云计算

第8讲

云安全

任桐炜，李传艺

南京大学软件学院

2017-10-18

观点

- 乐观：云计算将会增强计算机安全
  - 通过部署集中的云计算中心，可以组织安全专家以及业化安全服队伍实现整个系统的安全管理，避免了现在由个人维护安全，由于不专业导致安全漏洞频出而被客利用的情况
- 悲观：云计算是安全的恶梦，安全是云计算的阿喀琉斯之踝
  - 集中管理的云计算中心将成为黑客攻击的重点目标，由于系统的巨大规模以及前所未有的放性与复杂性，其安全性面临着比以往更为严峻的考验

现实

- **AWS和Google Apps都出现过一定规模的故障，并对其上运行的应用造成了一定影响**
- 部分云计算服务曾出现数据泄露

现有的系统安全吗？

- 人们总是容易忽略企业内部数据中心在安全性方面的不足，而假定其固若金汤
- 企业数据中心的不足
  - 成本高：通常在运行初期就需要引入昂贵的第三方安全解决方案，运行时也需要专门的运维团队
  - 复杂度高：制定复杂的规则和流程，系统存在严重的异构性
  - 内部盗窃：核心数据容易被内部盗窃

云平台面临的挑战

- 信任边界的变化
  - 现有系统：所有资源都是处于企业部门的监控中
  - 云平台：资源都是部署和运行在远离企业管理的数据中心
- 更多的利益相关方
  - 现有系统：企业IT部门
  - 云平台：云供应商
- 数据存放地点
  - 现有系统：企业可控制
  - 云平台：企业无法控制（当地法律法规可能不符合企业期望）

云平台面临的挑战（续）

- 互联网的接入
  - 现有系统：通常位于企业内部网络
  - 云平台：通过互联网来提供服务
- 虚拟化技术
  - 现有系统：不使用虚拟化或小型机虚拟化
  - 云平台：X86虚拟化

云计算安全现状

- 各国政府的关注
  - **2010** 年 **3** 月，欧洲各国呼吁制定关于数据保护的全球协议，以解决云计算的数据安全弱点
  - **2010** 年 **11** 月，美国政府 **CIO** 委员会发布关于政府机构采用云计算的政府文件，要求政府及各机构评估云计算安全风险并与自己的安全需求比对分析
  - 日本政府启动官民合作项目，组织信息技术企业与有关部门对于云计算的实际应用开展安全性测试

云计算安全现状（续）

- 工业界的技术发展
  - **Sun公司发布开源的云计算安全工具可为Amazon的EC2、S3以及虚拟私有云平台提供安全保护**
  - **微软为云计算平台Azure筹备代号为Sydney的安全计划，帮助企业用户在服务器和Azure云之间交换数据，以解决虚拟化、多租户环境中的安全性**
  - **EMC、Intel、Vmware 等公司联合开展“可信云体系架构”的合作项目，并提出相应的概念证明系统**
  - **Hadoop推出安全版本，引入 kerberos 安全认证技术，对共享商业敏感数据的用户加以认证与访问控制，阻止非法用户对Hadoop clusters的非授权访问**

云平台的优势

- 安全管理
  - 云平台的同构性和专业性，能使得安全管理方面有的放矢
- 高可用性
  - 可用性（3个9）逐步接近昂贵的企业高可用性解决方案（5个9）
- 数据安全
  - 快照、备份、容灾等措施
- 专业人才
  - 以更低的成本吸引更多的优秀专业人员

