

Protecting Confidential Data on Personal Computers with Storage Capsules

Kevin Borders, Eric Vander Weele, Billy Lau, and Atul Prakash





Problem: Malicious Software

- Computing becomes pervasive, so is malware
 - Over 23 million computers cleansed in 2008 [1]
- Consequences are severe:
 - Financial loss
 - Identity theft
 - Fraud

[1] Microsoft Security Intelligence Report Volume 5



Scenario

- Tasks that require confidentiality protection
 - Perform financial analysis of credit card expenditure
 - Writing journal containing controversial political beliefs
 - Writing business proposal

Microsoft Excel - Credit Card Account Information.xls

File Edit View Insert Format Tools Data Window Help Adobe PDF

Type a question for help

Arial 10 B I U

C5 fx

	A	B	C	D	E	F	G	H	I	J
1										
2	Account Number	1234-5678-9012-3456								
3	Login Name	KBorders01								
4	Password	secret								
5										
6	4/6/2009	(\$505.39)	CLICK-TO-PAY PAYMENT, THANK YOU	1						
7	4/9/2009	\$0.00	LATE PAYMENT - FEE NOT CHARGED	1						
8	3/12/2009	\$208.55	DTE ENERGY PAYMENT DETROIT MI	2						
9	3/14/2009	\$25.62	SPEEDWAY 05399 583 MICHIGAN CITY IN	2						
10	3/14/2009	\$25.74	CAFE BA-BA REEBA CHICAGO IL	2						
11	3/15/2009	\$43.63	VZWRLSS*APOCC VISN 800-922-0204 CA	2						
12	3/17/2009	\$21.54	JEWEL-OSCO 3443 CHICAGO IL	2						
13	3/19/2009	\$17.15	SPEEDWAY 07786 855 PAW PAW MI	2						
14	3/22/2009	\$18.73	KROGER #689 YPSILANTI MI	2						
15	3/22/2009	\$140.69	SAMS CLUB YPSILANTI MI	2						
16	3/24/2009	\$26.93	YPSILANTI FUEL STOPQ17 YPSILANTI MI	2						
17	3/26/2009	\$11.26	KROGER #605 ANN ARBOR MI	2						
18	4/4/2009	\$28.39	KROGER #689 YPSILANTI MI	2						
19	4/5/2009	\$27.11	MEIJER INC#227 Q01 WHITE LAKE MI	2						
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										
30										
31										

Credit Card Account Information

Ready NUM

TrueCrypt

Volumes System Keyfiles Tools Settings Help

Homepage

Drive	Volume	Size	Encryption algorithm	Type
M:				
N:				
O:				
P:				
Q:				
R:				
S:				
T:				
U:				
V:				
W:				
X:				
Y:				
Z:				

Enter password for C:\Documents and Settings\kborders\Desktop\acco...

Password:

OK

Cache passwords and keyfiles in memory

Display password

Use keyfiles

Keyfiles...

Cancel

Mount Options...

IS THIS SAFE ENOUGH?

Create Volume

Volume Properties...

Wipe Cache

Volume



C:\Documents and Settings\kborders\Desktop\accounts.tc

Select File...

Never save history

Volume Tools...

Select Device...

