The ISC Int'l Journal of Information Security
ISeCure

July 2018, Volume 10, Number 2 (p. 163)
http://www.isecure-journal.org

Persian Abstract

مروری بر راهکارهای تشخیص ناهنجاری در اینترنت اشیا

مرتضی بهنیافر[۱]، علیرضا نوروزی[۲] و حمیدرضا شهریاری[۳]

[۱]دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر، تهران، ایران
[۲]دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران
[۳]دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران

اینترنت اشیا شبکه‌ای رو به رشد از گره‌ها و اشیای محدود و ناهمگون است که علیرغم اتصال محلی به شبکه جهانی اینترنت نیز متصل می‌باشد. در همین راستا امنیت در این‌گونه شبکه‌ها نقش بسزایی پیدا می‌کند. تجربیات ثابت کرده است که رمزنگاری و احراز هویت برای امنیت شبکه‌ها کافی نبوده است و احتیاج به سیستم تشخیص نفوذ برای تشخیص و جلوگیری از حملات و نفوذ گره‌های مخرب است. در همین راستا سیستم‌های تشخیص نفوذ مبتنی بر تشخیص ناهنجاری به شناسایی رفتار ناهنجار شبکه و به تبع آن به تشخیص نفوذ احتمالی و حملات ناشناخته و نهان می‌پردازند. در این زمینه این مقاله به شناخت، تحلیل، ارزیابی و دسته‌بندی راهکارهای تشخیص ناهنجاری و سیستم‌های ارائه شده به‌منظور تشخیص ناهنجاری اختصاصی برای اینترنت اشیا پرداخته است. برای این هدف، راهکارها و سیستم‌های تشخیص ناهنجاری از سه دیدگاه مختلف معماری ، جایگاه کارکردی و در نهایت از دیدگاه روش تشخیص مورد بررسی و تحلیل و ارزیابی قرارگرفته‌اند و دسته‌بندی شده‌اند تا خواننده بتواند دید خوبی در رابطه با کارهای انجام‌شده و ابعاد آن‌ها و نقاط قوت و ضعف کارهای مختلف به دست آورد.

واژه‌های کلیدی: تشخیص ناهنجاری، سیستم تشخیص نفوذ، اینترنت اشیا، امنیت اطلاعات.

The ISC Int'l Journal of Information Security
ISeCure

July 2018, Volume 10, Number 2 (p. 164)
http://www.isecure-journal.org

Persian Abstract

تحلیل تفاضل ناممکن Deoxys-BC-256

علیرضا مهرداد[1]، فرخ‌لقا معظمی[1] و هادی سلیمانی[1]

[1]پژوهشکده فضای مجازی دانشگاه شهید بهشتی، تهران، ایران

مسابقه بین‌المللی چندمرحله‌ای CAESAR به منظور انتخاب یک (یا چند) طرح رمزگذاری توأم با احراز اصالت، با قابلیت و کارآیی بالا در حال برگزاری است. در هر مرحله‌ی این مسابقه، تعدادی از الگوریتم‌های پذیرفته شده به دلیل نقص امنیتی یا ضعف در کارآمدی کنار گذاشته شده‌اند و اکنون این مسابقه به مرحله نهایی رسیده است. الگوریتم Deoxys یکی از الگوریتم‌های نهایی است که از یک رمز قالبی tweakable به نام Deoxys-BC استفاده می‌کند که علاوه بر کلید و متن اصلی، از یک ورودی دیگر با عنوان توئیک که غیر مخفی است بهره می‌برد. برای اولین بار است که امنیت رمز قالبی کاهش یافته Deoxys-BC-256، با در نظر گرفتن جهت درست جایگشت قسمت تولید کلید، توسط تحلیل تفاضل ناممکن بررسی شده است. تحلیل‌های ارائه شده، از نوع تک-کلید و کلید-مرتبط است که تمامی این تحلیل‌ها از یک مشخصه تفاضل ناممکن ۴٫۵ دوری که توسط روش فقدان در میانه تولید شده است، بهره می‌برند. حملات ارائه شده به هشت و نه دور الگوریتم اعمال شده، حال آن که با توجه به ادعای طراحان Deoxys که اعمال تحلیل تفاضلی به هشت دور Deoxys-BC-256 را غیرممکن می‌خوانند، نتایج ارائه شده در این مقاله به منظور فهم کران امنیتی دقیق این رمز قالبی می‌تواند مفید باشد. حمله هشت دوری تک-کلید و حملات کلید-مرتبط هشت و نه دوری تنها حملات اعمال شده تفاضل ناممکن به این تعداد دور، با در نظر گرفتن جهت درست جایگشت بوده و پیچیدگی به مراتب پایین‌تری از جستجوی فراگیر دارد.

