



# Lecture 17: 云计算安全

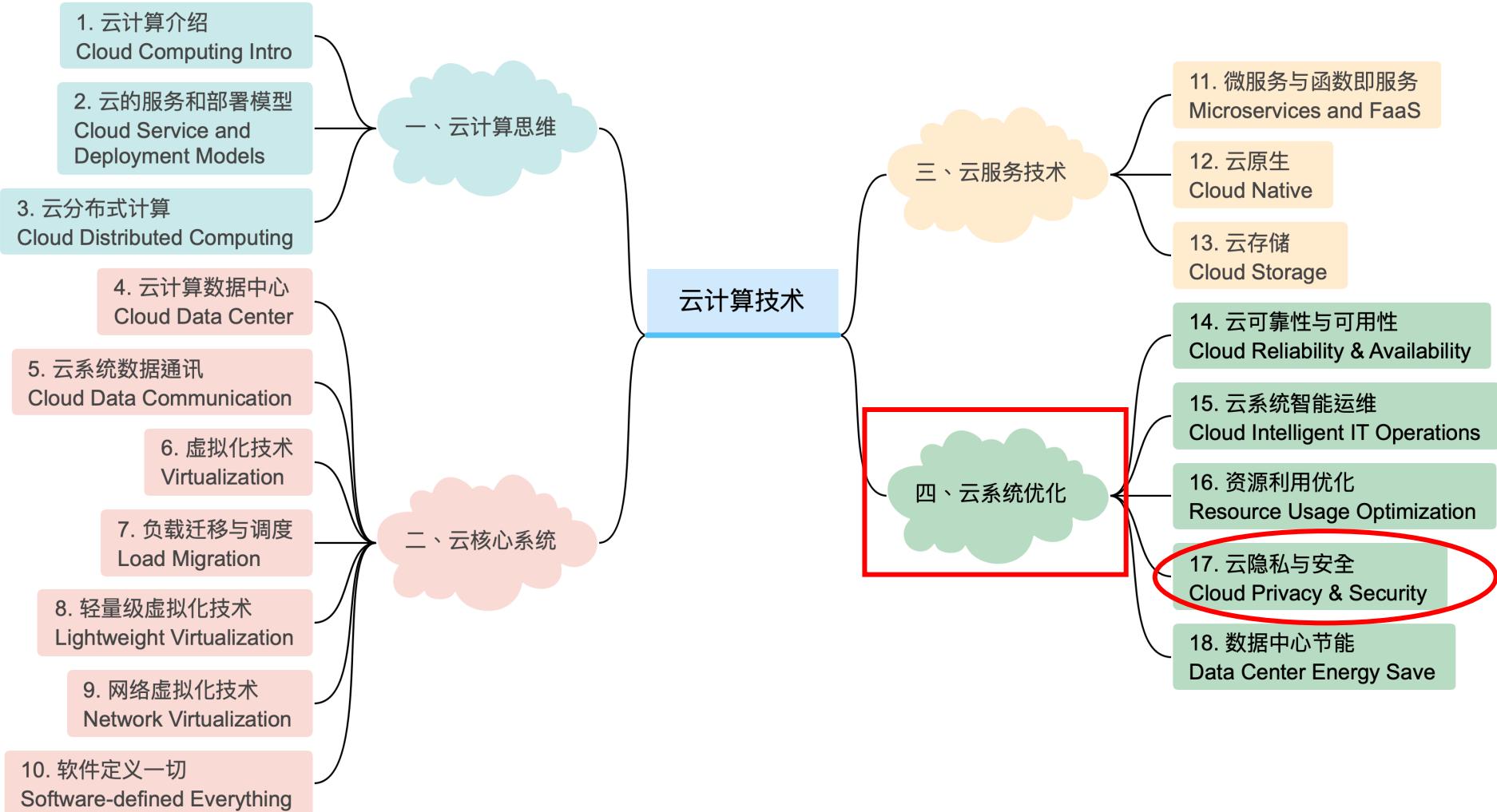
SSE316: 云计算技术  
Cloud Computing Technologies

---

陈壮彬

软件工程学院

chenzhb36@mail.sysu.edu.cn



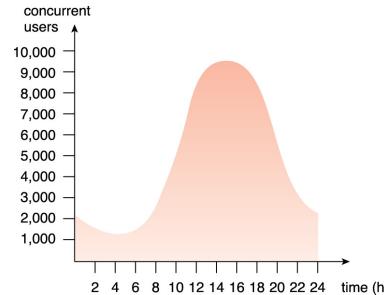
# Today's topics

□ 云计算安全

□ 性能攻击

# 云计算的优势

□ 更低的 IT 初始/运营成本 (Pay-as-you-go)



□ 可扩展性和灵活性



□ 更高的可用性与可靠性 (数据备份, 自动系统运维)



□ ...

# 使用云计算的顾虑

如果云计算这么好，为什么  
不是人人都用呢？



安全和隐私是用户  
最大的顾虑！

# 新技术早期顾虑

- 口人们对新技术通常会有很多担忧
- 口在云计算中，用户对要把数据运行在第三方平台存在顾虑
- 口然而，随着时间的推移，这种担忧逐渐消失，特别是对价值追求的意向足够强大时

# ChatGPT 存在类似的顾虑

- 2023年4月10日：Yoshua Bengio 和马斯克一起，联合众多科学家签署了关于“**暂停6个月 AI 大模型研究**”的呼吁申请
- Andrew Ng 和 Yann LeCun 对此有不同意见

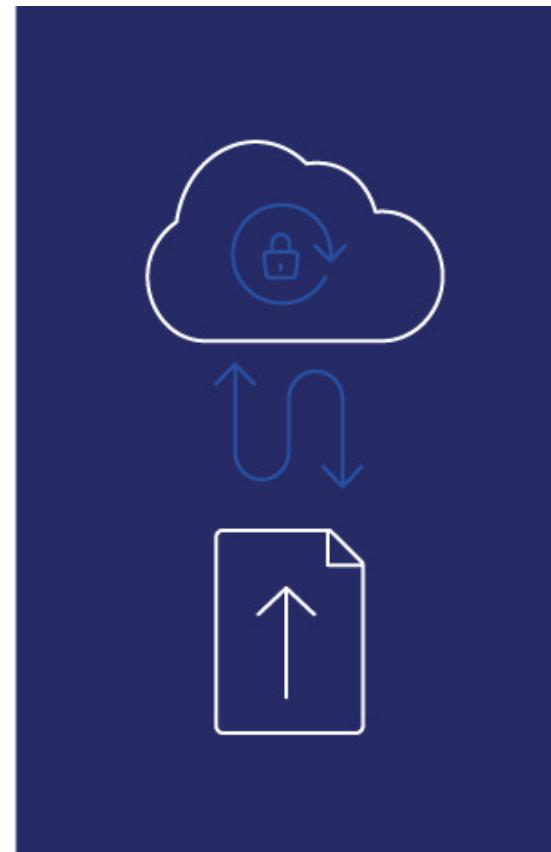
**GPT-5不能停！吴恩达LeCun直播回怼：  
汽车都还没发明要什么安全带**

▷ 播报文章

# 现今云计算安全的表现

□自建数据中心同样存在安全问题！

94% of business claimed saw an improvement in security after switching to the cloud. 91% said it the cloud makes it easier to meet government compliance requirements.



# 然而，云安全问题仍频繁发生

**McDonald's discloses data breach after theft of customer, employee info**

Jun 11, 2021



"While we were able to close off access quickly after identification, our investigation has determined that a small number of files were accessed, some of which **contained personal data including Korea and Taiwan customer data**"

