现代密码学

属性基加密

信息与软件工程学院

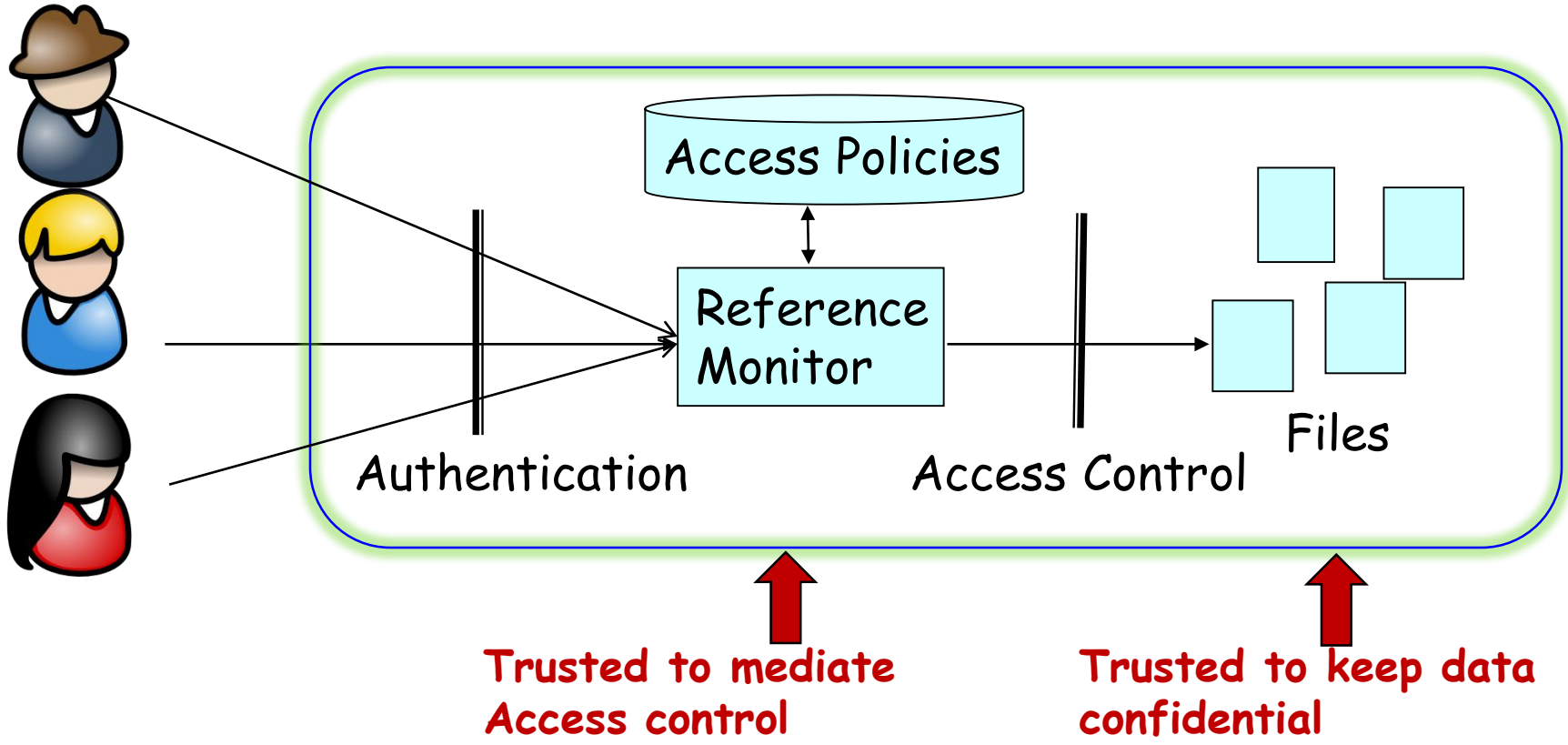
云存储系统中的访问控制

云存储系统

云存储系统中的访问控制

- 传统的访问控制模型

  - 优点：灵活，可扩展，MAC，DAC，RBAC - 缺点：数据容易受到损害



云存储系统中的访问控制

- 数据泄露的重大案例

  http://www.identityhawk.com/biggest-examples-data-breaches

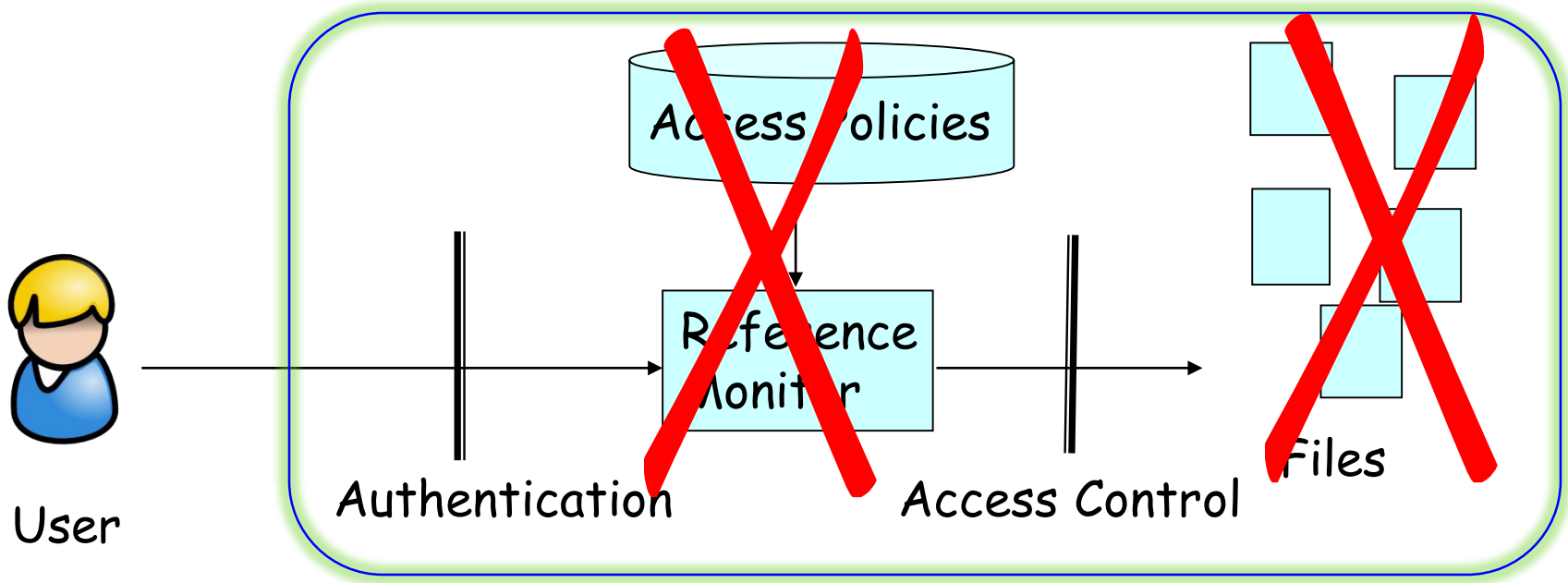
- 2008年2月纽约梅隆银行：丢失了包含1250万人信息的数据存储磁带，导致未被披露数量的资金被盗.....
- 2009年初Heartland支付系统：黑客渗入其数据库并获得了每月处理的1亿多笔信用卡交易记录。该公司支付了超过4110万美元来解决索赔。
- …

云存储系统中的访问控制

- 假设服务器是可信的，通常是不现实的
- 用于外包数据存储的云计算：不受数据拥有者者直接控制的硬件
- 存储用于紧急访问的电子病历的便携式设备：设备可能丢失或被盗
- 软件不保证没有错误
- 内部攻击
- ...