واژه‌های کلیدی: الگوریتم رمزگذاری احرازاصالت‌شده، تحلیل تفاضل ناممکن، کلید مرتبط، مسابقه سزار، Deoxys.

The ISC Int'l Journal of Information Security
ISeCure

July 2018, Volume 10, Number 2 (p. 165)
http://www.isecure-journal.org

Persian Abstract

منطق نادانی توزیع شده و امنیت

رحیم رمضانیان

دانشکده علوم ریاضی، دانشگاه صنعتی شریف، تهران، ایران

در علم امنیت اطلاعات عبارت «نادانی موهبت نیست» مشهور است. همواره یادآوری می‌شود که پنهان نمودن پروتکل مورد استفاده از دیگران امنیت ساز و کار را افزایش نمی‌دهد. اما مواردی وجود دارد که نادانی باعث تولید پروتکل می‌شود. در این پژوهش منطق نادانی توزیع شده به عنوان گسترشی از منطق نادانی ارائه شده است. به طور شهودی یک فرمول نادانی توزیع شده در یک گروه است هرگاه از مجموع دانش اعضای گروه نتیجه نشود. در این پژوهش با روش‌های صوری طرح تسهیم راز (خاصیتی که براساس نادانی عامل‌ها ساخته می‌شود) و یک حمله مرد میانی به یک پروتکل ضعیف را در منطق نادانی توزیع شده بررسی می‌کنیم. همچنین شرایطی را معرفی می‌کنیم که آزاد نمودن یک راز می‌تواند منجر به پنهان شدن رازی دیگر برای همیشه شود. در انتها قضایای صحت و تمامیت را برای این منطق اثبات می‌کنیم و همچنین نشان می‌دهیم که منطق ارائه شده از منطق نادانی و منطق شناختی قوی‌تر است.

واژه‌های کلیدی: منطق نادانی، منطق نادانی توزیع شده، طرح تسهیم راز، حمله مرد میانی.

The ISC Int'l Journal of Information Security
ISeCure

July 2018, Volume 10, Number 2 (p. 166)
http://www.isecure-journal.org

Persian Abstract

بحث در مورد امنیت O-PSI تعیین اشتراکات امن به‌صورت برون‌سپاری شده

مهدی مهدوی علیائی[۱]، مهشید دلاور[۱]، محمدحسن عامری اختیارآبادی[۱]، جواد مهاجری[۱] و محمدرضا عارف[۲]

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

در سال‌های اخیر، تعیین اطلاعات مشترک به‌صورت امن و مؤثر بین دو طرف در شبکه‌های اجتماعی به یک مسئله مهم تبدیل‌شده است. بسیاری از پروتکل‌های تعیین اشتراکات به‌صورت امن (PSI) برای رسیدگی به این موضوع معرفی‌شده‌اند. با استفاده از این پروتکل‌ها، دو طرف می‌توانند اشتراکات بین مجموعه خود را بدون افشای اطلاعات در مورد اعضای غیرمشترک، محاسبه کنند. با توجه به طیف وسیعی از منابع محاسباتی که ابر می‌تواند برای کاربران آن فراهم کند، تعیین اشتراکات توسط ابر ممکن است هزینه محاسباتی کاربران را کاهش دهد. پروتکل‌های پیشنهادی توسط آبادی و همکاران دو پروتکل در این زمینه هستند. در این مقاله، ما نشان می‌دهیم که پروتکل‌های آن‌ها در برابر حمله شنود آسیب‌پذیر هستند. همچنین یک راه حل برای حفاظت از پروتکل ذکر شده پیشنهاد می‌شود. علاوه بر این، ما تجزیه و تحلیل عملکرد پروتکل‌های PSI و O-PSI اصلاح شده نشان می‌دهد که طرح ما با پروتکل O-PSI قابل مقایسه است. در واقع، یک راه حل بدیهی برای طرحهای ارائه شده توسط آبادی و همکاران، استفاده از یک کانال امن مانند TLS است. با این حال، در ارزیابی عملکرد، ما تغییرات اعمال شده را با این راه حل بدیهی مقایسه می‌کنیم و نشان می‌دهیم که اصلاح پیشنهاد ما بیشتر از آن چیزی است که رمزگذاری اضافی توسط TLS تحمیل می‌کند.

