تحلیل مقاله در رابطه با درس معماری پیشرفته

تهیه و ارائه از: مسعود باقری

دوره کارشناسی ارشد

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، Intelو RISC-V

جرالدین شایرلی

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 ویژگی ها و آسیب پذیری های مختلف موجود در پلتفرم های ARM TrustZone و Intel SGX و RISC-V می‌پردازد.
- سوال اصلی این است که کدام معماری انتخاب امن‌تری است؟

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. (IoT)
- 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 IPو معماری سیستم بستگی دارد.(*Intellectual property مالکیت معنوی*)
- خنثی کردن مشکلات مالکیت معنوی، تأمین امنیت سیستم‌های روی تراشه با حفظ سطح عملکرد سیستم، مشکلی است که بایست حل شود. (از نظر حملات سخت افزاری، طرح‌های SoC باید از هرگونه دسترسی غیرمجاز محافظت شوند.)

چه ضرورتی برای مطرح شدن مسئله است؟

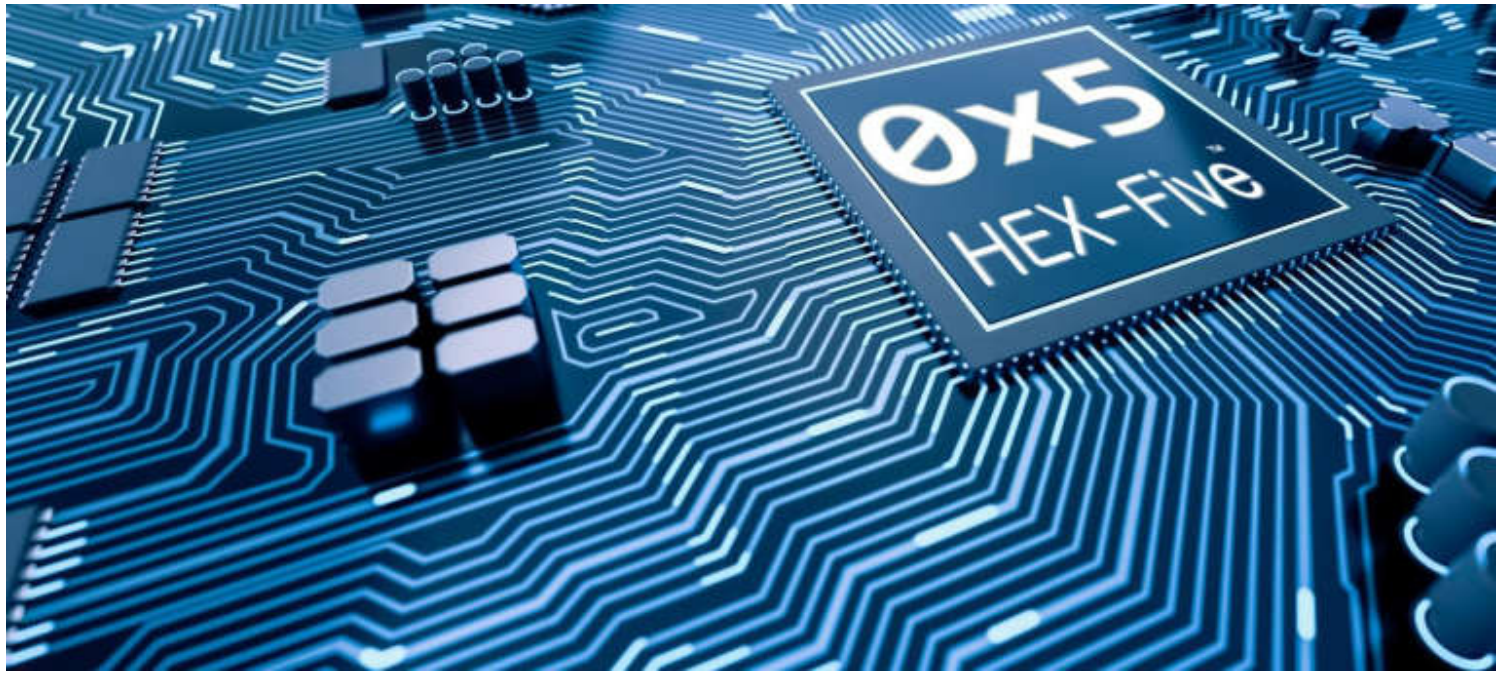
- سیستم‌های الکترونیکی در فناوری‌های نوظهور در معرض تهدیدهای امنیتی متعددی هستند
- هر دستگاه فعال متصل به شبکه در برابر حملات سفت افزاری آسیب پذیر است.
- هر دستگاه به عنوان یک جزء متصل به شبکه، نقش اساسی در امنیت سیستم دارد و یک دشمن می‌تواند با بهره‌گیری از نقاط ضعف یک نود متصل، کنترل کل آن سیستم را به دست می‌گیرد.
- حملات میان افزار یا فریموری (Firmware)، شامل اجزا و تکنیک‌های مختلفی است که در حملات سنتی مبتنی بر نرم افزار وجود ندارد. (حملات شبکه، انکار سرویس یا عدم ارائه خدمت، درج تروجان و غیره)