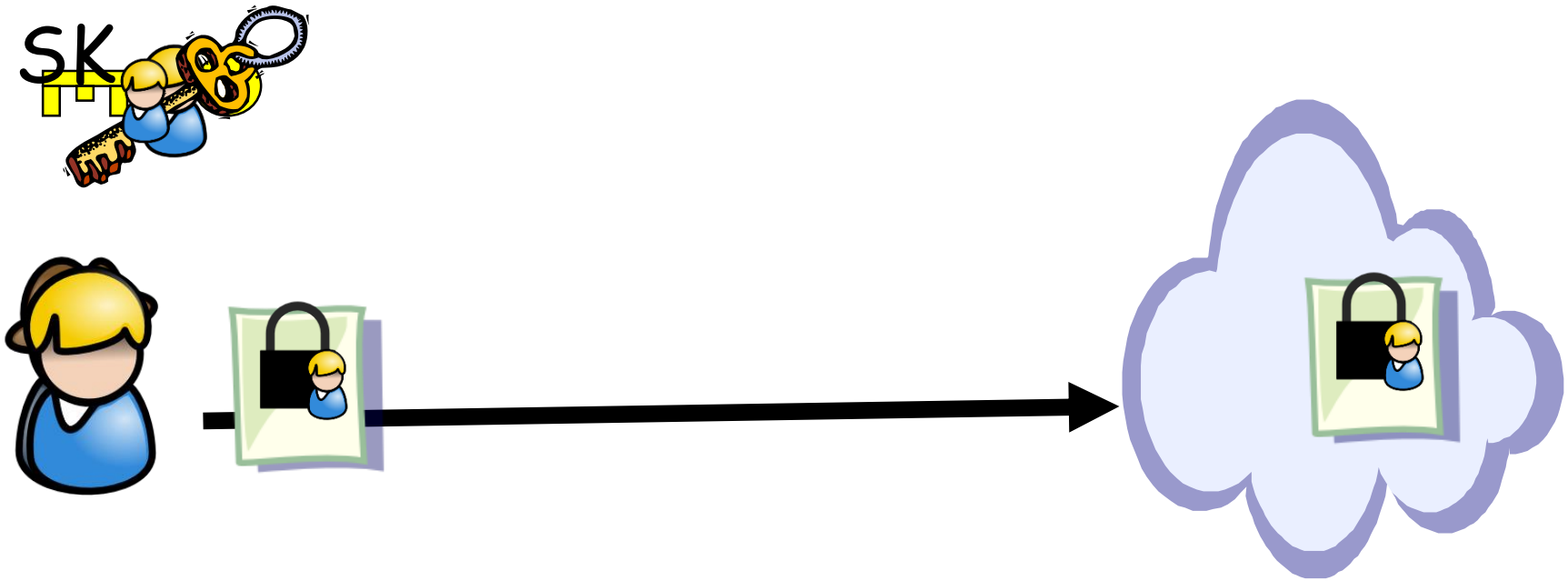
云存储系统中的访问控制

- 不可信的服务器
  - 一般解决方案：以加密形式存储数据
  - 即使对于“可信”服务器也是很好的做法 → 深度防御原则



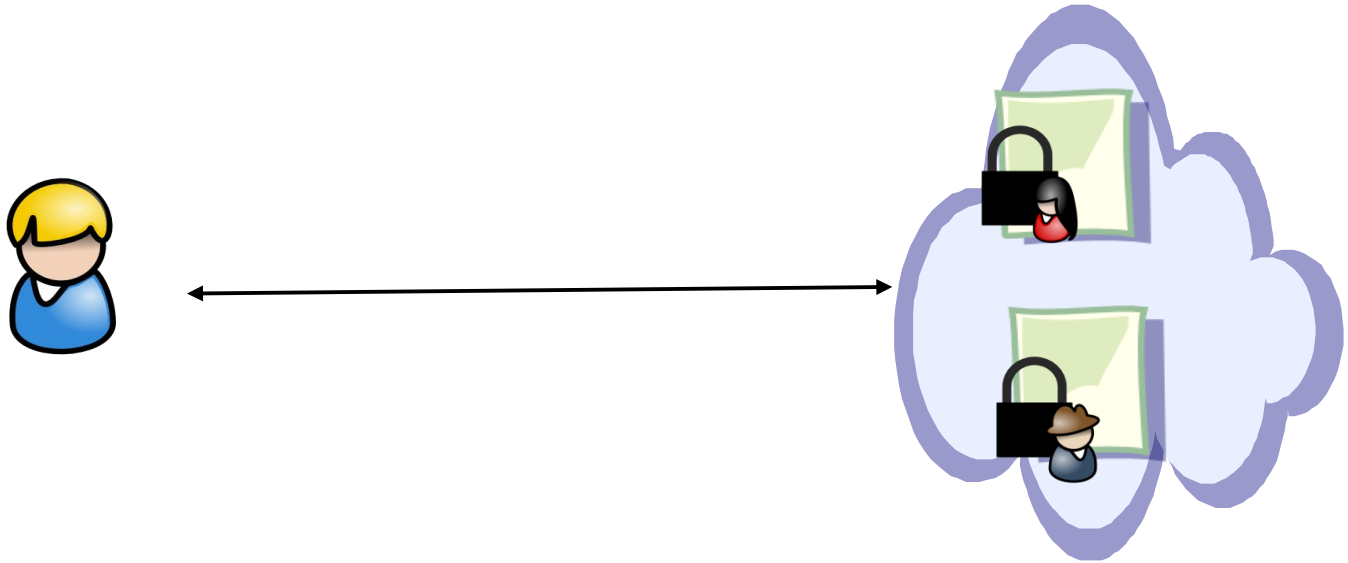
云存储系统中的访问控制

- 通过加密进行访问控制
  - 需要密钥才能访问数据
  - Ciphertexts存储在服务器上
  - 每个用户都可以解密自己的数据



