هفتمین کنفرانس بین المللی انجمن رمز ایران
۲۴ و ۲۵ شهریورماه ۱۳۸۹، دانشگاه صنعتی خواجه نصیرالدین طوسی
!
انجمن رمزایران
دانشگاه صنعتی خواجه نصیرالدین طوسی

ARM: مدل رفع ناهنجاری در پایگاه قواعد دیوار آتش‌های توزیع‌شده

سید محمد مهدی قطبی[۱]، محمد رضا ذاکری‌نسب[۲]، رسول جلیلی[۳]

تهران، دانشگاه صنعتی مالک اشتر، گروه امنیت[۱]
ghotbi@ce.sharif.edu

تهران، دانشگاه صنعتی شریف، مرکز امنیت شبکه شریف[۲و۳]
{zakeri@ce, jalili@}sharif.edu

چکیده

هدف از ارائه مدل رفع ناهنجاری، افزایش قابلیت اطمینان و پایداری ابزارهای امنیتی شبکه و رفع آسیب‌پذیری ناشی از ناهنجاری‌های درون و میان پایگاه قواعد دیوارآتش‌های توزیع‌شده است. در این پژوهش علاوه بر ارائه یک دسته‌بندی جامع از ناهنجاری‌ها، مدل رفع ناهنجاری ARM جهت کشف، شناسایی نوع و رفع ناهنجاری موجود در پایگاه قواعد دیوارآتش‌های توزیع‌شده ارائه شده است. ARM با ارائه هستان‌شناسی خود موجب عدم وابستگی مدل به همبندی شبکه و قابلیت بکارگیری آن در محیط‌های ناهمگن می‌شود. ARM با صوری سازی مفهوم ناهنجاری و پشتیبانی منطق، ماشین قواعد استنتاج ناهنجاری را ارائه می‌دهد که باعث خودکارسازی استنتاج ناهنجاری‌ها و توسعه‌پذیری مدل می‌شود. ARM با دو رویکرد پیشگیرانه و اصلاحی به رفع ناهنجاری در پایگاه قواعد دیوار آتش‌های توزیع شده می‌پردازد. از ویژگی‌های دیگر ARM می‌توان به قابلیت بکارگیری در شبکه‌های سرعت‌بالا، سهولت استفاده برای مدیران امنیتی، تکامل در رفع ناهنجاری‌ها و امکان تولید خودکار پایگاه قواعد پس از رفع ناهنجاری‌های آن اشاره کرد.

واژه‌های کلیدی

ناهنجاری، صوری‌سازی، دیوارآتش‌های توزیع‌شده، آسیب‌پذیری، امنیت.

۱- مقدمه !

خط مشی امنیتی، توصیف سطح بالای نیازمندی‌های امنیتی یک سازمان است [۱]. مکانیزم امنیتی، ابزار یا رویه‌ای برای اعمال خط مشی امنیتی است [۱]. یکی از گام‌های مهم اعمال خط مشی امنیتی در هر شبکه استقرار دیوار آتش در آن شبکه است. طراحی و مدیریت پایگاه قواعد دیوار آتش‌ها خسته کننده، زمان بر و مستعد خطا است [۲]. با توجه به تعریف جیمز اندرسون [۳] از آسیب‌پذیری امنیتی، در حوزه دیوار آتش مسائل مختلفی نظیر رفع ناسازگاری و افزونگی پایگاه قواعد دیوار آتش و رفع عدم تطبیق بین خط مشی امنیتی و پایگاه قواعد مربوطه مطرح می‌شود. مدیریت درست این مسائل، کاهش آسیب‌پذیری این ابزار امنیتی را به همراه داشته و موجب افزایش کارایی و کارآمدی این گلوگاه شبکه‌ای می‌گردد. از جمله عوامل دخیل در بروز ناهنجاری که منجر به آسیب‌پذیری امنیتی می‌شود، می‌توان به تنوع تجهیزات شبکه و تولیدکنندگان، ضعف و نقص در تعریف قواعد، زبان سطح پایین دیوارآتش، اهمیت ترتیب قواعد، حجم بالای

قواعد، خطای انسانی و اعمال خط‌مشی توسط چند مدیر امنیتی نام برد [۴].

۲- کارهاي مرتبط

با بررسی زبان‌های کنترل دسترسی این نکته دریافت می‌شود که بین رسایی و پیچیدگی آنها رابطه عکس وجود دارد به طوری که زبان پیچیده‌تر رسایی کمتری دارد. در [۵-۷] مروری خوب بر زبان‌های کنترل دسترسی ارائه شده است. در [۸] برای افزایش شیوایی، زبانی عمومی برای بکارگیری در حوزه دیوار آتش ارائه شده است که به هیچ یک از زبان‌های سطح پایین دیوار آتش قابل تبدیل نیست.

برای تسهیل تولید پایگاه قواعد دیوار آتش، ابزارهایی گرافیکی نظیر فایروال بیلدر [۹] نیز ارائه شده که به دلیل پنهان ننمودن جزئیات سطح پایین بسیار پیچیده است. دیگر ایراد این ابزارها یک طرفه بودن آنها است که تنها قادرند خط مشی امنیتی را به پایگاه قواعد تبدیل کنند.

تعدادی از کارهای انجام شده زیرساختی صوری داشته که از این دسته می‌توان به روش‌های مبتنی بر تئوری نوع [۱۰]، مبتنی بر قواعد استنتاج [۱۱] و مبتنی بر ASP [۱۲] نام برد.

یکی از ویژگی‌های اصلی هر مدل، توانمندی در بازنمایش مفاهیم دیوار آتش نظیر استثنا و پوشش (mask) است که ناتوانی در این زمینه باعث به وجود آمدن نقص‌هایی در مدل و از بین رفتن خوانایی پایگاه قواعد برای مدیر امنیتی می‌شود. راهکار ارائه شده در [۱۳] فقط خط مشی در منطق مثبت را بیان می‌کند و بیان استثنا را پیچیده کرده که بزرگترین محدودیت ابزار فیرماتو محسوب می‌شود. [۱۴] نیز در بیان استثنا ناتوان است. زتینگ در [۱۵]، الشائر در [۱۶, ۱۷] و در کارهای [۱۸, ۱۹] بیان نکرده‌اند که از پوشش چگونه استفاده شده است.

در [۴, ۱۳, ۲۰] ابزاری برای تحلیل خودکار دیوار آتش ارائه شده که پیکربندی دیوار آتش را به صورت کلی بررسی کرده‌است. در [۲۱] رویکرد نرم‌افزاری توسعه مبتنی بر مدل (MBD) ارائه شده‌است. در [۲۰] با رویکردی غیر صوری با تولید پرسش‌های خودکار به تست پایگاه قواعد پرداخته‌شده‌است. در مقابل به کارهایی نظیر [۲۲] می‌توان اشاره نمود که با رویکردی مبتنی بر تست موردی به بررسی انطباق بین پایگاه قواعد و خط‌مشی مورد نظر پرداخته‌است. در کارهای [۱۳, ۲۳] تولید پرسش برای وارسی سازگاری به صورت دستی انجام می‌شود.

