The ISC Int'l Journal of Information Security
ISeCure

July 2019, Volume 11, Number 2 (p. 185)
http://www.isecure-journal.org

Persian Abstract

طراحی بازی امنیت وابسته بر روی شبکه‌های با تاثیرات خطی مقیّد

سیدعلیرضا هاشمی نسب[1]، بهروز ترک لادانی[1]، تنسو آلپکان[2]

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

[2] دانشکده مهندسی برق و الکترونیک، دانشگاه ملبورن، ملبورن، استرالیا

در دنیای به شدت مرتبط شده امروزی، امنیت موجودیت‌ها اغلب به هم وابسته است. این بدین معنی است که تصمیمات امنیتی موجودیت‌ها در شبکه نه‌تنها متأثر از سرمایه‌گذاری امنیتی، هزینه‌ها و قیود خود آن‌ها است، بلکه تحت تأثیر تصمیمات امنیتی، هزینه‌ها و قیود همسایگان آن‌ها نیز هست. نظریه بازی مجموعه‌ای غنی از ابزارها را برای تحلیل چنین شبکه‌های مقیّد تاثیرگذاری فراهم می‌کند. در یک مدل بازی، بازیکنان سعی می‌کنند بهره‌ی خود را از طریق سرمایه‌گذاری‌های امنیتی با توجه به ساختار شبکه، هزینه‌ها و محدودیت‌ها، که توسط صاحب شبکه تعیین شده‌اند، به حداکثر برسانند. با این حال، تصمیمات موجودیت‌های خودخواه برای به حداکثر رساندن بهره خود همیشه منجر به یک راه‌حل بهینه اجتماعی برای کل سیستم نمی‌شوند. بنابراین انگیزه دادن به بازیکنان برای رسیدن به بهینه اجتماعی از نقطه نظر متصدی شبکه ارزش بالایی دارد. در واقع متصدی شبکه قصد دارد از طریق طراحی پارامترهای بازی، امنیت کلی شبکه را بیشینه نماید. مطالعات انجام شده در این پژوهش نشان می‌دهد که کار موفق قابل توجهی در زمینه طراحی مناسب بازی در شبکه‌های وابسته وجود ندارد. در این مقاله، یک مدل دقیق سرمایه‌گذاری امنیتی ارائه می‌شود که در آن تصمیمات بازیکنان به دقت مورد تحلیل قرار گرفته و در نهایت، در شرایطی که این تصمیمات منجر به شرایط نامطلوب از دیدگاه سراسری شوند، سازوکارهای تنظیم منافع محلی بر مبنای اهداف سراسری ارائه شده‌است. بر این اساس چند روش طراحی با استفاده از تغییر هزینه‌ها، وابستگی‌های متقابل و قیود سرمایه‌گذاری بازیکنان برای همسو کردن انگیزه‌های آنان با یک هدف سراسری ارائه شده است. همچنین یک بررسی جامع از وجود و شرایط یکتایی تعادل نش در چنین محیط‌هایی ارائه شده و نتایج عددی اعمال سازوکارهای پیشنهادی در یک نمونه کاربردی واقعی نشان داده شده‌است.

واژه‌های کلیدی: طراحی بازی، امنیت وابسته، نقطه تعادل نش، بهینه اجتماعی.

The ISC Int'l Journal of Information Security
ISeCure

July 2019, Volume 11, Number 2 (p. 186)
http://www.isecure-journal.org

Persian Abstract

یک طرح تبادل کلید سبک وزن حافظ حریم خصوصی برای شبکه هوشمند انرژی

مجید بیات[۱]، زهرا زارع جوشقانی[۲]، آشوک کومار داس[۳]، پیتام سینگ[۴]، سارو کوماری[۵]، محمدرضا عارف[۲]

