The ISC Int'l Journal of Information Security
ISeCure

July 2013, Volume 5, Number 2 (p. 227)
http://www.isecure-journal.org

Persian Abstract

یک مدل کنترل دسترسی مبتنی بر نقش و آگاه از معنا برای محیط‌های محاسباتی فراگیر

سید احمد جوادی[1] و مرتضی امینی[1]

[1]آزمایشگاه امنیت داده و شبکه، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران

کنترل دسترسی در محیط‌های پویایی هم‌چون محیط‌های محاسباتی فراگیر یک فرآیند بسیار پیچیده بوده و نیازمندی‌های جدیدی را شامل می‌گردد. از یک طرف می‌بایست از اطلاعات زمینه‌ای در فرایند کنترل دسترسی استفاده گردد و از طرف دیگر، امکان استخراج اطلاعات زمینه‌ای مورد نیاز به صورت کامل و درست در همه زمان‌ها و مکان‌ها وجود ندارد. از این رو، یک مدل کنترل دسترسی مناسب برای محیط‌های فراگیر نه تنها باید مبتنی بر اطلاعات زمینه‌ای باشد بلکه باید بتواند راه‌کاری برای مقابله با چالش اطلاعات ناتمام ارائه دهد. علاوه بر این، به دلیل گستردگی و ناهمگونی منابع و کاربران در محیط‌های فراگیر، پشتیبانی از خط‌مشی‌های پیش‌فرض و استثناء یک نیازمندی بسیار مهم برای یک مدل کنترل دسترسی است. این مقاله یک مدل کنترل دسترسی مبتنی بر نقش و آگاه از مبنا را ارائه می‌کند که در آن از منطق $MKNF^+$ استفاده شده است و قادر است نیازمندی‌های مذکور را برآورده سازد. اصلی‌ترین نوآوری این مقاله تعریف یک هستان‌شناسی برای اطلاعات زمینه‌ای و در کنار آن استفاده از قواعد منطقی موجود در $MKNF^+$ به منظور تعریف خط‌مشی‌های فعال‌سازی نقش و تخصیص مجوز آگاه از زمینه است. تقسیم خط‌مشی‌های فعال‌سازی نقش و تخصیص مجوز به سه لایه مجزا و استفاده از محمول‌های انتزاعی و عینی نه تنها موجبات قابلیت انعطاف و مدیریت‌پذیری بیشتر خط‌مشی‌های امنیتی را فراهم ساخته بلکه امکان تعریف خط‌مشی‌های پیش‌فرض و استثناء را نیز فراهم می‌سازد. قابلیت بیان مدل پیشنهادی در قالب یک مطالعه موردی تشریح شده است.

واژه‌های کلیدی: کنترل دسترسی، منطق غیریکنوا، محیط محاسباتی فراگیر، آگاه از زمینه.

The ISC Int'l Journal of Information Security
ISeCure

July 2013, Volume 5, Number 2 (p. 228)
http://www.isecure-journal.org

Persian Abstract

مدلی محاسباتی و قضیه همگرایی برای انتشار شایعه در شبکه‌های اجتماعی

مسعود آموزگار[1] و رسول رمضانیان[1]

[1]آزمایشگاه سیستم های چندعاملی دانشکده علوم ریاضی دانشگاه صنعتی شریف، تهران، ایران

انتشار شایعه‌ها که معمولا گزاره‌هایی با منشا نامشخص و غیر معتبر هستند، می‌تواند امنیت هر جامعه‌ای را تهدید کند، به همین دلیل کنترل آن‌ها برای سازمان‌های درگیر با امنیت ملی هر کشوری اهمیت بسزایی دارد. لذا تشخیص عوامل موثر در انتشار شایعه‌ها در کنترل و یا توقف آن‌ها نقش بسزایی ایفا می‌کند. در این مقاله ابتدا مدلی محاسباتی شامل مولفه‌های مهم یک شایعه و هم‌چنین چگونگی انتشار آن در یک جامعه ارائه شده است. سپس در ادامه پژوهش، با تمرکز بر ارتباط بین همگن بودن باورهای اعضای جامعه و همگرایی شایعه انتشار یافته، با استناد به شبیه‌سازی‌ها و مدل محاسباتی نشان داده شده است که همگن بودن باورهای افراد یک جامعه شرطی لازم برای همگرایی شایعه‌ی منتشر شده در آن جامعه است.

