان‌کاوی کور، تبدیل کانتورلت، ممان‌های زرنایک، ممان‌های تابع مشخصه، تحلیل‌های آماری.

The ISC Int'l Journal of Information Security
ISeCure

July 2014, Volume 6, Number 2 (p. 198)
http://www.isecure-journal.org

Persian Abstract

یک روش تشخیص دو مرحله‌ای جهت تشخیص حمله‌ی کرم‌چاله در شبکه‌های موردی سیار

شیوا شماعی[1] و علی موقر[1]

[1]دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران

حمله‌ی کرم‌چاله از جمله حملاتی است که از مسیریابی توزیع‌شده در شبکه‌های موردی سیار سوءاستفاده می‌کند. در این حمله حداقل دو گره که در فاصله‌ی دوری از یکدیگر قرار دارند با برقراری تونل بین خود، خود را همسایه‌ی یک گامی یکدیگر معرفی می‌کنند. از این رو با فریب سایر گره‌های شبکه منجر به اختلال در فرآیند مسیریابی می‌شوند. به‌علاوه گره‌های بدخواه با ایجاد تونل بین خود بستری برای اجرای سایر حملات فراهم می‌آورند. در این مقاله روش تشخیصی برای این حمله ارائه شده که به دو پارامتر متوسط تأخیر هر گام و رفتار گره‌های همسایه در ارسال بسته‌های داده توجه می‌کند. این روش بدون نیاز به سخت‌افزار اضافی یا همزمان‌سازی گره‌ها قادر به تشخیص تمام حالات حمله از جمله حالات درون شبکه‌ای یا برون شبکه‌ای و حالات مخفی یا آشکار است. همچنین علاوه بر تشخیص حمله، گره‌ی بدخواه را شناسایی می‌کند و از اجرای مجدد حمله توسط آن جلوگیری می‌کند. نتایج شبیه‌سازی نشان دهنده‌ی برتری روش پیشنهادی نسبت به روش‌های مورد مقایسه در این مقاله است.

واژه‌های کلیدی: شبکه‌های موردی سیار، راهکار تشخیص حمله‌ی کرم‌چاله، حمله‌ی کرم‌چاله، تونل کرم‌چاله.