Scientific Journal of Electronical & Cyber Defence
Vol. 12, No. 3, Autumn2024, Serial No. 47

Evaluation of Side-Channel Attacks for Different Types of Processors Vulnerabilities

A. GhannadanZadeh, M. Mollazadeh *, A.Moghaddasi , M. Esfahani

* Assistant Professor, Imam Hossein University, Tehran, Iran

Received:2024 /07/30, Revised: 2024/09/18, Accepted: 2024/10/14, Published: 2024/10/22

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.3.1.3

ABSTRACT

In recent years, electronic devices such as laptops, computers, smart mobile phones and other smart electronic devices have greatly increased, and all these electronic devices use one or more processors inside them, which according to the type of architecture of each processor may have different vulnerabilities. In this paper investigation and evaluation of side channel vulnerabilities based on the vulnerabilities of processors has been done based on two hierarchical analysis and CVSS parameter methods. In our hierarchical analysis, according to type of vulnerabilities, the attacks have been divided into 6 general categories which attacks have been evaluated based on criterias such as time, possibility, effectiveness, and used resources. Among the 6 examined attacks, 3 of them which are time-based attack, cache-based attack and power side channel attack with software measurement have respectively assigned the most points based on the evaluation criterias and the power side-channel with hardware measurement attack has the lowest score. The overall inconsistency ratio was 0.06 which was acceptable. Also, 3 sub-criteria of have had the greatest impact on decision options which are key (password) recovery percentage, access level and covert channel ability. Finally, in addition to the overall ranking, these options are also scored based on each of the criteria. For example, for possibility criteria, the time-based attack and the power side channel attack with software measurement have the highest and lowest priority, respectively and for effectiveness criteria, time-based attack and side-channel power attack with hardware measurement have higher and lower priority, respectively. Next, the risk level of these 6 strategies was scored and ranked using the CVSS parameter. The results of this evaluation show that 3 time-based attacks, micro-architectural-based attacks and cache-based attacks are more dangerous for the victim, respectively and will cause the most damage for him.

Keywords: Processors Vulnerability, Hierarchical Analysis, Cache, Risk Assessment

❖ Corresponding Author Email: mollazadeh@dspri.com

«پدافند الکترونیکی و سایبری»
سال دوازدهم، شماره ۳، فصل پاییز ۱۴۰۳؛ ص ۱۱۸-۱۰۱

ارزیابی کاربردی حملات کانال جانبی بر اساس انواع آسیب‌پذیری‌های پردازنده‌ها

احمد قنادان زاده، مهدی ملازاده، علی مقدسی، مهدی اصفهانی
۱-دانشجوی دکتری ۲-استادیار،۳- استادیار، دانشگاه جامع امام حسین(ع)، تهران، ایران ،۴ -پژوهشگر، دانشگاه صنعتی شریف، تهران، ایران

(دریافت: ۱۴۰۳/۰۵/۰۹، بازنگری: ۱۴۰۳/۰۶/۲۸، پذیرش: ۱۴۰۳/۰۷/۲۳، انتشار: ۱۴۰۳/۰۸/۰۱)

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.3.1.3

ناشر: دانشگاه جامع امام حسین (ع)

چکیده

در سال‌های اخیر وسایل الکترونیکی همچون لپ‌تاپ، کامپیوتر، تلفن‌های همراه هوشمند و دیگر وسایل الکترونیکی هوشمند به‌شدت افزایش‌یافته که تمام این وسایل الکترونیکی از یک یا چندپردازنده در داخل خود استفاده می‌نمایند که باتوجه‌به نوع معماری هر پردازنده ممکن است آسیب‌پذیری‌های متفاوتی داشته باشند. در این مقاله بررسی و ارزیابی آسیب‌پذیری‌های کانال جانبی مبتنی بر آسیب‌پذیری‌های پردازنده‌ها بر اساس دو روش تحلیل سلسله‌مراتبی و پارامتر CVSS انجام شده است. در تحلیل سلسله‌مراتبی، حملات بر اساس نوع آسیب‌پذیری‌ها به شش دستهٔ کلی تقسیم‌بندی شده است که این حملات بر اساس شاخص‌هایی چون زمان، امکان‌پذیری، اثربخشی و منابع مورداستفاده مورد ارزیابی قرار گرفته است. در بین شش حملهٔ بررسی شده، سه حملهٔ مبتنی بر زمان، حملهٔ مبتنی بر حافظهٔ نهان و حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری به ترتیب بیشترین امتیاز را بر اساس معیارهای ارزیابی به خود اختصاص داده‌اند و حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری کمترین امتیاز را داشته است. نرخ ناسازگاری کلی برابر با مقدار ۰/۰۶ شده است که قابل‌قبول است. همچنین سه زیرمعیار درصد بازیابی کلید(گذرواژه)، سطح دسترسی و قابلیت ایجاد کانال پنهان بیشترین تأثیر را بر روی گزینه‌های تصمیم داشته‌اند. در نهایت این گزینه‌ها علاوه بر رتبه‌بندی کلی بر اساس هرکدام از معیارها نیز امتیازبندی شده‌اند. به‌عنوان‌مثال از منظر امکان‌پذیری حملهٔ مبتنی بر زمان و حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری به ترتیب دارای بیشترین و کمترین اولویت بوده و از منظر اثربخشی حملهٔ مبتنی بر زمان و حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری به ترتیب اولویت بیشتر و کمتری داشته‌اند. در ادامه میزان خطر این شش راهکار با استفاده از پارامتر CVSS امتیازدهی شده و رتبه‌بندی شد. نتایج این ارزیابی نشان می‌دهد که سه حملهٔ مبتنی بر زمان، حملهٔ مبتنی بر ریز معماری و حملهٔ مبتنی بر حافظهٔ نهان به ترتیب بیشترین خطر را برای قربانی داشته و بیشترین آسیب را وارد خواهند نمود.

کلیدواژه‌ها: آسیب‌پذیری پردازنده‌ها، تحلیل سلسله‌مراتبی، حافظهٔ نهان، ارزیابی خطر

۱- مقدمه

در عصر حاضر به‌ازای هر نفر چندین عدد رایانه، وسایل ارتباطی و دستگاه‌های محاسباتی از نوع ثابت و قابل‌حمل از قبیل لپ‌تاپ، رایانهٔ شخصی، تلفن‌های همراه هوشمند، وسایل ارتباطی هوشمند، وسایل الکترونیک خانگی، کارت‌های خرید و... وجود دارد که روزبه‌روز در حال افزایش بوده و باتوجه‌به کاربرد، نیازمند شرایطی همچون محرمانگی[1]، حریم خصوصی[2]، یکپارچگی[3]، احراز اصالت[4] و دیگر پارامترهای امنیتی می‌باشند. پایهٔ اصلی امنیت این‌گونه ابزارها، بر علم رمزنگاری استوار بوده و می‌توان گفت علم رمزنگاری (و به بیانی دیگر هنر رمزنگاری) و تحلیل رمز پشتوانه‌ای برای امنیت اطلاعات می‌باشد. به همین منظور با

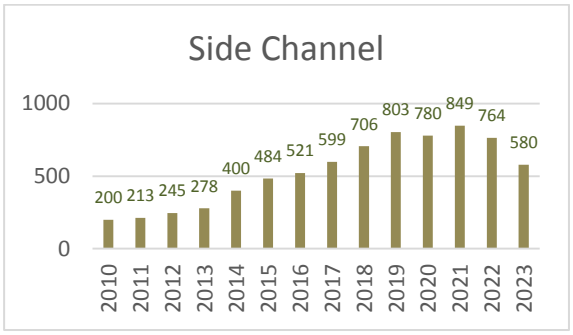
[1] Confidentially
[2] Privacy
[3] Integrity
[4] Authentication

* رایانامه نویسنده مسئول: mollazadeh@dspri.com

پیدایش این علوم، الگوریتم‌های رمزنگاری متقارن و غیرمتقارن مختلفی معرفی شده و مورداستفاده قرار گرفت که از جمله معروف‌ترین آن‌ها می‌توان به استاندارد رمزنگاری داده[۱]، DES سه‌گانه[۲]، ماهی بادکنکی[۳]، رمز رئوست ۴[۴]، استاندارد رمزنگاری پیشرفته[۵] و رمز رئوست-شمیر-ادلمن[۶] اشاره نمود که دراین‌بین دو الگوریتم رمزنگاری AES و RSA مورد استقبال بیشتری قرار گرفته و بسته به کاربرد در پیاده‌سازی‌های مختلف از هریک از آن‌ها استفاده می‌شود. تا سال‌ها اساس اثبات الگوریتم‌های رمزنگاری بر پایهٔ اثبات ریاضی و تئوری آن‌ها بود؛ اما در سال‌های اخیر دسته‌ای از حملات با عنوان حملات کانال جانبی[۷] معرفی شده‌اند که علی‌رغم امنیت قابل‌اثبات الگوریتم‌ها در تئوری، در این حملات از ضعف‌های موجود در پیاده‌سازی این الگوریتم‌ها استفاده شده که موجب دستیابی به کلیدهای رمزنگاری و داده‌های حساس قربانی خواهد شد که در این مقاله به ارزیابی کاربردی آن‌ها پرداخته خواهد شد. ساختار کلی این مقاله بدین شکل است: در بخش ۲ ادبیات موضوع و کارهای قبلی انجام شده به طور کامل مرور خواهد شد. در بخش ۳ روش تحقیق معرفی شده و معیارها، زیرمعیارها و گزینه‌های تصمیم معرفی خواهند شد. در بخش ۴ نتایج حاصل از ارزیابی‌ها مورد بحث‌وبررسی قرار می‌گیرد. در بخش ۵ نتیجه‌گیری نهایی ارائه شده و در بخش ۶ نیز مراجع مورداستفاده آورده شده است.

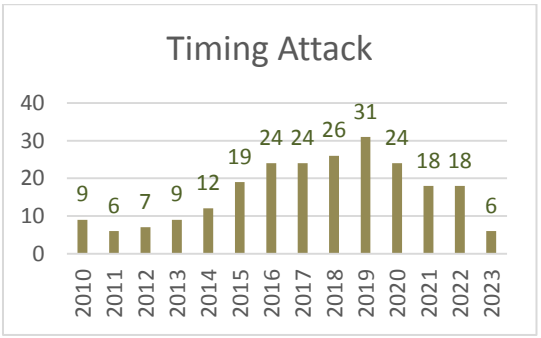
۲- ادبیات و پیشینه‌ی تحقیق

یکی از انواع حملاتی که در دو دههٔ اخیر بسیار مورد توجه قرار گرفته است، حملات کانال جانبی است که به گزارش مرجع Web of Science [1] همان‌طور که در شکل(۱) قابل‌مشاهده است، در بازهٔ بین سال‌های ۲۰۱۰ تا ۲۰۲۳ مقالات این حوزه سالانه روبه‌افزایش بوده است. حملات کانال جانبی منتشر شده عمدتاً شامل حملات تحلیل توان و همچنین حملات الکترومغناطیس، تحلیل نرم‌افزاری، تحلیل زمان، حافظهٔ نهان[۸]، آکوستیک، ریز معماری[۹] و ... می‌باشند.



شکل (۱). تعداد مقالات با موضوع کانال جانبی در بازه‌ی ۲۰۱۰ تا ۲۰۲۳ مستخرج از Web of Science

حملات الکترومغناطیس و آکوستیک از نظر نوع حمله متفاوت هستند و نیاز به تجهیزات و شرایط خاصی برای انجام حمله دارند و در این مقاله مورد بررسی قرار نمی‌گیرند. دسته‌بندی حملات کانال جانبی مورد بررسی در این مقاله در بخش روش تحقیق آورده شده است؛ اما به‌طورکلی این حملات شامل حملهٔ کانال جانبی توان، حملهٔ مبتنی بر زمان، حملهٔ مبتنی بر حافظهٔ نهان، حملهٔ مبتنی بر ریز معماری و حملهٔ مبتنی بر هوش مصنوعی هستند. به‌عنوان نمونه حملات زمانی یکی از نمونه‌های حملات کانال جانبی است که در برخی از مقالات بر روی آن کار شده است. البته باید توجه داشت که حملات زمانی ممکن است از نوع کانال جانبی نباشند. در شکل(۲) تعداد مقالات مرتبط با حملات زمانی منتشر شده در همان بازهٔ زمانی قابل‌مشاهده است.



شکل (۲). تعداد مقالات با موضوع حملات زمانی در بازه‌ی ۲۰۱۰ تا ۲۰۲۳ مستخرج از Web of Science

به همین ترتیب می‌توان باقی نمونه‌های این حمله را نیز از نظر تکرار بررسی نمود. به طور خلاصه می‌توان گفت حملات مبتنی بر حافظهٔ نهان و همچنین حملات مبتنی بر ریز معماری در چند سال اخیر مورد توجه قرار گرفته و درحال‌توسعه هستند. حملات مبتنی بر هوش مصنوعی و محیط اجرایی امن[۱۰] نیز از جدیدترین حملاتی هستند که اخیراً معرفی شده‌اند. از منظر نوع پردازندهٔ مورد حمله نیز می‌توان این حملات را دسته‌بندی نمود که براین‌اساس می‌توان از پردازنده‌های اینتل، AMD، FPGA و

[1] Data Encryption Standard (DES)
[2] Triple DES (3DES)
[3] Blowfish
[4] Rivest Cipher 4 (RC4)
[5] Advanced Encryption Standard (AES)
[6] Rivest–Shamir–Adleman (RSA)
[7] Side-Channel Attacks
[8] Cache
[9] Microarchitecture
[10] Trusted Execution Environments (TEE)

نشانه نام برد. باتوجه‌به فراوانی پردازنده‌های اینتل در رایانه‌های خانگی و رایانهٔ کیفی‌ها و همچنین پردازنده‌های مبتنی بر نشانه در انواع تجهیزات الکترونیکی از جمله تلفن‌های هوشمند و بردهای صنعتی، حملات انجام شده بر روی این دو پردازنده در این مقاله مورد بررسی قرار می‌گیرند.

