عنوان مقاله:
رویکردی جدید مبتنی بر گراف حمله بیزی سببی و شباهت خصیصه ها برای همبسته سازی هشدارهای نفوذ و بازسازی سناریوهای حمله

محل انتشار:
بیست و یکمین کنفرانس مهندسی برق ایران (سال: 1392)

تعداد صفحات اصل مقاله: 8

نویسندگان:
فاطمه سادات میرتاج الدینی - *دانشگاه تربیت مدرس، دانشکده مهندسی برق و کامپیوتر*

مهدی آبادی

خلاصه مقاله:
در این مقاله، رویکردی جدید برای همبسته سازی هشدارهای نفوذ و بازسازی سناریوهای حمله پیشنهاد می شود که از دانش پس زمینه مدل شده در قالب گراف حمله بیزی سببی و شباهت خصیصه های هشدارها استفاده می کند. در هر گراف حمله بیزی سببی، گره ها و یال هاشرط های امنیتی، سوءاستفاده ها و روابط سببی میان آن ها را نمایش می دهند. به هر گره یک مقدار احتمالی نسبت داده می شود که احتمالسوءاستفاده از یک آسیب پذیری یا برقراری یک شرط امنیتی را نشان می دهد. در رویکرد پیشنهادی، ابتدا هشدارهای سطح پایین با نگاشت به گره های سوءاستفاده به فراهشدارها تبدیل می شوند. سپس در صورت امکان وابستگی های میان فراهشدارها بر اساس روابط سببی بین گره هایسوءاستفاده متناظر با آن ها در گراف حمله بیزی سببی کشف شده و یک سناریوی حمله ایجاد می شود. در صورت گم شدن تعدادی از هشدارها،سناریوی حمله با فرضیه سازی بازسازی می شود. اما در صورتی که وابستگی های میان فراهشدارها از طریق روابط سببی مدل شده در گراف حمله بیزی سببی قابل کشف نباشند، این وابستگی ها با توجه به شباهت خصیصه های هشدارها کشف می شوند. بنابراین، رویکرد پیشنهادی حتی در صورت عملکرد نامناسب سیستم های تشخیص نفوذ قادر است دید مناسبی از تلاش های مهاجم در اختیار مدیر امنیتی شبکه قرار دهد. نتایج آزمایش ها نشان می دهند که رویکرد پیشنهادی از صحت و تمامیت مناسبی برای همبسته سازی هشدارهای نفوذ و بازسازی سناریوهای حمله برخوردار است.

کلمات کلیدی:
فراهشدار، همبسته سازی، گراف حمله بیزی سببی، شباهت خصیصه، سناریوی حمله

لینک ثابت مقاله در پایگاه سیویلیکا: