The ISC Int'l Journal of Information Security
ISeCure

January 2020, Volume 12, Number 1 (p. 68)
http://www.isecure-journal.org

Persian Abstract

توسعه‌ی حمله‌ی مکعبی با معادلات احتمالاتی و کاربرد آن در تحلیل رمز کاتان

زهرا اسکندری و عباس قائمی بافقی

دانشگاه فردوسی مشهد، گروه مهندسی کامپیوتر، آزمایشگاه امنیت داده‌ها و ارتباطات

حملات مکعبی از نمونه حملات موفق جبری می‌باشد که در دو مرحله‌ی استخراج معادلات خطی و حل انجام می‌شود. به دلیل پیچیدگی بالا در یافتن گزینه‌های مناسب برای استخراج معادلات خطی، می‌توان معادلات غیرخطی که تقریب خطی با احتمال بالا داشته، را استخراج کرد. اینچنین معادلاتی را می‌توان معادلات خطی همراه با نویز در نظر گرفت. رویکردهای موجود برای حل سیستم معادلات نویزی در نرخ خطای پایین بخوبی عمل کرده ولیکن با افزایش نرخ خطا، نرخ موفقیت تعیین جواب درست، کاهش یافته و این رویکردها در نرخ خطای بالا غیرعملی می‌باشند. در این مقاله حمله‌ی مکعبی به حوزه‌ی احتمالاتی توسعه می‌یابد. برای انجام این امر در ابتدا، رویکرد تقریب مبتنی بر ترکیب خطی معادلات غیرخطی برای استخراج معادلات خطی احتمالاتی با احتمال بالا ارائه شده و سپس به بهبود کارایی روش‌های حل سیستم معادله نویزی در نرخ خطای بالا پرداخته می‌شود. در نهایت امر، با تکیه بر رویکردهای ارائه شده، سیستم معادله مکعبی با استفاده از معادلات احتمالاتی توسعه داده شده و با حل کارا سیستم معادلات حاصل، مقدار کلید با پیچیدگی کمتری در قیاس با حمله ی مکعبی پایه تعیین می‌شود.

واژه‌های کلیدی: تقریب، حل سیستم معادلات نویزی، حمله ی مکعبی، معادلات احتمالاتی.

The ISC Int'l Journal of Information Security
ISeCure

January 2020, Volume 12, Number 1 (p. 69)
http://www.isecure-journal.org

Persian Abstract

ارائه حملاتی به GAGE (v1)، InGAGE (v1,v1.03) و نسخه‌های CiliPadi (v1)

مجید نیکنام[۱]، صادق صادقی[۱]، محمد رضا عارف[۲] و نصور باقری[۳,۴]

[۱]دانشکده علوم ریاضی و کامپیوتر، دانشگاه خوارزمی، تهران، ایران
[۲]دانشکده برق، دانشگاه صنعتی شریف، تهران، ایران
[۳]دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
[۴]پژوهشکده علوم کامپیوتر، پژوهشگاه دانش‌های بنیادی، تهران، ایران