واژه‌های کلیدی: پروتکل O-PSI، سرور ابری، حمله شنود.

The ISC Int'l Journal of Information Security
ISeCure

July 2018, Volume 10, Number 2 (p. 167)
http://www.isecure-journal.org

Persian Abstract

اعمال خط‌مشی‌های کنترل دسترسی نقش مبنا روی داده‌های برون‌سپاری شده سمت کارگزار نامعتمد

نعیمه سلطانی[1]، رامین بهلولی[1] و رسول جلیلی[1]

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

امروزه بیشتر سازمان‌ها براي نگهداری و حفاظت داده‌ها و اطلاعات خود به برون‌سپاري روی آورده‌اند. یکی از مسائل مهم امنیتی در سناریوی برون سپاري داده‌ها، اعمال خط‌مشی‌های کنترل دسترسی مدنظر مالک داده‌ها است. این مسئله از منظر تعداد کلیدهای مورد نیاز کاربران، کارایی به روزرسانی خط مشی‌های کنترل دسترسی، پشتیبانی از مجوزهای نوشتن، سربارهاي سمت کارخواه و مالک، و همچنین حفظ محرمانگی این خط مشی‌ها قابل بررسی است. اغلب روش‌های ارائه شده در این زمینه تنها برخی از این چالش‌ها را مد نظر قرار داده و سربار غیر قابل قبولی به مالک داده‌ها و کاربران تحمیل می‌کنند؛ علاوه بر این بیشتر پژوهش‌ها، اعمال خطمشی‌های ماتریسی را هدف قرار داده‌اند و کمتر به اعمال خط‌مشی‌ها در مدل کنترل دسترسی نقش‌مبنا توجه شده است. این در حالی است که در مدل کنترل دسترسی نقش‌مبنا، به دلیل اعطای مجوزها به نقش‌ها و اعطای نقش‌ها به کاربران و همچنین بهره‌گیری از ساختار سلسله مراتب و قاعده ارث‌بری مجوزها بین نقش‌ها، مدیریت خطمشی‌ها ساده‌تر می‌گردد. در این مقاله به ارائه راهکاری جهت اعمال خط مشی هاي نقش مبنا، روي داده‌هاي رمزشده و برون‌سپاري‌شده سمت کارگزار پرداخته می شود. در راهکار پیشنهادی ضمن حفظ محرمانگی خطمشی‌ها، از قضیه باقیمانده چینی براي مدیریت کلیدها و اعطاي مجوزها به نقش‌ها و همچنین اعطای نقشها به کاربران استفاده شده است. بازستانی و اعطاي نقش از/به کاربران با کمترین سربار انجام شده و همچنین به‌روزرسانی‌های ساختار سلسله مراتب نقش‌ها مورد توجه قرار گرفته است. علاوه بر این، نحوه‌ی بهره‌گیری از ساختار سلسله مراتب نقش‌ها به گونه‌ای است که با افزودن نقشی جدید به ساختار، کاربران آن بدون نیاز به رمزگذاری مجدد و هیچ عملیات اضافه‌ی دیگری، به کلیه منابع مجاز رمزشده قبل و بعد از افزودن نقش، دسترسی دارند. در این راهکار نحوه‌ی رمزگذاری منابع به گونه‌ای است که حجم منبع رمزشده مستقل از تعداد کاربران و نقش‌ها و عمق ساختار سلسله مراتب بوده و فقط با حجم منبع خام رابطه‌ای خطی دارد. اعمال خط‌مشی‌های کنترل دسترسی نوشتن نیز از دیگر قابلیت‌ها و برتری‌های راهکار پیشنهادی این مقاله است.

