网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

从云安全感知网络空间安全的新威胁

张健

南开大学网络空间安全学院 教授/博导
中国网络空间安全协会 副秘书长

威胁框架：认知与实践

寒夜远征

寒夜远征

CONTENTS

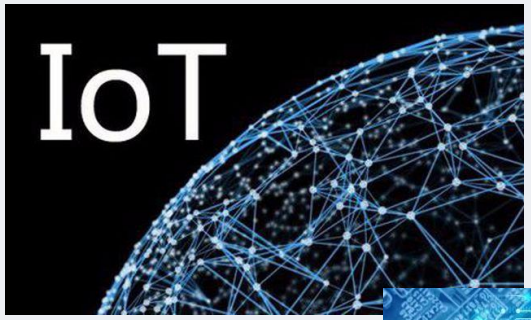
目 录

寒夜速记

威胁框架：认知与实践

01 网络技术和应用不断创新

新技术新应用快速发展


IoT


BIG
DATA
大数据
ADTIME
实时性计算
长时段跟踪
分析
可视化
可视化数据仓库


人工智能


5G


云计算


区块链

云计算

美国国家标准与技术研究院（NIST）对云计算的定义为：云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池（资源包括网络，服务器，存储，应用软件，服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

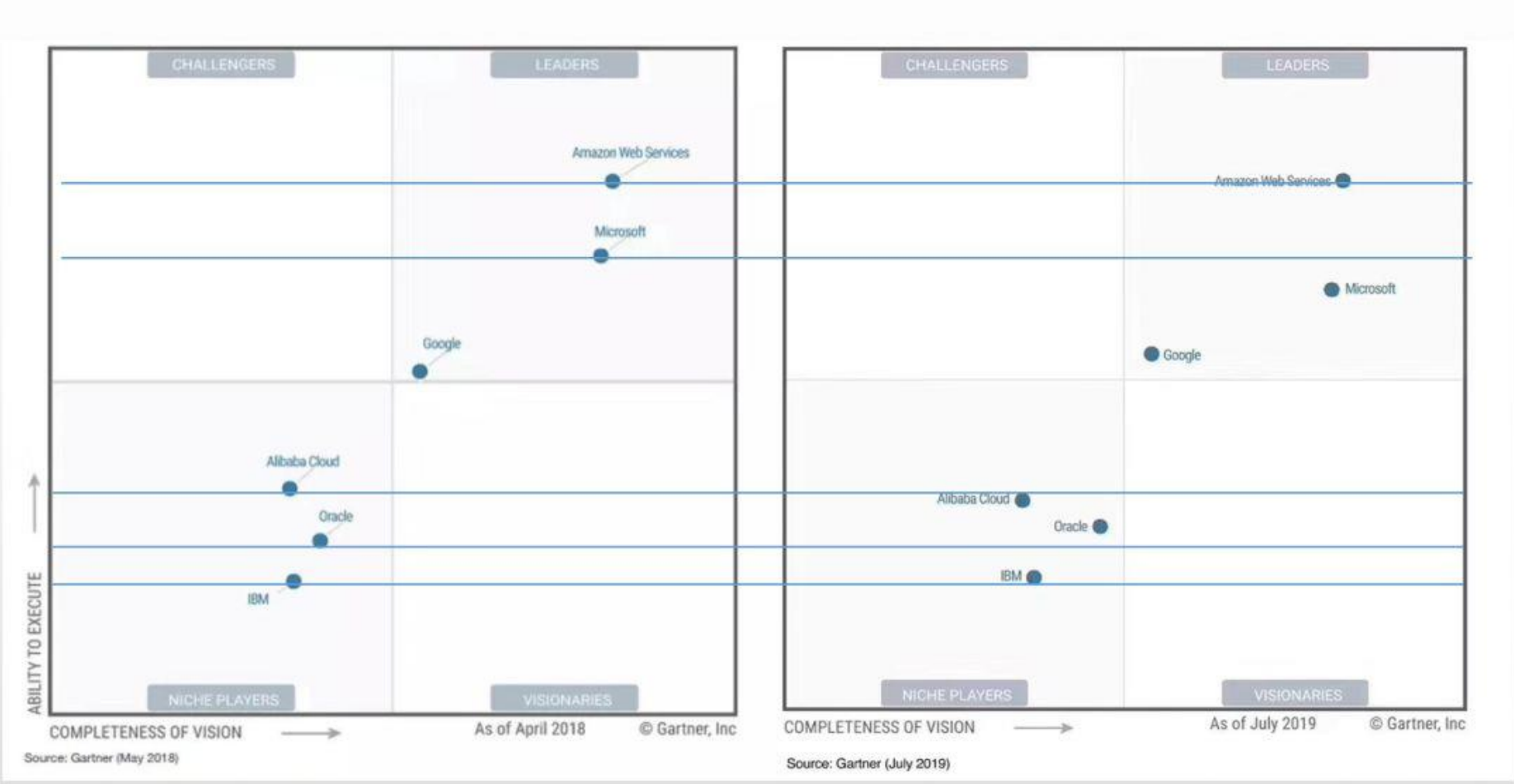
三种服务形式

- 软件即服务（SaaS）
- 平台即服务（PaaS）
- 基础设施即服务（IaaS）

四种部署形式

- 私有云（Private Cloud）
- 公有云（Public Cloud）
- 社区云（Community Cloud）
- 混合云（Hybird Cloud）

Gartner：2019年全球 IaaS 魔力象限



Gartner：2019年全球公有云收入超2100亿美元

Gartner发布的最新数据显示，全球公有云服务市场将从2018年的1824亿美元增至2019年的2143亿美元，增幅达17.5%。中国公有云服务终端用户支出将在2022年超过1.1千亿元人民币。

Gartner近期调查显示，超过三分之一的企业机构将云投资视作前三大投资重点之一，这将影响到市场产品与服务。Gartner预测，2019年年底之前，超过30%的技术提供商新增软件投资将从“云优先”转变为“云唯一”。

Gartner预计，到2022年云服务行业的市场规模与增幅将会是整体IT服务增幅的近三倍。未来三年将呈现爆发性增长。

从全球范围来看，目前阿里云继续保持着全球云计算市场前三的领先地位，份额仅次于亚马逊AWS、微软Azure。在国内，阿里云是当之无愧的云计算第一，2018年上半年市场份额为43%，超过了2-8名的总和。

微软击败亚马逊，拿下美政府100亿美元云计算合同

- 据报道， 美国国防部2019年10月25日宣布，美国政府已向微软授予了100亿美元的巨额云计算合同，该合同被称为联合企业防御基础设施（JEDI），将为五角大楼提供基本云服务和人工智能处理、机器学习及关键任务工作负载处理等高级服务。合同有效期为10年。
- 微软赢得了为美国政府制造“战争云”的10年协议后正文内容
- **JEDI的使命：**它始于2017年军方对西海岸科技企业的访问，其中包括在亚马逊和其他著名的科技公司停留。访问结束后，时任国防部长的James Mattis命令国防部官员准备一份计划，以使国防部的技术基础设施现代化。2018年初，五角大楼公布了这项计划，这是一项耗时10年、耗资100亿美元的军队信息技术操作现代化项目。
- 尽管军方和情报部门的不同分支多年来一直在进行各自的云计算项目，但新提案为整个国防部勾勒了一个统一的 IT 方法，包括机密和非机密行动。
- “国防部缺乏协调的企业级云计算基础设施和平台方法，使作战人员和领导人无法以‘任务速度’做出关键的数据驱动决策，从而对结果产生负面影响。”国防部的提案说。在缺乏现代化服务的情况下，作战人员和领导人不得不在放弃作战能力和通过漫长的获取、部署和供应过程中间艰难作出选择。
- **微软的工作：**微软的任务是彻底改造国防部的整个 IT 基础设施，创建一个全球可用和响应的网络，并提供对漏洞和破坏等问题的持续监测。该系统必须加强网络防御和有效的加密。
- 五角大楼对JEDI的主要目标之一是将人工智能和机器学习等现代计算技术应用于国防行动。
- 国防部的提案还要求供应商提供可用于全方位军事行动的战术边缘设备，这些设备为耐用、坚固、便携的计算和存储设备，也是模块化、可快速部署的数据中心。
- “我们感到自豪的是，我们是国防部整体云战略使命中不可或缺的合作伙伴，”微软美国监管行业总裁Toni Townes-Whitley在一份声明中表示，“正如在整个JEDI采购过程中所阐述的那样，国防部有一个单一的目标——部署最具创新性和最安全的商业可用技术，以满足当今作战人员的迫切和关键需求。”

