Virtualisering
Billigare och Säkrare?

tobbe@romab.com
andreas@romab.com

“x86 virtualization is about basically placing another nearly full kernel, full of new bugs, on top of a nasty x86 architecture which barely has correct page protection. Then running your operating system on the other side of this brand new pile of shit. You are absolutely deluded, if not stupid, if you think that a worldwide collection of software engineers who can't write operating systems or applications without security holes, can then turn around and suddenly write virtualization layers without security holes.”

“x86 virtualization is about basically placing another nearly full kernel, full of new bugs, on top of a nasty x86 architecture which barely has correct page protection. Then running your operating system on the other side of this brand new pile of shit. You are absolutely deluded, if not stupid, if you think that a worldwide collection of software engineers who can't write operating systems or applications without security holes, can then turn around and suddenly write virtualization layers without security holes.”

- Theo de Raadt

Eftersökes: Betrodd Hypervisor

Agenda

- Generella problem
- VM-specifika problem
  - VMware
  - XEN
  - Andra hypervisors
- Jails/zones
- Trender

Generella Problem

- Behörighetsdeligering
- Informationssäkerhet
- Systemintegritet
- Systemtillgänglighet
- Prestanda
- Ekonomi

Agenda

- Generella problem
- VM-specifika problem
  - VMware
  - XEN
  - Andra hypervisors
- Jails/zones
- Trender

Fördelar

- Enkelt att testa
- Enkelt att duplicera/klona/rulla tillbaka
- Isolation av tjänster
- Bättre tillgänglighet
- Enklare att leva upp till SLA
- Enklare att äska nedtid
- Enkelt att skapa nya maskiner
- Högre hw-utilization

VM problem

- Större TCB
- Single point of failure
- VM Sprawl
- Underhåll av dom0
- Ansvar för dom0
- Tid är en delad resurs

VM problem

- Ansvar för säkerhet flyttas till systemägare
  - Vem kommer att äga problemet?
- Kompromettерade guesthostar
- Hypervisorbuggar
  - Hypervisor rootkits
  - VMEscapes
  - DOS
- Biosbuggar vanligare (VT-X, VT-D|iommu)

VM problem

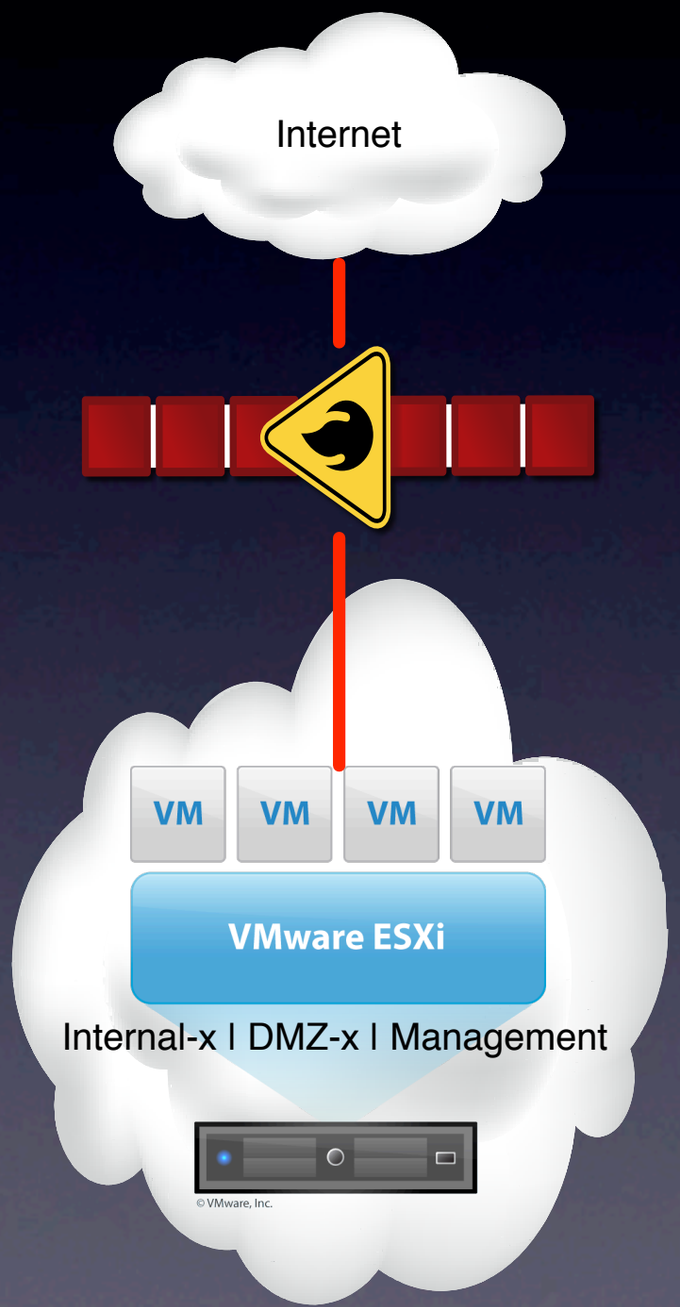
- Varför virtualisering
  - För konsolidering?
  - För separering?
  - kostnad ekonomi/energi Grön IT?
- Lätt att bli blasé över vikten av virtuella hostar