برخی از حملات کانال جانبی انجام شده بر روی این پردازنده‌ها از انواع الکترومغناطیس، آکوستیک، حرارتی و... بوده و از اثرات کانال جانبی این موارد برای انجام حمله استفاده شده است. در حملات دیگر، آسیب‌پذیری‌های سخت‌افزاری موجود بر روی پردازنده شناسایی شده و به‌صورت نرم‌افزاری از آن بهره‌برداری می‌شود. این آسیب‌پذیری‌ها می‌توانند از نوع زمانی، حافظهٔ نهان، ریز معماری توان و... باشند. در این بخش الگوهای مختلف مورد استفاده برای حملات کانال جانبی و حملات انجام شده توسط این الگوها مورد بررسی قرار خواهند گرفت. برای انجام این حملات تاکنون الگوهای مختلفی استفاده شده است که باتوجه‌به نوع آسیب‌پذیری، سطح حمله، سطح دسترسی، سطح حافظهٔ نهان و... از هرکدام از آن‌ها استفاده می‌شود. از جملهٔ این الگوها می‌توان به الگوهای پرایم+پروب[۱]، اخراج+زمان[۲]، فلاش+ریلود[۳]، فلاش+فلاش[۴] و... اشاره نمود که در ادامه به بررسی نحوهٔ عملکرد هریک از آن‌ها و حملات انجام شده با این الگوها پرداخته می‌شود.

۲-۱- الگوی حمله پرایم+پروب

یکی از الگوهای مورد استفاده در حملات کانال جانبی مبتنی بر حافظهٔ نهان، الگوی پرایم+پروب می‌باشد که روی سطح L1 از حافظهٔ نهان انجام شده است[۲]. در این نوع حمله مهاجم ابتدا حافظهٔ نهان را با داده‌های خود پر می‌نماید. پس از آن مهاجم به قربانی اجازه می‌دهد تا برنامه‌ی خود را اجرا نماید که هنگام اجرا قربانی با توجه به داده‌هایی که در حافظهٔ نهان ذخیره شده است، به بخش‌هایی از حافظه دسترسی پیدا نموده و با توجه به پر شدن آن‌ها توسط مهاجم، مغایرت[۵] حافظهٔ نهان ایجاد شده و در نتیجه این داده خارج[۶] می‌گردد و داده‌های مورد نظر قربانی در آن‌ها قرار می‌گیرد. سپس در مرحله‌ی کاوش[۷] مهاجم داده‌هایی که در حافظه ذخیره نموده بود را خوانده و زمان دسترسی به آن‌ها را اندازه‌گیری می‌کند و برمبنای آن تصمیم‌گیری در مورد داده انجام می‌شود[۳]. در [۴] این حمله به الگوریتم رمزنگاری RSA موجود در بسته‌ی اُپن‌اِس‌اِس‌اِل نسخه‌ی 0.9.7c انجام شده در حالیکه حملهٔ ارائه شده در [۵] بر روی الگوریتم رمزنگاری AES ۱۲۸ بیتی و نیز حملات ارائه شده در [۲] و [۶] نیز بر روی AES ۱۲۸ بیتی موجود بر روی بسته‌ی اُپن‌اِس‌اِس‌اِل نسخه‌ی 0.9.8 انجام گرفته است. این ۴ حمله همگی از طریق حافظهٔ نهان داده‌ی سطح L1[۸] انجام شده و در نتیجه می‌بایست پردازش‌های انجام شده توسط مهاجم و قربانی بر روی یک هسته انجام گیرد تا حملهٔ انجام شده موفقیت آمیز باشد.

دستهٔ دیگری از این نوع حمله به جای استفاده از حافظهٔ نهان داده از طریق حافظهٔ نهان سطح دستورالعمل L1[۹] انجام شده است([۷] و [۸]). هر دوی این حملات بر روی الگوریتم رمزنگاری RSA موجود در بسته‌ی اُپن‌اِس‌اِس‌اِل (در [۷] بر روی نسخه‌ی ۰.۹.۸d و در [۸] نسخه‌ی ۰.۹.۸e) انجام شده است.

حملات جدیدتر منتشر شده با استفاده از پرایم+پروب از طریق سطح آخر حافظهٔ نهان[۱۰] انجام شده و با توجه به اینکه از طریق سطح آخر انجام شده و سطح آخر بین هسته‌های پردازنده مشترک می‌باشد، می‌توان گفت این حمله در سطح کل CPU قابل انجام است و مهاجم و قربانی می‌توانند از دو هسته‌ی متفاوت استفاده نمایند. یک نمونه از این حمله بر روی رمزنگاری کلید عمومی اِلجمال[۱۱] در گنوپی‌جی[۱۲] نسخه‌های ۱.۴.۱۳ و ۱.۴.۱۸ انجام شده که این کلید عمومی ۳۰۷۲ بیتی بوده است[۹]. دو حملهٔ دیگر از این دسته بر روی الگوریتم رمزنگاری RSA انجام شده که در این دو حمله با روش‌هایی سازوکار افزونه‌های نگهبان نرم‌افزار[۱۳] را دور می‌زنند و علیرغم وجود SGX کلید RSA استخراج می‌گردد ([۱۰] و [۱۱]). به بیان دقیق‌تر با وجود جلوگیری SGX از حملات مبتنی بر فلاش+ریلود، این سازوکار شرکت اینتل در برابر حملات پرایم+پروب معرفی شده ضعف دارد[۱۲].

۲-۲- الگوی حمله اخراج+زمان

در این حمله مهاجم ابتدا باعث می‌شود که قربانی تابع رمزنگاری (به‌عنوان‌مثال AES) را به‌ازای یک متن اصلی[۱۴] مشخص با یک کلید نامعلوم اجرا نموده و رمزنگاری را به طور طبیعی انجام دهد که در این حالت با اجرای برنامه از حافظهٔ نهان استفاده شده و مهاجم زمان را اندازه‌گیری می‌نماید تا بتواند

[1] Prime+Probe
[2] Evict+Time
[3] Flush+Reload
[4] Flush+Flush
[5] Conflict
[6] Evict
[7] Probe

[8] L1 Data Cache
[9] L1 Instruction Cache
[10] Last Level Cache (LLC)
[11] Elgamal
[12] GnuPG
[13] Software Guard Extensions (SGX)
[14] Plaintext

یک خط پایه[1] (آستانه) را ایجاد نماید. سپس مهاجم برخی از خطوط حافظهٔ نهان را خارج نموده[2] و مجدداً به قربانی اجازه می‌دهد تا برنامهٔ خود را اجرا نماید که با مقایسهٔ زمان دسترسی فعلی با آستانهٔ به‌دست‌آمده، مهاجم می‌تواند مورداستفاده قرارگرفتن خطوط خارج شده را توسط قربانی تشخیص دهد. باتوجه‌به اینکه این حمله نیاز به چندین اجرا دارد، درصورتی‌که برنامهٔ مورداستفاده قربانی یکبار اجرا شود، نتایج دقیقی حاصل نخواهد شد [۳].

از اولین حملات حافظهٔ نهان انجام شده با این روش از طریق حافظهٔ نهان سطح L1 داده بر روی الگوریتم رمزنگاری AES ۱۲۸ بیتی موجود در بسته‌ی اُپن‌اِس‌اِس‌اِل نسخه‌ی ۰.۹.۸ انجام شده است [۲]. حملهٔ دیگر بر روی سازوکار تصادفی‌سازی چیدمان فضای آدرس[3] در حافظهٔ کرنل از طریق لایهٔ آخر حافظهٔ نهان انجام شده است که در سطح CPU معتبر است[۱۳].

۲-۳. الگوی حمله فلاش+ریلود

این الگو یکی از الگوهای مشهور در این حوزه است که در حملات بیشتری از آن استفاده شده است. در مرحله‌ی اول این حمله، قسمت فلاش[4] با استفاده از دستور سی‌اِل‌فلاش[5] انجام شده و باعث می‌شود خط مورد نظر فلاش شده، از همه‌ی سطوح حافظهٔ نهان خارج شود که در نتیجه از سطح آخر این حافظه نیز پاک می‌شود. در این حالت خط پاک شده به دلیل استفاده‌ی مهاجم و قربانی از دو هسته‌ی متفاوت اما لایهٔ سوم حافظهٔ نهان مشترک، از حافظهٔ نهان سطح بالاتر قربانی نیز پاک شده و با توجه به وجود خاصیت کپی‌برداری حافظه[6]، این خط ممکن است حاوی داده‌های حساس مخصوص قربانی باشد. درصورتی‌که قربانی مجددا به عنوان مثال عملیات رمزنگاری را انجام دهد و مهاجم عملیات بارگذاری مجدد[7] را انجام دهد، مهاجم می‌تواند با تکرار این عمل و پیدا نمودن محل قرارگیری داده‌های حساس به کمک برخورد یا عدم برخوردهای اتفاق افتاده، محتوای این داده‌ها را به دست آورد. این روش ابتدا در [۱۴] به کار گرفته شده است اما کلمه‌ی Reload در این مقاله مشاهده نمی‌شود بلکه به‌صورت رسمی در [۱۵] اولین معرفی از فلاش+ریلود با این نام توسط یاروم[8] و همکارانش ارائه شد و هدف آن الگوریتم رمزنگاری RSA موجود بر روی گنوپی‌جی نسخه‌ی ۱.۴.۱۳ بود. این حمله قادر است تا در یک مرحله از رمزگشایی یا مشاهده‌ی یک امضا، ۹۶,۷ درصد بیت‌های یک کلید مخفی را بازیابی نماید [۱۵]. از این روش برای حمله به الگوریتم رمزنگاری AES موجود بر روی اُپن‌اِس‌اِس‌اِل نسخه‌ی ۰.۹.۸n استفاده شده است[۱۴].

در [۱۶] روش فلاش+ریلود که بر روی الگوریتم رمزنگاری AES موجود در اُپن‌اِس‌اِس‌اِل نسخه‌ی ۱.۰.۱f انجام شده است، علاوه بر اجرا در ابعاد بین CPU در ابعاد Cross-VM نیز اجرا شده است. در حمله‌ای دیگر، مهاجم از یک سری روش‌های آماری برای بازیابی کلید الگوریتم رمزنگاری AES استفاده می‌کند که موجب افزایش سرعت اجرای حمله می‌شود و در آن کلید AES را با ۱۵۰۰۰ عملیات رمزنگاری بازیابی می‌کند [۱۷]. پیاده‌سازی این روش بر روی الگوریتم امضای دیجیتال مبتنی بر خم بیضوی[9] موجود بر روی اُپن‌اِس‌اِس‌اِل نسخه‌ی ۱.۰.۱e نیز انجام شده است که همگی در سطح CPU پیاده‌سازی و اجرا شده‌اند. در این حملات، کلید خصوصی موجود در منحنی secp256k1 که در بیت کوین از آن استفاده می‌شود، شکسته شده است [۲۲–۱۹].

ژانگ و همکارانش یک چارچوب[10] حمله برای حملات کانال جانبی مبتنی بر حافظهٔ نهان ارائه داده‌اند که در محیط CPU و البته ماشین مجازی انجام شده و هدف آن جمع آوری اطلاعات حساس از فعالیت‌های کاربر در فضاهای ابری هم‌چون داده‌های حساس برنامه‌های کاربردی جهت سرقت اکانت کاربر بوده است [۲۲]. گراس و همکارانش یک چارچوب برای خودکارسازی حملاتی که به LLC از نوع شامل[11] انجام می‌شود، تهیه نموده‌اند که می‌تواند جهت بهره‌برداری[12] از آسیب‌پذیری‌های مرتبط با این نوع از LLC در هر برنامه‌ی در حال اجرا استفاده شود. هدف این حمله بررسی کلید ورودی در کیبورد در هر دو سیستم عامل ویندوز و لینوکس بوده است که توانسته است آنتروپی پسوردها را مخصوصا در لینوکس به طور قابل ملاحظه‌ای کاهش دهد. [۲۳]. فاکتور مهم محدودکننده در این حمله زمان زیاد اجرای حملهٔ الگوی حافظهٔ نهان[13] است که اصفهانی و همکاران آن را اصلاح نموده و سرعت اجرای حمله را افزایش داده‌اند. پیاده‌سازی آن بر روی الگوریتم AES موجود در بسته‌ی اُپن‌اِس‌اِس‌اِل نسخه‌ی ۱.۱.۰f انجام شده است [۲۴]. در [۲۵] نیز گزارش دیگری از این گروه موجود است. یکی دیگر از حملات فلاش+ریلود بر روی الگوریتم امضای دیجیتال[14] موجود بر روی نسخه‌های اُپن‌اِس‌اِس‌اِل از اکتبر ۲۰۰۵ اجرا شده است [۲۶].