风起云涌

寒夜速纪

威胁框架：认知与实践

02 云安全总体形势严峻

CNCERT发布《2019年上半年我国互联网网络安全态势》

目　录

（五）云平台安全

问题趋势： 根据CNCER…在我国云平台上的网络安全事件或威胁情况相比2018年进一步加剧。

- 首先，发生在我国主流云…北仍然较高，
  - 其中云平台上遭受DI…数的69.6%、
  - 被植入后门链接数量…53.1%、
  - 被篡改网页数量占境…

  云平台及其承载的业务…者——成为黑客眼中的肥肉）
- 其次，攻击者经常利用我…
  - 其中利用云平台发起…占监测发现的DDoS攻击总次数的78.8%
  - 发起对境内目标DD…平台的IP地址占72.4%、
  - 承载的恶意程序种类…序种类数量的71.2%、
  - 木马和僵尸网络恶意…恶意程序控制端IP地址数量的84.6%。

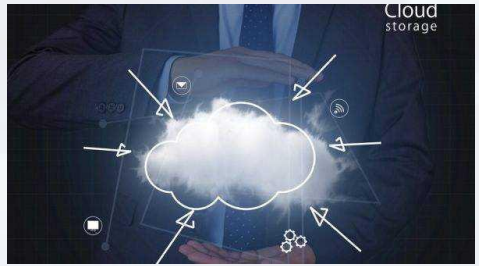
  云平台成为主要的攻击…提供了资源保障）
- 另外，自2019年以来，C…Elasticsearch等数据库数据泄露风险应急处置过程中，发现存在隐患的数…占比超过40%。

  云平台是承载重要敏感数…滴漏

“Ryuk”等勒索软件开始“云勒索”

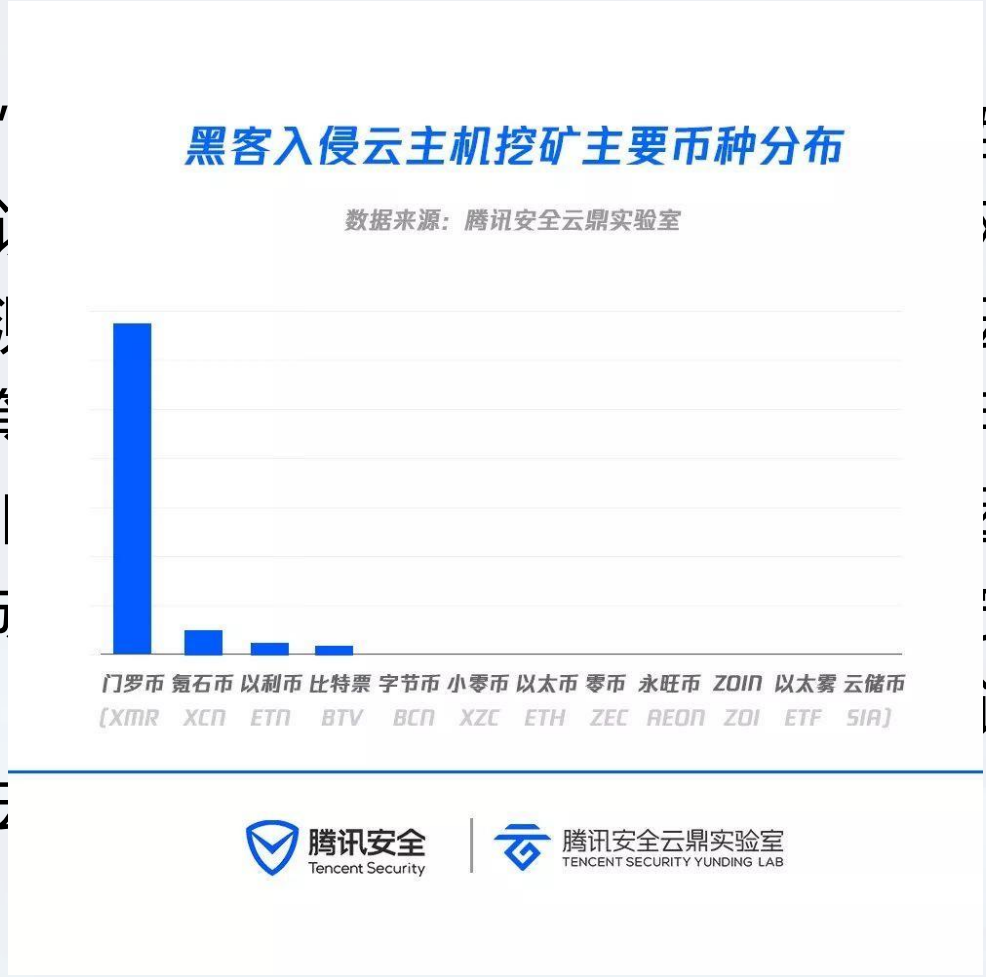
2018年底，著名云托管服务提供商Dataresolution.net在圣诞节前夕遭遇勒索软件攻击，正竭力使系统恢复如初。该公司表示，其系统受到了Ryuk勒索软件的攻击，上周末同一种恶意软件搞垮了美国多家知名报刊的印刷和发货业务。

总部位于加利福尼亚州圣胡安卡皮斯特拉诺的Data Resolution LLC为全球约30000家公司企业提供软件托管、业务连续性系统、云计算和数据中心等服务。



“云挖矿”严重威胁云安全

非法“挖矿”…互联网企业和网络安全企业分析…网络安全问题。其中，腾讯云监…云主机成为挖取门罗币、以利币等…用云主机计算资源进行“挖矿”…团队监测发现，“争夺矿机”已成…安全技术团队监测发现一种新型…该病毒在两个月内疯狂传播，非法…



阿里云出现故障

2018年6月27号下午，阿里云服务器出现故障，估计很多人都发现自己网站登不进，随后阿里云发布公告称，阿里云工程师正在紧急处理中。下午5点半，部分网站已恢复正常，阿里工程师回复：敬畏每一行代码，敬畏每一份托付。

【异常通告】6月27日阿里云部分产品及账号登录访问异常通告

【阿里云】【异常通告】

异常时间：北京时间2018年6月27日16:21左右。

异常概述：于北京时间2018年6月27日16:21左右开始，阿里云官网的部分管控功能、及MQ、NAS、OSS等产品的部分功能出现访问异常，阿里云工程师正在紧急处理中，请您稍后重试。

给您带来诸多不便实在抱歉！有任何问题，可随时通过服务电话95187联系反馈。

【异常更新】

北京时间2018年6月27日 17:30

目前受影响的产品功能大部分已经恢复正常，请您确认。若还有异常，请您跟我们反馈，谢谢。

北京时间2018年6月27日 16:50

目前受影响的产品功能正在逐步恢复中，若遇到异常，请您稍等后重试。

创业公司投诉腾讯云硬盘故障致数据丢失

- 一家名为前沿数控的创业公司投诉腾讯云，称2018年7月20日，近千万元级的平台数据全部丢失，原因就是选用了腾讯云服务器。前沿数控称，在与腾讯云的交涉过程中他们给出的答复始终是“已向公司相关部门反馈，请耐心等待”。直到事故发生第14天，腾讯云才给出答复，答复是：补偿责任总额不超过腾讯云公司就违约服务收取服务费用总额，另赠一个腾讯云价值10万元的套餐包。前沿数控称，随后，腾讯云很快将赔偿方案中的10万套餐包改为13.29万元现金，说这是他们争取的最大赔偿了。
- “一个创业公司花二年多心血打造的平台就这样被腾讯云给毁了，在公司生与死的抉择关口，腾讯云公司口口声声说重视，他们会对事故负责，我们也期盼腾讯云能提供合理的赔偿资金来还创业公司的一线生机。”前沿数控说，经过苦苦等待十多天，得到的结果却是少得可怜的赔偿。
- 腾讯云发布公告，称希望可以尽快帮助用户恢复业务，将损失降低最低，因此提出“赔偿+补偿”总金额达到136469元的解决方案，这是其在腾讯云平台中用云金额的37倍。“‘前沿数控’基于自身评估就此次故障对腾讯云提出了高达11016000元的索赔要求。”腾讯云说，毫无疑问，这远远高于自身能够提供的方案。这也是此次双方目前未能达成一致的主要原因之一。腾讯云还说，对此次故障给用户业务带来影响再次表示最诚恳的歉意。后续，针对云盘产品会额外实行定期强灾备措施，进一步保障用户数据的可靠性。

重要的云计算平台应当属于关键信息基础设施

第十八条 下列单位运行、管理的网络设施和信息系统，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，应当纳入关键信息基础设施保护范围：

（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；

（二）电信网、广播电视网、互联网等信息网络，以及提供**云计算**、大数据和其他大型公共信息网络服务的单位；

（三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；

（四）广播电台、电视台、通讯社等新闻单位；

（五）其他重点单位。

寒夜速纪

威胁框架：认知与实践

03 云计算环境面临的安全威胁

The top 7 cloud computing security threats

1.Data Breach

A data breach (or leak) is possibly the most widespread cloud security concern. It usually happens as a result of cloud computing security attacks, when unauthorized users or programs gain access to confidential data and can view, copy, or transmit it.

