УДК 004.056.5

В. І. Білоконь

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ КОНТЕЙНЕРИЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДО SUPPLY CHAIN АТАК У ХМАРНИХ ІНФРАСТРУКТУРАХ НА ОСНОВІ КОНТЕКСТНО-АДАПТИВНОЇ РЕДУКЦІЇ

Вінницький національний технічний університет

Анотація

У роботі запропоновано метод підвищення захищеності контейнеризованого програмного забезпечення шляхом застосування контекстно-адаптивної редукції образів у хмарних інфраструктурах. Такий підхід дозволяє динамічно відстежувати системну активність середовища виконання за допомогою технології eBPF, виконувати рекурсивний аналіз ELF-залежностей бінарних файлів та автоматизовано формувати захищені мікро-контейнери типу Distroless, мінімізуючи загальну поверхню атаки та нівелюючи ризики вразливостей ланцюжків поставок (Supply Chain атак).

Ключові слова: контейнеризація, Docker, eBPF, редукція образу, поверхня атаки, Supply Chain атаки, інформаційна безпека..

Abstract

The paper proposes a method for improving the security of containerized software by applying context-adaptive image reduction in cloud infrastructures. This approach allows dynamically tracking system activity in runtime using eBPF technology, performing recursive analysis of ELF-dependencies of binary files, and automated generation of secure Distroless micro-containers, minimizing the overall attack surface and mitigating the risks of software supply chain vulnerabilities..

Keywords: containerization, Docker, eBPF, image reduction, attack surface, Supply Chain attacks, information security.

Вступ

Стрімкий розвиток та впровадження технологій контейнеризації на базі платформ Docker та Kubernetes стали стандартом для розгортання сучасних хмарних застосунків. Проте, стандартні базові Docker-образи часто містять надлишкові компоненти операційної системи (командні оболонки, утиліти адміністрування, пакетні менеджери), які не використовуються під час штатної роботи сервісу. Це створює значні безпекові ризики, розширюючи поверхню потенційних атак та полегшуючи зловмисникам реалізацію атак на ланцюжки поставок програмного забезпечення (Supply Chain attacks) [1].

Застосування виключно статичного аналізу вихідного коду або сканування образів на відомі вразливості (CVE) не вирішує проблему наявності надлишкового інструментарію розвідки в runtime-середовищі. Тому доцільним є використання динамічного комплексного підходу, який поєднує низькорівневий моніторинг ядра операційної системи та автоматизовану редукцію файлового складу контейнера до мінімально необхідного контексту виконання.

Результати дослідження

Запропонований метод контекстно-адаптивної редукції базується на концепції побудови безпечних мікро-образів архітектури Distroless, що збираються з нульового базового шару scratch. Процес мінімізації та підвищення захищеності контейнеризованого ПЗ формалізується у вигляді чотирьох послідовних взаємопов’язаних етапів.

На першому етапі здійснюється розгортання та ініціалізація вихідного Docker-образу (RAW-образу) в ізольованому тестовому середовищі (Sandbox). Це необхідно для безпечного профілювання його поведінки без ризику компрометації робочої інфраструктури хмари [2].

На другому етапі пропонується використання технології eBPF (Extended Berkeley Packet Filter) для динамічного моніторингу системних викликів на рівні ядра Linux у реальному часі. eBPF-трейсер перехоплює виклики openat, execve та read, фіксуючи виключно ті файли, бібліотеки та утиліти, до яких фактично звертається додаток під час виконання функціональних тестів. Такий підхід забезпечує нульовий оверхед (навколишнє навантаження) на операційну систему й гарантує високу точність фіксації об'єктів активного контексту F_{active} [3].

