АНОТАЦІЯ

Залива В.В. Методика підвищення надійності веб-компонентів на базі методу Isabelle/HOL.

Дисертація на здобуття наукового ступеня доктора філософії в галузі знань 12 - Інформаційні технології за спеціальністю 123 – Комп’ютерна інженерія. – Державний університет інформаційно-комунікаційних технологій. – Київ, 2023.

Дисертаційна робота присвячена підвищенню надійності веб-компонентів з використанням методу Isebelle/HOL. У даній роботі було проведено аналіз вразливостей моделі DOM, на основі яких розроблено методику підвищення надійності веб-компонентів.

У вступі наведено загальну характеристику роботи, обґрунтовано актуальність теми досліджень, сформульовано мету та задачі досліджень, представлено наукову новизну та практичну цінність отриманих результатів, відзначено особистий внесок автора, наведено дані про апробацію, практичне впровадження та наявні публікації.

У першому розділі дисертації розглянуто різні аспекти впливу веб-компонентів на розвиток комп'ютерної інженерії. Основна увага приділена тому, як веб-компоненти, які включають HTML-теги, CSS-стилі та JavaScript-функції, змінюють спосіб створення веб-додатків. Ці компоненти дозволяють розробникам створювати додатки як набір незалежних взаємозамінних частин, сприяючи переходу від традиційних монолітних архітектур до більш гнучких модульних та мікросервісних підходів. Ця зміна парадигми в розробці веб-додатків відкриває нові можливості для масштабування та оновлення окремих частин системи.

У другому розділі дисертації, що зосереджується на аналізі проблем надійності веб-компонентів, була реалізована детальна розробка формальної моделі Document Object Model (DOM) з використанням методики Isabelle/HOL. Ця модель включає основні елементи, їх взаємодію та поведінку. Вона стала ключовим

елементом у формальному доведенні безпекових властивостей веб-компонентів. Такий підхід значно покращує надійність та безпеку веб-додатків, йдучи далі від звичайних тестувань та аналізів, та створює міцну основу для розвитку більш передових методів проектування та аналізу в сфері веб-технологій.

У третьому розділі дисертації, присвяченому оцінці методик безпеки веб-компонентів, здійснено аналіз ефективності розробленої методології забезпечення безпеки веб-компонентів. Особлива увага була приділена порівняльному аналізу цієї методології з іншими існуючими підходами, такими як статичний аналіз та методи машинного навчання.

Проведені практичні тести підтвердили високу ефективність запропонованої методології у запобіганні атакам Cross-Site Scripting (XSS) та Cross-Site Request Forgery (CSRF), особливо в порівнянні з методами, що базуються на Content Security Policy (CSP). Були також розглянуті обмеження існуючих методів, особливо в контексті виявлення нових або маскованих шкідливих змістів, та запропоновано напрямки для подальших досліджень. Це включає розробку нових методів навчання, які є ефективнішими у виявленні нових типів шкідливого вмісту та методів виявлення, які краще реагують на прихований або замаскований шкідливий вміст.

У четвертому розділі дисертації здійснено оцінку ефективності методики, спрямованої на підвищення надійності веб-компонентів, яка базується на методі Isabelle/HOL. Визначені ключові показники ефективності включали повноту виявлення та точність виявлення загроз.

Було проведено експериментальну оцінку, яка включала порівняння з іншими науковими інструментами, такими як статичний аналіз та машинне навчання. Результати експериментів показали, що розроблена методика на 21% ефективніше за існуючу CSP.

Аналіз стану:

Поточний стан безпеки веб-компонентів демонструє складність викликів та постійних зусиль, спрямованих на зменшення ризиків. Важливим аспектом цього є безпека API, яка є невід'ємною частиною функціональності веб-компонентів.

Однією з головних проблем у сфері безпеки додатків, як підкреслює Cloudflare, є різноманітність векторів атак, що експлуатуються. До них відносяться інтеграції шкідливого вмісту, SQL-ін'єкції, включення файлів та атаки на програмне забезпечення. Отже, старі вразливості продовжують залишатися мішенями, що вказує на необхідність постійної пильності і регулярного оновлення заходів безпеки для захисту веб-компонентів як від нових, так і від існуючих загроз.

