

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора ПАЛАГІНА Володимира Васильовича
на дисертаційну роботу МАЗУРКА Валентина Олеговича
на тему «Створення засобів захисту оперативної пам'яті від атак типу RowHammer», представлену на здобуття наукового ступеня доктора філософії
з галузі знань 12 Інформаційні технології
за спеціальністю 125 Кібербезпека та захист інформації

Актуальність теми дисертації

У сучасних умовах розгалужених інформаційних систем загрози кібербезпеці все частіше виходять за межі виключно програмного рівня. Існуючі апаратні методи захисту від атак, зокрема на пам'ять обчислювальних систем, часто не забезпечують гнучкості, необхідної для адаптації до нових типів пам'яті, або мають значне енергоспоживання. Програмні рішення, своєю чергою, часто працюють із затримками або не відповідають вимогам реального часу. Усе це створює потребу в нових підходах, які поєднують апаратну точність із програмною адаптивністю.

Уразливість сучасної оперативної пам'яті до атак типу RowHammer є серйозною загрозою для безпеки обчислювальних систем, особливо з урахуванням стрімкої мініатюризації компонентів та зростання щільності розміщення даних у DRAM-чіпах. В умовах, коли апаратні засоби не завжди здатні забезпечити необхідний рівень ізоляції між комірками пам'яті, подібні атаки стають дедалі реальнішими і небезпечними. Вони здатні змінювати вміст осередків пам'яті без прямого доступу, що особливо критично в контексті захисту конфіденційної інформації, виконання привілейованого коду або гарантій цілісності обчислень. З огляду на це, дисертація, присвячена створенню ефективних засобів виявлення та запобігання RowHammer-атакам, відповідає сучасним викликам у сфері кібербезпеки.

Актуальність дослідження також визначається недостатньою ефективністю наявних захисних рішень, які часто базуються на спрощених моделях пам'яті, мають надмірні енергоспоживання та затримки. Розробка методів детектування атак на основі математичного моделювання та машинного навчання, які працюють у реальному часі, має практичну цінність для впровадження у сучасні комп'ютерні архітектури. Особливо важливо, що дослідження орієнтоване не лише на теоретичні моделі, але й на побудову тестової платформи та апробацію результатів у реальному середовищі, що підвищує їхню прикладну значущість та перспективність для подальшої інтеграції у промислові рішення.

Таким чином, актуальність теми дисертаційної роботи МАЗУРКА В.О., у якій розглянуто загрози і вразливості у пам'яті комп'ютерних систем, представлені методи та моделі захисту пам'яті обчислювальних систем від атак типу RowHammer, не викликає сумнівів.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

- вперше запропоновано та реалізовано модель захисту DRAM-систем на основі нейронних мереж, зокрема MLP, яка забезпечує виявлення атак RowHammer у режимі реального часу з високою точністю, використовуючи локальні особливості патернів доступу до пам'яті;
- вперше розроблено модель захисту пам'яті DRAM систем на основі лічильників доступу, який виключає проблему нерівномірного оновлення комірок пам'яті, типової для традиційних методів на основі періодичного оновлення, і дозволяє виявляти атаки з високою точністю при зниженому використанні ресурсів системи.

Робота комплексно вирішує задачу виявлення та запобігання атакам типу RowHammer через моделювання, реалізацію та тестування захисних рішень як апаратного, так і програмного рівня. Зокрема удосконалено методологію тестування за допомогою платформи для порівняння різних механізмів захисту з урахуванням таких параметрів, як точність виявлення, продуктивність, споживання ресурсів та адаптивність до змін у топології пам'яті. Такий підхід уперше забезпечує як гнучкість, так і повноту захисту, що робить запропоновану систему придатною для використання у високонадійних обчислювальних середовищах, включаючи сервери, дата-центри та об'єкти критично важливої ІТ-інфраструктури.

Отже, в дисертаційній роботі поставлене наукове завдання 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 напрямам 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 співпадіння, 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 / англійською мовами.

Робота написана з дотриманням академічного стилю та з використанням термінів, прийнятих у сучасній комп'ютерній інженерії та інформаційній безпеці. Стиль викладення сприяє не лише сприйняттю, а й критичному аналізу запропонованих рішень.

