مجموعه مقالات پانزدهمین کنفرانس بین‌المللی انجمن رمز ایران
دانشکده مهندسی برق، دانشگاه تربیت دبیر شهید رجایی، تهران، ۶-۷ شهریور ۱۳۹۷
(مقاله مدعو)

مدل‌سازی و تحلیل سرمایه‌گذاری امنیتی نهادهای وابسته به کمک نظریه بازی‌ها

منصوره اژه‌ای [۱]، بهروز ترک لادانی [۲]

[۱] دکتری، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، اصفهان
m_ezhei@eng.ui.ac.ir

[۲] عضو هیئت‌علمی دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه اصفهان، اصفهان
ladani@eng.ui.ac.ir

چکیده

تعیین سطح مناسب سرمایه‌گذاری‌های امنیتی، یکی از تصمیم‌گیری‌های حیاتی است که مدیران امنیتی ارشد با آن مواجه هستند. موضوعی که تصمیم در سرمایه‌گذاری‌های امنیتی را با چالش روبرو می‌کند، وابستگی متقابل نهادها (شامل سازمان‌های دولتی، موسسات خصوصی و ..) است. این به آن معنی است که امنیت یک نهاد، نه‌تنها به تصمیم سرمایه‌گذاری آن، بلکه به تصمیمات دیگران نیز بستگی دارد. با گسترش ارتباطات شبکه‌ای، امنیت بسیاری از دستگاه‌ها و نهادها به یکدیگر وابسته شده است به نحوی‌که آسیب دیدن یک نهاد، امنیت سایر نهادها را متأثر می‌کند. لذا نهادها با توجه به ارتباطاتی که با سایر نهادها به‌صورت مستقیم و یا غیرمستقیم دارند، سطح سرمایه‌گذاری امنیتی خود را تعیین می‌نمایند. در این مقاله با بهره‌گیری از ابزار اقتصاد محاسباتی، نظریه بازی و طراحی مکانیزم، تلاش می‌نماییم درک بهتری از انگیزه‌های نهادهای وابسته نسبت به سرمایه‌گذاری امنیتی به دست آوریم. میزان سرمایه‌گذاری امنیتی در نقطه تعادل نش و بهینه‌ی اجتماعی با توجه به تابع احتمال نقض امنیت و ساختار شبکه‌ی وابستگی محاسبه شده است. نهایتاً با در نظر گرفتن نتایج به دست آمده، مکانیزم‌هایی جهت دستیابی به نقطه‌ی بهینه‌ی اجتماعی ارائه‌شده است.

کلمات کلیدی

اقتصاد امنیت، امنیت وابسته، سرمایه‌گذاری امنیتی ، نظریه بازی

۱- مقدمه

بروز حملات سایبری و نقض امنیت، تبدیل به نگرانی عمده‌ای در سال‌های اخیر شده است. این حملات به طیف گسترده‌ای از نهادهای بزرگ و کوچک صورت گرفته و به نظر می‌رسد انگیزه‌ی مهاجمین امروزی بیشتر به سمت کسب سود مالی، سوق پیدا کرده است تا کنجکاوی شخصی و یا رفتارهای هیجان‌بخش . به همین دلایل، امنیت اطلاعات تبدیل به مسئله‌ای حیاتی برای نهادهایی شده که اینترنت جزئی از کسب‌وکار آن‌هاست.

راه مستقیم برای امن‌تر شدن نهادها افزایش **سرمایه‌گذاری در امنیت**[۱] اطلاعات است. به عنوان مثال، نهادها می‌توانند با سرمایه‌گذاری در فن‌آوری‌های امنیتی مانند نرم‌افزارهای ضدویروس، دیواره‌های آتش، فن‌آوری‌های رمزنگاری پیچیده، سیستم‌های تشخیص نفوذ و یا دستگاه‌های سخت‌افزاری دیگر، امنیت اطلاعات را افزایش دهند [۲]. تعیین سطح مناسب سرمایه‌گذاری‌های امنیتی، یکی از تصمیم‌گیری‌های حیاتی است که مدیران ارشد امنیتی با آن مواجه هستند. در واقع امروزه مسئله اساسی در مدیریت امنیت، از «امکان‌پذیری فنی» به «کارآمدی اقتصادی»، تغییر کرده است. هزینه حفاظت، نباید از ارزش دارایی‌هایی که ما می‌خواهیم آن‌ها را محافظت کنیم تجاوز کند؛ به‌عبارت‌دیگر، سرمایه‌گذاری باید پس از محاسبه‌ی پایاپای هزینه‌های سرمایه‌گذاری در برابر افزایش امنیت اطلاعاتی که این سرمایه‌گذاری به ارمغان می‌آورد انجام شود.

موضوعی که تصمیم‌گیری در سرمایه‌گذاری‌های امنیتی را با چالش روبه‌رو می‌کند، **وابستگی متقابل**[۲] نهادها است [۳]. این بدان معنی است که امنیت یک نهاد، نه‌تنها به تصمیم سرمایه‌گذاری آن، بلکه به تصمیمات دیگران نیز بستگی دارد. افزایش تعامل و همکاری بین نهادهای مختلف منجر به ایجاد وابستگی پیچیده‌ای در سطح جهانی شده است. درنتیجه‌ی این همکاری، این

