

ВІДГУК

офіційного опонента на дисертаційну роботу
Мазурка Валентина Олеговича
на тему «Створення засобів захисту оперативної пам'яті від атак типу
RowHammer»,
представлену на здобуття ступеня доктора філософії
в галузі знань 12 Інформаційні технології
за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертації.

Попри зростання зацікавлення в тематиці захисту оперативної пам'яті, більшість наукових праць на цю тему концентруються або на емпіричних прикладах, або на ізольованих теоретичних моделях. Водночас комплексні системи, що включають як створення тестових середовищ, так і імплементацію та оцінку різних типів захисту, залишаються рідкістю.

Саме тому робота Мазурка Валентина Олеговича є своєчасною та актуальною в сучасному дискурсі кібербезпеки: вона не тільки узагальнює відомі підходи до виявлення атак побічними каналами на пам'ять, а й вперше пропонує повний цикл дослідження — від моделювання атак до впровадження систем захисту в реальне апаратне середовище. Такий підхід дозволяє глибше осмислити проблему та сприяти практичному впровадженню рішень у промислові та дослідницькі середовища.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

В роботі розроблено модель захисту пам'яті DRAM на основі алгоритмів машинного навчання, зокрема з використанням нейронної мережі типу MLP. На відміну від вже описаних в літературі та наукових статтях методів, ця модель працює в реальному часі, враховуючи локальні патерни доступу до пам'яті, та досягає вищої точності виявлення атак RowHammer в порівнянні з існуючими підходами. Навчання на локально зібраних даних дозволяє адаптувати модель до конкретної апаратної оболонки системи, що підвищує її універсальність та ефективність.

Також було вперше запропоновано захисний механізм на основі частотного масиву та лічильників доступу, який є стійким до проблем нерівномірного оновлення комірок пам'яті. Це було типовим недоліком

апаратних методів виявлення RowHammer і не дозволяло виявляти атаки з високою точністю при зниженому використанні ресурсів системи.

В роботі пропонується удосконалений підхід до тестування DRAM-чипів, що включає побудову апаратно-програмного комплексу на основі FPGA з універсальною програмною платформою, що підтримує різні стандарти DDR (DDR3, DDR4, DDR5), і дозволяє порівнювати ефективність різних захисних механізмів на стандартизованому обладнанні.

Запропонований підхід відкриває можливості для інтелектуального моніторингу безпеки пам'яті без значного впливу на продуктивність системи. Це перше відоме в літературі рішення, яке поєднує підхід роботи в реальному часі, точність і низьке енергонавантаження, що особливо важливо для використання в енергоефективних та вбудованих системах.

Достовірність же наукових результатів дисертаційної роботи забезпечується 9-ма науковими статтями, та даними тестувань різних видів пам'яті, представленими у виді графіків та таблиць.

Отже, в дисертаційній роботі поставлене наукове завдання створення засобів захисту оперативної пам'яті від атак типу RowHammer виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Мазурка Валентина Олеговича повністю відповідає Стандарту вищої освіти зі спеціальності 125 Кібербезпека та захист інформації та напрямкам досліджень відповідно до освітньої програми Кібербезпека.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям Інформаційні технології.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадиння, можна зробити висновок, що дисертаційна робота Мазурка Валентина Олеговича є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Мова та стиль викладення результатів

Дисертаційна робота написана українською мовою. Дисертація вирізняється виваженістю й науковою глибиною викладення матеріалу, що гармонійно поєднується з чіткістю структури й доступністю викладених концепцій. Весь текст насичений точною галузевою термінологією, яка

використовувалася у відповідності до сучасних стандартів. Автор демонструє здатність комплексно охопити складну технічну тематику й подати її у зрозумілій і логічній формі, що підвищує загальну якість сприйняття роботи.

Дисертація складається з вступу, 4 розділів, висновків та списку літератури. Загальний обсяг дисертації 208 сторінок.

