



南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



Malware Analysis

Chapter 2: Malware Analysis in Virtual Machine

王志

zwang@nankai.edu.cn

updated on Sep. 17th 2021

College of Cyber Science

Nankai University

2021/2022



欧盟网络安全局（ENISA） 网络空间安全的十大趋势

1. 随着数字化转型进度的加快，网络安全攻击面持续扩大
2. 经历了新冠疫情之后，新的社会与经济秩序将逐步建立，并且对网络空间的**安全性**与**可靠性**提出更高要求
3. 在针对性攻击中，对**社交媒体平台**的使用已经成为一种显著趋势，而且涉及诸多不同威胁领域与威胁类型

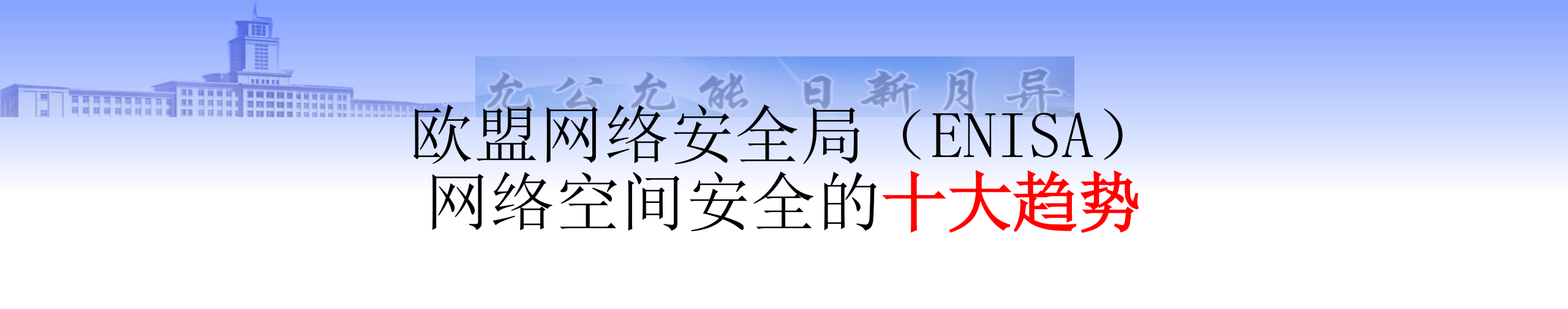




欧盟网络安全局(ENISA) 网络空间安全的**十大趋势**

4. 有**国家支持背景的攻击者**正针对高价值数据（例如知识产权与国家机密）开展精心策划且极具**针对性的持续攻击**。
5. 持续时间较短、影响范围极大的分布式攻击活动往往预设有多**多个目标**，例如凭证盗窃；





欧盟网络安全局（ENISA） 网络空间安全的**十大趋势**

- 6. 大多数网络攻击的基本动机仍然由**金钱驱动**
- 7. **勒索软件**仍然普遍，而且给众多组织带来巨大的经济损失
- 8. 相当一部分网络安全事件仍**未被发现**，或者时隔甚久才被曝光





欧盟网络安全局(ENISA) 网络空间安全的十大趋势

9. 随着安全自动化程度的提升，组织逐渐将网络威胁情报作为一项主动防御功能并给予持续投资
10. 网络钓鱼受害者数量不断增加，这也彰显出人为因素在安全体系内仍然属于薄弱环节





允公允能 日新月异

ENISA的预测

- 在**国家层面**，ENISA认为新一年中将出现“不受控制的**网络军备竞赛**”，届时所有国家都将争相获取“**网络空间战域**”中的最佳攻击工具，并借此实施**对抗**。





允公允能 日新月异

ENISA的预测

- “**网络犯罪预测**”方面，ENISA预计BEC（企业电子邮件威胁）、BPC（企业流程威胁）、以及针对托管服务供应商恶意软件还将继续肆虐。





允公允能 日新月异

Outline

- The Structure of a Virtual Machine
- Create a Virtual Machine
- Use a Virtual Machine
- The Risks





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



The Structure of a Virtual Machine



允公允能 日新月异

- **Fresh** malware can be full of surprises.