На третьому етапі конвеєра запускається спеціалізований модуль статичного аналізу бінарних файлів – ELF-парсер. Оскільки багато зафіксованих компонентів використовують динамічне лінкування (Dynamic Linking), виникає потреба рекурсивного розгортання графа їхніх транзитивних залежностей. ELF-парсер зчитує секції DT_NEEDED виконуваних файлів, автоматично визначаючи шляхи до специфічних системних бібліотек (.so-файлів), лінкерів та конфігураційних файлів, які критично важливі для збереження цілісності програми. На основі об'єднання динамічного та статичного аналізу формується фінальний безпековий маніфест мінімального набору файлів F_{min} [4]:

$$F_{min} = F_{\text{active}} \cup F_{\text{transitive}}$$

На четвертому етапі сформований маніфест передається до складального модуля, який взаємодіє з Docker API. Модуль ініціює створення нового порожнього шару FROM scratch і здійснює пофайлове копіювання об'єктів із "білого списку" F_{min}. У результаті генерується захищений редукований образ (Reduced Image), який повністю позбавлений інтерпретаторів (на кшталт bash, sh), мережевих утиліт розвідки (curl, wget, netcat) та менеджерів пакетів [5].

Експериментальні дослідження розробленого методу на базі популярних enterprise-образів (зокрема, СУБД MySQL та дистрибутивів Ubuntu/Debian) продемонстрували високу ефективність захисту. Коефіцієнт редукції розміру образів досягає від 89.05% до 99.58% (на прикладі мінімізації образу mysql:latest з 260.79 MB до 1.08 MB). При цьому повністю зберігається показник функціональної цілісності додатка (FI = 1), оскільки всі критичні бінарні зв'язки враховано під час транзитивного аналізу ELF-структур. Вилучення надлишкового ПЗ унеможливлює закріплення зловмисника всередині контейнера у випадку експлуатації zero-day вразливостей, радикально знижуючи загальну поверхню атаки хмарної інфраструктури [6].

Висновок

У роботі запропоновано метод підвищення захищеності контейнеризованого програмного забезпечення, що базується на комплексному використанні динамічного eBPF-моніторингу системних викликів ядра та статичного ELF-аналізу транзитивних залежностей бібліотек. Такий підхід дозволяє автоматизувати процес контекстно-адаптивної редукції образів до безпечного рівня Distroless, зменшуючи їхній об'єм та ліквідуючи потенційні вектори Supply Chain атак.

Практичне значення отриманих результатів полягає у розробці автоматизованого програмного комплексу на мові Python, який може бути інтегрований у сучасні CI/CD конвеєри безпечної розробки (DevSecOps) для захисту мікросервісних додатків. Подальше удосконалення технології пов’язане з оптимізацією алгоритмів автоматичного покриття коду тестами під час eBPF-профілювання та дослідженням сумісності редукції для багатоархітектурних контейнерних систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CNCF Software Supply Chain Best Practices [Електронний ресурс]. – Режим доступу: https://github.com/cncf/tag-security/blob/main/supply-chain-security/supply-chain-security-paper/v1/software-supply-chain-security-paper-v1.md
2. BPF Compiler Collection (BCC) Reference Guide [Електронний ресурс]. – Режим доступу: https://github.com/iovisor/bcc/blob/master/docs/reference_guide.md
3. pyelftools documentation [Електронний ресурс]. – Режим доступу: https://github.com/eliben/pyelftools
4. Docker SDK for Python documentation [Електронний ресурс]. – Режим доступу: https://docker-py.readthedocs.io/en/stable/
5. Google Container Tools - Distroless [Електронний ресурс]. – Режим доступу: https://github.com/GoogleContainerTools/distroless
6. OWASP Container Security Top 10 [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-container-security-top-10/

Білоконь Владислав Іванович - студент групи 2КІТС-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: zarootokv@gmail.com

Грицак Анатолій Васильович - кандидат технічних наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: *grytsak.a.v@gmail.com*

Bilokon Vladyslav Ivanovych *– student of group 2KITS-22B, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: zarootokv@gmail.com*

Supervisor: Hrytsak Anatolii Vasylovych *– Candidate of Technical Sciences, Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com*