[1] Baseline
[2] Evict
[3] Address Space Layout Randomization (ASLR)
[4] Flush
[5] clflush
[6] Memory Deduplication
[7] Reload
[8] Yarom
[9] Elliptic Curve Digital Signature Algorithm (ECDSA)
[10] Framework
[11] Inclusive
[12] Exploitation
[13] Cache Template Attack
[14] Digital Signature Algorithm (DSA)

۲-۴. الگوی حمله فلاش+ فلاش

سازوکارهای آشکارسازی[1] حملات با این فرض که تمام حملات مبتنی بر حافظهٔ نهان باعث تعداد بیشتری برخورد و عدم برخورد حافظهٔ نهان نسبت به برنامه‌های کاربردی بی‌خطر[2] خواهند شد، با استفاده از شمارنده‌های سخت‌افزاری اقدام به آشکارسازی این حملات می‌نمایند. به همین منظور برای دور زدن آشکارسازها، روش جدید فلاش+فلاش معرفی و استفاده شده است که در آن تنها بر زمان اجرای دستورالعمل فلاش و قرار گرفتن یا نگرفتن داده در حافظهٔ نهان تکیه شده است. بدین ترتیب برخلاف دیگر حملات مبتنی بر حافظهٔ نهان، این حمله هیچگونه دسترسی به حافظه ندارد در نتیجه می‌توان گفت که پنهان‌کار بوده و با روش‌های جدید ارائه شده برای آشکارسازی تا زمان ارائه‌ی این مقاله (۲۰۱۶) قابل شناسایی نمی‌باشد. این حمله به جداول T الگوریتم رمزنگاری AES موجود در اُپن‌اِس.اِس.اِل انجام شده است [۲۷]. نمونه‌ی دیگری از این حمله به یک الگوریتم رمزنگاری AES موجود در اُپن‌اِس.اِس.اِل نسخه‌ی 1.1.1g انجام شده است که در آن به کاهش نویز در این حمله پرداخته است [۲۸]. در این مقاله با ایجاد یک کانال مخفی به پهنای باند تقریبا سه برابر نسبت به روش مقاله‌ی [۲۷] که مقاله‌ی اولیه‌ی فلاش+فلاش بوده است، رسیده است. دو مقاله‌ی [۲۹] و [۳۰] که توسط یک گروه با شباهت‌های زیاد در دو سال ۲۰۲۰ و ۲۰۲۲ ارائه شده‌اند، به بررسی حملات مبتنی بر فلاش در محیط های نویزی پرداخته و مقایسه‌ی انجام شده در آن برای دو روش فلاش+فلاش و فلاش+ریلود بر روی الگوریتم رمزنگاری AES موجود بر روی اُپن‌اِس.اِس.اِل نسخه‌ی ۱.۰.۲ انجام شده است.

دسته‌ی دیگری از حملات مورد بررسی در این مقاله، حملات انجام شده بر روی پردازنده‌های مبتنی بر دستگاه‌های ریسک[3] پیشرفته[4] (به اختصار ARM) است که با توجه به آنچه در [۳۱] (و به طور رسمی در [۳۲]) عنوان شده است، بیش از ۶۰ درصد وسیله‌های نهفته[5] از پردازنده‌های مبتنی بر آرم استفاده می‌نمایند.

باتوجه‌به اینکه تلفن‌های هوشمند جدید از یک یا چندپردازندهٔ مبتنی بر آرم در داخل خود استفاده می‌نمایند، Lipp و همکارانش در دانشگاه Graz حملات پرایم+پروب، فلاش+ریلود، اویکت+ریلود[6] و فلاش+فلاش را بر روی تلفن‌های هوشمند اندرویدی روت نشده انجام داده‌اند که هیچ اجازه یا دسترسی ویژه نیاز نداشته‌اند. این حملات اولین حملات در سطح میان‌هسته‌ای[7] و بین CPU[8] بر روی پردازنده‌های آرم بوده‌اند که قابلیت نظارت و مانیتورکردن لمس[9]ها و کشیدن دست[10]، ضربه‌های روی کیبورد نرم‌افزاری و همچنین زمان‌بندی بین این ضربه‌ها را دارند [۳۳].

روشی جهت استفاده از نشت اطلاعات از تراست‌زون[11] و استفاده از درگیری بین دنیای امن و عادی توسط تراست‌زون جهت استخراج اطلاعات امن از دنیای امن، ارائه شده است و به عنوان اولین حملهٔ زمانی به تراست‌زون از آن نام برده شده است [۳۱]. حملهٔ پرایم+پروب ارائه شده در این مقاله با استفاده از جداول T مربوط به الگوریتم رمزنگاری AES موجود در بسته‌ی اُپن‌اِس.اِس.اِل نسخه‌ی 1.0.1f نشان می‌دهد که از طریق دنیای عادی امکان سرقت یک داده‌ی حساس ریزدانه[12] از دنیای امن با استفاده از حملات کانال جانبی مبتنی بر زمان امکان‌پذیر می‌باشد و بازیابی کامل کلید رمزنگاری AES از طریق هردو حملهٔ معرفی شده در این مقاله به طور کامل انجام شده است. در [۳۴] یک بردار حملهٔ نوین ارائه شده است که یک کانال ذخیره‌ی حافظهٔ نهان[13] کم نویز را که می‌تواند توسط روش‌های آنالیز زمانی کانال شناخته شده مورد بهره‌برداری قرار گیرد، افشا می‌کند. در این مقاله سه حملهٔ متفاوت با استفاده از این بردار حمله بر روی سرویس‌های مورد اطمینان[14] بر روی یک الگوریتم رمزنگاری AES ۱۲۸ بیتی پیاده‌سازی شده توسط کتابخانه‌ی مخصوص ابزارهای نهفته (در بسته‌ی وُلف.اِس.اِس.اِل[15] ارائه شده در [۳۵]) بر روی یک رزبری پای[16] ۲ با تراست‌زون فعال انجام شده است.

در [۳۶] به ارائه‌ی دلیل کمتر ارائه شدن حملات حافظهٔ نهان بر روی آرم و البته سخت‌تر بودن آن‌ها در مقایسه با پردازنده‌های دیگر هم‌چون اینتل اشاره می‌نماید. محور اصلی این مقاله سازوکاری به نام قفل خودکار[17] است که با رونمایی از آن به عنوان یک بهبوددهنده‌ی کارایی داخلی موجود در لایه‌های حافظه‌های نهان شامل در پردازنده‌های آرم، بیان می‌کند که قفل خودکار می‌تواند حملاتی از قبیل اخراج+زمان، پرایم+پروب و

[1] Detection
[2] Benign
[3] Reduced Instruction Set Computer (RISC)
[4] Advanced RISC Machines (ARM)
[5] Embedded Devices
[6] Evict+Reload
[7] Cross-Core
[8] Cross-CPU
[9] Touch
[10] Swipe
[11] TrustZone
[12] Fine-grained
[13] Cache Storage Channel
[14] Trusted Services
[15] WolfSSL
[16] Raspberry Pi
[17] Autolock

اویکت+ریلود توسط مهاجم را تحت تاثیر قرار دهد.

در سال ۲۰۱۸ یک بررسی آسیب‌پذیری‌های حیاتی[1] از معماری تراست‌زون مخصوص سامسونگ با استفاده از مهندسی معکوس پویا و ایستا ارائه شده و اشاره می‌شود که این قابلیت در گوشی‌های پرچم‌دار سامسونگ (موجود در زمان ارائه‌ی مقاله) مورد استفاده قرار گرفته است [۳۷]. همان گروه یک سال بعد به ارائه‌ی حملهٔ مبتنی بر حافظهٔ نهان بر روی تراست‌زون پردازنده‌های آرم و پیاده‌سازی آن بر روی الگوریتم رمزنگاری AES-256 و AES-256-GCM با استفاده از تحلیل مبتنی بر GPU پرداخته‌اند [۳۸]. مقاله‌ی [۳۹] به ارائه‌ی یک حمله زمانی جدید بر روی پردازنده‌ی آرم و پیاده سازی عملی آن بر روی برد رزبری پای ۳ (با پردازنده‌ی آرم سری Cortex-A53) با استفاده از رویداد تصادم پرداخته است.

در سال ۲۰۲۱ در مقاله‌ای حاصل از همکاری اساتید دانشگاه‌های صنعتی شریف و شهید بهشتی، با اشاره به فرض در نظر گرفته شده توسط لیپ و همکاران در [۳۳] در مورد دسترسی به مپینگ[2] آدرس مجازی به فیزیکی از طریق آدرس (/proc/self/pagemap) که یک فاکتور محدودکننده‌ی مهم در لینوکس و اندروید می‌باشد، اشاره می‌کند که دسترسی به این مپینگ نیازمند دسترسی روت توسط مهاجم بوده و در نتیجه حملهٔ ارائه شده در آن مقاله محدود به نسخه‌ی ۴,۴ اندروید شده است زیرا نیازی به دسترسی روت برای مپینگ تا این نسخه نبوده است [۴۰]. در این مقاله یک حملهٔ اویکت+ریلود بر روی پیاده‌سازی AES بر مبنای جداول T موجود در بسته‌ی اُپن‌اِس.اِل نسخه‌ی 1.1.0fپیاده‌سازی شده بر روی دستگاه‌های مبتنی بر آرم، معرفی شده است که شامل دو مرحله‌ی دسته‌بندی مشخصات و اکسپلویت می‌باشد. حملات ارائه شده در این مقاله بر روی دو سری از پردازنده‌های آرم (Cortex-A53 و Cortex-A57) به‌صورت عملی تست شده است.

یک حمله از نوع فلاش+ریلود بر روی پردازندهٔ آرم (ARMv8) از طریق پورت ارتباطی شتاب‌دهنده[3] ارائه شده است که با طراحی یک سخت‌افزار، بدون دسترسی ویژه باعث غیرمعتبر نمودن[4] حافظهٔ نهان در پردازنده‌های آرم از طریق این پورت می‌شود [۴۱]. در واقع با استفاده از IP ایجاد شده یک حملهٔ فلاش+ریلود بر روی جداول T مربوط به AES در مد کاربر بدون دسترسی ویژه انجام شده است که کارایی بهتری را نسبت به حملات قبلی انجام شده مبتنی بر فلاش نشان می‌دهد.

اولین حملهٔ کانال جانبی زمانی مبتنی بر حافظهٔ نهان بر روی دستگاه‌های تلفن همراه Apple در سال ۲۰۲۱ انجام شده است که در آن پیاده‌سازی یک حملهٔ حافظهٔ نهان مبتنی بر دسترسی با استفاده از الگوی پرایم+پروب به الگوریتم رمزنگاری AES موجود در بسته‌ی اُپن‌اِس.اِل نسخه‌ی 1.1.1d به عنوان اثبات مفهوم[5] انجام شده است [۴۲].

۳- روش تحقیق

در این تحقیق ابتدا مقالات مرتبط با حملات مبتنی بر آسیب‌پذیری پردازنده‌ها پس از جمع‌آوری، موردمطالعه و بررسی قرار گرفته و با معرفی چند شاخص (معیار) برای ارزیابی این حملات، به بررسی دقیق‌تر آن‌ها پرداخته می‌شود. به بیان دیگر بر مبنای فرآیند تحلیل سلسله‌مراتبی تعدادی معیار و زیرمعیار تعریف شده تا به کمک آن‌ها بتوان این حملات را بررسی و رتبه‌بندی نمود. برای ارزیابی تأثیرگذاری هریک از این معیارها یک شبکه از خبرگان انتخاب شده است تا بتوان ارزیابی دقیق‌تری از میزان تأثیرگذاری معیارها داشته و جداول مقایسات زوجی بیشترین تطابق را با واقعیت داشته باشد.

پیاده‌سازی این ارزیابی با استفاده از AHP و نرم‌افزار Expert Choice انجام شده است.

در مرحلهٔ بعد میزان خطر گزینه‌های موجود با استفاده از سیستم امتیازدهی آسیب‌پذیری مشترک[6] که به‌اختصار به آن پارامتر CVSS گفته می‌شود، مورد ارزیابی قرار گرفته و حملات بر اساس این پارامتر نیز امتیازبندی خواهند شد. این پارامتر تعریف شده است تا ارتباطی بین مشخصات و شدت یک حمله برقرار نموده و در نهایت با اعلام یک عدد که بیشترین مقدار آن ۱۰ می‌تواند باشد، شدت حملات را امتیازدهی نماید.

۳-۱- تحلیل سلسله‌مراتبی

۳-۱-۱- معیارها و زیرمعیارهای ارزیابی آسیب‌پذیری‌های ریزپردازنده

با بررسی‌های انجام‌گرفته ۴ معیار برای ارزیابی کاربردی بودن حملات احصاء شده است که در ادامه معرفی می‌گردد.

الف) معیارهای زمانی آسیب‌پذیری

این دسته از معیارها مواردی هستند که از نظر زمانی بر حملات اثر نموده و مرتبط با زمان هستند. با بررسی‌های انجام‌گرفته با خبرگان این حوزه زیرمعیارهای زیر برای ارزیابی

[1] Critical
[2] Mapping
[3] Accelerator Coherency Port (ACP)
[4] Invalidation
[5] Proof-of-Concept
[6] Common Vulnerability Scoring System (CVSS)

حملات استفاده شده است:

- زمان عملیاتی‌سازی
هرچه زمان عملیاتی‌سازی کمتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.
- زمان ماندگاری آسیب‌پذیری (ارائهٔ راهکار مقابله یا پچ شدن)
هرچه زمان ماندگاری بیشتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.
- زمان به‌روزرسانی (زمان مورد نیاز جهت به‌روزرسانی حمله)
هرچه زمان به‌روزرسانی کمتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.

