The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 93)
http://www.isecure-journal.org

Persian Abstract

یک شمای امضارمز فاقد گواهی کارآمد در مدل استاندارد

پروین رستگاری[1] و مهدی برنج‌کوب[1]

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

رمزنگاری کلید عمومی فاقد گواهی راه‌کاری مفید برای حل توأم مشکلات زیرساخت رمزنگاری کلید عمومی معمول (هزینه بالای محاسبه، ذخیره‌سازی و مخابره گواهی‌ها) و مشکلات رمزنگاری کلید عمومی مبتنی بر شناسه (اطلاع مرکز تولید کلید از کلیدهای خصوصی تمامی موجودیت‌ها) به شمار می‌آید. یک شمای امضارمز عنصری مهم در پروتکل‌های امنیتی است که اهداف امضا و رمزنگاری را به‌صورت هم‌زمان برآورده می‌سازد. در سال ۲۰۱۰، Liu و همکاران طرحی را به‌عنوان اولین شمای امضارمز فاقد گواهی در مدل استاندارد پیشنهاد کردند، اما تاکنون حملات زیادی به شمای پیشنهادی آن‌ها ارائه شده است. در این مقاله، با بهبود طرح Liu و همکاران، یک شمای امضارمز فاقد گواهی در مدل استاندارد ارائه می‌شود که نه‌تنها در برابر حملات مذکور مقاوم است، بلکه از سایر شماهای امضارمز فاقد گواهی ارائه شده در مدل استاندارد کارآمدتر نیز می‌باشد.

واژه‌های کلیدی: رمزنگاری کلید عمومی فاقد گواهی، شمای امضارمز، مدل استاندارد، مدل اوراکل تصادفی.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 94)
http://www.isecure-journal.org

Persian Abstract

خصوصیات پارامتری کانال جانبی در حملات تزریق کد

احسان اعرابی[1]، مهدی کیخا[1]، مهدی فاضلی[1]، احمد پاطوقی[1] و احمد اکبری[1]

[1]دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، ایران

گستره کاربرد سامانه‌های تعبیه‌شده به‌صورت روزافزون در صنایع و بخش‌های مختلف در حال توسعه است. محدودیت‌ها و کاربردهای خاص این سامانه‌ها، امکان اعمال روش‌های نظارتی را بر آن‌ها محدود ساخته است، به‌طوری‌که استفاده از مکانیسم‌های امنیتی موجود برای سامانه‌های عام منظوره در این سامانه‌ها ممکن نیست. از سوی دیگر رشد حملات به حوزه‌های صنعتی و بخصوص بخش تولید، ضرورت توجه به امنیت این سامانه‌ها را بیش از پیش روشن می‌نماید. در بسیاری از حوزه‌های کاربردی سامانه‌های تعبیه‌شده، مواجه با انواعی از این سامانه‌ها هستیم که امکان مداخله و تغییر سخت‌افزار و نرم‌افزار برای نظارت بر آن‌ها وجود ندارد، این امر نیاز به ناظرهایی که بتوانند با حداقل ورود به بخش‌های داخلی سامانه، بر رفتار آن نظارت نمایند را مشخص می‌نماید. در این مقاله با نظارت بر پارامترهای خارجی همچون توان/انرژی مصرفی، زمان اجرا و دمای پردازنده، یک ناظر بر رفتار سامانه پیشنهاد شده است که می‌تواند رخداد شرایط حمله را در این پارامترها شناسایی کند. این پارامترها توسط شبیه‌ساز سطح معماری PTscalar و برای حملات اعمال‌شده بر روی چند برنامه از برنامه‌های محک Mibench مورد ارزیابی قرارگرفته است. ناظر ارائه شده با استفاده از روش‌های هوش مصنوعی و یادگیری ماشین، رفتار عادی و غیرعادی سامانه در زمان اجرای برنامه‌ها را یادگرفته و سپس امکان کشف شرایط حمله را فراهم می‌نماید. نتایج شبیه‌سازی نشان داده است که استفاده از روش‌های یادگیری ماشین بر روی داده‌های حاصل از روش نظارتی پیشنهادی، برای تشخیص رفتار حمله از رفتار عادی در حملات شل کد واقعی بر روی برنامه‌های محک، با دقت میانگین بین ٪۹۵ تا ٪۱۰۰، قابل کشف است.

