The ISC Int'l Journal of Information Security
ISeCure

January 2016, Volume 8, Number 1 (p. 85)
http://www.isecure-journal.org

Persian Abstract

مقدمه‌ای کوتاه بر دو روش صوری‌سازی پروتکل‌های امنیتی: وارسی مدل و اثبات قضیه

محسن پورپونه[1] و رسول رمضانیان[2]

[1]دانشکده علوم ریاضی، دانشگاه صنعتی شریف، تهران، ایران
[2]دانشکده علوم ریاضی، دانشگاه فردوسی مشهد، مشهد، ایران

در این مقاله به مطالعه دو روش عمده درستی‌یابی پروتکل‌های امنیتی خواهیم پرداخت. روش اول، وارسی مدل نام دارد که درستی‌یابی یک پروتکل با ساخت گراف پردازه‌ای آن و بررسی خواص امنیت روی همه مسیرهای ممکن صورت می‌گیرد. به عنوان یکی از ابزارهای نسبتاً جدید از این روش به معرفی ابزار Scyther خواهیم پرداخت. سپس در ادامه به معرفی یک منطق ساده برای معرفی یک روش اثبات قضیه خواهیم پرداخت و با شرح قواعد استنتاجی این روش به چگونگی درستی‌یابی پروتکل‌های امنیتی خواهیم پرداخت. درنهایت تعدادی از پروتکل‌های شناخته شده را با استفاده از این دو روش بررسی خواهیم کرد.

واژه‌های کلیدی: پروتکل‌های امنیتی، روش‌های صوری‌سازی، وارسی مدل، اثبات قضیه.

The ISC Int'l Journal of Information Security
ISeCure

January 2016, Volume 8, Number 1 (p. 86)
http://www.isecure-journal.org

Persian Abstract

یک طرح تسهیم راز آستانه‌ای مشبکه-مبنا و بررسی امنیت آن

حمیدرضا امینی خوراسگانی[۱] ، صبا اسعد[۱] ، حسین پیل‌آرام[۱] ، ترانه اقلیدس[۲] و محمدرضا عارف[۱]

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

امنیت الگوریتم‌های رمزنگاری مبتنی بر مشبکه در برابر حمله‌های کوانتومی و کارایی و سادگی آن‌ها از مهمترین عواملی است که به واسطه‌ی آن‌ها رمزنگاری مبتنی بر مشبکه از توجه ویژه‌ای از سوی پژوهشگران در طی دهه‌ی گذشته برخوردار گشته است. در این مقاله یک طرح تسهیم راز آستانه‌ای مشبکه-مبنا ارائه می‌کنیم، که در آن از شیوه‌ای که اشتینفیلد و همکارانش از مشبکه‌ها صرفا برای افزودن قابلیت افزایش آستانه به طرح تسهیم راز (t, n) آستانه‌ای شامیر استفاده کرده‌اند الهام می‌گیریم. در طرحی که مؤلفان این مقاله پیشنهاد کرده‌اند، سهم هر شرکت‌کننده از افزودن یک نویز تصادفی به حاصلضرب داخلی دو بردار به دست می‌آید؛ یکی از این بردارها مخفی، اما ثابت است، به گونه‌ای که مؤلفه‌ی اول آن را برابر با مقدار راز اختیار می‌کنیم و سایر مؤلفه‌ها به طور تصادفی انتخاب می‌شوند. دیگری برداری است که به هر شرکت‌کننده تخصیص یافته است. برای بازیابی راز از الگوریتم نزدیک‌ترین صفحه بابای استفاده می‌کنیم، به‌طوری‌که بردار هدف به کمک سهم‌های t نفر شرکت‌کننده (مقدار آستانه) تولید می‌شود و پایه مشبکه بکاررفته به کمک بردارهای تخصیص یافته به t نفر شرکت‌کننده متناظر ساخته می‌شود. در نهایت، پس از اثباتِ درستی و امنیتِ مجانبی طرح، تأثیر اندازه‌ی بُعد مشبکه را روی درستی و امنیت طرح پیشنهادی مطالعه می‌کنیم.

واژه‌های کلیدی: طرح تسهیم راز آستانه‌ای، مسأله نزدیک‌ترین بردار، رمزنگاری مشبکه-مبنا.