2. Data Loss

Unlike data breaches, data loss often happens due to natural or man-induced disasters, as a result of the physical destruction of the servers or human error. However, it can also be a result of a targeted attack. Regardless of the cause, the result will be the same: you lose all of the data you've been collecting for years.

3. Denial Of Service (DoS)

Another popular type of cloud computing security attack, a Denial of Service (DoS) attack can shut down your cloud services, making them temporarily (or indefinitely) unavailable to your users. This can be done by either flooding the system with extensive traffic, which the servers simply can't buffer, or crash it by taking advantage of the bugs and vulnerabilities.

4. Cryptojacking

A relatively new cloud security threat, cryptojacking was widely adopted last year, largely due to the growing cryptocurrency frenzy. In this type of cloud computing security attack, hackers use your computing resources to process cryptocurrency transactions by installing a crypto mining script on your servers without your consent. This leads to an increased CPU load and, as a result, can significantly slow down your system.

The top 7 cloud computing security threats

5. Account Hijacking

Even if your employees aren't using default, insecure passwords, hackers still can "guess" the credentials, gain access to your cloud using your staffs' accounts, and, as a result, steal or manipulate your data or sabotage your business processes in general. This is called, "account hijacking."

6. Insecure APIs

Even if your own systems are safe, there are often third-party services that can introduce additional cloud security risks. Namely, IoT solutions are typically considered a threat to data privacy: devices, such as connected cars, health monitors, and home appliances, collect and transmit tons of sensitive data in real time. As a result, intruders can hijack your data by hacking your APIs, not the cloud itself.

7. Insider Threats

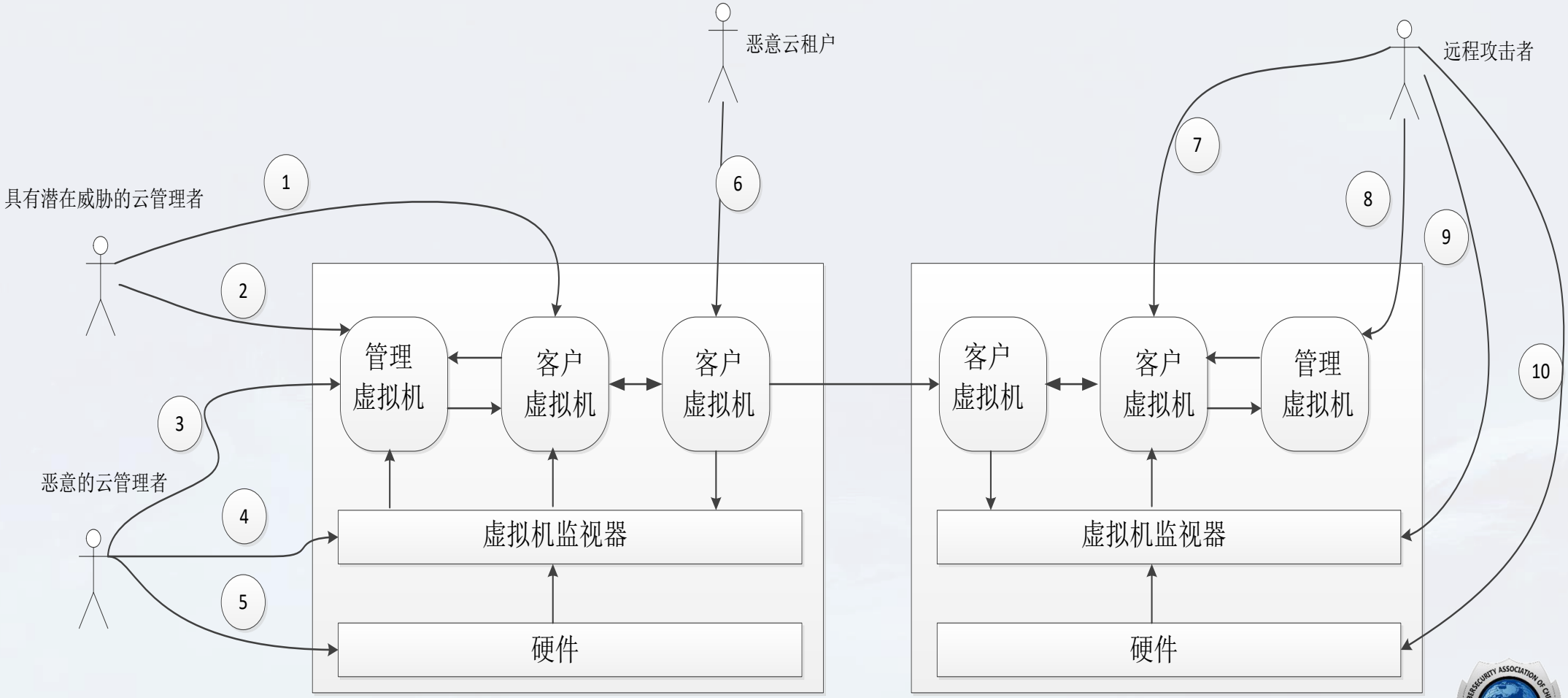
Apart from external security threats in cloud computing, there are enough internal risks. For example, your own employees can cause privacy violations or major data leaks. This can be due to targeted malicious behavior or simply a result of human error. Moreover, they can serve as an entry point for malware, e.g. by using their devices for work-related tasks as a part of the BYOD policy.

云面临的主要安全威胁

云面临的威胁主要有两类：

- 内部威胁
  - 具有潜在威胁的云管理者
  - 恶意的云管理者
  - 恶意的云租户
  - 内部安全责任事故
- 外部威胁
  - 远程的攻击者
  - 自然灾害
  - 安全事故

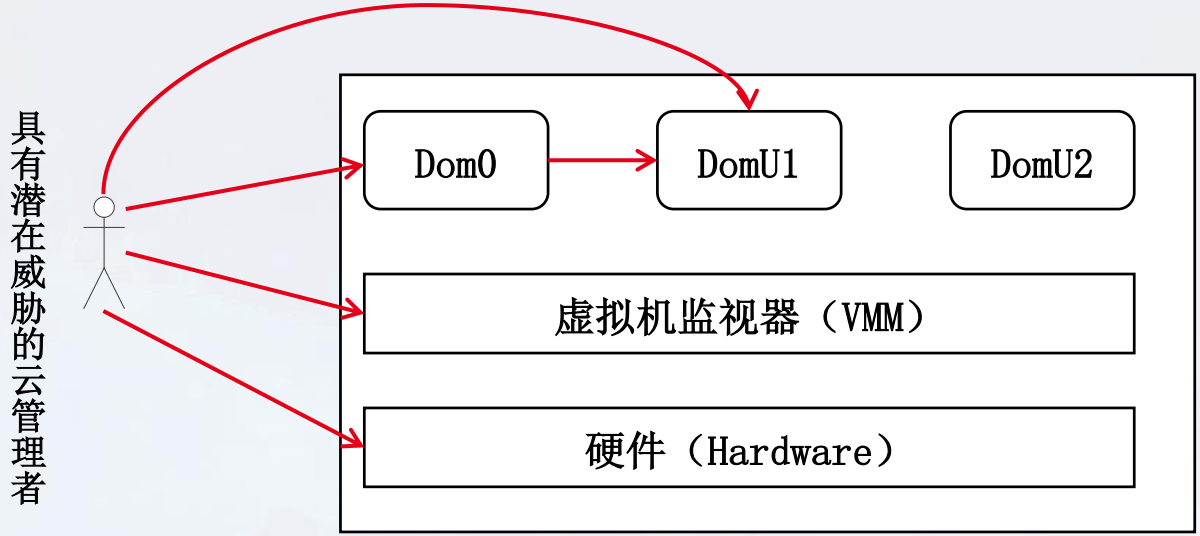
云环境安全威胁模型


恶意云租户
远程攻击者
具有潜在威胁的云管理者
恶意的云管理者
1
2
3
4
5
6
7
8
9
10
管理
虚拟机
客户
虚拟机
客户
虚拟机
客户
虚拟机
客户
虚拟机
管理
虚拟机
虚拟机监视器
虚拟机监视器
硬件
硬件