نهادها اغلب زیرساخت‌های اطلاعاتی و ارتباطی خود را با یکدیگر به اشتراک می‌گذارند و امکان دسترسی به داده‌ها، برنامه‌های کاربردی تجاری و خدماتی را برای یکدیگر فراهم می‌کنند. در چنین محیط پیچیده‌ای، امنیت بسیاری از سیستم‌ها و نهادها به یکدیگر وابسته شده است به‌نحوی‌که آسیب‌پذیری یک نهاد، ممکن است منجر به شکست زنجیره‌ای در سایر نهادها گردد و امنیت سایر نهادها را متأثر کند. به عنوان مثال، در دسامبر ۲۰۱۳، سامانه اطلاعاتی فروشنده بزرگ ایالات‌متحده، اتحادیه تارگت[۳] درهم‌شکسته شد و داده‌های شخصی و اطلاعات کارت‌های اعتباری بیش از ۱۱۰ میلیون مصرف‌کننده، به سرقت رفت [۴]. اما مسئله آنجا بود که چون شکستن سیستم اطلاعاتی نهاد تارگت مشکل بود، حمله‌کنندگان دستگاه‌های کنترل‌کننده سیستم تهویه هوا (HVAC)[۴] را که با سیستم اطلاعاتی نهاد تارگت ارتباط داشت و نقض آن آسان‌تر بود برای شروع حمله انتخاب کردند و سپس بر اساس این وابستگی متقابل به سیستم تارگت نفوذ پیدا کردند.

اطمینان از همکاری نهادهای وابسته در تأمین امنیت، چالشی است که مدیران ارشد امنیتی در دفاع از سیستم‌های شبکه‌ای با آن مواجه هستند. حتی در مواردی که انگیزه‌ی همکاری بین نهادها برای بهبود امنیت، وجود دارد، تصمیم‌گیری در تخصیص منابع امنیتی و تعیین سطح مناسب سرمایه‌گذاری امنیتی به‌عنوان چالش اساسی باقی می‌ماند. در پاسخ به چالش‌های فوق، مدل‌های **سرمایه‌گذاری امنیتی وابسته** [۱۰-۵]، جهت ارزیابی مخاطرات امنیتی، سود و انگیزه و سطح سرمایه‌گذاری توسط نهادهای وابسته ارائه شده است. این مدل‌ها، با رویکردی اقتصادی به توصیف انگیزه‌ی نهادها در به‌کارگیری اقدامات امنیتی و همچنین بیان مشکلات امنیتی می‌پردازند. در این مدل‌ها، با تخمین عددی پارامترهای سیستم، سطح سرمایه‌گذاری امنیتی هر نهاد تعیین می‌گردد. همچنین، طبیعت وابسته‌ی سرمایه‌گذاری امنیتی با مدل‌سازی روابط مابین نهادها انجام می‌گیرد.

هسته‌ی اصلی مدل‌های ارائه‌شده از تجزیه و تحلیل سرمایه‌گذاری‌های امنیتی به‌صورت زیر است: کاربران می‌توانند برای تأمین امنیت خود سرمایه‌گذاری کنند و یا بی‌دفاع باقی بمانند. امنیت هر کاربر، به میزان سرمایه‌گذاری امنیتی وی و همچنین سرمایه‌گذاری دیگر کاربران بستگی دارد. به عبارت دیگر، سرمایه‌گذاری امنیتی یک کاربر، می‌تواند تأثیرات مثبت یا منفی بر سطح امنیت سایر کاربران داشته باشد. این نوع تعاملات گاهی اوقات به‌عنوان **اثرات جانبی**[۵] با عوارض مثبت و منفی در نظر گرفته می‌شود. در **اثرات جانبی مثبت**، افزایش سرمایه‌گذاری امنیتی توسط یک کاربر نه‌تنها کمک می‌کند تا کاربر خود را در برابر حملات بالقوه محافظت کند، بلکه به حفاظت سایر کاربران که با وی تعامل داشته‌اند نیز کمک می‌نماید؛ زیرا کمتر احتمال دارد یک کاربر محافظت‌شده به خطر بیافتد و درنتیجه از او برای تولید و یا ترویج حملات علیه نهادهای دیگر استفاده شود؛ اما باید دانست که اثرات جانبی مثبت باعث می‌شود کاربران از سرمایه‌گذاری در امنیت امتناع ورزیده و از دیگران توقع داشته باشند که از آن‌ها حفاظت کنند. در **اثرات جانبی منفی**، سرمایه‌گذاری امنیتی یک کاربر در جهت محافظت خود، منجر به کاهش امنیت سایر کاربران می‌گردد. اثرات جانبی منفی هنگامی بروز می‌کند که بازیکنان با سرمایه‌گذاری بیشتر در دفاع امنیتی، از خود حفاظت می‌کنند. در عمل، گاهی پیش می‌آید که سرمایه‌گذاری امنیتی یک کاربر، سیستم اطلاعاتی‌اش را در برابر حملات مقاوم‌تر کرده و درنتیجه مهاجمین را به اهداف دیگر ترغیب می‌نماید. به‌این‌ترتیب، سایر کاربران به سرمایه‌گذاری بیشتر ترغیب می‌شوند.