ب) امکان‌پذیری

این معیار به بررسی میزان کاربردی یا عملیاتی بودن حمله و در مجموع امکان‌پذیری یک حمله در شرایط واقعی را بررسی می‌نماید. ازآنجایی‌که ممکن است برخی از حملات صرفاً به‌صورت تئوری و با درنظرگرفتن فرض‌های متعدد انجام شده باشد، این معیار کمک می‌کند تا درک بهتری از میزان کاربردی‌بودن و امکان‌پذیری آن به دست آید.

زیرمعیارهایی که برای این معیار در نظر گرفته شده است در زیر آورده شده است:

- وابستگی به پردازنده
هرچه وابستگی کمتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.
- وابستگی به سیستم‌عامل
هرچه وابستگی کمتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.
- سطح دسترسی
هرچه میزان دسترسی لازم کمتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.
- میزان تحقق عملی فرض‌های مسئله
هرچه میزان تحقق عملی فرض‌ها بیشتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.

ج) میزان اثربخشی

زمانی می‌توان گفت که یک حمله موفق بوده است که اثربخشی آن باتوجه‌به هدفی که در نظر گرفته شده است، قابل‌توجه باشد. به‌عبارت‌دیگر باید بتوان با استفاده از تعدادی پارامتر، میزان اثربخشی حملات مختلف را بررسی و ارزیابی نمود تا به هنگام دفاع در برابر این حملات راهکارهای مناسبی برای این منظور انتخاب و اجرا نمود. زیرمعیارهای مربوط به این بخش عبارت‌اند از:

- سطح حمله (میان‌هسته‌ای، بین CPU، بین VMها[1] و...)
هرچه سطح حمله وسیع‌تر باشد پارامتر گزینه عدد بیشتری خواهد داشت.
- درصد بازیابی کلید یا گذرواژه
هرچه درصد بازیابی کلید یا گذرواژه بیشتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.
- قابلیت ایجاد کانال پنهان
هرچه قابلیت ایجاد کانال پنهان بیشتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.

برای زیرمعیار آخر (قابلیت ایجاد کانال پنهان) می‌توان دو زیر معیار دیگر تعریف نمود. به بیان دیگر قابلیت ایجاد کانال پنهان با دو پارامتر پهنای باند و نرخ خطا قابل کمی‌سازی و ارزیابی است که می‌توان به کمک این دو پارامتر این زیر معیار را بهتر بررسی و ارزیابی نمود.

د) منابع مورداستفاده

آخرین معیار برای ارزیابی حملات منابع مورداستفاده برای حمله است که در بسیاری از موارد عامل تعیین‌کننده و حیاتی برای انجام حمله است. باتوجه‌به محدودیت‌های موجود در منابع مورداستفاده معمولاً یک مصالحه[2] بین منابع مورداستفاده ایجاد می‌شود که در تحلیل‌ها بررسی خواهد شد که این محدودیت منابع چطور می‌تواند بر فرآیند انجام حملات تأثیرگذار باشد. زیر معیارهای مرتبط با منابع مورداستفاده موارد زیر خواهند بود:

- حافظه
هرچه حافظهٔ مورداستفاده کمتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.
- داده
هرچه دادهٔ مورداستفاده کمتر باشد پارامتر گزینه عدد بیشتری خواهد داشت.

البته باید توجه داشت که زمان نیز به‌عنوان یکی از منابع در مقالات در نظر گرفته شده است؛ اما باتوجه‌به اینکه پارامتر زمان به‌صورت جداگانه به‌عنوان یک معیار مورد بررسی قرار می‌گیرد، از آوردن مجدد آن به‌عنوان زیر معیار صرف‌نظر شده است.

[1] Cross-VM
[2] Trade-Off

۳-۱-۲- راهکارهای اقدام استفاده از آسیب‌پذیری‌ها

باتوجه‌به مقالات بررسی شده در پیشینهٔ تحقیق حملاتی که در این حوزه امکان‌پذیر هستند به‌عنوان راهکارهای اقدام یا گزینه‌های تصمیم در نظر گرفته شده است. هدف از انتخاب گزینه‌های تصمیم این است که میزان تأثیر معیارها و زیرمعیارهای مختلف بر روی انجام این گزینه‌ها بررسی شده و در نهایت بتوان ارزیابی دقیقی از گزینه‌های بررسی شده به دست آورد. لیست گزینه‌های تصمیم به شرح زیر است:

- حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری

این نوع از حملات شناخته‌شده‌ترین حملات کانال جانبی هستند که در آن‌ها یک شاخصه از دستگاه قربانی که قرار است مورد حمله قرار گیرد، به‌صورت فیزیکی و با استفاده از ابزارهای مخصوص، اندازه‌گیری می‌شود. ویژگی این شاخصه‌ی مورد اندازه‌گیری اینست که می‌بایست اطلاعاتی در مورد پارامترهای مورد حمله توسط مهاجم (همچون کلید رمزنگاری، پسورد، اطلاعات مخفی و ...) بدهد. برخی از این شاخصه‌ها توان مصرفی، صدای تولید شده، تشعشعات الکترومغناطیسی و ... هستند. به عنوان مثال در مورد توان مصرفی می‌توان با استفاده از پروب‌گذاری به‌صورت فیزیکی (سخت افزاری) در محل‌هایی که احتمال می‌رود نشت اطلاعات از آن‌ها منجر به کسب دانشی در مورد پارامترهای مورد حمله شود، به این دستاورد رسید. به عبارت دیگر اگر فرض شود که به عنوان مثال یک عملیات رمزنگاری در مراحل مختلف خود هنگام استفاده از کلیدهای متفاوت توان مصرفی متفاوتی را مصرف نماید و بتوان این توان را به‌صورت فیزیکی (از باس داده، ترانزیستورها و ...) ردگیری[1] نمود، در این حالت امکان انجام این حمله وجود دارد. مقالات ارائه شده در [۴۲,۴۳] دو نمونه از این نوع از تحلیل کانال جانبی آورده شده است که به عنوان مثال در [۴۳] یک تحلیل توان بر روی رمز آیدا[2] انجام شده است.

- حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری

اخیراً ماژولی در ساختار پردازنده‌های اینتل شناسایی شده است که وظیفهٔ آن اندازه‌گیری توان مصرفی در پردازنده است و با نام RAPL[3] شناخته می‌شود. این ماژول از نظر عملکردی می‌تواند جایگزین پروب‌گذاری در حملهٔ قبلی شده و به‌صورت نرم‌افزاری اطلاعات مربوط به اندازه‌گیری توان را در اختیار قرار دهد. بنابراین می‌توان گفت حملهٔ انجام شده با این روش که در [۴۵] معرفی شده است، از نظر رویکرد به حملهٔ قبلی شباهت دارد اما اندازه‌گیری‌ها به‌صورت نرم‌افزاری انجام شده و در نتیجه دسترسی به سخت‌افزار به‌صورت فیزیکی و پروب‌گذاری فیزیکی در آن حذف شده است.

- حملهٔ مبتنی بر زمان

حملات مبتنی بر زمان اولین حملات ارائه شده در این حوزه بودند که اولین‌بار کوچر در [۴۶] از این حمله بر روی پیاده‌سازی دیفی-هلمن استفاده نمود. در این نوع از حمله مهاجم می‌تواند با توجه به زمان اجرای یک عملیات (پیاده‌سازی الگوریتم رمزنگاری، محاسبه‌ی هش، عملیات بر روی گذرواژه و ...) و تفاوت زمانی موجود بین عملیات‌های مختلف، اطلاعات مهمی را از سیستم قربانی استخراج نموده و مورد سوءاستفاده قرار دهد. این حملات به طور کلی با نام حملات زمانی[4] شناخته می‌شوند که به دسته‌بندی‌های مختلفی قابل تقسیم‌بندی هستند.

- حملهٔ مبتنی بر حافظهٔ نهان

پردازش دستورالعمل‌ها و دسترسی به حافظه به‌صورت سلسله‌مراتبی صورت می‌گیرد به این معنی که در لایهٔ اول پردازنده (در اینجا همان CPU) قرار دارد که سرعت پردازش بسیار بالایی داشته و وظیفهٔ پردازش اطلاعات را دارد. درصورتی‌که پردازنده به داده‌ای نیاز داشته باشد، اولین جایی که در آن جستجو می‌کند حافظهٔ نهان است. حافظهٔ نهان یک حافظه معمولاً از نوع RAM ایستا[5] (SRAM) می‌باشد که اندازهٔ کوچک اما سرعت دسترسی بسیار بالایی داشته و در پردازنده‌های مختلف تعداد سطوح یا لایه‌های متفاوتی دارد؛ اما به طور معمول در پردازنده‌های جدید شرکت اینتل دارای ۳ لایه به نام‌های L1، L2 و L3 می‌باشد. سطح L1 نزدیک‌ترین سطح به پردازنده بوده که دارای بیشتری سرعت و کمترین اندازه است. سطح L2 لایهٔ میانی بوده و سطح L3 که دورترین سطح نسبت به پردازنده است، اندازه‌ای به‌مراتب بزرگ‌تر و کمترین سرعت را دارد. در صورت عدم وجود داده در حافظهٔ نهان به ترتیب لایه‌های بعدی حافظهٔ اولیه[6] (اغلب همان RAM) و حافظهٔ ثانویه (که می‌تواند هارد، لوح فشرده[7] (CD)، لوح همه‌کارهٔ دیجیتال[8] (DVD)، فلش و... باشد) مورد بررسی قرار می‌گیرند.

در حملات مبتنی بر حافظهٔ نهان از ضعف موجود در فرآیند ذخیره‌سازی در حافظهٔ نهان استفاده شده و منجر به نشت اطلاعات خواهد شد.

- حملهٔ مبتنی بر ریز معماری

[1] Trace
[2] IDEA
[3] Running Average Power Limit (RAPL)
[4] Timing Attacks
[5] Static RAM
[6] Primary Memory
[7] Compact Disk
[8] Digital Versatile Disk

پیشرفت روزافزون در به‌کارگیری روش‌های طراحی، باعث بهبود کارایی پردازنده‌های جدید شده که این امر موجب افزایش پیچیدگی‌های این پردازنده‌ها شده است. آنچه که به‌عنوان معماری مجموعه دستورالعمل[1] (به طور مخفف ISA) ارائه می‌شود، در واقع یک خلاصه‌ای از پردازنده و معماری آن می‌باشد و در مورد پیاده‌سازی واقعی پردازنده مطلبی را ارائه نمی‌کند. باید گفت که جزئیات پیاده‌سازی یک ISA به‌وسیلهٔ ریز معماری تعیین می‌شود که بین پردازنده‌های مختلف که حتی با ISAهای یکسان پیاده‌سازی شده‌اند نیز می‌تواند متفاوت باشد. پارامترهای ریز معماری متنوعی وجود دارند که به‌منظور بهبود کارایی پردازنده‌ها در آن‌ها قرار گرفته‌اند که از جمله‌ی آن‌ها می‌توان به موارد زیر اشاره نمود:

- خط لولهٔ دارای اجرای خارج از ترتیب به جهت موازی‌سازی اجرا
- پیش‌بینی‌کننده‌های متنوع برای کاهش زمان توقف پردازنده‌ها
- حافظهٔ نهان به جهت کاهش تأخیر داده‌هایی که به‌صورت مکرر استفاده می‌شوند
- محیط اجرایی امن برای ایزوله نمودن فضای اجرایی پردازش‌هایی که از پردازش‌های عادی نیاز به امنیت بیشتری دارند

باتوجه‌به آنچه که بیان شد، درصورتی‌که هر بهبودی که توسط ریز معماری انجام می‌شود، تأثیر قابل مشاهده‌ای در کارایی پردازنده داشته باشد، اگر این بهبود وابسته به داده یا فراداده[2] باشد، نشت اطلاعات رخ خواهد داد که بدین معنی است که اگر یک عملیات به‌ازای ورودی‌های خاصی منابع کمتری (همچون توان، زمان و...) استفاده کند، مشاهدهٔ این بهبود توسط مهاجم به او اجازه می‌دهد که در مورد این ورودی‌ها بتواند حدس‌هایی بزند که در نتیجه این نشت اطلاعات منجر به حملاتی خواهد شد که به آن‌ها حملات ریز معماری[3] گفته می‌شود.

وظیفهٔ محیط اجرایی امن حفاظت از یکپارچگی کد و داده و همچنین محرمانگی داده است. این ساختارها به‌مرور در پردازنده‌های مختلف طراحی و پیاده‌سازی شده‌اند که از جمله‌ی آن‌ها می‌توان به SGX[4] در پردازنده‌های اینتل و TeustZone در پردازنده‌های مبتنی بر نشانه اشاره نمود. در هر دو ساختار معرفی شده پیاده‌سازی معماری پردازنده به شکلی طراحی شده است که دو بخش مجزا به نام‌های دنیای عادی[5] و دنیای امن[6] دارد و در این حالت پردازش‌های عادی در دنیای عادی و پردازش‌های خاص همچون پردازش کلیدهای رمزنگاری، گذرواژه‌ها و... در دنیای امن انجام خواهد شد. این نوع از حملات در دستهٔ حملات مبتنی بر ریز معماری قرار می‌گیرند.

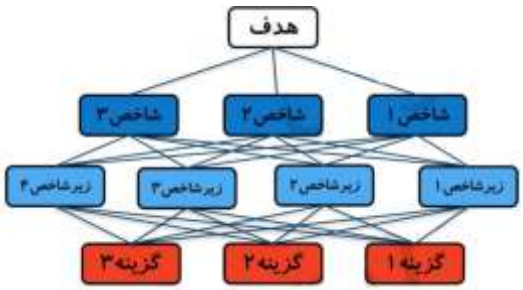
حملات Meltdown و Spectre که به ترتیب در [۴۷] و [۴۸] معرفی شده‌اند، نمونه‌ای از این نوع حملات هستند. پس از معرفی این دو حمله حملات زیادی مشابه آن‌ها منتشر شده است که در [۴۹] یک تقسیم‌بندی در مورد این این حملات انجام گرفته است.

