



انجمن رمز ایران  
Iranian Society of Cryptology



## سیستم‌های کامپیوتری مورد اعتماد: چالش‌های نو و راهکارهای پیش رو

با ورود سیستم‌های رایانه‌ای به بخش‌های مختلف صنعتی، آزمایشگاهی، پزشکی و به‌خصوص سازمان‌های حیاتی و حساس کشور، تامین امنیت این گونه سیستم‌ها اهمیت مضاعفی یافته است. با این حال محدود انگاشتن مساله امنیت سیستم‌های کامپیوتری به چند مقوله خاص و بیشتر پرداخته شده (از قبیل حملات نفوذ از طریق شبکه، تشخیص نفوذ با استفاده از پروفایل فراخوانی‌های سیستمی برنامه و ...) موجب شده است که در بهترین حالت مدیران و کارشناسان حوزه امنیت سازمان‌ها وظیفه خود را تنها به راهکارهای امنیتی خاصی چون استفاده از رمزنگاری، الزام به استفاده از نرم افزارهای سیستمی بومی، استفاده از ضد بدافزار و دیوار آتش، و انجام مستمر تست های نفوذ برنامه‌های تحت وب و موارد نظیر آن محدود ببینند.

این در حالی است که از نقطه نظر سیستمی، امنیت یک سیستم رایانه‌ای ابعاد متعدد دیگری نیز دارد که کمتر به آن‌ها پرداخته شده است. مواردی نظیر امنیت بخش‌های مختلف سیستم عامل از مدیریت حافظه تا زمان‌بند، حملات وارد به سیستم از طریق ثابت‌افزارها (Firmware)، امنیت بخش‌های مرتبط با مجازی‌سازی، اهمیت فناوری‌های سخت‌افزاری در تامین امنیت، حملات وارد بر خود نرم‌افزارها و سخت‌افزارهای امنیتی، از جمله این موارد هستند. در حقیقت به نظر می‌رسد بدون داشتن یک تصویر جامع‌تر از امنیت سیستم‌های کامپیوتری، تصمیم‌گیری درست در هر دو حوزه سیاست‌گذاری و عملیات نمی‌تواند به صورت صحیح و موثر انجام شود، و آنچه بدون توجه به این مطالب به دست می‌آید عملاً یک توهم از امنیت خواهد بود که از تصور ناامنی بسیار خطرناک‌تر است.

در این کارگاه چالش‌های تامین امنیت در لایه‌های مختلف سیستم (از پایین‌ترین دیوایس‌های نصب شده روی مادربورد، ثابت‌افزارها، نرم‌افزارهای سیستمی اعم از سیستم عامل و ناظر) به همراه جدیدترین حملات مطرح شده در هر لایه مرور شده و برخی راهکارهای موجود در این باره بررسی می‌گردند. در انتهای کارگاه انتظار می‌رود شرکت‌کنندگان تصویر نسبتاً کامل‌تری از مسائل مطرح در امنیت سیستم دریافت کنند و با چالش‌ها و حملات به‌روز شده‌ای در این باره آشنا شوند. محققین و دانشجویان تحصیلات تکمیلی نیز می‌توانند با برخی از موضوعات تحقیقاتی این حوزه آشنا شوند.