Дисертація складається з вступу, 4 розділів, висновків та списку літератури. Загальний обсяг дисертації 208 сторінок, у тому числі 167 сторінок основного тексту.

У *вступі роботи* обґрунтовується актуальність теми дисертаційної роботи, наведений огляд поточного стану проблеми атак на оперативну пам'ять, продемонстровано її важливість в контексті розвитку інформаційних систем, визначено мету роботи, задачу дослідження, зв'язок роботи з науковими програмами, мету дослідження, наукову новизну роботи і практичне значення її результатів.

У *першому розділі дисертації* систематизоване знання про оперативну пам'ять як предмет для атак, детально описано архітектуру пам'яті, механізми обробки даних і роль кеш-пам'яті різних рівнів. Зокрема, 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, розглянуто основні напрямки атак на DRAM, серед яких окрема увага приділяється RowHammer, як найбільш небезпечному типу. Наприкінці наведено сучасні методи захисту — як апаратні (ЕСС, підвищення частоти оновлення, лічильники доступу), так і програмні. У висновку продемонстровано, що ці підходи мають значні обмеження, і тому ключовою метою нових рішень є розробка методів своєчасного виявлення атаки до моменту пошкодження даних.

Другий розділ присвячено практичному аспекту виявлення вразливостей DRAM до атак типу RowHammer. Описано створення тестової платформи на основі FPGA, яка дозволяє порушувати стандартні таймінги та команди DRAM для виявлення не задокументованих реакцій мікросхем пам'яті. Такий підхід

забезпечив гнучке середовище для дослідження нестандартної поведінки модулів, що неможливо реалізувати за допомогою звичайних контролерів.

Представлено результати масового тестування 253 чіпів DRAM від провідних виробників, де продемонстровано рівень вразливості модулів DDR3, DDR4 і DDR5 та основні вектори атак для них. Наприкінці розділу було проведено практичний тест та аналіз найбільш поширених апаратних методів захисту — ECC і збільшення частоти оновлення. Виявлено їхні технічні обмеження, зокрема неспроможність виявляти специфічні патерни атак або зупиняти лавинні зміни, що підкреслює потребу в нових підходах до захисту пам'яті.

У *третьому розділі дисертації* розглядаються три підходи до детектування та протидії атакам типу RowHammer: метод випадкової вибірки рядків, засоби машинного навчання та використання частотного масиву. У підрозділі 3.1 проаналізовано метод вибірки рядків, в якому активований рядок з малою ймовірністю p потрапляє до контрольної вибірки. Запропоновано математичний підхід до уточнення ключового параметра p , що зазвичай є неточним і призводить до зниження рівня захисту, а також введено поняття радіуса дії атаки для точної локалізації агресивного впливу.

У підрозділі 3.2 запропоновано інноваційний підхід із використанням моделей машинного навчання для аналізу шаблонів доступу до пам'яті. Використано три архітектури: LSTM, MLP і CNN. Результати тестування показали, що всі моделі досягли понад 99% точності, а найкращу ефективність продемонстрував багаторівневий перцептрон (MLP) — 99,7% точності при швидкості виявлення 6,9 мкс, що свідчить про високу практичну придатність моделі.

У підрозділі 3.3 описано підхід із використанням частотного масиву, заснованого на лічильниках активації рядків DRAM. Хоча такі системи мають високу точність (до 99,8%), вони залежать від коректного налаштування параметра частоти запитів контролера пам'яті і синхронізації циклів оновлення пам'яті. Було продемонстровано, що навіть невеликі часові зсуви можуть значно знижувати рівень детектування атак. Тим не менш, при правильному налаштуванні параметрів, метод залишається одним із найефективніших засобів виявлення та протидії атакам RowHammer.

У *Розділі 4* представлено практичну реалізацію та тестування захисних механізмів проти RowHammer-атак у реальних умовах. На початку розділу акцентовано увагу на виборі комплектуючих тестової системи, що одночасно може аналізувати отримані результати тестування DRAM. Зокрема висока частота доступу ЦП і обробка даних дозволяє ефективно перевірити роботу запропонованих механізмів захисту в умовах, наближених до реальних.

