Secure In-Process Component Isolation Mechanism Using Hardware Virtualization

Xin Wu*, **, Wenchang Shi*, **, Bo Qin*, **

** Key Laboratory of Data Engineering and Knowledge Engineering (Renmin University), Ministry Of Education, Beijing 100872, China*

*** School of Information, Renmin University of China, Beijing 100872, China*

Xinw0707@gmail.com, wenchangshi@gmail.com, bo.qin@ruc.edu.cn

***Abstract*—Ensuring the entire code base of a browser to deal with the security concerns of integrity and confidentiality is a daunting task. The basic method is to split it into different components and place each of them in its own protection domain. OS processes are the prevalent isolation mechanism to implement the protection domain, which result in expensive context-switching overheads produced by Inter-Process Communication (IPC). Besides, the dependences of multiple web instance processes on a single set of privileged ones reduce the entire concurrency.**

In this paper, we present a secure in-process component isolation mechanism. First, we divide the browser code base into privileged components and constrained components which consist of distrusted web page renderer components and plugins. All constrained components are in the form of shared object (SO) libraries. Second, we create an isolated execution environment for each distrusted shared object library using the hardware virtualization support available in modern Intel and AMD processors. Third, to enhance the entire security of browser, we implement a validation mechanism to check the OS resources access from distrusted web page renderer to the privileged components.

By utilizing hardware virtualization, our approach reduces the size of the trusted computing base and avoids the difficulties encountered with software based approaches.

***Keyword*—Browser security; Component isolation; Hardware virtualization; System call interposition; KVM**

Xin Wu, Ph. D candidate, Department of Computer Science and Technology, Renmin University of China. Her research interests include browser security and trusted computing. Email: wxin@ruc.edu.cn

Wenchang Shi, Ph. D, professor, Dean of Department of Computer Science and Technology, Renmin University of China. His research interests include information security and trusted computing. Email: wenchang@ruc.edu.cn

.

Bo Qin, Ph. D, lecturer, Department of Computer Science and Technology, Renmin University of China. Her research interests include data security, privacy protection and applied cryptography. Email: bo.qin@ruc.edu.cn