Virtualization for Diversified Tamper-Resistance[1]

Bertrand Anckaert*[2],
Mariusz Jakubowski†[2],
Ramarathnam Venkatesan†[2],

* *ELIS, Ghent University, Sint-Pietersnieuwstraat 41, 9000 Gent, Belgium*
† *Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA*

ABSTRACT

Despite huge efforts by software providers, software protection mechanisms are still broken on a regular basis. Due to the current distribution model, an attack against one copy of the software can be reused against any copy of the software. Diversity is an important tool to overcome this problem. It allows for renewable defenses in space, by giving every user a different copy, and renewable defenses in time when combined with tailored updates. This paper studies the possibilities and limitations of using virtualization to open a new set of opportunities to make diverse copies of a piece of software. The performance impact is considerable and indicates that these techniques are best avoided in performance-critical parts of the code.

KEYWORDS: Software Protection; Intellectual Property

1 Introduction

The value contained in and protected by software is huge. According to the Business Software Alliance and the International Data Corporation, $31 billion worth of software was installed illegally in 2004. Digital containers are increasingly used to provide controlled access to copyrighted materials. The value of virtual characters and assets in massively multiplayer on-line games is becoming more and more real. For example, a virtual space resort in the game Entropia Universe sold for the equivalent of $100,000[3]. It is clear that the stakes in protecting software from tampering are rising, be it to protect copyrighted software or content or to prevent players from cheating.

When the incentive to tamper is that high, we should no longer expect to build one super-strong defense that will withstand attack for an extended period of time. Even hardware solutions are not safe. Research in software diversity is an assent that software protection

[1]This is a summary of the paper "Proteus: Virtualization for Diversified Tamper-Resistance" at ACM DRM'06
[2]E-mail: Bertrand.Anckaert@UGent.be,[mariuszj,venkie]@microsoft.com
[3]http://news.bbc.co.uk/1/hi/technology/4953620.stm