فرم پیشنهاد تحقیق

پایان‌نامه‌ی کارشناسی ارشد

عنوان تحقیق به فارسی:

دفع حملات کانال جانبی حافظه نهان با استفاده از جدول آدرس دهی جانبی حافظه نهان

نام و نام خانوادگی دانشجو: گروه تخصصی:

رشته تحصیلی: گرایش:

سال ورود به مقطع جاری: نیمسال ورودی:

نام و نام خانوادگی استاد (اساتید) راهنما: نام و نام خانوادگی استاد (اساتید) مشاور:

۱-

این قسمت توسط حوزه معاونت پژوهش و فناوری واحد تکمیل می‌گردد.

تاریخ دریافت توسط حوزه پژوهشی واحد :

تاریخ تصویب در گروه :

تائید کارشناس پژوهشی تائید معاونت پژوهش و فناوری:

به نام خدا

توجه: لطفاً این فرم با مساعدت و هدایت استاد راهنما تکمیل شود.

۱- اطلاعات مربوط به دانشجو :

نام : نام خانوادگی :

شماره دانشجویی :

مقطع: رشته تحصیلی: گروه تخصصی:

گرایش: سال ورود به مقطع جاری: نیمسال ورودی:

آدرس پستی در تهران:

تلفن ثابت محل سکونت: تلفن همراه:

پست الکترونیک:

آدرس پستی در شهرستان:.....

تلفن ثابت محل سکونت: .....تلفن محل کار: ..... دورنگار:.....

۲- اطلاعات مربوط به استاد راهنما :

اطلاعات مربوط به استاد راهنمای اول :

نام و نام خانوادگی : آخرین مدرک تحصیلی :

تخصص اصلی: تخصص جنبی :

رتبه دانشگاهی (مرتبه علمی) :

سنوات تدریس: شغل و سمت فعلی :

آدرس محل کار:

تلفن منزل : ..... تلفن همراه: ..... محل کار: ..... دورنگار: .....

پست الکترونیک *(Email)* :

نحوه همکاری با واحد الکترونیکی :

تمام وقت ☐ نیمه وقت☐ مدعو ■

تعداد پایان‌نامه‌های کارشناسی ارشد راهنمائی شده

واحد الکترونیکی: مجموعه دانشگاه آزاد اسلامی: سایر دانشگاهها:

تعداد رساله‌های دکتری راهنمائی شده

مجموعه دانشگاه آزاد اسلامی: سایر دانشگاهها :

تعداد پایان‌نامه‌های کارشناسی ارشد در دست راهنمائی

واحد الکترونیکی: مجموعه دانشگاه آزاد اسلامی: سایر دانشگاها:

تعداد رساله‌های دکتری در دست راهنمائی

مجموعه دانشگاه آزاد اسلامی: سایر دانشگاهها:

اطلاعات مربوط به استاد راهنمای دوم :

نام و نام خانوادگی : ..... آخرین مدرک تحصیلی .....

تخصص اصلی: ..... تخصص جنبی: ..... رتبه دانشگاهی (مرتبه علمی): .....

سنوات تدریس ..... شغل و سمت فعلی : .....

آدرس محل کار:.....

تلفن منزل:..... تلفن همراه:.....محل کار:.....دورنگار:.....

پست الکترونیک *(Email)* : .....

نحوه همکاری با واحد الکترونیکی :

تمام وقت ☐ نیمه وقت ☐ مدعو ☐

تعداد پایان‌نامه‌های کارشناسی ارشد راهنمائی شده

واحد الکترونیکی : مجموعه دانشگاه آزاد اسلامی : سایر دانشگاهها :

تعداد رساله‌های دکتری راهنمائی شده

مجموعه دانشگاه آزاد اسلامی : سایر دانشگاهها :

تعداد پایان‌نامه‌های کارشناسی ارشد در دست راهنمائی

واحد الکترونیکی : مجموعه دانشگاه آزاد اسلامی : سایر دانشگاهها :

تعداد رساله‌های دکتری در دست راهنمائی

مجموعه دانشگاه آزاد اسلامی : سایر دانشگاهها :

۳- اطلاعات مربوط به اساتید مشاور:

استاد مشاور اول :

نام و نام خانوادگی : آخرین مدرک تحصیلی :

تخصص اصلی : تخصص جنبی :

رتبه دانشگاهی (مرتبه علمی) :

سنوات تدریس شغل و سمت فعلی :

آدرس محل کار:

تلفن منزل:..... تلفن همراه:.....محل کار:.....دورنگار:.....

پست الکترونیک *(Email)* :

نحوه همکاری با واحد الکترونیکی :

تمام وقت ☐ نیمه وقت☐ مدعو ■

استاد مشاوردوم :

نام و نام خانوادگی : ..... آخرین مدرک تحصیلی .....