در [۱۶, ۱۷, ۲۴] استفاده از رویکردهای ناهمبسته‌سازی قواعد، موجب تغییرات زیاد در پایگاه قواعد اولیه و ناخوانا و حجیم نمودن آن می‌شود؛ در [۲۵] تلاش شده‌است با استفاده از OBDD با پیچیدگی زمانی نمایی بدون ناهمبسته‌سازی قواعد به رفع ناهنجاری‌ها پرداخته‌شود.

از معیارهای مقایسه روش‌ها، توسعه‌پذیری آنها است. در کارهای الشائر [۱۶, ۱۷, ۲۴, ۲۶] قواعد فقط با شش مؤلفه در نظر گرفته می‌شود که در صورت توسعه این الگوریتم‌ها با تعداد مؤلفه بیشتر، درخت حالت الگوریتم با انفجار فضای حالت مواجه می‌شود.

در [۲۱] برای مدل‌سازی پایگاه قواعد و تولید خودکار پایگاه قواعد هر دیوار آتش، یک مدل مستقل از پیاده‌سازی ارائه شده که از مجموعه زبان‌های دیوار آتش پشتیبانی می‌کند. در شبکه‌های سرعت‌بالا هر قاعده افزونه هزینه زیادی برای دیوار آتش ایجاد می‌کند و لذا کارهایی که در آنها از استثنا و پوشش پشتیبانی نشده، مناسب برای این حوزه نیستند.

اطمینان از اعمال صحیح و کامل خط مشی توسط دیوار آتش و حذف صحیح قواعد ناسازگار از پایگاه قواعد دیوار آتش، دو مثال از موارد بررسی تطبیق بین خط مشی و مکانیزم امنیتی است. در [۴] زبانی مجرد برای بازنمایش خط مشی ارائه شده‌است. همچنین در [۲۷] روشی مبتنی بر تئوری گراف و در [۲۸, ۲۹] یک روش مبتنی بر درخت تصمیم دودویی به همراه الگوریتم‌های تحلیلی مورد نیاز ارائه شده‌است.

۳- ارائه مدل ARM

در این بخش به معرفی ARM پرداخته می‌شود. بدین منظور در ابتدا به معرفی معماری ARM و سپس مفاهیم پایه تشکیل دهنده هستان‌شناسی آن پرداخته شده است.

۳-۱ معماری ARM

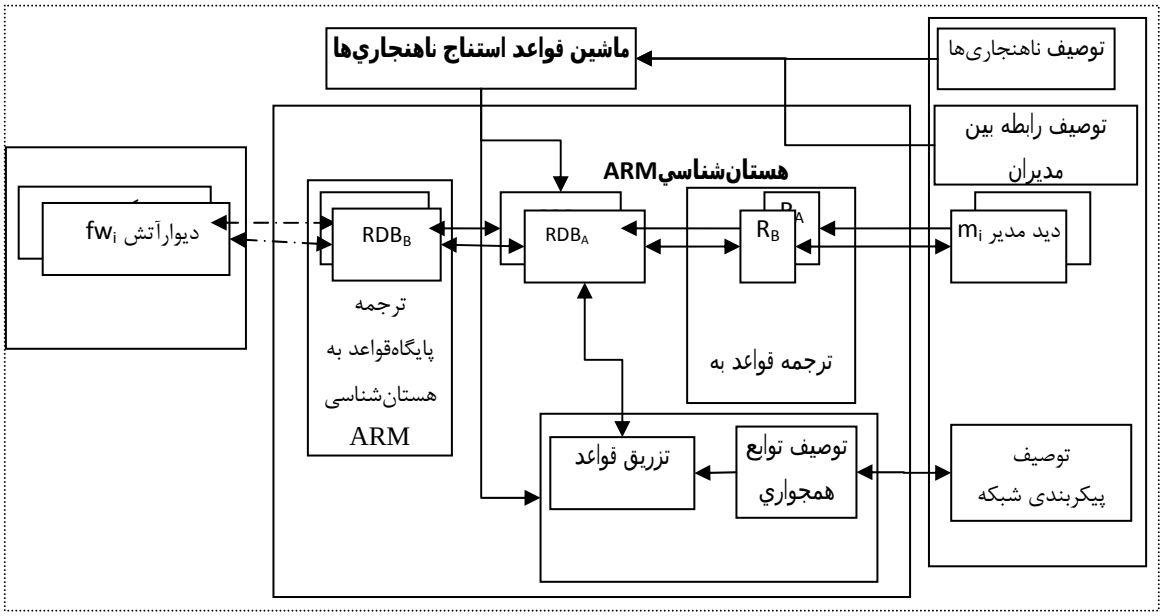
معماری ARM در شکل ۱ نشان داده‌شده‌است. این معماری از چهار بخش اصلی تشکیل شده است:

- واسط مدیران: از طریق این واسط ورود قسمتی از اطلاعات محیطی نظیر توصیف توپولوژی شبکه، معرفی و بیان رابطه مدیران و اعمال تغییر در دیوار آتش‌های تحت نظارت مدیران انجام می‌پذیرد.
- هستان‌شناسی: با ترکیب هستان‌شناسی دیوار آتش‌ها و اطلاعات زمینه‌ای شبکه، می‌توان ساختار داده‌ای مشخص برای هستان‌شناسی ARM تعریف کرد. با استفاده از این هستان‌شناسی علاوه بر نظم دادن به مفاهیم، امکان مقایسه پذیری مفاهیم برای استخراج ناهنجاری‌ها و بررسی سازگاری میان ابزارهای امنیتی ناهمگن فراهم می‌شود.
- واسط دیوار آتش: این بخش از معماری ARM نگاشتی از هستان‌شناسی هر دیوار آتش به هستان‌شناسی ARM فراهم می‌کند. همچنین این واسط قادر به بازگردانی قواعد از هستان‌شناسی ARM به هر دیوار آتش است.

- ماشین قواعد استنتاج ناهنجاری: این ماشین با استنتاج روی داده‌های هستان‌شناسی، وظیفه استخراج ناهنجاری‌ها را به عهده دارد.

۳-۲ مفاهیم موجود در مدل ARM

با توجه به مفاهیم موجود در ARM یک هستان‌شناسی بر اساس اطلاعات زمینه‌ای شبکه دارای دیوار آتش‌های توزیع‌شده شکل می‌گیرد. در این بخش این مفاهیم معرفی می‌شوند.



شکل۱. معماری ARM: در شکل بالا مؤلفه‌های ARM و نحوه تعامل این مؤلفه‌ها نشان داده شده است.