در این مقاله، ما چند حمله به الگوریتم‌های GAGE، InGAGE و CiliPadi که از کاندیدهای دور اول رقابت رمزنگاری سبک وزن (LWC) مؤسسه ملی استاندارد و فناوری (NIST) بودند، ارائه می‌دهیم. الگوریتم‌های GAGE و InGAGE به ترتیب تابع چکیده‌ساز سبک‌وزن و تابع احراز اصالت با داده همراه (AEAD) بر پایه ساختار اسفنجی هستند و از مجموعه‌ی متفاوتی از پارامترها حمایت می‌کنند. طول مقدار چکیده، کلید و برچسب همیشه به ترتیب برابر با ۲۵۶، ۱۲۸ و ۱۲۸ بیت هستند. در این مقاله نشان داده می‌شود که کران امنیتی برای بعضی از نسخه‌های تابع چکیده و AEAD از ادعای طراحان کمتر هستند. برای مثال، ادعای امنیتی طراحان در برابر حمله پیش‌تصویر برای تابع چکیده‌ساز، برای نرخ پردازش ۱۲۸ بیتی و ظرفیت ۲۵۶ بیتی، 2^{256} است. اما، ما نشان می‌دهیم که حد بالای امنیت در برابر حمله پیش‌تصویر، برای این مجموعه پارامتر، 2^{128} است. همچنین، از منظر محرمانگی ltrAEAD، سطح امنیتی مورد ادعای طراحان برای نرخ پردازش ۸ بیتی و ظرفیت ۲۲۴ بیتی، 2^{116} است در حالی‌که ما نشان می‌دهیم که حد بالای محرمانگی آن برابر با 2^{112} است. همچنین ساختار جایگشت استفاده شده در InGAGE را بررسی می‌کنیم و یک حمله بازیابی کلید دورکاهشی برای یک نسخه از InGAGE ارائه می‌دهیم. برای یک نمونه از ltrAEAD از InGAGE، با نرخ پردازش ۸ بیتی و مقدار ظرفیت ۲۲۴ بیتی، وقتی تعداد دور r_1 کمتر از ۸ است، مقدار کلید را بازیابی می‌کنیم. با ارائه نمونه‌های واقعی از پیام‌های جعلی، همچنین نشان داده می‌شود که الگوریتم CiliPadi در برابر حمله گسترش طول آسیب‌پذیر است.

واژه‌های کلیدی: رقابت رمزنگاری سبک‌وزن مؤسسه ملی استاندارد و فناوری، GAGE، InGAGE، حمله پیش‌تصویر، جامعیت، محرمانگی، بازیابی کلید، MILP، CiliPadi.

The ISC Int'l Journal of Information Security
ISeCure

January 2020, Volume 12, Number 1 (p. 70)
http://www.isecure-journal.org

Persian Abstract

روش پنهان‌نگاری شبکه مبتنی بر طول بسته با امنیت بالا

وجیهه ثابتی[1] و مینو شعاعی[2]

[1]استادیار، دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران

[2]دانشجوی کارشناسی ارشد، دانشکده فنی و مهندسی، دانشگاه الزهرا، تهران، ایران

در روش‌های پنهان‌نگاری شبکه مبتنی بر طول بسته، طول بسته‌ها به عنوان حاملی برای انتقال پیام محرمانه استفاده می‌شود. روش‌های موجود در این حوزه به دلیل رفتار غیرعادی ترافیک شبکه، در برابر کشف آسیب‌پذیر هستند. هدف اصلی در این مقاله، پیشنهاد روشی است که امنیت بالایی در برابر حملات ترافیک شبکه داشته باشد. در روش پیشنهادی اول، فرستنده در هر زوج شامل دو طول بسته‌ی غیریکسان، یک بیت داده را جاسازی می‌کند. در وضعیت موجود، اگر طول بسته اول زوج بزرگتر از طول بسته دوم آن باشد، بیت یک و در غیراین صورت بیت صفر را نشان می‌دهد. اگر بیت موردنظر فرستنده با وضعیت موجود مغایرت داشته باشد، فرستنده با جابه‌جا کردن بسته‌ها در ترافیک وضعیت موردنظر خود را ایجاد می‌کند. در این روش، بسته‌های زوج شده می‌توانند به صورت آزاد انتخاب شوند، اما در روش پیشنهادی دوم، بسته‌ها به باکت‌هایی تقسیم‌بندی شده و فقط بسته‌های داخل یک باکت می‌توانند با یکدیگر زوج شوند. در این حالت، روش جاسازی مشابه روش قبل است. نتایج تست نشان می‌دهد که روش پیشنهادی دوم با وجود ظرفیت جاسازی کم، در ترافیک واقعی امنیت بسیار بالاتری نسبت به روش‌های قبلی دارد. با توجه به تصادفی‌تر بودن طول بسته‌های پروتکل UDP نسبت به TCP، روش‌های پیشنهادی برای بسته‌های مبتنی بر پروتکل UDP ظرفیت جاسازی بالاتر و امنیت بیشتری دارند. روش‌های پیشنهادی فقط برای پروتکل‌هایی قابل استفاده است که طول بسته‌ها مقدار ثابتی نیست.

