УДК 004.056.53

А. В. Горбач

ЕВОЛЮЦІЯ ВРАЗЛИВОСТЕЙ ПЕРЕПОВНЕННЯ БУФЕРА ПАМ'ЯТІ У ПРИСТРОЯХ ІНТЕРНЕТУ РЕЧЕЙ: ВІД БАЗОВИХ ПОМИЛОК ДО СУЧАСНИХ АПАРАТНИХ ОБХОДІВ ЗАХИСТУ

Вінницький Національний Технічний Університет

Анотація

У роботі проаналізовано причини виникнення вразливостей переповнення буфера пам'яті. Визначено сучасні вектори їх розвитку та експлуатації, починаючи від базових помилок логіки до складних апаратних обходів. Оцінено ефективність існуючих методів захисту програмного та апаратного забезпечення, зокрема в контексті пам'яті мікроконтролерів та IoT-пристроїв.

Ключові слова: переповнення буфера пам'яті, кібербезпека, мікроконтролери, Інтернет речей (IoT), апаратний захист, вразливості пам'яті.

Abstract

The paper analyzes the causes of memory buffer overflow vulnerabilities. Modern vectors of their development and exploitation are identified, ranging from basic logic errors to complex hardware bypasses. The effectiveness of existing software and hardware protection methods is evaluated, particularly in the context of microcontroller memory and IoT devices.

Keywords: memory buffer overflow, cybersecurity, microcontrollers, Internet of Things (IoT), hardware protection, memory vulnerabilities.

Вступ

Останнім часом, поряд із подальшим стрімким розвитком інформаційних технологій, суттєво зростає загальна кількість кібератак, спрямованих на експлуатацію вразливостей пам'яті. Значний відсоток таких атак припадає на пристрої Інтернету речей (IoT) та мікроконтролери. Ця проблема стоїть особливо гостро, оскільки такі пристрої залишаються основною мішенню через використання застарілого коду, класичних типів RAM-пам'яті, жорстку економію апаратних ресурсів та часто повну відсутність базових механізмів захисту на рівні компілятора та операційної системи.

Метою роботи є аналіз принципів виникнення вразливостей переповнення буфера пам'яті, визначення сучасних векторів їх розвитку та експлуатації (від базових помилок логіки до апаратних обходів) та оцінка ефективності існуючих методів захисту програмного та апаратного забезпечення.

Основні проблеми атак переповнення буфера пам'яті

Фундаментальною причиною вразливостей переповнення буфера пам'яті залишаються помилки в логіці функціонування систем та відсутність жорсткого контролю над межами виділеного обсягу пам'яті. Як показує практика, такі вразливості часто формуються під час генерації конкретних машинних інструкцій та команд компіляторами або трансляторами, особливо коли мова йде про роботу з низькорівневим доступом до пам'яті в різних програмних середовищах.

Суть вразливості полягає в тому, що програма під час запису даних виходить за межі виділеного їй буфера. Це неодмінно призводить до перезапису суміжних комірок пам'яті. Зловмисникам це дозволяє змінити хід виконання програми, зробити доступними дані, які знаходяться в одній комірці для іншої, викликати відмову в обслуговуванні (DoS) або повністю скомпрометувати систему (наприклад, реалізувати атаки типу підміни — spoofing — на DNS-сервери).

Типовим прикладом подібних загроз є критичні вразливості класу переповнення буфера пам'яті у мережевих стеках IoT-пристроїв (наприклад, CVE-2020-11896) [1]. Для підвищення надійності таких си–

стем критично важливим є застосування додаткових методів контролю пам'яті мікроконтролерів (RAM/ Cache-пам'ять), зокрема апаратних механізмів виявлення та корекції помилок (ECC та ECC+) [2].

Водночас еволюція векторів експлуатації демонструє, що сучасні атаки вийшли далеко за межі простого переповнення стека пам'яті (Stack Smashing, Stack/Buffer Overflow). Сьогодні активно застосовуються складні техніки, зокрема переповнення динамічно розподіленої пам'яті (Heap Overflow), що дозволяють зловмисникам маніпулювати вмістом пам'яті навіть у таких доволі захищених середовищах, як ОС Windows 10 [3]. Прикладом такої комплексної загрози є відома вразливість CVE-2021-3156 в програмні утиліті Sudo.

Поступове впровадження програмних захисних механізмів, таких як ASLR, DEP/NX та Stack Canaries [1, 4], змусило атакуючих шукати нові шляхи обходу, змістивши фокус на апаратний рівень захисту пам'яті. Показовим прикладом цієї тенденції є використання мікроархітектурних багів, таких як спекулятивне виконання інструкцій, для подолання апаратних механізмів безпеки [5]. Зокрема, атака PACMAN на пам'ять процесорів архітектури ARM, які часто входять до складу IoT-систем, переконливо доводить, що експлуатація переповнення буфера може бути успішно реалізована навіть за наявності сучасного криптографічного захисту вказівників (Pointer Authentication Codes) [6].

Висновки

Вразливість переповнення буфера пам'яті не втратила своєї актуальності, а лише змінила форму. У сегменті IoT та legacy-систем вона продовжує існувати у класичному вигляді через нехтування практиками безпечної розробки. Ефективний захист вимагає комплексного підхода: від ревізії застарілого коду та використання безпечних мов програмування до впровадження нових архітектурних рішень (включно з ECC/ECC+ контролем) на рівні апаратного забезпечення (hardware).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. An In-Depth Survey of Bypassing Buffer Overflow Mitigation Techniques // MDPI. – URL: https://www.mdpi.com/2076-3417/12/13/6702 (Дата звернення: 05.03.2026).
2. Куперштейн Л. М. Аналіз загроз безпеки мікроконтролерів // Л. М. Куперштейн, В. І. Маліновський та ін. // Інформаційні технології та комп'ютерна інженерія. – URL: https://itce.vntu.edu.ua/index.php/itce/article/view/902/589 (Дата звернення: 10.03.2026).
3. Heap Overflow Exploitation on Windows 10 Explained // Rapid7 Blog. – URL: https://www.rapid7.com/blog/post/2019/06/12/heap-overflow-exploitation-on-windows-10-explained/ (Дата звернення: 07.03.2026).
4. Вразливості програмного забезпечення та мережеві атаки // Відкритий архів ХНУРЕ. – URL: https://openarchive.nure.ua/bitstreams/c896eb4e-b241-4f00-abee-10067476357c/download (Дата звернення: 13.03.2026).
5. Куперштейн Л. М. Аналіз механізмів апаратного захисту мікроконтролерів / Л. М. Куперштейн, В. І. Маліновський та ін. // Оптикоелектронні інформаційно-енергетичні технології. – URL: https://oeipt.vntu.edu.ua/index.php/oeipt/article/view/629/600 (Дата звернення: 14.03.2026).
6. PACMAN: Attacking ARM Pointer Authentication with Speculative Execution // MIT DSpace. – URL: https://dspace.mit.edu/bitstream/handle/1721.1/146470/3470496.3527429.pdf (Дата звернення: 20.03.2026).

Горбач Аліна Вікторівна, студентка групи 2БС-24б факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, horbachalina08@gmail.com.

Науковий керівник: ***Маліновський Вадим Ігорович***, кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Horbach Alina Viktorivna, student of the Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, horbachalina08@gmail.com.

Scientific supervisor: ***Malinovskyi Vadym Ihorovych***, PhD in Technical Sciences, Associate Professor of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia.