Your Connection to ICT Research

Security and Virtualisation

Syed Naqvi, PhD
syed.naqvi@cetic.be

BIC Workshop on Technical Themes in Trustworthy ICT, 22 June 2012, Brussels

cetic
Your Connection to ICT Research

Introduction

- Virtualisation
  - Abstraction of resources (computing, storage, networks, …)
  - Hides physical characteristics from users/applications
  - Ratio of physical and virtual resources is not 1:1

- Security
  - Tangible assets
  - Audit requirements
  - Compliance issues – physical security
  - Data export control
  - Chain of command, ownership and responsibility
  - Proof of trust and reliability

Security added values

- Sandboxing & isolation
  - Virtual machines as sandbox limit the attacks
- Abstraction – Fine grained access modes
  - User mode, kernel, mode, …
- Quick recovery (BCP/DRP)
  - Clean images
- Better security management
  - Patches, costs, privileges, …

Vulnerability Note VU#649219

SYSRET 64-bit operating system privilege escalation vulnerability on Intel CPU hardware

Original Release date: 12 juin 2012 | Last revised: 18 juin 2012

Print Tweet Send Share

Overview

Some 64-bit operating systems and virtualization software running on Intel CPU hardware are vulnerable to a local privilege escalation attack. The vulnerability may be exploited for local privilege escalation or a guest-to-host virtual machine escape.

Intel claims that this vulnerability is a software implementation issue, as their processors are functioning as per their documented specifications. However, software that does not take the unsafe SYSRET behavior specific to Intel processors into account may be vulnerable.

Description

A ring3 attacker may be able to specifically craft a stack frame to be executed by ring0 (kernel) after a general protection exception (#GP). The fault will be handled before the stack switch, which means the exception handler will be run at ring0 with an attacker's chosen RSP causing a privilege escalation.

Security Challenges (1/2)

- Security audit
  - Unit auditing (hardware, software, etc.)
  - For example, PCI DSS compliance audit
  - Data protection issues

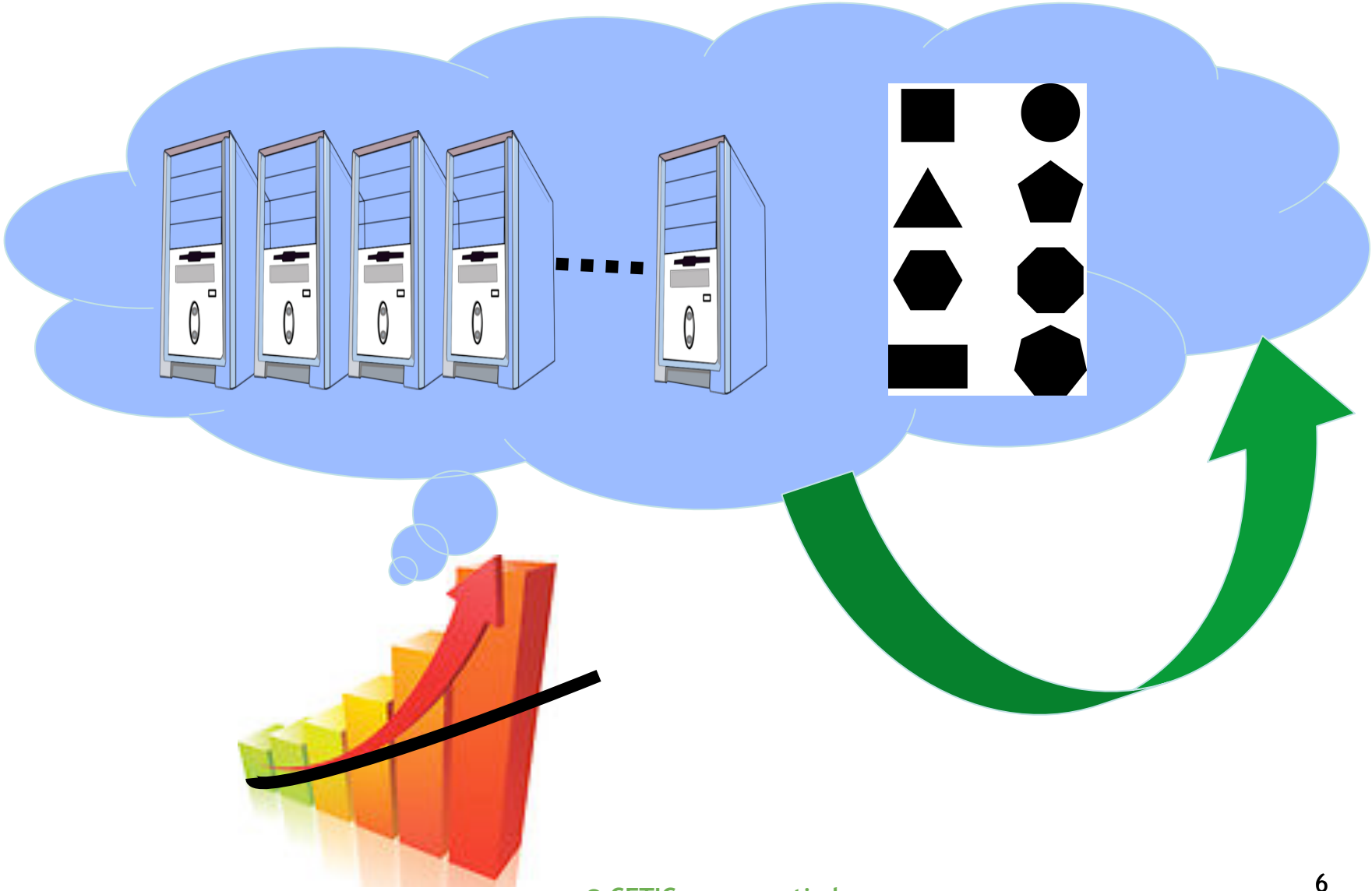
- Virtualisation infrastructures (such as Clouds) have no 'forensic friendly' design characteristics.
  - Right now individual PCs connected to a Cloud are investigated for the forensics purposes
  - Complete externalisation of software artefacts (from the operating systems to the applications) will not provide any meaningful information to the investigators.
    - Cloud PC (e.g. Wyse Technology's X00m Cloud PC)

Security Challenges (2/2)

- Virtualisation promises more flexibility and less costs
  - Impact of security controls and compliance constraints
  - Reduced **attractiveness** of virtualisation infrastructures if security requirements take their toll on flexibility & cost effectiveness
  - Trust on the outsourcing of security functions

- Root of trust
  - Ideal location of root of trust
  - Scope of TCP (Trusted Computing Platform)
  - Escrow / transfer of trust

BonFIRE Security Experiment



Your Connection to ICT Research

Thank you

SYED NAQVI, PHD

R&D Project Manager

Software & Services Technologies Dept.

syed.naqvi@cetic.be