
بسم الله الرحمن الرحيم

سمینار

عنوان

# روش‌های جلوگیری از درج تروجان‌های سخت‌افزاری

نگارنده:

فهرست مطالب

عنوان | صفحه

## فهرست اشکال

## چکیده

با توجه به افزایش تقاضا برای ادوات الکتریکی و در راستای کاهش هزینه‌ها، درخواست‌ها برای ساخت این قطعات به سوی مراکز کم هزینه و بیگانه در حرکت است که این کار مدارهای مجتمع را، در برابر تغییرات و فعالیت حمله کنندگان آسیب‌پذیر می‌کند. یکی از این تغییرات بدخواهانه و عمدی در مدارات الکترونیکی، تروجان سخت‌افزاری می‌باشد. تروجان سخت افزاری مداری است که با هدف از کارانداختن وسیله یا کسب اطلاعات حساس آن در زمان مورد نیاز در طرح اصلی قرار داده می‌شود. لذا، با توجه به قدرت نفوذ بالای این حمله، شناخت انواع تروجان‌های سخت‌افزاری و راه‌های کشف و مقابله با آن از اهمیت ویژه‌ای برخوردار می‌باشد. در این سمینار، به مطالعه وبررسی انواع تروجان‌های سخت‌افزاری و روش‌های کشف و مقابله با آن‌ها پرداخته می‌شود.



**کلمات کلیدی:** تشخیص، حملات، تروجان سخت افزاری، مدارات.

# فصل اول

# مقدمه

## ۱-۱- مقدمه

امروزه با توجه به پیشرفت فناوری مدارات و سخت‌افزارهای به کار رفته در اکثر سیستم‌ها روند رو به جلویی را به سمت افزایش مقیاس و اندازه مدارات شاهد بوده‌ایم، امر باعث می‌شود تا اجزای به کار رفته در مدارات نسبت به قبل ریزتر و کوچک‌تر شوند که این مهم مزیت‌های بسیار زیادی دارد مثلا می‌توان مدارات زیادی را در یک فضای محدود جاسازی کرد، اما با تمام این مزیت‌ها می‌تواند در برخی موارد خطرساز باشد. یکی از چالش‌های این موضوعات، مسئله برقراری امنیت مدارات به کار رفته در سیستم‌های سخت افزاری است، امروزه بحث امنیت یکی از موضوعات مهم و چالش برانگیز در این سیستم‌ها است چرا که همین طور که با پیشرفت فناوری همواره شاهد افزایش تراکم مدارات استفاده شده در سیستم ها هستیم به همان میزان آسیب پذیری این مدارات نیز بیشتر می‌شود و نباید از آنها غافل شویم. یکی از این تهدیدات تروجان‌های سخت‌افزاری هستند که به علت ماهیتی که دارند تشخیص آنها به شدت دشوار است و در برخی موارد شاید غیرممکن باشد. داستان از آن‌جا آغاز می‌شود که در زمان‌های بسیار دور، سربازان یونانی پس از ده سال تلاش برای تسخیر شهر تروا، درنهایت دست از محاصره شهر برداشتند و در پشت سر خود یک اسب عظیم چوبی را در ظاهر به‌عنوان پیشکش برجای گذاشتند .تروجان‌ها (نام اهالی تروا) خراج زیبا و باابهت را به داخل شهر کشاندند و آن‌جا بود که گروهی از سربازان یونانی نیمه‌شب از داخل اسب چوبین بیرون آمدند و دروازه‌های شهر را به روی افراد خود گشودند و به‌سادگی بر شهر خفته پیروز شدند. امروز و پس از گذشت سه هزار سال از آن اتفاق، «تروجان» به نرم‌افزار کوچک و به‌ظاهر بی‌آزاری اطلاق می‌شود که در واقع حاوی کدهای آسیب‌زننده است. شرکت‌های فعال در زمینه امنیت همواره در حال بررسی و آزمون این تهدیدات هستند. حال نوع جدیدی از تروجان‌ها به‌نام «تروجان سخت‌افزاری» نگاه‌ها را به سمت خود جلب می‌کند و به‌نظر می‌رسد مقابله با آن به‌مراتب سخت‌تر از نمونه نرم‌افزاری است. برای درک ماهیت یک تروجان سخت‌افزاری می‌توان دقیقاً به‌نام آن توجه کرد؛ تغییر کوچکی در یک مدار یک‌پارچه که ممکن است به ایجاد اختلال در عملکرد تراشه منجر شود. با یک طراحی مناسب، یک نفوذگر باهوش می‌تواند تراشه را به گونه‌ای تغییر دهد تا در لحظه حساس عملکرد خود را از دست بدهد یا سیگنال‌های اشتباه ایجاد کند. همچنین، فرد مهاجم قادر خواهد بود تا با ایجاد یک در پشتی کلیدهای رمزگذاری یا رمزهای عبور را شنود یا اطلاعات داخلی تراشه را به خارج از مجموعه ارسال کند. دلایل محکم زیادی برای نگرانی در این زمینه وجود دارد.

