数字证书如何在移动互联时代保证信息安全

主讲人：王梅

主要内容

- 数字证书简介
- 数字证书应用
- 移动平台安全需求分析
- 移动平台安全解决措施

什么是PKI/CA

PKI：Public Key Infrastructure 公钥基础设施

利用公开密钥技术建立的提供信息安全服务的在线基础设施。它利用加密、数字签名、数字证书来保护应用、通信或事务处理的安全。

是一个包括硬件、软件、人员、策略和规程的集合，用来实现基于公钥密码体制的密钥和数字证书的产生、管理、存储、分发和撤销等功能。

如同电力基础设施为家用电器提供电力一样，PKI为各种应用提供安全保障，提供网络信任基础。

CA：认证权威机构

签发管理数字证书

是PKI的核心

数字证书简介

- 绑定用户身份和公钥

- 网络世界的电子身份证
  - 与现实世界的身份证类似
  - 能够证明个人、团体或设备的身份
- 包含相关信息：
  - 包含姓名、地址、公司、电话号码、Email地址、 …
    - 与身份证上的姓名、地址等类似
  - 包含所有者的公钥
- 拥有者拥有证书公钥对应的私钥
- 由可信的颁发机构颁发
  - 比如身份证由公安局颁发一样
- 颁发机构对证书进行签名
  - 与身份证上公安局的盖章类似
  - 可以由颁发机构证明证书是否有效
  - 可防止擅改证书上的任何资料

数字证书简介

数字证书分类：

- **服务器证书(SSL证书)**
  - **确保从用户浏览器到服务器之间传输的信息自动加密，防止非法篡改和非法窃取。确保服务器身份的真实性。**
- **代码签名证书**
  - **确保软件代码在通过互联网发布时不会被非法篡改；让用户确信此代码的真实来源。**
- **客户端证书**
  - **个人数字证书、企业数字证书、邮件证书。**

数字证书的基本内容

证书至少需要包括如下内容： (1) 颁证机构，(2)证书持有者的名字 (3)证书持有者的公钥（标识）, (4) 证书有效期， (5) 证书颁发机构的签名

版本（Version）：v3
序列号（Serial No）：001b6
算法标识（Algorithms）：MI
证书持有者名字（Subject DN John Doe
有效期（Validity period）：f
公钥（Public key）：30 81 8 9c de a8 e5 53 1b 73 c7 f7 8 4b 13 7d …
CA签名（Signature）

证书扩展项（Certificate Extensions）		
证书关键用途（Key Usage）：	digitalSignature dataEncipherment nonRepudiation keyEncipherment	keyCertSign keyAgreement encipherOnly cRLSign decipherOny
扩展用途（Extended Key Usage）：	serverAuth timeStamping emailProtection	codeSigning clientAuth OCSPSigning
证书策略（Certificate Policies）：URL of CPS and Policy notice text		
证书持有者替换名（Subject Alternative Name）：rfc822name, IP Address, DNS Name		
黑名单发布点（CRL Distribution Point）：URL of the Certificate Revocation List		

CA：Certification Authority

- CA数字证书的发放机构，其主要功能包括：
  - 签发数字证书
    - 签发证书
    - 更新证书
  - 管理数字证书
    - 撤销、查询
    - 审计、统计
  - 验证数字证书
    - 黑名单认证（CRL）
    - 在线认证 （OCSP）

