



Virtualização & *Sandboxing*

Riscos e Vantagens

Bruno Morisson, CISSP
Consultor Sénior de Segurança Informática



“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

Virtualização

“a broad term that refers to the abstraction of computer resources”

- Network Virtualization
- Storage Virtualization
- Operating System Virtualization
- Para-Virtualization
- Full Virtualization
- ...

Virtualização

Utilização de software que permite a partilha simultânea de recursos de *hardware* entre sistemas operativos independentes (VMware, Xen, Hyper-V, Parallels, Sun xVM, IBM z/VM, ...)

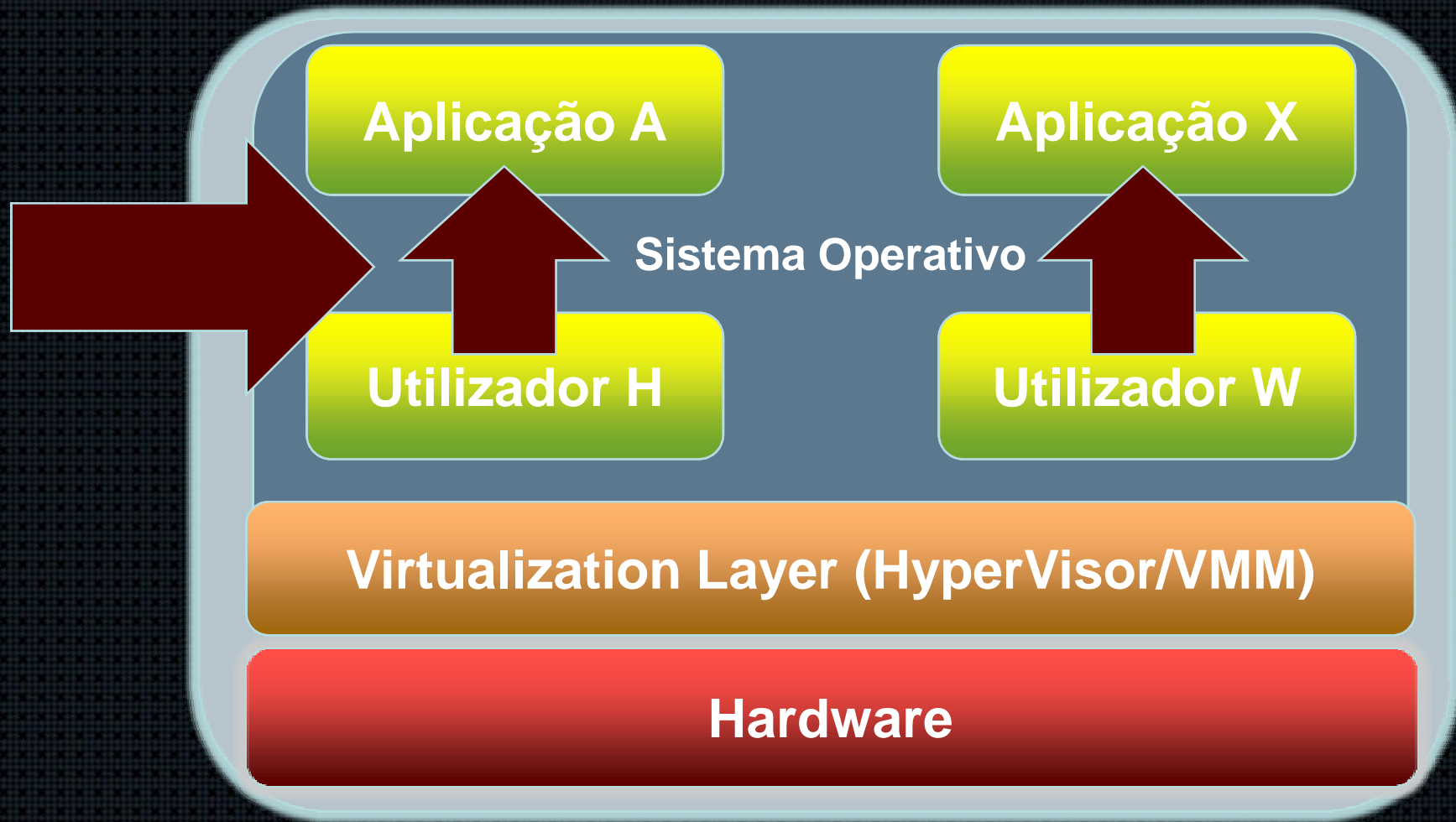
Virtualização & Segurança

Virtualização da Segurança

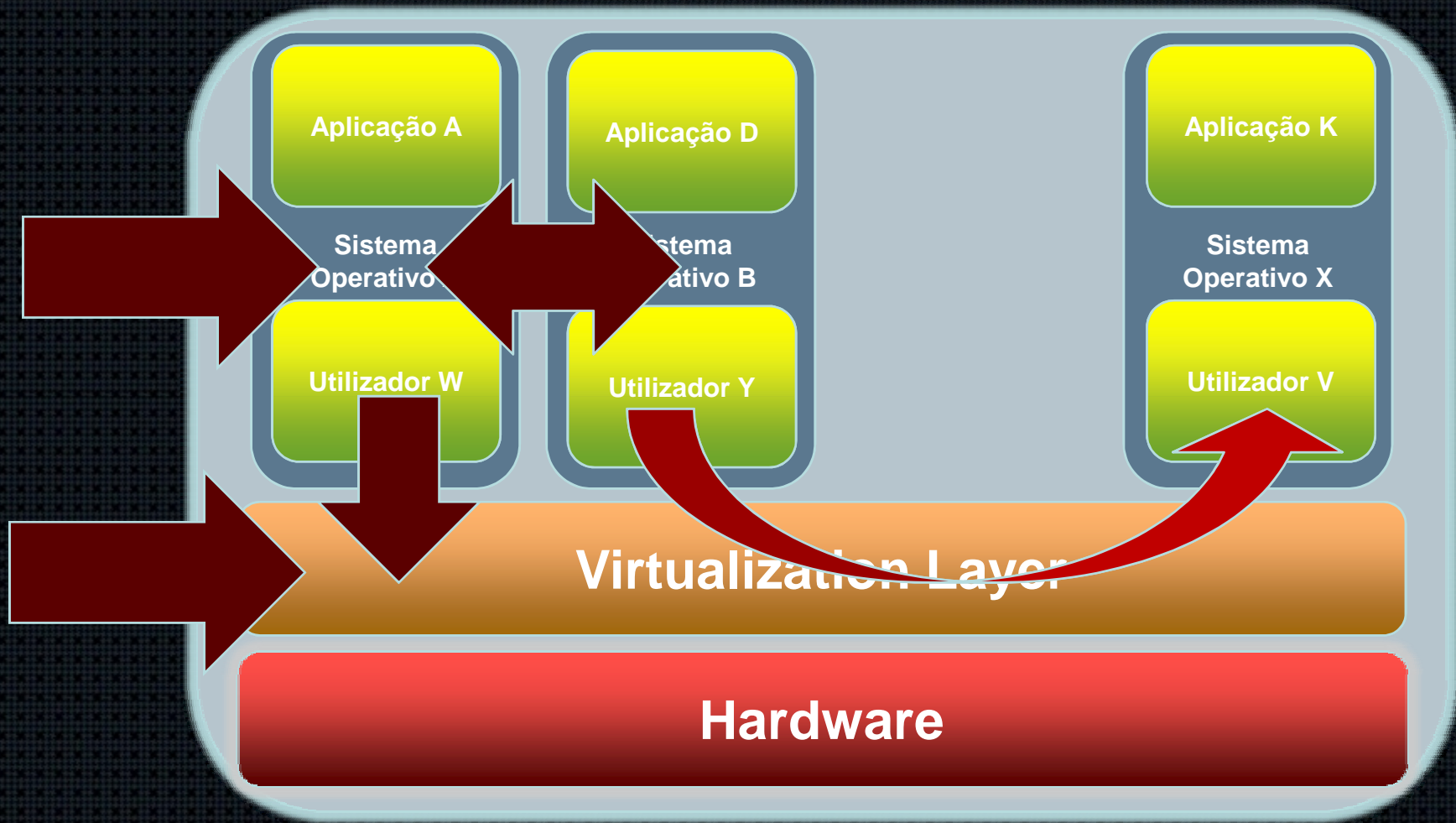
Segurança da Virtualização

Segurança via Virtualização

Modelo Tradicional



Novo Modelo



Alteração dos Riscos

Modelo Tradicional

- Ataques internos às Aplicações/SO
- Ataques externos às Aplicações/SO

Alteração dos Riscos

Virtualização

- Ataques Internos às Aplicações/SO
- Ataques Externos às Aplicações/SO
- Ataques entre Sistemas Virtuais
- Ataques Internos à VL
- Ataques via VL
- Ataques externos à VL
- Ataques da VL aos Sistemas Virtuais

Alteração dos Riscos

- Deixa de existir separação física;
- Gestão da Segurança feita de modo “transparente”;
- Separação de funções comprometida;
- Extremo poder do administrador da VL;
- *HyperVisors* maliciosos/subversão da VL;