内部威胁

来自具有潜在威胁的云管理者的威胁

具有潜在威胁的云管理者拥有管理虚拟机和客户虚拟机的访问权限，他们的操作不当可能导致云服务中断或者用户数据丢失，篡改或泄露

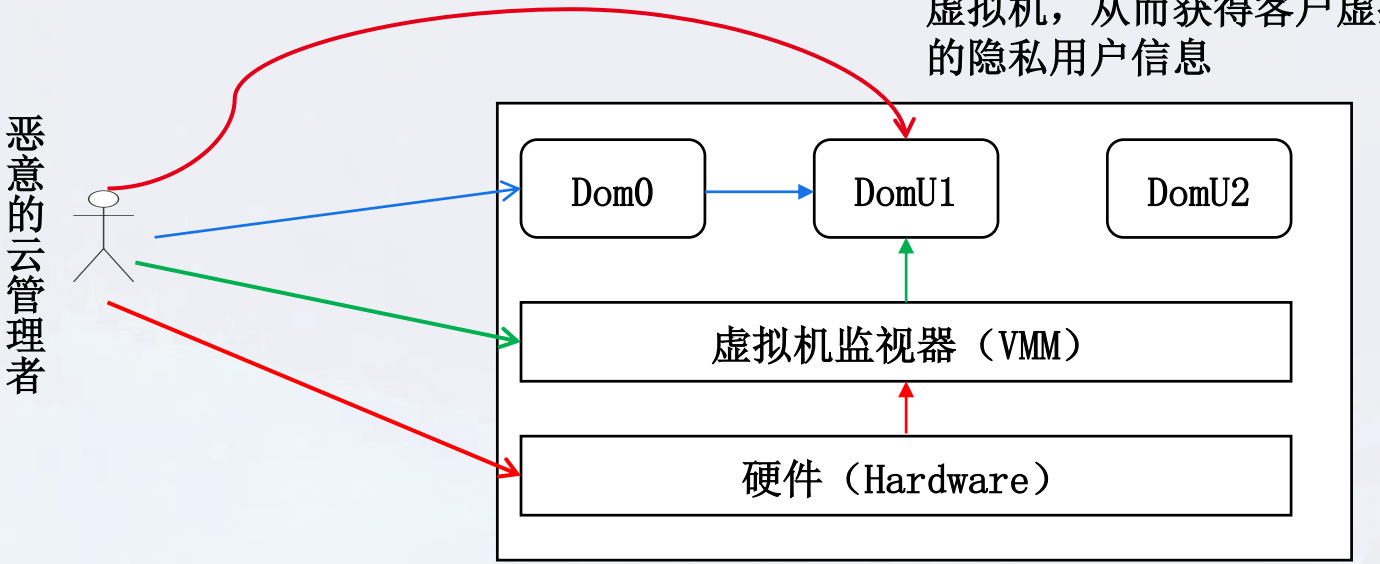


具有潜在威胁的云管理者也有能因为操作不当使VMM和硬件设施不能正常工作

内部威胁

来自具有恶意的云管理者的威胁

恶意的云管理者可以通过访问管理虚拟机来访问或控制客户虚拟机，从而获得客户虚拟机的隐私用户信息



恶意的云管理者可以利用部署在虚拟机监视器上VMI工具来获得用户的隐私信息或者通过修改配置文件来创建一个新的客户虚拟机或暂停、关闭正在运行的客户虚拟机

恶意的云管理者可以直接访问硬件，从而控制虚拟机监视器，进而发起更多的攻击

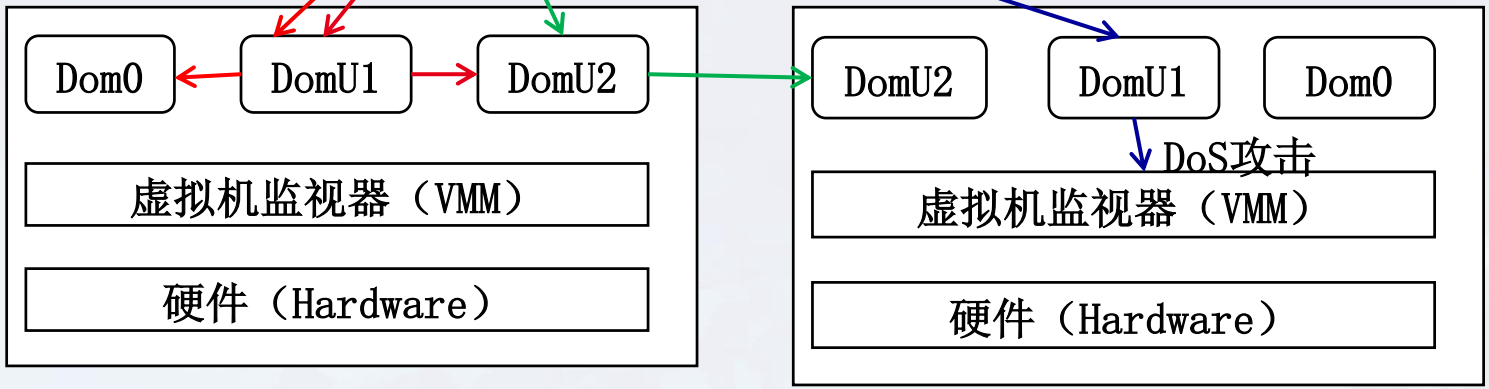
内部威胁

来自恶意云租户的威胁

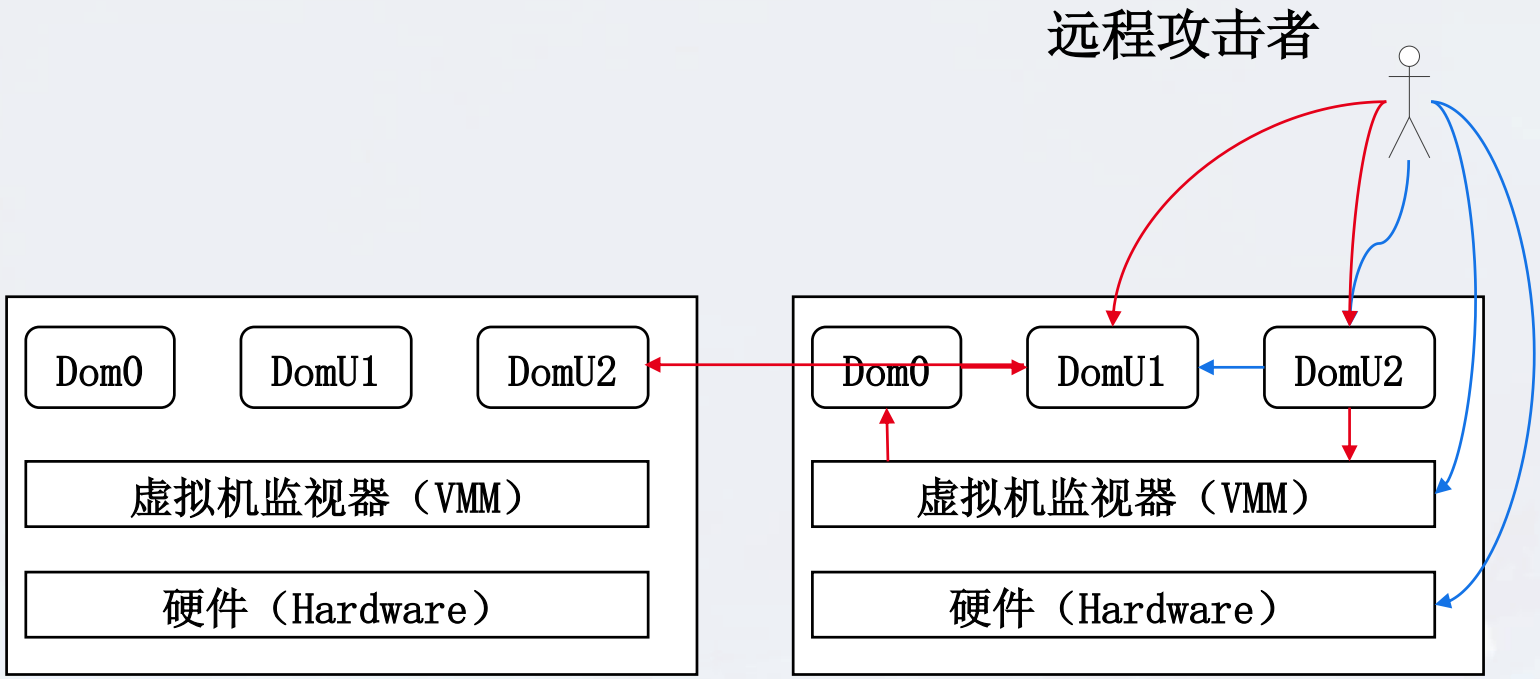
恶意云租户

恶意云租户可以利用侧信道对其它虚拟机发动跨虚拟机攻击；也可以利用虚拟机漏洞，攻击位于不同物理机上的虚拟机

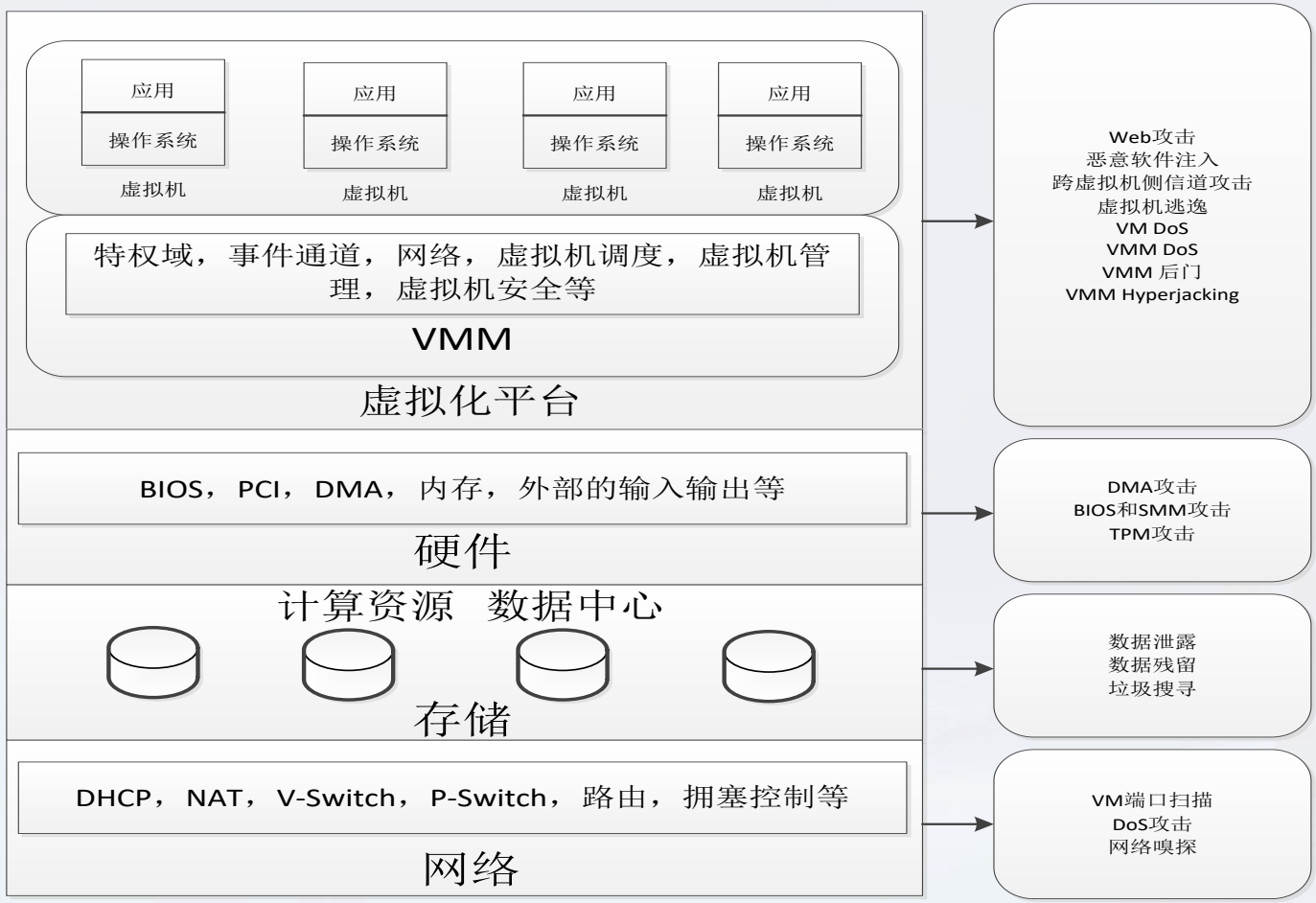
虚拟机逃逸



来自于远程攻击者的外部威胁



云面临的攻击


应用
操作系统
虚拟机
应用
操作系统
虚拟机
应用
操作系统
虚拟机
应用
操作系统
虚拟机
特权域，事件通道，网络，虚拟机调度，虚拟机管理，虚拟机安全等
VMM
虚拟化平台
BIOS，PCI，DMA，内存，外部的输入输出等
硬件
计算资源 数据中心
存储
DHCP，NAT，V-Switch，P-Switch，路由，拥塞控制等
网络