۳-۲-۱ توصیف صوری قواعد

قواعد در هستان‌شناسی ARM با r_i نشان داده شده و به صورت رابطه (۳-۱) تعریف می‌شوند. هر قاعده با مشخصه محتوایی قاعده (Cnt)، توسط مدیر (m) در دیوار آتش (fw) و در ترتیب (or) قرار می‌گیرد.

طبق رابطه (۳-۲) مشخصه محتوایی قاعده از دو بخش شرط قاعده (C) و تصمیم قاعده (A) تشکیل شده‌است. طبق رابطه (۳-۳)، ARM برای تصمیم قاعده دو حالت پذیرش و رد در نظر می‌گیرد و آن را با یک بیت نشان می‌دهد.

بخش شرط هر قاعده با پنج مؤلفه تعریف می‌شود. طبق رابطه (۳-۴) این مؤلفه‌ها عبارتند از: آدرس مبدأ (SIP) و آدرس مقصد (DIP) هرکدام در چهار بایت، درگاه مبدأ (SP) و درگاه مقصد (DP) هرکدام در دو بایت و نوع پروتکل (Pr) در یک بیت.

$$r_i = \{m, fw, or, Cnt\} \quad (۳-۱)$$

$$cnt = \{C, A\} \quad (۳-۲)$$

$$A = b_0 \quad (۳-۳)$$

$$Cnt = \{SIP, DIP, SP, DP, Pr\} \quad (۳-۴)$$

$$DIP, SIP = B_1, B_2, B_3, B_4 \quad (۳-۵)$$

$$DP, SP = B_1, B_2 \quad (۳-۶)$$

$$Pr = b_0 \quad (۳-۷)$$

۳-۲-۲ توصیف صوری دیوارآتش

طبق رابطه دیوار آتش به صورت یک پایگاه قواعد (RDB) بیان می‌شود که شامل مجموعه‌ای از قواعد (S_r) و مجموعه روابط دوتایی بین قواعد (R_r) است. R_r یک رابطه ترتیب‌کامل و S_r یک مجموعه کاملاً مرتب است.

$$fw = RDB(R_r, S_r) \quad (۳-۸)$$

$$S_r = \{r_1, r_2, r_3, ..., r_n\} \quad (۳-۹)$$

۳-۲-۳ توصیف صوری مدیران امنیتی

برای رفع ناهنجاری‌های میان‌خط مشیی، رابطه بین مدیران به صورت (۳-۱۰) تعریف می‌شود. R_M یک رابطه ترتیب جزئی (۳-۱۲) روی مجموعه مدیران (۳-۱۱) است و دارای خاصیت‌های انعکاسی، بازتابی و تراگذری است. قاعده r_i اولویت بالاتری نسبت به قاعده r_j دارد اگر رابطه (۳-۱۳) برقرار باشد. در این رابطه تابع $\xi()$ مدیر ایجاد کننده قاعده را باز می‌گرداند.

$$Poset(R_M, S_M) \quad (۳-۱۰)$$

$$S_M = \{m_1, m_2, m_3, ..., m_n\} \quad (۳-۱۱)$$

$$R_M \subset S_M \times S_M \quad (۳-۱۲)$$

$$prv(r_i, r_j) = \forall r_i, r_j (\xi(r_i), \xi(r_j)) \in R_M \quad (۳-۱۳)$$

۳-۲-۴ توصیف صوری شبکه

وضعیت دامنه‌ها و مؤلفه‌های امنیتی را در محیط توزیع‌شده می‌توان به صورت یک گراف همجواری نشان داد (۳-۱۴).

$$\begin{aligned} &Gh = \{V, L\} \\ &V = \{v \mid v \in com \vee v \in Z\} \\ &L = \{l_1, l_2, l_3, ..., l_n\} \\ &l_i = \{(v_i, v_j) \mid v_i \ related\ to\ v_j\} \\ &Z = \{z_1, z_2, z_3, ..., z_n\} \\ &com = \{Fw_i, router\} \end{aligned} \quad (۱۴-۳)$$

در این گراف هر گره (v) یک دامنه (Z) و یا یک مؤلفه امنیتی (com) است که وظایف دیوارآتش را نیز بر عهده دارد. ترکیب پایگاه قواعد دیوار آتش‌های سیستم‌باز (Fw_o) یا سیستم‌بسته (Fw_c) میان دو دامنه را می‌توان به صورت روابط عطفی ⊗(۳-۱۶) و فصلی ⊕ (۳-۱۷) بیان نمود.

$$com = Fw_o \mid Fw_c \quad (۱۵-۳)$$

$$\varphi = com \mid com \otimes \varphi \quad (۱۶-۳)$$

$$\phi = \varphi \mid \varphi \oplus \phi \quad (۱۷-۳)$$

دسترسی پذیری دو دامنه در (۳-۱۸) تعریف شده‌است. دو دامنه را دسترسی پذیر گویند اگر دسترسی‌های (λ_{z_i,z_j}) بین دو دامنه تهی نباشد. ترکیب فصلی تمام اعضای مجموعه λ_{z_i,z_j} تابع همجواری میان‌دامنه‌ای Ω_{z_i,z_j} نامیده می‌شوند (۳-۱۹). تابع همجواری میان‌دامنه‌ای Ω_{z_i,z_j} تمام مکانیزم‌های اعمال کننده خط مشی میان دو دامنه z_i و z_j را در هستان‌شناسی ARM بیان می‌کند.

$$\lambda_{z_i,z_j} = \{\phi \mid \phi = z_i . \bigotimes_{c_k \in Com} c_k . z_j\} \quad (۱۸-۳)$$

$$\Omega_{z_i,z_j} = \{\varphi = \bigoplus_{\forall \phi_k \in \lambda_k = z_i . \phi_k . z_j} \phi_k\} \quad (۱۹-۳)$$

۳-۲-۵ ترجمه قواعد به هستان‌شناسی ARM

دیوار آتش، دامنه‌ها را در دو دسته داخلی $Z_{fw_i}^{in}$ (که بر آنها نظارت می‌کند) و خارجی $Z_{fw_i}^{out}$ قرار می‌دهد. در رابطه (۳-۲۰) تابع $S(fw, D_i)$ تمام دامنه‌های D_j را که دیوار آتش fw در Ω_{D_i,D_j} نقش دارد را مشخص می‌کند.

$$S(fw, D_i) = \{D_j \mid fw \in \Omega_{D_i,D_j}\} \quad (۲۰-۳)$$

با استفاده از تعریف بالا مفاهیم محلی به مفاهیم سراسری برای ورود قواعد به هستان‌شناسی ARM ترجمه می‌شوند. هر آدرس مقادیر مختلفی می‌گیرد (۳-۲۱) که این مقادیر طبق روابط (۳-۲۲) تا (۳-۲۴) به مفاهیم هستان‌شناسی ترجمه می‌شود. رابطه (۳-۲۵) یک مثال از این ترجمه است. $D(ip)$ دامنه‌ای که ip به آن تعلق دارد را باز می‌گرداند.