Mount

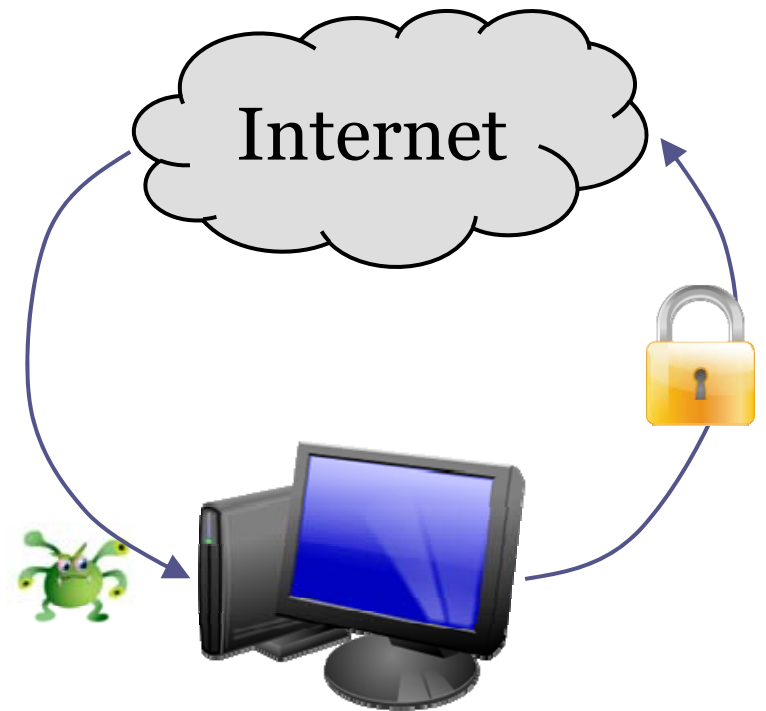
Auto-Mount Devices

Dismount All

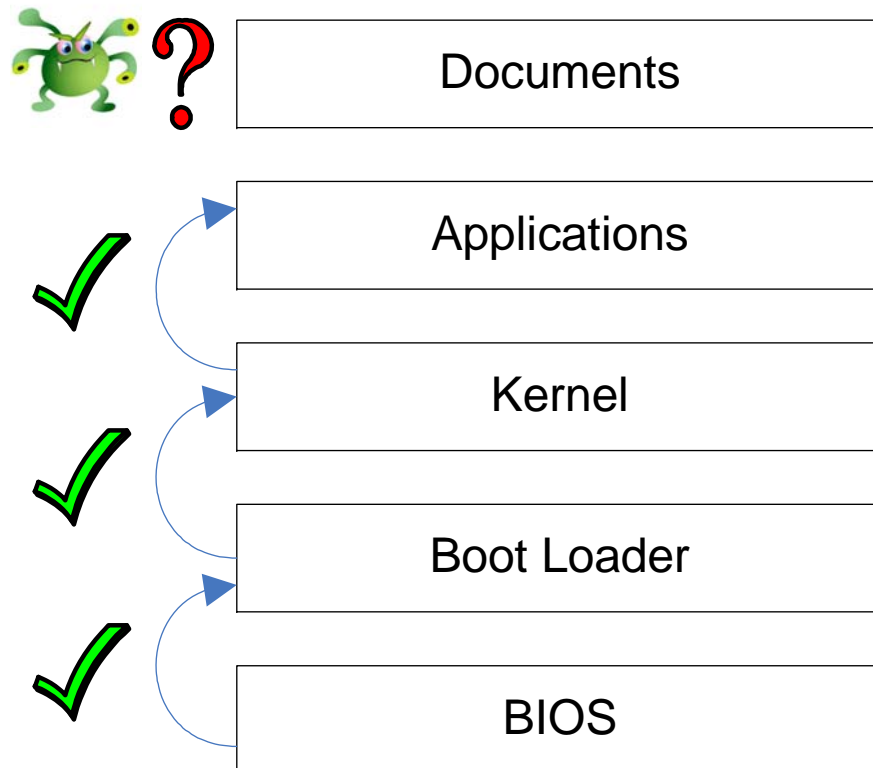
Exit

Goals

Provide confidentiality for local sensitive files against malicious software

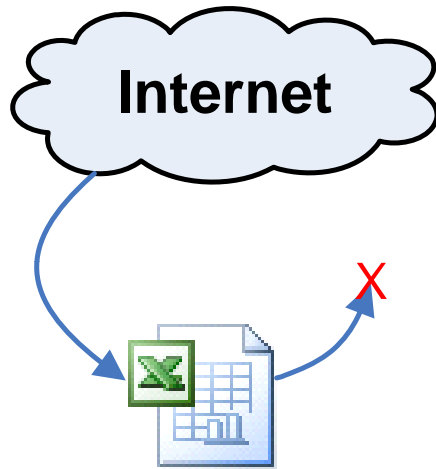


Related Work: Trusted Boot

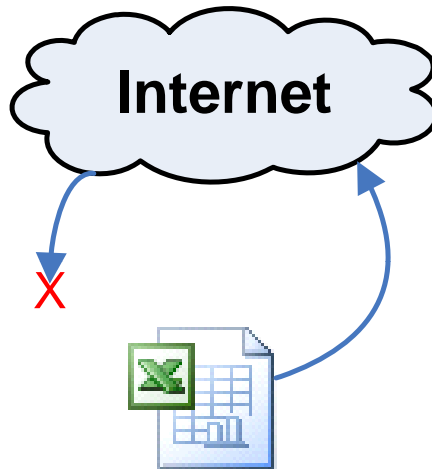


- Not 100% safe
- Need to verify all software prior to installation
 - Hard
- Verify documents
 - Even harder!!

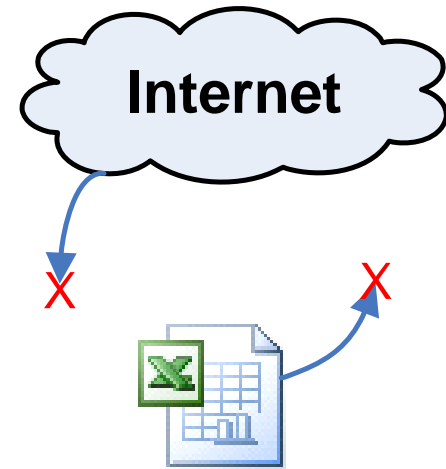
Related Work: Strict Inter-Process Flow Control



Mandatory Access
Control A



Mandatory Access
Control B



Air Gap

- Mandatory Access Control with strict control flow policy = **Limited Usability**
- Air gap greatly limits utility



Contribution - Storage Capsules

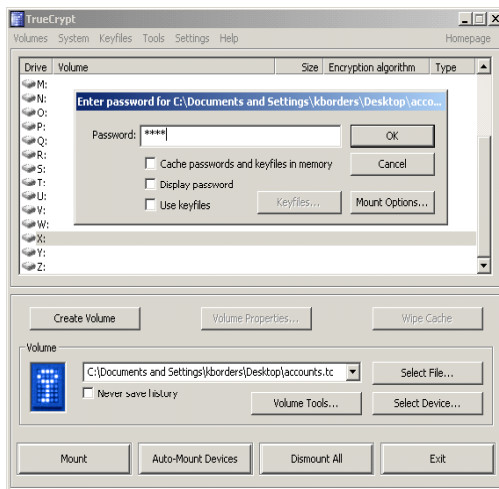
- A system that can securely access confidential information from a compromised commodity OS

Approach

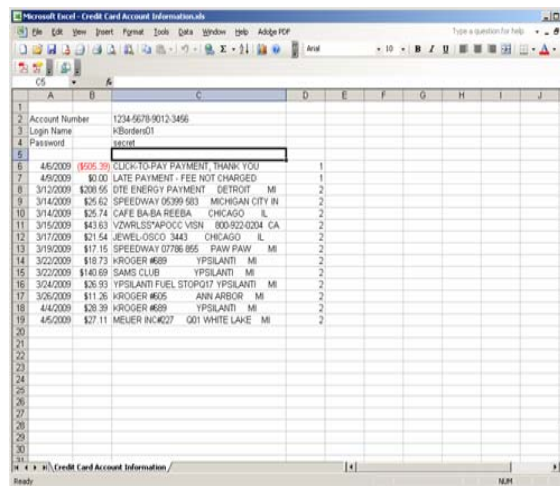
- Allow normal OS and standard applications to access sensitive data
- Two modes of operation:

Normal Mode	Secure Mode
• No restrictions	• Prevent network output
• Perform non-sensitive operations	• Edit sensitive documents
• No storage protection	• Encrypt changes to Storage Capsules