Dynamic Analysis

- Running malware deliberately, while monitoring the results
- Requires a **safe environment**
 - Quickly spread to other machines on the network
 - Air gap – no connection to Internet or other PC
 - Very difficult to remove





Physical Machines

- Disadvantages
 - **No Internet** connection, so parts of the malware may not work
 - Can be **difficult to remove** malware, so re-imaging the machine will be necessary





Virtual Machines

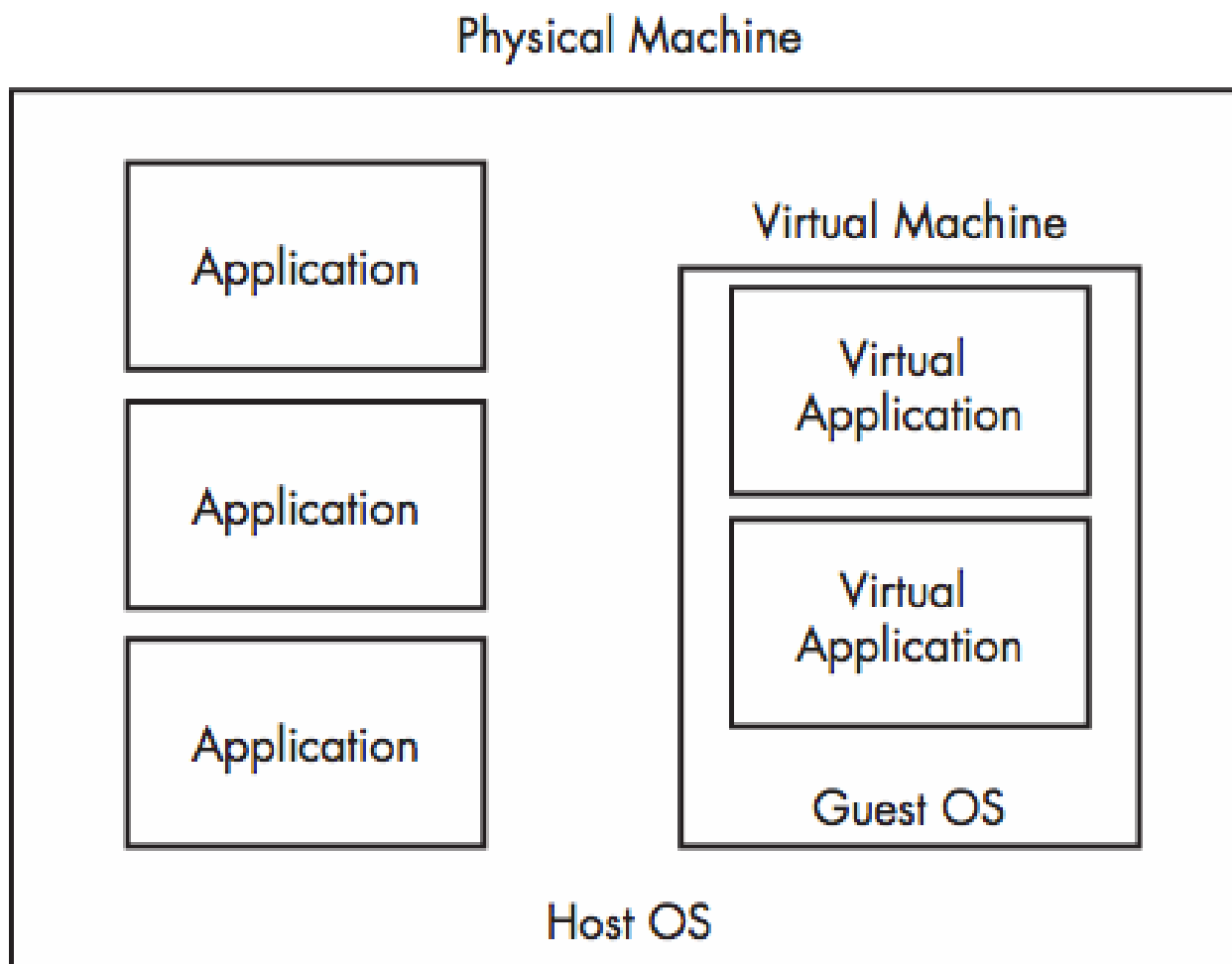
- The most common method
 - completely isolated
- This protects the host machine from the malware
 - Except for a few very rare cases of malware that escape the virtual machine and infect the host





允公允能 日新月异

VM Structure





VMware Player

- **Free** but limited
- Cannot take snapshots
- Cannot clone or copy VM
- VMware Workstation or Fusion is a better choice, but they cost money
- VirtualBox, Hyper-V, Parallels, or Xen.