**Audi, Volkswagen data breach affects 3.3 million customers**

Jun 12, 2021

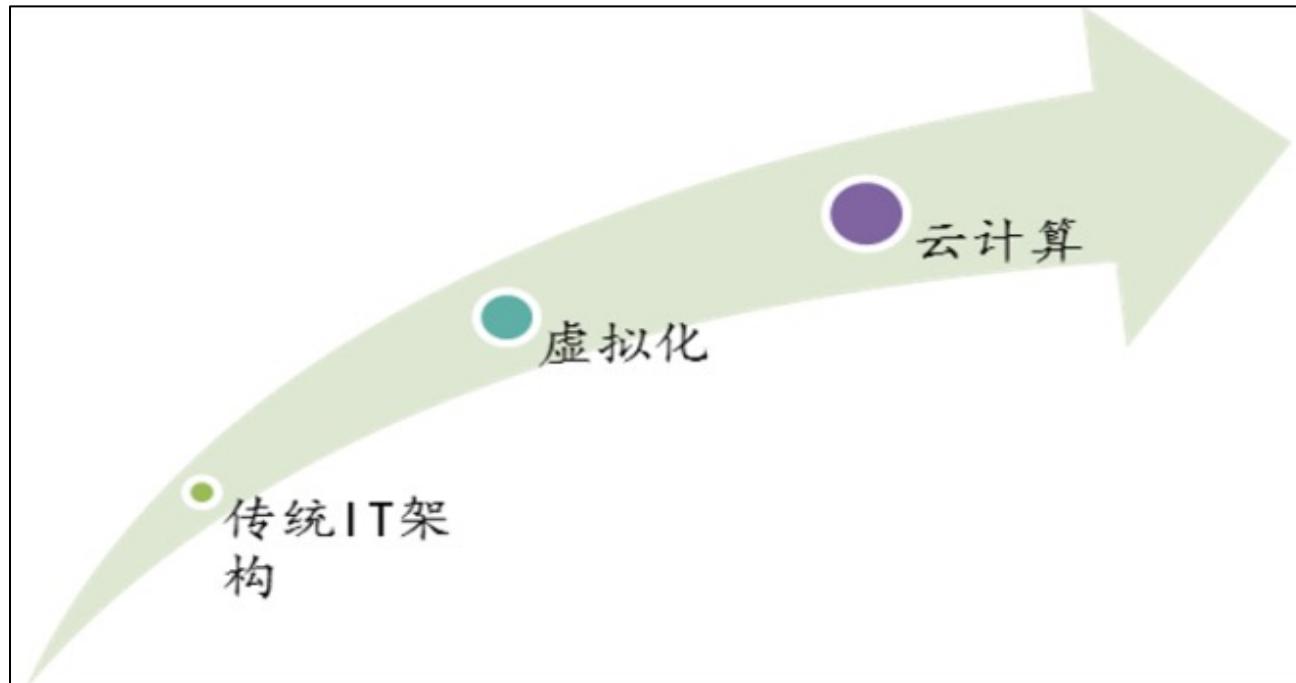


"The data also included more sensitive information relating to eligibility for a purchase, loan, or lease. **More than 95% of the sensitive data** included was driver's license numbers. "

# 信息安全 “云化”

## □ IT 基础架构的改变是信息安全 “云化”的根本原因

- “云安全”的诞生其实是信息安全对“云架构”的适应的结果，可以说是云环境下的信息安全



IT 基础架构的变迁

# 传统 IT 基础架构的信息安全

传统网络安全防护措施主要以网络边界上的防御为主，边界内的主机一般不具有或只具有很弱的防御能力

✓ 边界上的防护措施

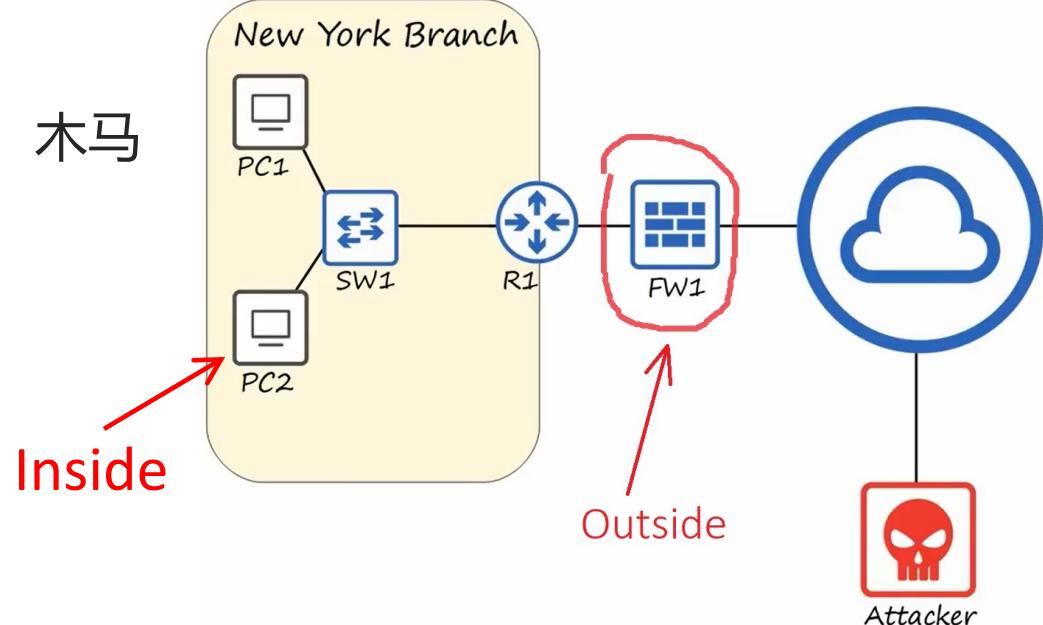
✓ 防火墙

✓ 入侵检测系统 (IDS, Intrusion Detection System)

✓ 入侵防御系统 (IPS, Intrusion Protection System)

✓ 边界内的主机防御

✓ 防恶意软件，如病毒、木马



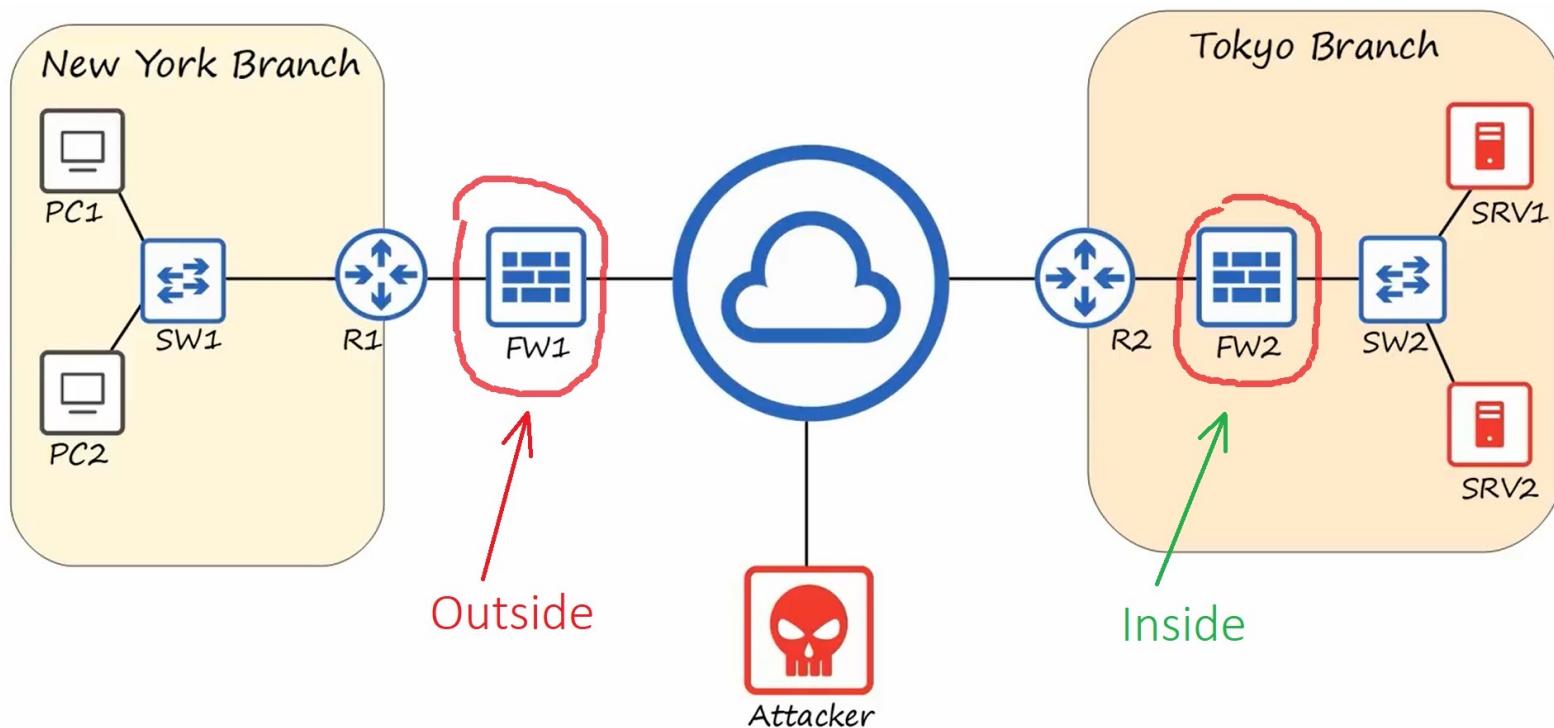
# 传统 IT 基础架构的信息安全

口然而，网络边界上的防护措施并不能阻隔所有的威胁

- ✓ 首先，防火墙自身可能存在**设计上的漏洞**
- ✓ 其次，内部黑客可以**从网络内部发起攻击**
- ✓ 再次，外部的黑客可以通过**绕过防火墙的连接**（如拨号上网）等方式攻入内部网络