VM problem

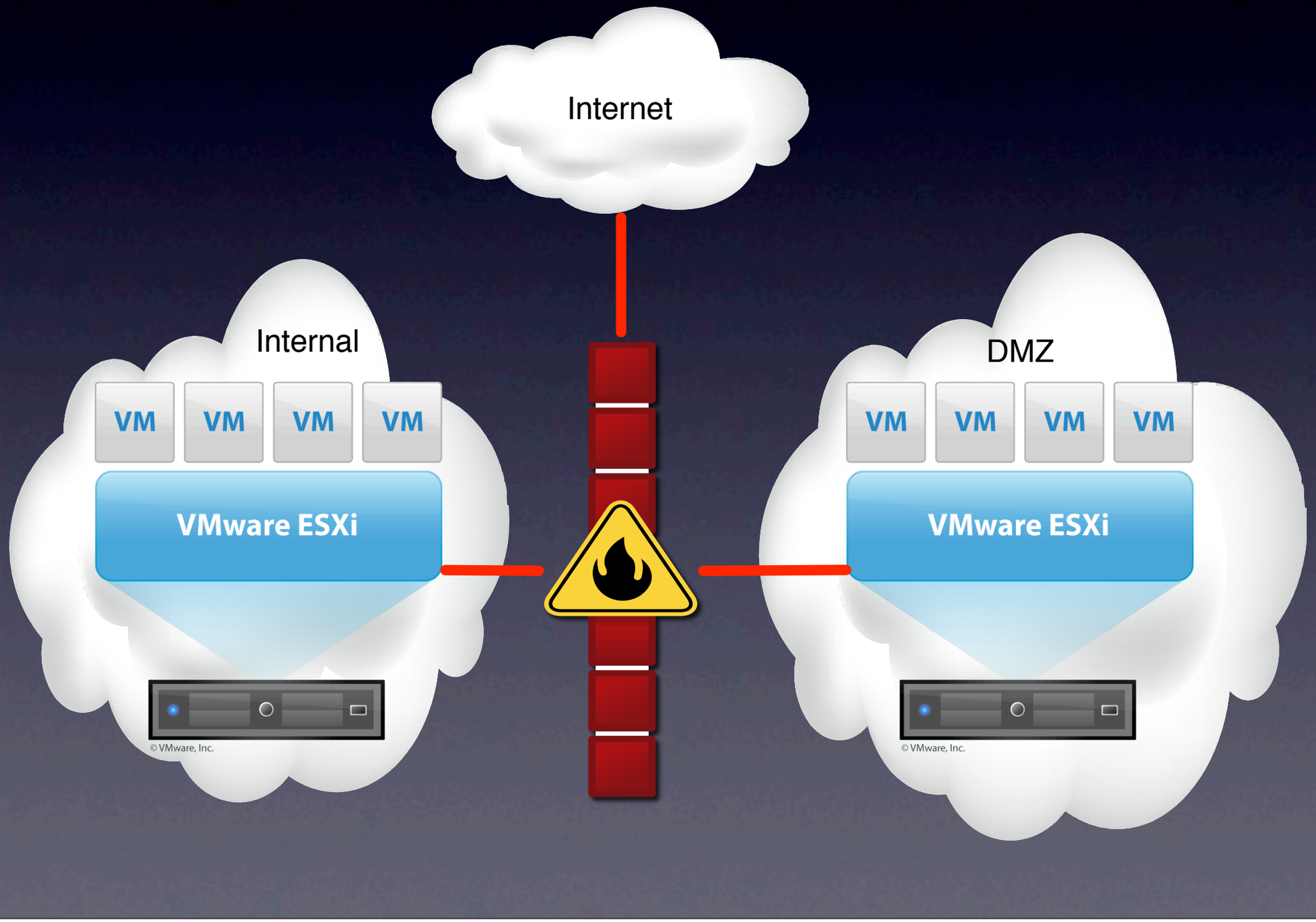
- Anses ofta vara lösningen på behörgihetsproblematik i OS.
  - Skapa ny vm, ge bort root/admin
  - Om något går sönder, återställ backup/snap

- Skapar en felaktig bild av problemet då sysadms först kommer logga in för att se om de kan lösa problemet
  - ger bort kerberostokens, eller annan behörighetsinformation