Ситуація з безпекою API, підкреслює зростаючу важливість API в цифровій екосистемі та відповідне зростання потенційних ризиків. Значна кількість організацій (57%) визнають критичну роль API, але існують недоліки в їх здатності повністю виявляти і захищати всі використовувані API. Лише 59% організацій можуть впевнено виявити всі API, які вони використовують, залишаючи значну кількість API потенційно вразливими до кіберзагроз. Ці недоліки створюють значні ризики, починаючи від несанкціонованого доступу до даних і закінчуючи операційними перебоями.

Крім того, лише меншість організацій (38%) мають рішення для розуміння контексту між діяльністю API, поведінкою користувачів, потоками даних та виконанням коду. Необхідність комплексного підходу до безпеки API очевидна, яка включає не лише виявлення та сканування API на наявність вразливостей, але й розуміння складних принципів взаємодії API та адаптацію реакцій безпеки на основі динамічних параметрів загроз.

Отже, незважаючи на значний прогрес у захисті веб-компонентів та API, природа кіберзагроз, що швидко розвивається, вимагає постійної пильності та адаптації стратегій безпеки. Це включає не лише впровадження надійних заходів безпеки, але й постійний моніторинг та оновлення цих заходів для усунення нових вразливостей та моделей атак.

Для досягнення поставленої мети дисертаційного дослідження, а саме розробки методики підвищення надійності веб-компонентів на базі методу Isabelle/HOL, були сформовані наступні завдання:

1. Провести аналіз наявних проблем з безпекою веб-компонентів.

2. Розробити формальну модель DOM для визначення безпечного веб-компоненту.

3. Дослідити метод підвищення надійності веб-компонентів.

4. Розробити методику для запобігання вразливостям при роботі з API.

В дисертаційній роботі представлено методику підвищення надійності веб-компонентів на базі Isabelle/HOL. Методика дала змогу підвищити ефективність запобігання загрозам на 21% у порівнянні з класичним методом CSP. Отримані наступні наукові результати:

1. Розроблено формальну модель fDOM, що дає змогу визначити безпечний веб-компонент.

2. Набув подальшого розвитку метод підвищення надійності веб-компонентів, що дає змогу виявляти проблеми з надійністю в будь-якому веб-компоненті, незалежно від того, як він реалізований.

3. Вперше розроблено методику для запобігання вразливостям при роботі з API на базі Isabelle/HOL, що дає змогу підвищити безпеку веб-компонентів та взаємодію веб-додатків між собою.

Результати, отримані у процесі виконання роботи, знайшли застосування в науково-дослідній роботі “Запобігання і протидія методам соціальної інженерії у забезпеченні інформаційної безпеки підприємства” (0123U100743), яка проводиться в Державному університеті інформаційно-комунікаційних технологій. Теоретичні і практичні положення дисертаційної роботи використовуються в навчальному процесі Державного університету інформаційно-телекомунікаційних технологій.

Ключові слова: веб-компоненти, Isabelle/HOL, формальна модель DOM, інформаційні системи, машинне навчання, автоматизація, ком’ютерна система, інформаційні технології, кібербезпека, система управління інформаційною безпекою, вразливість, програмування, алгоритм, математична модель

ABSTRACT

Zalyva V.V. Methodology for Improving the Reliability of Web Components Based on the Isabelle/HOL Method. Dissertation for the degree of Doctor of Philosophy in the field of knowledge 12 - Information Technologies, specialty 123 - Computer Engineering. - State University of Information and Communications Technology. - Kyiv, 2023. The dissertation work is dedicated to improving the reliability of web components using the Isabelle/HOL method. This work conducted an analysis of vulnerabilities in the DOM model, based on which a methodology for improving the reliability of web components was developed. The introduction presents a general characterization of the work, justifies the relevance of the research topic, formulates the purpose and objectives of the research, presents scientific novelty and practical value of the obtained results, notes the personal contribution of the author, and provides data on the approbation, practical implementation, and available publications. The first chapter of the dissertation considers various aspects of the impact of web components on the development of computer engineering. Particular attention is paid to how web components, which include HTML tags, CSS styles, and JavaScript functions, change the way web applications are created. These components allow developers to create applications as a set of independent interchangeable parts, contributing to the transition from traditional monolithic architectures to more flexible modular and microservice approaches. This paradigm shift in web application development opens new opportunities for scaling and updating individual parts of the system. The second chapter of the dissertation, focusing on the analysis of the reliability problems of web components, implemented a detailed development of the formal model of the Document Object Model (DOM) using the Isabelle/HOL methodology. This model includes the main elements, their interaction, and behavior. It became a key element in the formal proof of security properties of web components. Such an approach significantly improves the reliability and security of web applications, going beyond usual testing and analysis, and creates a solid foundation for the development of more advanced methods of design and analysis in the field of web

