The ISC Int'l Journal of Information Security
ISeCure

January 2019, Volume 11, Number 1 (p. 87)
http://www.isecure-journal.org

Persian Abstract

روشی احتمالاتی مبتنی بر اعتماد برای درستی‌سنجی کارا در برون‌سپاری پایگاه‌داده

سیمین قاسمی[۱]، محمدعلی هادوی[۲] و مینا نیک‌نفس[۳]

[۱]گروه مهندسی کامپیوتر، دانشگاه پیام نور، تهران، ایران
[۲]دانشگاه صنعتی مالک اشتر، تهران، ایران
[۳]گروه مهندسی کامپیوتر، دانشکده فنی مهندسی، دانشگاه ولی عصر(عج)، رفسنجان، ایران

درستی‌سنجی نتایج پرسمان‌ها یک چالش قابل توجه در سناریوی برون‌سپاری پایگاه‌داده محسوب می‌شود. بیشتر راهکارهای ارائه شده سربار زیادی تحمیل می‌کنند، به‌طوری‌که استفاده از این سناریو در دنیای واقعی غیرممکن می‌شود. راهکارهای احتمالاتی به منظور کاهش سربار مرتبط با فرآیند درستی‌سنجی ارائه شده‌اند. در این پژوهش، ما از مفهوم اعتماد به عنوان پایه روش احتمالاتی خود برای درستی‌سنجی کارا از پاسخ پرسمان‌ها استفاده کرده‌ایم. تاریخچه تعاملات بین کارپذیر و کارخواه‌ها به‌عنوان مبنای محاسبه‌ی اعتماد به عملکرد کارپذیر به‌شمار می‌رود. در راهکار ما، ساختار داده‌ی درخت چکیده‌ساز مرکل بهبود داده شده است؛ به‌گونه‌ای که میزان اعتماد به کارپذیر موجب می‌شود تا تنها بخشی از درخت برای درستی‌سنجی استفاده شود. نتایج پیاده‌سازی روش ما نشان می‌دهد که میزان اعتماد به کارپذیر که بر اساس تاریخچه ارتباطات محاسبه شده است، موجب ایجاد یک مصالحه بین کارایی و امنیت گردیده و سربار تحمیلی به کارخواه را کاهش داده است.

واژه‌های کلیدی: برون‌سپاری پایگاه‌داده، امنیت، درستی‌سنجی پاسخ پرسمان، اعتماد، درخت چکیده‌ساز مرکل.

The ISC Int'l Journal of Information Security
ISeCure

Janaru 2019, Volume 11, Number 1 (p. 88)
http://www.isecure-journal.org

Persian Abstract

SESOS: شمای برون سپاری جستجوپذیر قابل تایید برای داده‌های ساختار ترتیبی در پردازش ابری

جواد قره چمنی[۱،۲]، محمد صادق دوستی[۱]، رسول جلیلی[۱] و دیمیتریس پاپادوپولوس[۲]

[۱]دانشگاه صنعتی شریف، تهران، ایران
[۲]دانشگاه علم و تکنولوژی هنگ کنگ، هنگ کنگ

در حالی که پردازش ابری به سرعت در حال گسترش است، هنوز مشکلات بسیاری در زمینه حریم خصوصی وجود دارد. یک راه کار برای حل مشکل حریم خصوصی ذخیره سازی داده‌ها به‌صورت رمز شده روی ابر است. اما این کار باعث از دست رفتن قابلیت پردازش روی داده‌ها می‌شود. یکی از راهکاری‌هایی که برای فراهم‌کردن امکان پردازش در کنار رمز نگاه داشتن داده وجود دارد استفاده از روش‌های رمزنگاری کاملا همریخت است. اگرچه این روش‌ها امکان اجرای محاسبات را بر روی داده‌های رمز شده فراهم می‌کنند اما به دلیل کندی بیش از حد نمی‌توان از آن‌ها در کاربردهای واقعی بهره برد. راه کار دیگری که در این حوزه وجود دارد استفاده از روش‌های رمزنگاری خاص منظوره است که امکان اجرای یک یا تعداد محدودی عملیات را بر روی داده‌های رمز شده فراهم می‌کنند. در این مقاله ما یک روش رمزنگاری خاص منظوره ارائه کرده‌ایم که امکان جستجوی سریع بر روی داده‌های ساختارترتیبی مثل تاریخ و شناسه شبکه را فراهم می‌کند. روش ارائه شده SESOS نام دارد و امکان اجرای پرس و جوهای LIKE تساوی و مقایسه را میسر می‌سازد. همچنین در نسخه تکمیلی این روش امکان تایید صحت داده ارسال شده توسط سرور نیز وجود دارد. در این روش، سربار اجرای پرس و جوی تساوی و مقایسه بسیار ناچیز است. کارایی روش ارائه شده بطور قابل ملاحظه‌ای در مقایسه با روش‌های قبل ارتقا یافته به‌طوری‌که در زمان رمزگشایی تا ۵۲۰ برابر افزایش سرعت و در اجرای پرس و جوهای LIKE تا ۱۳۷۰ برابر افزایش سرعت بر روی مجموعه داده‌ای با اندازه ۱۰۰ هزار رکورد به‌دست آمده است.

