



Gestão de Riscos em Ambientes Virtuais

Bruno Morisson, CISSP, CISA
Consultor Sénior de Segurança Informática



OUR SERVERS ARE USING TOO MUCH ELECTRICITY. WE NEED TO VIRTUALIZE.



www.dilbert.com scottadams@aol.com

I DID MY PART BY READING ABOUT VIRTUALIZATION IN A TRADE JOURNAL. NOW YOU DO THE SOFTWARE PART.



2-12-08 © 2008 Scott Adams, Inc./Dist. by UFS, Inc.

WHY IS YOUR PART TAKING SO LONG?



Mas o que é “virtualização”?

A broad term that refers to the abstraction of computer resources.

VMware, Xen, Hyper-V, Parallels, OpenVZ, Sun VirtualBox, IBM z/VM, ...

"Through 2009, 60% of production VMs will be less secure than their physical counterparts."

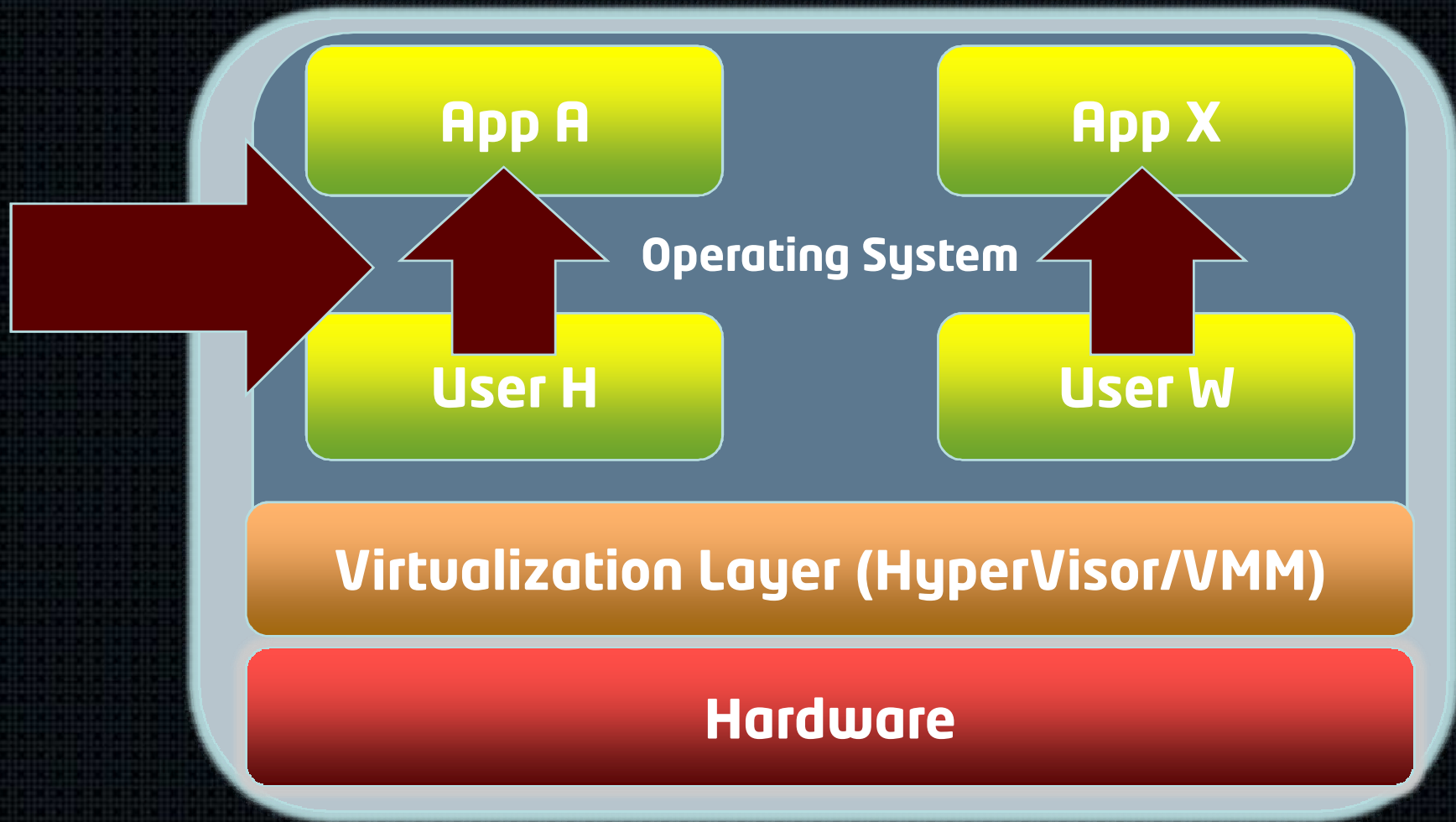
"Many organizations mistakenly assume that their approach for securing VMs will be the same as securing any operating system (OS)."