تخصص اصلی : ..... تخصص جنبی : ..... رتبه دانشگاهی (مرتبه علمی) : .....

سنوات تدریس ..... شغل و سمت فعلی : .....

آدرس محل کار:.....

تلفن منزل:..... تلفن همراه:.....محل کار:.....دورنگار:.....

پست الکترونیک *(Email)* : .....

نحوه همکاری با واحد الکترونیکی :

تمام وقت ☐ نیمه وقت☐ مدعو ☐

۴- اطلاعات مربوط به پایان‌نامه:

الف- عنوان تحقیق

۱- عنوان به زبان فارسی:

دفع حملات کانال جانبی حافظه نهان با استفاده از جدول آدرس دهی جانبی حافظه نهان

۲- عنوان به زبان انگلیسی/ (آلمانی، فرانسه، عربی) :

Secure Cache Alternative Address Table for mitigating cache logical side-channel attacks

ب – تعداد واحد پایان‌نامه: شش واحد

ج- بیان مسأله اساسی تحقیق به طور کلی (شامل تشریح مسأله و معرفی آن، بیان جنبه‌های مجهول و مبهم، بیان متغیرهای مربوطه و منظور از تحقیق) :

با پیشرفت صنعت الکترونیک و پیدایش پردازنده های مدرن، مدل حمله در الگوریتم ها و پروتکل های رمزنگاری نیز تغییر کرد. با وجود پیچیدگی محاسباتی در الگوریتم ها و پروتکل های رمزنگاری، پیاده سازی ها می توانند عاملی برای نشت اطلاعات محرمانه باشند. مهاجم می تواند زمانی حمله کند که قطعات الکترونیکی در حال اجرای عملگرهای رمزنگاری با استفاده از کلید مخفی بر روی داده های حساس هستند. در حین رایانش، نشت اطلاعات در قطعات الکترونیکی وجود دارد که به آن حملات کانال جانبی می گویند.

امنیت سیستم های حافظه به دلیل آسیب پذیری آنها در برابر حملات کانال های جانبی از اهمیت خاصی برخوردار است. یک رویکرد امیدوار کننده برای تشخیص حمله در زمان اجرا ، نظارت بر رفتار حافظه پنهان است. در صورت بروز حمله، باید یک راهکار برای دفع آن نیز وجود داشته

باشد. برای مقابله با حمله در این تحقیق از یک حافظه جانبی امن به نام SCAAT استفاده می شود.

SCAAT یک سیستم مقابله با حملات است که به سیستم نظارت متصل است تا حمله را شناسایی کرده و با تغییر مکان داده ها به صورت تصادفی در حافظه پنهان در در زمان اجرا ، سیستم را در برابر حملات مصون می دارد. استراتژی SCAAT با هدف تغییر الگوهای رفتاری حافظه پنهان، پیش بینی رفتار حافظه را دشوار می کند تا نتوان از این رفتار برای نشت اطلاعات استفاده کرد.

بنابراین، این سیستم از دو بخش تشکیل شده است. بخش اول مربوط به یک سیستم مانیتورینگ و بخش دوم SCAAT است. هنگامی که حمله توسط بخش مانیتورینگ تشخیص داده می شود ، یک سیگنال حمله برای مقابله با آن، به واحد SCAAT ارسال می شود. SCAAT یک حافظه است که فقط در صورت تشخیص حمله فعال می شود و محل ذخیره داده ها را تغییر می دهد. با تغییر آدرس داده ها در حافظه پنهان ، الگوهای دسترسی و زمان بندی رفتار حافظه پنهان نیز تغییر میکند.

ه- مرور ادبیات و سوابق مربوطه (بیان مختصر پیشینه تحقیقات انجام شده در داخل و خارج کشور پیرامون موضوع تحقیق و نتایج آنها و مرور ادبیات و چارچوب نظری تحقیق) :

برخی تحقیقات مکانیسم هایی را برای ایمن سازی حافظه پنهان پیشنهاد کرده اند. برای مثال، (Zhang و همکاران، ۲۰۱۶) یک سیستم اجرای ایمن به کمک حافظه پنهان به نام CaSE را پیشنهاد داده اند که می‌تواند در برابر حملات نرم‌افزاری و حملات افشای حافظه فیزیکی در دستگاه‌های مبتنی بر ARM محافظت کند.

در (Neagu ، ۲۰۱٤) ، روشی برای پنهان کردن داده های متن ساده از حافظه نهان L2 پیشنهاد شده است. به دنبال آن است که داده ها را در صورت بازیابی آنها غیرقابل استفاده کند و از انتقال الگوهای منظم بین CPU و حافظه پنهان جلوگیری کند.