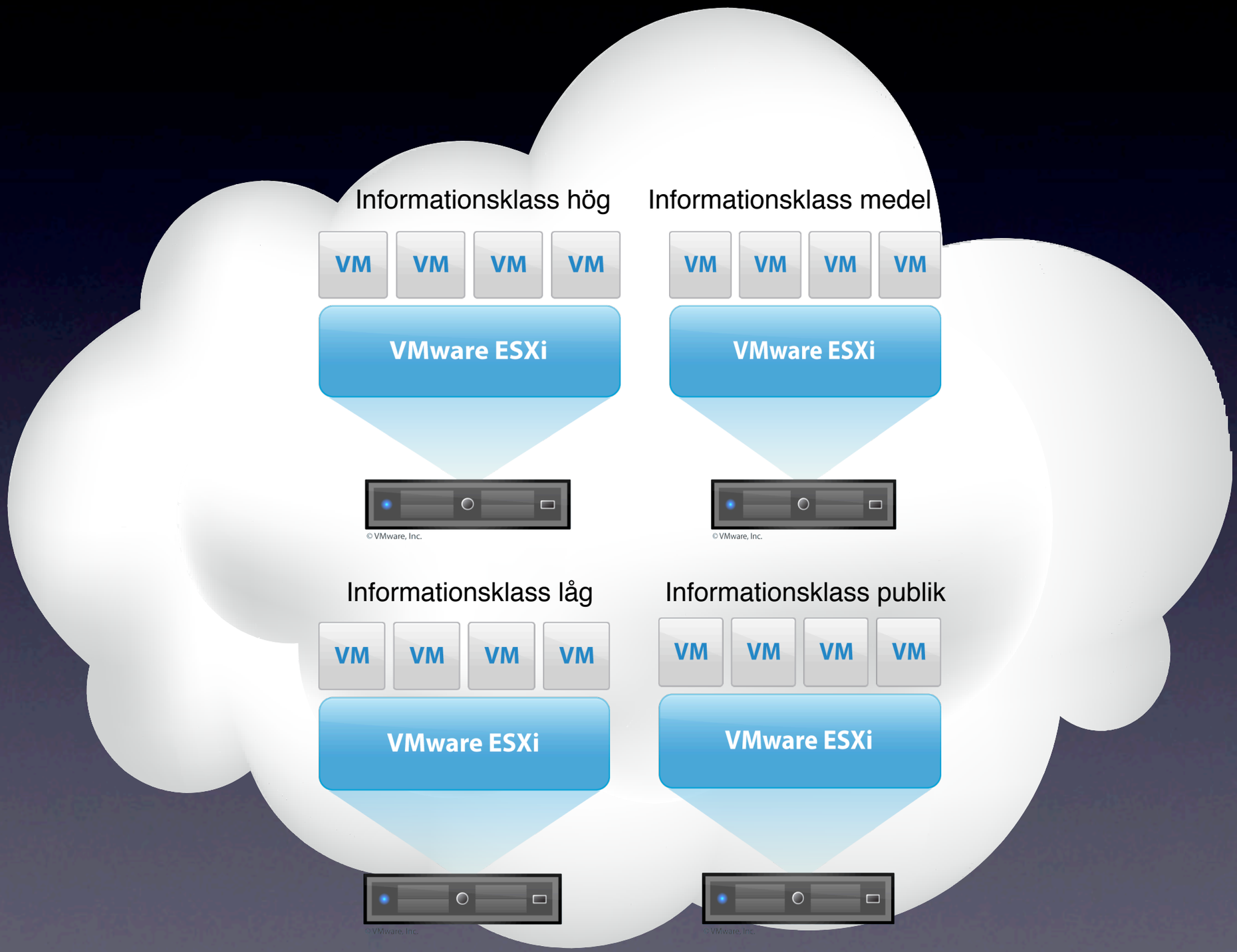
Nätverk


Internet
VM
VM
VM
VM
VMware ESXi
Internal-x I DMZ-x I Management
© VMware, Inc.

Nätverk


Internet
Internal
VM
VM
VM
VM
VMware ESXi
© VMware, Inc.
DMZ
VM
VM
VM
VM
VMware ESXi
© VMware, Inc.

Nätverk


Informationsklass hög
VM
VM
VM
VM
VMware ESXi
© VMware, Inc.
Informationsklass medel
VM
VM
VM
VM
VMware ESXi
© VMware, Inc.
Informationsklass låg
VM
VM
VM
VM
VMware ESXi
© VMware, Inc.
Informationsklass publik
VM
VM
VM
VM
VMware ESXi
© VMware, Inc.