واژه‌های کلیدی: انتشار اطلاعات، شبیه‌سازی پدیده‌های اجتماعی، مدلسازی عامل‌گرا.

The ISC Int'l Journal of Information Security
ISeCure

July 2013, Volume 5, Number 2 (p. 229)
http://www.isecure-journal.org

Persian Abstract

مدلی برای اعتماد گروه محور

منصوره اژه‌ای [1] و بهروز ترک لادانی [1]

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

امروزه با توسعه فضاهای مجازی از قبیل شبکه‌های اجتماعی و سازمان‌های مجازی، مدل‌سازی، محاسبه، و مدیریت اعتماد بسیار حائز اهمیت شده است. آسان‌ترین نمونه اعتمادسازی از طریق تعامل مستمر با افرادی است که به مدت طولانی آن‌ها را می‌شناسیم. مشکل اصلی اعتمادی که از تجربه‌ی شخصی افراد ایجاد می‌شود، محدود بودن قلمرو آن است. همچنین هر دو طرف رابطه‌ی اعتماد با مشکلات بزرگ جمع‌آوری اطلاعات و تشکیل باورهای معقول قابل اتکا رو به رو هستند. تکیه بر گروه‌ها علاوه بر اینکه مدلی طبیعی برای بیان روابط علی و معلولی و ماهیت اعتماد به ویژه در محیط‌های مبتنی بر تعامل مجموعه‌هایی از افراد (مانند شبکه های اجتماعی) است، راهی برای غلبه برمشکلات فوق نیز به شمار می‌رود. به عبارتی گروه‌ها می‌توانند زمینه ساز اعتماد به افرادی باشند که هرگز با آن‌ها آشنایی نداشته ایم. مدل ارائه شده در این مقاله، با نظامهای مدیریت اعتماد حاضر تفاوت دارد و به اعتماد به عنوان یک مشخصه مشترک و جمعی در گروه کاربران اشاره دارد. در این مدل، از عضویت گروهی، به عنوان معیار قضاوت درباره رفتار احتمالی یک فرد و نحوه‌ی اعتماد به وی استفاده می‌شود. به این ترتیب، اعتماد بین نهادها از عضویت گروه‌های آن‌ها درک می‌شود. مدل‌سازی روش ارائه شده بر اساس متاگراف صورت گرفته است. متاگراف ابزاری ریاضی است که به کمک آن می‌توان رابطه‌ای جهت‌دار ما بین دو مجموعه از عناصر را تعریف نمود و در آن هر یال زوج مرتبی از دو مجموعه است. چنین مدلی امکان اعتمادسازی بین نهادهای ناشناس نسبت به یکدیگر را به راحتی و با حجم کمتر ارتباطی و محاسباتی فراهم می‌سازد. علاوه بر این، می‌توان این شیوه را برای اعتماد سازی در محیط‌های بزرگ به کار برد.

واژه‌های کلیدی: اعتماد، گروه، اعتماد گروهی ، متاگراف.

The ISC Int'l Journal of Information Security
ISeCure

July 2013, Volume 5, Number 2 (p. 230)
http://www.isecure-journal.org

Persian Abstract

پیش‌بینی میزان قابلیت اعتماد کاربران در شبکه‌های اجتماعی مبتنی بر وب به کمک متن کاوی

حسین محمد حسن زاده[1] و حمیدرضا شهریاری[1]

[1]دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی امیرکبیر، تهران، ایران