برخی تحقیقات مانند (Lee و همکاران، ۲۰۰۵) ،(Zhang و همکاران، ۲۰۱۵) ، (Zhang و همکاران، ۲۰۱۲) از پارتیشن بندی استاتیک استفاده می کنند که در آن کش به طور فیزیکی به پارتیشن های مختلف تقسیم می شود و تداخل کش را در بین برنامه های مختلف حذف می کند.

یکی از مهم ترین منابع نشت اطلاعات کانال جانبی، تغییرات زمانی ناشی از اجرای محاسبات است. دسترسی ها به حافظه و وجود انشعاب ها در برنامه، در زمان اجرا هزینه بر هستند، بنابراین پردازنده ها برای کاهش این هزینه، از حافظه نهان و پیشگویی انشعاب استفاده می کنند. متاسفانه این بهینه سازی در زمان اجرا، منجر به ایجاد تغییرات زمانی در اجرای یک برنامه می شود. حافظه نهان در حملات کانال جانبی زمان، چالش برانگیزتر و کاربردی تر است. در این مقاله به مرور انواع حملات حافظه نهان روی پیاده سازی الگوریتم رمز AES خواهیم پرداخت. با پیاده سازی حملات و مقایسه نتایج، ضعف های امنیتی پیاده سازی الگوریتم رمز AES در برابر حملات حافظه نهان را استخراج و مورد مقایسه قرار خواهیم داد.

ز- اهداف مشخص تحقیق (شامل اهداف آرمانی، کلی، اهداف ویژه و کاربردی):

- طراحی یک حافظه پنهان امن همراه با یک سیستم نظارت برای شناسایی حملات و یک سیستم کاهش دهنده برای کاهش حملات در هنگام وقوع.
- بررسی تاثیر SCAAT بر رفتار کش.

- **آنالیز و ارزیابی SCAAT برای حافظه پنهان از نظر سربار و عملکرد**

ی) فرضیه‌های تحقیق

- **طراحی پیشنهادی منجر به کاهش حملات درحافظه پنهان می شودو**
- **SCAAT سربار کم و عملکرد بهتری نسبت به روشهای پیشین امن سازی حافظه نهان دارد.**

ک- تعریف واژه‌ها و اصطلاحات فنی و تخصصی (به صورت مفهومی و عملیاتی):

حافظه پنهان حافظه‌ای سریع درون پردازنده مرکزی است که جهت صرفه جویی در زمان مراجعه به حافظه اصلی بکار می‌رود.

زمانی که پردازنده مرکزی به مکانی در حافظه اصلی نیاز داشته باشد احتمالاً در آینده نزدیک مجدداً به آن محل دسترسی خواهد داشت که به این اصل همجواری زمانی Temporal) (Localityمی‌گویند. همچنین اگر پردازنده مرکزی به مکانی در حافظه اصلی نیاز داشته باشد احتمالاً در آینده نزدیک به مکان‌های مجاور آن نیز نیاز خواهد داشت که به این اصل همجواری مکانی (Spatial Locality) می‌گویند.

بر این اساس حافظه نهان گاهی در زمان دسترسی به یک مکان حافظه مکان‌های مجاور آن را نیز به درون پردازنده مرکزی می‌آورد تا در صورت نیاز سریعتر قابل دسترسی باشند و این اطلاعات را تا زمانی که مورد نیاز باشند در پردازنده مرکزی حفظ می‌کند. چون با افزایش سرعت پردازنده

مرکزی، پردازنده مرکزی زمان بیشتری را در حال انتظار پاسخ حافظه اصلی می‌گذراند، حجم حافظه پنهان تأثیر زیادی در بهبود کارایی پردازنده مرکزی دارد.

حملات کانال جانبی : در این روش سارقان می‌توانند با دستیابی به اطلاعات حساس دستگاه‌های سخت‌افزاری، این دستگاه‌ها را رمزگشایی کرده و مورد سو استفاده قرار دهند. در این روش مهاجم با محاسبه کلیدهای رمزنگاری شده یا جزئیات دستورالعمل‌ها و داده‌های اجرا شده در یک دستگاه سخت‌افزاری، می‌تواند آن‌ها را رمزگشایی کرده و مورد سرقت قرار دهد.

حملات کانال جانبی دسته‌ای از حملات به دستگاه‌های سخت‌افزاری هستند. هکرها در این روش اقدام به سرقت کلیدهای رمزنگاری شده و اطلاعات مهم تولید شده توسط یک سخت‌افزار کرده و می‌توانند کنترل آن‌ها را به‌دست بگیرند .