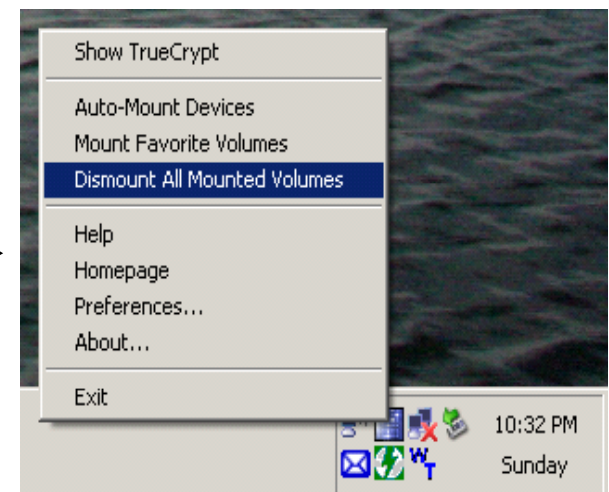
From the User's Perspective



1. Open Container



2. Edit Document

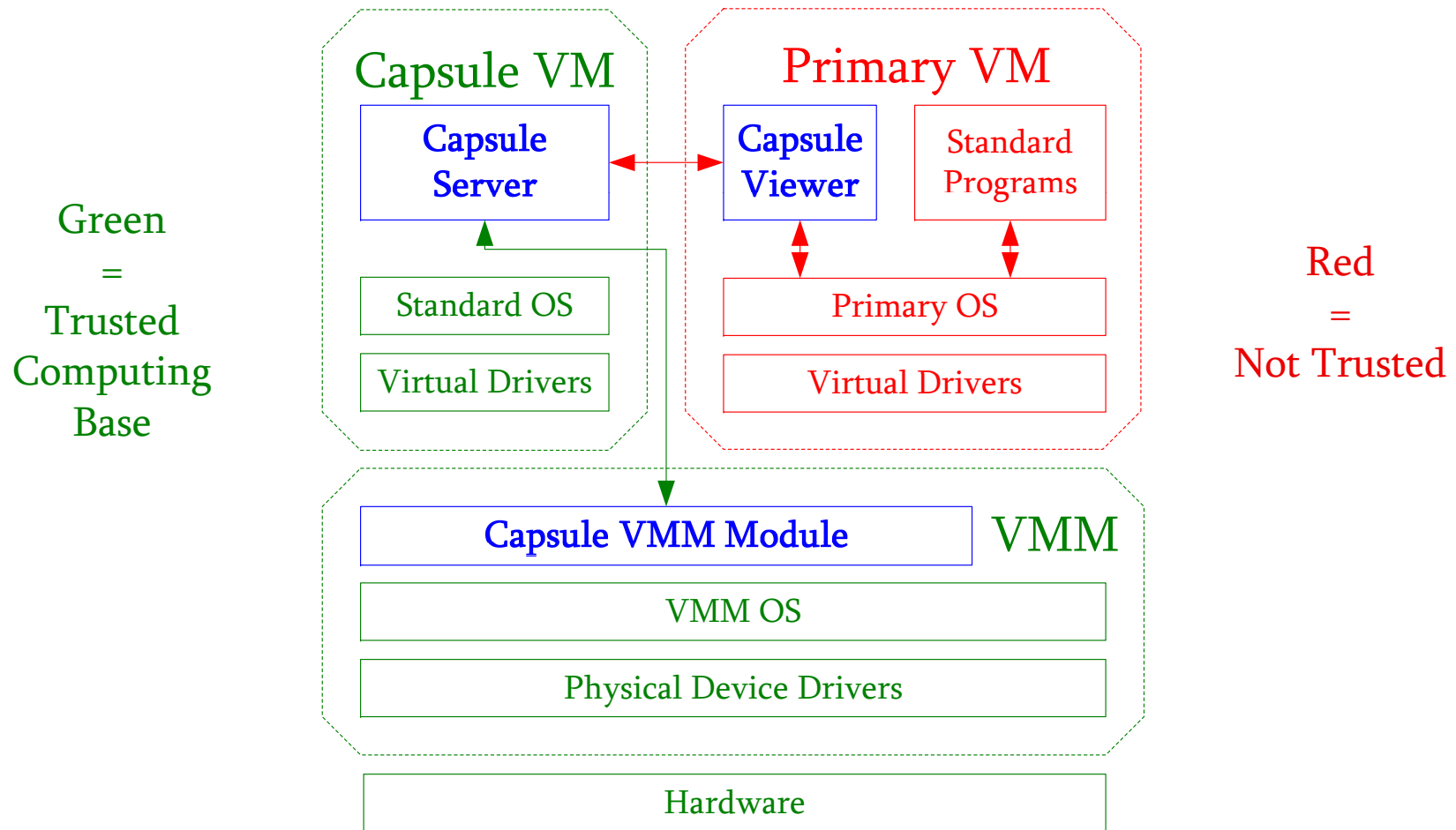


3. Close Container



Similar to TrueCrypt, but contents safe when open

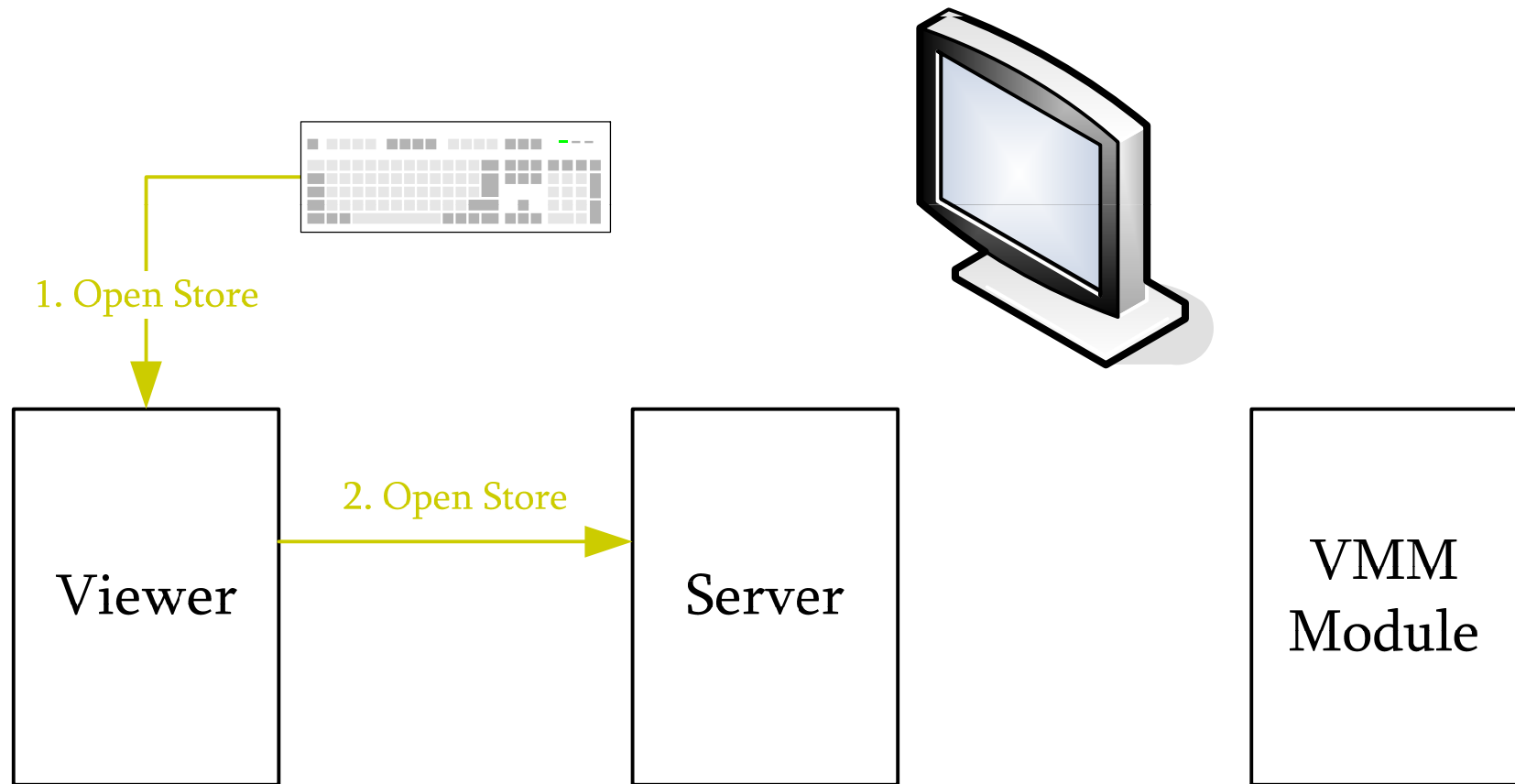
Capsule Architecture



