The ISC Int'l Journal of Information Security
ISeCure

July 2016, Volume 8, Number 2 (p. 161)
http://www.isecure-journal.org

Persian Abstract

مقاوم‌سازی مدارات مجتمع خاص منظوره در مقابل مهندسی معکوس در حین فرآیند ساخت با استفاده از مبهم‌سازی خودکار لیست گره مدار در فرآیند طراحی

شراره زمان‌زاده[1] و علی جهانیان[1]

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

در مدل تجاری بدون فرآیند ساخت در صنعت نیمه هادی، در خصوص امنیت سخت‌افزار نگرانی‌های جدی وجود دارد. در این مدل تجاری کمپانی‌های ساخت و شرکت‌های واسط غیرقابل اطمینان هستند و این احتمال وجود دارد که به‌منظور سرقت اطلاعات طراحی یا درج تروجان خرابکارانه، نقشه مدار ارائه شده برای ساخت را مورد آنالیز و مهندسی معکوس قرار دهند. هدف غایی مهندسی معکوس همان استخراج و درک همبندی لیست گره مدار می‌باشد. در این مقاله، یک مکانیزم رمزنگاری لیست گره مدار معرفی شده است که همبندی اتصالات داخلی تراشه را مخفی می‌نماید. به علاوه یک سلول استاندارد جدیدی (سلول‌های درهم‌ساز همبندی) طراحی شده است تا نقش رمزنگاری لیست گره مدار را ایفا نمایند. همچنین جریان طراحی جدیدی معرفی شده است که در آن سلول‌های درهم‌ساز به نحوی در لیست گره مدار درج شوند که بیشترین ابهام را در همبندی به وجود آورند و در عین حال کمترین سربار را موجب شوند. لازم به ذکر است که این مکانیزم بدون نیاز به اطلاعات جزئی از عملکرد و ساختار طراحی، قابل خودکارسازی است. مکانیزم پیشنهادی ما در یک چارچوب طراحی خودکار آکادمیک با نام EduCAD پیاده‌سازی شده است. نتایج آزمایش‌ها نشان می‌دهد که مهندسی معکوس با سربار قابل اغماض به طور قابل توجهی دشوار شده است. سربار مساحت حدود ۲۳٪، تأخیر ۳٫۲۵٪ و طول مجموع سیم ۱۴٫۵٪ می‌باشد. میزان دشوار شدن مهندسی معکوس در این مقاله با استفاده از حمله جستجوی فراگیر ارزیابی شده است و نشان داده شده است که با استفاده از این حمله میزان یادگیری از سیستم ۰٪ و فاصله همینگ خروجی نزدیک به ۵۰٪ است.

واژه‌های کلیدی: امنیت سخت‌افزار، رمزنگاری لیست گره مدار، ابهام‌سازی، مهندسی معکوس و دزدی مالکیت معنوی.

The ISC Int'l Journal of Information Security
ISeCure

July 2016, Volume 8, Number 2 (p. 162)
http://www.isecure-journal.org

Persian Abstract

بهبود عملکرد پروتکل احراز اصالت مبتنی بر استاندارد EPC C1 G2 ارائه‌شده در سال‌های اخیر در مقابله با حملات ردیابی

سید سلمان سجادی قائم‌مقامی[1]، افروز حق‌بین[1] و مهتاب میرمحسنی[2]

[1]دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، گروه مهندسی برق ، تهران، ایران
[2]دانشگاه صنعتی شریف، گروه مهندسی برق، تهران، ایران

با توجه به گسترش روزافزون کاربردهای فناوری شناسایی با استفاده از امواج رادیویی (RFID) در سراسر دنیا، پروتکل‌های متعددی توسط محققین جهت تأمین امنیت و حفظ حریم خصوصي کاربران ارائه‌شده است. در این مقاله به تحلیل پروتکل ارائه‌شده توسط آقایان ین و ژن در سال ۲۰۱۵ از نقطه نظر میزان حفظ حریم خصوصی می‌پردازیم و اثبات می‌کنیم که این پروتکل نمی‌تواند امنیت و محرمانگی کاربر را تضمین نماید. برای این منظور از مدل اویف-فان استفاده نموده‌ایم و نشان می‌دهیم که پروتکل در برابر حملات نشت مقدار مخفی، ردیابی و ردیابی پیشرو دارای ضعف امنیتی می‌باشد. در همین راستا و به منظور رفع ایرادات پروتکل مورد بحث، پروتکل بهبود یافته‌ای پیشنهاد شده است. در انتها پروتکل بهبود یافته را با برخی از پروتکل‌های ارائه شده در سال‌های اخیر مورد مقایسه قرار می‌دهیم که بهبود عملکرد در ایجاد امنیت و حفظ محرمانگی را نتیجه داده است.