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



Create a Virtual Machine



Configurations

- Disk
 - enough to store the guest OS and tools for malware analysis
 - 20 GB hard drive
 - Resizable





Configuration

- OS
 - **Windows XP** is still the most popular OS (Surprisingly)
 - The malware we are analyzing targets Windows XP, as most malware does
 - New programs are compatible to older system
 - We focus our explorations on Windows XP





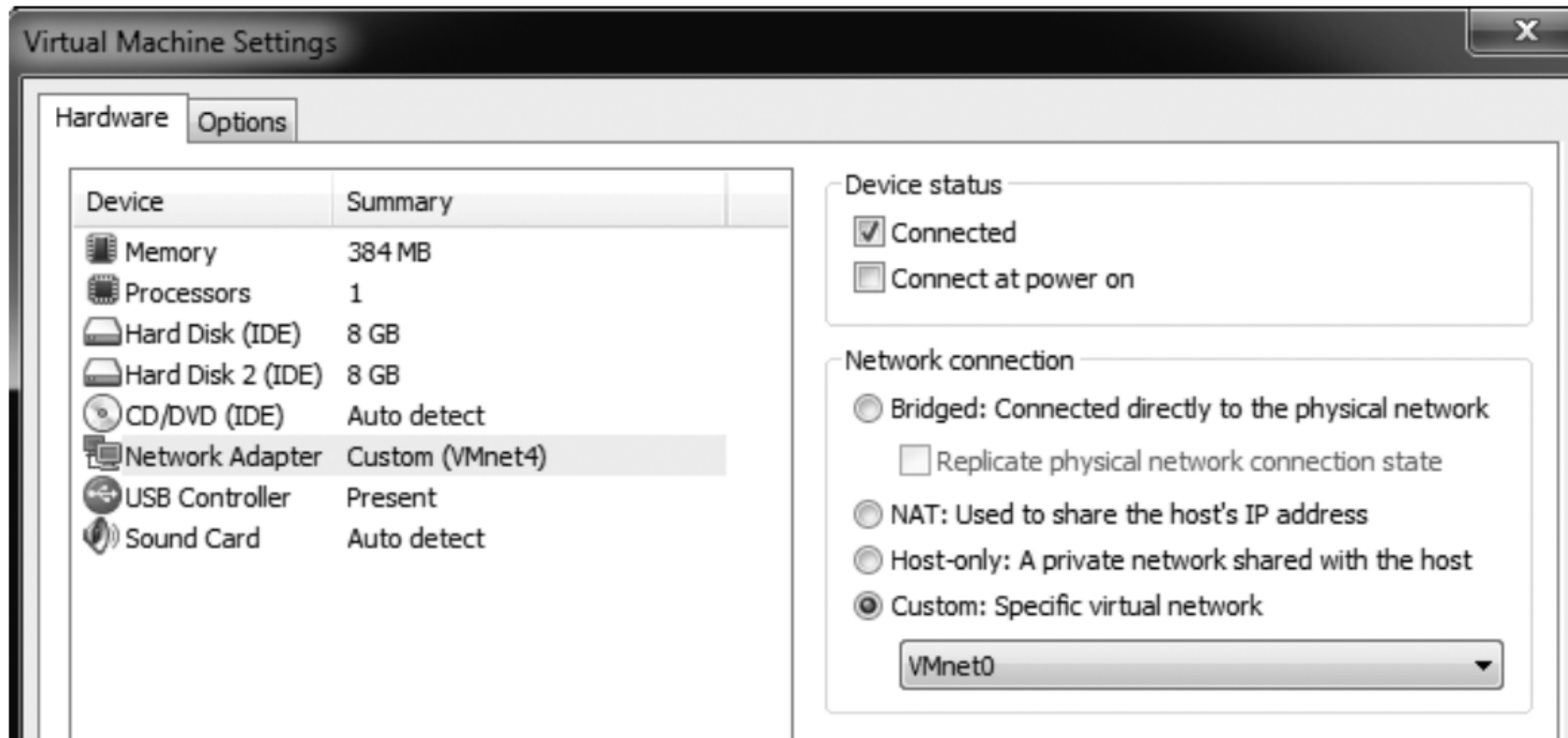
Configuration