云存储系统中的访问控制

- 与他人共享加密数据
  - 公钥解决方案：公钥证书管理的开销很大；一对一加密
  - 对称密钥解决方案：在线密钥分发

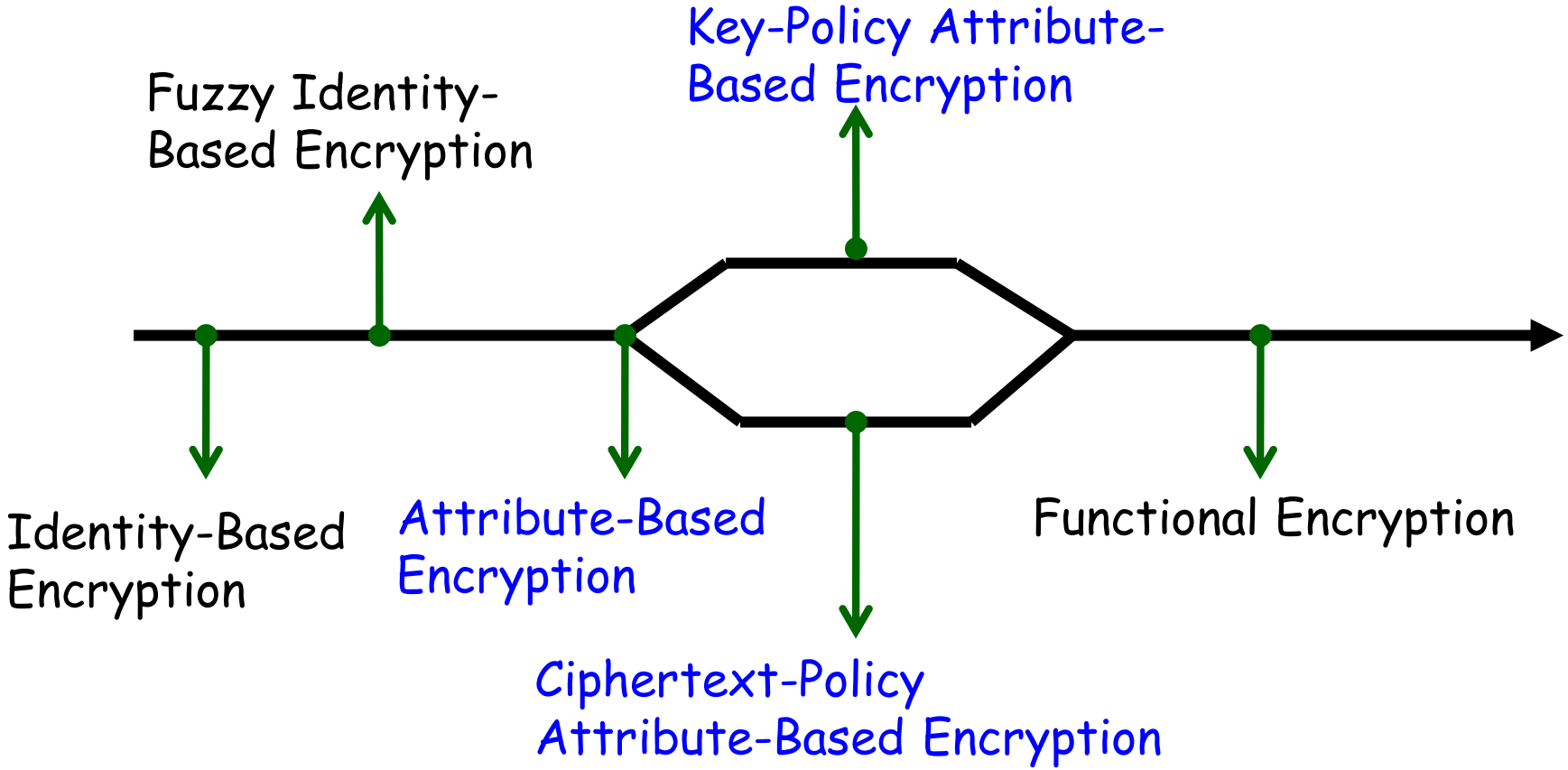


云存储系统中的访问控制

- 在不可信服务器上存储加密数据的期望列表
  - 密钥管理是可扩展和离线的
  - 无需一个在的线可信任方来调解访问控制
  - 灵活和可扩展的访问控制策略