Agenda

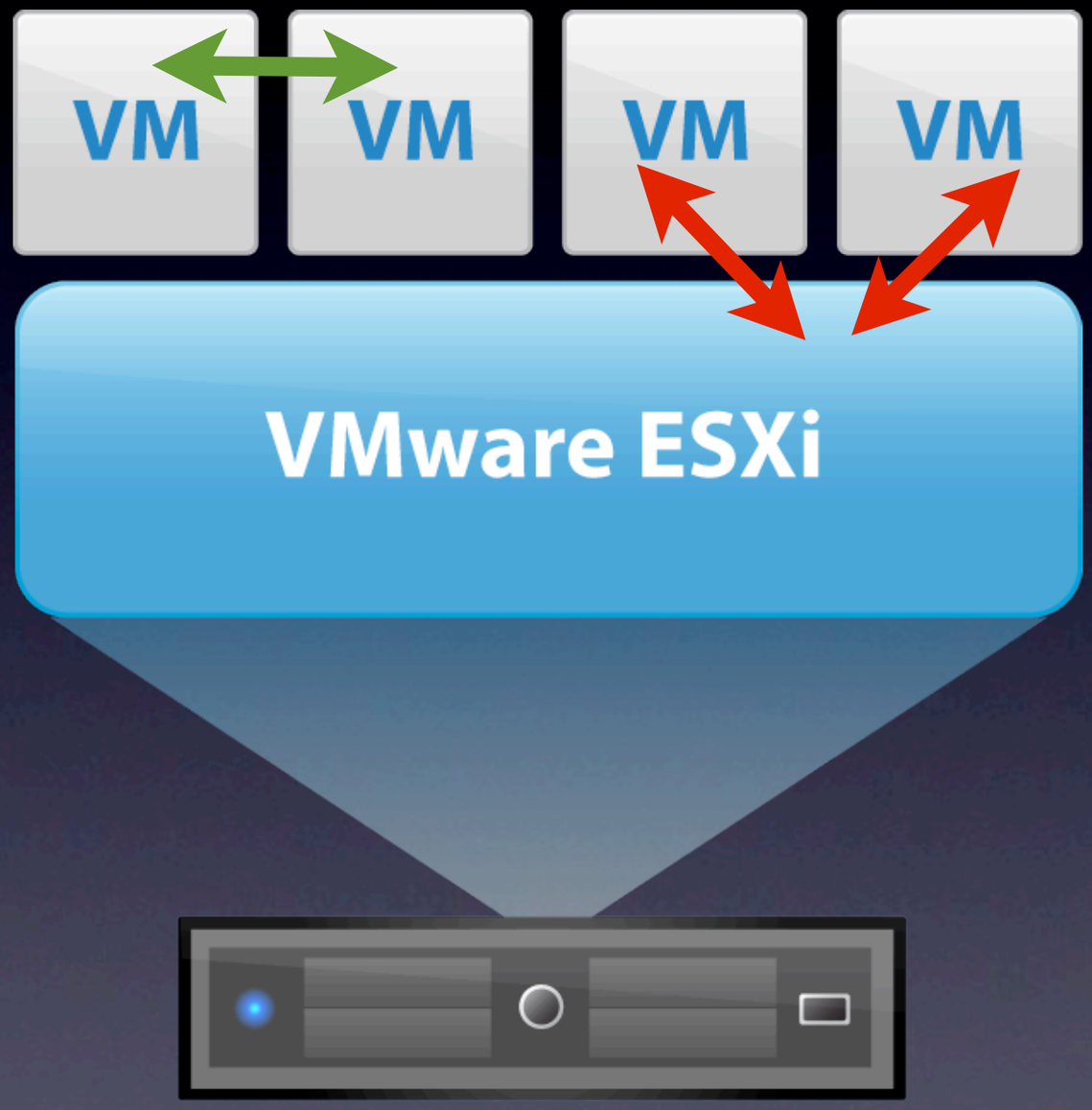
- Generella problem
- VM-specifika problem
  - VMware
  - XEN
  - Andra hypervisors
- Jails/zones
- Trender

