گزارشی از مقاله

# A Survey and Analysis on SoC Platform Security in ARM, Intel and RISC-V Architecture

بررسی و تجزیه و تحلیل امنیت پلتفرم سیستم روی تراشه در معماری ARM، Intel و RISC-V


**ارائه از :** **مسعود باقری**

**شماره دانشجویی:** **۳۹۹۱۲۳۴۱۰۵۷۰۴۱**


**ترم تحصیلی:** **۲-۹۹**

**درس:** **معماری پیشرفته**

**استاد:** **دکتر جاسبی**

❖ **تعریف مسأله و هدف اصلی مقاله:**

**سوال اصلی مطرح شده در مقاله:**

این مقاله به بررسی تهدیدات عمده در یک پلتفرم معماری و طراحی SoC می‌پردازد و به بررسی ویژگی‌ها و آسیب پذیری‌های مختلف موجود در پلتفرم های ARM TrustZone و Intel SGX می‌پردازد. سرانجام، یک راه حل برای افزایش امنیت با استفاده از معماری RISC-V ارائه می‌دهد.

**چه مشکلی باید برطرف شود؟**

پردازش ناهمگون مدرن شامل دستگاه‌های اینترنت اشیا و شبکه‌ها، عملکرد بهینه و پیشرفته همراه با سرعت بالا را ارائه می‌دهند اما برای دستیابی به نتایج مطلوب به اجزا یا مولفه‌های بیشتری متکی هستند. بهره‌وری در طراحی برای شتاب دهنده‌های سخت افزاری با پلتفرم‌های یادگیری ماشینی برای کاربردهای مختلف، پیشرفت چشمگیری در معماری‌های "سیستم روی تراشه" (SoC) دارد. بیشتر این فناوری‌ها، عملکرد مطلوبی را ارائه می‌دهند، با این وجود همیشه بین امنیت و عملکرد تعارض [با افزایش یکی دیگری کاهش می‌یابد] وجود دارد. نقش اصلی در ایجاد چارچوب‌های نرم افزاری برای حملات امنیتی سخت افزاری، به IP[1] و معماری سیستم بستگی دارد. RISC-V، بستری را برای اجرای اختصاصی شده افزونه‌های امنیتی در مقایسه با سایر معماری‌های سنتی فراهم می‌کند. که به حل تعارض بین امنیت و عملکرد در یک سیستم روی تراشه کمک نموده است.

**چه ضرورتی برای مطرح شدن مسئله است؟**

سیستم‌های الکترونیکی در فناوری‌های نوظهور در معرض تهدیدهای امنیتی متعددی هستند. هر دستگاه فعال متصل به شبکه در برابر حملات سفت افزاری (رابط بین نرم افزار کاربر و سخت افزار یا نرم افزار دائمی یا فریمور) و سخت افزاری آسیب پذیر است. حملات میان افزار یا فریموری (Firmware)، شامل اجزا و تکنیک‌های مختلفی است که در حملات سنتی مبتنی بر نرم افزار وجود ندارد. امروزه برخی از تهدیدات در سطح میان افزاری شامل، حملات شبکه، انکار سرویس یا عدم ارائه خدمت، درج تروجان و غیره است. این

[1] **Intellectual property**
**مالکیت معنوی**

حملات نقش اصلی را روی اجزای سیستم بازی می‌کنند، بطوریکه از آنجا یک دشمن با بهره‌گیری از نقاط ضعف یک سیستم، کنترل کل آن سیستم را به دست می‌گیرد. از نظر حملات سخت افزاری، طرح‌های SoC باید از هرگونه دسترسی غیرمجاز محافظت شوند.

**چه روش‌هایی قبلا برای این کار انجام شده؟**

ژانگ و همکاران در سال ۲۰۱۶ تحقیقاتی در مورد نشت اطلاعات کانال جانبی حافظه پنهان روی دستگاه‌های مبتنی بر arm انجام و منتشر نمودند. بنهانی و همکاران در سال ۲۰۱۷ یک ارزیابی از امنیت ARM TrustZone و آسیب‌پذیری آن ارائه نمودند. مختار و همکارانش در سال ۲۰۱۹ یک مقایسه بین ARM TrustZone و اینتل (SGX) انجام دادند. ولی هیچ مقایسه‌ای با RISC-V صورت نگرفت.