امنیت یک نهاد، نه‌تنها به تصمیم سرمایه‌گذاری آن، بلکه به تصمیمات دیگران نیز بستگی دارد. در این راستا نظریه بازی‌ها[۶] تکنیک ریاضی مناسب به‌منظور تجزیه و تحلیل چنین مسائلی است که دربرگیرنده‌ی موقعیت‌های استراتژیک هستند. این موقعیت، زمانی پدید می‌آید که موفقیت یک فرد وابسته به تصمیماتی است که دیگران انتخاب می‌کنند. هدفِ نهاییِ این دانش، یافتن استراتژی بهینه برای بازیکنان است.در هر بازی، بازیکنان به دنبال انتخاب بهترین استراتژی برای خود در مقابل استراتژی‌های ممکن برای رقیب هستند که این روند در انتها به یک نقطه‌ی **تعادل نش**[۷] ختم می‌شود. در نقطه‌ی تعادل نش هر بازیکن خودخواهانه عمل می‌کند و به حداکثر رساندن منافع خود را دنبال می‌نماید و به دنبال بهینه‌سازی تابع مطلوبیت فردی خود در مقابل استراتژی‌های ممکن برای رقیب می‌باشد. **کارایی** راه‌حل تعادل نش، می‌تواند در مقایسه با بردار استراتژی که از لحاظ اجتماعی بهینه است، اندازه‌گیری شود. **بهینه اجتماعی**[۸] به حداقل مجموع هزینه‌های فردی بازیکنان اطلاق می‌شود. چنانچه استراتژی بازیکنان در نقطه‌ی تعادل نش منجر به استراتژی بهینه‌ی اجتماعی نگردد، در این صورت، یک تنظیم‌کننده که **برنامه‌ریز اجتماعی** نیز نامیده می‌شود، تلاش می‌کند تا رفاه اجتماعی را به سطح بهینه برساند. بهبود استراتژی بازیکنان در نقطه‌ی تعادل نش، به سطح بهینه اجتماعی خود، نیازمند وضع مجموعه‌ای از مقررات اضافی و یا در نظر گرفتن طرح‌های تشویقی است؛ که موضوع نظریه‌ی **طراحی مکانیزم**[۹] است. طراح با ارائه‌ی مشوق‌ها و طراحی مکانیزم‌هایی رفتار بازیکنان را به سمت بهینه‌ی اجتماعی سوق می‌دهد.

در حالی‌که اغلب مدل‌های سرمایه‌گذاری امنیتی وابسته [۱۱-۱۵]به مدلسازی و تحلیل سرمایه‌گذاری امنیتی دو نهاد وابسته با در نظرگرفتن تابع نقض امنیتی خاص با استفاده از نظریه بازی‌ها پرداخته‌اند، در پژوهش پیش رو، تقابل بین n نهاد در ساختار شبکه‌ی وابستگی و تابع نقض امنیت کلی با استفاده از نظریه‌ی بازی مدل‌سازی و تحلیل می‌گردد. از دیدگاه نظریه‌ی بازی همه‌ی بازیکنان تصمیم‌گیرندگان منطقی هستند. درنتیجه، هر بازیکن در زمان بهینه‌سازی تصمیمات سرمایه‌گذاری خود، سرمایه‌گذاری سایر بازیکنان را به‌حساب می‌آورد. تعاملات این قبیل بازیکنان استراتژیک یک بازی را تشکیل می‌دهد که از این پس به‌عنوان **بازی امنیتی** به آن اشاره می‌شود.

در مدل ارایه شده، مطلوبیت هر نهاد به مجموع خطی وزن‌دار سطح دفاع همسایه‌ها بستگی خواهد داشت. به صورتی که وزن‌ها، وابستگی میان گره‌ها در ساختار شبکه‌ای می‌باشد. ما هم تعادل نش و هم پروفایل‌های بهینه اجتماعی را در نظر می‌گیریم و وجود تعادل نش و همچنین تفسیرهای نظری تلاش‌های بازیکنان در تعادل نش و پروفایل‌های بهینه‌ی اجتماعی را مطالعه خواهیم کرد. یافته‌های ما ابزار موردنیاز برای پاسخ به چالش‌های نظری و جنبه‌های طراحی مکانیزم در بازی‌های امنیتی را فراهم خواهند کرد.

این توصیفات به ما اجازه می‌دهند به سؤالاتی برحسب ساختار شبکه مانند سؤالات زیر پاسخ دهیم:

- چگونه نهادها سرمایه‌گذاری‌های خود را انجام می‌دهند؟
- چگونه نهادها را با سیاست‌های مالیاتی/یارانه‌ای هدف قرار دهیم تا ارائه‌ی امنیت را بهبود بخشیم؟

- چطور تغییر ساختار شبکه، تصمیمات بازیکنان را تحت تأثیر قرار می‌دهند؟

پاسخ به پرسش‌های بالا به استنباط‌های مهم سیاست و طراحی منجر خواهد شد.

در این راستا، در بخش ۲ چارچوب کلی سرمایه‌گذاری امنیتی را در ساختارهای وابسته مورد بررسی قرار می‌دهیم. در بخش ۳، به مطالعه تعادل نش و بهینه‌ی اجتماعی می‌پردازیم. هدف ما ارائه درک درستی از تعاملات استراتژیک نهادها در یک ساختار شبکه‌ای است. نهایتاً در بخش۴، مکانیزم-هایی مبتنی بر تغییر ساختار شبکه و پاداش/تنبیه جهت دستیابی به نقطه‌ی بهینه‌ی اجتماعی ارائه نموده‌ایم.

۲- مدل بازی پیشنهادی

ما یک بازی از n نهاد را در نظر گرفته‌ایم که در آن هر نهاد i برای محافظت از دارایی‌های اطلاعاتی خود به میزان $z_i(t)$سرمایه‌گذاری می‌کند. این سرمایه‌گذاری برای استخدام کارشناسان امنیتی و استفاده از فن‌آوری‌های امنیتی، مانند نرم‌افزار آنتی‌ویروس، فایروال، *IDS*، شبکه‌های خصوصی مجازی (*VPN*) و ... استفاده می‌شود. همچنین فرض می‌کنیم نهادها در یک ساختار شبکه‌ی وابستگی‌های متقابل قرار گرفته‌اند. این شبکه با استفاده از یک گراف جهت‌دار وزن‌دار شامل N گره و E یال نمایش داده می‌شود. هر گره نشان‌دهنده یک نهاد مستقل است. در حالی که لینک جهت‌دار بین گره‌ها نشان‌دهنده وجود نوعی از وابستگی بین آن دو نهاد است.