[۱]دانشکده کامپیوتر، دانشگاه شاهد، تهران، ایران
[۲]دانشکده برق، دانشگاه صنعتی شریف، تهران، ایران
[۳]مرکز امنیت موسسه فناوری اطلاعات، حیدرآباد، هند
[۴]دانشکده ریاضی، موسسه ملی فناوری موتیلال نهرو، الله آباد، هند
[۵]دانشکده ریاضی، دانشگاه چ چاران سینگ، میروت، اوتار پرادش، هند

مفهوم شبکه هوشمند برای اصلاح شبکه برق با استفاده از فن‌آوری جدید اطلاعات و ارتباطات معرفی شده است . شبکه هوشمند به اطلاعات برخط مصرف برق برای نظارت بر مصرف و ارائه خدمات مورد نیاز، نیاز دارد و برای این مسئله ، ارتباطات دو جهته اطلاعات ضروری است. امنیت و حریم خصوصی الزامات مهمی است که باید در ارتباطات برقرار شود. به دلیل طراحی پیچیده سیستم‌های شبکه هوشمند و استفاده متفاوت از فن‌آوری‌های جدید، فرصتهای بسیاری برای مهاجمان برای حمله ایجاد کرده است که می‌تواند مشکلات مهمی برای مشتریان به وجود آورد. طرح‌های احراز هویت حافظ حریم خصوصی یک عنصر مهم برای توسعه امن شبکه هوشمند انرژی است. اخیراً، محمود و همکاران [۱] یک طرح احراز هویت سبک وزن برای ارتباطات شبکه هوشمند ارایه داده‌اند و ادعا می‌کند که آن طرح الزامات امنیتی شبکه‌های هوشمند انرژی را برآورده می‌کند. متأسفانه متوجه شدیم که طرح آن‌ها دارای برخی از آسیب‌های امنیتی است و ویژگی‌های امنیتی لازم برای استفاده در شبکه هوشمند انرژی را ندارد. برای برطرف کردن این اشکالات، ما یک طرح احراز هویت حافظ حریم خصوصی سبک وزن، کارآمد و ایمن برای شبکه هوشمند انرژی ارایه می‌کنیم. امنیت طرح پیشنهادی را بطور فرمال با BAN و AVISPA بررسی خواهیم کرد. بررسی‌های امنیتی و کارایی طرح پیشنهادی و مقایسه با طرح‌های مرتبط کارایی و امنیت طرح ما را مورد تاکید قرار می‌دهد.

واژه‌های کلیدی: شبکه هوشمند انرژی، احراز اصالت، حریم خصوصی، BAN، AVISPA.

The ISC Int'l Journal of Information Security
ISeCure

July 2019, Volume 11, Number 2 (p. 187)
http://www.isecure-journal.org

Persian Abstract

تحلیل خطای تفاضلی تسهیل شده به SHA-3

سید احسان حسینی‌نژاد[1]، معصومه صفخانی[2]، نصور باقری[3,1]

[1]دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
[2]دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
[3]پژوهشکده علوم کامپیوتر، مرکز تحقیقات فیز نظری، تهران ،ایران

در این مقاله، یک شیوه جدید برای تحلیل تفاضلی خطای تابع چکیده‌ساز SHA-3 ارائه می‌کنیم، که مبتنی بر معادلات تفاضلی الگوریتم است. به‌کارگیری این روابط تفاضلی در تحلیل خطای تفاضلی SHA-3 قابلیت‌های جدیدی به حمله می‌دهد. به عنوان مثال، احتمال بالای تشخیص خطای القا شده، امکان بررسی مجدد خطای القا شده و بازیابی حالت میانی الگوریتم با استفاده از ۲۲ تا ۵۳ خطا از جمله این قابلیت‌ها هستند. ما همچنین دو بهبود دیگر نیز برای این حمله ارائه می‌کنیم، که عبارتند از استفاده از روابط تفاضلی در جهت معکوس، برای بهبود نتایج، و بهره‌گیری از روابط جبری حاکم بر الگوریتم، به عنوان راه‌کار دوم برای بازیابی حالت میانی الگوریتم SHA-3. در نتیجه این بهبودها، نشان می‌دهیم که به طور متوسط می‌توان با ۵ تا ۸ خطا کل حالت میانی الگوریتم SHA-3 را بازیابی کرد.

