**دانشگاه شهید بهشتی**

**دانشکده مهندسی و علوم کامپیوتر**

**اطلاعیه دفاع**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | **نام دانشجو: مریم رعیت علی‌آبادی**  **نام استاد راهنما:**  **دکتر رامک قوامی زاده**  **دکتر مجتبی وحیدی اصل**  **نام استاد مشاور:** | |
| **مقطع: دکترا** | **گرایش: نرم افزار** | | | **رشته: مهندسی کامپیوتر** |
| **تاریخ:۲۰ تیر** | | | **نوع دفاع:**   * **دفاع رساله دکترا** | |
| **ساعت: ۱۲-۱۵** | | |
| **مکان: آنلاین** /http://194.225.24.96/defa-computer-3 | | |
| **عنوان: ارائه روشی به منظورکاوش مشخصات مبتنی‌بر تحلیل پویا برای ایمن‌سازی سامانه‌های سایبر‌فیزیکال** | | | | |
| **داوران داخلی: دکتر حسن حقیقی و دکتر علیرضا شاملی** | | **داوران خارجی: دکتر رامتین خسروی و دکتر مهدی کارگهی** | | |
| **چکیده**  امروزه، سامانه‌‌های سایبرفیزیکال به‌طورگسترده در زیرساخت‌های مهم امنیتی به‌کارگرفته شده‌اند. از آنجا که در بسیاری از موارد، این سامانه‌ها وظایفی حیاتی به‌عهده دارند، اهدافی بالقوه برای حملات سایبری هستند. این امر ایجاد روش‌های تشخیص حمله برایسامانه سایبرفیزیکال را به یک ضرورت تبدیل می‌کند. اما، داشتن ویژگی‌های خاص، همچون نیازهای بلادرنگ و منابع (حافظه و توان محاسباتی) محدود، ساختِ سامانه‌ی تشخیص حمله را برای آن‌ها چالش‌برانگیز می‌کند. تحقیقات نشان داده‌است که با درنظرگرفتن توصیف صوری سامانه، تشخیص حمله‌ها به صورت کارآمدتری انجام‌پذیر است. راهکارهای موجود برای کاوشِ مشخصات (اجزای تشکیل دهنده توصیف صوری)، بر مبنای داده‌ها و رویدادهای سامانه عمل می‌کنند و پارامتر زمان را در نظر نمی‌گیرند. این درحالی است که پارامتر زمان در اکثر سامانه‌های سایبرفیزیکال از مهم‌ترین عوامل است. از این ‌رو، در نظر گرفتن "زمان" درکنار داده‌ها و رویدادها، می‌تواند به‌طور قابل‌ملاحظه‌ای بر میزان تشخیص حملات سایبری تاثیرگذار باشد. علاوه‌بر‌این، شناسایی حملات به جمع‌آوری اطلاعاتِ مربوط به عملکردِ داخلیِ سامانه نیاز دارد که می‌تواند از نظر زمانی و حافظه‌ای، فرآیندی پرهزینه باشد. بدیهی است که هرچه کاوش مشخصات با ریزدانگی و دقت بالاتری رخ ‌دهد، امکان تشخیص حمله نیز بالاتر می‌رود و به همان نسبت هم هزینه بیشتری را به سامانه تحمیل می‌کند که در اکثر اوقات این هزینه فراتر از میزان منابعِ در‌اختیار هستند. در این رساله، سه رویکرد را برای کاوشِ مشخصاتِ سامانه‌های سایبرفیزیکال ارائه می‌دهیم که در عینِ داشتنِ دقتِ زیاد از محدودیت‌های سامانه نیز فراتر نمی‌روند. رویکرد آرتینالی از طریق تجزیه و تحلیل پویای سامانه سایبر فیزیکال مشخصات آن‌را استخراج کرده و دراختیار سامانه تشخیص حمله میگذارد. نوآوری اصلی آرتینالی درنظر گرفتن تاثیر زمان بر روی مشخصه های سامانه سایبرفیزیکال در هنگام استخراج آنهاست. رویکرد آرتینالی++ به‌شکل پویا مشخصات را در امتداد چهار بعد داده، رویداد، زمان و حرکت فیزیکی برای سامانه سایبرفیزیکال با اندازه و پیچیدگی متنوع استخراج کرده و از آن، برای تشخیص ‌حمله استفاده می‌کند. رویکرد آرتینالی# قابلیت مقیاس‌پذیری را به سامانه‌‌یِ تشخیصِ حمله اضافه می‌کند. این رویکرد مجهز به یک روش فراکدگذاری هوشمندِ مبتنی‌بر شبکه بیزی است که با ایجاد حداقل سربارِ زمان و حافظه، حداکثر پوشش حمله‌ را در محدوده‌یِ منابعِ موجود در سامانه‌‌یِ سایبرفیزیکال تضمین می‌نماید. ما سامانه‌یِ تشخیص حمله را با استفاده از سه رویکرد پیشنهادی برای سه سامانه سایبرفیزیکال، شامل متر هوشمند، دستگاه پزشکی هوشمند و هواپیمای بدون سرنشین پیاده‌سازی نموده و دقت و سربار آن‌ها را دربرابر حملات شناخته‌شده و ناشناحته ‌اندازه‌گیری کردیم. نتایج آزمایشها نشان داده ‌است که آرتینالی نرخ مثبت کاذب و منفی کاذب در تشخیص حمله را به ترتیب تا ٪۳۰.۷۵ و۹۳.۴۰٪ نسبت به سایر ابزارهای کاوش مشخصات کاهش می‌دهد. همچنین، آرتینالی++ نرخ مثبت و منفی کاذب را به‌ترتیب تا ۱۹.۵٪ و۱۴.۳٪ برای سامانه‌های پیچیده نسبت به آرتینالی بهبود می‌بخشد. آرتینالی# نیز با حفظ دقتِ تشخیصِ حمله‌ی بیشینه (۹۸٪)، میزانِ سربارِحافظه و زمان را به‌ترتیب، تا ۵۲٪ و ۶۹٪ کاهش می‌دهد. | | | | |