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
- فناوری TEEمبتنی بر ARM TrustZoneروشی را برای جداسازی اجزای مهم امنیتی در یک سیستم فراهم می کند
- از منطقه محصور یا انکلاو افزونه های نگهبان اینتل (SGX) در پردازنده های جدید امروزی پشتیبانی می شود
- برخی از معماری های دیگر برای کاربردهای مهم امنیتی: بستر امن پردازشگرAMD ، فناوریهای رمزنگاری حافظه AMDو موتور مدیریت اینتل (ME)، TEEپرتابل 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 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، می‌توان ماژول‌های مختلفی را برای ایمن سازی سیستم از هر نوع حملات اجرا کرد (مالکیت معنوی شخص ثالث)
- RISC-V برای این مهم از Hex-Five بهره می‌برد. این ابزار، اولین محیط اجرای مطمئنRISC-V است.
- این یک لایه نازک از نرم افزار است که بلوک‌های امنیتی سخت افزار داخلیRISC-V را تنظیم می‌کند، تا امنیتی قوی را از طریق جداسازی داخلی سخت افزار خودش ایجاد کند
- MultiZone به عنوان یک زنجیره ابزار جامع تعمیم داده شده، بنابراین هیچ کدنویسیِ امنیتیِ تخصصی لازم ندارد.



multizone-datasheet-20200109.pdf

HEX-Five MultiZone® Security

توضیح راه حل پیشنهادی مقاله برای حل مسئله:

عوامل اصلی ایمن سازی یک سیستم روی تراشه

1. Root Of Trust (RoT) منبع قابل اعتماد همیشگی سیستم
2. Secure Boot بوت امن
3. Trusted Execution Environment (TEE) محیط اجرای مطمئن

نقشه راه حل مسأله

- مدل کردن انواع تهدید
- بررسی TEE در معماری ARM
- بررسی TEE در پردازنده‌های اینتل
- بررسی TEE در معماری RISC-V
- ارائه یک مدل امن سخت افزاری برمبنای پلت‌فرم Hex-Five