واژه‌های کلیدی: سامانه‌های تعبیه‌شده، امنیت، نظارت، حمله، انرژی مصرفی.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 95)
http://www.isecure-journal.org

Persian Abstract

روش پیش‌توزیع آماری کلید مبتنی بر مکان برای شبکه‌های بی‌سیم حسگر در مقیاس بزرگ با استفاده از رنگ‌آمیزی گراف

علیرضا احدی‌پور[1] و علیرضا کشاورز حداد[1]

[1]دانشکده مهندسی برق و کامپیوتر، دانشگاه شیراز، شیراز، ایران

امنیت ارتباط در شبکه‌های بی‌سیم حسگر با اختصاص کلیدهای رمزنگاری به گره‌ها بدست می‌آید. با توجه به محدودیت‌های منابع در این شبکه‌ها، روش‌های پیش‌توزیع کلید تصادفی بسیار مورد توجه می‌باشند. اگرچه در بسیاری از این روش‌ها هیچ اطلاعاتی از مکان در نظر گرفته نمی‌شود، سناریوهایی نیز وجود دارند که اطلاعات مکانی توسط گره‌ها پس از نصب آن‌ها حاصل می‌گردد. در این مقاله، ما یک روش پیش‌توزیع آماری کلید جدید را برای شبکه‌های بی‌سیم حسگر در مقیاس بزرگ معرفی می‌کنیم که با بهره‌گیری از اطلاعات مکانی موجب بهبود عملکرد پیش‌توزیع تصادفی کلید بصورت قابل ملاحظه‌ای می‌گردد. به منظور اعمال اطلاعات مکانی گره‌ها در فرآیند توزیع کلید، ما شبکه را به بخش‌هایی تقسیم کرده و با استفاده از تکنیک رنگ‌آمیزی گراف، کلیدهای تصادفی را بصورت کارا تخصیص داده‌ایم. روش معرفی شده مقیاس‌پذیری بالاتری با پشتیبانی از تعداد بیشتری گره و همچنین احتمال وجود کلید مشترک بالاتری در بین گره‌های مجاور یا به عبارت دیگر احتمال کمتری برای داشتن گره‌ای مجزا در مقایسه با روش‌های پیش‌توزیع کلید تصادفی موجود را داراست. نتایج شبیه‌سازی‌ها این موارد را تائید می‌کند.

واژه‌های کلیدی: پیش‌توزیع کلید تصادفی، مدیریت کلید متقارن، تسهیم آماری کلید، گراف رندوم، رنگ‌آمیزی گراف، شبکه‌های بی‌سیم حسگر.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 96)
http://www.isecure-journal.org

Persian Abstract

اثبات امنیتی جدید برای طرح کدگذاری چکش‌ناپذیر پیوسته FMNV

سید امیر مرتضوی[۱]، محمود سلماسی‌زاده[۲] و امیر دانشگر[۳]

[۱]دانشکده مهندسی برق، دانشگاه صنعتی شریف، تهران، ایران
[۲]پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران
[۳]دانشکده علوم ریاضی، دانشگاه صنعتی شریف، تهران، ایران

کدهای چکش‌ناپذیر دسته‌ای از سامانه‌های کدگذارها هستند که در برابر دستکاری مهاجم مقاوم هستند. مهم‌ترین ایده در طراحی کدهای چکش‌ناپذیر این است که مهاجم با دستکاری کلمه‌کد نتواند به اطلاعاتی در مورد پیام کد شده دسترسی پیدا کند. کدهای چکش‌ناپذیر در رمزنگاری مقاوم در برابر دستکاری به‌وفور استفاده می‌شوند. در مقالات انواع مختلفی از کدهای چکش‌ناپذیر تعریف‌شده‌اند که در این میان کدهای چکش‌ناپذیر پیوسته دارای اهمیت خاصی هستند. کدهای چکش‌ناپذیر پیوسته کدهایی هستند که در برابر تعداد چندجمله‌ای دستکاری وفقی مقاوم هستند. اولین کد چکش‌ناپذیر پیوسته در سال ۲۰۱۴ توسط فاوست و همکاران پیشنهادشده است. در این مقاله یک اثبات امنیتی جدید برای طرح چکش‌ناپذیر پیوسته مذکور پیشنهاد می‌شود که منجر به یک طرح با کارایی بالاتری خواهد شد. این اثبات نشان می‌دهد که می‌توان با استفاده از یک مخزن مقاوم در برابر نشت (Leakage Resilient Storage) با تعداد بیت نشتی کمتری به امنیت چکش‌ناپذیری پیوسته رسید. اثبات جدید نشان می‌دهد که طرح مذکور کاراتر و عملی‌تر برای استفاده در رمزنگاری مقاوم در برابر دستکاری است.

واژه‌های کلیدی: چکش‌ناپذیری، چکش‌ناپذیری پیوسته، رمزنگاری مقاوم در برابر دستکاری، رمزنگاری مقاوم در برابر نشت.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 97)
http://www.isecure-journal.org

Persian Abstract

فرانکشتاین کوتوله هنوز در حافظه موجود است: حمله بازاستفاده از کد کوچک

علی‌اکبر صادقی[1]، فرزانه امین‌منصور[1] و حمیدرضا شهریاری[1]