واژه‌های کلیدی: پروتکل‌های احراز اصالت RFID، حریم خصوصی، حمله ردیابی، حمله ردیابی پیشرو، حمله نشت مقدار مخفی.

The ISC Int'l Journal of Information Security
ISeCure

July 2016, Volume 8, Number 2 (p. 163)
http://www.isecure-journal.org

Persian Abstract

یک طرح مدیریت کلید نوین برای شبکه‌های حسگر بی‌سیم ناهمگن بر اساس موقعیت گره‌ها

طاها یاسین رضاپور[۱،۲]، رضا ابراهیمی آتانی[۱] و میرسهیل ابوالقاسمی[۱]

[۱] دانشکده مهندسی کامپیوتر، دانشگاه گیلان، رشت، ایران

[۲] دانشکده فناوری اطلاعات، سازمان بنادر و دریانوردی، تهران، ایران

شبکه‌های حسگر بی‌سیم دارای کاربردهای متنوعی در حوزه‌های تجاری، نظامی، پزشکی و محیط‌زیست می‌باشند. با توجه به استقرار گره‌های حسگر کم‌هزینه با منابع انرژی محدود، این شبکه‌ها با چالش‌های امنیتی فراوانی روبرو هستند. یک رویکرد اساسی برای آماده‌سازی ارتباطات بی‌سیم امن در WSNها به‌کارگیری یک پروتکل مدیریت کلید رمزنگاری کارآمد برای حصول بالاترین امنیت با کمترین هزینه می‌باشد. انگیزش اصلی این مقاله به‌کارگیری موقعیت گره‌های حسگر به‌عنوان جزئی از هویت به‌منظور مدیریت کلید در شبکه‌های حسگر ناهمگن می‌باشد. در طرح ارائه‌شده موقعیت گره‌های حسگر به‌عنوان جزئی از هویت برای احراز اصالت و تخصیص کلید برای تمامی ارتباطات شبکه بکار گرفته‌شده است. در مقایسه با سایر طرح‌های ارائه‌شده تکنیک پیشنهادی سطح بالاتری را از نظر مقیاس‌پذیری، امنیت، انعطاف‌پذیری و پیچیدگی حافظه کمتر ارائه داده است.

واژه‌های کلیدی: رمزنگاری مبتنی بر موقعیت مکانی، رمزنگاری، مدیریت کلید، شبکه‌های حسگر ناهمگن.

The ISC Int'l Journal of Information Security
ISeCure

July 2016, Volume 8, Number 2 (p. 164)
http://www.isecure-journal.org

Persian Abstract

کدگشای بهینه برای نشانه‌گذاری تصویر به روش طیف گسترده ضربی به کمک مدل لاپلاس

نعمت اله زرمهی[1] و محمدرضا عارف[1]

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

این مقاله به بررسی نشانه‌گذاری تصویر به روش طیف گسترده ضربی می‌پردازد. بیت اطلاعات به کمک یک دنباله تصادفی، در ضرایب مرکزی تبدیل کسینوسی هر بلوک از تصویر گسترده می‌شود. برخلاف روش‌های مرسوم مدلینگ سیگنال، ما فرض می‌کنیم که هم سیگنال و هم نویز توزیع لاپلاسی دارند زیرا مدل کردن از دست رفتن نمونه‌ها به کمک توزیع لاپلاس بهتر از توزیع گوسی انجام می‌شود. ما کدگشای بهینه برای روش درج ذکر شده را به کمک روش برآورد درست‌نمایی بیشینه به دست می‌آوریم. همچنین عملکرد روش درج را در حضور نویز آنالیز کرده و محاسبات تحلیلی و شبیه‌سازی نیز ارائه می‌گردد. نتایج شبیه‌سازی نشان می‌دهند که این روش عملکرد مناسب و شفافیت کافی برای کاربردهای نشانه‌گذاری دارد.