- حملهٔ مبتنی بر هوش مصنوعی

با پیدایش و توسعه‌ی سریع هوش مصنوعی در سال‌های اخیر سوءاستفاده‌ها و حملات مبتنی بر آن نیز ظهور نموده و در خال توسعه است. به عنوان مثال مقالات [۵۰] و [۵۱] در این دسته جای می‌گیرند. در [۵۰] یک حملهٔ کانال جانبی توان بر روی شبکه‌ی عصبی معرفی شده است که در آن معماری شبکه‌ی عصبی را با دقت ۹۰ درصد شناسایی نموده و با کاهش فضای جستجو در مورد نوع شبکه و تعداد لایه‌های آن، شناسایی معماری شبکه‌ی عصبی مورد حمله را آسان‌تر می‌نماید. همچنین در [۵۱] با استفاده از یادگیری عمیق[7] بیان شده است که می‌توان حملات مبتنی بر ریز معماری را پیش‌بینی نمود. با توجه به این موارد توجه به این دسته از حملات و بررسی آن‌ها به عنوان یکی از گزینه‌های تصمیم لازم است.

۳-۱-۳- تشکیل سلسله مراتب تصمیم‌گیری

پس از معین شدن هدف، معیارها، زیرمعیارها و گزینه‌های تصمیم، می‌توان سلسله‌مراتب تصمیم را تشکیل داد که این سلسله‌مراتب جهت تصمیم‌گیری در ۴ سطح همانند مثالی که در شکل(۳) آورده شده است، تشکیل شده است.



شکل (۳). مثالی از سلسله مراتب تصمیم [52]

۴-۱-۳- بررسی سازگاری در نتایج

[1] Instruction Set Architecture
[2] Meta Data
[3] Microarchitectural Attacks
[4] Software Guard Extensions (SGX)
[5] Normal World
[6] Secure World
[7] Deep Learning

باتوجه‌به اینکه در روش تحلیل سلسله‌مراتبی تصمیمات گرفته شده بر مبنای قضاوت خبرگان انجام می‌شود، می‌بایست یک معیاری وجود داشته باشد تا عدم تطابق نظرات با یکدیگر و یا خطا در ارائهٔ نظرات را مشخص و بررسی نمود. معیاری که برای این کار معمولاً استفاده می‌شود، نرخ ناسازگاری[1] است که باتوجه‌به عدد محاسبه شده برای آن می‌توان بررسی نمود که ناسازگاری در نظرات تا چه حد وجود دارد. اگر این عدد بیشتر از ۱۰ درصد باشد، به این معنی است که ناسازگاری در نظرات زیاد است و می‌بایست پرشسنامه مجددا بین خبرگان توزیع شده تا نظرات اصلاحی خود را بیان کنند و تجدید نظر در این حوزه صورت گیرد. نرخ ناسازگاری کمتر از ۱۰ درصد بیانگر قابل قبول بودن ناسازگاری در نظرات و صحیح بودن روش در انجام پرسش‌ها خواهد بود.

۳-۲- پارامترهای مربوط به ارزیابی خطر

همان‌طور که در بالا ذکر شد، در این مرحله با استفاده از پارامتر CVSS به تحلیل میزان خطر حملات پرداخته می‌شود. CVSS نسخهٔ ۴/۰ دارای چهار دسته معیار برای اندازه‌گیری می‌باشد که هرکدام از این معیارها دارای زیر پارامترهایی هستند که با مقداردهی به هرکدام از آن‌ها و انجام محاسبات مربوطه که در [53] آورده شده است، مقدار عددی محاسبه شده برای آن حمله به دست خواهد آمد.

۳-۲-۱- معیارهای امتیاز پایه

الف) معیارهای مربوط به قابلیت بهره‌برداری

این معیارها عبارت‌اند از: بردار حمله (شامل پارامترهای شبکه، شبکهٔ مجاور، محلی و فیزیکی)، پیچیدگی حمله (کم یا زیاد)، نیازمندی‌های[2] حمله (هیچ یا وجود دارد)، سطح دسترسی مورد نیاز (هیچ، کم‌وزیاد) و تعامل کاربر[3] (هیچ، فعال و غیرفعال)

هرکدام از این معیارها می‌توانند مقادیر بیان شده داخل پرانتز را داشته باشند.

ب) معیارهای مربوط به تأثیر

سه معیار محرمانگی، یکپارچگی و دسترس‌پذیری در این قسمت مقداردهی می‌شوند که هرکدام می‌توانند مقادیر تأثیر هیچ، کم یا زیاد را بپذیرند. این سه معیار بک بار برای سیستم آسیب‌پذیر و یک‌بار برای سیستم‌های تحت‌تأثیر[4] آن امتیازدهی می‌شوند. با تجمیع مقادیر این قسمت با معیارهای مربوط به قابلیت بهره‌برداری، پارامتر امتیاز پایهٔ CVSS به دست می‌آید.

۳-۲-۲- معیار تهدید

این معیار تنها یک زیر معیار دارد که میزان بلوغ بهره‌برداری از آسیب‌پذیری را نشان می‌دهد و می‌تواند مقادیر تعریف‌نشده، حمل‌شده، اثبات مفهوم و یا گزارش نشده را بپذیرد.

۳-۲-۳- معیارهای امتیاز محیطی

پارامترهای این معیارها دقیقاً مشابه معیارهای پایه هستند با این تفاوت که به گزینه‌های هرکدام از آن‌ها یک گزینهٔ تعریف نشده اضافه شده است. می‌توان گفت این معیارها معیارهای پایهٔ اصلاح شده هستند و بر اساس قرارگیری اجزا در زیرساخت سازمان مورد نظر مقادیر آن‌ها در این بخش به آن‌ها داده می‌شود که ممکن است با مقادیر داده شده در بخش پایه متفاوت باشد. علاوه بر این مقادیر سه زیرمعیار نیازمندی‌های محرمانگی، نیازمندی‌های یکپارچگی و نیازمندی‌های دسترس‌پذیری نیز وجود دارد که به‌طورکلی با عنوان نیازمندی‌های امنیتی نام‌گذاری شده است و می‌توانند مقادیر تعریف نشده، کم، متوسط و زیاد را بپذیرند. این سه معیار به‌منظور سفارشی‌سازی ارزیابی مصرف‌کننده بر اساس نوع نیاز به هریک از این سه معیار تعریف شده است و هرچه میزان امنیت مورد نیاز کمتر باشد، امتیاز کمتر خواهد بود.

۳-۲-۴- معیارهای تکمیلی

این معیارها که در CVSS نسخهٔ ۴/۰ اضافه شده‌اند، اختیاری بوده که ویژگی‌های خارجی اضافی یک آسیب‌پذیری را توصیف نموده و بر امتیاز نهایی محاسبه شده تاثیری ندارد. این معیارها عبارتند از: ایمنی[5](تعریف نشده، موجود و قابل صرف نظر)، قابلیت خودکارسازی (تعریف نشده، خیر و بله)، فوریت ارائه‌دهنده[6] (تعریف نشده، قرمز، قهوه‌ای، سبز و پاک[7])، قابلیت بازیابی (تعریف نشده، خودکار، توسط کاربر و غیرقابل بازیابی)، چگالی ارزش[8] (تعریف نشده، پراکنده و متمرکز) و تلاش برای پاسخگویی به آسیب‌پذیری (تعریف نشده، کم، درحد متوسط و زیاد)

در نهایت از مجموع این معیارهای کلی و با انجام محاسبات پارامتر CVSS نهایی به دست خواهد آمد که مقدار آن از ۰ تا ۱۰ می‌تواند باشد و هرچه بیشتر باشد نشان‌دهندهٔ خطر بیشتر آسیب‌پذیری و حملهٔ مرتبط با آن می‌باشد.

[1] Inconsistency
[2] Requirements
[3] User interaction
[4] subsequent
[5] Safety
[6] Provider Urgency
[7] Clear
[8] Value Density

۴- نتایج و بحث

۴-۱- نتایج مربوط به تحلیل سلسله‌مراتبی

پس از مشخص‌شدن بخش‌های مختلف سلسله‌مراتب تصمیم، جداول مربوط به مقایسات زوجی به توجه به نظرات خبرگان تعیین گردیده و محاسبات مربوط تعیین وزن‌ها باتوجه‌به تعداد زیرمعیارها با استفاده از نرم‌افزار Expert Choice انجام گردید که نتایج آن در ادامه آورده می‌شود.

نتایج حاصل از محاسبات مربوط به تعیین وزن معیارها و زیرمعیارها در جدول (۱) آورده شده است. همان‌طور که مشاهده می‌شود، با توجه به وزن‌های محاسبه شده، **میزان اثربخشی** در میان معیارهای اصلی وزن بالایی را به خود اختصاص داده است و پس از آن امکان‌پذیری حمله است که منطقی به نظر می‌رسد. به عبارت دیگر با توجه به مقایسات زوجی و محاسبات انجام شده اثربخشی یک حمله دارای بیشترین اهمیت در بین پارامترهای مورد بررسی بوده و پس از آن امکان‌پذیری در رتبه‌ی دوم قرار دارد. در میان تمام زیرمعیارها نیز سه پارامتر درصد بازیابی کلید(گذرواژه)، سطح دسترسی و قابلیت ایجاد کانال پنهان بیشترین وزن را به خود اختصاص داده‌اند. به بیان دیگر اهمیت درصد بازیابی کلید(گذرواژه) در بین زیرمعیارها برای تعیین گزینه‌های تصمیم از بقیه بیشتر بوده و پس از آن سطح دسترسی مورد نیاز برای انجام حمله و قابلیت ایجاد کانال پنهان به ترتیب با اهمیت هستند.

در این بررسی مشخص گردید اهمیت معیار منابع مورداستفاده از دیگر معیارها پایین‌تر است که البته باید توجه داشت که معیار زمان باتوجه‌به حضور در یک معیار جداگانه از زیرمعیارهای این بخش حذف شد. به جهت دقت در ارزیابی همهٔ پارامترها و اینکه این مصالحهٔ بین زمان، حافظه و داده در بسیاری از حمله‌ها مهاجم را با چالش جدی مواجه می‌کند، این معیار می‌تواند در جای خود از اهمیت برخوردار باشد.

جدول (۱). معیارها، زیرمعیارها و وزن‌های آن‌ها

زمان	۰,۱۷۸	زمان عملیاتی‌سازی	۰,۳۳۳	۰,۰۴۸
		زمان ماندگاری	۰,۵۷	۰,۱۰۱
		زمان به‌روزرسانی	۰,۰۹۷	۰,۰۱۹
امکان‌پذیری	۰,۲۷۴	وابستگی به پردازنده	۰,۰۸۷	۰,۰۲۱
		وابستگی به سیستم‌عامل	۰,۰۷	۰,۰۱۹
		سطح دسترسی	۰,۵۶۲	۰,۱۵۴
		تحقق عملی فرض‌ها	۰,۲۸۱	۰,۰۸۲
میزان اثربخشی	۰,۴۶۲	میزان گستردگی حمله	۰,۰۹۴	۰,۰۴۹
		درصد بازیابی کلید(گذرواژه)	۰,۶۲۷	۰,۲۸۹
		قابلیت ایجاد کانال پنهان	۰,۲۸	۰,۱۳۹
منابع مورداستفاده	۰,۰۸۶	حافظه	۰,۶۶۷	۰,۰۴۶
		داده	۰,۳۳۳	۰,۰۳۲

۴-۱-۱- نتایج کلی ارزیابی گزینه‌های تصمیم

در جدول (۲) نتایج ارزیابی۶ گزینه‌ی تصمیم با توجه به محاسبات انجام شده بر اساس مقادیر وزنی معیارها و زیرمعیارها و همچنین مقادیر داده شده بر اساس مقایسه‌ی بین گزینه‌های تصمیم با توجه به هر کدام از زیرمعیارها، آورده شده و براساس وزن آن‌ها رتبه‌بندی شده‌اند. نرخ ناسازگاری کلی در مجموع برابر ۰,۰۶ شده است و درنتیجه می‌توان گفت که قضاوت‌های انجام شده در مورد مجموع معیارها و زیرمعیارها از نظر ناسازگاری قابل قبول هستند. همچنین در ارزیابی مربوط به هرکدام از معیارها نیز این نرخ ناسازگاری برای هر ۴ معیار زیر ۱۰ درصد بود که برای این تحلیل قابل قبول است.

جدول (۲). نتایج کلی ارزیابی گزینه‌های تصمیم

حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری	۰,۰۸۳	۶
حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری	۰,۱۷۶	۳
حملهٔ مبتنی بر زمان	۰,۲۹۷	۱
حملهٔ مبتنی بر حافظهٔ نهان	۰,۱۸۵	۲
حملهٔ مبتنی بر ریز معماری	۰,۱۰۴	۵
حملهٔ مبتنی بر هوش مصنوعی	۰,۱۵۵	۴
نرخ ناسازگاری کلی: ۰,۰۶		

مشاهده می‌شود که در مجموع **حملهٔ مبتنی بر زمان** باتوجه‌به ارزیابی معیارهای چهارگانه بیشترین وزن را به خود اختصاص داده و به‌عنوان اولین گزینهٔ منتخب در بین ۶ گزینه‌ی موجود معرفی می‌شود. پس از آن به ترتیب دو حملهٔ مبتنی بر حافظهٔ نهان و حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری با اختلاف بسیار کمی در رتبه‌ی دوم و سوم هستند و می‌توان گفت که اولویت چندانی نسبت به یکدیگر ندارند. البته می‌بایست رتبه‌بندی حملات بر اساس هرکدام از ۴ معیار (که در ادامه مورد بررسی قرار خواهد گرفت) به تفکیک انجام شده و با توجه به شرایط و فرضیاتی که در عمل ممکن است محدودیت‌هایی ایجاد نماید، اولویت در انجام این حملات مورد بررسی قرار گیرد.

