**NET5039**

**BOYER CAROLE**
**TRÉCHEREL DIDIER**

## SUBJECT: VIRTUAL MACHINES ESCAPE

**Abstract** — Virtualization is not a recent invention, it's the result of decades of computer researches meeting different demands throughout history. Nowadays, virtualization plays a more and more important role in the world of computing and became a dazzling solution for companies. As a matter of fact, the ability to share the resources of a single physical machine (called *host*) between several isolated virtual machines (called *guests*) allows organizations to both create flexible and cost effective IT infrastructures, and reduce the space needed. Indeed, they avoid wasting unused hardware resources by sharing them between virtual machines. Moreover, it enables an easier management and migration of the computing systems. The system is also more secure by the fact that one can easily restore a compromised VM to a previous state, using the snapshot capability.

However, the rapid improvements made in virtualization come along with new security risks. An attacker who succeeds in escaping from its restrictive environment and in reaching the host machine would be able to both control and cause major damage to the whole system. In our paper, we first spell out virtualization, with its assets and flaws. The definition of a *hypervisor* is also given and the different categories (type 1 and 2) are described. As the isolation is not perfect, we explain how an attacker could know whether his system is virtualized, and how he can identify the used hypervisor.

As it is possible to know whether a system is in a virtual environment, we present different types of attacks that can be performed on virtualized systems, and the vulnerabilities exploited to perform these attacks. Two types of attacks are examined and explained: the *denial of service* which can cause big losses to an enterprise, and finally *virtual machine escape*, which is the most dangerous threat today.

Finally we show different solutions to achieve virtualization security. As the hypervisor represents the main threat to virtualization, the first one is to use a secure hypervisor. We first introduce three secure hypervisors: TERRA, SHYPE and VAX VMM. Although VAX VMM and SHYPE are the more secure, using MAC — VAX VMM has been given the top-level A1 security rating by the NCSC —, TERRA is much more flexible. The second solution is to enhance the security of an hypervisor: HYPERWALL allows to secure the memory of each virtual machine, and HYPERSAVE avoids the introduction of malicious code inside the hypervisor, thus, enhances the isolation. These solutions can be implemented to enforce the isolation, and to prevent virtual machines escape.