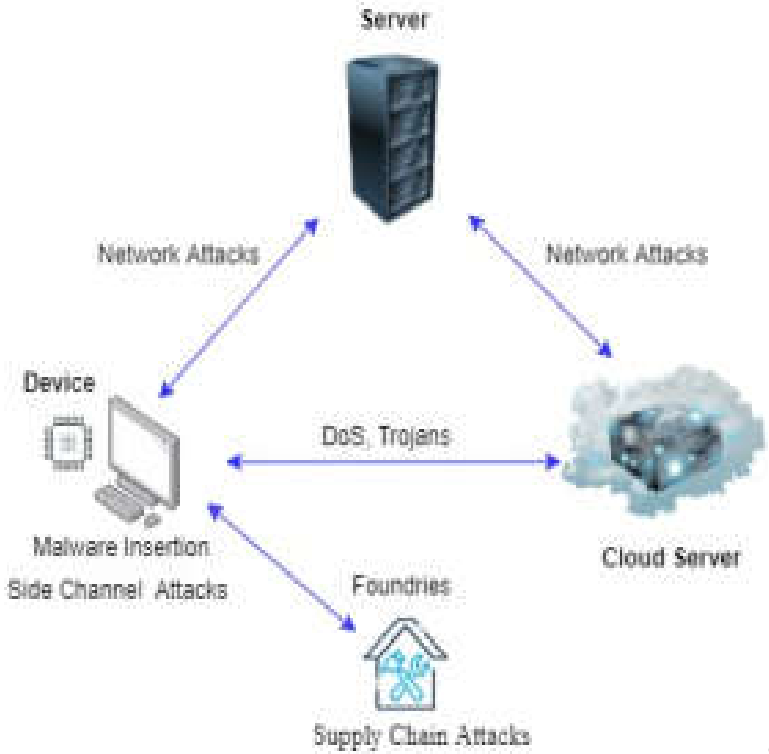
انواع سناریوی تهدید

درج بدافزار / دسترسی ناخواسته برنامه

حملات کانال جانبی

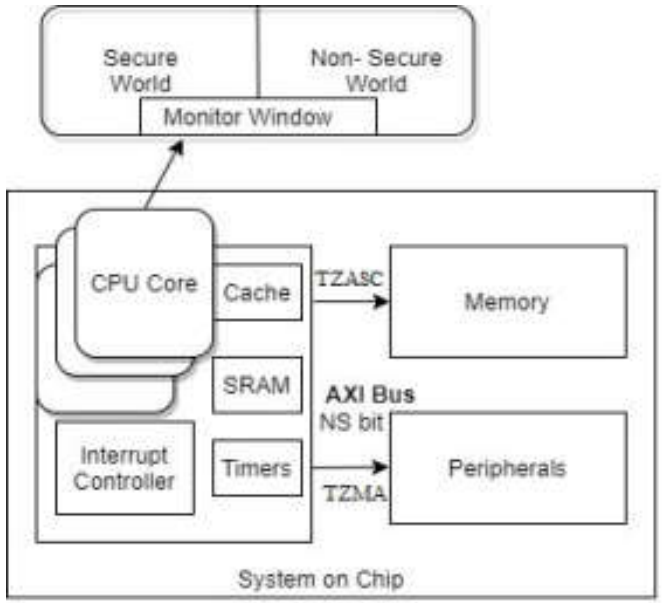
حملات زنجیره تأمین

حملات شبکه



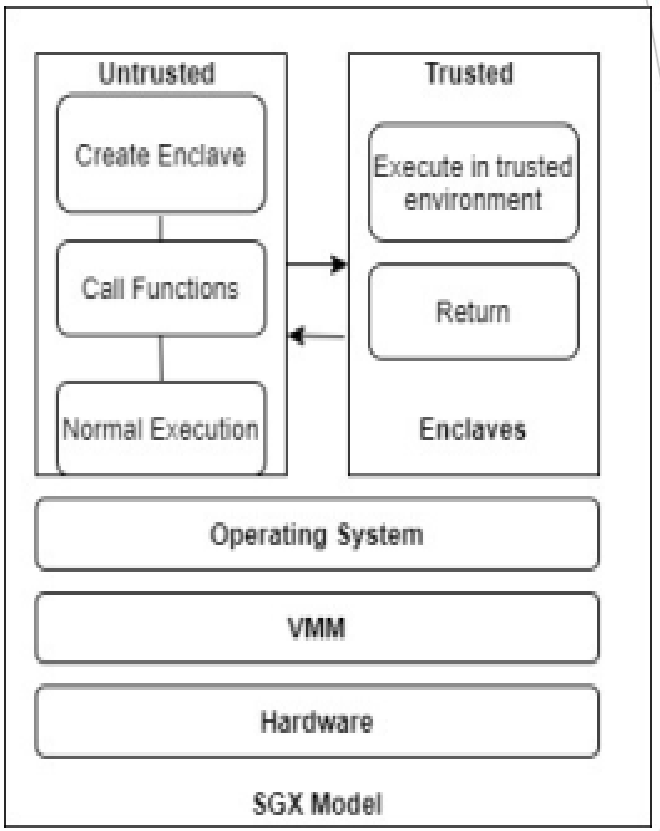
ARM TrustZone

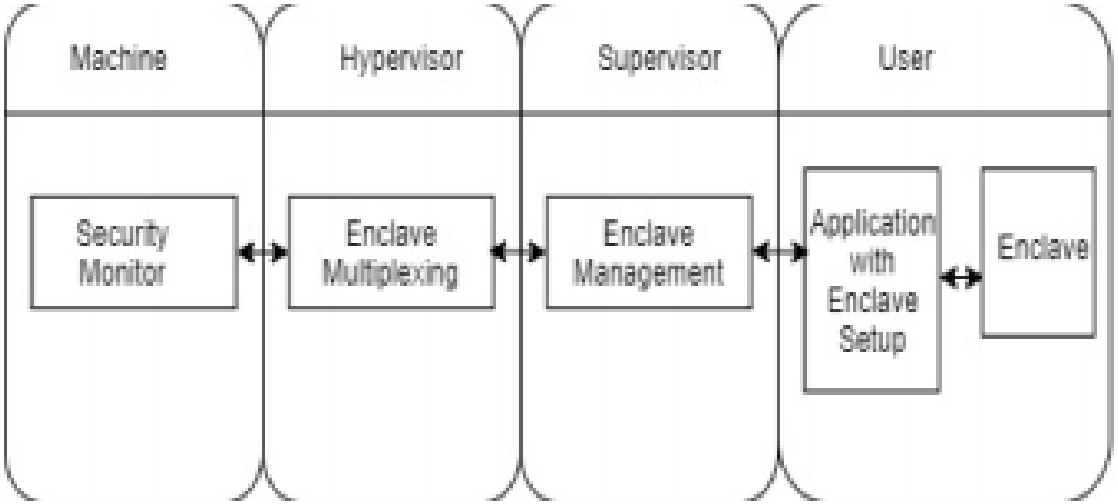
- پیاده سازی استاندارد TEE است که هسته‌های مالکیت معنوی را به دو بخش امن و غیر امن تقسیم می‌کند.
- . در هر دو بخش بین حافظه و واحدهای جانبی پارتیشن ایجاد شده و این تفکیک سخت‌افزاری، امنیت داده‌های مهم را تأمین می‌کند.
- با این حال سیستم در طراحی‌های بزرگ و جدید تمایل به بزرگ شدن با انبوهی از کتابخانه 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 امن با به خطر انداختن پلتفرم بخش غیرامن یا ردیابی سیگنال های قدرت (EMF) در هنگام تبادل کلید بین دو جهان امکان پذیر است.



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.
- . 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.





معماری پیشنهادی:

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.

جزئیات روش ارائه شده:

- 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 TEEهای مجازی	حملات کانال جانبی
مدل های ردیابی جریان اطلاعات ، ردیابی جریان داده ها برای محافظت از خرابی حافظه و کاهش حملات DoSتوسط مدل های تأیید [18]	حملات انکار سرویس
بوت امن استتار چند لایه برای SoCsهمراه با مدل های ردیابی داده [17]	درج بدافزار
مبهم سازی منطقی با مدل انعطاف پذیر حمله SATبرای سیستم عامل SoC	حملات زنجیره تأمین

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

- مدل کردن تهدیدهای مختلف
- ارائه مدل‌های امنیتی موجود
- آنالیز و تجزیه و تحلیل هر مدل امنیتی
- بررسی نقاط ضعف قوت مدل‌های امنیتی

نقاط قوت و ضعف مقاله:

نقاط قوت

- مدل‌های تهدید به خوبی دسته‌بندی شده‌اند
- مدل‌های امنیت بخوبی تشریح شده‌اند
- ضعف مدل‌های امنیتی و امکان نفوذ به خوبی مشخص شده.
- درکل آسیب شناسی خوبی ارائه شده

نقاط ضعف

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

خدا یار و نگهدار شما