$$DIP, SIP = \{sip \mid d_i \mid any_{in} \mid any_{out}\} \quad (۲۱-۳)$$

$$d_i, DIP, SIP >> Z_i \quad (۲۲-۳)$$

$$any_{in} >> Z_{fw_i}^{in} \quad (۲۳-۳)$$

$$any_{out} >> any_{out} \quad (۲۴-۳)$$

$$r_a = sip\, 2any > D(sip) 2S(fw_i, D(sip)) \quad (۲۵-۳)$$

۳-۲-۶ نگاشت قواعد به هستان‌شناسی ARM

برای نگاشت قواعد به هستان‌شناسی ARM توصیفی صوری به نام تزریق قواعد ارائه می‌شود. دو عملگر ضرب (ϑ) یکی برای قواعد عدم دسترسی (c) حقیقی (r_i^c) و مجازی ($r_i^{c\prime}$) در شبکه‌های سری ((۳-۲۶) و (۳-۲۷)) و موازی ((۳-۲۸) و (۳-۲۹)) و دیگری (τ) برای تزریق قواعد دسترسی (o) r_i^o در شبکه‌های سری (۳-۳۰) و موازی (۳-۳۱) تعریف شده‌است که با استفاده از این عملگرها قواعد در توابع میان‌دامنه‌ای تزریق می‌شود. قواعد مجازی برای اعمال تأثیر یک قاعده عدم دسترسی در دیوار آتش‌هایی که قاعده حقیقی حضور ندارد ولی تأثیرگذار است، به کار گرفته می‌شود و معمولاً بیش از یک حالت ω_i برای خروجی ضرب ایجاد می‌کند.

$$r_i^c \vartheta(\varphi \otimes \phi) = \begin{cases} \omega_1 = (r_i^c \vartheta\varphi) \wedge (r_i^{c\prime} \vartheta\phi) \\ \omega_2 = (r_i^{c\prime} \vartheta\varphi) \wedge (r_i^c \vartheta\phi) \end{cases} \quad (۲۶-۳)$$

$$r_i^{c\prime} \vartheta(\varphi \otimes \phi) = (r_i^{c\prime} \vartheta\varphi) \wedge (r_i^{c\prime} \vartheta\phi) \quad (۲۷-۳)$$

$$r_i^c \vartheta(\varphi \oplus \phi) = (r_i^c \vartheta\varphi) \wedge (r_i^c \vartheta\phi) \quad (۲۸-۳)$$

$$r_i^{c\prime} \vartheta(\varphi \oplus \phi) = (r_i^{c\prime} \vartheta\varphi) \wedge (r_i^{c\prime} \vartheta\phi) \quad (۲۹-۳)$$

$$r_i^o \tau(\varphi \otimes \phi) = (r_i^o \tau\varphi) \wedge (r_i^o \tau\phi) \quad (۳۰-۳)$$

$$r_i^o \tau(\varphi \oplus \phi) = (r_i^o \tau\varphi) \wedge (r_i^o \tau\phi) \quad (۳۱-۳)$$

۳-۲-۷ گراف ناهنجاری

وظیفه گراف ناهنجاری (AG) ایجاد ارتباط میان قواعد ناهنجار است. این گراف در دو دسته گراف ناهنجاری‌های افزونگی (AG_{Red}) برای قواعد با تصمیم یکسان و گراف ناهنجاری‌های تعارض (AG_{Con}) برای قواعد با تصمیم متفاوت قرار می‌گیرد. مزیت استفاده از این گراف افزایش دقت تصمیم‌گیری در بررسی ناهنجاری چندگانه و کاهش پیچیدگی زمانی در رفع ناهنجاری است. در هر گراف ناهنجاری، هر گره (v) شامل قاعده (r_i)، وضعیت قاعده (St)، و نوع ناهنجاری (At) است (۳-۳۳). St از دو بخش حالت ε و صورت γ تشکیل شده‌است (۳-۳۷). یال‌های گراف گره‌های همبسته را به هم متصل می‌کنند (۳-۳۵).

$$AG = \{V, L, T\}$$

$$V = \{v_1, v_2, v_3, ...v_n\} \quad (۳۲-۳)$$

$$v_i = \{r_i, St, Pm, At\} \quad (۳۳-۳)$$

$$L = \{l_1, l_2, l_3, ..., l_n\} \quad (۳۴-۳)$$

$$l_i = \{(v_i, v_j) \mid v_i.cnt.c \rightarrow v_j.cnt.c\} \quad (۳۵-۳)$$

$$T = \{AG_{\mathrm{Red}}, AG_{Con}\} \quad (۳۶-۳)$$

$$St = \{\varepsilon, \gamma\} \quad (۳۷-۳)$$

$$\gamma = b_0 \quad (۳۸-۳)$$

ε حالت هر قاعده در دیوار آتش است (۳-۳۷). اگر قاعده‌ای توسط مدیر امنیتی اعمال و در رفع یکی از ناهنجاری‌ها از پایگاه قواعد حذف شده ولی با خط مشی خواسته شده تعارض نداشته باشد، در هستان‌شناسی ARM به صورت غیر فعال باقی می‌ماند که به اصطلاح به وضعیت خاموش رفته است. در صورت رفع عامل ناهنجاری، قاعده به پایگاه قواعد دیوار آتش بازگشته و وضعیت آن روشن تلقی می‌شود. با توجه به مفهوم تزریق قواعد به توابع همجواری، برای هر گره دو حالت حقیقی و مجازی متصور می‌شود (γ).

۴- دسته‌بندی ناهنجاری‌ها

در [۳۰] با استفاده از تئوری مجموعه‌ها، ناهنجاری‌ها به چهار دسته افزونگی، همبستگی، سایه و تعمیم تقسیم شده و ناهنجاری‌های عام در نظر گرفته نشده‌اند. در [۱۱] با توصیف ناقص پیکربندی شبکه، برای دیوار آتش‌های توزیع‌شده دسته‌بندی متفاوتی ارائه شده‌است. در مدل ARM با رویکردی صوری و با استفاده از منطق گزاره‌ها، دسته‌بندی جامعی از ناهنجاری‌ها با توجه به اهمیت، حوزه خط مشی، حوزه مکانی، تعداد قواعد دخیل، اثر و نوع ناهنجاری ارائه شده و تمام نواقص دسته‌بندی‌های پیشین پوشش داده‌شده‌است.

اهمیت ناهنجاری: از نظر اهمیت، ناهنجاری‌های دیوار آتش در دو دسته مهم که ناشی از خطای انسانی و نامهم نظیر قواعد استثنا قرار می‌گیرند.

حوزه خط مشی: خط مشی امنیتی می‌تواند از ترکیب چند زیر خط مشی ایجاد شود و به علت ایجاد مستقل زیر خط مشی‌ها امکان بروز ناهنجاری وجود دارد. بر این اساس ناهنجاری‌ها در دو دسته درون‌خط مشیی و میان‌خط مشیی قرار می‌گیرند.

