The ISC Int'l Journal of Information Security
ISeCure

January 2018, Volume 10, Number 1 (p. 71)
http://www.isecure-journal.org

Persian Abstract

حمله تفاضل ناممکن بر روی الگوریتم رمز قالبی Midroi64

آیین رضایی شهمیرزادی[۱]، سید آرش عظیمی[۱]، محمود سلماسی زاده[۲]، جواد مهاجری[۲] و محمدرضا عارف[۳]

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

حمله تفاضل ناممکن یک حمله بسیار شناخته شده برای ارزیابی و آنالیز الگوریتم‌های رمز قالبی است. با استفاده از این حمله، میزان امنیت یک الگوریتم رمز قالبی سبک را به نام Midori بررسی کردیم. این الگوریتم با توجه به انرژی مصرف شده به هنگام رمزنگاری طراحی شده است به طوری که کمترین انرژی مصرف شود. این الگوریتم دارای دو نسخه به نام‌های Midori128 و Midori64 است که هر کدام به ترتیب دارای طول قالب ۶۴ بیت و ۱۲۸ بیت است و هر دو نسخه دارای ۱۲۸ بیت طول کلید است. در این مقاله، برای آنالیز امنیت الگوریتم یاد شده، از تکنیک‌های متنوعی مانند miss-in-the-middle، early-abort، و memory reallocation و توجه به الگوریتم بست کلید Midori64 استفاده شده است. در ابتدا ۲ مشخصه به طول هفت دور معرفی شده است که بیشترین طول مشخصه تا به حال است. بر اساس این دو مشخصه به ده، یازده و دوازده دور از Midori64 حمله شده است.

واژه‌های کلیدی: رمز قالبی، Modiri، حمله تفاضل ناممکن.

The ISC Int'l Journal of Information Security
ISeCure

January 2018, Volume 10, Number 1 (p. 72)
http://www.isecure-journal.org

Persian Abstract

یک پروتکل اشتراک داده امن، سبک وزن و محرک برای ارتباطات دستگاه به دستگاه در شبکه سلولی نسل پنجم

عاطفه محسنی اژیه[1]، مائده عاشوری تلوکی[1] و مجتبی مهدوی[1]

[1]گروه مهندسی فناوری اطلاعات، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، اصفهان، ایران

با افزایش تعداد دستگاه‌های هوشمند در سال‌های اخیر، ترافیک داده شبکه‌های سلولی رشد قابل ملاحظه‌ای یافته است. این امر باعث شده است نیاز به راه‌حل‌هایی جهت کاهش بار اپراتورها احساس شود. ارتباطات دستگاه به دستگاه به عنوان یک راه‌حل امیدبخش جهت استفاده از ظرفیت شبکه‌های سلولی و کاهش بار شبکه زیرساخت شناخته می‌شود. اما ارتباط مستقیم دستگاه‌ها به یکدیگر دارای آسیب‌پذیری‌های امنیتی است. در این مقاله، یک روش اشتراک داده امن، سبک وزن و محرک جهت ارتباطات دستگاه به دستگاه در شبکه سلولی نسل پنجم ارائه شده است که در آن تهدیدات امنیتی اصلی در پروتکل‌های اشتراک داده شامل محرمانگی، صحت، تشخیص تغییر پیام و اجتناب از انتشار داده اشتباه در نظر گرفته شده است. به علاوه از یک مکانیزم محرک (ایجاد انگیزه) جهت تشویق کاربران به همکاری در پروتکل اشتراک داده استفاده شده است. در واقع، همکاری کاربران در اشتراک داده در ارتباطات دستگاه به دستگاه نقش کلیدی دارد، بنابراین در این مقاله از مکانیزم چک مجازی جهت تشویق کاربران به همکاری در پروتکل اشتراک داده استفاده شده است. برخلاف روش‌های قبلی، روش ارائه شده در این مقاله به اطلاعات زمینه کاربران نیاز ندارد، بنابراین می‌تواند در هر زمان و مکانی استفاده شود. تحلیل‌های امنیتی پروتکل نشان می‌دهد که این روش نسبت به حملات امنیتی ایمن است و نیازمندی‌های امنیتی پروتکل‌های اشتراک داده را برآورده می‌کند. تحلیل کارایی پروتکل نشان می‌دهد روش ارائه شده نسبت به روش‌های موجود از نظر هزینه محاسبات و ارتباطات بهتر عمل می‌کند.