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

حملات باز استفاده از کد مانند حمله‌ی برنامه‌نویسی بازگشت‌گرا و حمله‌ی برنامه‌نویسی پرش‌گرا در میان حمله‌کنندگان بسیار محبوب می‌باشند. تعداد بسیار زیادی روش دفاعی عملی و غیرعملی به منظور جلوگیری از این حملات ارائه‌شده‌اند. این سیستم‌های تشخیص در سربار محاسباتی و کارایی، نیازمندی به سورس کد برنامه، نرخ تشخیص و نیازمندی‌های پیاده‌سازی با هم متفاوت می‌باشند. یکی از رفتارهای قابل استفاده در این سیستم‌های تشخیص، استفاده از طول زنجیره گجت‌های اجرا شونده حمله می‌باشد. استفاده از نرخ آستانه تعداد گجت‌های اجرا شونده باعث ایجاد نرخ مثبت کاذب (False Positive) و منفی کاذب (False Negative) در این سیستم‌های تشخیص می‌شود. نوآوری اصلی این مقاله ارائه یک روش هوشمندانه در طراحی حملات باز استفاده از کد می‌باشد که ما این روش را Tiny Code Reuse Attack نام‌گذاری کرده‌ایم. این روش ناکارآمد بودن روش‌های تشخیص مبتنی بر نرخ آستانه بر روی تعداد گجت‌های اجرا شونده را نشان می‌دهد. همچنین با حداقل مفروضات نماش داده‌ایم که Tiny-CRA گجت‌های اجرا شونده حمله را به حداقل می‌رساند. بنابراین سیستم تشخیص توانایی تشخیص تمایز بین اجرای نرمال برنامه و اجرای گجت‌های حمله را ندارد. به منظور انجام این کار ما گجت‌های پایه و گجت‌های مفید موجود در کتابخانه C را استخراج کرده‌ایم. همچنین به منظور نشان داده کارایی این روش ما ۹ کدپوسته متفاوت را طراحی و با استفاده از یک حمله واقعی سر ریز بافر در نرم‌افزار HT Editor 2.0.20 پیاده‌سازی کرده‌ایم.

واژه‌های کلیدی: امنیت نرم‌افزار، حملات باز استفاده از کد، حمله برنامه‌نویسی پرش‌گرا، حمله برنامه‌نویسی پرش‌گرا کوچک، گجت Kernel Trapper.

The ISC Int'l Journal of Information Security
ISeCure

January 2017, Volume 9, Number 1 (p. 98)
http://www.isecure-journal.org

Persian Abstract

مولّد خودکار موارد آزمون برای ارزیابی پیاده‌سازی سیاست‌های کنترل دسترسی

مرضیه صفرزاده[۱]، محبوبه تقی‌زاده[۱]، بهمن زمانی[۲] و بهروز ترک لادانی[۱]

[۱] دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، اصفهان، ایران

[۲] گروه پژوهشی مهندسی نرم‌افزار مدل‌رانده، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، اصفهان، ایران

یکی از مهم‌ترین نیازمندی‌های سیستم‌های نرم‌افزاری امنیت است. از جمله اصلی‌ترین نیازمندی‌های مرتبط با تأمین امنیت، کنترل دسترسی است که گاهی از آن به‌عنوان قلب امنیت یاد می‌شود. هدف اصلی سیاست‌های کنترل دسترسی حفاظت از منابع سیستم در برابر دسترسی‌های غیرمجاز است. با توجه به این‌که وجود خطا در پیاده‌سازی سیاست‌های کنترل دسترسی ممکن است نتایج نامطلوبی دربرداشته باشد، لازم است که با روش‌هایی از درستی پیاده‌سازی این سیاست‌ها اطمینان حاصل نمود و بهتر است که این روش‌ها به‌صورت خودکار باشند. در واقع روش‌های خودکار، قابلیت اطمینان بیشتر و سرعت بالاتری دارند. تاکنون نیز پژوهش‌های متعددی در زمینه‌ی خودکارسازی آزمون توصیف سیاست‌های کنترل دسترسی انجام شده است، اما بیشتر این تحقیقات مربوط به مرحله‌ی طراحی سیاست‌های کنترل دسترسی است و تعداد پژوهش‌های انجام‌شده در زمینه‌ی پیاده‌سازی سیاست‌ها بسیار کم است. به‌علاوه، به‌دلیل آن‌که کنترل دسترسی در دسته‌ی نیازمندی‌های غیرکارکردی سیستم قرار می‌گیرد، نمی‌توان آن را با روش‌های معمول و همراه با نیازمندی‌های کارکردی مورد آزمون قرار داد. برای رفع این مشکل، در این مقاله یک روش خودکار برای آزمون پیاده‌سازی سیاست‌های کنترل دسترسی سیستم‌های نرم‌افزاری ارائه شده است. این روش که مبتنی بر مدل است، قادر به استخراج موارد آزمون برای ارزیابی سیاست‌های کنترل دسترسی سیستم تحت آزمون است. برای تولید خودکار موارد آزمون، ترکیبی از مدل رفتاری سیستم و توصیف سیاست‌های کنترل دسترسی، که با زبان XACML نوشته شده است، استفاده می‌شود. نتایج نشان می‌دهد که روش پیشنهادی، قادر به کشف خطاهای پیاده‌سازی سیاست‌های کنترل دسترسی و پوشش کدهای مربوطه است.

واژه‌های کلیدی: کنترل دسترسی، خودکارسازی آزمون، آزمون مبتنی بر مدل، پیاده‌سازی سیاست‌های کنترل دسترسی، XACML.