Web攻击
恶意软件注入
跨虚拟机侧信道攻击
虚拟机逃逸
VM DoS
VMM DoS
VMM 后门
VMM Hyperjacking
DMA攻击
BIOS和SMM攻击
TPM攻击
数据泄露
数据残留
垃圾搜寻
VM端口扫描
DoS攻击
网络嗅探

网络空间威胁发生变化

- 攻击目标迁移
  - ✓ 转向云
  - ✓ 转向端
  - ✓ 转向关键基础设施
  - ✓ 转向高价值目标
  - ✓ 转向数据
- 攻击方式
  - ✓ 精准化
  - ✓ 隐蔽化
  - ✓ 智能化
  - ✓ 创新化
  - ✓ 复合化（物理与网络、社工相结合）
  - ✓ 持续化

寒夜速纪

威胁框架：认知与实践

04 云相关的关键信息基础设施保护

我国高度重视网络安全工作

4.19讲话

- 加快构建关键信息基础设施安全保障体系。

十九大报告

- 网络强国

网络安全法

- 共七章 七十九条

国家网络空间安全战略

- 四个方面

关键信息基础设施安全保护条例（征求意见稿）

- 共六章 五十九条

网络安全等级保护条例（征求意见稿）

- 共八章 七十三条

关基运营者的责任

第四章 运营者安全保护

第二十一条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第二十二条 运营者主要负责人是本单位关键信息基础设施安全保护工作第一责任人，负责建立健全网络安全责任制并组织落实，对本单位关键信息基础设施安全保护工作全面负责。

第二十三条 运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障关键信息基础设施免受干扰、破坏或者未经授权的访问，防止网络数据泄漏或者被窃取、篡改：