محیط اجرای مطمئن یا قابل اعتماد (TEE)، یک محیط اجرای جداگانه است که ویژگی های امنیتی را فراهم می کند، که در آن، نرم افزار و داده ها از طریق جدا سازی محافظت می شوند [۱]. فناوری TEE مبتنی بر ARM TrustZone روشی را برای جداسازی اجزای مهم امنیتی در یک سیستم فراهم می کند [۲]. از منطقه محصور یا انکلاو[2] افزونه های نگهبان اینتل (SGX) در پردازنده های جدید امروزی پشتیبانی می شود تا از سطح دسترسی ویژه برخی توابع یا عملکردهای مجاز محافظت کند [۳]. برخی از معماری های دیگر برای کاربردهای مهم امنیتی: بستر امن پردازشگرAMD ، فناوریهای رمزنگاری حافظه AMD و موتور مدیریت اینتل (ME)، TEE پرتابل منبع باز ، و معماریهای مختلف پلتفرم امن (PSA) هستند. اگرچه این معماری های قدیمی، محیط مطمئنی را تا سطح معینی فراهم می‌کنند، اما به دلیل جدا شدن پشته های مختلف کتابخانه‌ها، قادر به تضمین ایزوله بودن نیستند.

**روش پیشنهادی ارائه شده چیست؟**

RISC-V ، یک معماری منبع باز است که برخلاف معماری اختصاصی SoC با 3PIP[3] و یکپارچه سازی امنیت سیستم، بستر یا پلتفرمی را برای پیاده سازی سطوح مختلف امنیتی در یک سیستم فراهم می‌کند. که با استفاده از مزایای منبع باز بودن RISC-V، خصوصاً در زمینه امنیتی، می توان ماژول‌های مختلفی را برای ایمن سازی سیستم از هر نوع حملات اجرا کرد [۵].

RISC-V برای این مهم از Hex-Five بهره می برد. این ابزار، اولین محیط اجرای مطمئن RISC-V است. این یک لایه نازک از نرم افزار است که بلوک‌های امنیتی سخت افزار داخلی RISC-V را تنظیم می کند، تا

[2] محدوده یا منطقه‌ای که مثل یک جزیره جدا شده.

[3] مالکیت معنوی شخص ثالث

امنیتی قوی را از طریق جداسازی داخلی سخت افزار خودش ایجاد کند. MultiZone به عنوان یک زنجیره ابزار جامع تعمیم داده شده، بنابراین هیچ کدنویسی امنیتی تخصصی لازم ندارد.

این مقاله به بررسی تهدیدات عمده در یک پلتفرم معماری و طراحی SoC می‌پردازد و به بررسی ویژگی ها و آسیب پذیری‌های مختلف موجود در پلتفرم‌های ARM TrustZone و Intel SGX می‌پردازد. سرانجام، یک راه حل برای افزایش امنیت با استفاده از معماری RISC-V ارائه می‌دهد.

- **توضیح راه حل پیشنهادی مقاله برای حل مسئله:**

**روش پیاده سازی شده برای حل مسئله مقاله به چه صورت است؟**

ابتدا اصول ایمن سازی یک سیستم روی تراشه بررسی و ۳ عامل اصلی به شرح ذیل لیست شد:

۱. Root Of Trust (RoT) منبع قابل اعتماد همیشگی سیستم
۲. Secure Boot بوت امن
۳. Trusted Execution Environment (TEE) محیط اجرای مطمئن

در ادامه فقط به تجزیه تحلیل آسیب پذیری‌ها و حفره‌های TEE در معماری‌های گوناگون و بصورت خاص سه معماری مورد نظر تیتر مقاله پرداخته شده است. پس از آن به مدل کردن تهدیدهای مختلف بر اساس مدل‌های مرجع امنیت و چالش‌های مرتبط با طراحی SoC پرداخته و کلیه تهدیدهای موجود را در قالب چهار سناریوی متفاوت دسته‌بندی نموده است:

۱. درج بدافزار/ دسترسی ناخواسته برنامه
۲. حملات کانال جانبی
۳. حملات زنجیره تأمین
۴. حملات شبکه

در این مرحله به بررسی میزان ایمنی و آسیب‌پذیری TEE در سه معماری نام برده پرداخته است:

ARM TrustZone پیاده سازی استاندارد TEE است که هسته‌های مالکیت معنوی را به دو بخش امن و غیر امن تقسیم می‌کند. در هر دو بخش بین حافظه و واحدهای جانبی پارتیشن ایجاد شده و این تفکیک سخت‌افزاری، امنیت داده‌های مهم را تأمین می‌کند. با این حال سیستم در طراحی‌های بزرگ و جدید تمایل به بزرگ شدن با انبوهی از کتابخانه ها و عملکردهای بهینه شده دارد. از این رو، در طراحی سیستم های

امنیتی مدرن از کار می افتد و قابل استفاده نیست. از طرف دیگر این مدل، در برابر حملات کانال جانبی مبتنی بر حافظه پنهان [یا کش] آسیب پذیر است. استخراج کلیدها از موتورهای رمزنگاری فعال در بخش یا دنیای امن با به خطر انداختن پلتفرم بخش غیرامن یا ردیابی سیگنال های قدرت یا EMF در هنگام تبادل کلید بین دو جهان امکان پذیر است [۸].