مجموعه یال‌ها، شامل عنصر ij است اگر تصمیم گره i بر تصمیم گره j مؤثر باشد. برای هر یک از لبه‌ها یک وزن، $\eta_{ij} \in R$، تخصیص داده‌شده؛ که قدرت یال یا درجه نفوذ یک نهاد بر دیگر نهادها را نمایش می‌دهد. می‌توان ترکیب اتصالات و اطلاعات وزن را در یک ماتریس، $W \in R^{N\times N}$، به شرح زیر خلاصه نمود:

$$W_{ij} = \begin{cases} 1 & if \quad i = j \\ \eta_{ij} & if \quad e_{ij} \in \mathcal{E} \\ 0 & otherwise \end{cases}$$

(۱)

هر نهاد i برای محافظت از دارایی‌های اطلاعاتی خود به میزان $z_i(t)$ سرمایه‌گذاری می‌کند. این انتخاب‌ها توسط بردار استراتژی $\mathbf{z} = (z_1, z_2, ..., z_n)$ بیان می‌گردد که در آن n تعداد نهادها است. به‌واسطه‌ی وابستگی‌های متقابل بین دستگاه‌ها، اقدامات انجام‌شده توسط یک گره می‌تواند اثرات جانبی مثبت بر همسایگان خود ایجاد نماید. توجه داشته باشید که $(Wz)_i$ نشان‌دهنده سرمایه‌گذاری مؤثر کل در محل‌های امنیتی توسط همه نهادها در شبکه نسبت به گره i است. وابستگی بین شرکت‌ها در اثر شبکه بودن، باعث می‌شود درنهایت شرکت i دفاع متراکم (تجمعی) $z_i^a(t)$ زیر را داشته باشد:

(۲)

$$z_i^a(t) = (\mathbf{W}z)_i = z_i(t) + \sum_{j=1, j\neq i}^{n} \eta_{ij} z_j(t)$$

پارامتر η_{ij} درجه وابستگی مثبت دو شرکت در برابر حملات سایبری را نشان می‌دهد. وابستگی مثبت، به این معنی است که حمله‌ی موفقیت‌آمیز علیه یک شرکت می‌تواند به نسبت η_{ij} به شرکت دیگر انتقال یابد. در وابستگی مثبت هرچند هر شرکت، دفاع محکم‌تری را به‌واسطه‌ی همکاری با سایر شرکت‌ها دریافت می‌کند، اما در معرض حمله‌ی محکم‌تری به‌واسطه‌ی حمله از طریق سایر شرکت‌ها نیز قرار دارد.

تابع احتمال نقض امنیتی $V_i((\mathbf{Wz})_i)$ وابسته به دفاع تجمعی نهاد i بوده و بیانگر احتمال موفقیت حمله بر روی نهاد i با توجه به سطح سرمایه‌گذاری تجمعی این نهاد می‌باشد. $V_i((\mathbf{Wz})_i)$تابعی پیوسته و نسبت به z_i به‌صورت محدب افزایش می‌یابد.

میزان خسارت مورد انتظار یک نهاد در صورت بروز حمله به صورت $\mathrm{P}_i((\mathbf{Wz})_i) = -V_i((\mathbf{Wz})_i) \times L_i$ خواهد بود که L_i ضرر مالی است که هنگامی‌که سیستم اطلاعاتی نهاد i با موفقیت توسط مهاجم تخریب می‌شود، این نهاد متحمل می‌شود. این خسارت می‌تواند ملموس باشد مانند از دست دادن کسب‌وکار و هزینه‌های تعمیر و نگهداری خرابی سیستم یا می‌تواند غیرملموس باشد، مانند از دست دادن اعتماد مشتری، شهرت و رقابت. این خسارت می‌تواند در اثر نقض محرمانگی (ازجمله مواردی که در آن اطلاعات استراتژیک به رقبا داده می‌شود یا توسط مهاجم از اطلاعات کارت اعتباری استفاده جعلی می‌شود)، صحت (ازجمله تصمیمات غلط بر اساس داده‌های تغییریافته توسط مهاجم)، و یا دسترس‌پذیری (ازجمله کاهش سرویس‌دهی به دلیل عدم موفقیت کاربران مجاز در دسترسی در اثر حملات DoS) به نهاد وارد شود.

در نهایت تابع مطلوبیت هر نهاد به صورت زیر خواهد بود:

(۳)

$$u_i(\mathbf{z}, \mathbf{c}) = \mathrm{P}_i\left((\mathbf{Wz})_i\right) - h_i z_i$$

در معادله‌ی فوق، تابع $\mathrm{P}_i((\mathbf{Wz})_i)$ ویژگی‌های زیر را برآورده می‌سازد:

تابع $\mathrm{P}_i((\mathbf{Wz})_i)$تابعی پیوسته و نسبت به z_i به‌صورت مقعر افزایش می‌یابد.

۳- تحلیل نقاط تعادل

در این بخش، سطح سرمایه‌گذاری امنیتی در دو حالت بررسی می‌شود: نقطه‌ی تعادل نش و نقطه‌ی بهینه‌ی اجتماعی.