واژه‌های کلیدی: کنترل دسترسی، داده‌های برون‌سپاری شده، کنترل دسترسی نقش‌مبنا.

The ISC Int'l Journal of Information Security
ISeCure

July 2018, Volume 10, Number 2 (p. 168)
http://www.isecure-journal.org

Persian Abstract

تشخیص URL مخرب و نوع حملات آن با استفاده از ویژگی های URL و دسته بندهای چندکلاسه

هارماراج پاتیل[1] و جایانتراو پاتیل[1]

[1]گروه مهندسی کامپیوتر، موسسه فناوری پاتل، شیرپور، هند

امروزه، نشانی‌وب‌های URL مخرب تهدیدی مشترک برای کسب‌وکارها، شبکه‌های اجتماعی، و شبکه‌های بانکی هستند. با این حال، نشانی‌وب‌های مخرب با حملات تحت وب مختلفی از جمله فیشینگ، هرزنامه‌ها، و توزیع بدافزار سر و کار دارند. اکثر روش‌های موجود بر روی شناسایی دودویی مانند تشخیص مخرب یا غیر مخرب بودن نشانی‌وب متمرکز شده‌اند. تنها تعداد محدودی از پژوهش‌ها علاوه بر شناسایی نشانی‌وب مخرب، نوع حمله را نیز تشخیص می‌دهند. از این رو، تشخیص نوع حمله و اقتباس روش مقابله کارا یک مساله مهم به شمار می رود. در این پژوهش، راهکاری برای تشخیص نشانی‌وب‌های مخرب و نوع حمله آنها مبتنی بر دسته‌بندی چند کلاسه ارائه شده است. در این روش، ۴۲ ویژگی جدید شامل هرزنامه، فیشینگ، و نشانی‌وب‌های مخرب مانند ویژگی‌های نشانی‌وب، ویژگی‌های منبع نشانی‌وب، ویژگی‌های نام دامنه، و ویژگی‌های نشانی‌وب‌های کوتاه شده پیشنهاد شده است. این ویژگی‌ها در پژوهش‌های اخیر تشخیص نشانی‌وب‌های مخرب و نیز نوع حمله آن‌ها در نظر گرفته نشده‌اند. مجموعه داده‌های دودویی و چند کلاسه با استفاده از ۴۹۹۳۵ نشانی‌وب متشکل از ۲۶۰۴۱ نشانی‌وب سالم و ۲۳۸۹۴ مخرب که از میان نشانی‌وب‌های مخرب به ترتیب ۱۱۲۹۷، ۸۹۷۶، و ۳۶۲۱ مورد مربوط به بدافزار، فیشینگ، و هرزنامه است، ایجاد شده است. برای ارزیابی روش ارائه شده از دسته‌بندهای با ناظر دسته‌ای و برخط جدید در حوزه یادگیری ماشین بر روی مجموعه داده های دودویی و چند کلاسه استفاده شده است. در این ارزیابی، دسته‌بند یادگیری وزن‌دار معتمد با بهره‌گیری از ویژگی‌های ارائه شده نشانی‌وب در تنظیمات چند کلاسه، بهترین میانگین دقت در تشخیص به میزان ٪۹۸٫۴۴ با نرخ خطای ٪۱٫۵۶ و در تنظیمات دودویی دقتی برابر با ٪۹۹٫۸۶ با نرخ خطای قابل اقماض ٪۰٫۱۴ را به دست آورده است.

واژه‌های کلیدی: حملات تحت وب، نشانی‌وب مخرب، یادگیری برخط، استراخ ویژگی.