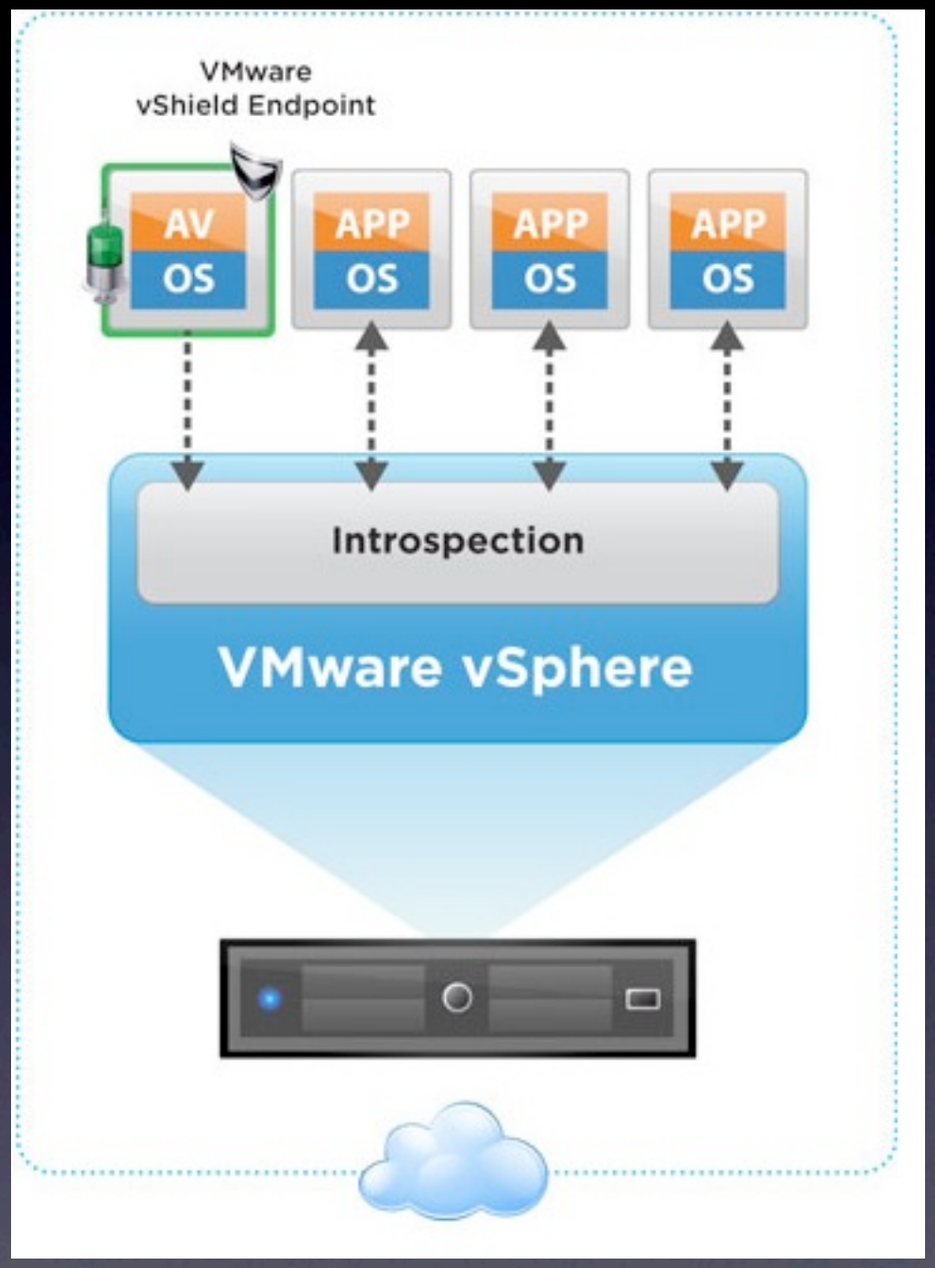
VMWare

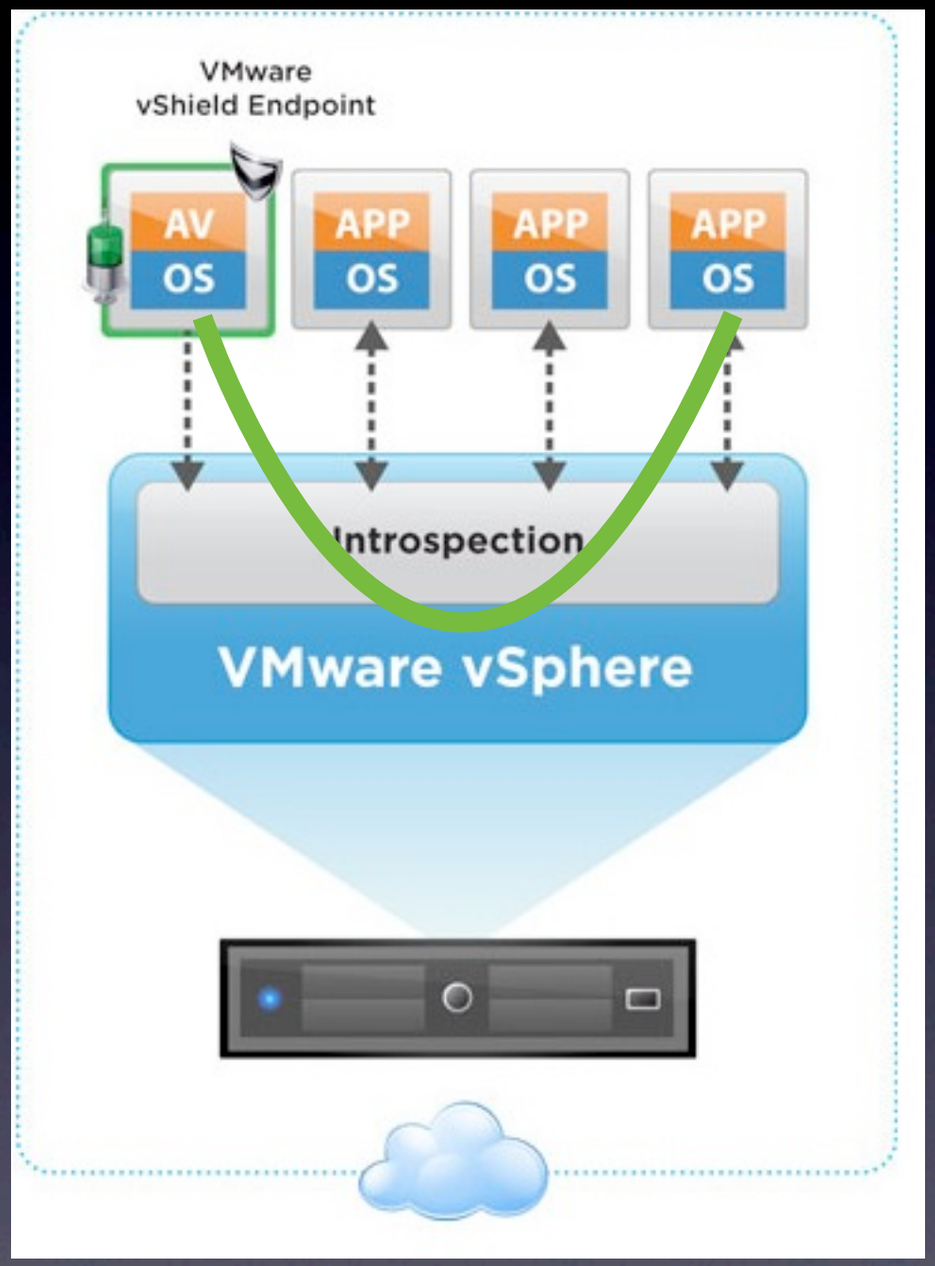
- Störst
- Har haft en del större buggar
- Kommer oftast in för att reducera mängden windowsmaskiner
- Börjar få “cloudbaserade” lösningar
  - VShield EDGE
  - VShield Endpoint