حوزه مکانی: از نظر حوزه مکانی، ناهنجاری بین قواعد r_a و r_i درون‌پایگاهی (A_i) است، اگر r_i در پایگاه قواعد دیوار آتش r_a باشد، در غیر این صورت ناهنجاری میان‌پایگاهی (EA_i) رخ داده است (۴-۱). تابع β برابر بودن دیوار آتش دو قاعده را بررسی می‌کند.

$$f_9 = \bigwedge_{i=1}^{k} \neg(\beta(r_i, r_a)) \quad (۱-۴)$$

تعداد قواعد دخیل در ناهنجاری: ناهنجاری‌ها طبق روابط (۲-۴) و (۳-۴) از نظر تعداد قواعد دخیل، در دو دسته ساده و عام قرار می‌گیرند. در ناهنجاری ساده قاعده r_i با شماره ترتیب کمتر موجب ناهنجاری برای قاعده r_a می‌شود ولی در ناهنجاری عام چند قاعده ($k>1$) موجب ناهنجاری برای قاعده r_a می‌شوند. تابع σ بیشتر بودن شماره ترتیب r_a را بررسی می‌کند.

$$f_0 = r_1, r_2, r_3, ..., r_k, r_a \quad (۲-۴)$$

$$f_1 = \bigwedge_{i=1}^{k} \sigma(r_a, r_i) \quad (۳-۴)$$

میزان تأثیر ناهنجاری: ناهنجاری‌ها بر اساس میزان اثر گذاری بر روی قواعد، به دو دسته ناهنجاری کامل و جزئی تقسیم بندی می‌شوند. در صورتی که قاعده r_i با شماره ترتیب کمتر بر تمام ترافیک منطبق بر r_a تطبیق داشته باشد ناهنجاری کامل اتفاق می‌افتد و عملاً قاعده r_a بر مکانیزم اعمالی اثر نمی‌گذارد. در ناهنجاری جزئی تنها بخشی از قاعده r_a دچار ناهنجاری شده و در دو دسته سایه و مرتبط قرار می‌گیرد. طبق گزاره در دسته جزئی سایه، r_a با کل ترافیک منطبق بر قاعده r_i تطابق دارد (استثنا روی قواعد). در ناهنجاری جزئی مرتبط، بخشی از قاعده r_a که دچار ناهنجاری شده بر تمام ترافیک منطبق بر قاعده r_i تطبیق ندارد.

$$f_4 = (Cn(r_a) \rightarrow \bigwedge_{i=1}^{k} Cn(r_i)) \quad (۴-۴)$$

$$f_5 = (\bigwedge_{i=1}^{k} Cn(r_i) \rightarrow Cn(r_a)) \quad (۵-۴)$$

$$f_6 = ((Cn(r_a)(x) \rightarrow \bigwedge_{i=1}^{k} Cn(r_i)(y_i)) \wedge (\bigwedge_{i=1}^{k} Cn(r_i)(x_i) \rightarrow Cn(r_a)(y))) \quad (۶-۴)$$

ناهنجاری قفل‌شدگی: در پدیده قفل‌شدگی قاعده r_i با شماره ترتیب کمتر از r_a و اعمال تصمیمی متضاد با آن و اشتراک در ترافیک تطبیقی، باعث عدم اعمال کامل تصمیم r_a می‌شود (۴-۷). تابع Ac شرط قاعده را بر می‌گرداند.

$$f_2 = \bigwedge_{i=1}^{k} \neg(Ac(r_i) \leftrightarrow Ac(r_a)) \quad (۷-۴)$$

ناهنجاری افزونگی: این نوع ناهنجاری تأثیری بر عدم تطابق مکانیزم اعمالی و خط مشی خواسته‌شده ندارد و تنها بر کارایی دیوار آتش خصوصاً در شبکه‌های سرعت‌بالا تاثیرگذار است. از دیگر دلایل رفع این ناهنجاری، رفع صحیح‌تر دیگر ناهنجاری‌ها است (۴-۸).

$$f_3 = \bigwedge_{i=1}^{k} (Ac(r_i) \leftrightarrow Ac(r_a)) \quad (۸-۴)$$

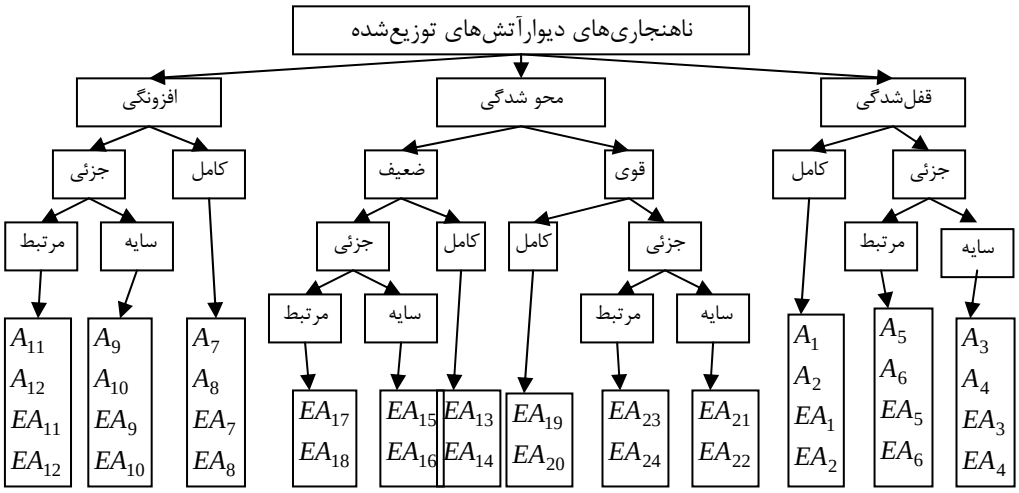
ناهنجاری محوشدگی ضعیف و قوی: اگر در شبکه‌ای با دیوار آتش‌های توزیع‌شده، دو مسیر متفاوت با دیوار آتش‌های غیر یکسان بین دو دامنه وجود داشته و مکانیزم اعمالی توسط این دو مسیر، معادل نباشد، ناهنجاری محوشدگی ایجاد می‌شود. در

محوشدگی ضعیف، قاعده‌ی با تصمیم پذیرش دچار ناهنجاری شده و به صورت کامل بر شبکه اعمال نمی‌شود (۴-۹). در محوشدگی قوی قسمتی از خط مشی دور زده می‌شود، این مسأله برای قواعد با تصمیم رد رخ می‌دهد (۴-۱۰).