# 传统 IT 基础架构的信息安全

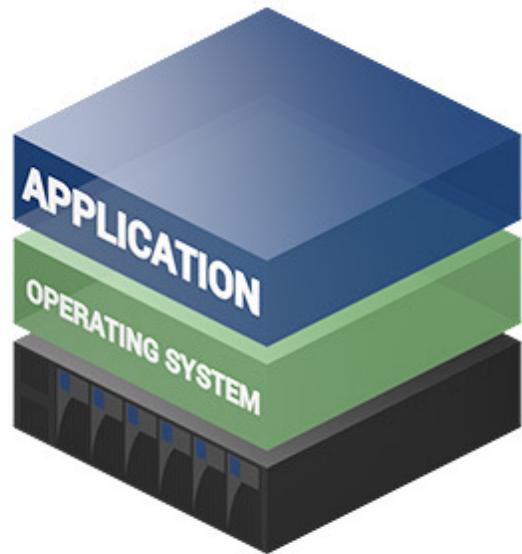
- 必须对边界内的主机进行更深层次的防护，与外部一样采取防火墙、防恶意软件、IDS/IPS的防御方式
- 与网络边界上的安全措施共同组成一个防护网



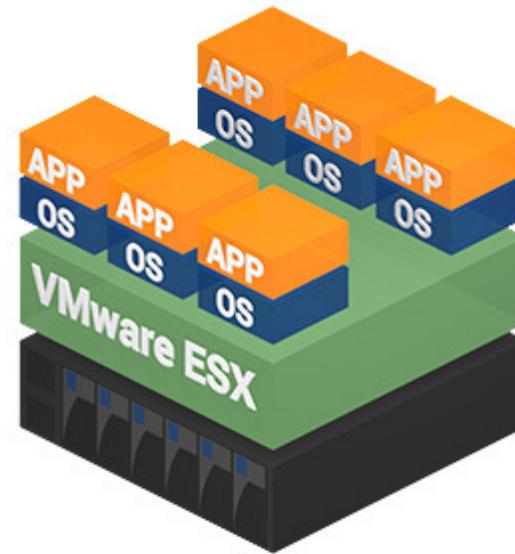
# 虚拟化架构

□ 虚拟化技术的两个关键特点均带来了新的安全威胁

- 多租户 (Multi-tenancy)
- 快速弹性 (Rapid elasticity)



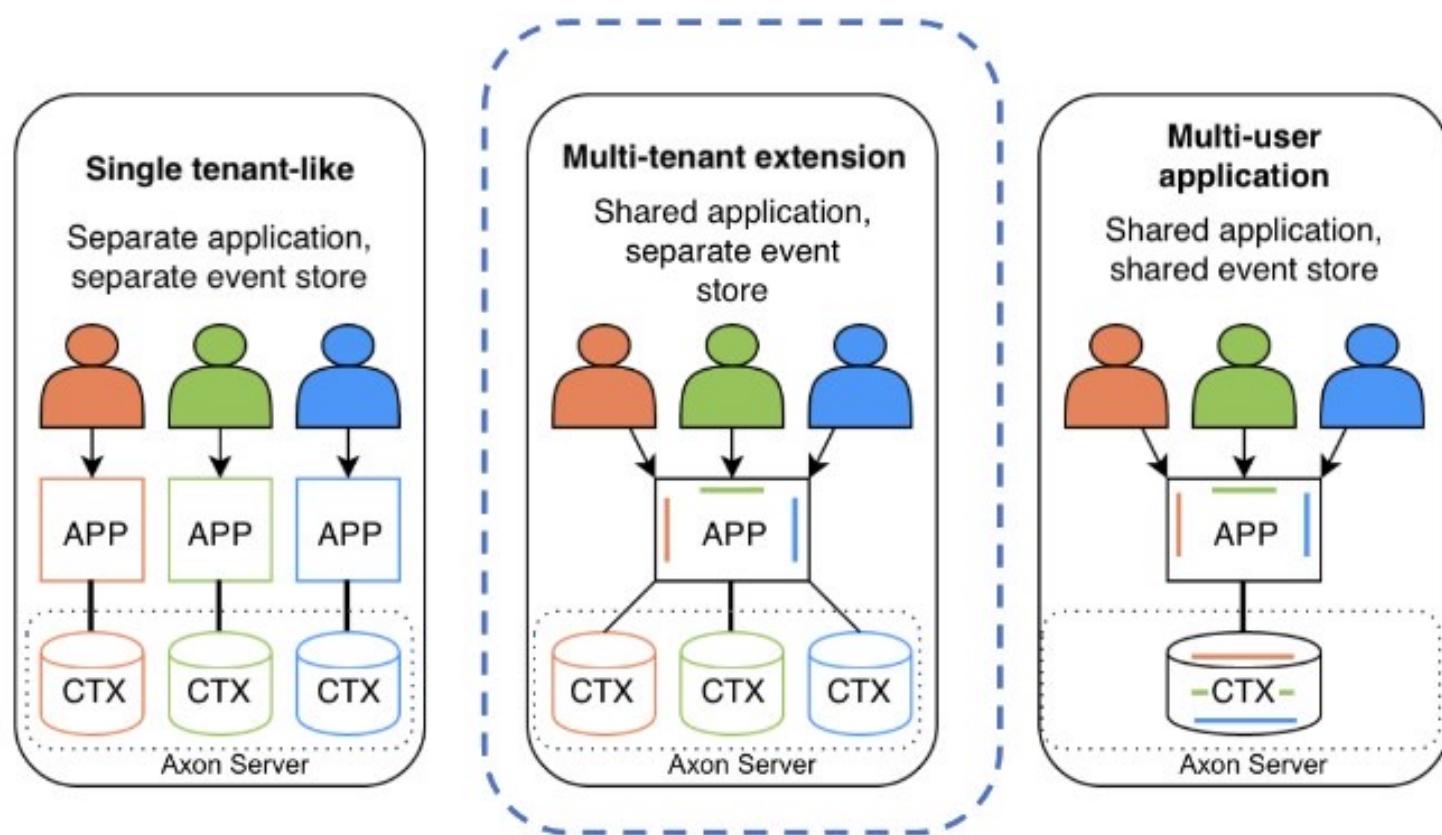
Traditional Architecture



Virtual Architecture

# 多租户带来的威胁

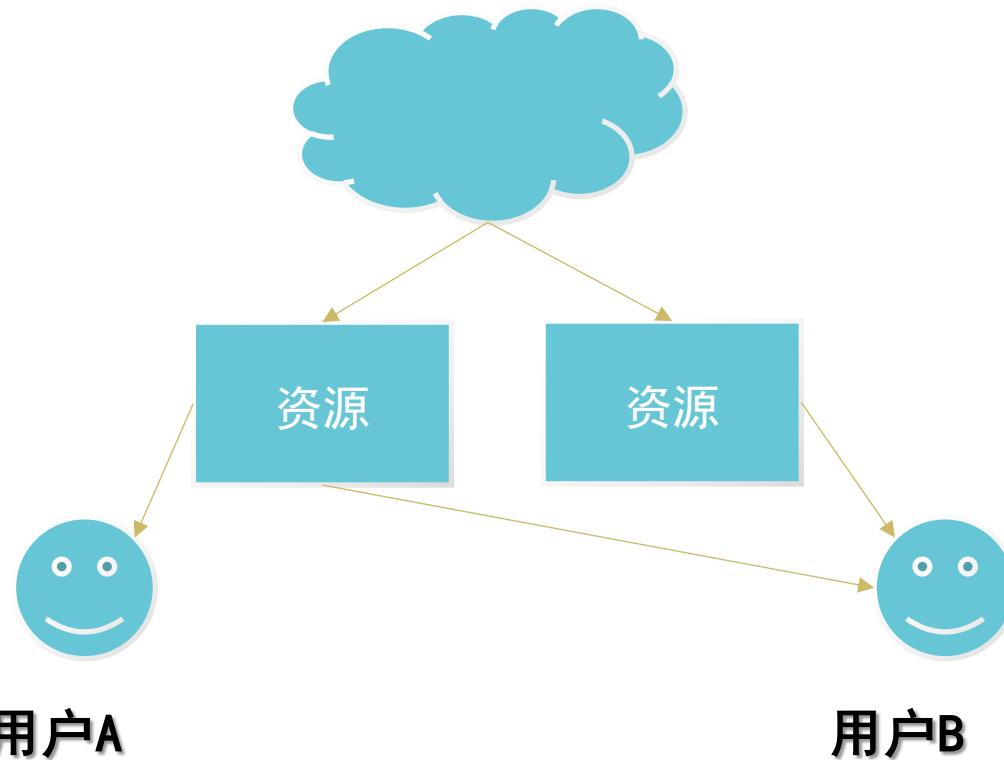
- 口多租户意味着用户之间需要分享**计算/存储资源、服务和应用**
- 口这是有安全风险的，**所有租户同时存在于相同的进程和硬件中**



