A User-Mode-Kernel-Mode Co-operative Architecture for Trustable Computing

Wenbo Mao

EMC Research China
Mao_Wenbo@emc.com

Abstract. The Trusted Computing Group's technology takes a load-time code measurement approach to compute platform security, in which a code in a more privileged layer of the software stack is supposed to be able to maintain the correctness for one in a less privileged layer. In this work we first report evidences that this load-time code measurement method is insufficient for maintaining the software execution correctness. We propose a user-mode-kernel-mode co-operative architecture for trustable computing in which a secure application in user mode works in co-operation with the privileged system management software in kernel mode. We argue for the necessity of co-operation between a secure application and the secure service code in kernel mode, and showcase the practicality of this method.

S. Qing, C.J. Mitchell, and G. Wang (Eds.): ICICS 2009, LNCS 5927, p. 2, 2009.