برای ایجاد یک رابطه‌ی قابل اطمینان در شبکه‌های اجتماعی، لازم است که کاربران برآوردی از میزان قابلیت اعتماد کاربران دیگر داشته باشند. تا کنون برخی مکانیزم‌های اعتماد و شهرت، با استفاده از سیستم امتیازدهی مستقیم، توانسته‌اند میزان اعتماد کاربران به یکدیگر را محاسبه و ارزیابی کنند. هرچند، در برخی شبکه‌های اجتماعی مبتنی بر وب، هیچ سیستم رتبه‌دهی میان کاربران وجود ندارد و تنها یک رابطه دودویی (دوستی یا عدم دوستی) میان آن‌ها برقرار است. ازاین‌رو، روشی جدید لازم است که بدون نیاز به رتبه‌های اعلام شده از طرف کاربران توانایی استنتاج مقادیر اعتماد را در شبکه داشته باشد. این مقاله تلاش دارد تا مقادیر اعتماد میان کاربران را با استفاده از شباهت کاربران، و بدون نیاز به رتبه‌دهی مستقیم، پیش‌بینی نماید. رهیافت پیشنهادی، که بر پایه‌ی مطالعات روانشناسی اجتماعی بنا نهاده شده، شباهت کاربران به کمک تکنیک‌های متن‌کاوی از اطلاعات نمایه کاربری و متون اشتراکی کاربر استخراج می‌شود. بدین طریق و براساس نسبت‌های Ziegler، نشان داده شد که اعتماد کاربران به افراد مورد اعتمادشان بیش از ۵۰٪ بیشتر از شباهت ایشان به کل کاربران است. این یافته، فرض اولیه مقاله مبنی بر استنتاج اعتماد از شباهت زبانی کاربران را تأیید می‌کند. علاوه بر آن، به جهت ارزیابی کارآیی روش پیشنهادی، مقادیر پیش‌بینی شده با مقادیر واقعی جمع‌آوری شده از کاربران مقایسه شده است. در این مقایسه نشان داده شد که ارقام استنتاجی با دقت قابل قبولی (۶۱٪) با ارقام واقعی اعتماد مطابقت دارند. همچنین کارآیی استفاده از زمینه در رهیافت پیشنهادی بررسی شده است. به‌کارگیری زمینه و تفکیک متون به چهار زمینه‌ی علمی، هنری فرهنگی، سیاسی اقتصادی و ورزشی، دقت روش را تا ۷۲٪ بالا برد. شایان ذکر است که علاوه بر کاربرد رهیافت پیشنهادی در شبکه‌های اجتماعی، این تکنیک را می‌توان برای صحت‌سنجی مقادیر اعتمادی اعلام شده از طرف کاربران در هر مکانیزم اعتماد به کار گرفت، و از تهدیدات احتمالی پیشگیری نمود.

واژه‌های کلیدی: اعتماد، شهرت، شبکه‌ی اجتماعی، شباهت کاربری، اندازه‌گیری شباهت، متن‌کاوی.

The ISC Int'l Journal of Information Security
ISeCure

July 2013, Volume 5, Number 2 (p. 231)
http://www.isecure-journal.org

Persian Abstract

امضا با یک (/چند) ارزیاب محدود با قابلیت تبدیل به ارزیابان نامحدود: ساختارهای جدید و کاربردها

سپیده آویژه[1] ، مریم رجب زاده عصار[1] و محمود سلماسی‌زاده[2]