The ISC Int'l Journal of Information Security
ISeCure

January 2016, Volume 8, Number 1 (p. 87)
http://www.isecure-journal.org

Persian Abstract

افزودن اعضای جانور: حملات باز استفاده از کد گشوده باز در معماری ARM

فرزانه امین‌منصور[1] و حمیدرضا شهریاری[1]

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

آمارها نشان می‌دهد که همه‌ساله تعداد آسیب‌پذیری‌های بیشتری بر روی دستگاه‌های تلفن همراه کشف می‌شود که نتیجه‌ی آن افزایش حملات بر روی این سامانه‌ها است. در این میان حملات سرقت کنترل اجرای برنامه‌ها از زمره‌ی قدرتمندترین و خطرناک‌ترین خانواده‌ی حملات محسوب می‌شوند که ارائه‌ی روش‌های تشخیص کارآمد را با چالش‌های متنوعی روبه‌رو ساخته‌اند. در سال‌های اخیر، اجرای حملات باز استفاده از کد بر روی دستگاه‌های هوشمند تلفن همراه با معماری استاندارد ARM مطرح شده است که تهدیدی جدی برای امنیت کاربران محسوب می‌شود. در این مقاله، ابتدا با در نظر گرفتن برخی ویژگی‌های خاص معماری ARM، مدل جامع حملات باز استفاده از کد، به همراه پنج زیر مدل جدید ارائه شده که آن را حمله‌ی باز استفاده از کد گشوده نام نهادیم. سپس الگوریتم جست‌جوی ابزارک‌های زیرمدل‌های مربوطه، تحت عنوان CaspianTiger معرفی گردیده است. در ادامه به‌منظور اثبات امکان‌پذیری مدل عنوان‌شده، نمونه‌ای عملی از حمله‌ی مذکور بر روی سیستم‌عامل اندروید ۴/۴/۴ پیاده‌سازی و نشان داده شده است.

واژه‌های کلیدی: اندروید، معماری ARM، حمله‌ی باز استفاده از کد گشوده، حمله‌ی بازگشت‌گرا.

The ISC Int'l Journal of Information Security
ISeCure

January 2016, Volume 8, Number 1 (p. 88)
http://www.isecure-journal.org

Persian Abstract

درج خودکار مسیر خود-اعتبار سنجی در طرح‌های سخت‌افزاری مبتنی بر آرایه‌های دروازه‌ای برنامه‌پذیر به منظور مقاوم‌سازی طرح‌ها در مقابل دستکاری خرابکارانه

شراره زمان‌زاده[1] و علی جهانیان[1]

[1]دانشکده مهندسی و علوم‌کامپیوتر، دانشگاه شهید بهشتی، تهران، ایران

تراشه‌های قابل برنامه‌ریزی به دلایل متعدد نظیر هزینه‌های پایین ساخت نمونه اولیه، زمان کوتاه تحویل به بازار و انعطاف پذیری زیاد، امروزه در کاربردهای مدرن طراحی دیجیتال مورد اقبال طراحان قرار دارند. قابلیت برنامه‌ریزی رشته بیت در آرایه‌های دروازه‌ای برنامه‌پذیر این تراشه را به یک بستر سخت افزاری منعطف با استفاده آسان تبدیل کرده است. این درحالیست که دسترسی به رشته بیت موجب افت امنیت مالکیت‌های معنوی در این نوع پیاده‌سازی می‌گردد، زیرا مکانیزم کارآمدی برای برنامه ریز این تراشه‌ها وجود ندارد تا اجازه دهد اصالت رشته بیت را تشخیص دهند. مشکل انتقال و پیکربندی ایمن اطلاعات به آرایه‌های دروازه‌ای برنامه‌پذیر هم برای استفاده کنندگان و هم برای ارائه‌دهندگان مالکیت‌های معنوی از اهمیت ویژه‌ای برخوردار است. در این مقاله یک متدولوژی خود اعتبار سنجی معرفی می‌شود که در آن اصالت زیربخش‌های مدار در رشته بیت موازی با عملکرد مدار بررسی می‌شود. در صورت کشف تهاجم، جریان حرکت طبیعی داده در مدار مخدوش و مدار قفل می‌شود. نتایج تحقیقات نشان می‌دهد که این متدولوژی امنیت مالکیت‌های معنوی را در مقابل بروز رسانی‌های خرابکارانه با سربار اندک، به‌طور قابل توجهی ارتقا می‌دهد.

واژه‌های کلیدی: آرایه‌های دروازه‌ای برنامه‌پذیر، امنیت سخت‌افزار، محافظت از مالکیت معنوی، مسیر امنیتی.