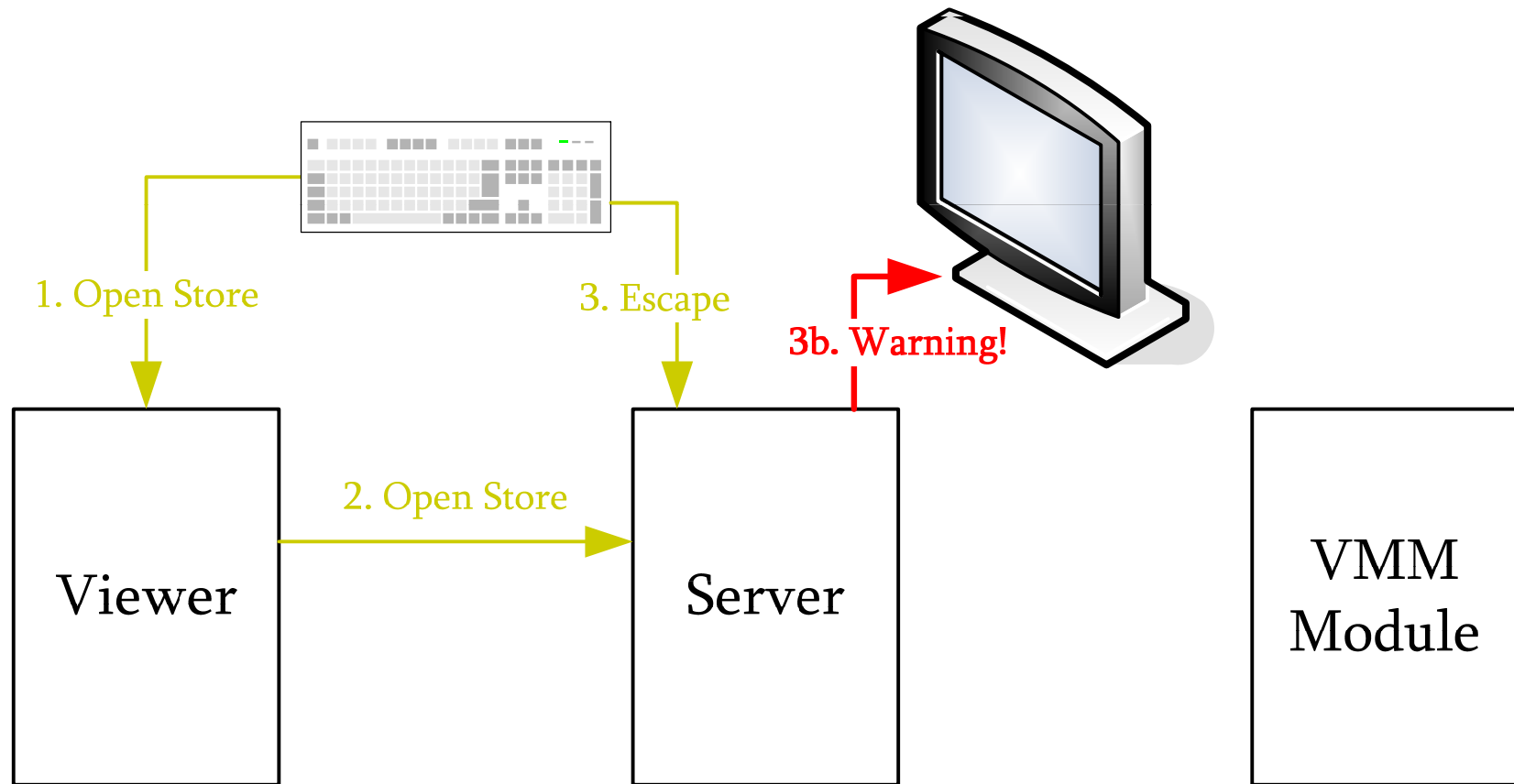
Threat Model

- We trust:
 - The user,
 - The capsule VM, and
 - The VMM
- Do not trust:
 - The primary OS
 - Applications
- Covert Channels
 - Channels within the primary VM are blocked
 - Channels in Capsule VM, VMM, and hardware may not be blocked