# 快速弹性带来的威胁

口云服务提供商根据当前的需求动态调整分给每个服务的资源

口这也意味着**租户有机会使用之前被分配给其他租户的资源**，导致信息泄漏



# 虚拟化架构的信息安全问题

安全问题	说明
Hypervisor 安全	(1) Hypervisor 本身代码量巨大、功能结构复杂存在大量已知的和未知的安全漏洞 (2) Hypervisor 承载了大量虚拟机，一旦被攻陷，所有受其管辖的虚拟机都将遭受未授权访问
虚拟机（VM）加固	虚拟机镜像可能存在安全漏洞，易导致用户遭受攻击，云服务提供商应该对虚拟机实施安全加固和保护
不同可信级别的虚拟机混杂	同一个物理机存在多个可信级别的 VM，如果低可信级别的虚拟机遭受攻击，很可能成为对其他高可信级别虚拟机进行进一步攻击的跳板，从而降低整体的安全级别
虚拟机间攻击	多租户环境下，多个用户共享计算、存储、网络等资源，如果某些共享模块存在漏洞，则租户可对其他租户发动攻击
虚拟机盲点	(1) 传统网络流量都会经过路由器和交换机，从而可以对流量进行安全分析和处理，但是通过虚拟化网络传输的流量不经过任何网络设备，从而对安全设备不可见 (2) 同一物理主机上的虚拟机可能通过硬件背板而不是网络进行通信，这些流量的安全性不可见
安全防护过期	当虚拟机被关闭时其配置是安全的，但是一段时间过后被再次启动时，所处环境可能已经发生重大变化，由于虚拟机未更新而导致安全防护过期，产生漏洞
虚拟机蔓延	(1) 由于业务需求保留一定量冗余的虚拟机，或虚拟机在创建时没有经过审核和验证导致不必要的配置，因为不知道这些虚拟机创建的原因，从而不敢删除和回收，不得不任其消耗计算资源； (2) 由于虚拟机生命周期管理流程的缺陷，许多虚拟机镜像文件及其副本依然保存在硬盘上，从而占据大量服务器存储资源
虚拟机镜像安全	虚拟机镜像有被窃取和篡改的脆弱漏洞，且以文件形式存在能够轻易通过网络传输到其他位置
虚拟机迁移安全	(1) 虚拟机在不同的物理服务器之间迁移增加了审计和安全监测的复杂度 (2) 在迁移过程（通道）中，可能发生被盗取和窃听的问题 (3) 一些重要虚拟机可能迁移到不安全的物理服务器上
虚拟机数据安全清除	当虚拟机从一个物理服务器上迁出或用户撤除云服务时，要确保没有任何数据残留在磁盘上从而避免被恶意恢复

资料来源：《云计算信息安全管理——CSA C-STAR 实施指南》，兴业证券研究所

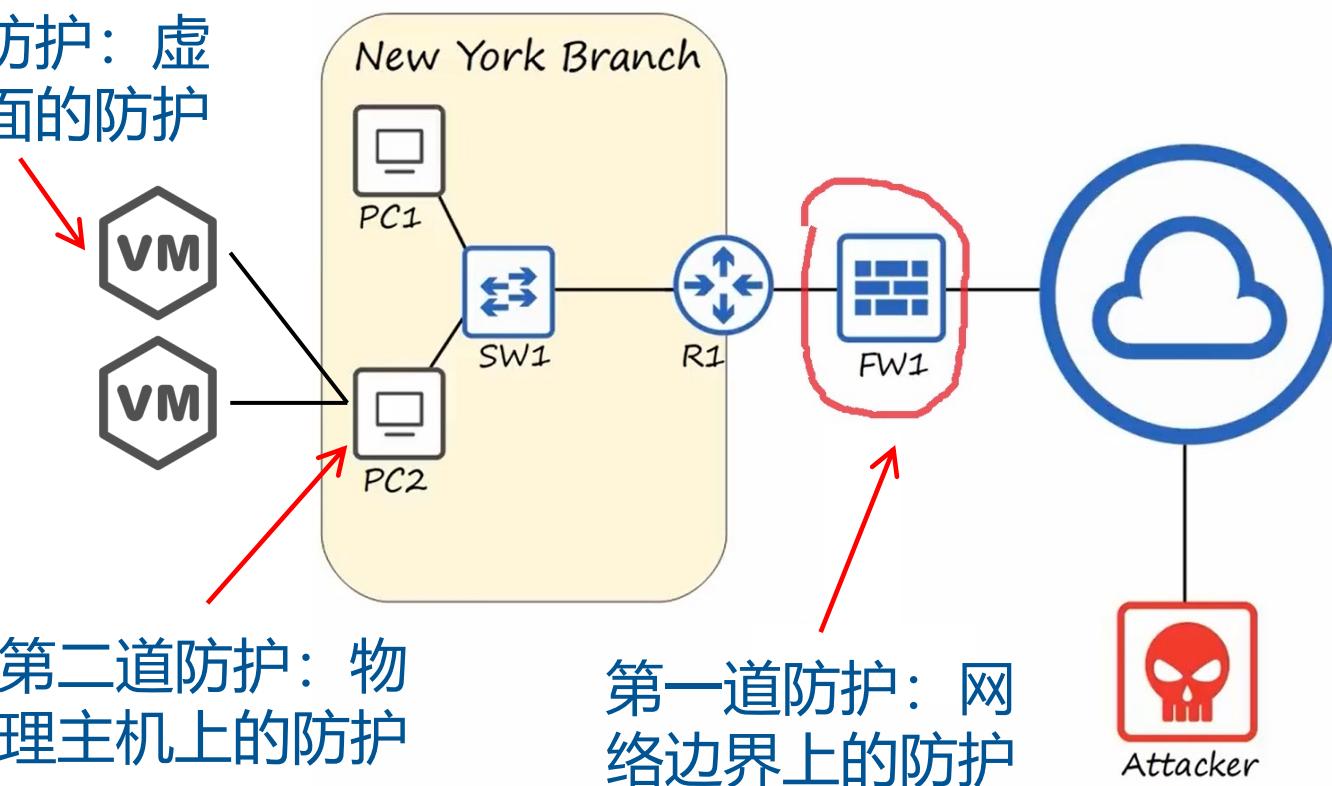
# 虚拟化架构的信息安全问题

安全问题	说明
Hypervisor 安全	(1) Hypervisor 本身代码量巨大、功能结构复杂存在大量已知的和未知的安全漏洞 (2) Hypervisor 承载了大量虚拟机，一旦被攻陷，所有受其管辖的虚拟机都将遭受未授权访问
虚拟机（VM）加固	虚拟机镜像可能存在安全漏洞，易导致用户遭受攻击，云服务提供商应该对虚拟机实施安全加固和保护