The ISC Int'l Journal of Information Security
ISeCure

January 2016, Volume 8, Number 1 (p. 89)
http://www.isecure-journal.org

Persian Abstract

کشف رویدادهای احراز هویت نشده در شبکه‌های حسگر بی‌سیم با استفاده از ویژگی چند پوششی گره‌های حسگر

میثم کمره‌ئی[1]، احمد پاطوقی[2] و مهدی فاضلی[2]

[1]دانشگاه جامع علمی و کاربردی، تهران، ایران
[2]دانشگاه علم و صنعت ایران، تهران، ایران

افزونگی در شبکه‌های حسگر بی‌سیم مساله‌ای بدیهی است به شکلی که هر نقطه درون محدوده شبکه توسط چند گره پوشش داده می‌شود. در این مقاله از این پدیده که به صورت چند پوششی گره‌های حسگر شناخته می‌شود جهت شناسایی رویدادهای احراز هویت نشده استفاده می‌شود. انتشار رویدادهای احراز هویت نشده در یک شبکه حسگر بی‌سیم باعث ازدحام شبکه، افزایش احتمال از بین رفتن بسته‌ها و افزایش مصرف انرژی شبکه می‌گردد. در روش پیشنهادی که مبتنی بر رویکرد هر چه بیشتر امن‌تر و هر چه کمتر نا امن‌تر است، هر رویداد امن باید توسط چند گره مختلف تایید گردد؛ در غیر اینصورت رویداد از شبکه حذف می‌گردد. در واقع روش پیشنهادی تمایل به ارسال رویدادهایی دارد که توسط چندین گره حسگر کشف شده اند. روش پیشنهادی به وسیله شبیه‌سازی و مدل‌سازی تحلیلی مورد ارزیابی واقع شده است. نتایج شبیه‌سازی‌ها که وسیله شبیه‌ساز ns-2 پیاده‌سازی شده‌اند نشان می‌دهد که روش پیشنهادی بیش از ۸۵ درصد رویدادهای جعلی را کشف می‌کند. همچنین به دلیل عدم تحمیل تأخیر به بسته‌های ورودی، روش پیشنهادی ۲۰ در صد تأخیر انتها به انتهای شبکه را نیز کاهش می‌دهد. همچنین روش پیشنهادی توسط یک مدل تحلیلی مبتنی بر شبکه‌های صف مورد ارزیابی قرار گرفته است. مدل پیشنهادی با دقت بالایی کارایی روش پیشنهادی را جهت کشف رویدادهای جعلی تخمین می‌زند.

واژه‌های کلیدی: حمله، شبکه‌های حسگر بی‌سیم، مکانیزم هر چه بیشتر امن‌تر هر چه کمتر نا امن‌تر، رویدادهای احراز هویت نشده.

The ISC Int'l Journal of Information Security
ISeCure

January 2016, Volume 8, Number 1 (p. 90)
http://www.isecure-journal.org

Persian Abstract

یک روش جدید برای تسریع حمله تفاضل ناممکن و کاربرد آن روی LBlock

اکرم خالصی[۱]، حسین بهرام‌گیری[۱،۲] و داود منصوری[۱،۲]

[۱]مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران، ایران
[۲]پژوهشکده امنیت اطلاعات و ارتباطات، دانشگاه صنعتی مالک اشتر، تهران، ایران

حمله تفاضل ناممکن، توسیعی از حمله تفاضلی و یکی از موثرترین روش‌های تحلیل رمزهای قالبی است. این روش حمله روی بیشتر رمزهای قالبی به‌کار برده شده و نتایج قابل توجهی داشته است. استفاده از ساختار، در نظر گرفتن طرح کلید، حذف زود هنگام و پیش‌محاسبات، تکنیک‌هایی متداول برای کاهش پیچیدگی‌های این روش حمله هستند. در این مقاله، روش جدیدی برای کاهش پیچیدگی زمانی این روش حمله ارائه می‌کنیم. این روش مبتنی بر تفکیک فضای جستجوی کلید به یک سری زیرفضا، بررسی هر یک از زیرفضاها به‌صورت مستقل و تعمیم نتایج حاصل از بررسی زیرفضاها به فضای کلید مورد جستجو است. برتری اصلی این روش جلوگیری از بررسی تأثیر تغییرات بیت‌های مستقل از زیرکلیدها روی یکدیگر است. با استفاده از مشخصه تفاضل ناممکن ۱۴-دوری معرفی شده روی LBlock، توسط بورآ و همکارانش در ASIACRYPT 2014، روش پیشنهادی را روی الگوریتم LBlock ۲۳-دوری به‌کار برده و نشان می‌دهیم این روش پیچیدگی زمانی را به $2^{71.8}$ با استفاده از 2^{59} متن اصلی انتخابی و 2^{73} بلوک حافظه کاهش می‌دهد.

واژه‌های کلیدی: رمز قالبی، حمله تفاضلی، حمله تفاضل ناممکن، LBlock.