Intel SGX، مفهوم دسترسی به حافظه مخفی محصور شده یا انکلاو (enclave memory) و جلوگیری از نگاشت و نقشه برداری از آدرس برنامه یا کاربرد را ارائه می دهد [۱۰]. این انکلاوها ناحیه ای از حافظه هستند که از هرگونه دسترسی و تغییر در امان هستند. انکلاوها، محیط های مورد اعتماد سخت افزاری جدا شده هستند که در آن واحد [یا در حین اجرا] رمزگذاری و رمزگشایی می کنند. نکته منفی این مدل این است که این انکلاو به تمام فضای آدرس برنامه یا کاربرد غیرقابل اعتماد دسترسی کامل پیدا می کند، که آن را در برابر بدافزارهای مخرب آسیب پذیر می کند.

نکته اساسی موجود در آسیب‌پذیری‌های فوق، تعارض بین عملکرد و امنیت عنوان شده، مالکان برای جلوگیری از افت عملکرد سیستم خود از ارائه به‌روزرسانی‌های امنیتی جدید خودداری می‌کنند و از طرفی طبق حقوق مالکیت معنوی، توسعه دهندگان نیز دسترسی و اطلاعات مورد نیاز برای پوشش حفره‌های امنیتی را ندارند.

درمقابل، RISC-V با بهره‌مندی از MultiZone Security و ماژول‌ها و افزونه‌های امنیتی فراوان که توسط توسعه دهندگان ارائه شده، انواع حملات را طبق جدول ذیل پاسخ می‌دهد:

| مدل های متقابل سازگار با RISC-V | مدل های تهدید |
|---|---|
| لایه های محافظ سخت افزار شفاف با قابلیت محافظت در برابر نشت دسترسی به حافظه | حملات حافظه پنهان |
| هسته های مقاوم سخت هسته ای با شتاب دهنده های سخت افزاری و TEE های مجازی | حملات کانال جانبی |
| مدل های ردیابی جریان اطلاعات ، ردیابی جریان داده ها برای محافظت از خرابی حافظه و کاهش حملات DoS توسط مدل های تأیید [۱۸] | حملات انکار سرویس |
| بوت امن استتار چند لایه برای SoCs همراه با مدل های ردیابی داده [۱۷] | درج بدافزار |
| مبهم سازی منطقی با مدل انعطاف پذیر حمله SAT برای سیستم عامل SoC | حملات زنجیره تأمین |

**روش ارائه شده به چه صورت پیاده سازی شده؟(نرم افزاری یا بصورت اثبات ریاضی دقیقا توضیح داده شود)**

مقاله مروری بوده و فاقد چیاده سازی است

**نحوه مقایسه ایده مطرح شده با دیگر ایدههای مطرح شده در مقاله**

نحوه مقایسه ایده مطرح شده در مقاله با دیگر ایده‌های مطرح، از طریق مدل سازی تهدیدهای امنیتی مختلف و آنالیز و تجزیه و تحلیل آن‌ها و مقایسه نقاط ضعف و قوت هر یک بوده است.

- **نقاط قوت و ضعف مقاله:**

Hex-five به خوبی تشریح نشده و هیچ توضیحی درمورد استراتژی هگزفایو درمورد RoT و Secure Boot داده نشده و فقط به توضیح نصفه نیمه TEE در معماری RISC-V پرداخته است ولی مدل‌های امنیت و مدل‌های تهدید به خوبی دسته‌بندی و توضیح داده شده است.

- **جمع بندی و پیشنهادات برای کارهای آتی:**

این مقاله سعی داشته طی یک مقایسه بین سه پردازنده اینتل، ARM و RISC-V به بررسی امنیت سیستم‌های روی تراشه بپردازد و درنهایت به یک نتیجه گیری و انتخاب بر مبنای تأمین امنیت همراه با عملکرد قابل قبول برسد. و با توجه به عدم بررسی کافی آسیب‌پذیری‌های RISC-V پیشنهاد می‌شود با دقت بیشتری انجام شود چون احتمالا نتیجه گیری درستی شده است ولی ادله کافی نیست.

- **شبیه سازی:**

ارائه و شبیه سازی آنچه در مقاله شبیه سازی یا پیاده سازی شده است