$$f_7 = (T \rightarrow Ac(r_a)) \quad (۴-۹)$$

$$f_8 = (Ac(r_a) \rightarrow F) \quad (۴-۱۰)$$

با توجه به تعاریف بالا می‌توان ناهنجاری‌ها را با توجه به شکل ۲ به صورت ۱۳ ناهنجاری درون‌پایگاهی و ۲۵ ناهنجاری میان‌پایگاهی بیان نمود. در هر نوع ناهنجاری، شماره ناهنجاری عام (EA_{i+1}) یکی بیشتر از شماره ناهنجاری ساده (EA_i) است. برای مثال EA_{13} ناهنجاری محوشدگی ضعیف کامل میان‌پایگاهی **ساده**، و EA_{14} ناهنجاری محو شدگی ضعیف کامل میان‌پایگاهی **عام** است. به علت تشابه از ذکر ناهنجاری‌های ساده صرف نظر



شکل ۲. دسته‌بندي ناهنجاري‌ها. شکل بالا دسته‌بندي جـامعي از ناهنجـاري‌هـاي درون‌پايگـاهي A_i و ميان‌پايگاهي EA_i ميان قواعد در پايگاه قواعد ديوارآتـش‌هـاي توزيـع‌شـده را نشـان مـي‌دهـد. ايـن دسته‌بندي شامل ۱۲ ناهنجاري درون‌پايگاهي و ۲۴ ناهنجاري ميان‌پايگاهي است.

می‌شود. (۴-۱۱) تا (۴-۱۶) ناهنجاری‌های عام درون‌پایگاهی هستند.

$$A_2(r_a) = f_0 \square f_1 \wedge f_2 \wedge f_4 \quad (۴-۱۱)$$
$$A_4(r_a) = f_0 \square f_1 \wedge f_2 \wedge f_5 \quad (۴-۱۲)$$
$$A_6(r_a) = f_0 \square f_1 \wedge f_2 \wedge f_6 \quad (۴-۱۳)$$
$$A_8(r_a) = f_0 \square f_1 \wedge f_3 \wedge f_4 \quad (۴-۱۴)$$
$$A_{10}(r_a) = f_0 \square f_1 \wedge f_3 \wedge f_5 \quad (۴-۱۵)$$
$$A_{12}(r_a) = f_0 \square f_1 \wedge f_3 \wedge f_6 \quad (۴-۱۶)$$

روابط (۴-۱۷) تا (۴-۱۹) ناهنجاری‌های عام قفل‌شدگی میان‌پایگاهی و روابط (۴-۲۰) تا (۴-۲۲) ناهنجاری‌های عام افزونگی میان‌پایگاهی را نشان می‌دهند.

$$\theta = \bigotimes_{m=1}^{L} fw_m, \quad (۴-۱۷)$$
$$EA_2(r_a) = \theta, f_0 \square f_9 \wedge f_7 \wedge f_2 \wedge f_4 \quad (۴-۱۸)$$
$$EA_4(r_a) = \theta, f_0 \square f_9 \wedge f_7 \wedge f_2 \wedge f_5 \quad (۴-۱۹)$$
$$EA_6(r_a) = \theta, f_0 \square f_9 \wedge f_7 \wedge f_2 \wedge f_6 \quad (۴-۲۰)$$
$$EA_8(r_a) = \theta, f_0 \square f_9 \wedge f_8 \wedge f_3 \wedge f_4 \quad (۴-۲۱)$$
$$EA_{10}(r_a) = \theta, f_0 \square f_9 \wedge f_8 \wedge f_3 \wedge f_5 \quad (۴-۲۲)$$
$$EA_{12}(r_a) = \theta, f_0 \square f_9 \wedge f_8 \wedge f_3 \wedge f_6$$

روابط (۴-۲۳) تا (۴-۲۵) ناهنجاری محوشدگی ضعیف روابط و (۴-۲۶) تا (۴-۲۸) ناهنجاری محوشدگی قوی میان‌پایگاهی را نشان می‌دهند.

$$A = \theta = \bigoplus_{m=1}^{L} \theta_m, \theta_m = \bigotimes_{m'=1}^{L'} fw_{m,m'} \quad (۴-۲۳)$$
$$B = \exists \{r_1, r_2, r_3, ..., r_k, r_a\} \in \{\theta_1, ..., \theta_L\}$$
$$EA_{14}(r_a) = A, B \square f_9 \wedge f_2 \wedge f_7 \wedge f_4$$

$$EA_{16}(r_a) = A, B \square f_9 \wedge f_2 \wedge f_7 \wedge f_5 \quad (۴-۲۴)$$
$$EA_{18}(r_a) = A, B \square f_9 \wedge f_2 \wedge f_7 \wedge f_6 \quad (۴-۲۵)$$
$$EA_{20}(r_a) = A, B \square f_9 \wedge f_3 \wedge f_8 \wedge f_4 \quad (۴-۲۶)$$
$$EA_{22}(r_a) = A, B \square f_9 \wedge f_3 \wedge f_8 \wedge f_5 \quad (۴-۲۷)$$
$$EA_{24}(r_a) = A, B \square f_9 \wedge f_3 \wedge f_8 \wedge f_6 \quad (۴-۲۸)$$

۵- رویکردهای رفع ناهنجاری

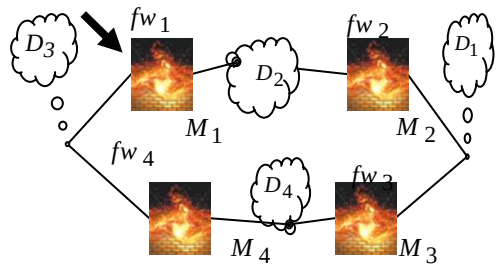
رویکرد اصلاح [۱۶, ۱۷] و پیشگیری [۱۲] دو رویکرد رفع ناهنجاری در دیوار آتش است. ARM نیز با دو گام اصلی محلی و سراسری به رفع ناهنجاری‌ها در دیوار آتش‌های توزیع‌شده می‌پردازد. شکل ۳، چهار دامنه (D_i) را نشان می‌دهد که خط-مشی آنها توسط چهار مدیر امنیتی (M_i) با استفاده از دیوار-آتش‌های fw_i که در پیکربندی شبکه قرار دارند، به صورت توزیع‌شده اعمال می‌شود.

۵-۱- رویکرد پیشگیری

زمانی که مدیر امنیتی و یا سیستم تشخیص نفوذ، تصمیم به افزودن قاعده‌ای جدید به دیوار آتش‌های شبکه را دارد رویکرد پیشگیری از بروز ناهنجاری جلوگیری می‌کند و موجب حفظ سازگاری میان قواعد می‌شود. این رویکرد در هشت گام صورت می‌گیرد:

۱. توصیف پیکربندی شبکه: در گام نخست دامنه و دیوار-آتش‌های شبکه و مسیرهای ارتباطی میان آنها توصیف می‌گردد. این توصیف توسط مدیران و از طریق واسط مدیر و با استفاده از گراف همجواری انجام می‌گیرد که در روابط (۵-۱) تا (۵-۳) آورده شده‌است.

۲. توصیف مدیران و روابط میان آنها: توصیف مدیران و روابط میان آنها طبق روابط (۵-۴) و (۵-۵) انجام می‌شود.



