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

## Trusted Computing Systems: Challenges and Potential Solutions


**چکیده فارسی:**

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 سخت افزاری در تامین امنیت، حملات وارد بر خود نرم افزارها و سخت افزارهای امنیتی، از جمله این موارد هستند. در حقیقت به نظر می رسد بدون داشتن یک تصویر جامع‌تر از امنیت سیستم‌های کامپیوتری، تصمیم گیری 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 می آید عملا یک توهم از امنیت خواهد بود که از تصور ناامنی بسیار خطرناک‌تر است.

در این کارگاه چالش های تامین امنیت در لایه های مختلف سیستم (از پایین ترین دیوایس های نصب شده روی مادربورد، ثابت‌افزارها، نرم افزارهای 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 می گردند. در انتهای کارگاه انتظار می رود شرکت کنندگان تصویر نسبتا 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 می توانند با برخی از موضوعات تحقیقاتی این حوزه آشنا شوند.

- سر فصل مطالب کارگاه:

بخش اول: طرح موضوع به صورت عمومی و بررسی های موردی به جهت ورود به بررسی جامع

| | عنوان | محتوا | زمان (دقیقه) |
|---|---|---|---|
| ۱ | مقدمه و تبیین مساله | | ۵ |
| ۲ | تخیلات امنیتی: ۵ تصور نادرست درباره یک سیستم معتمد<br>- برای تامین امنیت سیستم‌های وارداتی کافی است آزمایشگاه‌های تست سخت افزار را تاسیس کرده و برنامه‌های متن باز تهیه کنیم.<br>- برای تامین نرم افزار امن کافی است برنامه های خریداری شده (اعم از متن باز یا بسته) را در یک آزمایشگاه مستقل برای نبود حفره های امنیتی در آنها تست کرد.<br>- برای داشتن یک سیستم عامل بومی امن کافی است کد یک سیستم عامل را تولید کنیم یا از نبود تروجان در یک سیستم عامل متن باز مطمئن شویم.<br>- برای حفاظت از داده های افراد و سیستم های با داده های حساس کافی است همه داده ها و یا کل دیسک را رمزنگاری کنیم. در این صورت حتی اگر دیسک دزدیده شود چیزی به دست دشمن نمی افتد.<br>- اینکه مدیریت توان سیستم‌های رایانه‌ای چطور باشد ارتباط چندانی به کارشناس امنیت سازمان ندارد مگر اینکه حمله کننده بخواهد سیستم ما را خاموش و روشن کند! | آیا می دانستید برنامه‌ها ممکن است بعد از کامپایل کارهایی انجام دهند که در کد مرجع آن‌ها وجود نداشته است؟<br>آیا می دانستید کدهای اسمبلی یک برنامه نیز ممکن است به شما دروغ بگویند و هیچ نشانی از خطرات متوجه سیستم شما نداشته باشند؟ به عنوان مثال:<br>Compiler/Managed-code/Microcode rootkits<br>آیا می دانستید که یک برنامه می تواند بدون دستکاری داده ها یا کد بسیاری از سیستم عامل ها به صورت کاملا قانونی ولی مخفی سی پی یو بدزد؟ (Scheduler-attacks)<br>آیا می دانستید که اطلاعات شما در حافظه سیستم هم در خطر هستند؟( Memory attacks, Cold boot)<br>آیا می دانستید لپ تاپ با دیسک رمزنگاری شده می تواند در معرض خطر افشای محتویات قرار گیرد، بی آنکه صاحب آن متوجه سرقت اطلاعاتش شود؟ (Evil-maid attack)<br>آیا می دانستید چگونه روت کیت های خاصی با استفاده از استاندارد مدیریت توان در سیستم شما اجرا می شوند؟ (ACPI attacks) | ۲۵ |

| | | | |
|---|---|---|---|
| ۳ | خواستن توانستن است!<br>تامین امنیت در لایه نرم افزار سطح کاربر | -انواع محیط های مدیریت شده<br>- جایگاه این محیط ها در رویکرد دفاعی MTD<br>- معایب امنیتی | ۱۰ |
| ۴ | امنیت در سیستم عامل | - معماری عمومی سیستم عاملها برای دیدن حملات در لایه های مختلف<br>- اشاره کوتاه بخش های بیشتر شناخته شده از سیستم عامل برای کارشناسان امنیتی<br>✓ کنترل دسترسی<br>✓ فراخوانی های سیستمی<br>✓ اشیاء و اشاره گرهای هسته<br>- اشاره به بخش های کمتر پرداخته شده از امنیت سیستم عامل<br>✓ حملات مرتبط با حافظه<br>✓ حملات مرتبط با زمان بند<br>✓ حملات مرتبط با مدیریت توان<br>✓ حملات جدید دیگری چون Iago attack | ۱۵ |
| ۵ | حفره های مجازی:<br>امنیت ناظر | - مرور سریع انواع مجازی سازی<br>- ایده های مبتنی بر مجازی سازی جهت دفاع از برنامه در قبال پلت فرم نامعتمد<br>- ایده های مبتنی بر مجازی سازی جهت دفاع از پلت فرم در قبال برنامه نامعتمد<br>- خطرات متوجه خود فناوری مجازی سازی | ۲۰ |
| ۶ | پرسش و پاسخ | پرسش و پاسخ | ۵ |

بخش دوم :

| | عنوان | محتوا | زمان |
|---|---|---|---|
| ۱ | نه سخت و نه نرم:<br>امنیت در لایه ثابت‌افزار (Firmware) و دیوایس های جانبی | - معرفی ثابت‌افزار<br>- جریان بوت در سیستم های امروزی و حملات وارد بر آن<br>- حباب های باینری (Binary blobs)<br>- قابلیت های موجود در option-ROMها<br>- تامین امنیت دیوایس ها<br>- حملاتی مانند Sipi attack و GPU-assisted | ۲۰ |
| ۲ | الماس های سخت افزاری:<br>امنیت در لایه سخت افزار | - کدهای hard-wiredدر قبال میکروکدها<br>- افزونه MPX<br>- افزونه SGX<br>- اهمیت انتخاب معماری سخت افزار مناسب در امنیت | ۲۵ |
| ۳ | آن را که یافت می نشود:<br>مرور محصولات قابل اعتماد | - معرفی اجمالی TPM ها و معایب امنیتی در کنار مزایا<br>- لپ تاپ های متن باز<br>- سیستم عامل های امن | ۲۰ |
| ۴ | معرفی نهادها و رویه های اعتماد سیستمی در چند کشور | - مرور قانون فدرال مدیریت امنیت اطلاعات<br>- جایگاه امنیت سیستم در فریم ورک بهبود امنیت فضای سایبری موسسه ملی استاندارد و تکنولوژی آمریکا<br>- رویکرد اخیر مهندسی امنیت سیستم ها در موسسه ملی استاندارد و تکنولوژی ایالات متحده (در مقابل رویکرد دفاع پیرامونی پروژه انیشتین) | ۱۵ |
| ۵ | پرسش پاسخ | پرسش پاسخ | ۱۰ |