Knowledge Transfer Office
香港城市大學
City University of Hong Kong

A Browser-based Security Framework against Malicious Extensions

Communications & Information

Computer/AI/Data Processing and Information Technology

Others

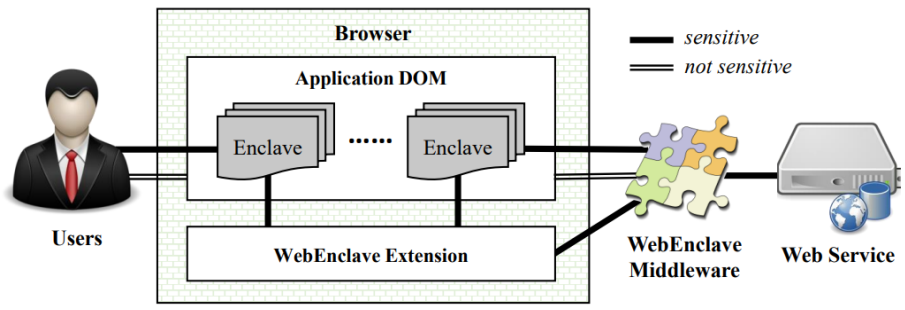


Fig. 1 The overall architecture of WebEnclave

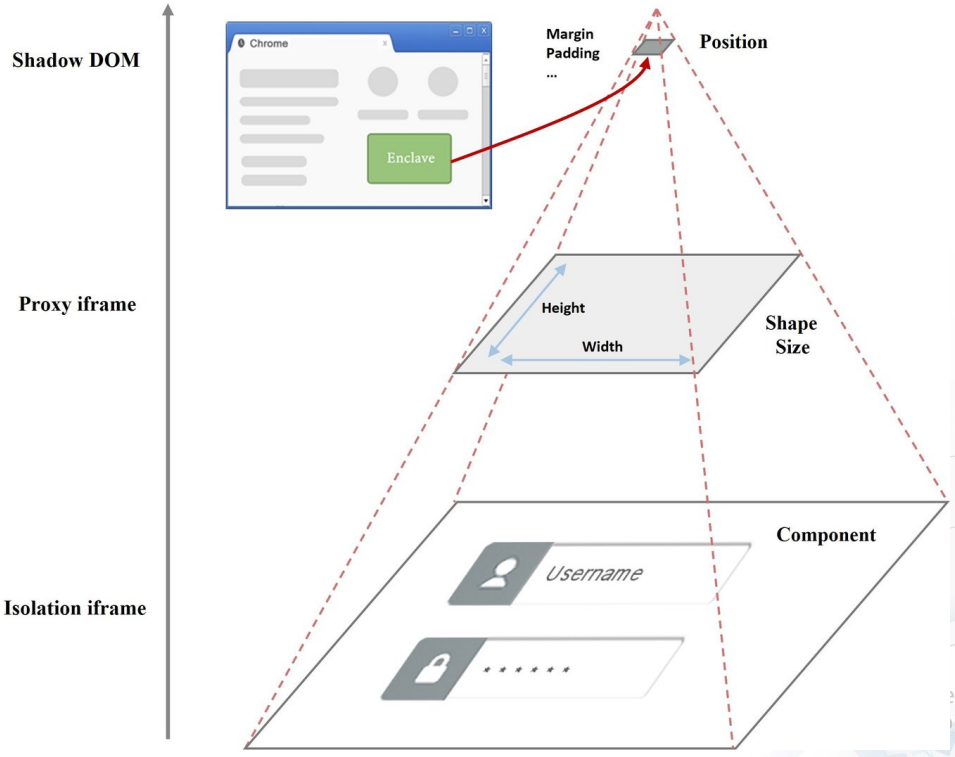


Fig. 2 Isolation of sensitive components with the use of enclaves to defend against malicious extensions

IP Status
Patent granted

Technology Readiness Level (TRL) 5

Inventor(s)