واژه‌های کلیدی: پرداش ابری، برون سپاری داده، رمزنگاری حافظ ترتیب، رمزنگاری جستجو پذیر.

The ISC Int'l Journal of Information Security
ISeCure

January 2019, Volume 11, Number 1 (p. 89)
http://www.isecure-journal.org

Persian Abstract

ماتریس‌های سبک‌وزن MDS از مرتبه ۴ برای اولیه‌های رمزنگاری با پیاده‌سازی در سخت‌افزار

اکبر محمودی ریشکانی[۱]، محمدرضا میرزایی شمس آباد[۲] ، سید مجتبی دهنوی[۳]، محمد امین امیری[۴]، حمیدرضا میمنی[۱] و نصور باقری[۱]

[۱]دانشکده علوم، دانشگاه تربیت دبیر شهید رجایی، تهران، ایران
[۲]دانشکده علوم ریاضی، دانشگاه شهید بهشتی، تهران، ایران
[۳]پژوهشکده شهید بهشتی، صنایع مخابرات ایران، ایران
[۴]پژوهشکده شهید بهشتی، صنایع مخابرات ایران، ایران
[۵]دانشکده برق، دانشگاه صنعتی مالک اشتر، تهران، ایران

لایه‌های انتشار یکی از اجزای مهم توابع درهم‌ساز و الگوریتم‌های رمز بلوکی سبک‌وزن هستند. در این مقاله مجموعه‌ای از ماتریس‌های MDS سبک‌وزن از مرتبه ۴ که هزینه پیاده‌سازی‌شان با وارون‌شان برابر است را ارائه می‌دهیم. هدف اصلی مقاله طراحی لایه‌های انتشار سبک‌وزن برای اولیه‌های رمزنگاری با پیاده‌سازی در سخت‌افزار است. معیار سنجش نیز بر اساس تعداد XORهای لازم برای پیاده‌سازی در نظر گرفته شده است. در ابتدا، شرایط لازم و کافی برای MDS بودن ماتریس‌هایی که از حاصل‌ضرب ماتریس‌های باینری و ماتریس‌های نظیر sigma-LFSRها حاصل می‌شوند را به دست آورده و اثبات می‌کنیم هزینه پیاده‌سازی این ماتریس‌های MDS برابر XOR است. سپس بر اساس تجربه حاصل از بررسی ماتریس‌های مذکور، فضای جستجو را گسترش می‌دهیم و خانواده‌هایی از ماتریس‌های MDS سبک‌وزن از مرتبه ۴ با هزینه‌های پیاده‌سازی و XOR ارائه می‌دهیم. هزینه پیاده‌سازی سبک‌وزن‌ترین ماتریس‌های MDS از مرتبه ۴ که در این مقاله ارائه شده‌اند با هزینه پیاده‌سازی سبک‌وزن‌ترین ماتریس MDS موجود برابری می‌کند.

واژه‌های کلیدی: لایه انتشار، عدد شاخه‌ای، اولیه‌های رمزنگاری سبک‌وزن، ماتریس MDS، ماتریس همراه.

The ISC Int'l Journal of Information Security
ISeCure

January 2019, Volume 11, Number 1 (p. 90)
http://www.isecure-journal.org

Persian Abstract

پیاده‌سازی طراحی به‌صورت امن بر بستر FPGA با استفاده از پر کردن فضاهای خالی

منصوره لباف‌نیا[1] و رقیه سیدی[2]

[1]دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، اصفهان، ایران
[2]پژوهشکده ICT، مرکز تحقیقات مخابرات ایران، تهران، ایران

امروزه حملات گوناگونی بر بستر FPGA اتفاق می‌افتد. از آنجا که FPGAها در کاربردهای مختلفی مانند IoT استفاده می‌شوند، امنیت آن‌ها مورد توجه قرار گرفته است. یکی از انواع مهم حملات تروجان‌های سخت‌افزاری است که این تروجان‌ها در فضاهای خالی بستر سخت‌افزاری درج می‌شوند. در این مقاله به ارائه روشی می‌پردازیم که در آن فضای خالی روی FPGA را به نحو مؤثری پر می‌کنیم به طوری که فضایی برای درج تروجان وجود نداشته باشد. برای این منظور از ساختارهای شیفت رجیستر و زنجیره گیت استفاده می‌کنیم. نتایج شبیه‌سازی روی بنچمارک IWLS نشان می‌دهد روش ارائه‌شده علاوه براینکه سربار مصرف توان ندارد، سایر پارامترها مانند کارایی و تأخیر در طراحی اصلی با امن کردن بستر سخت‌افزاری، دستخوش تغییر نخواهند شد.

