网络安全 – 信息系统安全保障体系

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

上周回顾

1. 与GSM系统、GPRS系统相比，3G系统的安全保护的特殊性在哪里?

2. 备份的误区

3. 数据备份、网络备份

4. 冷备份、热备份

3G安全 – 安全层次 1

网络接入安全：目的是抗击针对无线链路的攻击。

- 这其中主要包括身份保密、用户位置保密、用户行踪保密、实体身份认证、加密密钥分发、用户数据与信令数据的保密以及身份认证

核心网络安全：目的是保证核心网络实体之间能够安全地交换数据。

- 这其中包括网络实体间的身份认证、数据加密、消息认证以及对欺骗信息的收藏

3G安全 – 安全层次 2

用户安全：目的是保证对移动平台的安全接入。

- **这其中包括用户与智能卡之间的认证、智能卡与终端的认证以及其链路保护**

应用安全：目的是保证用户与服务提供商之间能够安全地交换应用程序的信息。

- **这其中包括应用实体间的身份认证、应用数据重放攻击的检测、应用数据完整性保护以及接入确定等**

认证

授权

密码管理

密钥管理

可信任时间戳的管理

认证

授权

密码管理

密钥管理

可信任时间戳的管理

信息系统安全保证体系

在安全保证体系中，认证与授权体系的概念，各自的设计方案及实现过程，并简单介绍了分布式授权系统；

密码管理说明密码在设置、更改、存储及使用过程中须遵循的一些原则；

密钥管理介绍了密钥管理的生成、分配、托管等和各种可行的方案；

最后介绍可信任时间戳的管理情况。

认证

认证与鉴别的概念

- 认证：认证用户身份，是访问控制的基础
- 鉴别：通过质询响应机制提供私人或者指定证书

认证方式

- 静态UID/ 密码
- 双要素认证
- 一次性密码(OTP)认证
- 单一登录(SSO)认证
- X.509认证方式

认证 – X.509

以密码为基础，用户直接登录方式，无需安装特殊软件

- **密码记录的繁杂，泄密**

以证书为基础

- **公钥证书的格式（用户公钥、识别、有效期等）**
- **认证过程：单项、双向、三项**

基于信息分级策略的鉴别和认证要求

信息分析	鉴别和认证要求
公共	无
内部	用户ID和密码
机密	增强认证（加密的UID、密码、令牌和证书）
限制	增强认证（加密的UID、密码、令牌和证书）

认证

授权

密码管理

密钥管理

可信任时间戳的管理

授权 – 基本概念

授予进程和用户特权的过程。

网络管理员控制用户能够在网络中使用的功能和进行的操作。

当用户通过认证后，系统必须保证他们有足够权限，执行所请求的操作，拒绝其他不被允许的操作。

一个系统可以有多个授权用户，每个用户访问权限可能不相同。

授权 – 授权技术

资源预先分配

- **分配给三个级别的用户：所有者，组员，全部用户**

访问控制列表(ACL)

- **路由器端的过滤机制**
- **基于IP、端口、路由器接口**
- **兼容IPv4、IPv6**

按访问控制策略授权

- **自由访问控制**
- **强制访问控制**
- **角色访问控制**

授权 – 授权管理

集中：只有一个授权者允许对用户许可或者取消授权

合作：特定资源的行政管理需要几个授权者的合作

分散：在分散刑侦管理中，客体的所有者也可以许可其他用户对此客户的许可特却

所有权：用户是他创造客体的专有者，主体可以许可或者取消其他用户对此客体的访问

授权 – 授权实现 1

要求

- 保证不被绕过（特别是离受保护资源近的授权控制措施更难饶过）
- 遵循最小原则，规定进程及用户应享有完成工作所需最小权限

实现

- 访问数据的用户、访问时间
- 确定用户物理性访问的服务器、数据库、网段
- 限制特定的组

授权 – 授权实现 2

分布式授权

- 条件：时间、空间、实现手段、系统平台运行条件不同
- 方式
  - 机器代理：通过内部代理服务器进行
  - 应用代理：代理服务器-资源提供方服务器
  - 认证：证书时候在多个合作单位都有效
  - 代理/认证相结合：代理服务器对用户认证，同时向资源提供商提供认证证书，后续由用户与资源提供商建立联系