5 - روش‌شناسی تحقیق:

الف- شرح کامل روش تحقیق برحسب هدف، نوع داده‌ها و نحوه اجرا (شامل مواد، تجهیزات و استانداردهای مورداستفاده در قالب مراحل اجرایی تحقیق به تفکیک):

این سیستم از دو بخش تشکیل شده است. بخش اول مربوط به یک سیستم مانیتورینگ و بخش دوم SCAAT است. هنگامی که حمله توسط بخش مانیتورینگ تشخیص داده می شود ، یک سیگنال حمله برای مقابله با آن، به واحد SCAAT ارسال می شود. SCAAT یک حافظه است که فقط در صورت تشخیص حمله فعال می شود و محل ذخیره داده ها را تغییر می دهد. با تغییر آدرس داده ها در حافظه پنهان ، الگوهای دسترسی و زمان بندی رفتار حافظه پنهان نیز تغییر میکند.

ب- متغیرهای مورد بررسی در قالب یک مدل مفهومی و شرح چگونگی بررسی و اندازه گیری متغیرها:

LINES : تعداد خطوط کش

CACHE_SETS : تعداد کش

CPU_DATA_BITS : پهنای بیت رابط داده حافظه نهان و پردازنده (CPU).

MEM_DATA_BITS : پهنای بیت رابط داده حافظه نهان و حافظه اصلی

ج – شرح کامل روش (میدانی، کتابخانه‌ای) و ابزار (مشاهده و آزمون، پرسشنامه، مصاحبه، فیش‌برداری و غیره) گردآوری داده‌ها :

در این مطالعه برای جمع‌آوری داده‌ها و اطلاعات تحقیق، از منابع کتابخانه‌ای استفاده می‌شود. این منابع عبارت‌اند از:

- مقالات علمی معتبر که در پایگاه‌های علمی معتبری همچون google scholar و سایر پایگاه‌ها و نشریات علمی
- استفاده از کتب علمی منتشرشده
- مطالعه پایان‌نامه‌ها و تحقیقات سایر دانشجویان و اساتید کشور

و) فهرست منابع و مأخذ

۱. **جدیدی، محمد و اصفهانی، مهدی و محمدقلی، اسماعیل،۱۳۹۹،بررسی حملات کانال جانبی حافظه نهان بر روی پیاده سازی الگوریتم رمز AES،https://civilica.com/doc/1330360**

2. **Shalabi, A., Ghasempouri, T., Ellervee, P., & Raik, J. (2020, August). SCAAT: Secure Cache Alternative Address Table for mitigating cache logical side-channel attacks. In 2020 23rd Euromicro Conference on Digital System Design (DSD) (pp. 213-217). IEEE.**

3. **N. Zhang et al., "Case: Cache-assisted secure execution on arm processors," in 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016, pp. 72–90.**
4. **M. Neagu et al., "Interleaved scrambling technique: A novel low-power security layer for cache memories," in 2014 19th IEEE European Test Symposium (ETS). IEEE, 2014, pp. 1–2.**
5. **R. B. Lee et al., "Architecture for protecting critical secrets in microprocessors," in ISCA'05, June 2005. [18]**
6. **D. Zhang et al., "Language-based control and mitigation of timing channels," SIGPLAN Not., vol. 47, Jun. 2012.**
7. **D. Zhang et al., "A hardware design language for timing-sensitive information-flow security," SIGPLAN Not., vol. 50, Mar. 2015. [20] Y. Wang et al., "Secdcp: Secure dynamic cache partitioning for efficient timing channel protection," in 53nd ACM/EDAC/IEEE DAC, June 2016.**

۶- زمان بندی انجام تحقیق:

پیش‌بینی زمان‌بندی فعالیت‌ها و مراحل اجرایی تحقیق و ارائه گزارش پیشرفت کار

ردیف	شرح فعالیت	زمان کل (ماه)	زمان اجرا به ماه																							
			۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴
۱	مطالعات اولیه مقالات مرتبط با موضوع پژوهش	۲																								
۲	بررسی الگوریتم‌های مختلف داده کاوی	۱																								
۳	ارائه روش پیشنهادی	۱																								
۴	پیاده‌سازی روش پیشنهادی	۲																								
۵	انجام تست‌های آزمایشگاهی	۲																								
۶	بهینه سازی روش پیشنهادی بر مبنای نتایج حاصله	۱																								
۷																										
۸																										
۹																										
۱۰																										
۱۱																										
۱۲																										

توجه:

۱- زمان و نوع فعالیت‌های اجرایی پایان‌نامه، حتی‌الامکان باید با مندرجات جدول منطبق باشد.

۲- حداقل زمان قابل قبول برای پیش‌بینی مراحل مطالعاتی و اجرایی پایان‌نامه کارشناسی ارشد ۶ ماه و حداکثر ۱۲ ماه می‌باشد.

(هزینه‌ها فقط برای دانشجویان مشمول دریافت هزینه‌ها تکمیل و ارائه شود.)