# 虚拟化架构的信息安全

□ 安全措施需要覆盖至每一个逻辑主机节点上，即将原来只延伸到物理主机上的防护扩展至每一个虚拟机（VM）上

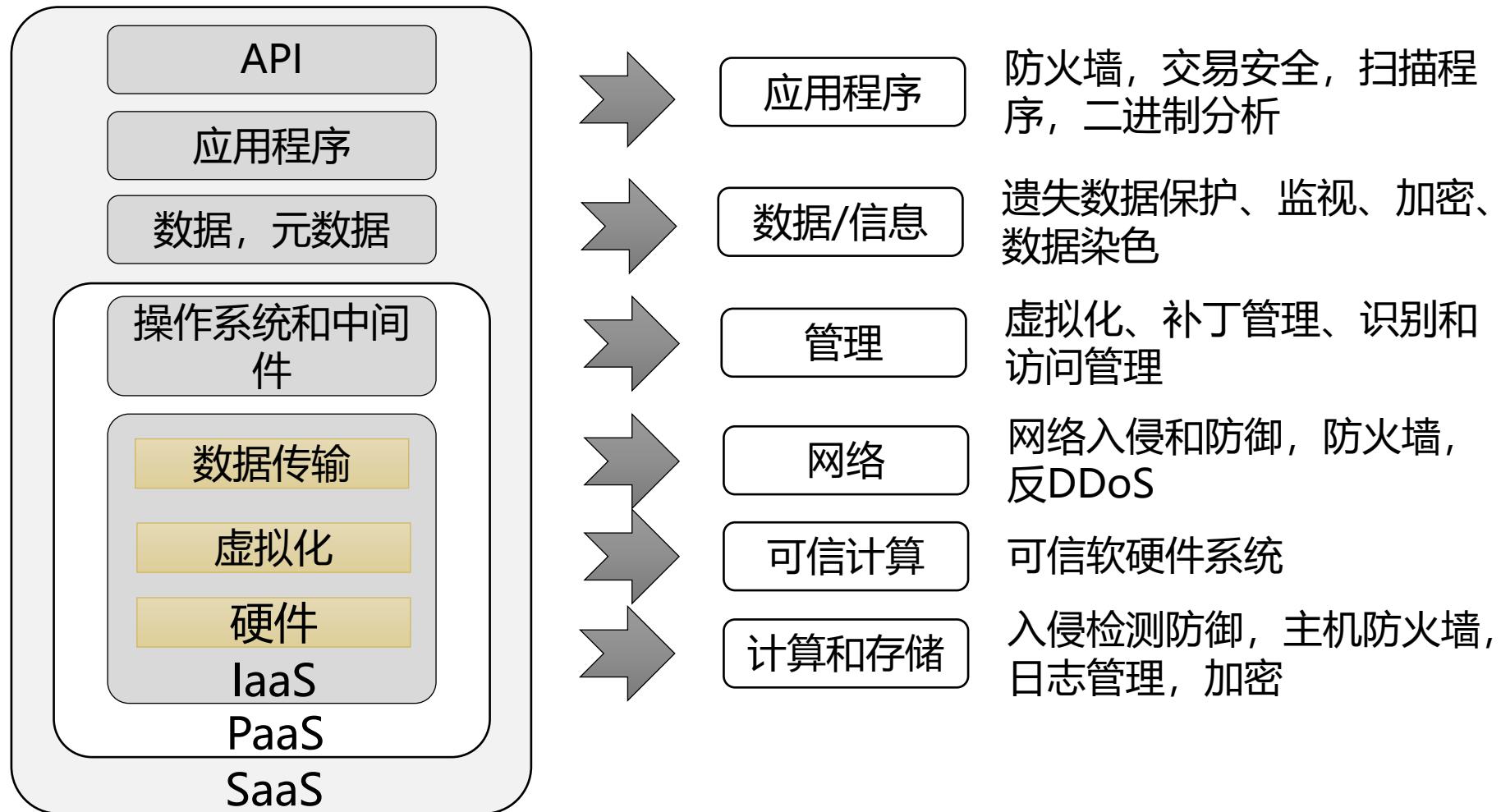
第三道防护：虚  
拟机层面的防护



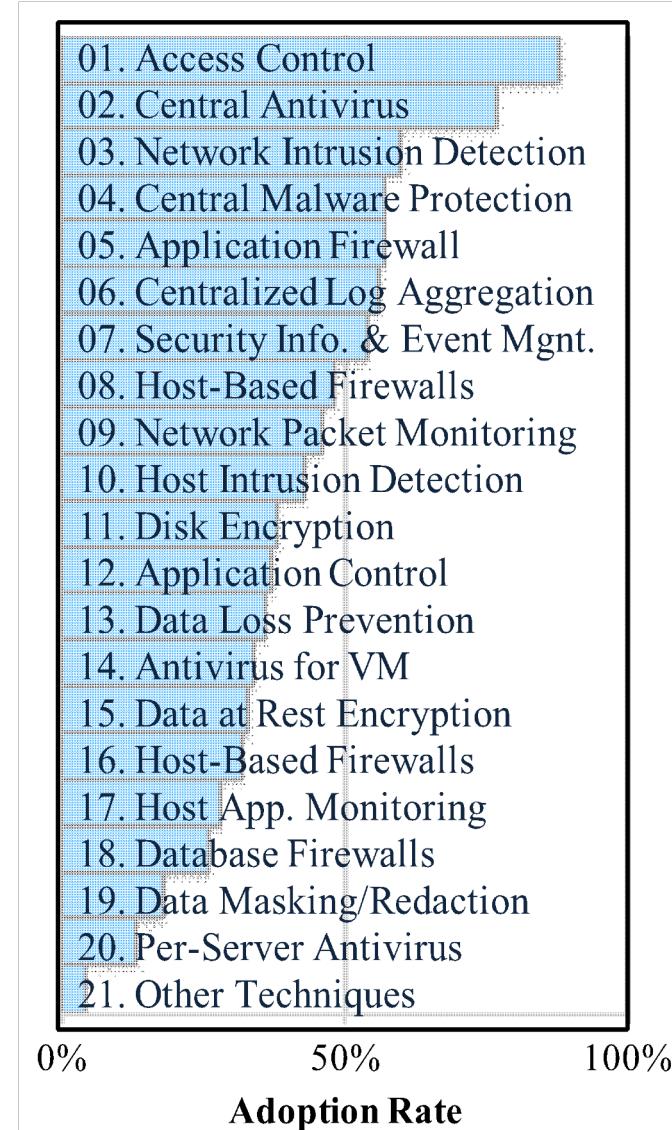
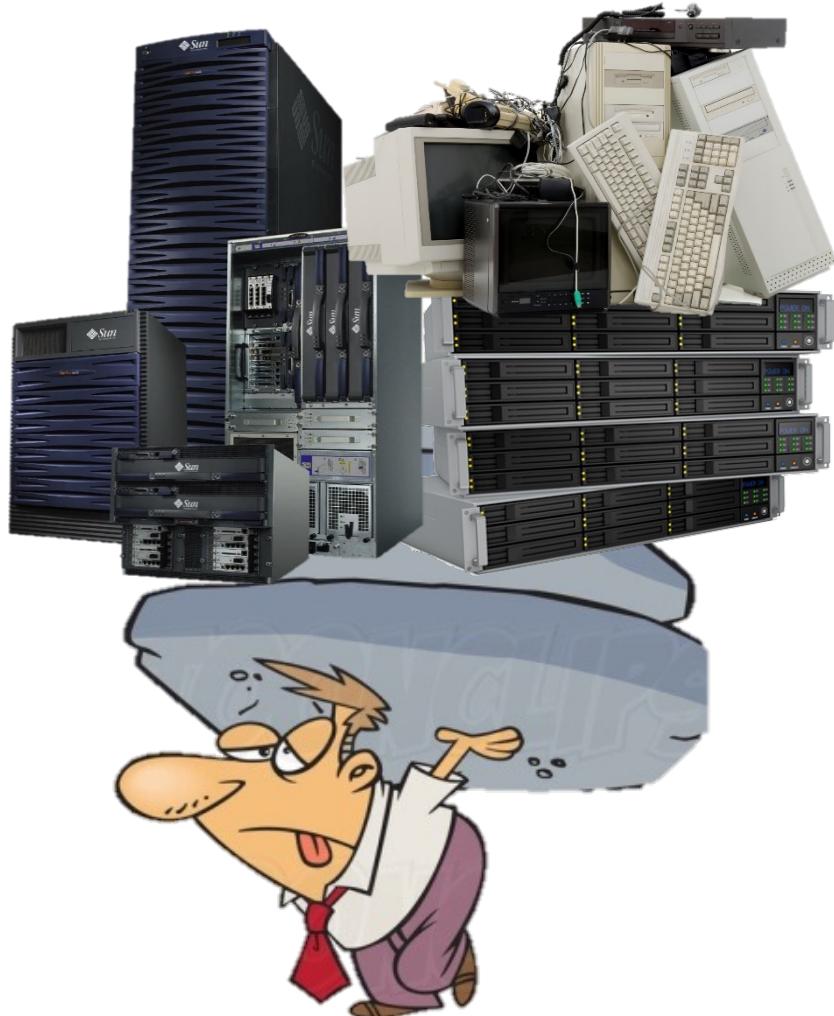
第二道防护：物  
理主机上的防护