بنابراین، تروجان‌ها معمولا به صورت یک بمب ساعتی عمل می‌کنند و هنگامی که در یک سیستم قرار می-گیرند وضعیتی به صورت خاموش و آرام دارند و به محض برقراری یک شرط یا یک رخداد از حالت خاموش در آمده و به حالت فعال تغییر وضعیت می‌دهند. هدفی که این تروجان‌ها دنبال می‌کنند خرابکارانه است و بیشتر به منظور اهداف جاسوسی نظیر نشت اطلاعات محرمانه به محیط خارج و یا تخریب مدارات است. روش‌های زیادی برای حل این مشکل ارائه شده است، روش‌های سنتی نظیر مهندسی معکوس که زیرمجموعه‌ای از روش‌های تخریبی به شما می‌آید یکی از پرهزینه‌ترین روش‌هاست که توجیه اقتصادی ندارد و در اکثر موارد زمان بر است. در ادامه چالش‌های مهم امنیتی را لیست کرده‌ایم:

۱-انتخاب یک مدل مناسب برای تشخیص تروجان زمانی که تروجان در حالت خاموش قرار دارد.

۲-یکی از مهم‌ترین چالش‌ها وجود تغییرات فرآیندی است و اینکه یکی از علت‌های تشخیص دشوار تروجان‌ها همین علت است زیرا در غیر اینصورت حتی با وجود یک تروجان به راحتی با مشاهده‌ی تغییرات، تروجان قابل تشخیص خواهد بود. اما بحثی که مطرح است این است که تفاوت بین تغییرات فرآیندی و تغییرات تروجان قابل تمایز نیست. به همین منظور به فکر توصیف ویژگی‌های فیزیکی هر گیت از مدار افتادند. از قبیل طول موثر کانال، عرض گیت و ویژگی‌های ظاهری نظیر تاخیر و توان.

۳-بررسی میزان حساسیت فعالیت تروجان در برابر پارامترهای سمت کانال

٤-اندازه گیری نویز

بنابراین، استفاده از تجهیزات الکترونیکی در زندگی روزمره‌ی افراد بطور اجتناب ناپذیری گسترش یافته است. بیشتر تراکنش‌های اطلاعات مالی و شخصی افراد به راحتی از طریق کامپیوترهای شخصی یا استفاده از اینترنت روی موبایل فراهم شده است. بخش اعظم پردازش اطلاعات از طریق پردازنده‌های خاص منظوره یا حتی عام منظوره صورت می‌گیرد در نتیجه امنیت این تراشه‌ها در حفظ امنیت داده افراد بسیار حایز اهمیت است. یکی از نقاط ضعف امنیتی تراشه‌ها، نفوذ مهاجم به سیستم در فرآیند طراحی تراشه یا پروسه‌ی ساخت آن است و این باعث نگرانی‌های جدی برای سیستم‌های نظامی، اقتصادی و حتی خانگی شده است. همان گونه که در طراحی و کاربرد نرم‌افزارهای تحت وب امکان نفوذ بدافزارها از قبیل تروجان‌های نرم‌افزاری وجود دارد، از دید سخت‌افزاری نیز می‌توان هسته‌های سخت‌افزاری در حین پروسه‌ی ساخت در درون تراشه‌ها قرار داد که به صورت یک تروجان در حین کارکرد تراشه نقش بازی کند. همانطور که قبلا بیان کردیم تروجان سخت‌افزاری یک مدار اضافی مخرب است که به همراه مدار اصلی و با هدف خاصی پیاده‌سازی می‌شود و می‌تواند عملکرد سخت‌افزار اصلی را تحت تاثیر قرار دهد.

