عنوان مقاله:
اولویت بندی تهدیدها برای حملات چرخش براساس نظریه بازی ها

محل انتشار:
اولین کنفرانس ملی توسعه پایدار در علوم ومهندسی و فرهنگ ایرانی (سال: 1397)

تعداد صفحات اصل مقاله: 8

نویسندگان:
سینا دامی - *استادیار گروه کامپیوتر، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران*

رومین فرزانه - *دانشجوی کارشناسی ارشدITواحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران*

خلاصه مقاله:
مقدار اطلاعاتی که در سیستمهای کامپیوتری جمع آوری و ذخیره میشود، به سرعت در حال افزایش است. درعینحال حساسیت چنین اطلاعاتی اغلب برای هر دو مهاجمین خارجی و افراد مخرب داخلی با ارزش جلوه میکند. یکی از انواع پیشرفته حملات، استفاده از تکنیک چرخش است که از طریق آن مهاجمان یک تونل پخش فرمان از طریق دو یا چند میزبان برای رسیدن به هدف نهایی خود ایجاد میکنند. برای مقابله با این نوع حملات و جلوگیری از سواستفاده، انواع مختلفی از سیستمهای تشخیص نفوذ و سواستفاده ارایه شده است که هشدارهایی برای تهدیدهای مشکوک که ارزش بررسی پیگیری دارند، فراهم میکنند. با اینحال، در عمل، این سیستمها ممکن است تعداد زیادی هشدار کاذب تولید کند و زمان بررسی را تلف کنند. یک چالش مهم در تعیین اولویتبندی تهدیدها این است که دشمنان میتوانند از چنین رفتارهایی برای جلوگیری از تشخیص استفاده کنندبه ویژه با نصب حملات که هشدارهایی را به وجود میآورد که کمتر مورد بررسی قرار میگیرند. در این مقاله، ما اولویتبندی تهدیدها را با مخالفان سازگار با استفاده از بازی استاکلبرگ و روشی برای محاسبه اولویتبندی بهینه انواع هشدارها ارایه میکنیم که مسیرهای تشخیص داده شده براساس نمره تهدید را به عهده می گیرد. ما رویکردمان را با استفاده از مجموعه داده های آزمایشی که شامل شبکه ای واقعی است که توسط پروبهایی که در یک سازمان بزرگ قرار گرفته اند، ارزیابی میکنیم که دقت بالا و عملکرد آنها را در برابر الگوریتم های مرتبط نشان میدهد.

کلمات کلیدی:
اولویت بندی تهدیدها ، حملات چرخش، هشدار کاذب، نظریه بازی ها