第一道防护：网  
络边界上的防护

# 云计算不同层面的安全问题



# 网络空间安全主要技术



# 云计算安全策略

**不管是公有云还是私有云，绝大多数公司在管理云应用安全是需要考虑以下策略**

## 1. 集中化

□ 将一组安全控制、流程、策略和服务进行合并，减少需要管理和实施安全功能的地方

## 2. 标准化

□ 安全应该是一种在整个企业内共享的核心服务，而不是针对某一特定应用的解决方案

## 3. 自动化

□ 一旦将创建环境和部署软件的过程自动化，就能够在自动进行的步骤中落实适当的安全控制和流程

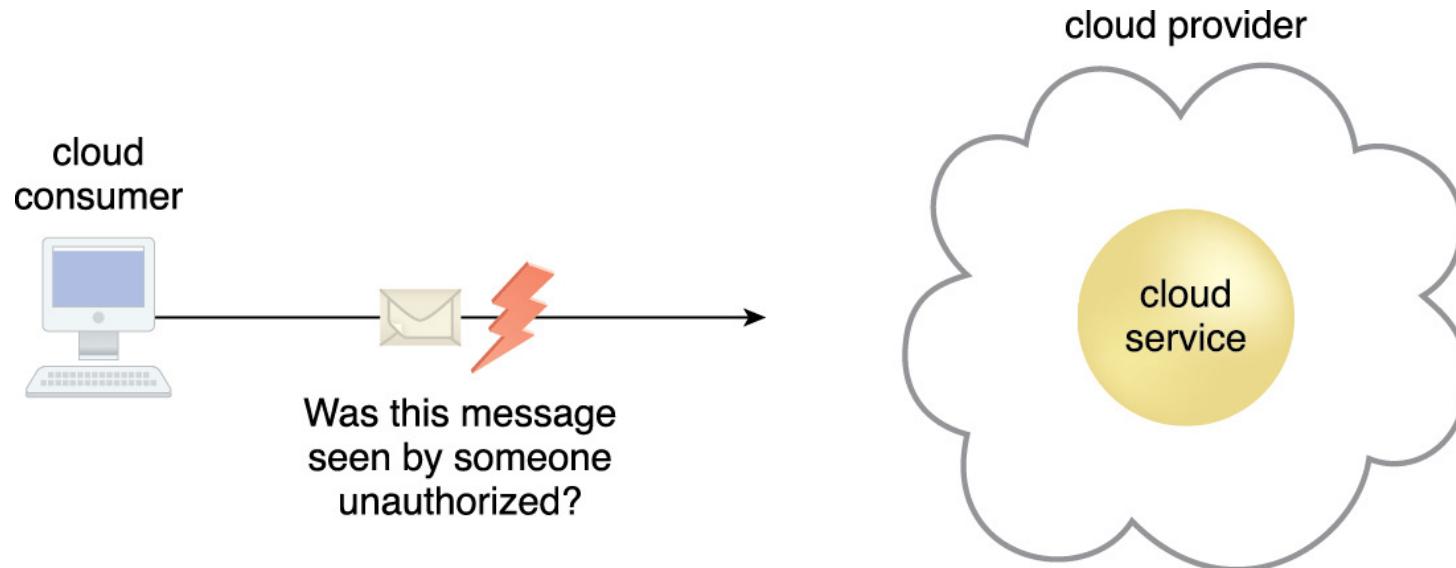
# 信息安全核心三要素

□ 保密性 (Confidentiality) : **事物只有被授权才能访问**

- 在云中，保密性主要是关于对**数据的传输和存储的访问限制**

□ 用户担心的问题

- ✓ 失去对数据的控制 (由于恶意的攻击或无意的失误)
- ✓ 云提供商本身是否会诚实，不会窥探数据？



# 人工智能时代下的保密性问题

□ 大规模数据挖掘引发的隐私问题 (Privacy issues raised via massive data mining)

- ✓ 云存储来自许多客户的数据，可以运行数据挖掘算法来获取客户端的大量信息

## OpenAI confirms ChatGPT data breach

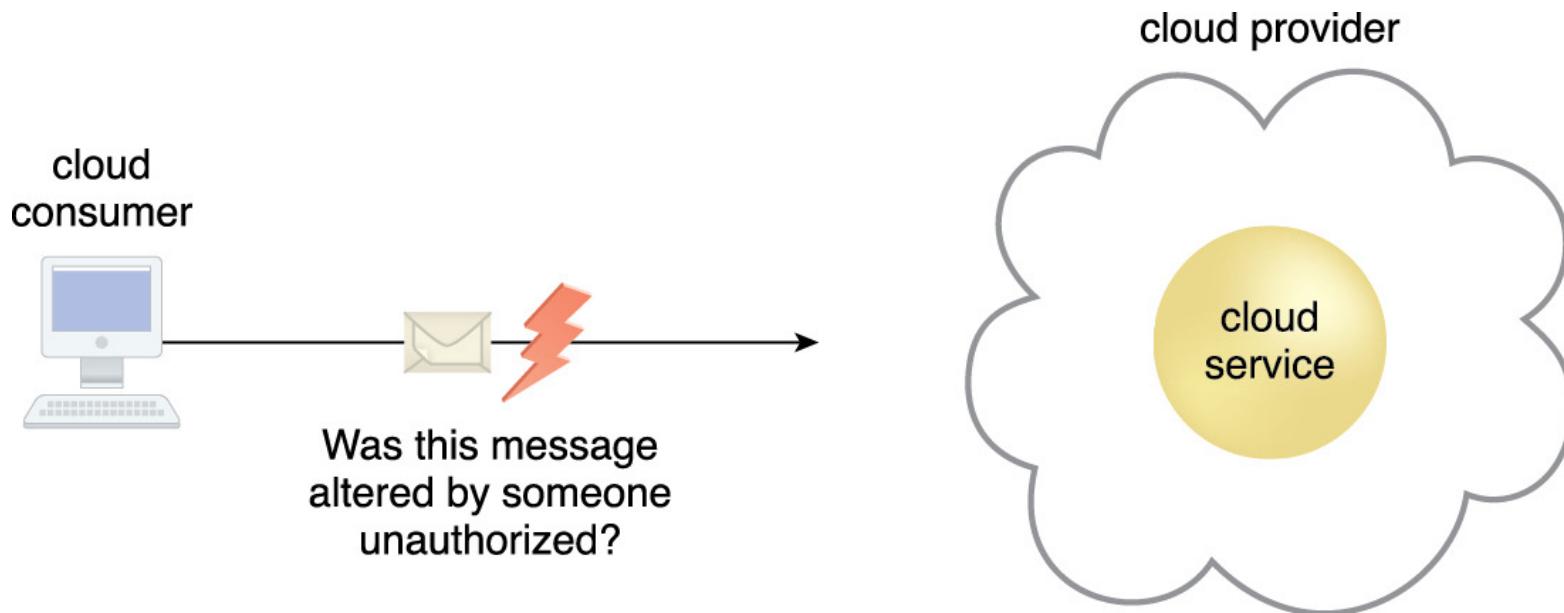
Some users payment information may have been visible to other users

# 信息安全核心三要素

□完整性 (Integrity) : **数据未被篡改的特性**

□用户关心的问题

- ✓我如何知道数据在传输过程中未被篡改?
- ✓我如何确保云提供商在不篡改我存储的数据?

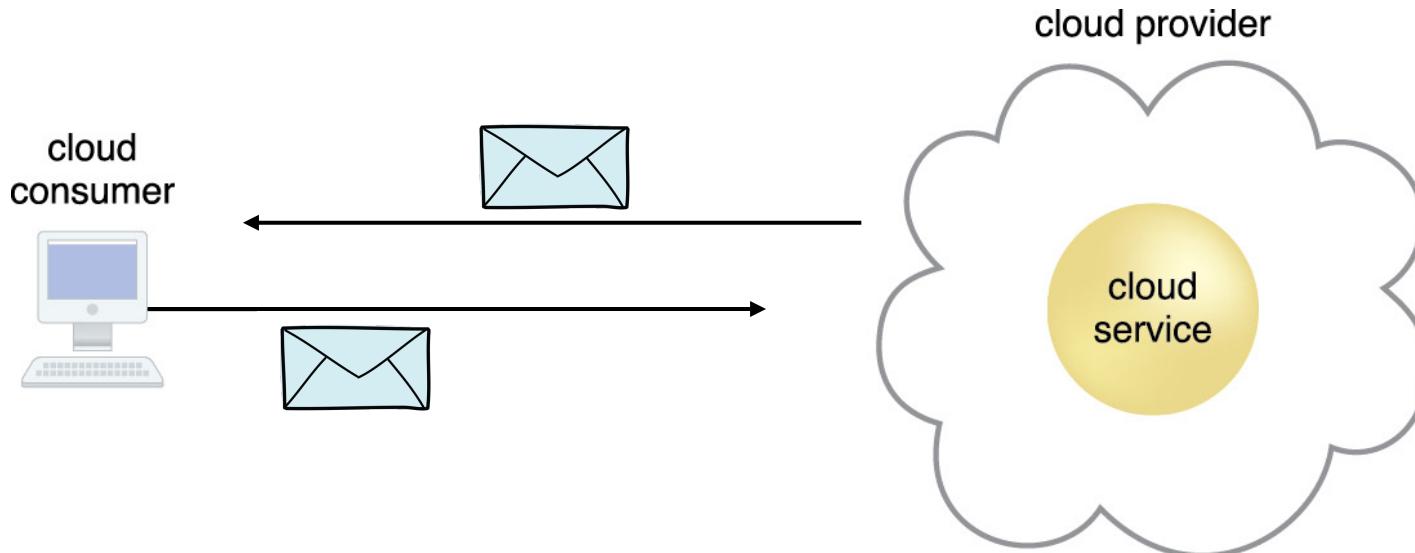


# 信息安全核心三要素

口可用性 (Availability) : **用户在特定时间段内可以访问和使用数据的特性**

口用户关心的问题

- ✓ 如果提供商受到攻击，客户的关键系统会崩溃吗？
- ✓ 如果云提供商倒闭，会发生什么？
- ✓ 云的规模足够存储所有数据 (及备份) 吗？



# 从性能看安全

□ 传统安全关注 CIA，但从计算机系统角度来看，处理性能遭到破坏也是一种安全危险，即 DoS 或 DDoS 攻击

□ 主要有两大类攻击方式

- 恶意资源竞争
  - 抢占处理器资源、内存资源、网路带宽、功耗配给等
- 恶意应用干扰
  - 造成正常**应用缓存不命中率增加**，服务器状态切换频率增加，虚拟机通讯开销增加等

# 功率攻击

口理解系统超额用电的脆弱性

软件层面

## **Not Sensitive to Individual Power Peak**

Each server is allowed to reach its peak power as long as the total rack utilization is within the budget.