واژه‌های کلیدی: توزیع لاپلاس، کدگشایی برآورد درست‌نمایی بیشینه، روش طیف گسترده، نشانه‌گذاری.

The ISC Int'l Journal of Information Security
ISeCure

July 2016, Volume 8, Number 2 (p. 165)
http://www.isecure-journal.org

Persian Abstract

ارزیابی کمی امنیت نرم‌افزار: روشی مبتنی بر UML/SecAM و نظریه شواهد

علی صداقت‌باف[1] و محمد عبداللهی ازگمی[2]

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

ارزیابی کمّی و مدل-مبنای امنیت نرم‌افزار در مرحله طراحی معماری امکان تشخیص زودهنگام خطاهای طراحی و در نتیجه کاهش هزینه‌های تغییر در مراحل بعدی چرخه حیات نرم‌افزار را فراهم می‌کند. در عین حال، دقت پارامترهای ورودی مدل‌ها در مراحل اولیه توسعه چالش‌برانگیز است. در حقیقت، به دلیل عدم وجود دانش کافی، تخمین دقیق پارامترهای امنیتی به ندرت امکان‌پذیر است. این موضوع در اغلب روش‌های ارزیابی موجود نادیده گرفته شده است. هدف از این مقاله توجه صریح به عدم قطعیت پارامترهای ورودی در فرایند ارزیابی امنیت است. به عبارت دقیق‌تر، ما از نظریه شواهد به منظور توصیف عدم قطعیت در پارامترهای ورودی و سنجش اثر آن بر معیارهای امنیتی استفاده می‌کنیم. در روش پیشنهادی از نمودارهای UML به منظور توصیف حملات امنیتی و از نمایه SecAM به منظور توصیف پارامترهای امنیتی استفاد می‌شود. همچنین، به منظور ارزیابی احتمال رخنه امنیتی، مدل‌های UML/SecAM به درخت‌های حمله تبدیل می‌شوند. در ضمن، به منظور بررسی کاربردپذیری روش پیشنهادی یک مطالعه موردی برروی یک سامانه خرید و فروش اینترنتی انجام گرفته و نتایج آن گزارش شده است.

واژه‌های کلیدی: معماری نرم‌افزار، ارزیابی امنیت، کمّی‌سازی عدم قطعیت، نظریه شواهد.

The ISC Int'l Journal of Information Security
ISeCure

July 2016, Volume 8, Number 2 (p. 166)
http://www.isecure-journal.org

Persian Abstract

نوشته‌ای بر امنیت دو پروتکل RFID

معصومه صفخانی[۱] و نصور باقری[۲]

[۱]دانشکده مهندسی کامپیوتر، دانشگاه شهید رجائی، تهران، ایران
[۲]دانشکده مهندسی برق، دانشگاه شهید رجائی، تهران، ایران

اخیراً، باقری و همکاران چندین حمله به دو پروتکل RFID، یعنی پروتکل Yoon و پروتکل Jung و همکاران، اعمال کرده و نسخه بهبود یافته آن‌ها را نیز ارائه کرده‌اند. اما، در این یادداشت، ما نشان می‌دهیم که نسخه بهبود یافته پروتکل Jung وهمکاران در مقابل حمله غیرهمزمان سازی آسیب‌پذیر است و نسخه بهبودیافته پروتکل Yoon در مقابل حمله بازیابی مقادیر مخفی آسیب‌پذیر است. شانس موفقیت حمله غیرهمزمان سازی ارائه‌شده برای حمله به نسخه بهبود یافته پروتکل Jung و همکاران [۲] $(۱ - ۲^{-۲n})$ است، در حالی‌که پیچیدگی حمله تنها سه بار اجرای پروتکل است، در این‌جا n طول متغیرهای مورد استفاده در پروتکل است. شانس موفقیت حمله بازیابی مقادیر مخفی ارائه‌شده برای نسخه بهبودیافته پروتکل Yoon تقریباً ۱ است درحالی‌که پیچیدگی حمله تنها دو بار اجرای پروتکل و بار ارزیابی تابع PRNG در حالت برون‌خط است.

واژه‌های کلیدی: احراز اصالت، RFID.