واژه‌های کلیدی: کانال نهان، امنیت داده، نهان‌نگاری شبکه، طول بسته، نهان‌کاوی.

The ISC Int'l Journal of Information Security
ISeCure

January 2020, Volume 12, Number 1 (p. 71)
http://www.isecure-journal.org

Persian Abstract

ریزتجمیع یک‌متغیره بهبودیافته برای داده‌های عددی صحیح

رضا مرتضوی

گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه دامغان، دامغان، ایران

یکی از دغدغه‌های اصلی هنگام انتشار داده‌ها مربوط به حریم خصوصی است. این مسئله در حوزه کنترل افشای آماری بررسی می‌شود که هدف آن تولید داده‌های محافظت‌شده‌ای است که در عین حال برای کاربران نهایی مانند سازمان‌های دولتی و گروه‌های تحقیقاتی نیز مفید باشد. این مطلب در مدل‌های حریم خصوصی محاسباتی متعددی از جمله در مدل k-بی‌نامی مورد توجه قرار گرفته است. در این مدل، داده‌ها در گروه‌هایی با حداقل k عضو خوشه‌بندی می‌شوند. ریزتجمیع مکانیزمی برای پیاده‌سازی این مدل است که هدف آن انتساب رکوردهای مجموعه داده به خوشه‌ها و جایگزینی مقادیر اصلی با مراکز خوشه‌ی منتسب شده است. این مراکز خوشه به صورت میانگین مقادیر منتسب به آن محاسبه می‌شوند تا اتلاف اطلاعاتی بر حسب معیار SSE کاهش یابد. گرچه مسئله ریزتجمیع در حالت کلی جزو مسائل NP-hard است، اما ثابت شده که برای مجموعه داده‌های یک‌متغیره یک الگوریتم بهینه با زمان اجرای چندجمله‌ای وجود دارد. این مقاله نشان می‌دهد که انتساب صورت گرفته در این نسخه یک‌متغیره نمی‌تواند خوشه‌های بهینه را برای مجموعه داده‌های صحیحی که می‌بایست مقادیر منتشر شده مراکز خوشه نیز صحیح باشند، به‌دست آورد. به بیان دیگر، قید مربوط به صحیح بودن بر روی داده‌های منتشر شده باید در ضمن اجرای الگوریتم در نظر گرفته شود. در ادامه، الگوریتم کارایی با لحاظ قید فوق ارائه و بررسی شده است که می‌تواند بر روی مجموعه داده‌های خیلی بزرگ هم کار کند. نتایج ارزیابی تجربی موید این مطلب است که الگوریتم توسعه‌داده شده در این مقاله نه تنها مجموعه داده‌های محافظت‌شده سودمندتری را تولید می‌کند، بلکه نسبت به روش یک‌متغیره عمومی کارآمدتر نیز هست.

واژه‌های کلیدی: حریم خصوصی داده‌ها، پایگاه داده‌های آماری، محافظت از ریزداده، ریزتجمیع، بهینه‌سازی عدد صحیح.

The ISC Int'l Journal of Information Security
ISeCure

January 2020, Volume 12, Number 1 (p. 72)
http://www.isecure-journal.org

Persian Abstract

کشف حملات وب مبتنی بر ناهنجاری: کاربرد شبکه عصبی عمیق seq2seq با سازوکار Attention

شهریار محمدی و امین نمدچیان

گروه فناوری اطلاعات، دانشکده مهندسی صنایع، دانشگاه صنعتی خواجه نصیرالدین طوسی، تهران، ایران