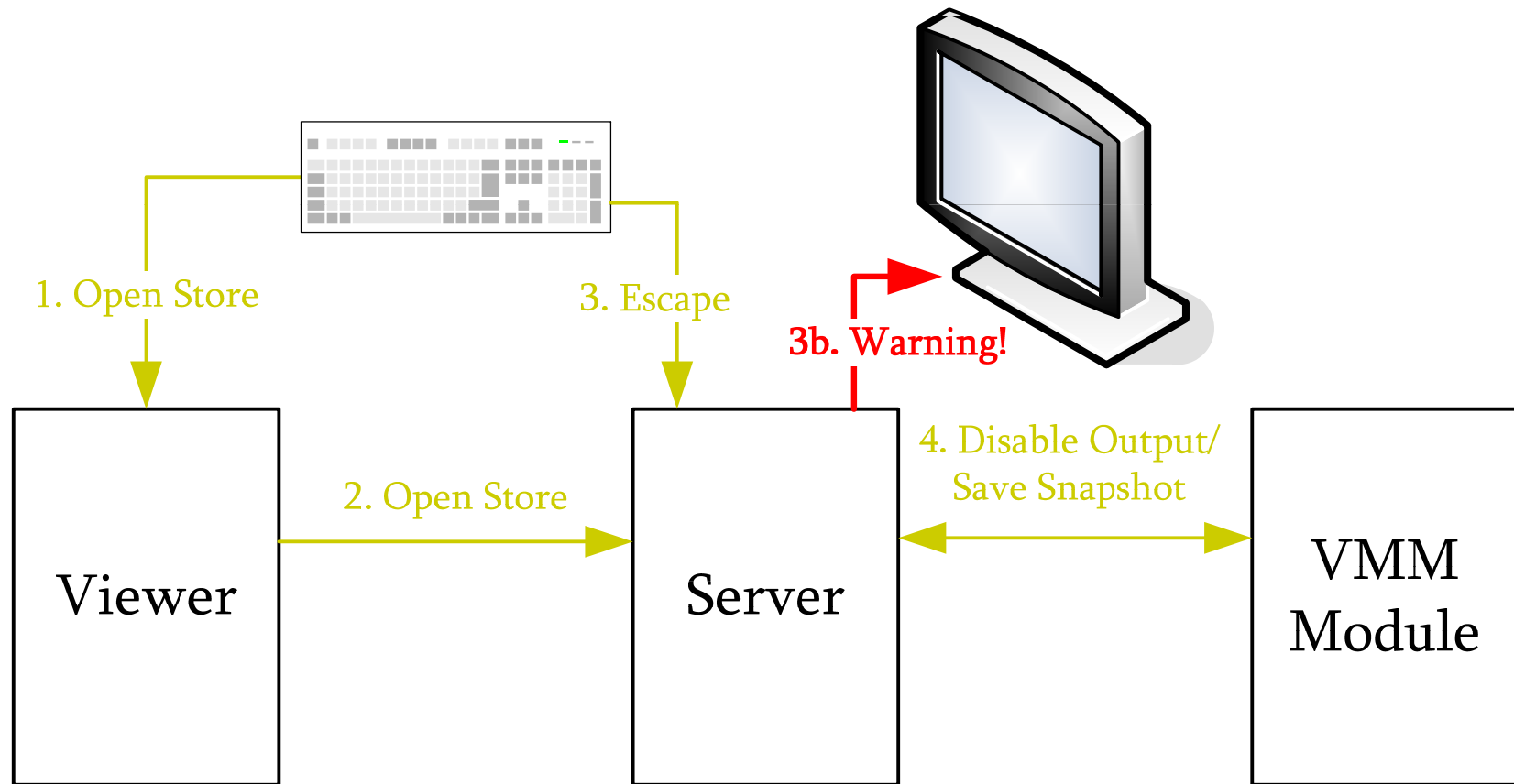
Opening a Storage Capsule



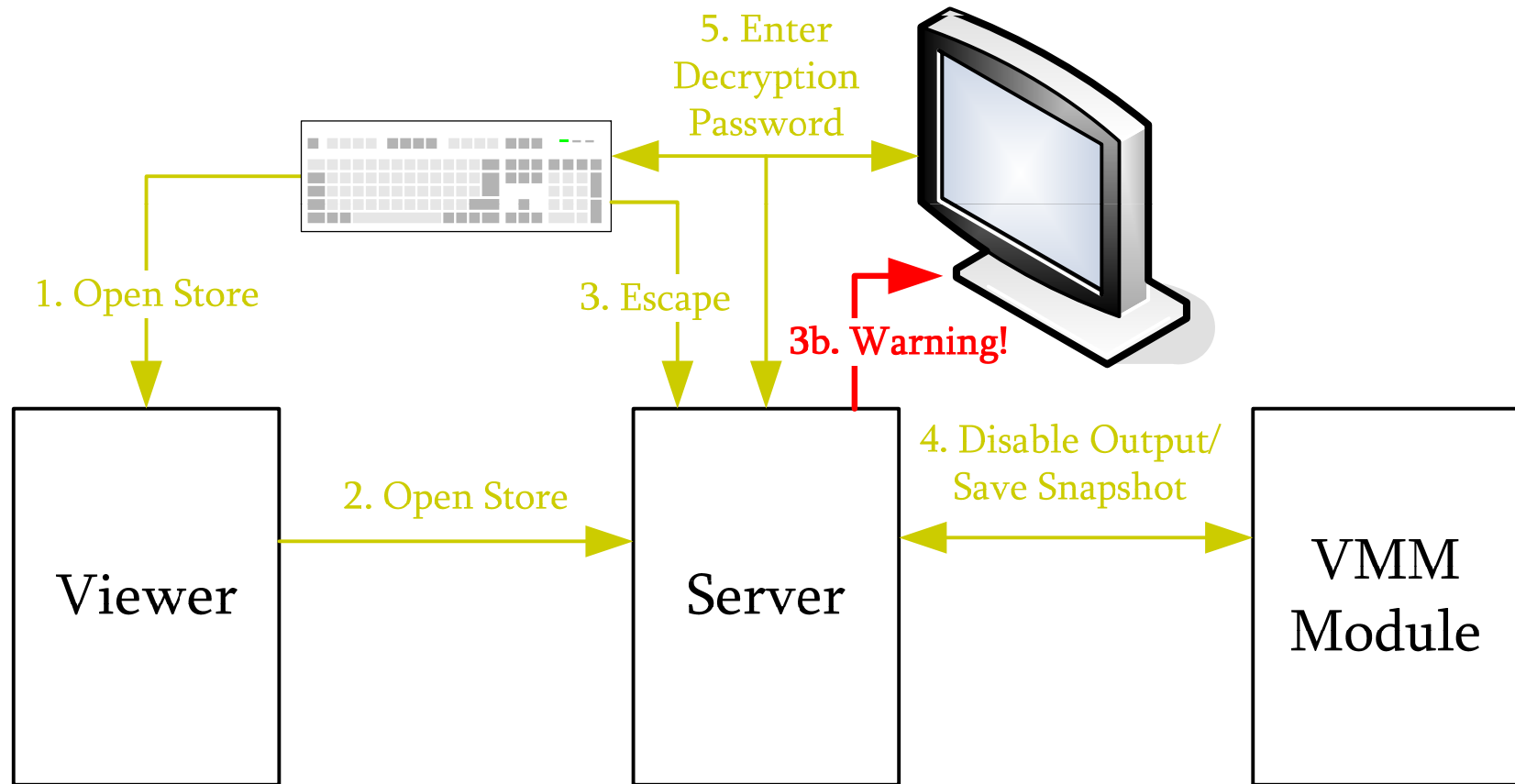
Opening a Storage Capsule



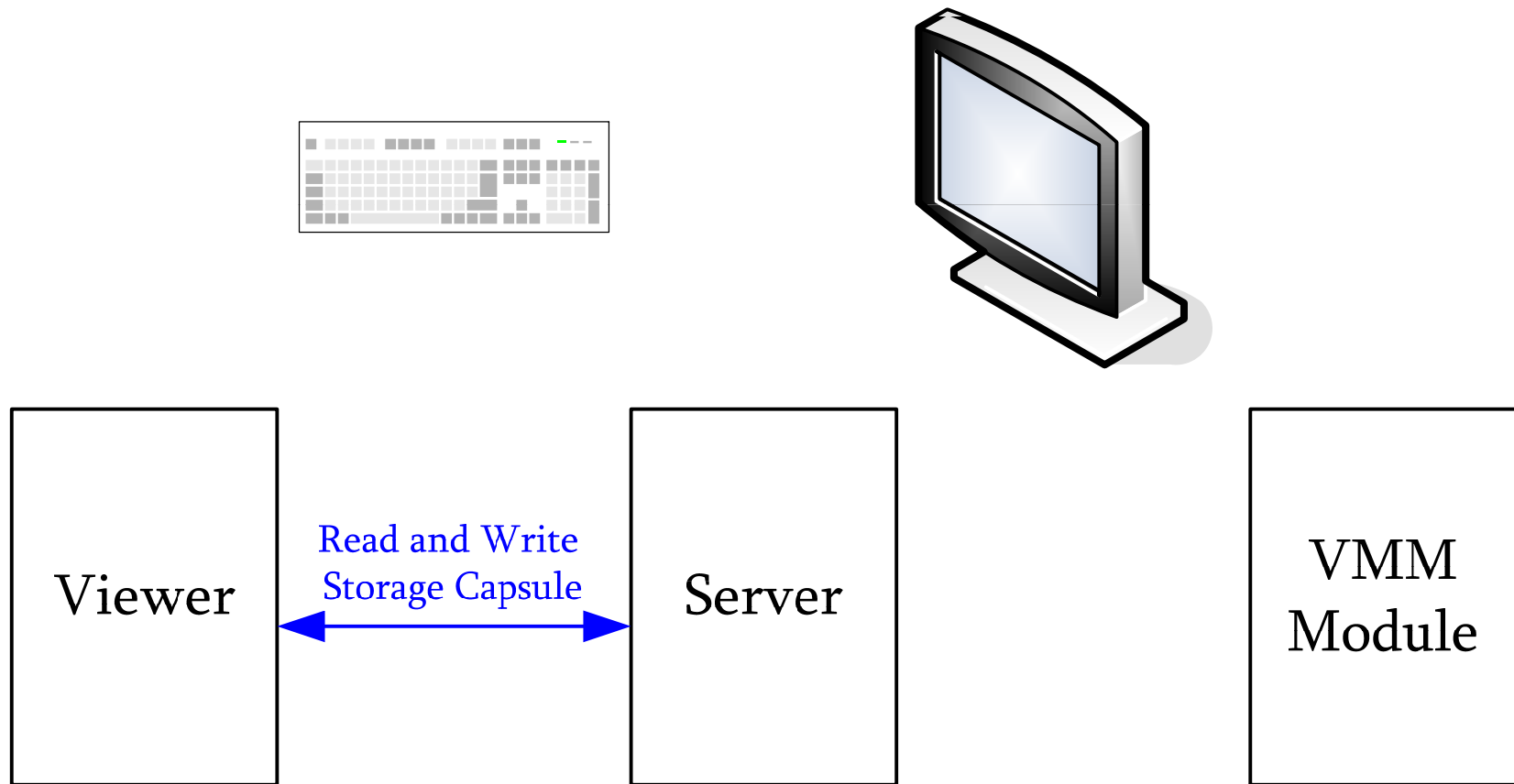
Opening a Storage Capsule



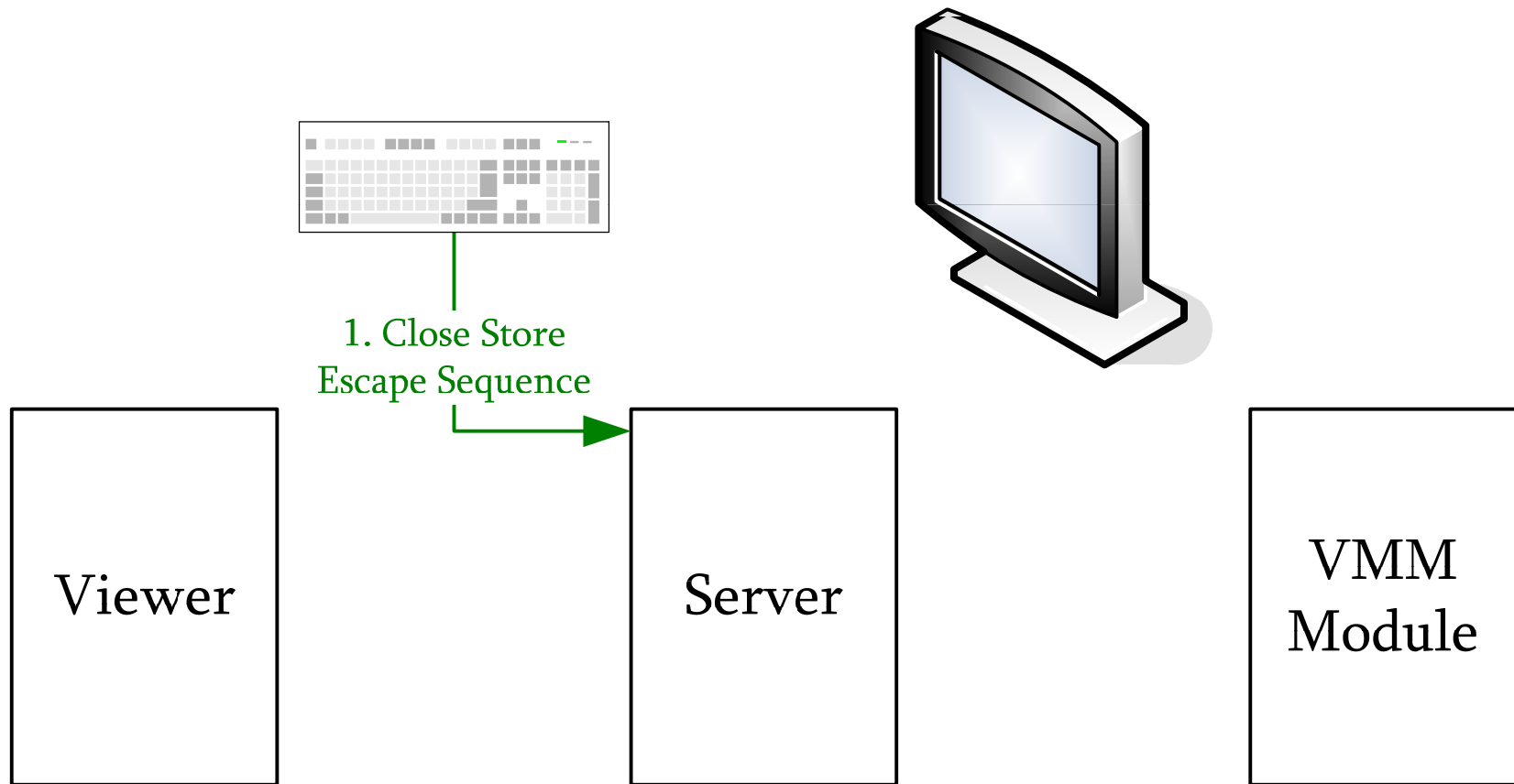
Opening a Storage Capsule