تعادل نش بردار استراتژی است که در آن هیچ بازیکنی، چنانچه سایر بازیکنان استراتژی خود را تغییر ندهند، تمایلی به تغییر استراتژی خود

ندارد. از دیدگاه امنیت اجتماعی، نتیجه ایده‌آل در یک بازی امنیتی، به‌عنوان راه‌حل بهینه‌ی اجتماعی شناخته شده است. راه‌حل بهینه‌ی اجتماعی در بازی امنیتی، سطوح تلاشی از نهادها است که در آن هزینه‌ی جمعی امنیت برای تمام نهادها به حداقل رسیده است در صورتی‌که استراتژی بازیکنان در نقطه‌ی تعادل نش منجر به استراتژی بهینه‌ی اجتماعی نگردد، در این صورت، یک طراح که برنامه‌ریز اجتماعی نیز نامیده می‌شود، تلاش می‌کند تا رفاه اجتماعی را به سطح بهینه برساند. طراح با ارائه‌ی مشوق‌ها و طراحی مکانیزم‌هایی رفتار بازیکنان را به سمت بهینه‌ی اجتماعی سوق می‌دهد.

۳-۱- تعادل نش

در نقطه تعادل نش، هیچ‌یک از طرفین بازی به‌صورت یک‌طرفه عمل نمی‌کند، بلکه با توجه به منطقی بودن بازیکنان، مناسب‌ترین پاسخ تعیین می‌شود. در این بخش، ما سرمایه‌گذاری‌های نهادها را در نقطه‌ی تعادل نش تحلیل می‌کنیم. تعادل نش، بردار استراتژی پایداری است که توسط بازیکنان خودخواه اتخاذ می‌شود. در نقطه‌ی تعادل نش هر بازیکن خودخواهانه عمل می‌کند و به حداکثر رساندن منافع خود را دنبال می‌نماید و به دنبال بهینه‌سازی تابع مطلوبیت فردی خود در مقابل استراتژی‌های ممکن برای رقیب می‌باشد.
مطلوبیت نهاد i به‌صورت زیر بیان می‌شود.

$$J_{F_i} = \mathrm{P}_i\left((\mathbf{Wz})_i\right) - h_i z_i$$

(۴)

شرایط مرتبه اول به‌صورت زیر است:

$$\frac{\partial \mathrm{P}_i\left((\mathbf{Wz})_i\right)}{\partial z_i} - h_i = 0$$

(۵)

با در نظر گرفتن معادلات فوق مقادیر سرمایه‌گذاری درنقطه‌ی تعادل نش به به‌صورت زیر دست آورده می‌شود.

$$\begin{cases} x_i^+ = 0 \quad if & \dfrac{\partial \mathrm{P}_i\left((\mathbf{Wz})_i\right)}{\partial z_i} - h_i > 0 \\ x_i^+ = 0 \quad if & \dfrac{\partial \mathrm{P}_i\left((\mathbf{Wz})_i\right)}{\partial z_i} - h_i = 0 \end{cases}$$

(۶)

سطح بهینه‌ی اجتماعی به‌عنوان یک معیار کارایی سرمایه‌گذاری به‌کاربرده می‌شود در ادامه مورد بحث قرار می‌گیرد.

۳-۲- بهینه اجتماعی

در این بخش، با در نظر گرفتن این‌که برنامه‌ریز اجتماعی تصمیمات خود در مورد سرمایه‌گذاری امنیت را به‌صورت متمرکز اتخاذ می‌کند، در ادامه سرمایه‌گذاری‌های نهادها تحلیل می‌شود. مطلوبیت اجتماعی از دیدگاه برنامه‌ریز اجتماعی به‌صورت معادله مقیّد زیر است:

$$J_{SP} = \sum \mathrm{P}_i\left((\mathbf{Wz})_i\right) - h_i z_i$$

(۷)

شرایط مرتبه اول به‌صورت زیر است:

$$\sum \rho_{ji} \frac{\partial \mathrm{P}_i\left((\mathbf{Wz})_i, (\mathbf{Wc})_i\right)}{\partial z_i} - h_i = 0$$

(۸)

با در نظر گرفتن معادلات فوق مقادیر سرمایه‌گذاری درنقطه‌ی تعادل نش به به‌صورت زیر دست آورده می‌شود.

$$\begin{cases} x_i^* = 0 \quad if & \sum \rho_{ji} \dfrac{\partial \mathrm{P}_i\left((\mathbf{Wz})_i, (\mathbf{Wc})_i\right)}{\partial z_i} - h_i > 0 \\ x_i^* = 0 \quad if & \sum \rho_{ji} \dfrac{\partial \mathrm{P}_i\left((\mathbf{Wz})_i, (\mathbf{Wc})_i\right)}{\partial z_i} - h_i = 0 \end{cases}$$

(۹)

با مقایسه‌ی معادلات (۶) و (۸) مشاهده می‌شود سطح امنیت ارائه‌شده توسط نهادها معمولاً از سطح بهینه اجتماعی آن‌ها دور است و خوب برآورده نشده است. این عدم بهینگی از این واقعیت نشأت می‌گیرد که نهادها در هنگام انتخاب سطح تلاششان، حساب تأثیرات برونی اعمال خود را نمی‌کنند؛ چراکه فقط در حال بهینه‌سازی سودهای خود هستند. علاوه بر این، برخی از نهادها سطح تلاش‌های خود را کاهش می‌دهند، چراکه آن‌ها می‌توانند از اقدامات دیگران سوءاستفاده کنند. بنابراین، بهبود تأمین امنیت به سطح بهینه اجتماعی خود نیازمند وضع مجموعه‌ای از مقررات اضافی و یا در نظر گرفتن طرح‌های تشویقی است. این مقررات/انگیزه‌ها به یک ساختار بازی تغییریافته منجر می‌شوند تا تعادل‌های حاصل از آن‌ها هم به نتیجه‌ی مورد نظر طراح منتهی شوند. در ادامه، روش‌هایی برای مشکل عدم بهینگی تصمیمات امنیتی نهادها با تمرکز بر طراحی مکانیزم‌های تشویقی/انگیزه‌ای ارائه می‌شود.