Розглянуто дискретизацію параметрів часу, дозволяє налаштувати систему таким чином, щоб забезпечити максимальну ефективність виявлення при мінімальних апаратних витратах. Описано результати тестування інтегрованих захисних систем, зокрема нейромережових моделей та частотного масиву, у різних конфігураціях.

У *Висновках* дисертаційної роботи описано розв'язану актуальну науково-прикладну задачу розробки методів захисту оперативної пам'яті DRAM від сучасних атак типу RowHammer. Продемонстровано спроби 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 формування власних висновків. У роботах простежується поєднання теоретичних положень із практичними результатами, що демонструє сформованість дослідницьких навичок. Підготовлені матеріали відповідають стандартам академічної доброчесності.

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

Недоліки та зауваження до дисертаційної роботи

1. В тексті дисертації відсутні посилання на деякі наведені в роботі рисунки, зокрема рис.1.1, 2.9, 2.10 та ін.
2. Інформація, наведена на деяких рисунках не співпадає по змісту з наведеними підрисунковим поясненням, наприклад на рис.2.12 та ін.
3. Перший розділ дисертації перенасичений наведеним аналізом, частину якого без втрати якості роботи можна було б перенести в додатки. Так само як п.3.3.1 «Вибір моделі машинного навчання» на стор.138 містить широко відому оглядову інформацію, а нумерація цього підрозділу дублюється на стор.151.

4. В третьому розділі дисертації наводиться аналіз машинного навчання з підкріпленням (стор.142-143), але в роботі такий підхід не застосовується.
5. В роботі розглядається обробка даних методами машинного навчання. Разом з цим не описаний механізм збору даних, їх обсяг, препроцесінг даних, вибір ознак та їх кількість, вибір головних ознак, не описані питання балансування даних тощо, що є важливими параметрами для побудови будь-якої якісної моделі.
6. В таблиці 3.3. наводяться метрики отриманих моделей, але відсутній такий інтегральний показник, як метрика f1, яка найбільш об'єктивно оцінює якість отриманих моделей.
7. В третьому розділі дисертації наводяться лістинги для трьох моделей машинного навчання (лістинг 3.2-3.4), але не наводиться обґрунтування та аналіз вибору саме таких структур нейромереж, підбір їх гіперпараметрів, кількість епох навчання, аналіз перенавчання моделей тощо.
8. Не наведений порівняльний аналіз запропонованих методів з вже відомими результатами по даному напрямку досліджень, в тому числі методами машинного навчання.
9. В тексті дисертації наявні деякі стилістичні помилки.

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

Висновок про дисертаційну роботу

Зміст дисертаційної роботи МАЗУРКА Валентина Олеговича на тему «Створення засобів захисту оперативної пам'яті від атак типу RowHammer» є завершеною науково-дослідною працею, у якій отримано нові наукові обґрунтовані результати. У дисертаційній роботі В.О.Мазурка здійснено всебічне дослідження проблеми захисту оперативної пам'яті від атак типу RowHammer, розроблено математичну модель пам'яті DRAM, що враховує реальні фізичні характеристики мікросхем, а також створено ефективні методи детектування атак на основі машинного навчання та обліку частоти доступу до рядків пам'яті. Автором запропоновано програмні, апаратні та комбіновані засоби захисту, які продемонстрували високу точність виявлення загроз без суттєвого впливу на продуктивність системи.

Вважаю, що дисертаційна робота 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 12 «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, а її автор МАЗУРОК Валентин Олегович заслуговує на присудження йому наукового ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 125 - «Кібербезпека та захист інформації».

Офіційний опонент:

завідувач кафедри робототехнічних
і телекомунікаційних систем та кібербезпеки
Черкаського державного технологічного
університету, д.т.н., професор

Володимир ПАЛАГІН

Підпис д.т.н., професора Володимира ПАЛАГІНА засвідчую:

Учений секретар
Черкаського державного технологічного
університету, к.т.н., доцент



Ірина МИРОНЕЦЬ