Prof. WANG Cong

Mr. WANG Xinyu

Dr. DU Yuefeng

Enquiry: kto@cityu.edu.hk

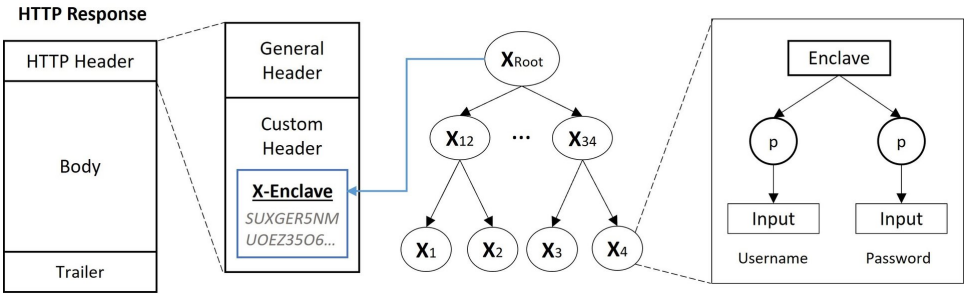


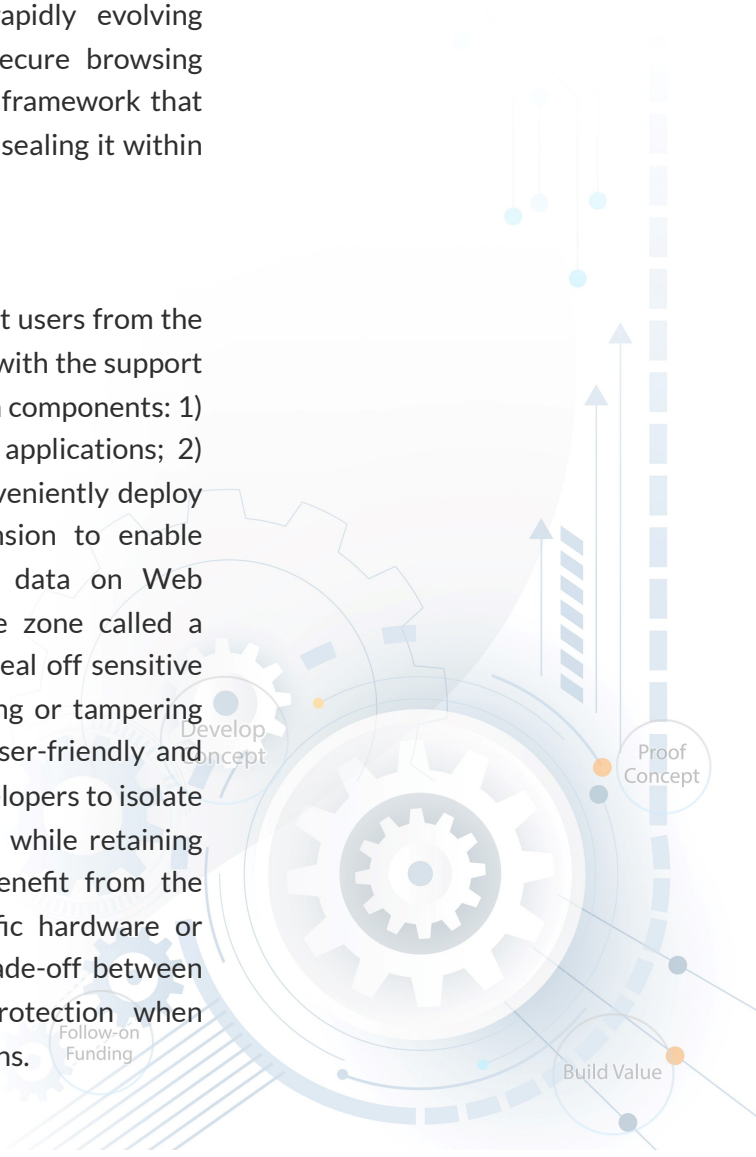
Fig.3 Integrity check of isolated enclaves throughout their lifecycle to prevent unauthorized adversarial modification.

Opportunity

More and more people are using browser extensions to “customize” their browsing experience by installing search toolbars, advertisement blockers and password managers. However, such extensions also raise security and privacy concerns, as they have privileged access to sensitive user data that can be used to launch sophisticated cyberattacks. There is a pressing need to protect the enormous—and growing—Internet user base from the malicious behaviors of browser extensions. Existing security mechanisms do not cover extensions that can read and write on Web applications at any time, and even state-of-the-art detection methods cannot track the rapidly evolving behaviours of malicious extensions. To create a more secure browsing environment, researchers have developed a novel security framework that protects sensitive user information on Web applications by sealing it within an “enclave” that malicious extensions cannot access.

Technology

WebEnclave is the first browser-based framework to protect users from the malicious behaviours of fully privileged browser extensions with the support of Web application developers. The invention has three main components: 1) a javascript library to help developers build secure Web applications; 2) middleware that enables Web application providers to conveniently deploy the novel security mechanism; and 3) a browser extension to enable individual users to isolate and protect their sensitive data on Web applications. The key feature of WebEnclave is a secure zone called a software enclave in which Web application providers can seal off sensitive data, preventing malicious browser extensions from stealing or tampering with user information. In practice, WebEnclave provides user-friendly and fine-grained application program interfaces that enable developers to isolate specific sensitive parts of Web applications for protection while retaining their original functionality and appearance. Users can benefit from the invention’s security guarantees without relying on specific hardware or installing modified browsers. They can also control the trade-off between security and functionality by, for instance, disabling protection when browsing sites that require fully functional browser extensions.



Advantages

- To the best of the researchers' knowledge, WebEnclave is the first browser-based solution to protect sensitive parts of Web applications from the malicious behaviour of browser extensions with full privileges. It has no direct competitors.
- WebEnclave does not require a specific hardware configuration to work, unlike its few indirect competitors (e.g. Fidelius and Protection).
- Unlike competitors such as Fidelius, WebEnclave does not affect users' browsing experience by changing the user interface or behavior of a Web application.

Applications

- The design and algorithm can be sold to browser vendors to enhance their defense against malicious browser extensions in the face of ever more sophisticated cyberattacks.
- For ordinary users, a template of the WebEnclave extension can be easily installed on modern browsers, giving them confidence that their secrets are protected.
- Web-based banking services can use WebEnclave to protect sensitive financial data and operations without damaging the user experience.
- Online advertisers can use the technology to deny access to browser extensions that block ads for products and services online, thus attracting more potential customers and increasing their profits.