更多的措施

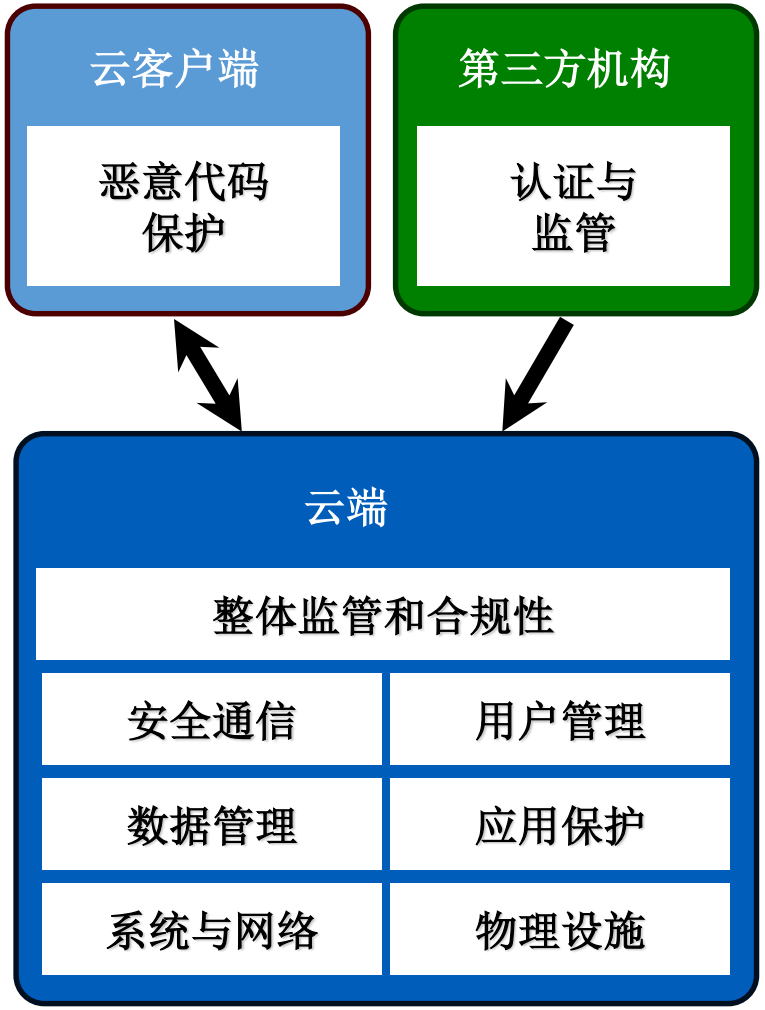
- 提供更好的安全保障
  - 更好的保障机制
  - 更严格的隔离、用户管理，更低成本且更高级别的服务
- 防护策略的改变
  - 安全模式从“拒敌于国门之外”变为“全民皆兵”
  - 利用云计算的优势协同防护
  - 规范和立法