У вступній частині дисертації визначено важливість дослідження теми безпеки оперативної пам'яті, наведено критичний огляд існуючих рішень, підкреслено актуальність проблеми RowHammer у сучасних інформаційних технологіях. Також представлено мету роботи, основні задачі, її інтеграцію в наукові напрями, наукову цінність отриманих результатів і можливості практичного застосування.

У першому розділі дисертації систематизовано знання про оперативну пам'ять як ціль атак, детально описано її архітектуру, механізми обробки даних і роль кеш-пам'яті різних рівнів. Зокрема, в підрозділі 1.1 розкрито принципи кешування, пояснено різницю між влучанням і промахом по кешу, що є важливим при аналізі поведінки RowHammer-атаки, а також введено математичну модель, яка дозволяє описати процеси доступу до пам'яті формально.

Далі, в підрозділі 1.2, розглянуто основні напрямки атак на DRAM, серед яких окрема увага приділяється RowHammer як найбільш небезпечному типу. У підрозділі 1.3 наведено сучасні методи захисту — як апаратні (ECC, підвищення частоти оновлення, лічильники доступу), так і програмні. Аналіз показав, що ці підходи мають значні обмеження, і тому ключовою метою нових рішень є розробка методів своєчасного виявлення атаки до моменту пошкодження даних.

У другому розділі дисертації описано побудову експериментальної інфраструктури для глибокого аналізу атак типу RowHammer. Підрозділ 2.1 висвітлює технічні особливості створення апаратної тестової платформи з використанням FPGA, що дозволяє обійти обмеження контролера пам'яті та отримати доступ до глибинних властивостей DRAM.

У підрозділі 2.2 представлено масив емпіричних даних, зібраних у результаті тестування великої кількості модулів DRAM, а в підрозділі 2.3 — результати перевірки ефективності існуючих методів захисту. Було виявлено, що навіть сучасні вдосконалені методики детектування, не здатні гарантувати повний захист системи. Це підтверджує необхідність розробки нових рішень, що враховуватимуть специфіку динамічної поведінки пам'яті.

У третьому розділі дисертації запропоновано три підходи до детектування атак RowHammer: метод вибірки рядків, моделі машинного навчання та частотний масив. У підрозділі 3.1 розглянуто проблему налаштування ймовірності у методі ймовірнісної вибірки та запропоновано математичну

формалізацію цього параметра для підвищення точності виявлення. Окрім цього, введено поняття радіуса дії атаки, яке враховує щільність комірок пам'яті та потенціал пошкодження віддалених рядків.

Підрозділ 3.2 демонструє методологію використання моделей машинного навчання для виявлення атак типу RowHammer. Завдяки методології вибору параметрів всі представлені моделі продемонстрували високу ефективність детектування понад 99%. У підрозділі 3.3 описано механізм частотного масиву на базі лічильників доступу. Розділ демонструє комплексний аналіз переваг і обмежень кожного з методів та обґрунтовує необхідність їх адаптивного поєднання в практичних системах захисту.

У четвертому розділі дисертації детально описано імплементацію механізмів захисту від RowHammer-атак у реальну апаратну систему. Першочергово підкреслено важливість використання потужного процесора для моделювання високочастотного доступу до пам'яті. Окрему увагу приділено технічним деталям реалізації частотного масиву, зокрема питанням перетворення часових параметрів у дискретні значення для лічильників, що дозволяє адаптувати захист під конкретну DRAM-конфігурацію.

Тестування в реальному середовищі, описане в підрозділі 4.3, охоплює як нейромережеві моделі, так і метод частотного масиву. Моделі машинного навчання показали понад 99% точності при локальному тренуванні, а MLP досягла 88,95% при використанні універсального датасету на новітній DDR5-пам'яті. Проте найвищий рівень надійності продемонстрував частотний масив — 99,8% точності незалежно від навантаження, що підкреслює його ефективність у практичних умовах, попри залежність від апаратних параметрів.