- 基于属性的加密（Attribute-Based Encryption，ABE）就可以实现上述期望！

基于属性的访问控制

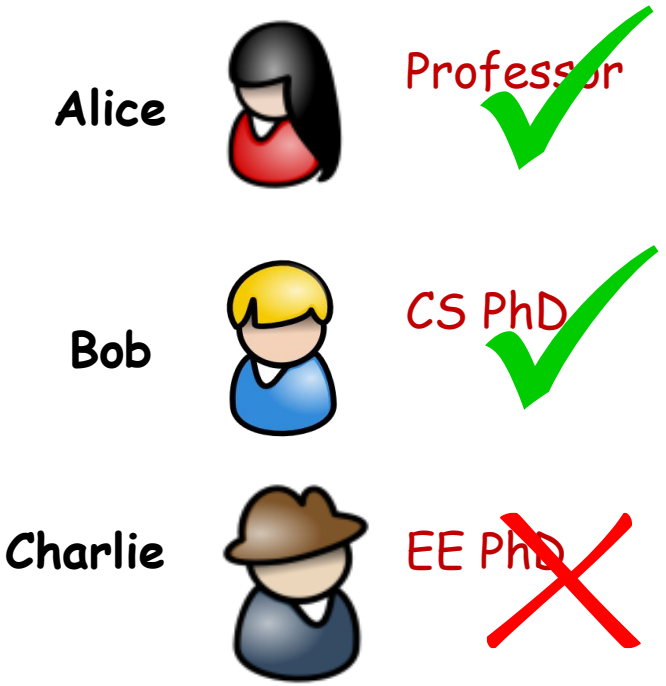


属性基加密的演化

基于属性的访问控制

- 属性基加密 [Sahai, Waters CCS'05]
  - 将数据加密给具有某些属性的用户
  - 一对多公钥加密
  - 内置访问控制机制

"All professors, CS PhD"



感 谢 聆 听!

xionghu.uestc@gmail.com