شکل ۳. پیکربندی یک شبکه نمونه برای اعمال رویکردهای رفع ناهنجاری ARM

$$L = \{(fw_1, fw_2), (fw_3, fw_4), (fw_1, D_2), (fw_1, D_3), (fw_2, D_2), (fw_2, D_1), (fw_3, D_1), (fw_3, D_4), (fw_4, D_3), (fw_4, D_4)\} \quad (۵-۱)$$
$$Z = \{D_1, D_2, D_3, D_4,\} \quad (۵-۲)$$
$$com = \{fw_1, fw_2, fw_3, fw_4\} \quad (۵-۳)$$
$$S_M = \{M_1, M_2, M_3, M_4\} \quad (۵-۴)$$
$$R_M = \{(M_1, M_2), (M_1, M_4), (M_4, M_3)\} \quad (۵-۵)$$

۳. دریافت درخواست به روزرسانی دیوار آتش‌ها: مدیر M_1 درخواست اعمال قاعده‌ی R_{M_1} را مطابق رابطه (۵-۶) به دیوار آتش fw_1 می‌دهد. طبق روابط (۵-۷) و (۵-۸) R_{M_1} فقط اجازه دسترسی به *mail server* را به دامنه D_3 می‌دهد.

$$R_{M_1} = r_3 r_2 \quad (۵-۶)$$
$$r_3 = D_3 2MS, accept \quad (۵-۷)$$
$$r_2 = D_3 2any_{in}, denay \quad (۵-۸)$$

۴. ترجمه قواعد به هستان‌شناسی ARM

الف. درخواست به روزرسانی طبق رابطه (۵-۹) ترجمه می‌شود.

$$r_3 = D_3 2D_2, accept$$
$$r_2 = D_3 2D_1 D_2, denay \quad (۵-۹)$$

ب. پایگاه قواعد هر دیوار آتش (RDB_{fw_i}) مشابه درخواست به روزرسانی ترجمه می‌شود.

۵. کاهش ناهنجاری‌های درون‌پایگاهی: این مرحله از رویکرد پیشگیری از سه گام جدا سازی، جذب و خوردگی تشکیل شده‌است.

الف. جداسازی: در جداسازی، قواعد جدید و پایگاه قواعد بر اساس مؤلفه تصمیمشان دسته‌بندی می‌گردند (دسته پذیرش و رد).

ب. جذب: در مرحله جذب به ترتیب زیر به ترکیب قواعدی که تصمیم یکسانی دارند پرداخته می‌شود:

۱. تشکیل گراف‌های افزونگی: در هر دسته، قواعدی که مؤلفه شرطشان همبستگی دارند گراف افزونگی را تشکیل می‌دهند.

۲. استخراج ناهنجاری: با استفاده از ماشین استنتاج ناهنجاری، نوع ناهنجاری‌های افزونگی وارسی شده و بر روی هر گره برچسب نوع ناهنجاری قرار می‌گیرد.

۳. رفع ناهنجاری: با استفاده از رابطه اولویت قواعد به رفع ناهنجاری پرداخته می‌شود.

ج. خوردگی: در این مرحله با تشکیل گراف تعارض بین قواعد با تصمیم متضاد به رفع ناهنجاری‌های قفل‌شدگی پرداخته می‌شود. قواعدی که تصمیم به حذف آنها گرفته می‌شود به صورت گره خاموش در گراف‌ها باقی می‌ماند تا در صورت از بین رفتن علت حذف قاعده، دوباره به وضعیت روشن برگردد.

۶. نگاشت قواعد به هستان‌شناسی ARM

الف. توصیف توابع همجواری: بر اساس گراف همجواری توصیف شده در سطح یک ARM توابع همجواری میان‌دامنه‌ای استخراج می‌گردد. برای مثال ذکر شده، روابط (۵-۱۰) این توصیف را نشان می‌دهند.

$$\begin{aligned}
&\Omega_{D1,D4} = fw_3 \\
&\Omega_{D1,D3} = fw_1 \otimes fw_2 \oplus fw_4 \otimes fw_3 \\
&\Omega_{D1,D2} = fw_2 \\
&\Omega_{D2,D3} = fw_1 \\
&\Omega_{D3,D4} = fw_4
\end{aligned} \qquad (۵-۱۰)$$

ب. ارتباط بین قواعد و توابع همجواری: توابع همجواری میان‌دامنه‌ای مرتبط با هر قاعده طبق رابطه (۵-۱۱) مشخص می‌شوند.

$$\begin{aligned}
&D(r_2) \in \Omega_{D1,D3} \\
&D(r_2), D(r_3) \in \Omega_{D2,D3}
\end{aligned} \qquad (۵-۱۱)$$

ج. ضرب زیر قواعد در توابع همجواری مرتبط: در ARM برای تزریق هر قاعده جدید به یکی از دیوار آتش‌های توزیع‌شده آن را در تابع همجواری میان‌دامنه‌ای مرتبط، مطابق رابطه (۵-۱۲) ضرب می‌شود.

$$r_2 \vartheta \Omega_{D1,D3} \wedge r_3 \tau (r_2 \vartheta \Omega_{D1,D3}) \qquad (۵-۱۲)$$

نتیجه حاصل طبق روابط زیر چهار حالت ممکن ω_i برای دیوار آتش‌های توزیع‌شده است:

$$\begin{aligned}
\omega_1 &= r_3 \tau r_2 \vartheta Fw_1 \wedge r_2' \vartheta Fw_2 \wedge r_2 \vartheta Fw_4 \wedge r_2' \vartheta Fw_3 \\
\omega_2 &= r_3 \tau r_2 \vartheta Fw_1 \wedge r_2' \vartheta Fw_2 \wedge r_2' \vartheta Fw_4 \wedge r_2 \vartheta Fw_3 \\
\omega_3 &= r_3 \tau r_2' \vartheta Fw_1 \wedge r_2 \vartheta Fw_2 \wedge r_2 \vartheta Fw_4 \wedge r_2' \vartheta Fw_3 \\
\omega_4 &= r_3 \tau r_2' \vartheta Fw_1 \wedge r_2 \vartheta Fw_2 \wedge r_2' \vartheta Fw_4 \wedge r_2 \vartheta Fw_3
\end{aligned}$$

۷. رفع ناهنجاری‌های سراسری: اثر هر قاعده با نگاشت قاعده و انتشار قواعد مجازی در تابع همجواری روی کل دیوار آتش‌ها در نظر گرفته می‌شود. پس از اضافه شدن قواعد مجازی در دیوار آتش‌های دیگر، مشابه گام یک عمل می‌شود.

۸. به روزرسانی پایگاه‌قواعد: پس از رفع ناهنجاری‌ها تغییرات به وجود آمده به مدیر هر دیوار آتش گزارش می‌شود و در نهایت دیوار آتش‌های توزیع‌شده به حالت بهینه تغییر می‌یابند.