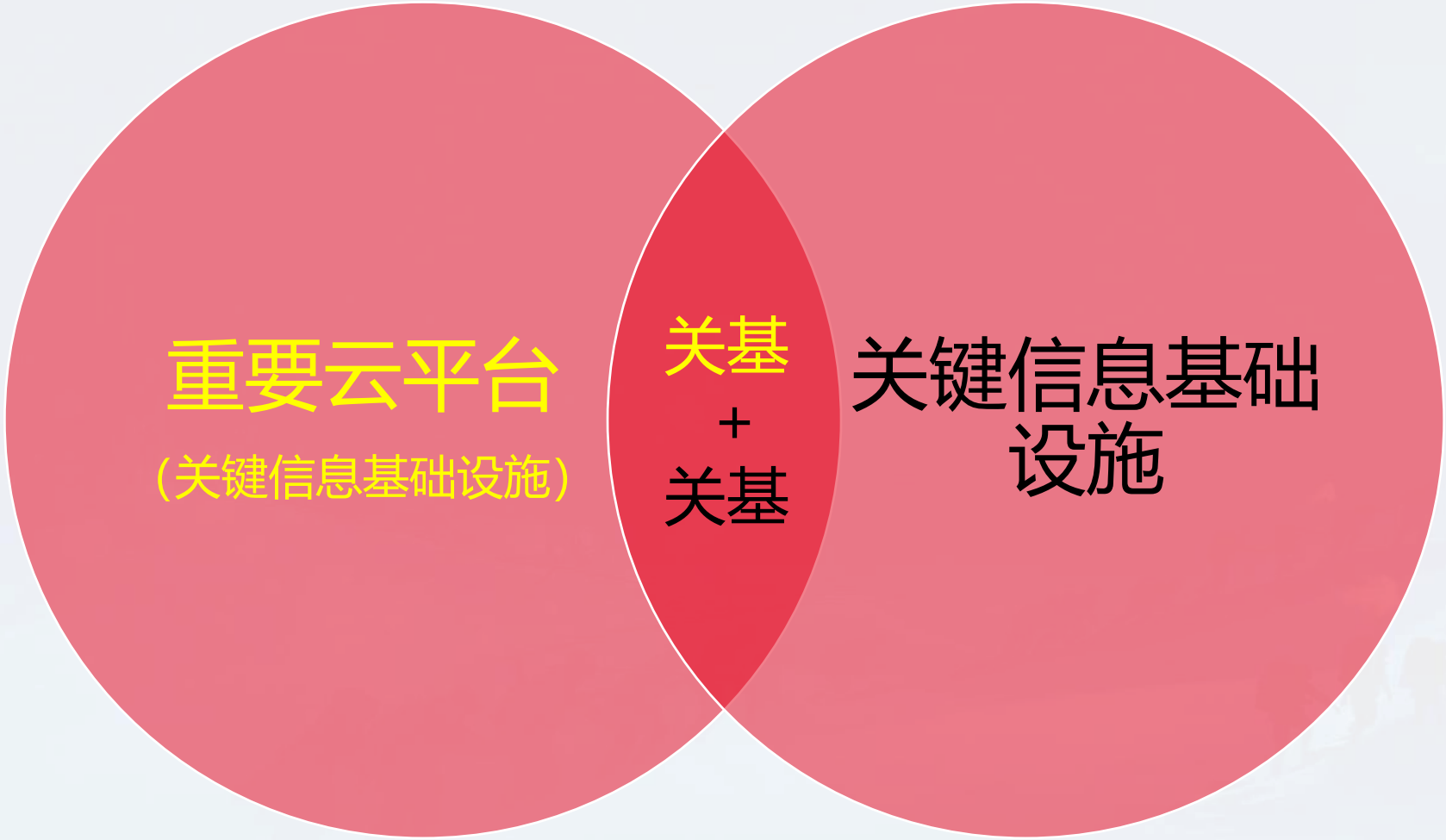
（一）制定内部安全管理制度和操作规程，严格身份认证和权限管理；

（二）采取技术措施，防范计算机病毒和网络攻击、网络侵入等危害网络安全行为；

（三）采取技术措施，监测、记录网络运行状态、网络安全事件，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密认证等措施。

云相关的关键信息基础设施



中美云安全发展进程


美国 云计算
2005 年 概念兴起
05-09 年 技术驱动
08-10 年 广泛应用
至今 高速发展
滞后 3-4 年
美国 云安全
2009 年 概念兴起
10-12 年 政策催化
13-14 年 技术趋熟
至今 高速发展
CSA 成立
《云安全指南 1.0》
2011.06 BSI
《云计算提供商安全建议白皮书》
2011.11 CSA
《云安全指南 3.0》
2012.04 ENISA
《云计算安全服务水平检测指南》
2010 IBM
云安全解决方案
2011 趋势科技
云保护战略
2012-2014
大量初创云安全公司成立、新技术融入云安全平台
截止 2018 年
全球云安全市场规模达到 60 亿美元
预计到 2021 年超过 100 亿美元
中国 云安全
2011 年 概念兴起
12-13 年 技术驱动
14-17 年 全面布局
18 年至今 高速发展
仅限于 P2P 技术的杀毒软件应用
云计算市场技术成熟
公有云厂商渐成规模
完善云计算基础设施服务催生云安全市场
阿里、华为、百度、腾讯等公有云全面布局云安全、云安全服务落地
2014 中国电信
电信云堤推出，抗 DDoS 压制与清洗
2014 阿里云
《阿里云安全白皮书 1.0》
2013-2016
大量初创云安全公司成立
云安全生态逐渐形成
初创公司与公有云安全厂商竞合关系逐步形成

NIST Cloud Computing Related Publications

NIST Special Publication 500 Series:

NIST Special Publication 500-291 version 2, NIST Cloud Computing Standards Roadmap, July 2013

NIST Special Publication 500-291, NIST Cloud Computing Standards Roadmap, July 2011

NIST Special Publication 500-292, NIST Cloud Computing Reference Architecture, September 2011

NIST Special Publication 500-293, US Government Cloud Computing Technology Roadmap, Volume I and Volume II, October 2014

NIST Special Publication 500-299, NIST Cloud Computing Security Reference Architecture (Draft)

NIST Special Publication 500-316, Framework for Cloud Usability, December 2015

NIST Cloud Computing Related Publications

NIST Special Publication 800 Series:

NIST Special Publication 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, June 2010

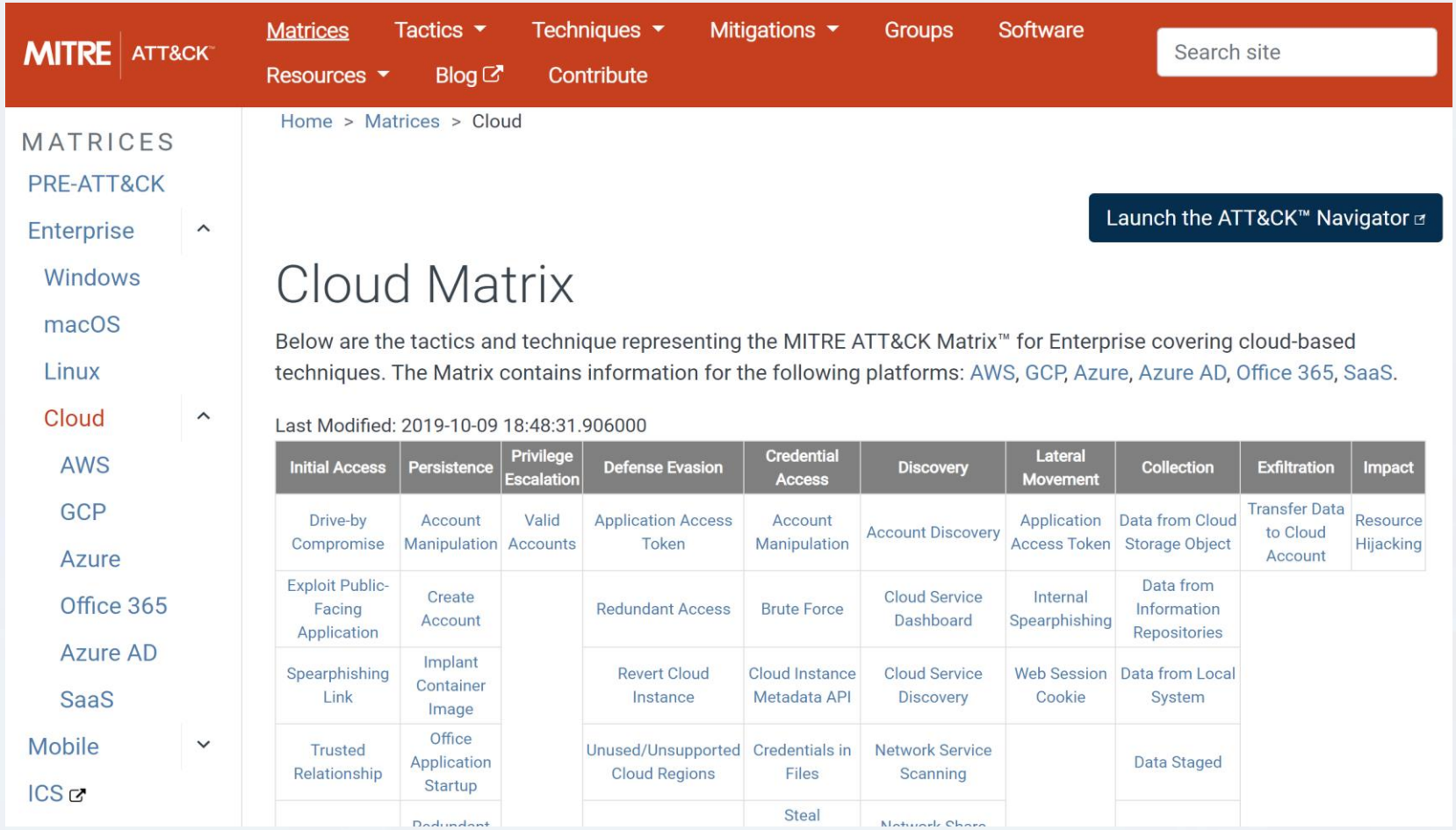
NIST Special Publication 800-125, Guide to Security for Full Virtualization Technologies, January 2011

NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011

NIST Special Publication 800-145, NIST Definition of Cloud Computing, September 2011

NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations, May 2012

ATT&CK for Cloud



MITRE | ATT&CK

Matrices | Tactics | Techniques | Mitigations | Groups | Software | Resources | Blog | Contribute | Search site

MATRICES
- PRE-ATT&CK
- Enterprise
  - Windows
  - macOS
  - Linux
  - Cloud
    - AWS
    - GCP
    - Azure
    - Office 365
    - Azure AD
    - SaaS
- Mobile
- ICS

Home > Matrices > Cloud

Launch the ATT&CK™ Navigator

Cloud Matrix

Below are the tactics and technique representing the MITRE ATT&CK Matrix™ for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation	Account Discovery	Application Access Token	Data from Cloud Storage Object	Transfer Data to Cloud Account	Resource Hijacking
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force	Cloud Service Dashboard	Internal Spearphishing	Data from Information Repositories		
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API	Cloud Service Discovery	Web Session Cookie	Data from Local System		
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files	Network Service Scanning		Data Staged		
	Redundant			Steal	Network Share				

加强了党政部门云安全管理

四部委发布《云计算服务安全评估办法》

第一条 为提高党政机关、关键信息基础设施运营者采

第二条 云计算服务安全评估坚持事前评估与持续监督和政策规定，参照国家有关网络安全标准，发挥专业技（以下简称“云平台”）的安全性、可控性，为党政机

本办法中的云平台包括云计算服务软硬件设施及其相

第三条 云计算服务安全评估重点评估以下内容：

（一）云平台管理运营者（以下简称“云服务商”）

（二）云服务商人员背景及稳定性，特别是能够访问

（三）云平台技术、产品和服务供应链安全情况；

（四）云服务商安全管理能力及云平台安全防护情况

（五）客户迁移数据的可行性和便捷性；

（六）云服务商的业务连续性；

（七）其他可能影响云服务安全的因素。

中华人民共和国财政部

Ministry of Finance of the People's Republic of China 国库司（政府采购管理办公室、国库支付中心）

2019年10月11日 星期五 关键字 国库司 搜索 高级检索 返回主站

当前位置：首页>政务信息>规章制度

关于发布《云计算服务安全评估办法》的公告

2019年第2号

为提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部制定了《云计算服务安全评估办法》，现予以发布。

附件：云计算服务安全评估办法

国家互联网信息办公室 国家发展和改革委员会

工业和信息化部 财政部

2019年7月2日

附件下载：云计算服务安全评估办法

【大 中 小】【打印此页】【关闭窗口】

培育形成良好的云安全生态

网络和基础设施安全

主机和终端节点安全性

数据保护和加密

监管、风险与合规性（技术合作伙伴）

日志记录、监控、威胁检测和分析

身份和访问控制

漏洞和配置分析

应用程序安全

咨询合作伙伴

安全工程

监管、风险与合规性

安全运营与自动化

CNCERT关于云平台安全建议

- 云服务商和云用户应加大对网络安全的重视和投入，分工协作提升网络安全防范能力。（各打五十大板）
  - 云服务商应提供基础性的网络安全防护措施并保障云平台安全运行，全面提高云平台的安全性和可控性，全面加强网络安全事件监测和处置能力。
  - 云用户对部署在云平台上的系统承担主体责任，需全面落实系统的网络安全防护要求。

摘自：《2019年上半年我国互联网网络安全态势》

云相关的关键信息基础设施保护

- 统筹协调云相关的关键信息基础设施保护工作（加强组织领导）
- 加强国家监测、防御、处置工作（发挥国家力量）
- 明确各方责任（制度文件和标准）
- 加强对云服务的第三方监管（监督检查）
- 提高云服务商和云用户自身监管能力（举证能力）
- 提升云安全防护技术能力（创新产品和服务）
- 加强云安全技术的研究（提升防护对抗能力）