vSphere

- VMwares produkt för att administrera VM
- Finns i flera olika prismodeller beroende på funktionalitet
- Gratis alternativet är ett WebGUI




VMware
vShield Endpoint
AV
OS
APP
OS
APP
OS
APP
OS
Introspection
VMware vSphere


VMware
vShield Endpoint
AV
OS
APP
OS
APP
OS
APP
OS
Introspection
VMware vSphere

Vshield Endpoint

- Flyttar virusscanning till en härdad virtuell maskin
- Gör detta genom en driver i guest os:et som hookar open()-calls
- hur fungerar konceptet månadsscan?
- Vad händer om den virtuella aw-maskinen inte orkar pga att en virtuell maskin har intensiv IO? SPOF?

VMEscape

- Samlingsnamn på att bryta sig ur en guest
- 18 sårbarheter de senaste 3 åren i ESX
- Ex, Cloudburst
  - Dök upp i immunity CANVAS 2009
  - Bröt sig ur en gäst via SVGA2 drivern
  - Detta genom att skriva till rektanglar utanför framebuffern
- Demo

Vem äger VMWare i organisationen?

- Oftast Windowsgruppen
- Oftast ingen koll på unix
  - VMware service console
- Oftast samma problem som uppstår när ingen "äger problemet"

Hur används VMware

- Bara en “admin-användare”
  - Annars uppstår problem med ägarskap av filer
  - Ingen spårbarhet
- Ingen integration med övriga behörighetssystem (krb5/AD/etc)
  - Lösenord byts manuellt at best.

Agenda

- Generella problem
- VM-specifika problem
  - VMware
  - XEN
  - Andra hypervisors
- Jails/zones
- Trender

XEN

- Vanligt bland opensource OS
- Har massvis med kommersiella implementationer
  - Citrix XenServer
  - Oracle VM
  - SunXVM (Oracle)
  - VirtualIron (Oracle, underhålls inte)
  - Rhel5

XEN

- Designat för seperation mellan VM
  - Och precis som alla andra VM:s, inte för säkerhet
- Har haft 29 sårbarheter de senaster 3 åren
- ~230K SLOC

XEN

- Favvohypervisor hos många
- Första stora OpenSource virtualiseringskerneln
  - Första versionen utvecklades på Cambridge
- Var standard i RHEL5, FC6-11
  - Blev senare petad som till förmån av KVM

XEN

- Var skyddat av SeLinux under fedora och RHEL5
- Ex sårbarhet RHSA-2008-0194
  - Även här är det framebuffern som utnyttjas för vm-breakout
- Kompromiss över användbarhet resulterade i att xen fick läsa diskar öht, istället för diskar med xen_image_t label
- invisiblethings labs lyckades ladda in kernelmoduler genom skriva till rådevice

XenServer(citrix)

- Är idag en Enterprise produkt

Free	Advance	Enterprise	Platinum
Live Migration	HA	RBAC	Site recovery
Snapshot	Performance alerting and reporting	Automated workload balancing	Lifecycle management

Agenda

- Generella problem
- VM-specifika problem
  - VMware
  - XEN
  - Andra hypervisors
- Jails/zones
- Trender

Qubes

- Desktop-virtualisering för en secure desktop
- XEN-baserad
- Alla appar kör i varsinn VM eller VM efter syfte

1 - Open...

work: - Mozilla Thunderbird

random: Mozilla Firefox

personal: Mozilla Firefox

bank: Mozilla Firefox

shopping: Mozilla Firefox

work: Untitled 1 - OpenOffice.org Cal

Enter Master Key

vault: /rw/home/user/jo...