حملهٔ مبتنی بر هوش مصنوعی در رتبهٔ چهارم قرار گرفته است. باید به این نکته توجه داشت که این نوع از حملات باتوجه‌به جدید بودن، پیچیدگی‌های خاص خود را داشته و ممکن است باتوجه‌به این پیچیدگی‌ها به‌عنوان‌مثال از معیارهایی همچون منابع امتیاز مناسب را کسب نکنند و در رتبه‌بندی پایین‌تر قرار گیرند؛ اما باتوجه‌به کاربرد مورد انتظار این احتمال وجود داشته باشد که بتوان به بهره‌وری بهتری با این حملات رسید.

به‌عنوان‌مثال در این رتبه‌بندی حملهٔ مبتنی بر ریز معماری در ارزیابی کلی در رتبهٔ پنجم قرار گرفته است؛ اما مشاهدهٔ نتایج حاصل از تحلیل گزینه‌ها بر اساس ۴ معیار موجود، نشان می‌دهد که این حمله از نظر امکان‌پذیری (مطابق جدول (۴)) رتبه‌ی ۴ را دارد و حملات انجام شده در مقالات گزارش شده در بخش مرور تاریخچه نیز صحت این مطلب را تایید می‌کند.

۴-۱-۲- نتایج ارزیابی گزینه‌های تصمیم از منظر زمان

جدول (۳) نتایج تحلیل گزینه‌ها از منظر زمان را نشان می‌دهد که در آن نرخ ناسازگاری معیارها برابر با ۰,۰۶ است که نرخ قابل قبولی است. مشاهده می‌شود که در این رتبه‌بندی همچنان رتبه‌ی اول مربوط به حملهٔ مبتنی بر زمان است اما رتبه‌ی دوم به حملهٔ مبتنی بر هوش مصنوعی اختصاص پیدا نموده است. باید توجه داشت که با وجود اینکه این دسته از حملات در فازهای مربوط به آموزش ممکن است از نظر زمانی از دیگر حملات ضعیف‌تر و طولانی‌تر باشند، اما در مجموع پارامترهای زمانی همچون ماندگاری می‌توانند بهتر عمل کرده و مزیت داشته باشند. رتبه‌ی سوم به‌صورت مشترک با امتیاز دقیقا مشابه هم به دو حملهٔ مبتنی بر حافظهٔ نهان و حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری اختصاص یافته است. ترتیب رتبه‌بندی در این بخش تقریبا مشابه ارزیابی کلی حملات است با این تفاوت که حملهٔ مبتنی بر هوش مصنوعی از رتبه‌ی ۴ به رتبه‌ی ۲ رسیده است.

جدول (۳). نتایج تحلیل گزینه‌ها از منظر زمان

حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری	۰,۰۵۵	۶
حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری	۰,۱۶۹	۳
حملهٔ مبتنی بر زمان	۰,۲۹۴	۱
حملهٔ مبتنی بر حافظهٔ نهان	۰,۱۶۹	۳
حملهٔ مبتنی بر ریز معماری	۰,۰۸۱	۵
حملهٔ مبتنی بر هوش مصنوعی	۰,۲۳۳	۲
نرخ ناسازگاری: ۰,۰۶		
وزن معیار زمان: ۰,۱۷۸		

۴-۱-۳- نتایج ارزیابی گزینه‌های تصمیم از منظر امکان‌پذیری

گزینه‌های حمله از نظر امکان‌پذیری نیز مورد ارزیابی قرار گرفته‌اند که نتایج محاسبات آن در جدول (۴) آورده شده است که نرخ ناسازگاری در آن ۰,۰۷ است. اولین نکته‌ی قابل توجه در این رتبه‌بندی وزن مربوط به حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری است که این گزینه علیرغم حضور در رتبه‌ی بالاتر در مقایسات قبل، در اینجا با اختلاف کمی با حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری در رتبه‌ی آخر قرار گرفته است. یکی از دلایلی که برای این موضوع می‌توان بیان نمود، وابستگی این حمله به سیستم‌عامل لینوکس است که جزء زیرمعیارهای امکان‌پذیری است. نکته‌ی دیگر اینکه اجرای این حمله با توجه به جدید بودن آن شرایط خاصی نیاز دارد که شاید تحقق عملی فرض‌ها و حتی سطح دسترسی را تحت تاثیر قرار دهد. البته در نگاه کلی‌تر می‌توان اینطور در نظر گرفت که احتمالا این حملهٔ نیاز به نوآوری‌های بیشتر در جهت کاربردی‌تر نمودن آن دارد که می‌تواند مورد توجه قرار گیرد. ایده‌ای که برای ادامه‌ی کار در این حوزه باید بررسی شود، توسعه‌ی این نوع حمله با توجه به محدودیت‌های موجود و حتی تغییر در پردازنده‌های مورد حمله است به طوریکه امکان‌پذیری آن را افزایش دهد.

حملهٔ مبتنی بر حافظهٔ نهان در این ارزیابی در جایگاه دوم قرار دارد که بیانگر امکان‌پذیری مناسب این نوع از حملات است و ارزیابی‌های انجام‌گرفته از مقالات ارائه شده در این حوزه نشان می‌دهد که در سال‌های اخیر این حمله جایگاه ویژه‌ای در بین حملات کانال جانبی داشته است.

حضور حملهٔ مبتنی بر هوش مصنوعی در رتبهٔ سوم نیز نشان‌دهندهٔ سرعت پیشرفت این حمله در سال‌های اخیر است که باوجوداینکه نسبت به دیگر حملات مورد بررسی سابقهٔ کمتری داشته است، اما از نشر امکان‌پذیری حمله شرایط خوبی را دارد.

حملهٔ مبتنی بر ریز معماری نیز در جایگاه چهارم قرار دارد. درصورتی‌که بتوان در این نوع از حمله برخی از پیچیدگی‌های موجود در اجرای حمله (به‌عنوان‌مثال در حملات مبتنی بر محیط اجرایی امن) را کاهش داده و پارامترهای مربوط به دیگر معیارها را بهبود داد، این حمله قابلیت این را دارد تا اولویت بهتری را در مقایسات کسب نموده و در عمل به‌عنوان یکی از حملات مؤثر معرفی شود.

جدول (۴). نتایج تحلیل گزینه‌ها از منظر امکان‌پذیری

حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری	۰,۱۰۵	۵
حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری	۰,۱۰۴	۶
حملهٔ مبتنی بر زمان	۰,۳۳۸	۱
حملهٔ مبتنی بر حافظهٔ نهان	۰,۱۸۱	۲
حملهٔ مبتنی بر ریز معماری	۰,۱۱۳	۴
حملهٔ مبتنی بر هوش مصنوعی	۰,۱۵۹	۳
نرخ ناسازگاری: ۰,۰۷		
وزن معیار امکان‌پذیری: ۰,۲۷۴		

۴-۱-۴- نتایج ارزیابی گزینه‌های تصمیم از منظر اثربخشی

معیار سوم برای ارزیابی حملات اثربخشی بود که در جدول (۵) وزن‌های به دست آمده برای این معیار آورده شده است. در این ارزیابی نیز نرخ ناسازگاری برابر با عدد ۰,۰۷ بوده و رتبه‌های حملات با رتبه‌های مربوط به ارزیابی کلی حملات مشابه هستند. با این تفاوت که حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری و حملهٔ مبتنی بر حافظهٔ نهان در این تحلیل جابه‌جا شده و حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری با اختلاف رتبه‌ی دوم را کسب نموده است. به عبارت دیگر می‌توان این‌طور تحلیل نمود که این نوع حمله با توجه به عملکرد آن، اثربخشی بیشتری را نسبت به حملهٔ مبتنی بر حافظهٔ نهان دارد و به همین جهت رتبه‌ی بالاتری را به خود اختصاص داده است. در صورت انجام نوآوری‌های بیان شده بر روی این حمله و بهبود معیار امکان‌پذیری آن می‌تواند کاربرد مناسبی در اجرا داشته باشد.

ازآنجایی‌که این معیار بیشترین وزن (۰,۴۶۲) را در بین معیارها دارد، وزن‌های مربوط به حملات در این معیار تاثیر بیشتری بر روی وزن میانگین خواهد گذاشت و مشابه بودن رتبه‌بندی این معیار با رتبه‌بندی کلی نیز بیانگر همین موضوع است.

جدول (۵). نتایج تحلیل گزینه‌ها از منظر میزان اثربخشی

حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری	۰,۰۴۶	۶
حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری	۰,۲۲۸	۲
حملهٔ مبتنی بر زمان	۰,۲۸۲	۱
حملهٔ مبتنی بر حافظهٔ نهان	۰,۱۹۴	۳
حملهٔ مبتنی بر ریز معماری	۰,۱۰۷	۵
حملهٔ مبتنی بر هوش مصنوعی	۰,۱۴۳	۴
نرخ ناسازگاری: ۰,۰۷		
وزن معیار اثربخشی: ۰,۴۶۲		

۴-۱-۵- نتایج ارزیابی گزینه‌های تصمیم از منظر منابع مورد استفاده

منابع مورد استفاده آخرین معیار مورد نظر برای ارزیابی بوده که باتوجه‌به وزن کمتر آن تأثیر کمتری بر روی نتایج کلی خواهد داشت. نتایج این ارزیابی در جدول (۶) آورده شده است که نرخ ناسازگاری در آن ۰,۰۶ شده است و قابل قبول است. از نتایج این

جدول مشاهده می‌شود که همچنان **حملهٔ مبتنی بر زمان** رتبه‌ی اول را داشته و در نتیجه کمترین میزان استفاده از منابع را در بین حملات خواهد داشت. رتبه‌ی بعد متعلق به حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری است که به دلیل دسترسی فیزیکی به ابزارهای مورد حمله، منابع مورد استفاده در این حمله به نسبت کمتر خواهد بود. رتبه‌ی سوم در این ارزیابی مربوط به حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری است. به عبارت دیگر این حمله علیرغم نیاز به ردگیری از میزان توان مورد استفاده‌ی سیستم مورد حمله، از سه حمله‌ی دیگر نیاز به داده و حافظهٔ کمتری برای انجام دارد. قرارگیری حملهٔ مبتنی بر هوش مصنوعی در رتبه‌ی پنجم به این معنی است که این حمله علاوه بر اینکه به داده‌های متنوع و زیادی در مورد هدف مورد نظر یا اهداف مشابه آن نیاز دارد، برای فاز اجرا (و البته فاز آموزش) نیز به حافظهٔ به نسبت بیشتر از ۴ حمله‌ی با رتبه‌ی قبل از آن نیاز دارد.

جدول (۶). نتایج تحلیل گزینه‌ها از منظر منابع مورد استفاده

حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری	۰,۲۹۸	۲
حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری	۰,۱۲۷	۳
حملهٔ مبتنی بر زمان	۰,۲۵۷	۱
حملهٔ مبتنی بر حافظهٔ نهان	۰,۱۷۲	۴
حملهٔ مبتنی بر ریز معماری	۰,۱۰۱	۶
حملهٔ مبتنی بر هوش مصنوعی	۰,۰۴۵	۵
نرخ ناسازگاری: ۰,۰۶		
وزن معیار هزینه: ۰,۰۸۶		

۴-۲- نتایج مربوط به ارزیابی خطر

با انجام مقداردهی به معیارهای مربوط به پارامتر CVSS، مقادیر نهایی خروجی محاسبه شده و به دست آمد که در جدول (۷) آورده شده است. همچنین با اتمام مقداردهی به معیارها یک‌رشته از موارد انتخاب شده برای هر گزینه قابل‌استخراج است که در جدول (۸) آورده شده است. پارامتر CVSS برای حملهٔ مبتنی بر زمان دارای بیشترین مقدار بوده و در نتیجه این حمله بیشترین آسیب را برای قربانی در پی خواهد داشت. حملهٔ مبتنی بر ریز معماری و حملهٔ مبتنی بر حافظهٔ نهان نیز اعداد بالای ۷ را به خود اختصاص داده‌اند. لازم به ذکر است که طبق [۵۴] برای پارامتر CVSS عدد بین ۷ تا ۸/۹ به معنی خطر بالای حمله بوده و نشان می‌دهد که شدت حملهٔ انجام شده و میزان تخریب آن بالا می‌باشد و اگر این عدد بالای ۹ باشد به معنای بحرانی بودن شدت حمله است. عدد بین ۴ تا ۶/۹ بیانگر تخریب متوسط و زیر ۴ تخریب پایین را نشان می‌دهد. حمله ی مبتنی بر هوش مصنوعی با مقدار ۶/۹ نزدیک به مقدار ۷ بوده و نشان‌دهنده‌ی اهمیت این نوع جدید از حملات و میزان آسیبی است که به قربانی وارد می‌سازند. به بیان دیگر با توسعه‌ی بیشتر این دسته از حملات می‌توان انتظار داشت این امتیاز و در نتیجه شدت و میزان آسیب حملات بیشتر شود.

