ارائه معماری جدید برای بهبود همبسته‌سازی هشدار مبتنی بر مدل قابلیت

حدیث بابایی [*۱]، علی‌جبار رشیدی
۱- گروه امنیت اطلاعات، مجتمع ICT، دانشگاه صنعتی مالک اشتر، تهران، ایران
۲- دانشیار گروه مخابرات، دانشگاه صنعتی مالک اشتر، تهران، ایران
[*]**نویسنده مسئول:** Rashidi@mut.ac.ir

خلاصه

با توسعه‌ی گسترده‌ی اینترنت و سامانه‌های شبکه‌ای، تشخیص نفوذ به یک امر مهم برای تمام سازمان‌ها مبدل شده است. سامانه تشخیص نفوذ یک ابزار امنیتی است که سامانه‌های کامپیوتری و شبکه‌ها را، به‌منظور تشخیص و هشدار دهی در هنگام نفوذ، نظارت و رصد می‌کند؛ بنابراین به‌محض وقوع هشدارها، مدیر امنیتی سیستم یا سامانه‌های پاسخگویی خودکار می‌توانند، به‌منظور کاهش خسارات ناشی از حملات و فهمیدن رفتار آن‌ها، پاسخ سریعی به این حملات بدهند.

سامانه‌های تشخیص نفوذ فعلی از مشکلات شناخته‌شده بسیاری رنج می‌برند. درواقع سامانه‌های تشخیص نفوذ قدیمی در سطح حملات سطح پایین یا آنومالی کار می‌کنند و هشدارهای غلط و نامرتبط زیادی تولید می‌کنند. به‌منظور کشف ارتباط بین هشدارهای سامانه‌های تشخیص نفوذ و ایجاد دید سطح بالاتری نسبت به این هشدارها همبسته سازی هشدار پیشنهاد می‌شود. روش‌های مختلفی برای همبسته سازی هشدار ارائه‌شده است که یکی از آن‌ها همبسته سازی هشدار بر اساس مدل قابلیت است. این مدل قابلیت از قابلیت‌های به‌دست‌آمده توسط مهاجم به‌عنوان یک بلوک سازنده اصلی استفاده می‌کند و بر اساس آن الگوریتم‌هایی را برای همبسته سازی هشدار ارائه می‌کند. مدل قابلیت ارائه‌شده قادر به بررسی حملات فراموش‌شده است و نویددهنده‌ای برای ادغام هشدارها و همبسته سازی بهتر آن‌ها است.

کلمات کلیدی: حملات سایبری، همبسته سازی هشدار، مدل‌سازی قابلیت، سیستم تشخیص نفوذ

۱. مقدمه

نظارت و پایش امن شبکه‌ها، عمدتاً با استفاده از سامانه‌های تشخیص نفوذ صورت می‌گیرد. جریان رویدادهایی که توسط سیستم تشخیص نفوذ موردبررسی قرار می‌گیرند به دو گروه تشخیص آنومالی و تشخیص سوءاستفاده تقسیم‌بندی می‌شوند. در سامانه‌های تشخیص آنومالی، از اطلاعات گذشته در خصوص فعالیت سیستم و یا رفتارهای ویژه کاربران و برنامه‌ها، برای ساخت یک پروفایل مربوط به عملکرد نرمال سیستم استفاده می‌شود. سپس سامانه‌های تشخیص آنومالی در

[*] **Corresponding author: دانشجوی کارشناسی ارشد**
Email: h_babaie_1388@yahoo.com
[†] Intrusion Detection System(IDS)