Thursday, October 14, 2010

CONFIDENTIAL : RESTRICTED

Trust No One.sxw - StarOffice 7

File Edit View Insert Format Tools Window Help

/export/home/sb73685/Documents/Trust No On

Default Thorndale 22 B I U

This is some text in a Star
Document that is classifie
Restricted

CONFIDENTIAL : INTERNAL USE ONLY

Untitled 1 (modified) - gedit

Tools Documents Help

Print Undo Redo Cut Copy Paste Find Replace

Trusted Path

Selection Manager

Transfer not authorised.
You are not authorised to downgrade this information

Orignal Information
CNF : RESTRICTED
Type: UTF8_STRING
Owner: sb

New Information
CNF : INTERNAL USE ONLY
Type: UTF8_STRING (93 bytes)
Owner: sb

Selection View as: Text

This is some text in a StarOffice Writer Document that is classified Confidential: Restricted

Time remaining to complete: 1:41

Help Cancel OK

HyperSafe

- Liten hypervisor vars mål är att skyda hypervisorn
- ~8700 SLOC
- Stödjer i sin tur två hypervisors, bitvisor och XEN
- Tillhandahåller hypervisor controlflow-integritet.
- TPM garanterar vad som laddas, inte vad som körs

HyperSafe

- Använder två tekniker för att skydda sig
- Non-Bypassable Memory Lockdown
  - Sätter W^X på minnessidor
- Restritcted Pointer Indexing

SecVisor

- Liten hypervisor vars mål är att skydda guestkerneln
  - stödjer bara UP
  - stödjer bara linux
  - Virtualiserar MMU och minne till hosten för att kunna gör kontrollcheckar.
- Extremt dyr att använda prestandamässigt
- Skyddar inte mot alla attacker (return-to-libc)