寒夜速纪

威胁框架：认知与实践

05 我们开展的工作

建立行业会商机制

网络安全态势行业会商机制

2018年7月，协会组织网络安全态势感知专题研讨会，会上研究确定建立网络安全态势研判行业会商机制，该机制得到了主管部门的高度肯定。

成立研判工作组

研判工作组
成员单位
（16家）

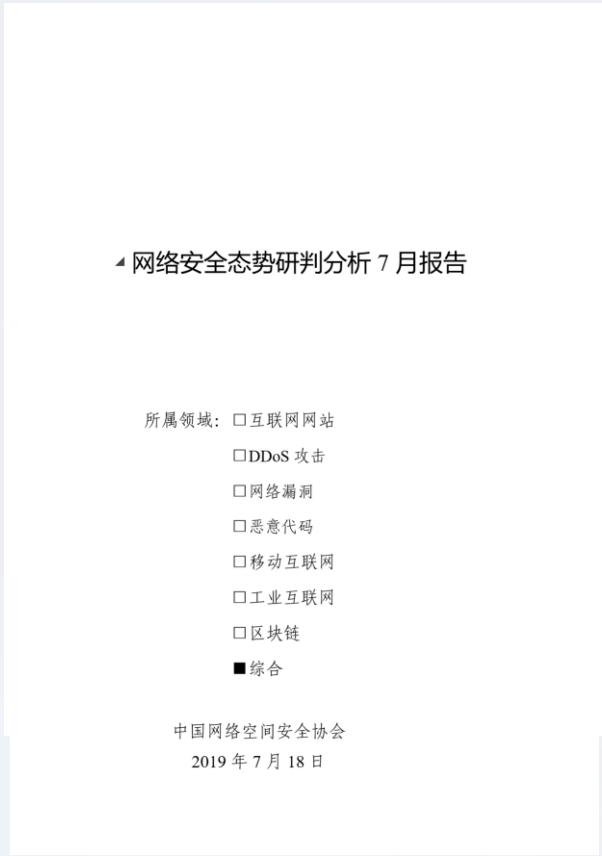
南开大学、北京邮电大学、天津理工大学

安天、 360、阿里、安恒、
恒安嘉新、美亚柏科、绿盟

任子行、深信服、网宿科技、
锐安科技、南京烽火、启明星辰

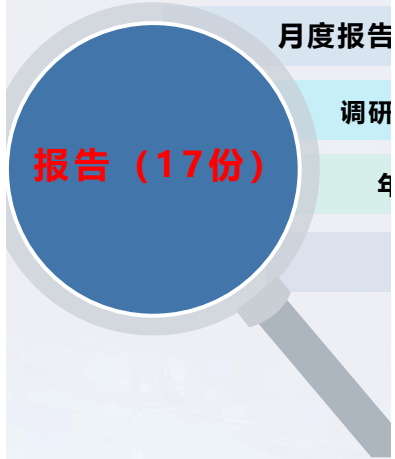
组织网络安全态势感知分析研判

编制报告


网络安全态势研判分析 7 月报告

所属领域：☐互联网网站
☐DDoS 攻击
☐网络漏洞
☐恶意代码
☐移动互联网
☐工业互联网
☐区块链
■综合

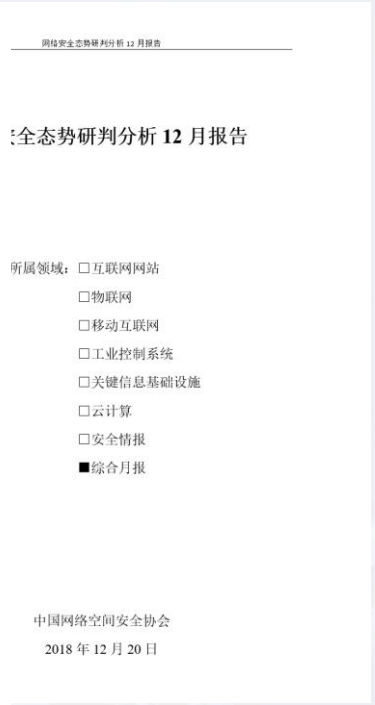
中国网络空间安全协会
2019 年 7 月 18 日




网络安全态势研判分析 2018 下半年度
综合报告

所属领域：☐互联网网站
☐物联网
☐移动互联网
☐工业控制系统
☐关键信息基础设施
☐云计算
☐安全情报
■综合报告

中国网络空间安全协会
2018 年 12 月 20 日


网络安全态势研判分析 12 月报告

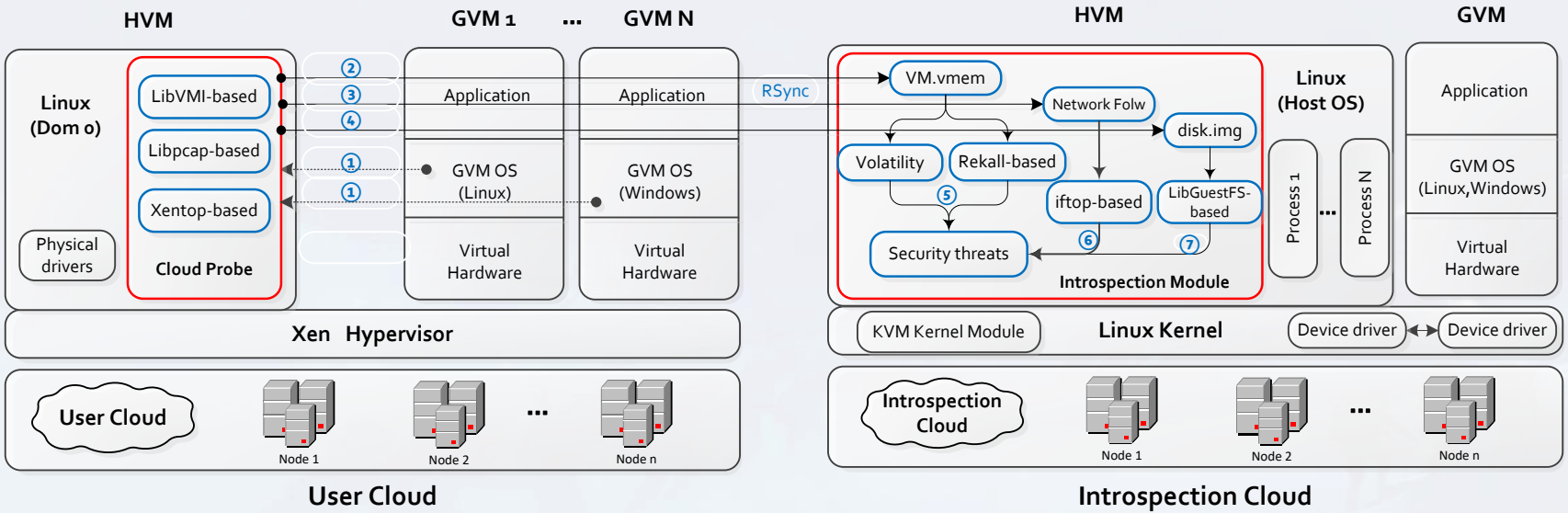
全态势研判分析 12 月报告

所属领域：☐互联网网站
☐物联网
☐移动互联网
☐工业控制系统
☐关键信息基础设施
☐云计算
☐安全情报
■综合月报

中国网络空间安全协会
2018 年 12 月 20 日

提出基于云探针的自省云架构

基于云计算平台，采用虚拟机自省技术，通过云探针实现对用户云的监测分析。



基于带外动态多特征的恶意软件检测

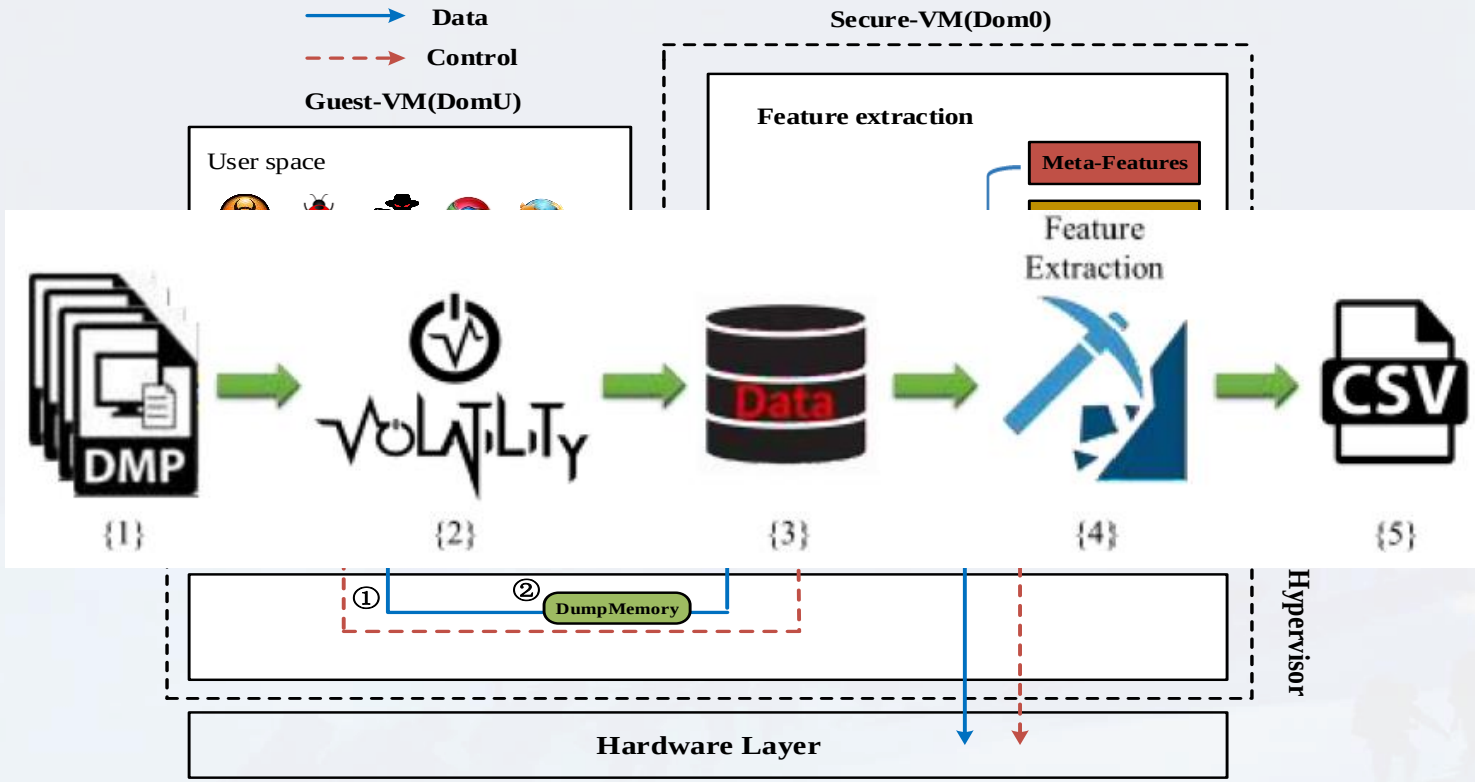


Figure 1. Feature extraction process.

网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

请批评指正！

寒夜远征

威胁框架：认知与实践