متاسفانه آشکارسازی اجزای جاسازی شده یعنی تروجان‌ها به دلایل زیر مشکل است:

اندازه‌های نانومتری ICها و پیچیدگی سیستم‌ها، آشکارسازی تروجان‌ها را توسط بازدید سطحی تراشه و روش مهندسی معکوس، سخت و پرهزینه کرده است. علاوه بر این روش مهندسی معکوس مخرب است و تضمین نمی‌کند که ICهایی که مورد بازبینی دقیق قرار گرفته‌اند، از تروجان محفوظ هستند. مدارهای تروجان به این صورت طراحی شده‌اند که در شرایط خیلی خاص فعال شوند و این باعث می‌شود که فعالسازی و آشکارسازی آنها، با استفاده از شرایط تصادفی، سخت باشد. علاوه بر این روش‌های خودکار تولید الگوی تست استفاده شده در صنعت، برای پیدا کردن نقص‌ها، در شرایط بدون تروجان عمل می‌کنند. بنابراین الگوریتم‌های ATPG موجود نمی‌توانند تروجان را فعال‌سازی و آشکار کنند، مگر اینکه به صورت مناسبی برای آشکارسازی تغییر پیدا کنند. برای توسعه دادن روش‌های طراحی شده برای بهبود ضریب اطمینان IC، نیاز است که ابتدا به طور جامع تروجان‌ها دسته‌بندی شوند. دسته‌بندی تروجان در این فصل بررسی خواهد شد. معیار اصلی این طبقه‌بندی از روی ویژگی‌های پارامتری تروجان‌ها ناشی شده است که شامل ویژگی‌های فیزیکی، فعال‌سازی و عملکردی آنهاست. صنعت میکروالکترونیک نقش زیادی در ارتباطات و اطلاعات محرمانه و نیز مدیریت و کنترل تجهیزات بازی می‌کند. این نوع از اتوماسیون مبتنی بر میکروالکترونیک، سیستم‌ها را نسبت به حملات، آسیب‌پذیر کرده است. مهاجم‌های نرم‌افزاری برای امنیت، به خوبی شناخته شده هستند و تکنیک‌هایی برای مقابله با آنها پیشنهاد و پیاده‌سازی شده است؛ ولی حضور مهاجمان سخت‌افزاری در حوزه امنیت پیشینهی زیادی ندارد و حتی لایه‌های امن نرم‌افزاری را تحت تاثیر قرار داده است.

توجه به تروجان‌های سخت‌افزاری از دو دیدگاه اهمیت دارد:

**تمرکز کمپانی‌های ساخت مدارهای مجتمع**: با توجه به فشارهای اقتصادی جهانی، مراکز ساخت ادوات الکترونیکی در سراسر جهان گسترش یافته و در راستای کاهش هزینه‌ی تولید این ادوات، زنجیره‌های تأمین IC به سرعت به سوی مکان‌های کم هزینه در حال حرکت هستند و در این راستا، در پروسه‌ی تولید سیستم‌ها، اعتماد به مراکز نامطمئن، ممکن است خطرات جبران ناپذیری را به بار آورد.

**برون سپاری طرح‌های بزرگ به طراحان مختلف**: در طرح‌های بزرگ، برای ساده کردن، کم هزینه کردن و بالابردن سرعت، کار تقسیم‌بندی می‌شود و با تقسیم‌بندی طرح، طراحان مختلف ممکن است حین اجرای طرح مدار مخربی را برای مقاصد بعدی روی طرح مربوط به خود پیشبینی کند. بنابراین کارفرمای اصلی برای اطمینان، باید طرح را مورد بازنگری قرار دهد.

در آخر این را بیان می‌کنیم که، مقابله با تهدید تروجان‌های سخت‌افزاری به تصمیمات دشوار و انبوهی از تغییرات در روش تولید نیازمند خواهد بود. این حرف به این معنا است که باید مفهوم اعتماد را برای خود بازتعریف کنیم. در هر صورت، با تلاش مناسب می‌توان شرایطی به وجود آورد تا تعداد حملات کاهش پیدا کند و تأثیرات آن نیز کم‌رنگ‌تر شود. شاید با این روش بتوان داستان اسب تروا را به اعماق افسانه‌های تاریخی، یعنی همان جایی که به آن تعلق دارد، بازگردانیم.