۴- طراحی مکانیزم

بین سرمایه‌گذاری نهاد در تعادل نش و سطح بهینه سرمایه‌گذاری از دیدگاه برنامه‌ریز اجتماعی، تفاوت‌هایی وجود دارد؛ بنابراین، برنامه‌ریزان اجتماعی، در جستجوی روش‌هایی برای طراحی عوامل سیستم

می‌باشند. هدف طراحی عبارت است از: تشویق نهادهای خودخواه برای سرمایه‌گذاری در سطح بهینه اجتماعی. در این بخش، دو طرح مبتنی بر سرمایه‌گذاری امنیتی و طرح مبتنی بر امنیت به‌منظور به دست آوردن بهینه اجتماعی معرفی می‌نماییم. همچنین نشان می‌دهیم چگونه با طراحی مناسب ساختار شبکه وابستگی، نهادها تشویق می‌شوند تا در سطح بهینه از لحاظ اجتماعی، سرمایه‌گذاری کنند.

۴-۱- طراحی شبکه‌ی وابستگی مناسب

در این بخش نشان داده می‌شود، چه طور تغییر ساختار شبکه‌ی وابستگی می‌تواند نهادها را تشویق کند تا در سطح بهینه‌ی اجتماعی، سرمایه‌گذاری کنند. به این منظور، ابتدا، بهینه اجتماعی بازی بر اساس ساختار فعلی شبکه‌ی وابستگی تعیین می‌شود. سپس ساختار شبکه‌ی وابستگی، به نحوی اصلاح می‌شود تا سطح سرمایه‌گذاری نهادها بر بهینه اجتماعی منطبق گردد. تغییر شبکه‌ی وابستگی به صورتی باید انجام گیرد که این تغییر بر بهینه اجتماعی تأثیر نگذارد.

چنانچه $\mathbf{z}^* > 0$ بهینه اجتماعی مبتنی بر ماتریس وزن فعلی $\mathbf{W}$ باشد. ماتریس حاصل از اشتراک بین دو مجموعه‌ی $\mathbf{W}_1$ و $\mathbf{W}_2$ زیر $\mathbf{W}^* \subseteq \mathbf{W}_1 \cap \mathbf{W}_2$ به یک تعادل نش کارآمد منتهی خواهد شد.

$$\mathbf{W}_1 = \left\{ \frac{\partial \mathrm{P}_i\left((\mathbf{W}^*\mathbf{z}^*)_i\right)}{\partial z_i} - h_i \;\; = 0 \right.$$

(۱۰)

$$\mathbf{W}_2 = \left\{ \sum \rho_{ji} \frac{\partial \mathrm{P}_i\left((\mathbf{W}^*\mathbf{z}^*)_i\right)}{\partial z_i} \;\; - h_i = 0 \right.$$

(۱۱)

با جایگذاری $\mathbf{z}^*$ در معادله‌ی ***Error! Reference source not found.*** گروه اول محدودیت‌ها حاصل می‌شود. گروه اول محدودیت‌ها، مجموعه ماتریس‌های $\mathbf{W}_1$ را پیدا می‌کند که تضمین می‌کند $\mathbf{z}^*$ تعادل نش بازیکنان نیز خواهد بود. گروه دوم محدودیت‌ها با جایگذاری $\mathbf{z}^*$ در معادلات ***Error! Reference source not found.*** حاصل می‌شود. گروه دوم محدودیت‌ها مجموعه ماتریس‌های $\mathbf{W}_2$ را پیدا می‌کند تا اطمینان یابد که مطلوبیت اجتماعی با تغییر شبکه‌ی وابستگی، ثابت مانده است. درنتیجه، اگر یک تقاطع بین این مجموعه‌ها وجود داشته باشد، نتایج $\mathbf{W}^* \subseteq \mathbf{W}_1 \cap \mathbf{W}_2$ به یک تعادل نش کارآمد منتهی خواهد شد.

۴-۲- طرح مبتنی بر سرمایه‌گذاری امنیتی

در این طرح، برای میزان سرمایه‌گذاری z_i ، شرکت i، پاداشی معادل با $\zeta(z_i)$ از شرکت j دریافت می‌کند و بالعکس. مطلوبیت کل شرکت i تحت این طرح هماهنگی به‌صورت زیر خواهد بود:

$$Ji(x) \;=\; \mathrm{P}_i\left((\mathbf{Wz})_i\right) - h_i z_i + \sum_{j=1,\, j\neq i}^{n} \zeta(z_i) - \zeta(z_j)$$

(۱۲)

شرایط مرتبه اول به‌صورت زیر خواهد بود:

$$\frac{\partial \mathrm{P}_i\left((\mathbf{Wz})_i\right)}{\partial z_i} - h_i \;\; + (n-1)\frac{\partial \zeta(z_i)}{z_i} = 0$$

(۱۳)

فرض کنید z^* مقادیر بهینه‌ی اجتماعی باشند. با جایگذاری z^* در معادلات بالا، تابع جریمه $\zeta(z_i)$ که درمجموعِ معادلات زیر صدق کند، منجر به بهینه‌ی اجتماعی می‌شود:

$$\frac{\partial \mathrm{P}_i\left((\mathbf{Wz}^*)_i\right)}{\partial z_i} - h_i \;\; + (n-1)\frac{\partial \zeta(z_i)}{z_i} = 0$$

(۱۴)

با اجرای طرح هماهنگی فوق، سطح سرمایه‌گذاری z_i که از معادله بالا به دست می‌آید. هزینه‌ی اجتماعی را کاهش می‌دهد.