基础设施

## **Coarse-Grained Monitoring**

Calculate power demand based on the monitored the total energy consumption at coarse-grained intervals

硬件控制

## **Slow Power Capping**

Normal power capping mechanisms cannot respond quickly enough to limit the sudden spikes

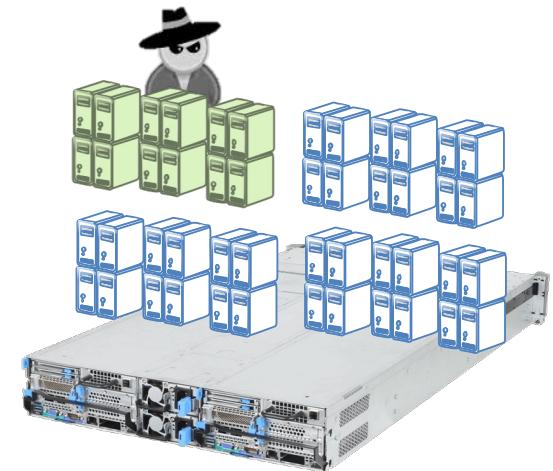
# 功率攻击

## 口 攻击模型

- A sophisticated adversary can manipulate its subscribed nodes to overload a larger cluster

**Opportunistically look for such a host by monitoring the VM IP**

**Keep rebooting a few VMs until they reach the same desired location**



**Generate simultaneously occurred power surge to overload the system**

# 功率攻击

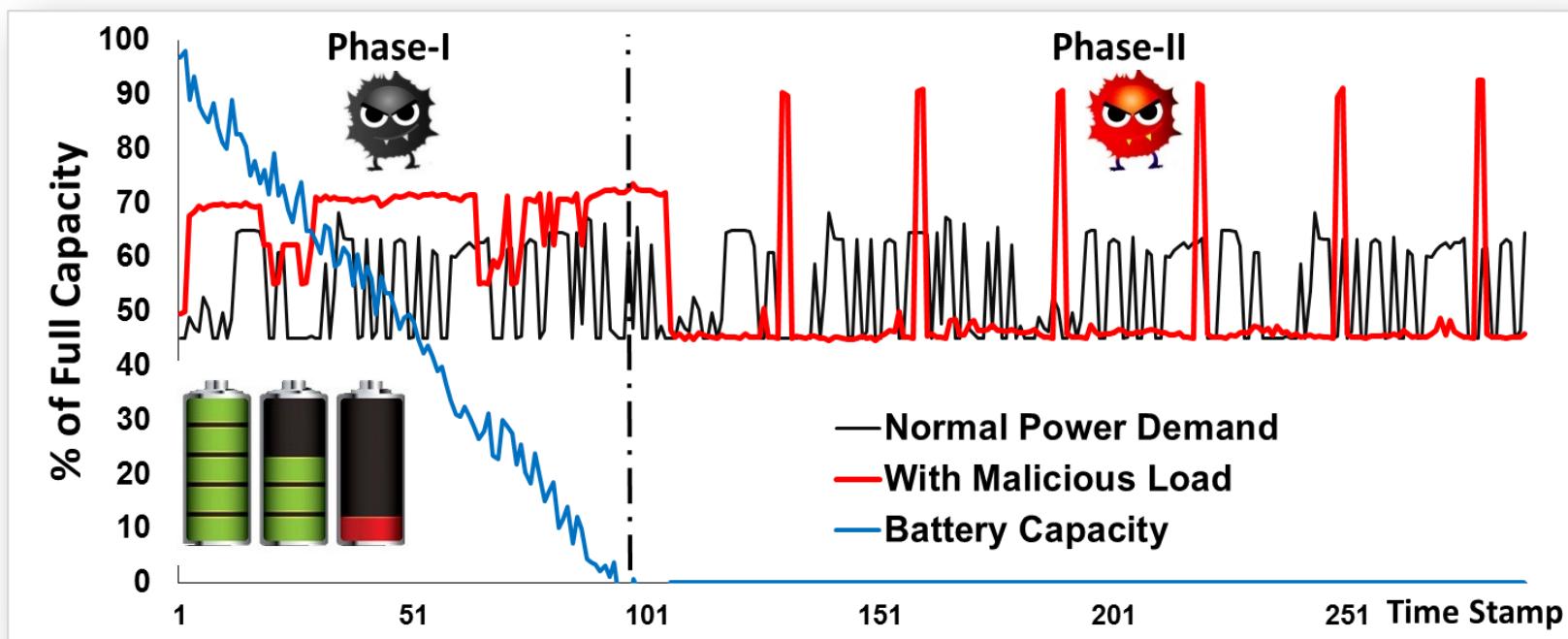
## □ Power Draining Attack 分阶段攻击方案

### Phase-I: Peak Power

- Aims at drain the UPS battery system
- Visible to data centers

### Phase-II: Power Spikes

- Aims at overload the server rack