امروزه بسیاری از فعالیت‌ها و داده‌های مهم در سایت‌های اینترنتی قرار دارد، لذا تلاش برای نفوذ به آن‌ها رشد زیادی داشته است. سیستم‌های تشخیص نفوذ حملات وب یکی از راه‌کارهایی است که برای محافظت از کاربران انجام می‌شود. اما این سیستم‌ها مشکلاتی از قبیل دقت پایین در شناسایی حملات جدید دارند که برای رفع این مشکل در سال‌های اخیر از روش‌های مختلف یادگیری ماشین در این حوزه استفاده شده است. درخواست‌های حمله تفاوت اندکی نسبت به درخواست‌های عادی دارند، لذا روش‌های تشخیص ناهنجاری نتوانستند دقت مناسبی در تشخیص حملات جدید بدست آورند. معمولا در درخواست‌ها و پاسخ‌های وب مقادیر زیادی داده مرتبط با یکدیگر جابه‌جا می‌شود که در نظر گرفتن تمامی ارتباطات بین آن‌ها برای تشخیص ناهنجاری‌ها لازم ولی بسیار مشکل است. لذا در اغلب پژوهش‌ها تنها به تحلیل URL و بخشی از درخواست برای یافتن حملات اکتفا می شود. ما در این پژوهش روش جدیدی برای تشخیص حملات وب بر اساس شبکه‌های seq2seq با استفاده از Attention ارائه دادیم که توانستیم با پیش‌بینی پاسخ‌های احتمالی و اندازه‌گیری تفاوت با پاسخ‌های واقعی وب‌سرور، ترافیک وب را کلاس‌بندی نماییم.

دقت بهتر مدل پیشنهادی نسبت به روش‌های مشابه نشان داد که استفاده از سازوکار Attention می‌تواند چالش تحلیل درخواست و پاسخ‌های طولانی وب را تا حد زیادی مرتفع نماید. مدل ما در حملاتی مانند SQL Injection و XSS که پاسخ سرور در موفقیت‌آمیز بودن آن نقش زیادی دارد، توانست دقت خوبی کسب نماید که این مسئله ناشی از در نظر گرفتن ارتباط بین درخواست و پاسخ در شناسایی حملات وب در روش پیشنهادی است.

واژه‌های کلیدی: شبکه seq2seq عمیق، سامانه تشخیص نفوذ وب، سازوکار Attention.

The ISC Int'l Journal of Information Security
ISeCure

January 2020, Volume 12, Number 1 (p. 73)
http://www.isecure-journal.org

Persian Abstract

کشف حملات وب مبتنی بر ناهنجاری: کاربرد شبکه عصبی عمیق seq2seq با سازوکار Attention

بشیر نادری[۱]، حسین خیری[۲] و وجیهه وفائی[۲]

[۱]دانشکده ریاضی، دانشگاه پیام نور، تهران، ایران
[۲]دانشکده علوم ریاضی، دانشگاه تبریز، تبریز، ایران

در این مقاله، یک روش مخابرات امن بر اساس همزمان‌سازی دو سیستم آشوبناک مرتبه کسری یکسان ارائه شده است. مشتق مرتبه کسری به مفهوم کاپوتو در نظر گرفته شده و برای همزمان‌سازی، از روش کنترلی مدلغزشی قوی استفاده شده است. به دلیل استفاده از یک تکنیک خاص برای سیستم‌های مرتبه کسری، سطح لغزشی طراحی شده، ساده در نظرگرفته شده است. همچنین برخلاف اکثرمقالات، مرتبه مشتقات کسری متغیرهای حالت می‌توانند، متفاوت انتخاب شوند. پایداری سیستم خطا با استفاده از پایداری لیاپانوف برای سیستم‌های مرتبه کسری ثابت شده است. شبیه‌سازی‌های عددی اثربخشی و توانایی روش پیشنهادی را نشان می‌دهند. همچنین نتایج همزمان‌سازی در مخابرات امن با استفاده از روش مخفی کردن داده‌ها در متغیرهای حالت مورد استفاده قرار می‌گیرد. تحلیل امنیتی نشان می‌دهد که الگوریتم معرفی شده دارای یک فضای کلیدی گسترده، حساسیت بالا به کلیدهای رمزگذاری، امنیت بالاتر و سرعت عملکردی قابل قبول است.

واژه‌های کلیدی: سیستم‌های مرتبه کسری، کنترل مدلغزشی، همزمان‌سازی، مخابرات امن.