Journal of Network and Computer Applications 93 (2017) 259–279

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Review

Cross-VM cache-based side channel attacks and proposed prevention mechanisms: A survey

Shahid Anwar[a,*], Zakira Inayat[b,c,*], Mohamad Fadli Zolkipli[a], Jasni Mohamad Zain[f], Abdullah Gani[b], Nor Badrul Anuar[b], Muhammad Khurram Khan[d], Victor Chang[e]

[a] Faculty of Computer Systems & Software Engineering (FTKPP), Universiti Malaysia Pahang, Lebuh Tun Razak, Gambang, 26300 Kuantan, Malaysia

[b] Department of Computer Science, University of Engineering and Technology Peshawar, Peshawar 25000, Pakistan

[c] Department of Computer Science, University of Engineering and Technology Peshawar, Peshawar 25000, Pakistan

[d] Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia

[e] IBSS, Xi'an Jiaotong-Liverpool University, Suzhou, China

[f] Center for Computer Technology & Networking Studies, Faculty of Computer & Mathematical Sciences,Universiti Teknologi MARA (UiTM), 40450 Shah Alam, Malaysia

ARTICLE INFO

Keywords:
Cloud computing
Cache-based Side channel attacks
Cross-VM Cache-based side channel attacks
Countermeasures

ABSTRACT

The state-of-the-art Cloud Computing (CC) has been commercially popular for shared resources of third party applications. A cloud platform enables to share resources among mutually distrusting CC clients and offers cost-effective, on-demand scaling. With the exponential growth of CC environment, vulnerabilities and their corresponding exploitation of the prevailing cloud resources may potentially increase. Although CC provides numerous benefits to the cloud computing tenant. However, features namely resource sharing and Virtual Machine (VM) physical co-residency raising the potential for sensitive information leakages such as Side Channel (SC) attacks. In particular, the physical co-residency feature allows attackers to communicate with another VM on the same physical machine and leak the confidential information due to inadequate logical isolation. Unlike encryption, which protects information from being decoded by unauthorized persons, SC attacks aim to exploit the encryption systems and to hide the occurrence of communication. SC attacks were initially identified as the main threat on multi-level secure systems i.e. OS, database, and networks. More recently, the focus of the researchers has shifted toward SC attacks in CC. Since the last level cache (L2 or L3) is always shared between VM, is the most targeting device for these attacks. Therefore, the aim of this article is to explore cross-VM SC attacks involving the CPU cache and their countermeasures in CC and to compare with the traditional SC attacks and countermeasures. We categorized the SC attacks according to the hardware medium they target and exploit, the ways they access the module and the method they use to extract confidential information. We identified that traditional prevention mechanisms for SC attacks are not appropriate for prevention of cross-VM cache-based SC attacks. We also proposed countermeasures for the prevention of these attacks in order to improve security in CC.