УДК 004.056.52

Луканов М.В.
Карпінець В.В.

ЦИФРОВИЙ ПІДПИС ЯК МЕТОД АВТЕНТИФІКАЦІЇ В СИСТЕМАХ КОНТРОЛЮ ВЕРСІЙ ВИХІДНОГО КОДУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Вінницький національний технічний університет

Анотація

У цьому дослідженні було проведено комплексний аналіз сучасних методів автентифікації у системах контролю версій вихідного коду програмного забезпечення та можливість покращення захисту від неавтентифікованих змін, що може бути корисно для підприємств, для яких питання ретельної перевірки коду є критичним.

В результаті комплексного аудиту, було визначено можливість використання цифрового підпису як перспективний метод автентифікації та контролю коду на всіх етапах життєвого циклу програмного забезпечення.

Ключові слова: *системи контролю версій, автентифікація, захист даних, версіонування, цифровий підпис.*

Abstracts.

This study presents a comprehensive analysis of modern authentication methods in version control systems for software source code and explores the potential to enhance protection against unauthorized changes. This research could benefit enterprises where rigorous code verification is critical.

As a result of an in-depth audit, the use of digital signatures was identified as a promising method for authentication and code control at all stages of the software lifecycle.

Keywords*: version control systems, authentication, data protection, versioning, digital signature.*

Вступ

На сьогоднішній день робота з вихідним кодом програмного забезпечення потребує високого рівня захисту, особливо на етапах його перевірки, збереження та внесення змін. Однією з основних загроз є ризик несанкціонованих модифікацій коду, що може призвести до серйозних наслідків, зокрема для підприємств, де надійність та безпека програмного забезпечення є особливо чутливим.

Сучасні системи контролю версій дозволяють зберігати історію змін, але не завжди гарантують захист від втручання сторонніх осіб, а також диверсії. Традиційні методи автентифікації забезпечують певний рівень захисту, однак із зростанням складності загроз цього може бути недостатньо. Одним із перспективних підходів до вирішення цієї проблеми є використання цифрових підписів, які забезпечують автентифікацію та контроль цілісності коду на всіх етапах його життєвого циклу та забезпечення, що код в кінцевого користувача пройшов перевірку аудитора і не містить шкідливих або небезпечних компонентів.

У цьому дослідженні проведено аналіз сучасних методів автентифікації у системах контролю версій та запропоновано використання цифрового підпису як надійного засобу для підвищення безпеки вихідного коду.

Результати дослідження

Системи контролю версій вихідного коду програмного забезпечення відіграють ключову роль у процесі розробки програмного забезпечення, ставши певним стандартом, забезпечуючи збереження історії змін, координацію між розробниками та підтримку цілісності коду. Проте безпека цих систем залишається критичним питанням, особливо з огляду на ризики внесення неавторизованих змін сторонніми особами або під час диверсії. Автентифікація користувачів та контроль цілісності коду є основними заходами, які дозволяють підвищити захист у таких системах.

Серед основних загроз, які стосуються автентифікації можна виділити:

- Supply Chain Attacks – атака шляхом націлювання на менш безпечні елементи в ланцюзі поставок [1];

- Code Injection – зловмисник впроваджує шкідливий код в програму, яка потім виконується додатком [2];
- компрометація облікових записів – отримавши доступ до акаунту розробника, зловмисник може внести несанкціоновані зміни, а маючи необхідні права – приховати діяльність в історії змін;
- атаки через автоматизацію процесів – зловмисники можуть інтегрувати шкідливий код на етапах тестування чи розгортання.

Сучасні методи автентифікації включають використання паролів, багатофакторної автентифікації, ssh-ключів токенів доступу [3]. У таблиці 1 представлено аналіз основних методів автентифікації, їхніх переваг та недоліків.

Таблиця 1 – Аналіз основних методів автентифікації

Метод автентифікації	Рівень захисту	Переваги	Недоліки
Пароль	Низький	Простота використання, низькі вимоги до впровадження	Уразливість до атак методом підбору, фішингу, необхідність регулярної зміни
Двофакторна автентифікація	Середній	Значно підвищує безпеку, захист навіть у разі компрометації пароля	Залежність від другого фактора (SMS, додаток тощо), потребує додаткових ресурсів
SSH-ключі	Високий	Сильне шифрування, автоматизація доступу, складність підробки	Складність управління великою кількістю ключів, можливість втрати ключа
Токени доступу	Низький	Зручність використання в автоматизованих системах, мінімізація потреби в паролях	Короткий термін дії (якщо не встановлено належним чином); компрометація токена може надати повний доступ

Усі вищеперераховані методи дозволяють налаштувати безпеку для сесій користувачів та автоматизованих систем, хоч і мають свої недоліки і вразливості. Однак у випадку, коли аналіз коду перед його поширенням, в тому числі, в CICD – практик безперервного розгортання вихідного коду програмного забезпечення на кінцевих точках [5], є критичним питанням, стандартні методи не дозволяють проводити оцінку та погодження/не погодження змін з високим рівнем захисту. Для забезпечення даних потреб пропонується використання цифрового підпису.

Впровадження незалежної системи цифрового підписування та верифікації підпису дозволяє уповноваженим особам після аналізу та погодження вихідного коду підтверджувати зміни, підвищуючи рівень автентифікації. Також вказана система повинна містити функціонал, який дозволяє в будь-який момент часу, незалежно від місця розміщення файлів проекту перевірити їх на наявність неавтентифікованих змін та фіксувати події в SIEM та SOAR системах.

Висновки

Отже, з огляду на проведене дослідження сучасних методів автентифікації та їхніх переваг і недоліків, можна зробити висновок, що традиційні методи, такі як паролі, двофакторна автентифікація та SSH-ключі, мають певний рівень захисту, проте вони не забезпечують достатню надійність у випадку складних загроз. Найбільш перспективним підходом до підвищення безпеки вихідного коду є використання цифрового підпису, який гарантує автентичність та цілісність коду на всіх етапах його життєвого циклу. Впровадження системи цифрового підпису дозволить не лише захистити код від несанкціонованих змін, але й забезпечити контроль над його розповсюдженням, надаючи додатковий рівень безпеки для автоматизованих процесів розгортання та зберігання даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Supply Chain Attack. *DOU*. URL: https://dou.ua/forums/topic/47587/ (дата звернення 10.11.2024).

2. Впровадження коду. URL: https://cqr.company/ua/web-vulnerabilities/code-injection/ (дата звернення 10.11.2024).

3. About authentication to GitHub. URL: https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/about-authentication-to-github. (дата звернення 10.11.2024).

4. Elisa Bertino, Emilio Montolivo, Giancarlo Martella, Emilio Montolivo. Computer Security. 2005. pp 44–64

5. What is CI/CD? URL: https://about.gitlab.com/topics/ci-cd/ (дата звернення 10.11.2024).

6. Kaur R., Kaur A. Digital Signature. International Conference on Computing Sciences (ICCS), Phagwara, India, 14–15 September 2012.

Луканов Максим Всеволодович – студент групи КІТС-23м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail

Науковий керівник: **Карпінець Василь Васильович** – к.т.н., доц. каф. МБІС

Lukanov Maksym V. – student of group KITS-23m, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail

Scientific adviser: **Karpinets Vasyl V.** – Candidate of Technical Sciences, Associate Professor. MBIS.