МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

Розголошення інформації, як правило, зустрічається в двох формах. Перший – розголошення про компоненти і структуру веб-застосунку, а другий – витік інформації з веб-застосунку, з причин, не надійного захисту.

Логічні атаки спрямовані на експлуатацію функцій додатка або логіки його функціонування. Логіка додатка є очікуваний процес функціонування програми при виконанні певних дій, наприклад, відновлення пароля, реєстрація облікового запису або транзакції в інтернет-магазинах. Застосунок може вимагати від користувача коректного виконання декількох послідовних дій для виконання певного завдання. Зовнішній порушник обходить або використовує ці механізми в своїх цілях. До таких атак можна віднести DoS та DDoS.

Існує два основних види атак на веб-застосунки – це цільові атаки і нецільові атаки.

Цільові атаки – це будь-які напади зовнішніх порушників на конкретний сайт або їх групу, об'єднану однією ознакою. Такі операції протиставляються масовим атакам за допомогою вірусів або інших шкідливих програм, де жертва обирається за принципом доступності. Мета у таких атак, зазвичай, є отримання конфіденційної інформації для матеріальної вигоди.

Нецільові атаки здійснюються на випадкові сайти. Основним завданням нецільової атаки, є отримання несанкціонованого доступу до веб-застосунків, атакуючи відразу велику вибірку ресурсів, відібраних за якимось критерієм, наприклад, веб-застосунки працюють на певній системі управління контентом. При позитивному результаті, зовнішній порушник, створює акаунт адміністратора всередині веб-застосунку для впровадження на ресурс шкідливих сценаріїв, або для крадіжки бази даних.

Поширення атак на веб-застосунки пов'язані з двома головними факторами: відсутність безпеки, або ж, знижена безпека веб-застосунку і низький поріг входу для зовнішніх порушників.

Як правило, більшість веб-застосунків не використовують спеціальні засоби моніторингу та виявлення загроз, а також захисту від загроз. Також причиною може служити безвідповідальність адміністратора і команди розробників, які допускають до фінальної версії, код з помилками.

У даній роботі були зібрані і класифіковані, за кількома ознаками, основні загрози і види атак веб-застосунків, а також були вказані основні причини поширення атак на веб-застосунки. Для позбавлення від можливості зіткнення з даними проблемами, необхідно дотримуватися базових заходів безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Уязвимости и угрозы веб-приложений в 2019 году [Електронний ресурс] // Positive Technologies. – Режим доступу: https://www.ptsecurity.com/ru-ru/
2. Уязвимости сайтов [Електронний ресурс] // ANTI-MALWARE. – Режим доступу: https://www.anti-malware.ru/
3. Классификация угроз безопасности Web-приложений [Електронний ресурс] // InfoSecurity. – Режим доступу: http://www.infosecurity.ru/
4. Как защитить сайт: виды угроз безопасности и способы их избежать [Електронний ресурс] // RedKrab. – Режим доступу: https://webevolution.ru/

UDC: 004.056.5:336.74

PROOF OF ZERO-KNOWLEDGE IN THE TASKS OF ANONYMIZATION OF FINANCIAL TRANSACTIONS

PROKOPOV E. K.(*prokopov.emmanuil@stud.onu.edu.ua*)
Odessa I.I. Mechnikov National University

Often for financial systems based on blockchain technology, high transaction transparency may be undesirable. It is possible to achieve greater anonymity by using protocols based on zero-knowledge proofs. Range proof, as an example of zero-knowledge proofs, is used in some modern blockchain protocols based on elliptic-curve cryptography that provide high transaction anonymity.

In this work, we consider the possibility of applying protocols based on zero-knowledge proofs to increase the anonymity of financial transactions in financial systems based on blockchain technology. The relevance of this topic is driven by the growing interest in financial systems based on blockchain protocols. Today financial instruments based on blockchain technology have become widespread. The high interest in it is caused by its properties such as decentralization, high transparency of transactions, data safety, and resistance to data spoofing. However, in many areas of human activity, especially in finance, high transaction transparency may be undesirable. So, for example, in the Bitcoin payment system, if the address of one of the users is known, it is possible to obtain information about the history of his transactions, and details of the transactions. This work explores the possibility of using zero-knowledge proofs to achieve greater anonymity of financial transactions and discusses some of the common protocols such as ZK-SNARK and Mimblewimble.

Zero-knowledge proof is an interactive cryptographic protocol that allows one of the communicating parties to verify the validity of a statement without receiving any unnecessary information from the other party [1]. The idea is to prove that one of the parties has a piece of information without revealing its content. The protocol requires interactive input from the verifier, usually in the form of a task or a problem. The goal of the prover in this protocol is to convince the verifier that he has a solution, without revealing even part of the "secret" proof. The purpose of the verifier is to make sure that the prover indeed has the required information. Also, there are zero-knowledge proof protocols that do not require interactive input. Most of such protocols rely on the assumption of a perfect cryptographic hash function. The idea of using such protocols for validating transactions in financial systems without excessive disclosure of transaction details is very promising. Zero-knowledge proofs are widely used in many blockchain protocols that require high transaction anonymity. For example, the idea behind the Mimblewimble protocol is to hide the details of financial transactions using elliptic-curve cryptography. Due to the properties of elliptic curves, this protocol needs to use the range proofs [2] to avoid creating transactions with negative values. Range proof is proof that a number is within a specified interval, without revealing the number itself. There are also some other similar protocols, for example, ZK-SNARK, which uses elliptic-curve cryptography, and the alternate protocol ZK-STARK, which uses hash functions. Thus, using blockchain protocols based on zero-knowledge proofs allows achieving greater anonymity of financial transactions.

[1] N. R. Gowravaram, "Zero Knowledge Proofs and Applications to Financial Regulation", PhD thesis, Harvard College, 2018. [Online]. Available: https://dash.harvard.edu/handle/1/38811528. [Accessed Apr. 11, 2021].
[2] B. Bunz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille and G. Maxwell, "Bulletproofs: Short Proofs for Confidential Transactions and More," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2018, pp. 315-334.

УДК 004.91

РОЗРОБКА ПРОГРАМИ ДЛЯ ПЕРЕВІРКИ ТЕКСТІВ НА ОРИГІНАЛЬНІСТЬ

БЕВЗ С.В. (*svbevz@i.ua*), БУРБЕЛО С.М. (*burbelo@vntu.edu.ua*),
ВОЙТКО В.В. (*dekanfki@i.ua*), ЗАВАЛЬНЮК Є.К. (*qq9272627@gmail.com*)
Вінницький національний технічний університет

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.