technologies. The third chapter of the dissertation, dedicated to assessing the safety methods of web components, conducted an analysis of the effectiveness of the developed methodology for ensuring the safety of web components. Particular attention was paid to the comparative analysis of this methodology with other existing approaches, such as static analysis and machine learning methods. Practical tests confirmed the high efficiency of the proposed methodology in preventing Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) attacks, especially compared to methods based on Content Security Policy (CSP). The limitations of existing methods were also considered, especially in the context of detecting new or masked malicious content, and directions for further research were proposed. This includes the development of new training methods that are more effective in detecting new types of malicious content and detection methods that better respond to hidden or disguised malicious content. The fourth chapter of the dissertation assessed the effectiveness of the methodology aimed at improving the reliability of web components, based on the Isabelle/HOL method. Key performance indicators included completeness of detection and accuracy of threat detection. An experimental evaluation was conducted, which included comparison with other scientific tools such as static analysis and machine learning. The experimental results showed that the developed methodology is 21% more effective than the existing CSP. Analysis of the state: The current state of security of web components demonstrates the complexity of challenges and ongoing efforts to reduce risks. An important aspect of this is API security, which is an integral part of the functionality of web components. One of the main problems in the field of application security, as emphasized by Cloudflare, is the diversity of attack vectors exploited. These include malicious content integration, SQL injections, file inclusion, and software attacks. Therefore, old vulnerabilities continue to be targets, indicating the need for constant vigilance and regular updating of security measures to protect web components from both new and existing threats. The situation with API security highlights the growing importance of APIs in the digital ecosystem and the corresponding increase in potential risks. A significant number of organizations (57%)

recognize the critical role of APIs, but there are shortcomings in their ability to fully detect and protect all used APIs. Only 59% of organizations can confidently detect all APIs they use, leaving a significant number of APIs potentially vulnerable to cyber threats. These shortcomings create significant risks, ranging from unauthorized data access to operational disruptions. In addition, only a minority of organizations (38%) have a solution to understand the context between API activity, user behavior, data flows, and code execution. The need for a comprehensive approach to API security is clear, which includes not only detecting and scanning APIs for vulnerabilities but also understanding the complex principles of API interaction and adapting security responses based on dynamic threat parameters. Thus, despite significant progress in protecting web components and APIs, the rapidly evolving nature of cyber threats requires constant vigilance and adaptation of security strategies. This includes not only implementing robust security measures but also constant monitoring and updating of these measures to address new vulnerabilities and attack patterns. To achieve the goal of the dissertation research, namely the development of a methodology for improving the reliability of web components based on the Isabelle/HOL method, the following tasks were formed:

1. Conduct an analysis of existing problems with the security of web components.
2. Develop a formal DOM model to define a secure web component.
3. Investigate the method of improving the reliability of web components.
4. Develop a methodology to prevent vulnerabilities when working with APIs.

The dissertation work presents a methodology for improving the reliability of web components based on Isabelle/HOL. The methodology allowed increasing the effectiveness of threat prevention by 21% compared to the classical CSP method. The following scientific results were obtained:

1. A formal model of fDOM was developed, allowing to define a secure web component.

2. The method of improving the reliability of web components was further developed, allowing to detect reliability problems in any web component, regardless of how it is implemented.
3. For the first time, a methodology for preventing vulnerabilities when working with APIs based on Isabelle/HOL was developed, allowing to increase the security of web components and the interaction of web applications with each other.

The results obtained in the course of the work found application in the scientific research "Prevention and Counteraction of Social Engineering Methods in Ensuring Information Security of an Enterprise" (0123U100743), which is conducted at the State University of Information and Communications Technology. The theoretical and practical provisions of the dissertation work are used in the educational process of the State University of Information and Telecommunications Technology.

Keywords: web components, Isabelle/HOL, formal DOM model, information systems, computer science, automation, computer system, information technology, cybersecurity, security information management system, spillover, programming, algorithm , mathematical model