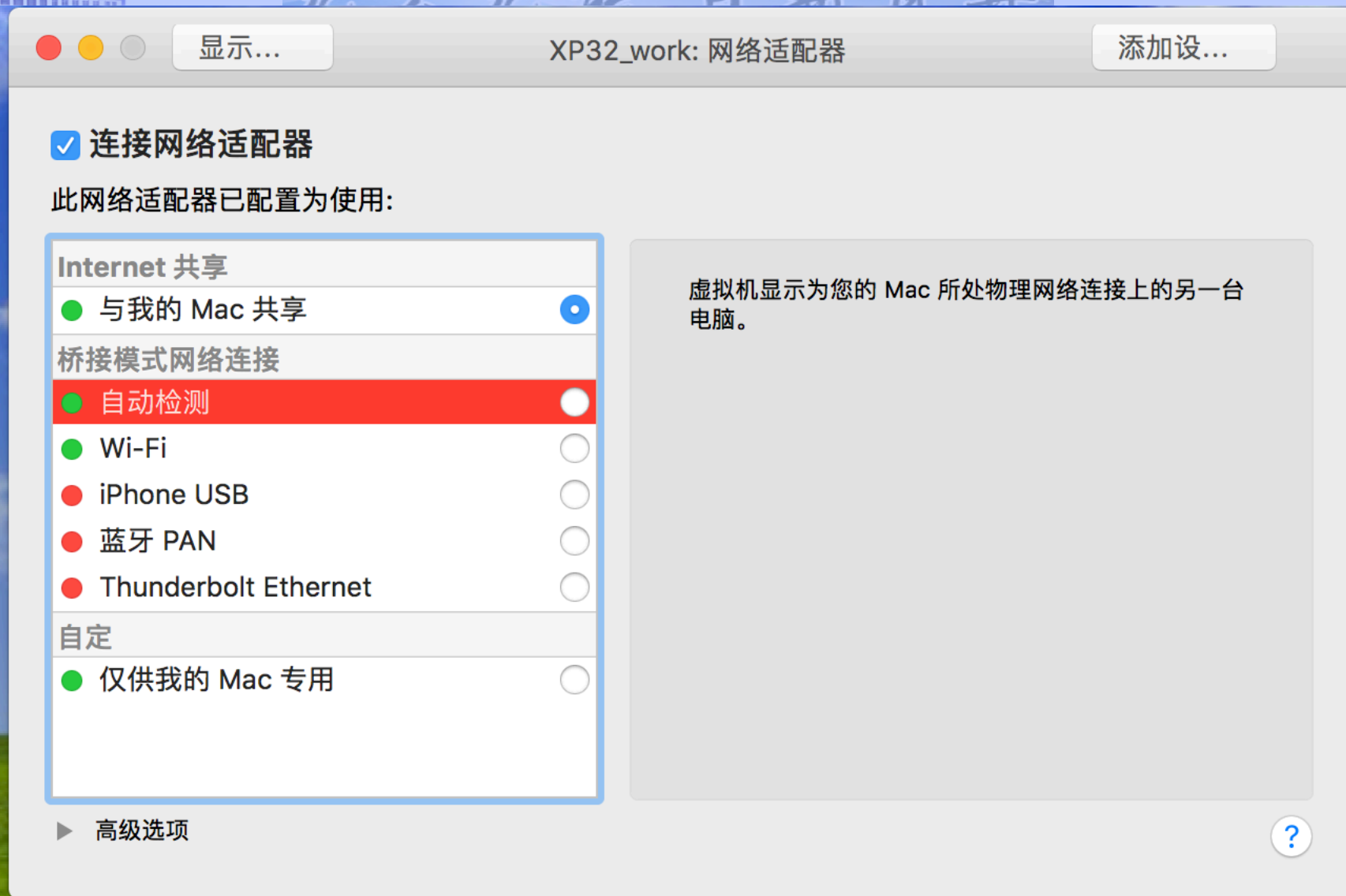
- Application
 - VMware tools
 - tools for malware analysis
 - IDA Pro
 - Ollydbg
 - ...
 - Appendix B
 - tools.pediy.com



Configuring VMware

- We can disable networking by disconnecting the virtual network adapter







南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異



Use a Virtual Machine



允公允能 日新月异

Connecting Malware to the Internet

- For a more realistic analysis
- **Risks:** propagation, DDoS, Spam,...
- **Pre-analysis:** what might do when connected