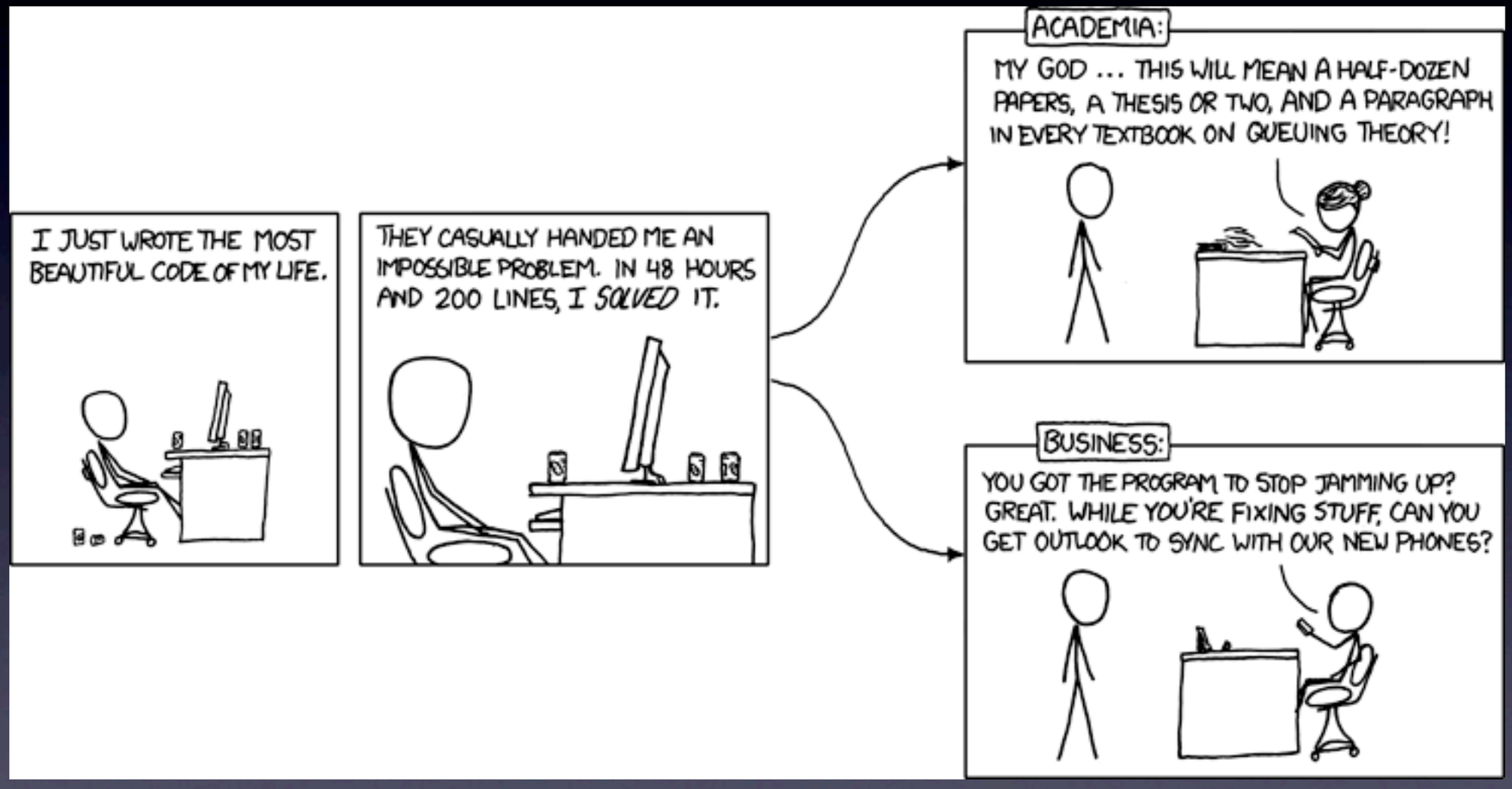
SecVisor

- Liten (~1700 SLOC, eftersträvar formell verifiering)
- 2.6.20 krävde 10 rader extra kod för att köra över secvisor.
- allt kernelminne är W^X
- hypervisorn verifierar att minnet är ok före den exekverar (polymorfiska kernels funkar ej)
- Visar det sig att minnet inte är ok krashar den virtuella maskinen

SLOC

- XEN ~230K
- HyperSafe ~8,7K
- SecVisor ~ 1.7K
- Buggar per 1k SLOC efter tester (enl MS) 0,5

Qubes, HyperSafe, SecVisor



Agenda

- Generella problem
- VM-specifika problem
  - VMware
  - XEN
  - Andra hypervisors
- Jails/zones
- Trender

Alternativ

- Jails/zones
- Sandboxing
- KVM

- LPAR (IBM SystemP)
  - HMC för hwkontroll
- LDOM (oracle SF T-XXXX)
  - IOdomäner
  - Kontrolldomän/servicedomän

SELinux FC11

VM	VM-process-label	VM-image-label
VM1	system_u:system_r:svirt_t:s0:c0,c10	system_u:object_r:svirt_image_t:s0:c0,c10
VM2	system_u:system_r:svirt_t:s0:c101,c230	system_u:object_r:svirt_image_t:s0:c101,c230

MCS-labels sätts dynamiskt av libsvirt

Agenda

- Generella problem
- VM-specifika problem
  - VMware
  - XEN
  - Andra hypervisors
- Jails/zones
- Trender

Trender

- MOOOOLNET
- Hyra vm-infrastruktur
- Mer funktionalitet i vm-infrastrukturen
  - Praktiskt att kunna flytta både fw-regler och hostar
  - Nätverksvirtualisering
- Strunta i säkerhet, problemet är bara virtuellt ändå


F Exception(14) in world 9074:sfchd ip 0x41802bbff21e addr 0x10
ame=0x4100c1b97a78 ip=0x41802bbff21e cr2=0x10 cr3=0x41ab9000
r=0 rflags=0x10246 cr4=0x168
x=0x0 rbx=0xfffffff4 rcx=0x0
x=0x4100b9a326a7 rbp=0x4100c1b97b68 rsi=0x4100b9a32010
i=0x4100c1b97af8 r8=0xdc r9=0x417fec75c690
0=0x0 r11=0x1 r12=0x4100b9a32010
3=0x0 r14=0x4100b9801458 r15=0x417fec87d240
5246/hostd 1:4097/idle1 2:4098/idle2 *3:9074/sfchd
4100/idle4 5:5391/hostd 6:5248/hostd 7:4103/idle7
de starts at 0x41802b600000
4100c1b97b68:[0x41802bbff21e]smbios_get_64bit_cru_info+0xb1 stack: 0x4100c1b9
8
4100c1b97b78:[0x41802bbff342]cru_init_cru+0x11 stack: 0x466fc5c0
4100c1b97b98:[0x41802bbff4b9]cru_ioctl+0x110 stack: 0x4100c1b97da8
4100c1b97d18:[0x41802b994426]LinuxCharIoctl+0x241 stack: 0x4100c1b97eb8
4100c1b97d88:[0x41802b69a21f]VmkApiCharDevIoctl+0xe2 stack: 0x410000000000
4100c1b97e08:[0x41802b7f32ca]DevFSIoctl+0x3e9 stack: 0x4100c1b97ea8
4100c1b97e48:[0x41802b7df135]FSS_Ioctl+0x178 stack: 0x840018def5
4100c1b97eb8:[0x41802b750135]UserFile_PassthroughIoctl+0x44 stack: 0x4100c1b9
8
4100c1b97ef8:[0x41802b75b8ef]LinuxFileDesc_Ioctl+0x7e stack: 0xec1b97f28
4100c1b97f28:[0x41802b73bf5c]User_LinuxSyscallHandler+0xa3 stack: 0x0
K uptime: 0:00:01:15.237 TSC: 199918357432
Sbase (0x0) GSbase (0x466fdb90) kernelGSbase (0x0)
:00:00:02.824 cpu3:4302)Mod: 2877: Initialization for tpm_tis failed with -19.
tarting coredump to disk.
sing slot 1 of 1... 98766666666665432110 DiskDump Successful.
ebugger is listening on serial port ...
ress Escape to enter local debugger

Frågor?