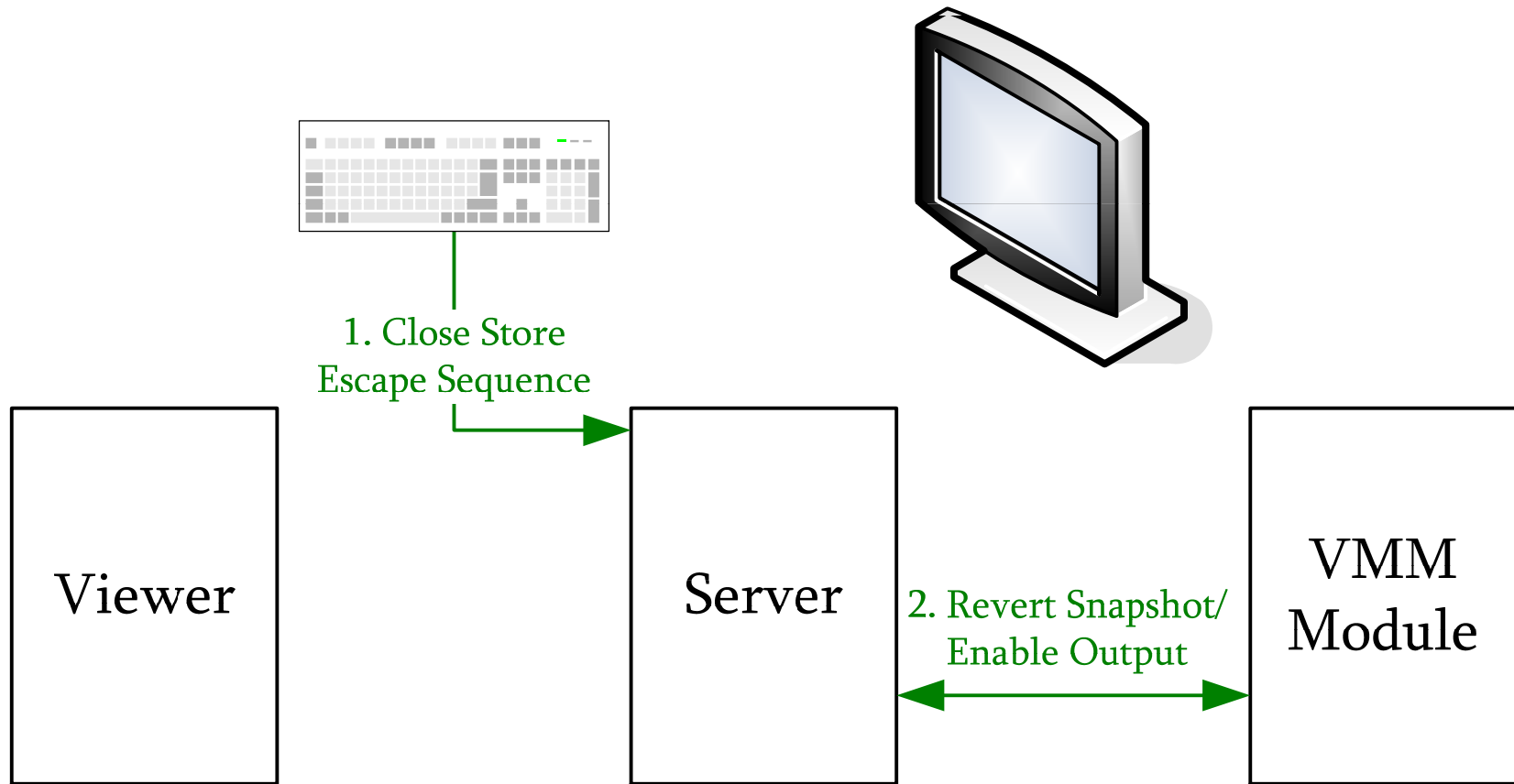
Accessing a Storage Capsule



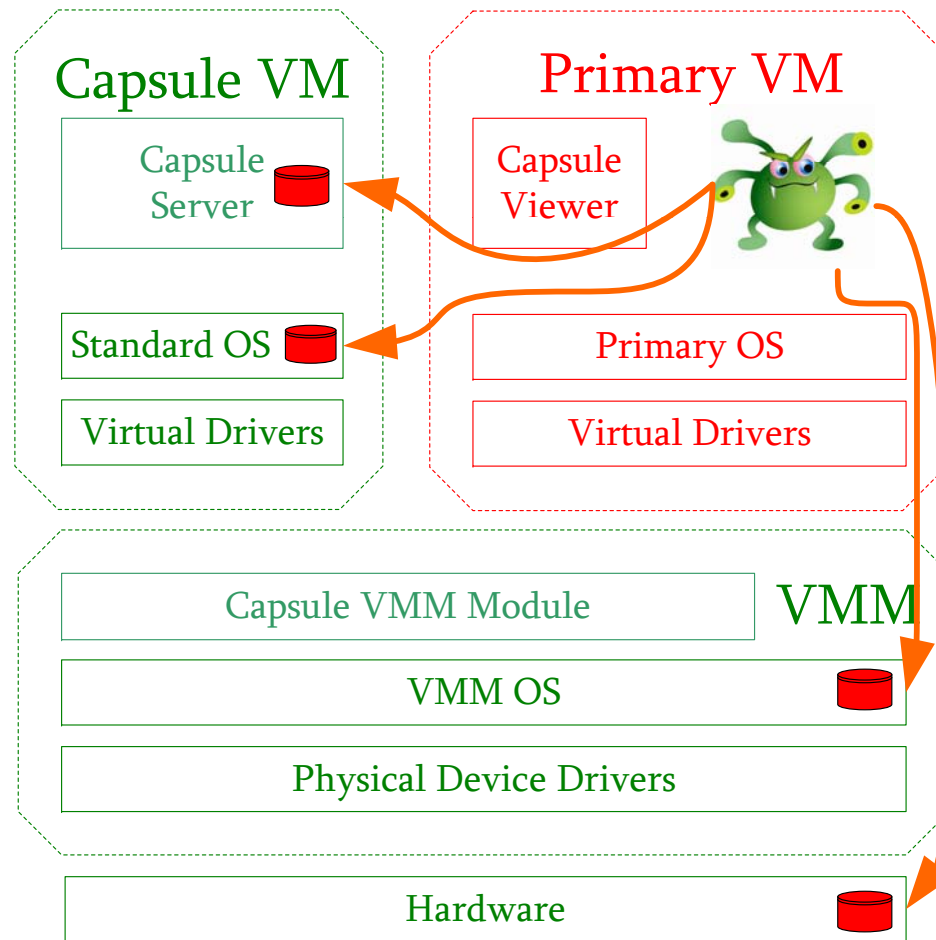
Closing a Storage Capsule



Closing a Storage Capsule



Covert Channels Illustrated



Attacks - Covert Channels

- Primary OS and Capsule could be manipulated, but we:
 - Fix the file store size
 - Re-encrypt the store before every export
 - The user controls transition timing with a secure key escape sequence
- External Devices – store data on floppy, CD-ROM, USB, SCSI, etc.
 - Device output is disabled in secure mode