واژه‌های کلیدی: تابع چکیده‌ساز، SHA-3، تحلیل خطای تفاضلی، بازیابی حالت میانی، معادلات تفاضلی، روابط جبری، خطای چند بایتی.

The ISC Int'l Journal of Information Security
ISeCure

July 2019, Volume 11, Number 2 (p. 188)
http://www.isecure-journal.org

Persian Abstract

حملات نقطه ثابت جدید به رمز قالبی GOST2 با بهبودهایی در پیچیدگی حافظه

سیاوش احمدی[1]، محمدرضا عارف[1]

[1]دانشگاه صنعتی شریف، تهران، ایران

رمز قالبی GOST در دهه ۱۹۷۰ طراحی و در سال ۱۹۸۹ به عنوان استاندارد GOST 28147-89 در اتحادیه جماهیر شوروی منتشر شد. به منظور بهبود امنیت رمز قالبی GOST پس از پیشنهاد حملات مختلف روی آن، طراحان نسخه اصلاح‌شده‌ای از GOST، با نام GOST2، را در سال ۲۰۱۵ منتشر کردند که دارای یک فرانمای کلید جدید و همچنین انتخاب صریح برای S-Boxهای آن بود. در این مقاله، با استفاده از سه بخش دقیقا یکسان از GOST2 و ایده نقطه ثابت، حملات نقطه ثابت بهبودیافته‌تری برای حذف کلیدهای اشتباه ارائه شده‌است. به عبارت دیگر، تمرکز حملات جدید روی کاهش پیچیدگی حافظه و در عین حال عدم تغییر پیچیدگی‌های دیگر است. نتایج کسب‌شده، کاهش قابل توجهی در پیچیدگی حافظه حملات را نشان می‌دهد، حال آن که پیچیدگی زمانی به میزان کمی در مقایسه با حملات نقطه ثابت قبلی افزایش پیدا کرده است. بر اساس دانش فعلی ما، کمترین پیچیدگی حافظه برای یک حمله روی نسخه دور-کامل رمز قالبی GOST2 در این‌جا ارائه شده است.

واژه‌های کلیدی: تحلیل رمز، حمله نقطه ثابت، رمز قالبی GOST2، ملاقات در میانه.

The ISC Int'l Journal of Information Security
ISeCure

July 2019, Volume 11, Number 2 (p. 189)
http://www.isecure-journal.org

Persian Abstract

تشخیص ناهنجاری با استفاده از SVM به عنوان طبقه‌بندی و درخت تصمیم برای بهینه‌سازی بردارهای ویژگی

الهام سرکانی[1]،حسین قرایی[2]، ناصر محمدزاده[1]