لازم به ذکراست که جهت پیاده‌سازی طرح مبتنی بر سرمایه‌گذاری، شخص ثالث مستقلی موردنیاز است تا بر نحوه‌ی تبادل مقادیر پاداش نظارت داشته باشد و آن را تسهیل کند. وظیفه این شخص ثالث، نظارت بر سرمایه‌گذاری‌های امنیتی نهاد، جمع‌آوری و بازپرداخت بر اساس پاداش تعیین‌شده توسط طرح مبتنی بر سرمایه‌گذاری امنیتی است.

۴-۳- طرح مبتنی بر امنیت

در این بخش، مکانیزم دیگری بر اساس سطح امنیت هر نهاد پیشنهاد شده است. نهادها به یکدیگر (بیشتر از طریق یک شخص ثالث) بر اساس سطح آسیب‌پذیری خود پرداخت می‌کنند. برخلاف طرح مبتنی بر سرمایه‌گذاری که هزینه‌ها به‌راحتی قابل مشاهده نیست، در این طرح، به‌خصوص با استفاده از امکانات حسابرسی اطلاعات امنیتی[۱۱] (ISA) مشاهده وضعیت امنیتی نهاد ها آسان‌تر است. ISA سیستم ارزیابی امنیتی نهادها است و به ارائه یک روش معقول و قابل اندازه‌گیری برای بررسی چگونگی تأمین امنیت یک سیستم اطلاعاتی واقعی می‌پردازد.

ISA را می‌توان در سطح ملی (توسط استانداردهایی مانند گواهی حسابداران[۱۲]، OTS فدرال، DOJ و ...) و یا در سطح نهاد (به عنوان مثال توسط یک حسابرسی اینترنتی حرفه ای[۱۳](CIAP)) انجام داد. به

هر حال، نتایج حسابرسی می تواند به عنوان یک معیار مناسب برای اجرای سیاست های امنیت اطلاعات دولت / نهاد ها با استفاده از مکانیزم ارائه شده در این بخش مورد استفاده قرار گیرد.

در این طرح، نهادها به یکدیگر برای نگه‌داشتن یک سیستم امن پاداش می‌دهند. در این طرح، برای میزان سرمایه‌گذاری z_i، شرکت i، هزینه‌ای معادل با $\zeta\left(\mathrm{P}_i(\mathbf{Wz})_i\right)$ به شرکت j پرداخت می‌کند و بالعکس. مطلوبیت کل شرکت i تحت این طرح هماهنگی به‌صورت زیر خواهد بود:

$$Ji(x) = \mathrm{P}_i((\mathbf{Wz})_i) - h_i z_i + \sum_{j=1, j\neq i}^{n} [\zeta\left(\mathrm{P}_j(\mathbf{Wz})_j\right) - \zeta\left(\mathrm{P}_i(\mathbf{Wz})_i\right)] \quad (۱۵)$$

شرایط مرتبه اول با توجه به z_i به‌صورت زیر خواهد بود.

$$\frac{\partial \mathrm{P}_i\left((\mathbf{Wz})_i\right)}{\partial z_i} - h_i + \Delta = 0$$

$$\Delta = \sum_{j=1, j\neq i}^{n} [\rho_{ij} \frac{\partial \zeta\left(\mathrm{P}_j(\mathbf{Wz})_j\right)}{\partial \mathrm{P}_j(\mathbf{Wz})_j)} \frac{\partial \mathrm{P}_j\left((\mathbf{Wz})_i\right)}{\partial z_j} - \frac{\partial \zeta\left(\mathrm{P}_i(\mathbf{Wz})_i\right)}{\partial \mathrm{P}_i(\mathbf{Wz})_i)} \frac{\partial \mathrm{P}_i\left((\mathbf{Wz})_i\right)}{\partial z_i}]$$

(۱۶)

فرض کنید z^* مقادیر بهینه‌ی اجتماعی باشند. با جایگذاری z^* در معادلات بالا، تابع جریمه $\zeta\left(\mathrm{P}_i(\mathbf{Wz})_i\right)$ که درمجموعِ معادلات زیر صدق کند، منجر به بهینه‌ی اجتماعی می‌شود.

$$\frac{\partial \mathrm{P}_i\left((\mathbf{Wz}^*)_i, (\mathbf{Wc}^*)_i\right)}{\partial z_i} - h_i + \Delta = 0$$

$$\Delta = \sum_{j=1, j\neq i}^{n} [\rho_{ij} \frac{\partial \zeta\left(\mathrm{P}_j\left((\mathbf{Wz}^*)_j\right)\right)}{\partial \mathrm{P}_j\left((\mathbf{Wz}^*)_j\right)} \frac{\partial \mathrm{P}_j\left((\mathbf{Wz}^*)_j\right)}{\partial z_j^*} - \frac{\partial \zeta\left(\mathrm{P}_i\left((\mathbf{Wz}^*)_i\right)\right)}{\partial \mathrm{P}_i\left((\mathbf{Wz}^*)_i\right)} \frac{\partial \mathrm{P}_i\left((\mathbf{Wz}^*)_i\right)}{\partial z_i^*}]$$

(۱۷)

بر این اساس، نهاد i به نهاد j مقدار $\zeta\left(\mathrm{P}_i(\mathbf{Wz})_i\right)$ بر اساس سطح امنیتی خود پرداخت می‌کند. سرمایه‌گذاری کمتر از بهینه‌ی اجتماعی، منجر به‌احتمال نقض امنیت بالاتر می‌شود که منجر به پرداخت بالاتر می‌گردد، بنابراین در این وضعیت انگیزه برای سرمایه‌گذاری بیشتر و کاهش آسیب‌پذیری افزایش می‌یابد و نهادها به سرمایه‌گذاری در سطح بهینه اجتماعی تشویق می‌شوند.