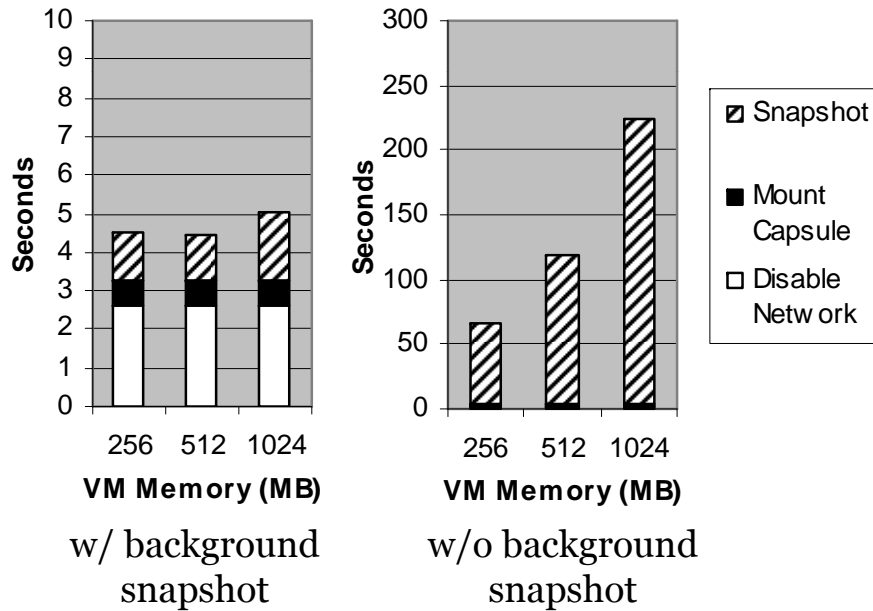
Attacks - Covert Channels (pt. 2)

- VMM – manipulate memory utilization and layout, store information in virtual network
 - VMM does not over-commit memory and uses fixed layout
 - Restart the virtual network during transition to normal mode
- Hardware – store data in CPU or disk cache
 - Restoration code adds noise to CPU, full reset would completely clear CPU
 - Would need to clear all disk caches or move all files to block disk covert channels

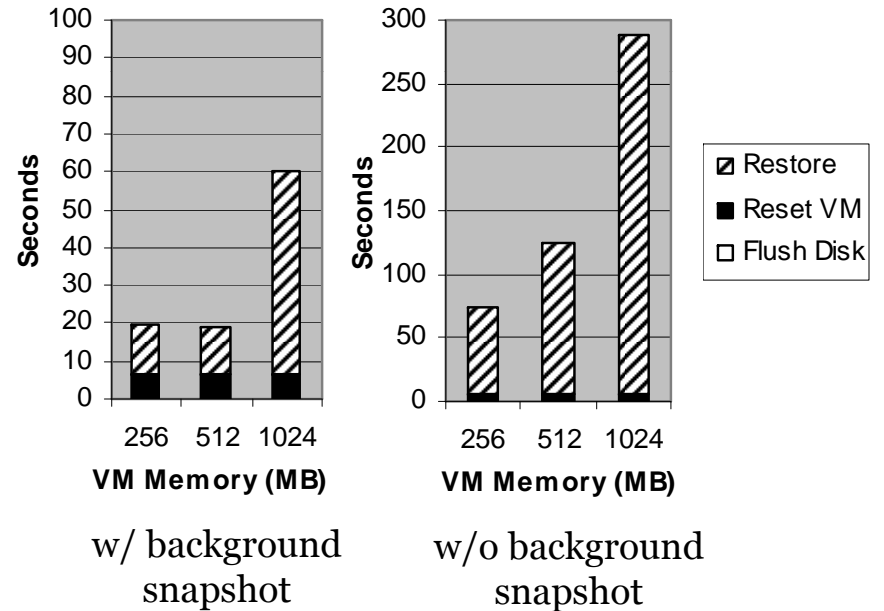
Attacks - Secure Mode Forgery

- Malware could fake secure mode UI
- To be safe, users are only required to:
 - Remember that they are supposed to enter a key escape sequence (like ctrl+alt+del) to enter secure mode
 - Heed warnings

Performance - Transitions

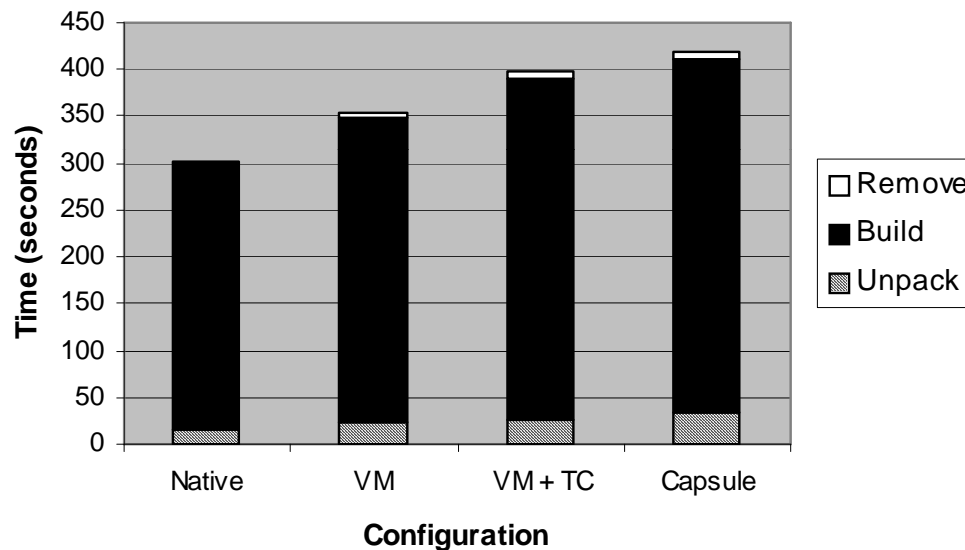


To Secure Mode



To Normal Mode

Disk Performance - Secure Mode



- For Apache build:
 - Storage Capsules 38% slower than native system
 - Only 5.1% slower than running TrueCrypt in VM



Limitations

- Changes made outside Capsules in secure mode are lost
 - Background computations
- Network connections are lost in secure mode
 - Downloads, services, etc.
- Short-lived sessions are impractical due to transition time



Conclusion

- Introduced Storage Capsules, a new mechanism for securing files on personal computers
 - Similar to existing file encryption software
 - Provide better protection and usability
 - Works in the face of a compromised OS
- Covert channel analysis
 - Explores covert channels on many layers

Questions

¿ ? ¿ ?