جدول (۷). نتایج محاسبات مربوط به امتیاز پایه

۱	**حملهٔ کانال جانبی توان با اندازه‌گیری سخت‌افزاری**	۵,۶	متوسط	۶
۲	**حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری**	۵,۷	متوسط	۵
۳	**حملهٔ مبتنی بر زمان**	۹,۳	زیاد	۱
۴	**حملهٔ مبتنی بر حافظهٔ نهان**	۸,۲	زیاد	۳
۵	**حملهٔ مبتنی بر ریز معماری**	۸,۶	زیاد	۲
۶	**حملهٔ مبتنی بر هوش مصنوعی**	۶,۹	متوسط	۴

جدول (۸). رشته‌ی خروجی CVSS برای پارامترهای انتخاب شده

۱	CVSS:4.0/AV:P/AC:L/AT:P/PR:H/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:A/CR:H/MAV:P/MAC:L/MAT:P/MPR:H/MUI:P/MVC:H/MSC:H/AU:N/V:D/RE:L/U:Red
۲	CVSS:4.0/AV:L/AC:L/AT:P/PR:H/UI:A/VC:H/VI:L/VA:N/SC:H/SI:N/SA:N/E:A/CR:H/MAV:L/MAC:L/MAT:P/MPR:H/MUI:A/MVC:H/MVI:L/MSC:H/MSI:L/S:N/AU:Y/V:D/RE:M/U:Red
۳	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:L/VA:N/SC:H/SI:L/SA:N/E:A/CR:H/MAV:N/MAC:L/MAT:N/MPR:L/MUI:N/MVC:H/MVI:H/MSC:H/MSI:H/S:N/AU:Y/V:D/RE:M/U:Red

۴	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:N/SC:H/SI:L/SA:N/E:A/CR:H/IR:L/MAV:L/MAC:L/MAT:N/MPR:L/MUI:N/MVC:H/MVI:L/MSC:H/MSI:L/AU:Y/V:D/RE:L/U:Red
۵	CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:N/SC:H/SI:L/SA:N/E:A/CR:H/IR:M/MAV:A/MAC:L/MAT:P/MPR:L/MUI:N/MVC:H/MVI:H/MSC:H/MSI:H/AU:Y/V:D/RE:H/U:Red
۶	CVSS:4.0/AV:A/AC:H/AT:P/PR:L/UI:P/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N/E:A/CR:H/IR:M/MAV:A/MAC:L/MAT:P/MPR:L/MUI:P/MVC:H/MVI:H/MSC:H/MSI:H/AU:Y/V:C/RE:M/U:Red

علاوه بر امتیاز CVSS نهایی که پس از انتخاب زیرمعیارها محاسبه می‌شود، می‌توان در مورد ۶ پارامتر قابلیت بهره‌برداری حمله، پیچیدگی حمله، سیستم آسیب‌پذیر، سیستم تحت تاثیر، بهره‌برداری انجام شده و نیازمندی‌های امنیتی اظهارنظر نمود. این پارامترها با توجه به مقادیر داده شده برای معیارها محاسبه شده و با سه مقدار کم، متوسط و زیاد که به ترتیب با مقادیر ۲، ۱ و ۰ نشان داده می‌شود، گزارش می‌شوند. در جدول (۸) نتایج حاصل از این مقادیر و عدد شش رقمی اختصاص داده شده به هر دسته حمله که با عنوان بردار ماکرو[1] معرفی شده، آورده شده است. به جهت محدودیت در نمایش جدول اسامی گزینه‌های تصمیم حذف شده و از همان ردیف‌های مربوط به آن‌ها در جدول (۷) به‌صورت افقی استفاده شده است.

جدول (۸). نتایج محاسبات مربوط به بردار ماکرو

	کم	کم	متوسط	متوسط	متوسط	کم
	متوسط	متوسط	زیاد	زیاد	متوسط	متوسط
	متوسط	متوسط	زیاد	متوسط	زیاد	زیاد
	متوسط	متوسط	متوسط	متوسط	متوسط	متوسط
	زیاد	زیاد	زیاد	زیاد	زیاد	زیاد
	زیاد	زیاد	زیاد	زیاد	زیاد	زیاد
	۲۱۱۱۰۰	۲۱۱۱۰۰	۱۰۰۱۰۰	۱۰۱۱۰۰	۱۱۰۱۰۰	۲۱۰۱۰۰

مشاهده می‌شود که قابلیت بهره‌برداری در سه حملهٔ مبتنی بر زمان، حملهٔ مبتنی بر ریز معماری و حملهٔ مبتنی بر حافظهٔ نهان که دارای بیشترین مقدار CVSS بودند، بیشتر از بقیهٔ حملات است. پیچیدگی حملات در دو حملهٔ حملهٔ مبتنی بر زمان و حملهٔ مبتنی بر حافظهٔ نهان زیاد بوده؛ اما در بقیه‌ی حملات این پیچیدگی متوسط ارزیابی شده است. به عبارت دیگر این دو حمله با اینکه دارای شدت آسیب‌پذیری بالایی هستند اما پیچیدگی آن‌ها بالا بوده و این مورد می‌تواند در اجرای آن‌ها چالش‌هایی بیشتری را در مقایسه با دیگر حملات ایجاد نماید. در مورد سیستم آسیب‌پذیر مشاهده می‌شود که در سه حملهٔ مبتنی بر زمان، حملهٔ مبتنی بر ریز معماری و حملهٔ مبتنی بر هوش مصنوعی آسیب‌پذیری سیستم بالا ارزیابی شده است اما در همین حملات آسیب‌پذیری سیستم تحت تاثیر متوسط ارزیابی شده است. با توجه به اینکه تمام دسته حملات بررسی شده به‌صورت عملی اجرایی شده و حملاتی از آن‌ها گزارش شده است، بهره‌برداری انجام شده برای همه‌ی آن‌ها زیاد به دست آمده است. در مورد پارامتر نیازمندی‌های امنیتی با توجه به اینکه در تمام حملات بررسی شده محرمانگی به شدت تحت تاثیر قرار می‌گیرد، می‌توان انتظار داشت که نیازمندی‌های امنیتی که شامل سه پارامتر محرمانگی، یکپارچگی و دسترس‌پذیری است، تحت تاثیر قرار گرفته و مقدار زیاد برای همه‌ی گزینه‌ها به دست آید.

با بررسی مقالات منتشر شده در سال‌های اخیر توسط نویسنده، نمونه‌ای که به این شکل علاوه بر انجام تحلیل سلسله‌مراتبی بر روی آسیب‌پذیری‌های پردازنده‌ها، تحلیل میزان خطر با استفاده از پارامتر CVSS انجام شده باشد، یافت نشد. البته مشابه‌ترین نمونه مقالات [۵۵] و [۵۶] هستند که به بررسی پارامتر CVSS حملات کانال جانبی پرداخته‌اند اما علاوه بر متفاوت بودن نحوه‌ی دسته‌بندی، برای امتیازدهی از نسخه‌ی قدیمی (نسخه‌ی ۲ و یا ۳) استفاده نموده‌اند. در مقاله‌ی [۵۵] آسیب‌پذیری‌های نسخه‌های مختلف OpenSSL و GNU crypto که در سال‌های مختلف محاسبه شده جمع‌آوری و مقایسه شده است و در نهایت با میانگین‌گیری مقادیر موجود در جدول شکل (۴) به دست آمده است. در این جدول دو حملهٔ کانال جانبی و ریز معماری به چشم می‌خورد اما اعداد موجود در جدول مربوط به میانگین‌گیری از نسخه‌ی ۲ پارامتر CVSS و قابل مقایسه با کار این مقاله نیست.

[1] Macro Vector

	CVSS			Count
	Base	Exploit	Impact	
Denial of Service	5.74	9.46	4.33	157
Buffer Overflow	6.76	9.43	5.77	43
Side channel	**3.32**	**6.27**	**2.90**	**37**
Code Execution	7.98	9.08	7.74	35
Mem Corruption	6.56	9.72	5.29	20

(a) Comparisons with different vulnerabilities

	CVSS			Count
	Base	Exploit	Impact	
Asymmetric Crypto	2.86	5.48	2.90	18
Crypto Protocol	3.76	7.02	2.90	19
Microarchitecture	**3.04**	**5.87**	**2.90**	**16**
Physical	1.97	3.57	2.90	3
Network	3.87	7.22	2.90	18

(b) Comparisons of side-channel vulnerabilities

شکل (۴). مقادیر پارامتر CVSS برای چند حمله [55]

همچنین در [۵۶] نیز از نسخه‌ی ۳ این پارامتر استفاده نموده است و در آن همانطور که در شکل (۵) مشاهده می‌شود، پارامتر CVSS برای مراحل انجام هرکدام از ۴ الگوی فلاش+ریلود، اویکت+ریلود، پرایم+پروب و اخراج+زمان و دو حملهٔ Meltdown و Spectre که در ابتدای این مقاله مقالات آن بررسی شده‌اند، محاسبه شده است. مشاهده می‌شود که از حملات به سه مرحله تقسیم‌بندی شده و مقدار پایه‌ی این پارامتر برای آن‌ها محاسبه شده است. این نمونه هم به دلیل تفاوت نسخه و همچنین نوع دسته‌بندی ارائه شده، قابل مقایسه با موارد مطرح شده در این مقاله نیست.

Attacks	Attack Step	CVSS (Formula)	CVSS (Base Score)
Flush + Reload	Flush	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	5.5 (Medium)
	Wait	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N	2.8 (Low)
	Reload	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	3.3 (Low)
Evict + Reload	Evict	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3 (Low)
	Wait	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N	2.8 (Low)
	Reload	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	3.3 (Low)
Prime + Probe	Prime	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3 (Low)
	Wait	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N	2.8 (Low)
	Probe	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	3.3 (Low)
Evict + Time	Time	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N	2.8 (Low)
	Evict	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3 (Low)
	Time	CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N	2.8 (Low)
Evict + Reload with Spectre	Evict	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3 (Low)
	Spectre	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	6.3 (Medium)
	Reload	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5 (Medium)
Evict + Reload with Meltdown	Evict	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	3.3 (Low)
	Meltdown	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N	5.6 (Medium)
	Reload	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N	5.5 (Medium)

شکل (۵). مقادیر پارامتر CVSS برای ۴ الگو و دو حمله [56]

باتوجه‌به موارد می‌توان نتیجه گرفت که تحلیل انجام شده در این مقاله تاکنون مورد مشابهی نداشته و می‌تواند برای تصمیم‌گیری مورد استفاده قرار گیرد.

۵. نتیجه گیری

در این مقاله یک بررسی جامع از مقالات مربوط به حوزهٔ کانال جانبی بر روی پردازنده‌های اینتل و نشانه انجام شد و پس از آن با ارائه یک دسته‌بندی کلی از این حملات، چند معیار و زیرمعیار معرفی گشت و با استفاده از آن‌ها به ارزیابی این حملات پرداخته شد. همچنین پارامتر CVSS که برای ارزیابی میزان خطر و شدت یک حمله مورداستفاده قرار می‌گیرد، برای ۶ حملهٔ کاندید محاسبه و مورد بررسی قرار گرفت. باید توجه داشت که نتایج حاصل از این ارزیابی می‌تواند جهت تصمیم‌گیری در مورد میزان شدت این حملات و راهکارهای مقابله با آن‌ها (باتوجه‌به معیارها و اولویت‌های بررسی شده) در اختیار مدیران قرار گرفته تا با بررسی نتایج این ارزیابی بتوانند تصمیمات مطمئن‌تری در این حوزه داشته باشند.

از نکات مهم حاصل از ارزیابی سلسله‌مراتبی این مورد است که میزان اثربخشی در بین پارامترها از اهمیت بالایی برخوردار بوده و معیارهای مربوط به آن می‌تواند نقش تعیین‌کننده در نتایج ارزیابی داشته باشد. همچنین در میان تمام زیرمعیارها سه پارامتر درصد بازیابی کلید(گذرواژه)، سطح دسترسی و قابلیت ایجاد کانال پنهان بیشترین وزن را به خود اختصاص داده‌اند که می‌تواند قابل‌توجه باشد.

نتایج ارزیابی‌ها نشان می‌دهد که حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری از نظر کاربردی‌بودن با چالش مواجه است که این خود می‌تواند گویای این مطلب باشد که نوآوری در این حوزه می‌تواند به کاربردی نمودن این حمله و استفادهٔ بهتر از آن کمک نماید که کاهش پیچیدگی و فرض‌های مسئله و همچنین توسعهٔ آن در سطح پردازنده و سیستم‌عامل می‌تواند از جمله‌ی این نوآوری‌ها باشد. همچنین پارامتر CVSS این حمله نشان‌دهندهٔ آسیب متوسط این حمله به قربانی است که با بهبود این حمله و در نتیجه تغییر برخی از زیر پارامترهای موجود در محاسبه، این عدد افزایش‌یافته و ممکن است به بالای ۷ برسد.