更多的措施（续）

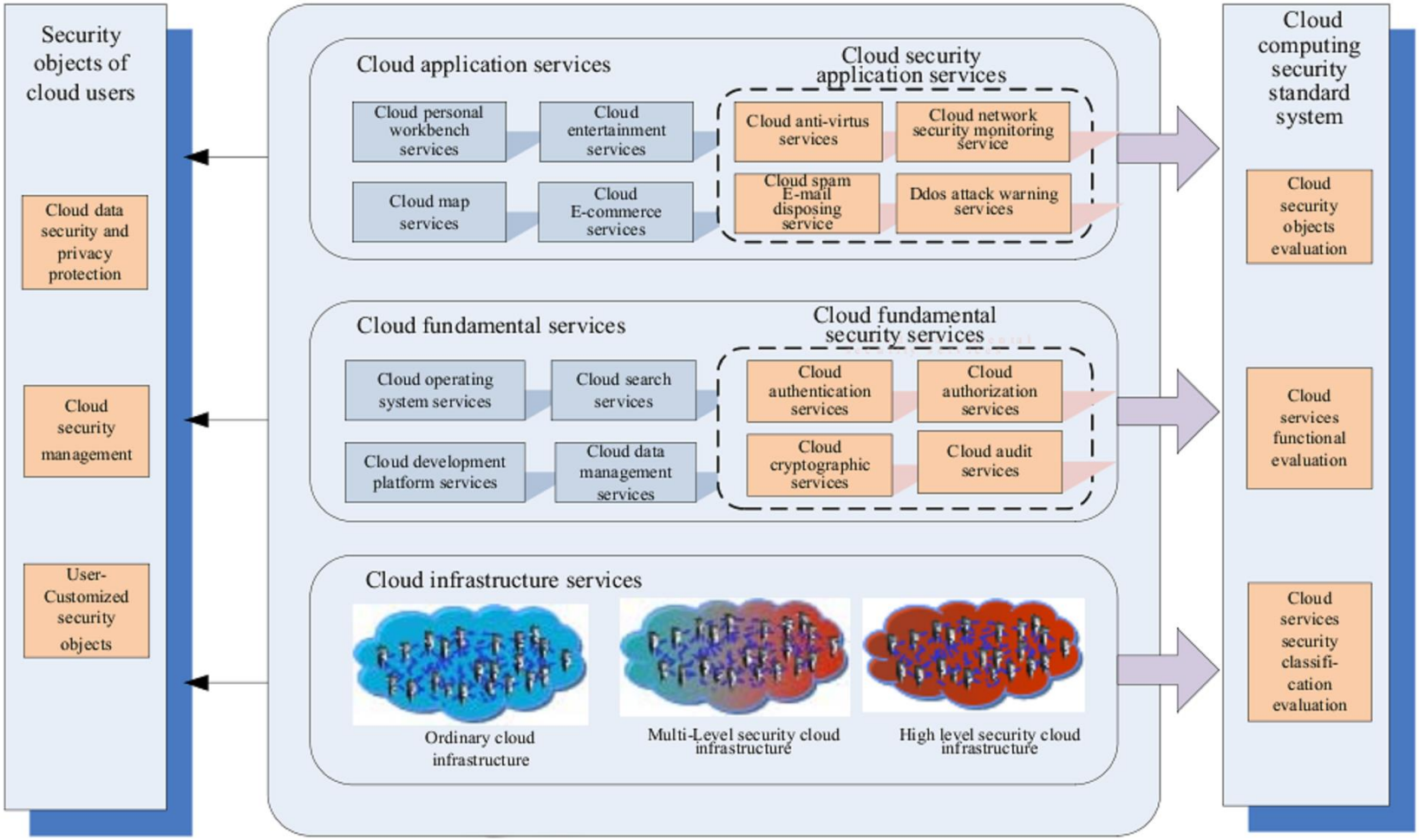
- 防止非法访问用户
  - 发送和存储尽量少的个人信息到云中，并加密处理
  - 最大限度地实现用户对个人信息的控制
  - 对多用户数据进行隔离
- 防止公司“作恶”
  - 允许用户自由加入/退出
- 防止合法的泄漏
  - 充分考虑不同国家和地区在相关法律、法规间的差异
  - 允许用户对数据存放进行个性化设置

安全架构设想

- 云客户端
  - 防火墙，杀毒软件，打补丁，沙箱，……
- 云端
  - 整体监管，合规性，大容量安全通信，用户授权访问，数据隔离、加密和备份，加固应用的服务协议和对外接口，事务隔离，设备冗余和管理员限制
- 第三方机构
  - 对服务提供商进行安全认证，实时监控运行状况



安全架构设想（续）


Security objects of cloud users
Cloud data security and privacy protection
Cloud security management
User-Customized security objects
Cloud application services
Cloud personal workbench services
Cloud entertainment services
Cloud map services
Cloud E-commerce services
Cloud security application services
Cloud anti-virtus services
Cloud network security monitoring service
Cloud spam E-mail disposing service
Ddos attack warning services
Cloud fundamental services
Cloud operating system services
Cloud search services
Cloud development platform services
Cloud data management services
Cloud fundamental security services
Cloud authentication services
Cloud authorization services
Cloud cryptographic services
Cloud audit services
Cloud infrastructure services
Ordinary cloud infrastructure
Multi-Level security cloud infrastructure
High level security cloud infrastructure
Cloud computing security standard system
Cloud security objects evaluation
Cloud services functional evaluation
Cloud services security classifi-cation evaluation

谢 谢