۵-۲- رویکرد اصلاح ناهنجاری

رویکرد اصلاح به رفع ناهنجاری در دیوار آتش‌هایی می‌پردازد که پایگاه قواعد آنها از پیش ایجاد شده‌است. گام‌های یک تا چهار رویکرد اصلاح مشابه رویکرد پیشگیری است با این تفاوت که قاعده جدیدی توسط مدیر امنیتی درخواست داده نشده است. در گام پنجم، ARM با فرض جدید بودن همه قواعد به رفع ناهنجاری درون‌پایگاهی می‌پردازد. در رفع ناهنجاری‌های میان‌پایگاهی نیز روش کار مشابه است با این تفاوت که ARM پایگاه قواعدهایی تهی را جایگزین پایگاه قواعد هر دیوار آتش نموده و با جدید فرض نمودن هر قاعده، مراحل بعدی رویکرد پیشگیری را در پی می‌گیرد و پس از تزریق همه قواعد به رفع ناهنجاری‌های میان‌پایگاهی می‌پردازد.

۶- نتیجه گیری

در این پژوهش یک دسته‌بندی جامع از ناهنجاری‌ها در حوزه دیوارآتش ارائه شد. این دسته‌بندی دربرگیرنده توصیف جامعی از ناهنجاری‌های دیوار آتش‌های توزیع‌شده با در نظر گرفتن ناهنجاری عام است که آن را نسبت به کارهای پیشین متمایز می‌کند. همچنین ارائه مدل ARM با هستان‌شناسی مناسب موجب عدم وابستگی مدل به همبندی شبکه و قابلیت بکارگیری در محیط‌های ناهمگن شده، و سهولت استفاده برای مدیران امنیتی را فراهم می‌نماید. زیرساخت صوری ARM موجب توسعه‌پذیری مدل شده‌است. این مدل با استفاده از استنتاج روی قواعد ناهنجاری‌ها را با دو رویکرد پیشگیری و اصلاح رفع می‌نماید.

مراجع

[1] M. Bishop, "Computer Security Art and Science," *2nd ed: Addison-Wesley*, 2003.

[2] A. Wool, "A quantitative study of firewall configuration errors," *Computer*, pp. 62-67, 2004.

[3] S. Kumar, "Classification and Detection of Computer Intrusion, Computer Science Department, Purdue University Ph. D," dissertation, August 1995.

[4] A. Mayer, A. Wool, and E. Ziskind, "Offline firewall analysis," *International Journal of Information Security*, vol. 5, pp. 125-144, 2006.

[5] S. De Capitani Di Vimercati, S. Foresti, P. Samarati, and S. Jajodia, "Access control policies and languages," *International Journal of Computational Science and Engineering*, vol. 3, pp. 94-102, 2007.

[6] C. A. Ardagna, E. Damiani, S. De Capitani di Vimercati, and P. Samarati, "XML-based access control languages," *Information Security Technical Report*, vol. 9, pp. 35-46, 2004.

[7] A. El-Atawy, "Survey on the use of formal languages/models for the specification, verification, and enforcement of network access-lists," *School of Computer Science, Telecommunication, and Information Systems, DePaul University, Chicago, Illinois*, vol. 60604.

[8] N. Damianou, N. Dulay, E. Lupu, and M. Sloman, "The ponder policy specification language," *Lecture Notes in Computer Science*, pp. 18-38, 2001.

[9] V. Kurland and V. Zaliva, "Firewall builder," *White paper*, 2003.

[10] V. Capretta, B. Stepien, A. Felty, and S. Matwin, "Formal correctness of conflict detection for firewalls," 2007, p. 30.

[11] A. Bouhoula and Z. Trabelsi, "Handling Anomalies in Distributed Firewalls," *Innovations in Information Technology, 2006*, pp. 1-5, 2006.

[12] W. Deng, Y. Liang, and K. Gao, "Discover Inconsistencies between Firewall Policies," 2008, pp. 809-813.

[13] Y. Bartal, A. Mayer, K. Nissim, and A. Wool, "Firmato: A novel firewall management toolkit," *ACM Transactions on Computer Systems (TOCS)*, vol. 22, pp. 381-420, 2004.

[14] B. Zhang, E. Al-Shaer, R. Jagadeesan, J. Riely, and C. Pitcher, "Specifications of a high-level conflict-free firewall policy language for multi-domain networks," 2007, p. 194.

[15] P. Eronen and J. Zitting, "An expert system for analyzing firewall rules," 2001, pp. 100–107.

[16] E. S. Al-Shaer and H. H. Hamed, "Firewall policy advisor for anomaly discovery and rule editing," 2003, p. 17.

[17] E. S. Al-Shaer and H. H. Hamed, "Discovery of policy anomalies in distributed firewalls," 2004, pp. 2605-2616.

[18] F. Baboescu and G. Varghese, "Fast and scalable conflict detection for packet classifiers," *Computer Networks*, vol. 42, pp. 717-735, 2003.

[19] A. Hari, S. Suri, and G. Parulkar, "Detecting and resolving packet filter conflicts," 2000, pp. 1203-1212.

[20] A. Wool, "Architecting the lumeta firewall analyzer," 2001, p. 7.

[21] S. Pozo, R. Ceballos, and R. M. Gasca, "Model-Based Development of firewall rule sets: Diagnosing model inconsistencies," *Information and Software Technology*, vol. 51, pp. 894-915, 2009.

[22] D. Senn, D. Basin, and G. Carenni, "Firewall conformance testing," *Lecture Notes in Computer Science*, vol. 3502, pp. 226-241, 2005.

[23] A. Mayer, A. Wool, and E. Ziskind, "Fang: A firewall analysis engine," 2000, pp. 177-189.

[24] E. Al-Shaer and H. Hamed, "Modeling and management of firewall policies," *IEEE Transactions on Network and Service Management*, vol. 1, pp. 2–10, 2004.

[25] L. Yuan, J. Mai, Z. Su, H. Chen, C. N. Chuah, and P. Mohapatra, "FIREMAN: A toolkit for firewall modeling and analysis," 2006, pp. 199-213.

[26] E. Al-Shaer, H. Hamed, R. Boutaba, and M. Hasan, "Conflict classification and analysis of distributed firewall policies," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 2069-2084, 2005.

[27] T. E. Uribe and S. Cheung, "Automatic analysis of firewall and network intrusion detection system configurations," *Journal of Computer Security*, vol. 15, pp. 691-715, 2007.

[28] J. D. Guttman, "Filtering postures: Local enforcement for global policies," 1997, pp. 120-129.

[29] J. D. Guttman and A. L. Herzog, "Rigorous automated network security management," *International Journal of Information Security*, vol. 4, pp. 29-48, 2005.

[30] H. Hamed and E. Al-Shaer, "Taxonomy of conflicts in network security policies," *IEEE Communications Magazine*, vol. 44, pp. 134-141, 2006.