- Invisible to data center



# 功率攻击

## 口分阶段攻击方案



Disguised as benign job



Energy-intensive load



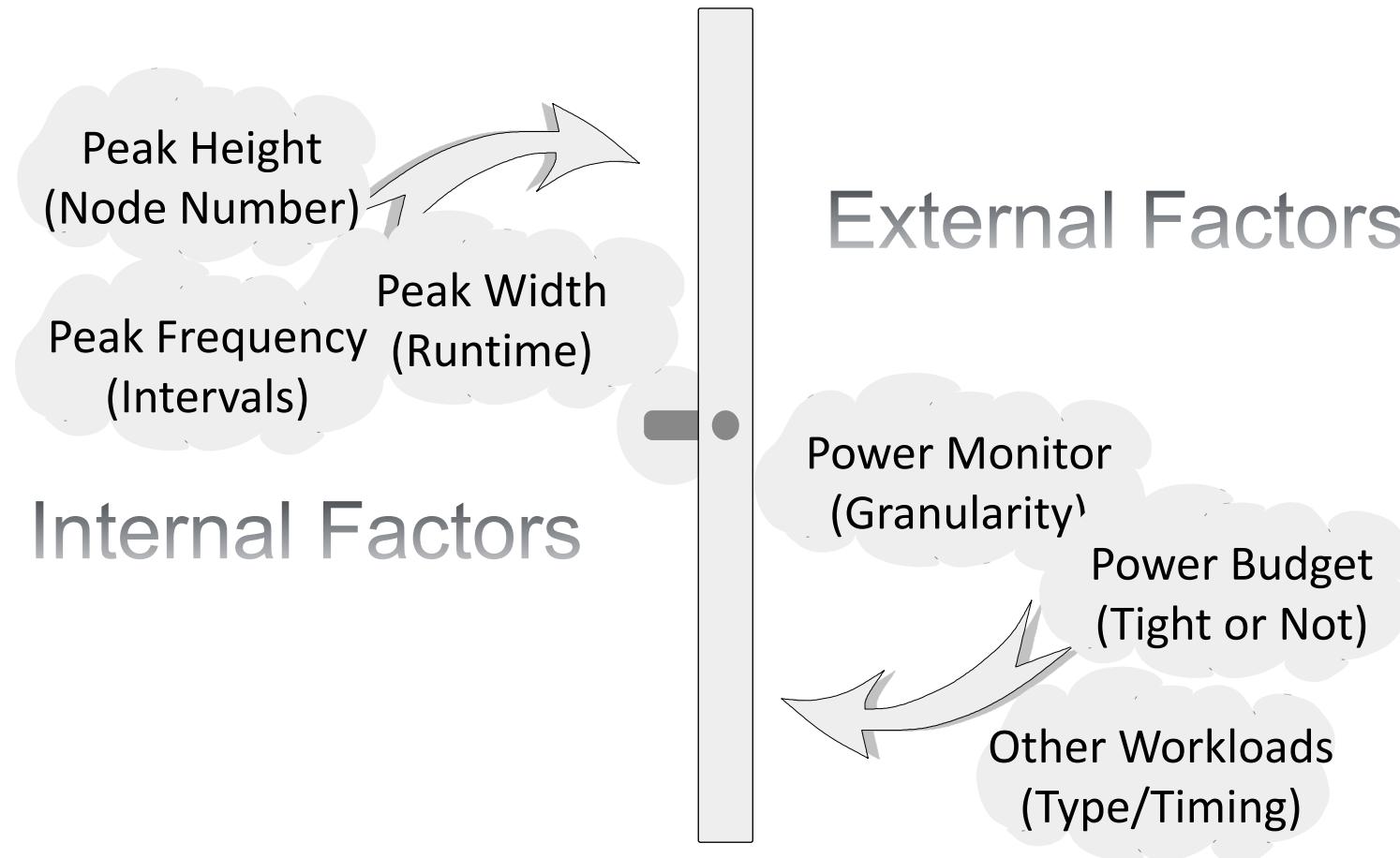
Invisible to data center



Excessive power surge

# 功率攻击

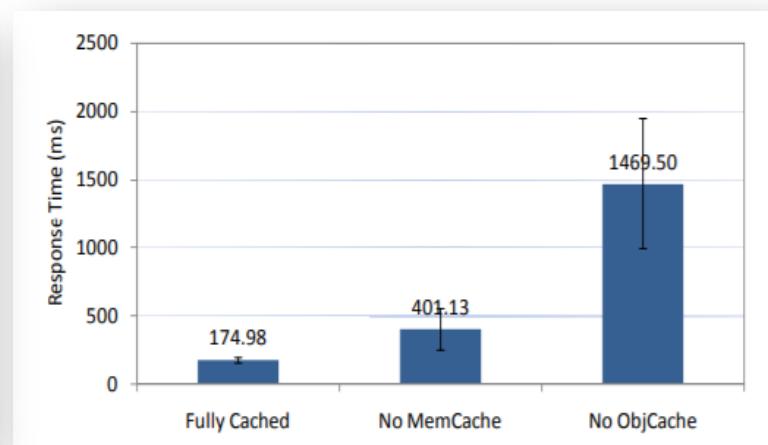
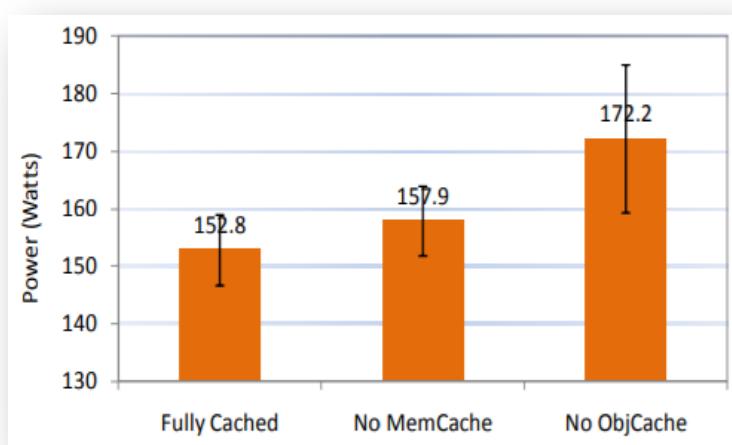
## □效果影响因素



# 能效攻击

口理解网页服务效率的脆弱性

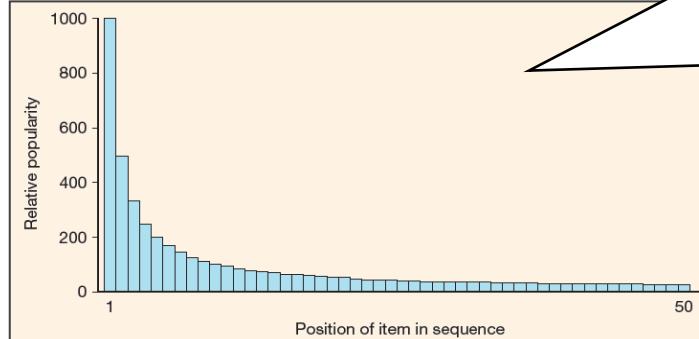
**服务器在运行过程中，对热点数据和请求的缓存是改善性能的关键手段。对有关缓存机制的破坏，不仅仅会带来额外的数据独写操作（增加功耗），也会增加处理时间**



**由于功耗和计算时长的双重增加，系统整体能耗是以乘数方式上升的！**

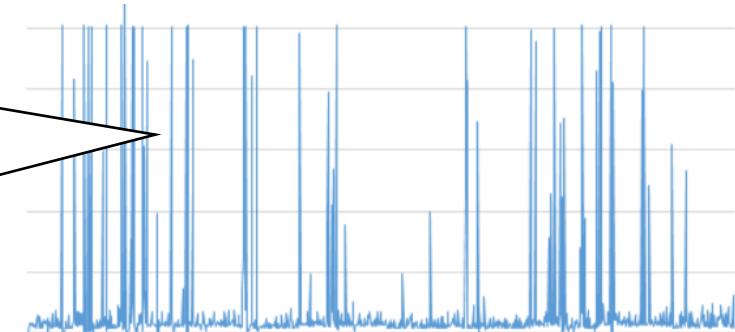
# 能效攻击

## 口 攻击模型



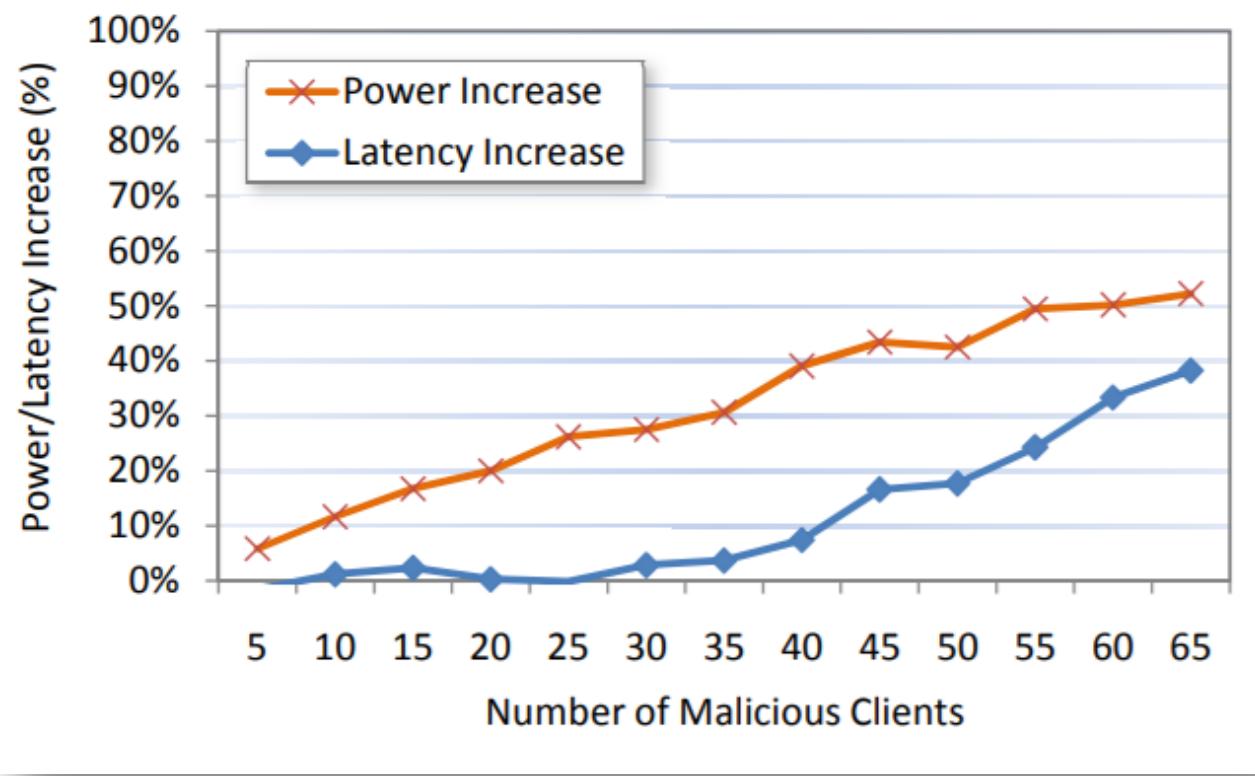
网页缓存机制是针对**幂律分布**定制的，因此攻击者只需要选择一种与之截然不同的分布方式（如均匀分布）则可以对其机制造成损害

通过模拟正常用户的“活跃-不活跃”访问方式，可以掩盖攻击者行为



# 能效攻击

## 口能耗和延时的攻击效果





中山大學 软件工程学院  
SUN YAT-SEN UNIVERSITY SCHOOL OF SOFTWARE ENGINEERING

谢谢

陈壮彬  
软件工程学院  
[chenzhb36@mail.sysu.edu.cn](mailto:chenzhb36@mail.sysu.edu.cn)