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

[2]پژوهشکده الکترونیک، دانشگاه صنعتی شریف، تهران، ایران

امضا با یک (/چند) ارزیاب محدود با قابلیت تبدیل به ارزیابان نامحدود (CL(M)VS) امکان وارسی امضا را به صورت کنترل شده فراهم کرده و حریم خصوصی امضاکننده را حفظ می‌کند. به علاوه، یک (/چند) ارزیاب محدود می تواند امضا را در موارد ضروری به نهاد سومی تخصیص دهد یا آن را برای ارزیابی نامحدود به یک امضای معمولی تبدیل کند. در این مقاله، ابتدا یک ساختارعام برای امضای CLVS معرفی می شود که تمامی طرح های ارائه شده پیش از آن در این ساختار می‌گنجند. سپس، این الگو گسترش داده شده، دو ساختارعام برای امضای CLVS با چند ارزیاب محدود (CLMVS) طراحی می‌شود که در هر دو این ساختارها فقط یک امضا برای همه ارزیاب‌ها تولید می‌شود و از این جهت کارا هستند. در ساختار اول هر یک از ارزیابان محدود می‌توانند به تنهایی امضا را وارسی کنند و در ساختار دوم همکاری ارزیابان محدود برای وارسی امضا الزامی است. همچنین در این مقاله، بر مبنای ساختار عام دوم، اولین طرح امضای CLMVS مبتنی بر زوج های دوخطی و دارای ویژگی اثبات محکم طراحی می‌شود که امنیت آن در مدل استاندارد قابل اثبات است. در انتها، با استفاده از طرح CLMVS پیشنهادی با یک ارزیاب محدود (CLVS) ، یک پروتکل رأی گیری الکترونیکی جدید طراحی می‌گردد.

واژه‌های کلیدی: امضا با یک (یا چند) ارزیاب محدود با قابلیت تبدیل به ارزیابان نامحدود (CL(M)VS)، امضا با یک (/چند) ارزیاب معین فراگیر (UD(M)VS) ، زوج های دوخطی، رأی گیری الکترونیکی، احرازاصالت حاشاپذیر.

The ISC Int'l Journal of Information Security
ISeCure

January 2013, Volume 5, Number 2 (p. 232)
http://www.isecure-journal.org

Persian Abstract

STRL: یک الگوریتم تئوری خطر نوین، بر پایه الگوریتم TLR ساخت یافته

رضا عزمی[1] و بشری پیشگو[1]

[1]آزمایشگاه امنیت سیستم‌عامل، دانشگاه الزهرا (س)، تهران، ایران

تا کنون از رویکرد سیستم‌های ایمنی مصنوعی، در زمینه امنیت کامپیوتری و به خصوص سیستم‌های تشخیص نفوذ استفاده گردیده است. به طور کلی، تشخیص نفوذ بر پایه‌ی سیستم‌های ایمنی مصنوعی به دو دسته‌ی عمده تقسیم می‌گردد. نسل اول این الگوریتم‌ها، تنها از عکس‌العمل‌های سیستم ایمنی انطباقی الهام می‌گیرند، اما در نسل دوم که تئوری خطر نامیده می‌شود، همزمان بر عکس‌العمل‌های سیستم‌های ایمنی ذاتی و انطباقی تمرکز می‌نمایند تا بتوانند سیستم ایمنی انسانی را بهتر مدل کنند. دو الگوریتم TLR و DCA از الگوریتم‌های مطرح در این حوزه می‌باشند که هر دوی آن‌ها سعی می‌کنند تا آنتی ژن‌ها را از طریق شماره شناسایی یکتای آنها شناسایی نمایند. این دو الگوریتم به دلیل نادیده گرفتن ساختار آنتی‌ژن از دقت مناسبی برخوردار نمی‌باشند. در این مقاله، یک الگوریتم تئوری خطر جدید به نام STLR ارائه می‌گردد که نسخه‌ی توسعه یافته‌ی الگوریتم TLR می‌باشد و ضمن مدل‌سازی رفتار سیستم‌های ایمنی ذاتی و انطباقی، از ساختار آنتی‌ژن‌ها هم در جهت شناسایی رفتار نرمال و غیرنرمال بهره می‌گیرد. آزمایشات صورت گرفته در این زمینه نشان می‌دهند که الگوریتم STLR از طریق بهره‌گیری از جنبه‌های ساختاری آنتی‌ژن‌ها می‌تواند میزان دقت و نرخ تشخیص را افزایش دهد.

واژه‌های کلیدی: تشخیص ناهنجاری، تئوری خطر، الگوریتم TLR، الگوریتم STLR ، سیستم‌های ایمنی مصنوعی.