允公允能 日新月异

Connecting Malware to the Internet

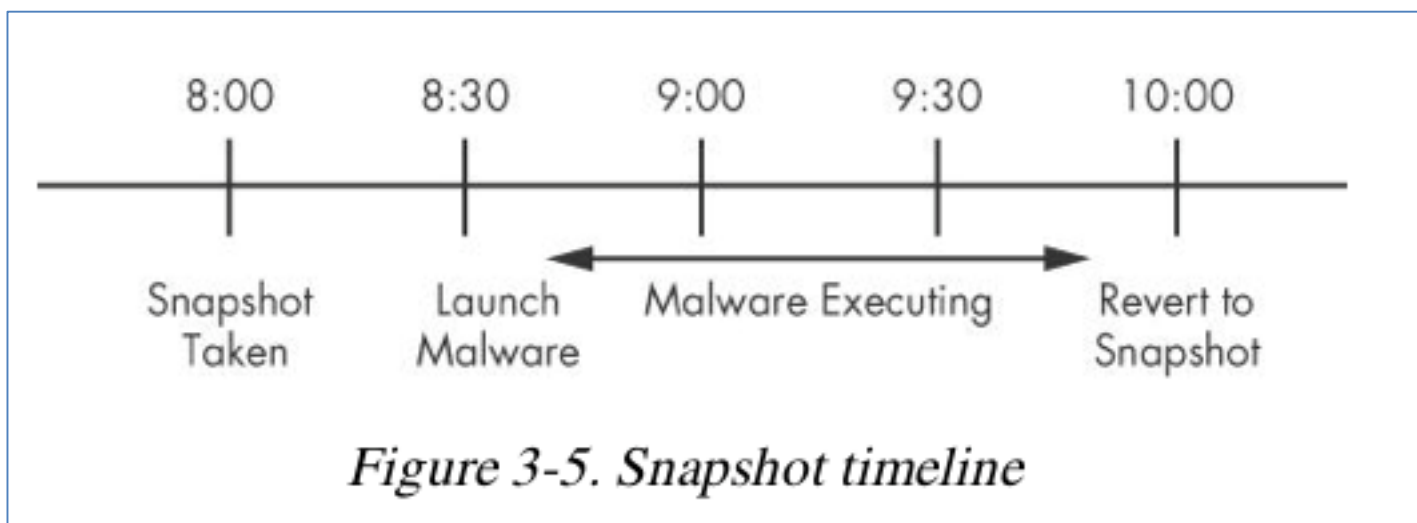
- **NAT** mode lets VMs see each other and the Internet, but puts a virtual router between the VM and the LAN
- **Bridged** networking connects the VM directly to the LAN
- Can allow malware to do some harm or spread – **controversial**
- You would send spam or participate in a DDoS attack





允公允能 日新月异

Snapshots





允公允能 日新月异

Transfer File

- VMware **drag-and-drop** feature
 - from host OS to guest OS
 - from guest OS to host OS
- **Shared folder**
 - accessible from both the host and guest OS





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

A light blue world map is centered in the background of the slide.

The Risks



Risks of Using VMware for Malware Analysis

- Malware may **detect** that it is in a VM and run differently
 - Chapter 17: anti-VMware techniques
- VMware has **bugs**: malware may crash or exploit it
 - drag-and-drop vuln
 - fully patched
- Malware may **spread** or affect the host – don't use a sensitive host machine





Virtual Machine Escape

- Breaking out of VM
 - CVE-2007-1744 Directory traversal vulnerability in shared folders feature for VMware
 - CVE-2008-0923 Directory traversal vulnerability in shared folders feature for VMware
 - CVE-2009-1244 Cloudburst: VM display function in VMware
 - CVE-2012-0217 The x86-64 kernel system-call functionality in Xen 4.1.2 and earlier
 - CVE-2014-0983 Oracle VirtualBox 3D acceleration multiple memory corruption
 - CVE-2015-3456 VENOM: buffer-overflow in QEMU's virtual floppy disk controller





南開大學

NANKAI UNIVERSITY, P.R. CHINA 1919

允公允能 日新月異

Malware Analysis

Chapter 2: Malware Analysis in Virtual Machine

王志

zwang@nankai.edu.cn

updated on Sep. 17th 2021

College of Cyber Science

Nankai University

2021/2022