واژه‌های کلیدی: FPGA، امنیت، نقطه کنترل پذیر، نقطه مشاهده پذیر، تروجان های سخت افزاری.

The ISC Int'l Journal of Information Security
ISeCure

January 2019, Volume 11, Number 1 (p. 91)
http://www.isecure-journal.org

Persian Abstract

حمله دو بخشی به رمزهای قالبی LBlock و Twine-80 با پیچیدگی داده عملی

سیاوش احمدی[۱]، زهرا احمدیان[۲]، جواد مهاجری[۱] و محمدرضا عارف[۱]

[۱]دانشگاه صنعتی شریف، تهران، ایران
[۲]دانشگاه شهید بهشتی، تهران، ایران

در حمله دوبخشی، استفاده از دوبخشی کوتاه‌تر معمولا منجر به کاهش پیچیدگی داده می‌شود، اما در عین حال پیچیدگی محاسباتی را افزایش می‌دهد. با استفاده از روش حذف اولیه در قسمت تطبیق جزئی حمله دوبخشی می‌توان این محاسبات را مقداری جزئی کاهش داد. در مقاله حاضر، با استفاده از این روش، اما به جای کاهش جزئی پیچیدگی محاسباتی، مقدار این پیچیدگی را ثابت نگه داشته‌ایم و پیچیدگی داده را به بهره‌گیری از دوبخشی کوچکتر، به میزان قابل توجه کم کرده‌ایم. با این رویکرد، رمز LBlock را در دو حالت معمولی و با فرانمای کلید اصلاح‌شده (که برای مقاومت در برابر حمله دوبخشی طراحی شده است)، هر دو با پیچیدگی داده 2^{12} تحلیل کرده‌ایم. در مورد LBlock معمولی، بهترین حمله قبلی دارای پیچیدگی داده 2^{52} بوده و در مورد LBlock با فرانمای کلید اصلاح‌شده، تا کنون حمله دور کاملی ارائه نشده بود. اگرچه پراکنش کم الگوریتم رمز LBlock موجب آسیب‌پذیری آن در برابر حمله دوبخشی صرف نظر فرانمای کلید آن می‌شود، اما به منظور تقویت بیشتر LBlock در برابر حمله دوبخشی، فرانمای کلید جدیدی نیز برای آن پیشنهاد کرده‌ایم. ضمنا، با استفاده از این روش، Twine-80 را نیز با پیچیدگی داده 2^{12} تحلیل کرده‌ایم. برای Twine-80، کمترین پیچیدگی داده قبلی برابر 2^{60} بوده است. در تمامی حملات ارائه شده در این مقاله، پیچیدگی‌های محاسباتی نیز مقداری نسبت به سایر حملات موجود بهبود پیدا کرده‌اند.

واژه‌های کلیدی: رمزنگاری سبک، تحلیل دوبخشی، تطبیق جزئی، روش حذف اولیه.

The ISC Int'l Journal of Information Security
ISeCure

January 2019, Volume 11, Number 1 (p. 92)
http://www.isecure-journal.org

Persian Abstract

یک طرح SPHF و پروتکل PAKE براساس حلقه‌ها روی مشبکه‌های ایده‌آل

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

[۱]گروه ریاضی، دانشگاه گیلان، رشت، ایران

[۲]گروه مهندسی کامپیوتر، دانشگاه گیلان، رشت، ایران

توابع چکیده‌سازی تصویری هموار SPHF به عنوان الگوی خاصی از سامانه‌های اثبات هیچ - آگاهی، ابزارهای پایه‌ای برای ساخت بسیاری از طرح‌ها و پروتکل‌های کارا هستند. به عنوان یک کاربرد از SPHFها، پروتکل تبادل کلید احراز اصالت شده مبتنی بر کلمه عبور PAKE یک حوزه تحقیقاتی در سال‌های اخیر شده است. در سال ۲۰۰۹ میلادی، Katz و Vaikuntanathan اولین SPHF مبتنی بر مشبکه‌ها را براساس مسئله LWE ارائه دادند. در این مقاله، یک خانواده از توابع چکیده‌سازی تصویری هموار کارا و مبتنی بر حلقه‌ها Ring-SPHF را براساس سامانه رمزنگاری طرح دوگان و مسئله Ring-LWE پیشنهاد داده می‌شود. به علاوه، براساس Ring-LWE پیشنهادی، یک پروتکل تبادل کلید احراز اصالت شده مبتنی بر کلمه عبور کارا Ring-PAKE روی حلقه‌ها ارائه می‌شود که امنیت آن وابسته به فرضیات مسائل مشبکه‌های ایده‌آل است.

واژه‌های کلیدی: رمزنگاری مشبکه-مبنا، Ring-LWE، CTRU، SPHF، PAKE.