**دانشگاه شهید بهشتی**

**دانشکده مهندسی و علوم کامپیوتر**

**اطلاعیه دفاع**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **نام استاد راهنما:** آقای دکتر علیرضا شاملی سندی  **نام استاد مشاور:** | | | **نام دانشجو:** آقای پویا پاکشاد | |
| **مقطع:** کارشناسی ارشد | **گرایش:** نرم افزار | | | **رشته: مهندسی کامپیوتر** |
| **تاریخ:** 28/04/1400 | | | **نوع دفاع:**   * **دفاع پروپوزال □** * **دفاع پایان نامه** ◼ * **دفاع رساله دکترا □** | |
| **ساعت:** 17:00 الی 19:00 | | |
| <http://194.225.24.96/defa-computer-4> **مکان:** | | |
| **عنوان:** ارائه يك پيشگوي آزمون امنيتي مبتني بر ويژگي‏هاي امنيتي استخراج‏شده از كدبرنامه | | | | |
| **داوران داخلی:** دکتر مجتبی وحیدی اصل | | **داوران خارجی:** دکتر حمیدرضا شهریاری | | |
| **چکیده:**  امروزه، یکی از مهم‏ترین چالش‏ها در حوزه امنیت نرم‏افزار مسئله‏ی شناسایی و کشف آسیب‏پذیری‏های امنیتی است. با افزایش اعتماد به عملکرد درست سیستم‏های رایانه‏ای، شناسایی و از بین بردن نقاط آسیب‏پذیر در کدمنبع برنامه نرم‏افزاری از اهمیت بیشتری برخوردار شده‏ است. پیشگویی مکان‏هایی از کدمنبع که بالقوه آسیب‏پذیر هستند به عنوان یک مرحله پیشین برای ارزیابی آسیب‏پذیری می‏تواند بسیار موثر باشد. به‏ عنوان مثال می‏تواند به محققان‏امنیتی یا آزمون‏گر نفوذ برنامه کمک کند تا زمان و تلاش خود را در جایی از برنامه که بیشتر مورد نیاز است قرار دهند. روش‏های بسیاری برای تحلیل و کشف آسیب‏پذیری در برنامه‏های نرم‏افزاری ارائه شده است. در این‏ پژوهش، برای شناسایی توابع بالقوه آسیب‏پذیر برنامه نرم‏افزاری یک پیشگوی آزمون امنیتی عمومی و قابل‏توسعه پیشنهاد می‏کنیم. پیشگوی ‏آزمون با استفاده از روش‏های یادگیری‏ماشین و استخراج ویژگی‏های امنیتی از کد برنامه نرم‏افزاری به عنوان معیارهایی متفاوت از آنچه تاکنون در روش‏های پیشین ارائه‏شده بود، تلاش می‏کند تا داده‏های مورد نیاز برای ایجاد مدلی دقیق‏تر برای پیش‏بینی آسیب‏پذیری‏های بالقوه موجود در کدمنبع برنامه را تولید کند. در مدل یادگیرنده پیشگوی آزمون، با استفاده از آسیب‏پذیری‏های واقعی از پیش ‏شناخته‏شده، تلاش‏شده است تا نوع حملات امنیتی منجر به وقوع آسیب‏پذیری موجود در برنامه با دقتی مناسب تشخیص داده شود. بنابراین پیشگوی آزمون امنیتی در مرحله نخست توابع بالقوه آسیب‏پذیر برنامه را با دقتی به مراتب بهتر از روش‏‏‏های پیشین و نوع آسیب‏پذیری موجود در تابع برنامه را نیز شناسایی می‎نماید. دقت و صحت روش پیشنهادی برای شناسایی آسیب‏پذیری در این پژوهش با روش‏های پیشین مورد مقایسه قرار گرفته است. نتایج تجربی در 5 پروژه واقعی نشان داده ‏است که پیشگوی آزمون امنیتی پیشنهادی می تواند با شناسایی 20% از توابع به عنوان توابع بالقوه آسیب‏پذیر، 94% از توابع واقعا آسیب‏پذیر را درست و 86% نوع آسیب‏پذیری توابع شناسایی‏شده را بطور صحیح پیشگویی نماید. | | | | |