- Garantias de Confidencialidade?
- Garantias de Integridade?
- *Compliance*?

Futuro

- Implementação de mecanismos que garantam CI nos *HyperVisors: Trusted HyperVisors* (ex: sHype);
- Mais funcionalidades suportadas directamente no hardware (ex: Intel TXT);
- Novas soluções para mitigar riscos associados à Virtualização.

Virtualização - Sandboxes

- Controlo granular reduzindo o acesso das aplicações a recursos do sistema:
 - “Firewall” entre as aplicações e o sistema
 - Permitir apenas escrever num determinado local do *filesystem*;
 - Apenas ler determinados ficheiros;
 - Não permitir ligações *outbound* à rede.

Sandboxes - Exemplos

- JavaVM
- ActiveX
- Jails/Chroot (Unix)
- TrustedBSD
- Seatbelt (Mac OSX)
- Sandboxie
- Systrace (Linux/BSD)
- SELinux/AppArmor/etc (Linux)
- Web Sandbox (MS Live Labs)
- Google Chrome

Vantagens – Virtualização & Sandboxes

- Disponibilidade;
- Isolamento de Aplicações e Utilizadores;
- Recuperação de Incidentes;
- Análise de Malware/Vírus;
- Utilização de aplicações inseguras;
- Análise Forense;

Conclusões

- A Virtualização não é a panaceia.
- Tornar uma infraestrutura virtual segura é diferente de tornar uma infraestrutura física segura. **Novas ameaças, novas vulnerabilidades, novos riscos.**
- Podemos tirar partido da Virtualização, se esta for implementada depois de bem pensada.



onicommunications

youuniversal business solutions

www.onicommunications.pt