河海大学
HOHAI UNIVERSITY

云计算技术与应用

云计算安全技术

主讲人：孙 宁

本专题主要内容

河海大学 HOHAI UNIVERSITY

1 云计算安全挑战

2 云计算面临的安全问题

3 云计算安全关键技术

1 云计算安全

河海大学 HOHAI UNIVERSITY

Google安全挑战

云计算特有的数据和服务外包、虚拟化、多租户和跨域共享等特点,带来了前所未有的安全挑战。

本专题主要内容

河海大学 HOHAI UNIVERSITY

1 云计算安全挑战

2 云计算面临的安全问题

3 云计算安全关键技术

2 云计算面临的安全问题

河海大学 HOHAI UNIVERSITY

虚拟化安全问题

- 如果主机受到破坏，那么主机所管理的客户端服务器有可能被攻克；
- 如果虚拟网络受到破坏，那么客户端也会受到损害；
- 需要保障客户端共享和主机共享的安全，因为这些共享有可能被不法之徒利用其漏洞；
- 如果主机有问题，那么所有的虚拟机都会产生问题

2 云计算面临的安全问题

河海大学 HOHAI UNIVERSITY

- 数据集中后的安全问题
  - 如何保证云服务提供商内部的安全管理和访问控制机制符合客户的安全需求；
  - 如何实施有效的安全审计，对数据操作进行安全监控；
  - 如何避免云计算环境中多用户共存带来的潜在风险

2 云计算面临的安全问题

云平台可用性问题

- 用户的数据和业务应用处于云计算系统中，其业务流程将依赖于云计算服务提供商所提供的服务，这对服务商的云平台服务连续性、 SLA 和 IT 流程、安全策略、事件处理和分析等提出了挑战
- 另外，当发生系统故障时，如何保证用户数据的快速恢复也成为一个重要问题

2 云计算面临的安全问题

河海大学 HOHAI UNIVERSITY

- 云平台遭受攻击的问题
  - 云计算平台由于其用户、信息资源的高度集中，容易成为黑客攻击的目标，由于拒绝服务攻击造成的后果和破坏性将会明显超过传统的企业网应用环境
- 法律风险问题
  - 云计算应用地域性弱、信息流动性大，信息服务或用户数据可能分布在不同地区甚至不同国家，在政府信息安全监管等方面可能存在法律差异与纠纷；
  - 同时由于虚拟化等技术引起的用户间物理界限模糊而可能导致的司法取证问题也不容忽视

2 云计算面临的安全问题

结论

- 对于云计算的安全保护，需要有一个完备的体系，涉及多个层面，需要从法律、技术、监管三个层面进行
- 传统安全技术，如加密机制、安全认证机制、访问控制策略通过集成创新，可以为隐私安全提供一定支撑，但不能完全解决云计算的隐私安全问题
- 需要进一步研究多层次的隐私安全体系（模型）、全同态加密算法、动态服务授权协议、虚拟机隔离与病毒防护策略等，为云计算隐私保护提供全方位的技术支持

本专题主要内容

河海大学 HOHAI UNIVERSITY

1 云计算安全挑战

2 云计算面临的安全问题

3 云计算安全关键技术

3 云计算安全关键技术

可信访问控制

- 在云计算模式下，研究者关心的是如何通过非传统访问控制类手段实施数据对象的访问控制
- 得到关注最多的是基于密码学方法实现访问控制，包括：
  - 基于层次密钥生成与分配策略实施访问控制的方法
  - 利用基于属性的加密算法
  - 基于代理重加密的方法、在用户密钥或密文中嵌入访问控制树的方法等

3 云计算安全关键技术

密文检索与处理

- 密文检索有两种典型的方法
  - 一是基于安全索引的方法，通过为密文关键词建立安全索引，检索索引查询关键词是否存在；
  - 二是基于密文扫描的方法，对密文中每个单词进行比对，确认关键词是否存在，以及统计其出现的次数

3 云计算安全关键技术

河海大学 HOHAI UNIVERSITY

数据存在与可使用性证明

- 云用户需在取回很少数据的情况下，通过某种知识证明协议或概率分析手段，以高置信概率判断远端数据是否完整
- 典型的方法包括：
  - 面向用户单独验证的数据可检索性证明（POR）方法
  - 公开可验证的数据持有证明（PDP）方法

3 云计算安全关键技术

数据隐私保护

- 云中数据隐私保护涉及数据生命周期的每一个阶段：数据生成阶段、计算阶段、存储和使用阶段等
- 隐私保护系统一般采用以用户为中心的信任模型、匿名数据搜索引擎等技术

3 云计算安全关键技术

虚拟化安全技术

- 使用虚拟化技术的云计算平台上的云架构提供者必须向其客户提供安全性和隔离保证
- 除了虚拟机的安全隔离技术，虚拟机映像文件的安全问题也应该得到重视，每一个映像文件对应一个客户应用，它们必须具有高完整性，且需要可以安全共享的机制

3 云计算安全关键技术

云资源访问控制

- 在云计算环境中，各个云应用属于不同的安全管理域，每个安全域都管理着本地的资源和用户
- 当用户跨域访问资源时，需在域边界设置认证服务，对访问共享资源的用户进行统一的身份认证管理
- 在跨多个域的资源访问中，各域有自己的访问控制策略，在进行资源共享和保护时必须对共享资源制定一个公共的、双方都认同的访问控制策略，因此，需要支持策略的合成

3 云计算安全关键技术

可信云计算

- 将可信计算技术融入云计算环境，以可信赖方式提供云服务已成为云安全研究领域的一大热点
- 可信计算技术提供了可信的软件和硬件以及证明自身行为可信的机制，可以被用来解决外包数据的机密性和完整性问题