认证

授权

密码管理

密钥管理

可信任时间戳的管理

密码管理

密码的设置选择

密码的更改

密码的存储

密码的使用

密码制度

密码的配置选择

1. 用户密码最短应该包含7个字符或以上
2. 用户密码不能是字典中能找到的词
3. 用户密码必须是字母和非字母符号的组合
4. 相对于一般密码，系统和网络管理员密码必须更长、更复杂、有效时间更短
5. 用户密码不能包含用户或者姓名，服务差异化设置
6. 分配或者更改密码时，不能通过不具有安全功能的方式把密码传给用户
7. 必须保留历史上用过的密码列表，防止重用
8. 不能再批处理登陆过程中，使用明文ID和密码
9. 不能使用通用账户和组密码，保证个人可信赖性
10. 各种附带的用户账户和密码数据库，必须通过产品使用的最强加密方法进行加密

密码的更改

1. 如果给用户一个初始密码，第一次登录就必须更改
2. 软硬件附带的默认密码，必须在收到软硬件后禁止或者修改
3. 密码在经过一段预订时间后必须失效
4. 用户在需要更改密码时候，必须先登录
5. 为用户分配新密码或者重新设置密码，必须是唯一，不易被猜中
6. 新密码生效前，必须要求用户多次输入新密码
7. 只有在拥有用户ID的人提出请求时，才能清除该ID和密码

密码的使用

1. 新创建的账户如果在预定时间内未使用，则应该失效
2. 除非有特殊业务需求，否则同一个账户在同一个时刻只能允许一个人登录
3. 认证发生3次或者3次以上失败，登陆进程必须停用
4. 重新设定密码的请求必须得到验证和核实
5. 激活：一名合同制或者兼职雇员的密码激活期限应该截止合同到期日
6. 使用：在用户拿到密码时，必须签字表示同意使用策略
7. 终止：用户在被终止使用后，其账户应立即禁用

密码制度

1. 中国政府于1999年10月7日颁发了《商用密码管理条例》，对商用密码在科研、生产、销售、使用等多方面作出了相应管理，如：
2. 第三条：商用密码技术属于国家秘密。国家对商用密码产品的科研、生产、销售和使用实行专控管理
3. 第四条：国家密码管理委员会及其办公室主管全国的商用密码管理工作
4. 第七条：规定商用密码产品由国家密码管理机构指定的单位生产。未经指定，任何单位或者个人不得生产商用密码产品
5. 第十三条：进出口密码产品以及含有密码技术的设备或者出口商用密码产品，必须报经国家密码管理机构批准
6. 第十四条：任何单位或者个人只能使用经国家密码管理机构认可的商用密码产品，不得使用自行研制的或者境外上产的密码产品

认证

授权

密码管理

密钥管理

可信任时间戳的管理

密码管理

密钥的生成

- 增大密钥空间
- 强钥选择
- 随机数生成密钥

密钥的分配

- 单钥加密体制的密钥分配
- 公钥加密体制的密钥管理
- 公钥加密分配单钥密码体制的密钥

密钥托管技术（存储数据恢复密钥的方案）

密钥传送检测（误差校正，校验和）

密码管理 - 3

密钥的使用

密钥存储与备份

密钥的泄露

密钥的生存期

密钥的销毁

认证

授权

密码管理

密钥管理

可信任时间戳的管理

可信任时间戳的管理 - 1

时间戳概述

- **证明电子文档在某一特定时间创建、或者签署的一系列技术**
- **应用于：确认建立文档的时间、延长数字签名生命周期等**

为提供完善的时间戳服务，Time Stamp Authority（TSA）还需要包含其他权威机构，如CA，将公钥与实体对应，满足公钥可信性

可靠时间源Secure-Time Source（STS）也非常重要，提供单调增加的时间值，与国际标准时间同步

可信任时间戳的管理 - 2

时间戳技术

- 基本时间戳
- 链式时间戳

时间误差的管理控制

- 对重要设备实施物理隔离，如国家标准时间部的时间服务器，时间认证中心等存放在单独封闭室中
- 采取认证防护措施，保证时间分配真实性
- 保证系统时间具有良好的可追溯性
- 访问控制级别的划分

课后问题

1. 信息保证体系的基础是什么？可将其具体分为几步骤?

2. 认证可以分为几种方式？每种方式是如何进行的?

3. 授权的具体方式有几种?

4. 请简单叙述授权的实现过程?

5. 分布式授权的特点是什么?

谢谢!