بسم الله الرحمن الرحیم

جلسه ارائه هفتگی آزمایشگاه امنیت داده و شبکه

مروری بر روش‌های فعالانه کشف روت‌کیت در سیستم عامل ویندوز

سیده‌عاطفه موسوی

زمان: شنبه، ۱۵ اسفندماه، ساعت ۹:۰۰

مکان: دانشکده کامپیوتر، آزمایشگاه امنیت داده و شبکه

روت‌کیت‌ها مؤلفه‌ای از حدود ۱۰٪ از بدافزارهای امروزی هستند که با هدف قرار دادن سیستم‌عامل مقاصد مخرب بدافزار را اعم از اقامت پنهان، جاسوسی، گروگیری و ... محقق می‌سازند. در سال‌های اخیر استفاده از این مؤلفه‌ها افزایش یافته و به دلیل فرض اولیه اعتماد به سیستم‌عامل در اغلب ضدبدافزارهای موجود، فرایند کشف آن‌ها با چالش روبرو بوده است. روش‌های مختلفی برای کشف روت‌کیت‌ها پیشنهاد و پیاده‌سازی شده است که اغلب منفعلانه به تعریف الگوهای رفتاری دیده شده از سوی روت‌کیت‌ها پرداخته‌اند. در انتهای دیگر طیف دسته‌ای از روش‌ها ، سعی دارند زیرساخت‌های پیشگیرانه‌ای را در قبال نفوذ روت‌کیت‌ها در سیستم تعبیه کنند. در سال‌های اخیر اما رویکردهای میانی نسبتا فعالانه‌ای نیز مطرح شده اند که به بررسی فعال نقاط مستعد نفوذ در سیستم‌عامل پرداخته‌اند. این ارائه به معرفی اولیه موضوع روت‌کیت‌ها و بررسی ابعاد مختلف این پژوهش‌های فعالانه می‌پردازد.

شرکت در این جلسه برای تمامی دانشجویان علاقه‌مند آزاد است.