بسمه تعالی زمان نصب در تابلوی اعلانات:

🞎 دفاع از رساله دکتری 🞎 سمينار عمومي (Colloquium)

**◼** دفاع از پایان‌نامه کارشناسی‌ارشد  **🞎 سمينار تخصصي (Seminar)**

 **🞎 سمينار تخصصي و مشورتي (Informal Seminar)**

###### عنوان : **تشخیص بدافزارهای دگردیس با استفاده از آنتروپی رفتاری**

سخنران : کامبیز واحدی

**چکیده:** بدافزارهای دگردیس با تغییر امضاء بدافزار با بهره‌گیری از روش‌های مبهم سازی کد، مانع از تشخیص بدافزارها توسط روش‌های شناسایی مبتنی بر امضای بدافزار می‌گردند. روش‌های جدید شناسایی بدافزارهای دگردیس مبتنی بر تحلیل آماری کد بدافزار و اندازه‌گیری تشابه بین کدها وضعیت به مراتب بهتری نسبت به ابزارهای شناسایی مبتنی بر امضاء دارند اما در مقابل روش‌های مبهم سازی کد ازجمله اضافه نمودن کدهای زائد مشابه کدهای برنامه‌های سالم و جایگزینی دستورالعمل با دستورالعمل معادل کارایی لازم را ندارند. در این پژوهش روشی متکی بر تجزیه و تحلیل رفتار و فعالیت فایل اجرایی، جهت بهبود تشخیص بدافزارهای دگردیس شده ارائه شده است. این فرایند شامل دو مرحله است؛ ابتدا، تحلیل و درک رفتار فایل در زمان اجرا و به دست آوردن الگوی رفتاری آن و مرحله بعد، مقایسه الگوهای رفتاری فایل‌های بدافزار با فایل نمونه برای تعیین تشابه بین آنها. در مرحله تحلیل و درک رفتار فایل، بدافزار در محیط نظارتی همانند سندباکس اجرا می‌شود و سپس شاخصه‌های رفتاری مخرب آن استخراج می‌گردد. وضعیت این شاخصه‌های رفتاری در کنار هم یک الگوی رفتاری از بدافزار را می‌سازد. با این کار بانکی از الگوهای رفتاری بدافزارها تهیه می‌گردد. مرحله دوم، اندازه‌گیری شباهت بین بدافزارهای ثبت‌شده در بانک تهیه‌شده در مرحله اول با فایل‌های نمونه برای تعیین میزان شباهت بین آنها است. نتایج تجربی به دست آمده نشان می‌دهد این روش پیشنهادی با اندازه‌گیری تشابه الگوهای رفتاری، تشخیص بدافزارهای دگردیس شده را به میزان چشمگیری ارتقاء داده و مقدار مثبت کاذب را به 0% رسانده است.

## **زمان برگزاری: 17/06/1395 – ساعت 16:00**

#### **مکان برگزاری: دانشکده مهندسی و علوم کامپیوتر**