در نهایت در ارزیابی کلی معیارها بر اساس تحلیل AHP، سه حملهٔ مبتنی بر زمان، حملهٔ مبتنی بر حافظهٔ نهان و حملهٔ کانال جانبی توان با اندازه‌گیری نرم‌افزاری به ترتیب به‌عنوان گزینه‌های اولیه معرفی شده‌اند. حملهٔ مبتنی بر زمان در هر دو ارزیابی رتبهٔ اول را داشته و به نظر می‌رسد به همین دلیل گزینهٔ مناسبی برای مهاجمان بوده است. باوجوداینکه حملهٔ مبتنی بر ریز معماری در بین این سه نیست؛ اما عدد بالای CVSS برای این حمله (رتبهٔ دوم) و همچنین معیار امکان‌پذیری نشان می‌دهد که این حمله قابلیت انجام و تخریب بالا داشته و در مقالات اخیر نیز استفاده از این نوع حمله مؤید این موضوع است. در این حوزه حملات مبتنی بر محیط اجرایی امن علاوه بر حملاتی که مشابه Meltdown و Spectre هستند، قابلیت توسعه و کاربردی‌تر شدن داشته و علاوه بر آنها شناسایی آسیب‌پذیری‌های جدید در حوزهٔ ریز معماری به توسعهٔ این دسته از حملات و افزایش بهره‌وری

آنها کمک خواهد کرد که نیازمند بررسی‌های بیشتر خارج از فضای این مقاله است.

حملهٔ مبتنی بر هوش مصنوعی در تحلیل AHP در رتبهٔ چهارم قرار گرفته است؛ اما باید در نظر داشت که جدید بودن این حمله و پیچیدگی‌های موجود در آن باعث رتبهٔ پایین‌تر آن باتوجه‌به معیارهای تعریف شده در این مقاله شده است. به‌عبارت‌دیگر توسعهٔ این دسته از حملات باتوجه‌به فراگیر بودن آن در حوزه‌های مختلف و پیشرفت سریع آن می‌تواند چالشی جدی در این حوزه برای امنیت ابزارهایی باشد که مورد حمله قرار می‌گیرند.

۶. مراجع

[1] "Web of Science." [Online]. Available: https://www.webofscience.com/wos/woscc/basic-search. [Accessed: 10-Nov-2022].

[2] D. A. Osvik, A. Shamir, and E. Tromer, "Cache Attacks and Countermeasures: The Case of AES," in Journal of Cryptology, vol. 23, no. 1, 2006, pp. 1–20.

[3] C. Su and Q. Zeng, "Survey of CPU Cache-Based Side-Channel Attacks: Systematic Analysis, Security Models, and Countermeasures," Secur. Commun. Networks, vol. 2021, pp. 1–15, Jun. 2021.

[4] C. Percival, "Cache missing for fun and profit," BSDCan 2005. 2005.

[5] M. Neve and J. P. Seifert, "Advances on access-driven cache attacks on AES," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 4356 LNCS. pp. 147–162, 2007.

[6] E. Tromer, D. A. Osvik, and A. Shamir, "Efficient Cache Attacks on AES, and Countermeasures," J. Cryptol., vol. 23, no. 1, pp. 37–71, Jan. 2010.

[7] O. Aciiçmez, "Yet another MicroArchitectural attacks: Exploiting I-cache," Proceedings of the ACM Conference on Computer and Communications Security. pp. 11–18, 2007.

[8] O. Aciiçmez and W. Schindler, "A vulnerability in RSA implementations due to instruction cache analysis and its demonstration on OpenSSL," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 4964 LNCS. pp. 256–273, 2008.

[9] F. Liu, Y. Yarom, Q. Ge, G. Heiser, and R. B. Lee, "Last-level cache side-channel attacks are practical," Proceedings - IEEE Symposium on Security and Privacy, vol. 2015-July. pp. 605–622, 2015.

[10] F. Brasser, U. Müller, A. Dmitrienko, K. Kostiainen, S. Capkun, and A. R. Sadeghi, "Software grand exposure: SGX cache attacks are practical," 11th USENIX Workshop on Offensive Technologies, WOOT 2017, co-located with USENIX Security 2017. 2017.

[11] M. Schwarz, S. Weiser, D. Gruss, C. Maurice, and S. Mangard, "Malware guard extension: Using SGX to conceal cache attacks," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2017, vol. 10327 LNCS, pp. 3–24.

[12] J. Götzfried, M. Eckert, S. Schinzel, and T. Müller, "Cache Attacks on Intel SGX," in Proceedings of the 10th European Workshop on Systems Security, 2017, pp. 1–6.

[13] R. Hund, C. Willems, and T. Holz, "Practical timing side channel attacks against kernel space ASLR," Proceedings - IEEE Symposium on Security and Privacy. pp. 191–205, 2013.

[14] D. Gullasch, E. Bangerter, and S. Krenn, "Cache Games -- Bringing Access-Based Cache Attacks on AES to Practice," in 2011 IEEE Symposium on Security and Privacy, 2011, pp. 490–505.

[15] Y. Yarom and K. Falkner, "{FLUSH+RELOAD}: A High Resolution, Low Noise, L3 Cache {Side-Channel} Attack," in 23rd USENIX Security Symposium (USENIX Security 14), 2014, pp. 719–732.

[16] G. Irazoqui, M. S. Inci, T. Eisenbarth, and B. Sunar, "Wait a minute! A fast, cross-VM attack on AES," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8688 LNCS. pp. 299–319, 2014.

[17] B. Gülmezo Ğ Lu, M. S. İnci, G. Irazoqui, T. Eisenbarth, and B. Sunar, "A faster and more realistic flush+reload attack on AES," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2015, vol. 9064, pp. 111–126.

[18] N. Benger, J. van de Pol, N. P. Smart, and Y. Yarom, "'Ooh Aah... Just a Little Bit' : A Small Amount of Side Channel Can Go a Long Way," 2014, pp. 75–92.

[19] J. van de Pol, N. P. Smart, and Y. Yarom, "Just a Little Bit More," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9048, 2015, pp. 3–21.

[20] Y. Yarom and N. Benger, "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack," IACR Cryptology. pp. 12–14, 2014.

[21] T. Allan, B. B. Brumley, K. Falkner, J. Van De Pol, and Y. Yarom, "Amplifying side channels through performance degradation," ACM International Conference Proceeding Series, vol. 5-9-Decemb. pp. 422–435, 2016.

[22] Y. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Cross-tenant side-channel attacks in PaaS clouds," in Proceedings of the ACM Conference on Computer and Communications Security, 2014, pp. 990–1003.

[23] D. Gruss, R. Spreitzer, and S. Mangard, "Cache template attacks: Automating attacks on inclusive last-level caches," in Proceedings of the 24th USENIX Security Symposium, 2015, pp. 897–912.

[24] M. Esfahani, H. Soleimany, and M. R. Aref, "Modified Cache-Template Attack on AES," Scientia Iranica, vol. 29, no. 4. p. 8, 2022.

[25] H. Soleimany, M. Esfahani, and M. R. Aref, "Practical Implementation of A Novel Side-Channel Flush+Reload Attack on AES," Sci. J. Adv. Def. Sci. Technol., vol. 10, no. 4, pp. 383–392, 2020. (In Persian).https://dor.isc.ac/dor/20.1001.1.26762935.1398.10.4.5.3

[26] C. Pereida García, B. B. Brumley, and Y. Yarom, "Make Sure DSA Signing Exponentiations Really are Constant-Time," in Proceedings of the 2016 ACM SIGSAC

FLUSH+RELOAD Attack on Armv8 System via ACP," in 2021 International Conference on Information Networking (ICOIN), 2021, pp. 32–35.

[42] G. Haas, S. Potluri, and A. Aysu, "ITimed: Cache Attacks on the Apple A10 Fusion SoC," Proceedings of the 2021 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2021. pp. 80–90, 2021.

[43] A. Mirghadri and H. Bagheri, "Side Channel Analysis of International Data Encryption Algorithm (IDEA)," J. Electron. Cyber Def., vol. 7, no. 4, pp. 51–57, 2020. (In Persian).

[44] H. Momeni and M. A. Taheri, "Time Analysis Attack on a Stream Cipher Algorithm's," J. Electron. Cyber Def., vol. 4, no. 1, pp. 51–57, 2016. (In Persian).https://dor.isc.ac/dor/20.1001.1.23224347.1395.4.1.5.7

[45] M. Lipp et al., "PLATYPUS: Software-based power side-channel attacks on x86," Proceedings - IEEE Symposium on Security and Privacy, vol. 2021-May. pp. 355–371, 2021.

[46] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman," CRYPTO - Annual International Cryptology Conference. pp. 104–113, 1996.

[47] M. Lipp et al., "Meltdown: Reading kernel memory from user space," in 27th USENIX Security Symposium (USENIX Security 18), 2018, pp. 973–990.

[48] P. Kocher et al., "Spectre attacks: Exploiting speculative execution," Proceedings - IEEE Symposium on Security and Privacy, vol. 2019-May. pp. 1–19, 2019.

[49] C. Canella et al., "A systematic evaluation of transient execution attacks and defenses," Proc. 28th USENIX Secur. Symp., pp. 249–266, 2019.

[50] D. Ryu, Y. Kim, and J. Hur, "Gamma-Knife: Extracting Neural Network Architecture Through Software-Based Power Side-Channel," IEEE Trans. Dependable Secur. Comput., pp. 1–17, 2023.

[51] B. Gulmezoglu, A. Moghimi, T. Eisenbarth, and B. Sunar, "FortuneTeller: Predicting Microarchitectural Attacks via Unsupervised Deep Learning," arXiv Prepr. arXiv1907.03651, vol., no., p. 16, Jul. 2019.

[52] M. Mollazadeh, H. Lashkarian, M. Sheikh Mohammadi, and K. Mirzaei, "Evaluation Model of Vulnerabilities of Network Centric Warfare Based on Hierarchical Analysis Process," J. Command Control, vol. 2, no. 1, p. 25, 2019. (In Persian)

[53] "Common Vulnerability Scoring System." [Online]. Available: https://www.first.org/cvss/. [Accessed: 14-Sep-2023].

[54] "CVSS v4.0 Specification Document." [Online]. Available: https://www.first.org/cvss/v4.0/specification-document. [Accessed: 25-Jan-2024].

[55] X. Lou, T. Zhang, J. Jiang, and Y. Zhang, "A Survey of Microarchitectural Side-channel Vulnerabilities, Attacks, and Defenses in Cryptography," ACM Comput. Surv., vol. 54, no. 6, pp. 1–37, Jul. 2022.

[56] L. Wang, Z. Zhu, Z. Wang, and D. Meng, "Colored Petri Net Based Cache Side Channel Vulnerability Evaluation," IEEE Access, vol. 7, pp. 169825–169843, 2019.

Conference on Computer and Communications Security, 2016, vol. 24-28-Octo, pp. 1639–1650.

[27] D. Gruss, C. Maurice, K. Wagner, and S. Mangard, "Flush+Flush: A Fast and Stealthy Cache Attack," 2016, pp. 279–299.

[28] G. Didier and C. Maurice, "Calibration Done Right: Noiseless Flush+Flush Attacks," 2021, pp. 278–298.

[29] A. Saxena and B. Panda, "DABANGG : Time for Fearless Flush based Cache Attacks," Cryptology ePrint Archive, no. Report 2020/637. 2020.

[30] A. Saxena and B. Panda, "DABANGG: A Case for Noise Resilient Flush-Based Cache Attacks," in 2022 IEEE Security and Privacy Workshops (SPW), 2022, pp. 323–334.

[31] N. Zhang, K. Sun, D. Shands, W. Lou, and Y. T. Hou, "Truspy: Cache side-channel information leakage from the secure world on arm devices," Cryptol. ePrint Arch., 2016.

[32] N. Zhang, K. Sun, D. Shands, W. Lou, and Y. T. Hou, "TruSense: Information Leakage from TrustZone," in Proceedings - IEEE INFOCOM, 2018, vol. 2018-April, pp. 1097–1105.

[33] M. Lipp, D. Gruss, R. Spreitzer, C. Maurice, and S. Mangard, "Armageddon: Cache attacks on mobile devices," Proceedings of the 25th USENIX Security Symposium. pp. 549–564, 2016.

[34] R. Guanciale, H. Nemati, C. Baumann, and M. Dam, "Cache Storage Channels: Alias-Driven Attacks and Verified Countermeasures," in Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016, 2016, pp. 38–55.

[35] "wolfSSL: Embedded SSL/TLS Library." [Online]. Available: https://www.wolfssl.com/products/wolfssl/. [Accessed: 06-Sep-2022].

[36] M. Green, L. Rodrigues-Lima, A. Zankl, G. Irazoqui, J. Heyszl, and T. Eisenbarth, "AutoLock: Why cache attacks on arm are harder than you think," Proceedings of the 26th USENIX Security Symposium. pp. 1075–1091, 2017.

[37] B. Lapid and A. Wool, "Navigating the samsung trustzone and cache-attacks on the keymaster trustlet," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, vol. 11098 LNCS, pp. 175–196.

[38] B. Lapid and A. Wool, "Cache-Attacks on the ARM TrustZone Implementations of AES-256 and AES-256-GCM via GPU-Based Analysis," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2019, vol. 11349 LNCS, pp. 235–256.

[39] V. Meraji and H. Soleimany, "Introducing a New Timing Attack on the ARM Processor and its Practical Implementation on the Raspberrypi3 Board," J. Electron. Cyber Def., vol. 8, no. 1, pp. 125–132, 2020. (In Persian).https://dor.isc.ac/dor/20.1001.1.23224347.1399.8.1.10.0

[40] M. Esfahani, H. Soleimany, and M. R. Aref, "Enhanced cache attack on AES applicable on ARM-based devices with new operating systems," Comput. Networks, vol. 198, 2021.

[41] H. Lee, S. Jang, H.-Y. Kim, and T. Suh, "Hardware-Based