移动平台的安全需求

- 1、客户端系统安全需求：

  客户端APP运行期间能够防止病毒、木马对移动业务系统影响。

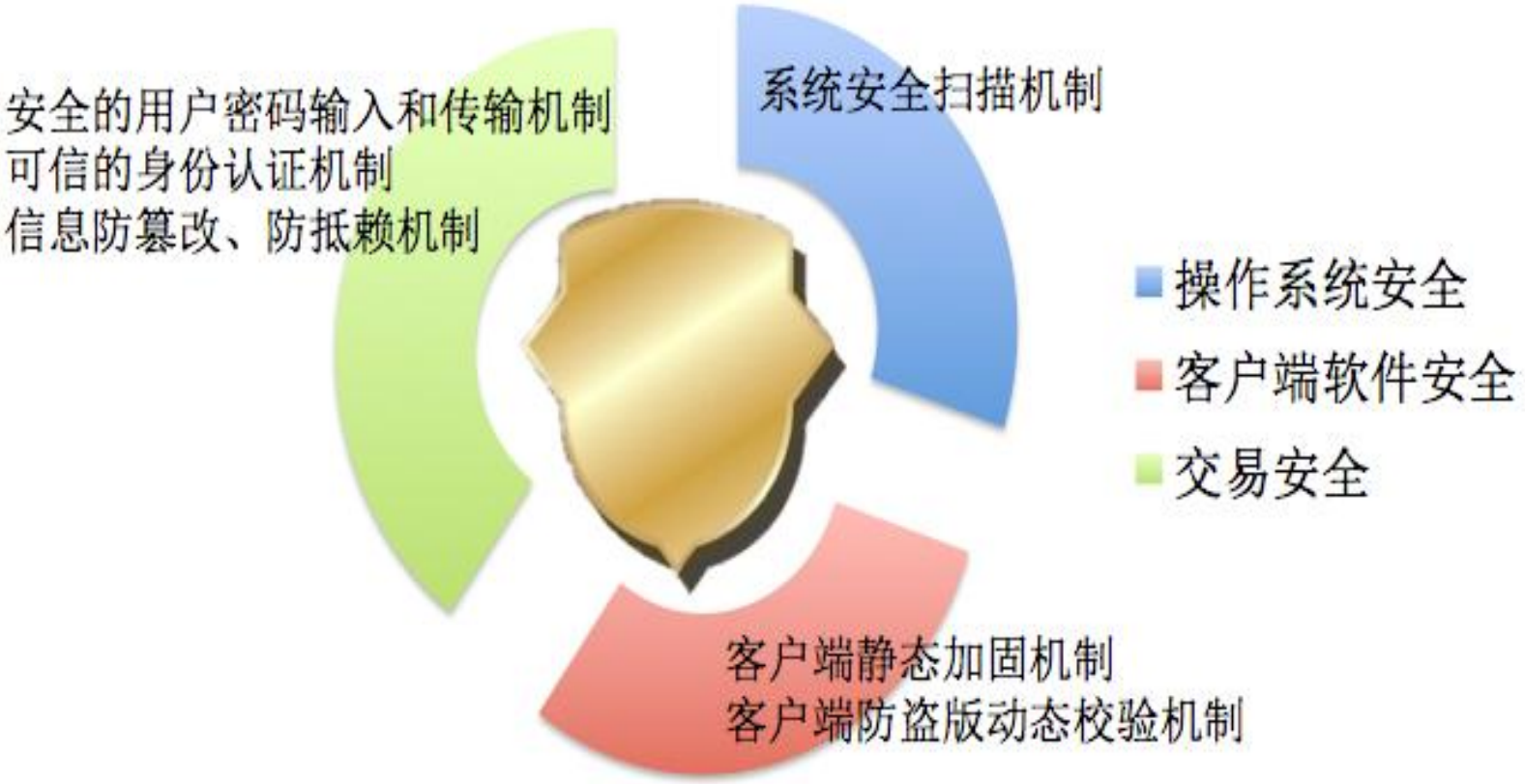
- 2、客户端软件安全需求：

  如何保障客户端软件的真实合法性（目前移动应用市场上有15%以上的软件被盗版，如二次打包）

- 3、交易防篡改、防抵赖：防止中间人攻击。
- 4、强身份认证：使用户身份不容易被伪造。
- 5、数据防窃听：

  加强用户敏感信息的输入和传输安全。

移动平台整体安全


安全的用户密码输入和传输机制
可信的身份认证机制
信息防篡改、防抵赖机制
系统安全扫描机制
操作系统安全
客户端软件安全
交易安全
客户端静态加固机制
客户端防盗版动态校验机制

解决措施

- 客户端清场助手：识别6000多种病毒，能区分恶意扣费、隐私窃取、远程控制、恶意传播等多类型恶意软件。
- 客户端静态加固平台：通过证书下载加固后的客户端应用程序。
- 安全输入过程组件（SIP）：对用户输入信息进行加密传输，到服务器端时解密。已通过国家权威测评机构的测试。

解决措施

- 安全数字证书应用中间件（SCAP）：

1、完成数字证书管理、应用和过程监督服务

2、提供数字证书在线下载、更新、口令更改和信息查看功能。

3、提供基于数字证书的数字签名、数字信封解密等应用功能，也可进行证书有效性验证、客户端验证签名等。

4、带有验证码机制，保障每次签名都是用户本人发起和确认；

5、带有签名信息回显功能，有效避免被篡改而发生所见非所签现象。

6、支持双接口蓝牙key、双接口音频key、手机证书等。


谢谢大家！