سرمایه‌گذاری بیشتر از بهینه‌ی اجتماعی، منجر به‌احتمال نقض امنیت پایین‌تر می‌شود که منجر به پرداخت پایین‌تر می‌گردد، بنابراین در این وضعیت انگیزه برای سرمایه‌گذاری کمتر افزایش می‌یابد و نهادها به سرمایه‌گذاری در سطح بهینه اجتماعی تشویق شوند.

۵- جمع بندی

میزان سرمایه‌گذاری امنیتی در نقطه تعادل نش و بهینه‌ی اجتماعی با توجه به تابع احتمال نقض امنیت و ساختار وابستگی به دست آورده شد. ما این نتایج را بکار بردیم تا شبکه‌ی وابستگی متقابل بین نهادها، به نحوی طراحی شود که شرکت‌ها تشویق شوند تا در سطح بهینه‌ی اجتماعی، سرمایه‌گذاری کنند. به‌علاوه، برای سطح مورد نظر وابستگی متقابل بین نهادها، ما دو مکانیزم دیگر طراحی نمودیم که شرکت‌ها را در سرمایه‌گذاری در سطح بهینه ازلحاظ اجتماعی تشویق می‌کرد. نتایج حاصل از این تحلیل‌ها به مدیران ارشد امنیتی به شیوه های مختلف از جمله موارد زیر کمک می‌کند:

- بهینه‌سازی منابع شرکت در برابرحملات (یافتن طرح سرمایه‌گذاری مطلوب)
- توجه به اهمیت یافتن وابستگی متقابل بین نهاد ها و تاثیر آن در طراحی و نگهداری شبکه‌های مقاوم‌تر.
- برنامه‌ریز اجتماعی می‌تواند از طریق اجرای مکانیزم‌های پاداش یا مجازات پیشنهادی منجر به سرمایه‌گذاری نهادها در سطح بهینه‌ی اجتماعی گردد.

مراجع

[1] K.-K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Computers & Security*, vol. 30, pp. 719-731, 2011.

[2] M. Çakanyıldırım, W. T. Yue, and Y. U. Ryu, "The management of intrusion detection: Configuration, inspection, and investment," *European Journal of Operational Research*, vol. 195, pp. 186-204, 2009.

[3] H. Kunreuther and G. Heal, "Interdependent security," *Journal of risk and uncertainty*, vol. 26, pp. 231-249, 2003.

[4] B. Krebs, "Email Attack on vendor set up breach at target," *Krebs on Security, February*, vol. 12, 2014.

[5] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, pp. 186-192, 2013.

[6] V. A. Kumar, R. Rajaraman, Z. Sun, and R. Sundaram, "Existence theorems and approximation algorithms for generalized

network security games," in *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, 2010, pp. 348-357.

[7] A. Laszka, M. Felegyhazi, and L. Buttyan, "A survey of interdependent information security games," *ACM Computing Surveys (CSUR)*, vol. 47, p. 23, 2014.

[8] M. Lelarge, "Coordination in network security games: a monotone comparative statics approach," *Selected Areas in Communications, IEEE Journal on*, vol. 30, pp. 2210-2219, 2012.

[9] W. Saad, T. Alpcan, T. Basar, and A. Hjorungnes, "Coalitional game theory for security risk management," in *Internet Monitoring and Protection (ICIMP), 2010 Fifth International Conference on*, 2010, pp. 35-40.

[10] G. Theodorakopoulos, J.-Y. Le Boudec, and J. S. Baras, "Selfish response to epidemic propagation," *Automatic Control, IEEE Transactions on*, vol. 58, pp. 363-376, 2013.

[11] M. Ezhei and B. Tork Ladani, "Information Sharing vs. Privacy: A Game Theoretic Analysis," *Expert Systems with Applications*, vol. 88, pp. 327-337, 2017.

[12] M. Ezhei and B. Tork Ladani, "Interdependency analysis in security investment against strategic attacks," *Information Systems Frontiers*, pp. 1-15, 2018.

[13] H. Ogut, N. Menon, and S. Raghunathan, "Cyber Insurance and IT Security Investment: Impact of Interdependence Risk," in *WEIS*, 2005.

[14] X. Gao, W. Zhong, and S. Mei, "A game-theoretic analysis of information sharing and security investment for complementary firms," *Journal of the Operational Research Society*, vol. 65, pp. 1682-1691, 2014.

[15] X. Gao, W. Zhong, and S. Mei, "Security investment and information sharing under an alternative security breach probability function," *Information Systems Frontiers*, vol. 2, pp. 423-438, 2015.

زیرنویس‌ها

[1] **Security Investment**
[2] **Interdependency**
[3] **Target corporation**
[4] **Heating, Ventilation, and Air Conditioning**
[5] **Externality**
[6] **Game Theory**
[7] **Nash Equilibrium**
[8] **Social Optimum**
[9] **Social Planner**
[10] **Mechanism Design**
[11] **Information Security audit**
[12] **Certified accountants**
[13] **Certified Internet Auditor Professional**