

РЕЦЕНЗІЯ

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.

У сучасному світі зростаючі загрози кібербезпеці дедалі частіше виходять за межі програмного рівня. RowHammer є прикладом атаки на фізичний рівень, яку неможливо відстежити звичними методами захисту, такими як антивіруси чи міжмережеві екрани. Такий тип атаки ставить під загрозу як персональні пристрої, так і серверні системи, адже він дозволяє змінювати дані в пам'яті без наявності адміністративних прав чи доступу до ядра системи.

У цьому контексті дисертаційна робота є надзвичайно актуальною, оскільки вона фокусується не лише на виявленні таких атак, а й на практичній реалізації засобів захисту, які можуть бути інтегровані в реальні системи. Це має вагоме значення для побудови більш безпечного цифрового середовища, де захист охоплює не лише програмну, а й апаратну складову.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- вперше розроблено методологію збору експериментальних даних про вразливість DRAM-чипів до атак RowHammer із використанням уніфікованої FPGA-платформи;

- запропоновано модель захисту та апаратно-програмний комплекс для тестування модулів DDR3, DDR4 і DDR5, що забезпечує автоматизоване виявлення змін бітів у реальних умовах експлуатації.

- удосконалено методологію тестування вразливостей чипів DDR5 та створено програмну оболонку для роботи з різними типами пам'яті, що дозволило провести їх масштабне тестування і сформулювати унікальний набір даних для подальшого аналізу.

Також у роботі вдосконалено підхід до створення засобів захисту від вразливості типу RowHammer. Були визначені чіткі критерії ефективності, розроблено уніфіковані процедури порівняння та запропоновано підхід до

виявлення вразливостей у вже існуючих апаратних і програмних рішеннях. Ці досягнення становлять основу для стандартизації майбутніх досліджень в цій галузі та дозволяють проводити об'єктивну оцінку ефективності засобів захисту пам'яті.

Наукові дослідження були виконані здобувачем на кафедрі інформаційної безпеки КПІ ім. Ігоря Сікорського в рамках НДР на кафедрі інформаційної безпеки згідно вимог щодо забезпечення захищеності та безперебійного функціонування інформаційних та комунікаційних систем об'єктів критичної інфраструктури, визначених в Концепції забезпечення національної системи стійкості, ухваленої Указом Президента України № 479/2021 від 27.09.2021 року під керівництвом кандидата технічних наук, доцента Луценко Володимира Миколайовича.

Отже, в дисертаційній роботі поставлене наукове завдання створення методів та методології 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, а порушення принципів академічної доброчесності відсутні.

Мова та стиль викладення результатів.

Дисертаційна робота написана українською мовою. Стиль написання дисертації відзначається академічною строгістю й логічною послідовністю, що забезпечує високий рівень наукової культури викладення. Автор ефективно використовує усталену технічну термінологію, подаючи її в доступній і систематизованій формі. Завдяки вдало побудованій структурі тексту й

узгодженості між розділами, читач має змогу легко простежити хід дослідження від постановки проблеми до отриманих результатів.

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

Вступ дисертації висвітлює актуальність теми дослідження з урахуванням сучасного стану кібербезпекових загроз до DRAM, обґрунтовує важливість її розв'язання для сталого розвитку обчислювальних систем. У цьому розділі визначено мету, завдання, зв'язок дослідження з науковими проектами, а також описано його інноваційність і практичну значущість.

Розділ 1 формує фундаментальне підґрунтя для розуміння суті проблеми RowHammer, починаючи з пояснення принципів роботи DRAM і закінчуючи оглядом існуючих засобів захисту. Підрозділ 1.1 розкриває функціонування кеш-пам'яті, її розмежування на рівні L1, а також роль кеш-потраплянь і кеш-промахів у процесах доступу до оперативної пам'яті. Завершується підрозділ представленням формалізованої моделі пам'яті.

У підрозділі 1.2 детально досліджуються актуальні вектори атак, з фокусом на RowHammer, яку через схожість з нормальною роботою системи складно виявити. Підрозділ 1.3 надає аналіз апаратних і програмних засобів протидії, вказуючи на їхні обмеження: підвищене енергоспоживання, втрату продуктивності або надмірну залежність від статичних параметрів. Такий аналіз підкреслює актуальність пошуку більш ефективного механізму раннього детектування атаки.

Розділ 2 містить опис експериментальної частини дослідження, спрямованої на виявлення реальних загроз, пов'язаних із RowHammer. Підрозділ 2.1 розглядає архітектуру спеціально створеної платформи на базі FPGA для порушення типових таймінгів DRAM і моделювання нестандартних режимів роботи. Особливу увагу приділено можливостям виявлення неочікуваної поведінки чіпів за межами стандарту.

У підрозділі 2.2 узагальнено дані тестування сотень DRAM-чіпів трьох поколінь. У підрозділі 2.3 зосереджено увагу на обмеженнях існуючих засобів захисту. Показано, що ECC та інші механізми можуть не встигати реагувати на складні сценарії атак, а збільшення частоти оновлення не вирішує проблему без істотних компромісів у продуктивності.

Розділ 3 зосереджено на побудові ефективних методів детектування атак RowHammer. Підрозділ 3.1 аналізує класичний метод вибірки рядків, де активований рядок випадково включається до моніторингу. Запропоновано вдосконалення цієї стратегії через формалізацію ймовірності вибірки та врахування "радіуса дії атаки", що дозволяє виявляти не лише прямі, а й непрямі впливи на суміжні та віддалені рядки.

У підрозділі 3.2 описано використання сучасних методів машинного навчання, зокрема моделей LSTM, MLP і CNN. Усі три підходи продемонстрували високу ефективність у виявленні сигнатури атаки RowHammer на основі великих масивів даних, що надходять від DRAM-підсистем.

Підрозділ 3.3 присвячено методу виявлення на основі частотного масиву, який базується на лічильниках активації рядків і дозволяє виявляти перевищення безпечних порогів активації для комірок пам'яті. Хоча метод демонструє найвищу точність в умовах відомих конфігурацій пам'яті, його ефективність знижується при відхиленні від апаратних параметрів конкретних чіпів пам'яті. Тим не менш, він залишається одним із найнадійніших варіантів захисту при правильному налаштуванні системи.

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.

В підрозділі 4.3 описане тестування в реальному середовищі, яке охоплює як нейромережеві моделі, так і метод частотного масиву. Показано точність виявлення атаки як при локальному навчанні так і на загальному дата сеті.

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 свідчать про глибоке розуміння тематики дослідження, послідовність наукового мислення та здатність до формулювання власних висновків. У роботах простежується поєднання теоретичних положень із практичними результатами, що демонструє сформованість дослідницьких

навичок. Підготовлені матеріали відповідають стандартам академічної доброчесності: усі джерела зазначено коректно, факти наукових запозичень чітко ідентифіковано, відсутні ознаки плагіату.

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

Недоліки та зауваження до дисертаційної роботи.

Незначним недоліком дисертаційної роботи є обмежена деталізація обсягу та структури навчального датасету, що використовувався для тренування моделей машинного навчання. Хоча досягнута висока точність виявлення атак, більш розгорнутий аналіз вибірки, зокрема її репрезентативності щодо різних поколінь DRAM-чипів, посилив би достовірність висновків щодо універсальності запропонованого підходу.

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 галузі знань Інформаційні технології. 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.

Рецензент:

к. т. н., доцент кафедри ІБ
НТУУ «КПІ ім. Ігоря Сікорського»



Коломицев М. В.

М.П. «____» _____ 20__ року