У висновках дисертаційної роботи описано розв'язану актуальну науково-прикладну проблему розробки методів захисту оперативної пам'яті DRAM від сучасних атак типу RowHammer. Продемонстровано способи детектування, що здатні виявляти до 99.8% атак на сучасні типи пам'яті DDR4 та DDR5. Також описано отримано такі наукові та практичні результати.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи

Наукові результати дисертації висвітлені у 4 наукових публікаціях здобувача, серед яких 4 статті у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України.

Також результати дисертації були апробовані на 5 наукових фахових конференціях. Наукові публікації здобувача відповідають вимогам до фахових видань, демонструють належний рівень теоретичної підготовки та практичної

реалізації досліджень. У роботах дотримано принципів академічної доброчесності.

Таким чином, наукові результати описані в дисертаційній роботі повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи.

На основі аналізу вмісту дисертації, було виявлено наступні недоліки та слабкі місця у роботі:

1. Недостатня деталізація алгоритму машинного навчання. У роботі не надано повної специфікації архітектури моделей (MLP, CNN, LSTM), що використовувалися для виявлення атак RowHammer. Це ускладнює можливість повторення експериментів іншими дослідниками.

2. Відсутність обґрунтування вибору метрик оцінки ефективності захисту. Не зазначено чітких критеріїв, за якими обрані FP та FN показники, а також специфічні метрики для RowHammer — це зменшує обґрунтованість методології оцінки.

3. Обмеженість тестового набору даних. Дані для навчання та тестування моделей отримані лише з обмеженого числа DRAM-чіпів, що може призвести до зміщення результатів і погіршення узагальнення моделі на нові типи пам'яті.

4. Недостатньо оптимізована модель машинного навчання для реального часу. Незважаючи на заявлену швидкодію (6,9–236 мкс), у роботі не розглянуто питання оптимізації моделей для вбудованих систем із обмеженими ресурсами.

5. Відсутність порівняльного аналізу з сучасними аналогами. Робота не містить глибокого порівняння запропонованих механізмів з іншими відомими методами, наприклад, Graphene або BlockHammer, що зменшує наукову цінність пропозицій.

6. Не враховано варіації в архітектурі пам'яті DDR3/DDR4/DDR5. Запропоновані методи не адаптовані окремо для кожного покоління пам'яті, що може призвести до зниження точності виявлення атак у нових системах.

7. Відсутність експериментальної перевірки стійкості до обхідних атак. Не проведено аналізу, наскільки запропоновані методи стійкі до нових видів RowHammer-атак, таких як Fast-Rowhammer або Non-adjacent Rowhammer.

8. Обмеженість у виборі моделей машинного навчання. Використані моделі (MLP, CNN, LSTM) є базовими, але не розглянуто сучасніші методи, як-от Transformer-based архітектури або ансамблі, які могли б забезпечити кращу продуктивність.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на позитивну оцінку дисертаційної роботи.

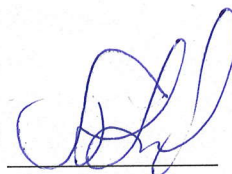
Висновок про дисертаційну роботу

Вважаю, що дисертаційна робота здобувача ступеня доктора філософії Мазурка Валентина Олеговича на тему «Створення засобів захисту оперативної пам'яті від атак типу RowHammer» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має істотне значення для */вказати галузь знань/*. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п.6 – 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувач **Мазурок Валентин Олегович** заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Офіційний опонент:

Д. т. н., с.н.с., доцент кафедри
кібербезпеки та захисту інформації
КНУ ім. Тараса Шевченка



Олександр ЛАПТЄВ

« 04 » 06 2025 року

ПІДПИС ЗАСВІДЧУЮ
ВЧЕНИЙ СЕКРЕТАР НДЧ
КАРАУЛЬНА