واژه‌های کلیدی: ارتباطات دستگاه به دستگاه، کاهش بار، امنیت، سبک وزن، اشتراک داده، انگیزه.

The ISC Int'l Journal of Information Security
ISeCure

January 2018, Volume 10, Number 1 (p. 73)
http://www.isecure-journal.org

Persian Abstract

طبقه‌بندی ترافیک رمزگذاری شده با استفاده از روش‌های آماری

احسان مهدوی[1]، علی فانیان[1] و هما حسن‌نژاد[1]

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

دسته‌بندی ترافیک نقش مهمی در بسیاری از کاربردهای شبکه مانند شناسایی انواع ترافیک، شناسایی کاربردهای بدخواه، اعمال سیاست جهت محدودسازی دسترسی به شبکه و غیره ایفا می‌کند. روش‌های پایه، شناسایی ترافیک را بر اساس پارامترهای ظاهری بسته نظیر شماره پورت یا شماره پروتکل بسته‌ها انجام می‌دهند. اما امروزه با تغییراتی که کاربردها در پارامترهای بسته اعمال می‌کنند، این روش‌ها نمی‌توانند به‌خوبی دسته‌بندی ترافیک را انجام دهند. از این رو، روش‌های شناسایی ترافیک براساس یادگیری ماشین امروزه استفاده می‌شوند. در این مقاله، یک روش یادگیری نیمه نظارتی مبتنی بر خوشه‌بندی و انتشار برچسب پیشنهاد می‌گردد. در قسمت خوشه‌بندی از نظریه گراف و الگوریتم درخت کمینه فراگیر استفاده می‌گردد. در سطح بعد، تعدادی از نمونه‌های مهم و تاثیرگذار انتخاب می‌شوند تا برچسب آن‌ها از خبره سوال شود. پس از مشخص شدن برچسب آن‌ها، سایر نمونه‌هایی که در کلاس مشابه قرار گرفته‌اند دارای برچسب آن نمونه‌ها می‌شوند. در نهایت الگوریتم درخت تصمیم برای دسته‌بندی ترافیک به‌کار می‌رود. نتایج ارزیابی و شبیه‌سازی روش پیشنهادی نشان‌دهنده آن است که این روش دارای دقت و کارایی مناسبی در دسته‌بندی ترافیک‌های رمز شده می‌باشد. این روش همچنین می‌تواند برای ترافیک‌های غیر رمز به خصوص داده‌های نامتعادل نیز عمل دسته‌بندی و شناسایی ترافیک را به‌خوبی انجام دهد.

واژه‌های کلیدی: طبقه‌بندی ترافیک اینترنت، نظریه گراف، ترافیک رمزگذاری شده.

The ISC Int'l Journal of Information Security
ISeCure

January 2018, Volume 10, Number 1 (p. 74)
http://www.isecure-journal.org

Persian Abstract

NETRU: یک سامانه رمزنگاری ناجابجایی و امن براساس طرح رمزنگاری CTRU

رضا ابراهیمی آتانی[۱]، شهاب الدین ابراهیمی آتانی[۲] و امیر حسنی کرباسی[۱]

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

[۲]گروه ریاضی، پردیس دانشگاهی، دانشگاه گیلان، رشت، ایران

سامانه NETRU عضوی از خانواده سامانه‌های رمزنگاری مشبکه-مبنای شبه NTRU است که مبتنی بر میدان‌های متناهی و نسخه ناجابجایی از سامانه CTRU است و بر اساس حلقه ناجابجایی $M = M_k(\mathbb{Z}_p)[T,x]/ < X^n - I_{k\times k} >$ عمل می‌کند به طوری که M یک حلقه ماتریسی از ماتریس‌های $k \times k$ روی چندجمله‌ای‌های $R = \mathbb{Z}_p[T,x]/ < x^n - ۱ >$ است. در تحلیل امنیتی NETRU نشان می‌دهیم که محاسبات رمزگذاری و رمزگشایی در آن ناجابجایی بوده و در مقابل حملات مشبکه و حملات جبر خطی مقاوم است.