In *"Security Considerations and Best Practices for Securing Virtual Machines"*

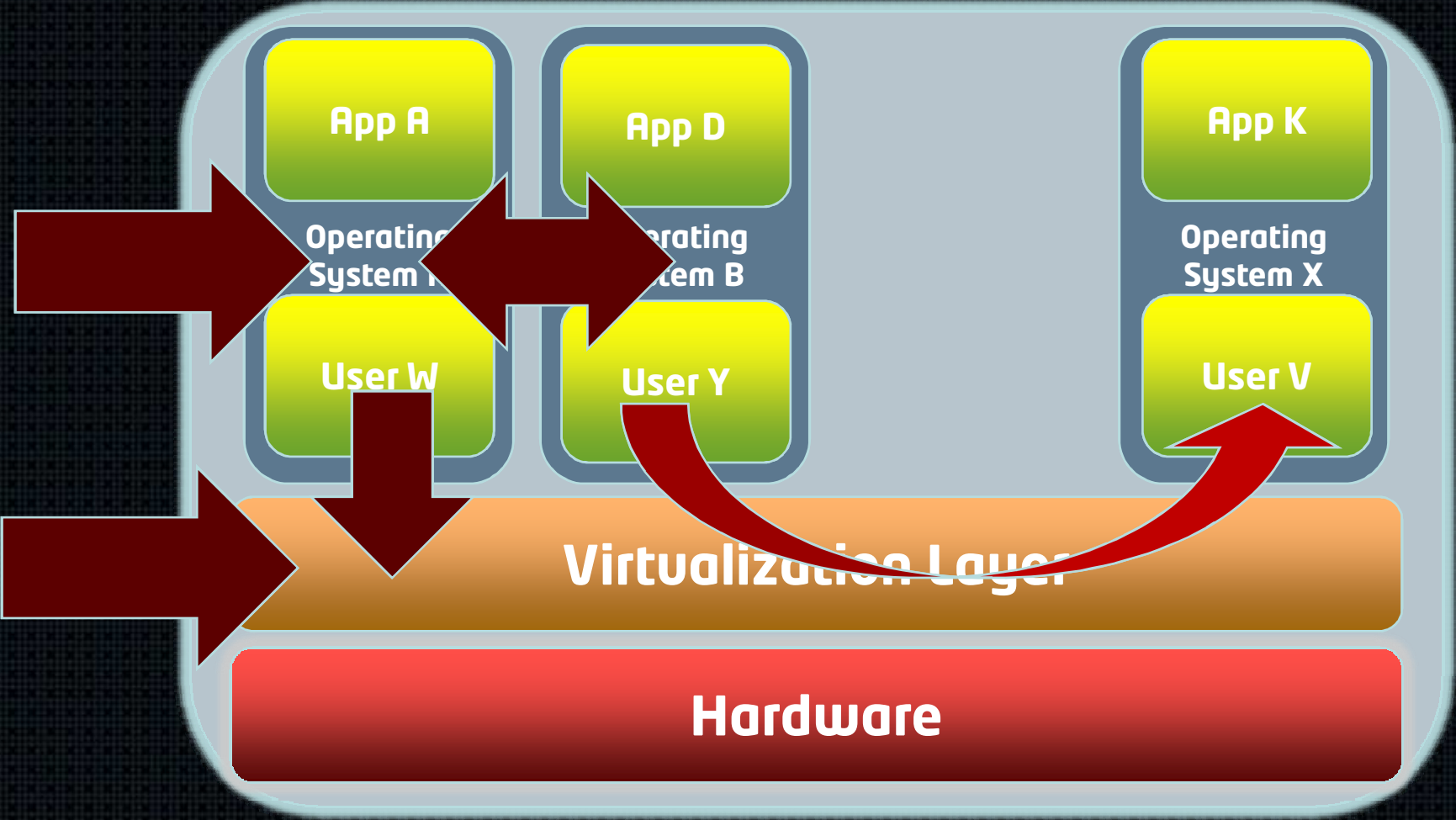
Gartner

Mas os riscos não são os mesmos ?

Threat Model tradicional



Novo Threat Model



Desafios Técnicos

Vulnerabilidades no HyperVisor

VM Escaping

Guest-to-Guest

Guest-to-Host

HyperVisor Rootkits

(in)Segurança do software de gestão

Desafios Técnicos - Caso #1

(2009-04-03)

Privilege Escalation Vulnerability

"A vulnerability in vmci.sys could allow privilege escalation on Windows-based machines. This could occur on Windows-based hosts or inside Windows-based guest operating systems."

Desafios Técnicos - Caso #2

(2009-04-10)

Host code execution Vulnerability

"A critical vulnerability in the virtual machine display function might allow a guest operating system to run code on the host."

Desafios Técnicos - Caso #3

(2009-06-14)

Lxlabs Kloxo Hosting Platform Multiple Security Vulnerabilities

"Lxlabs Kloxo Hosting is prone to multiple security vulnerabilities, including security-bypass, information-disclosure, cross-site scripting, SQL-injection, denial-of-service, command-injection, and insecure-file-creation issues.."

Desafios Administrativos

VM Sprawl

Rogue VMs

Unpatched VMs

Separation of Duties

Isolamento

Garantir Zonas de Segurança

Compliance

Mas podem haver vantagens ?

Claro que podem haver vantagens!

Disponibilidade

Isolamento

Desenvolvimento & Testes

Controlo Centralizado

Disaster Recovery

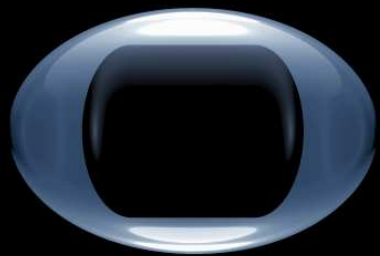
Análise Forense

Lembrem-se!

A Virtualização não é a panaceia!

Tornar uma infraestrutura virtual segura não é o mesmo que tornar uma infraestrutura física segura. Novas ameaças, novas vulnerabilidades, novos riscos.

Podemos tirar partido da Virtualização se for implementada depois de bem pensada.



onicommunications

youuniversal business solutions

www.onicommunications.pt