[1]دانشکده فنی و مهندسی، دانشگاه شاهد، تهران، ایران

[2]مرکز تحقیقات مخابرات ایران

با پیشرفت و فراگیرشدن فناوری‌های مبتنی بر شبکه‌های کامپیوتری، راه برای نفوذگران هموارترشده است؛ لذا به منظور تشخیص تهدیدات و حملات، روز به روز بر اهمیت سامانه‌های تشخیص نفوذ به عنوان یکی از اصلی‌ترین عناصر امنیتی، افزوده می‌شود. یکی از چالش‌های سامانه‌های تشخیص نفوذ، ابعاد زیاد ویژگی‌های ترافیک شبکه است. کاهش ویژگی‌های غیر ضروری پیش از آموزش سامانه‌ی تشخیص نفوذ، از جمله راه حل‌های مقابله با این مشکل است. روش‌های یادگیری ماشین جزء بهترین راه‌های آموزش سامانه‌های تشخیص نفوذند. در روش ارائه شده از ترکیب دو روش یادگیری ماشین برای طراحی سامانه تشخیص نفوذ استفاده شده‌است. به طوری که ابتدا انتخاب ویژگی توسط هرس درخت تصمیم C5.0 صورت می گیرد، سپس ویژگی‌هایی با کمترین اهمیت پیش‌بینی کنندگی حذف و پس از حذف هر ویژگی، LSSVM آموزش داده می‌شود. مجموعه ویژگی‌هایی که بالاترین مقدار سطح زیر نمودار ROC را برای LSSVM ایجاد کرده‌اند به عنوان ویژگی‌های نهایی در نظر گرفته می‌شوند. نتایج روی دو مجموعه داده‌ی KDD Cup 99 و UNSW-NB15 نشان دهنده بهبود معیارهای TP و FP و دقت نسبت به سایر کارهای مشابه می‌باشد.

واژه‌های کلیدی: تشخیص نفوذ، انتخاب ویژگی، ماشین‌های بردار پشتیبان، درخت تصمیم.

The ISC Int'l Journal of Information Security
ISeCure

July 2019, Volume 11, Number 2 (p. 190)
http://www.isecure-journal.org

Persian Abstract

تشخیص حساب‌های کاربری جعلی در شبکه‌های اجتماعی مبتنی بر دسته‌بندی تک کلاسه

محمدابراهیم شیری[۱]، محمدرضا محمدرضایی[۲]، امیرمسعود رحمانی[۳]

[۱]دانشکده ریاضی و علوم کامپیوتر، دانشگاه صنعتی امیرکبیر، تهران، ایران
[۲]دانشکده کامپیوتر، دانشگاه آزاد اسلامی، واحد بروجرد، بروجرد، ایران
[۳]دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد علوم تحقیقات، تهران، ایران

تشخیص حساب‌های کاربری جعلی در شبکه‌های اجتماعی امری چالش برانگیز است. روش‌های پیشین برای کشف حساب‌های کاربری جعلی قدرت ارتباطات میان کاربران را در نظر نگرفته و این باعث کاهش کارایی روش‌های پیشین است. در این تحقیق، ما یک روش تشخیص مبتنی بر شباهت کاربران که ارتباطات شبکه‌ای کاربران را نیز پوشش می‌دهد، ارایه می‌کنیم. در گام اول معیارهای شباهت از قبیل دوستان مشترک، تعداد یال‌های گراف همسایگی، معیار شباهت کسینوس و معیار شباهت جاکارد را از روی ماتریس مجاورت گراف محاسبه می‌شوند. در ادامه به منظور کاهش پیچیدگی‌های محاسباتی و بدست آوردن ویژگی‌های جدید، روش آنالیز مولفه‌های اصلی را روی هر یک از ماتریس‌های شباهت اعمال می‌کنیم. سپس با استفاده از روش البو مجموعه‌ای از مقادیر بردار ویژه که دارای بیشترین بار اطلاعاتی هستند را انتخاب و ماتریس نهایی را تشکیل می‌دهیم. ویژگی‌های استخراج شده برای آموزش الگوریتم دسته‌بند تک کلاسه استفاده می‌شوند. درنهایت این مدل آموزش داده شده برای تشخیص حساب‌های کاربری جعلی استفاده می‌شود. نتایج بدست آمده از آزمایش روش پیشنهادی نشان می‌دهد که دقت تشخیص و نرخ تشخص نادرست به ترتیب ۶.۹۹ % و ۰ % می‌باشند. ما نشان دادیم که تعریف شباهت‌های میان کاربران و همچنین استفاده از الگوریتم‌های تک کلاسه نسبت به چند کلاسه برای آموزش مدل بهتر عمل می‌کنند.

واژه‌های کلیدی: شبکه‌های اجتماعی، حریم خصوصی، حساب‌های کاربری جعلی، دسته‌بندی تک کلاسه.