واژه‌های کلیدی: رمزنگاری مشبکه-مبنا، سامانه رمز، CTRU حلقه‌های ماتریسی، میدان‌های متناهی.

The ISC Int'l Journal of Information Security
ISeCure

January 2018, Volume 10, Number 1 (p. 75)
http://www.isecure-journal.org

Persian Abstract

ارائه‌ی یک روش مبتنی بر هیورستیک برای تشخیص بات‌نت

احسان خوشحال‌پور[1] و حمیدرضا شهریاری[1]

[1] دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر، تهران

بدون تردید امروزه بات‌نت‌ها از ابزارهای اساسی برای انجام حملات اینترنتی به شمار می‌آیند. بات‌نت در حقیقت شبکه‌ای از کامپیوترهای مورد سوءاستفاده قرار گرفته (بات) است که از طریق یک کانال فرمان و کنترل تحت کنترل یک مهاجم (بات‌مستر) عمل می‌کنند. بات‌نت‌ها برای انجام فعالیت‌های بدخواه مختلف از جمله حملات ممانعت از سرویس توزیع شده، ارسال هرزنامه، تقلب کلیک، میزبانی سایت‌های کلاه‌برداری و سرقت اطلاعات به کار برده می‌شوند. روش‌های مختلفی برای تشخیص بات‌نت ارایه شده است. اما بسیاری از این روش ها به دلیل تکیه بر یک مشخصه ی خاص از بات نت ها، با تغییر جزئی در پروتکل، ساختار و یا عملکرد دیگر کارامد نخواهند بود. همچنین اکثر آنها در صورت وجود تنها یک بات در شبکه ی تحت نظارت دیگر قادر به تشخیص حضور بات نخواهند بود. به همین دلیل در این مقاله با تکیه بر مفهوم چرخه‌ی حیات بات‌نت به عنوان وجه مشترک تمام بات‌نت‌ها، الگوهای رفتاری ترافیکی بات ها در یک میزبان که آنها را از سایر پردازه‌های مشروع متمایز می سازد معرفی گردد. سپس یک روش مبتنی بر هیوریستیک برای شناسایی این الگوهای رفتاری در ترافیک بات پیشنهاد می گردد. روش پیشنهادی برای بات‌ها و برنامه های کاربردی پرکاربرد مختلف مورد ارزیابی قرار گرفته است. نتایج حاصل از ارزیابی حاکی از آن است که روش پیشنهادی به طور موثری قادر به تشخیص پردازه بات در میزان سایر پردازه‌های فعال موجود در سیستم عامل است.

واژه‌های کلیدی: تشخیص بات‌نت، چرخه حیات بات‌نت، الگوریتم هیوریستیک.

The ISC Int'l Journal of Information Security
ISeCure

January 2018, Volume 10, Number 1 (p. 76)
http://www.isecure-journal.org

Persian Abstract

یک پروتکل قرعه‌کشی برخط غیرمترکز

رسول رمضانیان[1] و محسن پورپونه[2]

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

قرعه‌کشی در بسیاری از شرایط اجتماعی و نیز موقعیت‌های اقتصادی جهت انتخاب یک فرد یا گروه به صورت "عادلانه" مورد استفاده قرار می‌گیرد. از طرفی با توجه به رشد روزافزون اینترنت، مکانیسم‌های اقتصادی و اجتماعی زیادی نیازمند اجرای قرعه‌کشی برخط هستند. اجرای این قرعه‌کشی‌های باید به نحوی باشد که عامل‌های شرکت کننده بتوانند از صحت و نیز عادلانه بودن اجرای قرعه‌کشی اطمینان حاصل نمایند. در این مقاله ما به ارائه یک پروتکل قرعه‌کشی غیرمترکز برخط می‌پردازیم. در این پروتکل برنده نهایی قرعه‌کشی با همکاری تمامی افراد شرکت‌کننده در پروتکل انتخاب می‌شود. پروتکل ارائه شده در این مقاله بسیاری از ویژگی‌های یک قرعه‌کشی واقعی، مانند عادلانه بودن، تصادفی بودن، بازبودن و عدم انکار را دارا می‌باشد.

واژه‌های کلیدی: پروتکل برخط غیرمتمرکز، قرعه‌کشی، طراحی مکانیسم.