Android APK的数字签名的作用和意义

yangkewx 于 2014-09-24 16:53:55 发布

1. 什么是数字签名?

数字签名就是为你的程序打上一种标记，来作为你自己的标识，当别人看到签名的时候会知道它是与你相关的

2. 为什么要数字签名?

最简单直接的回答： 系统要求的。

Android系统要求每一个Android应用程序必须要经过数字签名才能够安装到系统中，也就是说如果一个Android应用程序没有经过数字签名，是没有办法安装到系统中的!
Android通过数字签名来标识应用程序的作者和在应用程序之间建立信任关系，不是用来决定最终用户可以安装哪些应用程序。
这个数字签名由应用程序的作者完成，并不需要权威的数字证书签名机构认证，它只是用来让应用程序包自我认证的。

3. 数字证书的机制?

Android使用Java的数字证书相关的机制来给apk加盖数字证书，要理解android的数字证书，需要先了解以下数字证书的概念和java的数字证书机制。

4. 程序使用相同的数字证书的好处

(1)有利于程序升级

当新版程序和旧版程序的数字证书相同时，Android系统才会认为这两个程序是同一个程序的不同版本。如果新版程序和旧版程序的数字证书不相同，则Android系统认为他们是不同的程序，并产生冲突，会要求新程序更改包名。

(2)有利于程序的模块化设计和开发。

Android系统允许拥有同一个数字签名的程序运行在一个进程中，Android程序会将他们视为同一个程序。所以开发者可以将自己的程序分模块开发，而用户只需要在需要的时候下载适当的模块。

(3)可以通过权限(permission)的方式在多个程序间共享数据和代码。

Android提供了基于数字证书的权限赋予机制，应用程序可以和其他的程序共享概功能或者数据给那那些与自己拥有相同数字证书的程序。如果某个权限(permission)的protectionLevel是signature，则这个权限就只

能授予那些跟该权限所在的包拥有同一个数字证书的程序。

5. **在签名时，需要考虑数字证书的有效期**:
(1)数字证书的有效期要包含程序的预计生命周期，一旦数字证书失效，持有改数字证书的程序将不能正常升级。
(2)如果多个程序使用同一个数字证书，则该数字证书的有效期要包含所有程序的预计生命周期。
(3)Android Market强制要求所有应用程序数字证书的有效期要持续到2033年10月22日以后。

6. 数字证书的要点:
Android数字证书包含以下几个要点:
(1)**所有的应用程序都必须有数字证书**，Android系统不会安装一个没有数字证书的应用程序
(2)Android程序包使用的数字证书可以是**自签名的**，不需要一个权威的数字证书机构签名认证
(3)**如果要正式发布一个Android，必须使用一个合适的私钥生成的数字证书来给程序签名**，而不能使用adt插件或者ant工具生成的调试证书来发布。
(4)数字证书都是有**有效期**的，Android只是在应用程序安装的时候才会检查证书的有效期。如果程序已经安装在系统中，即使证书过期也不会影响程序的正常功能。
(5)Android使用标准的java工具 **Keytool and Jarsigner** 来生成数字证书，并给应用程序包签名。
6）使用 **zipalign**优化程序。

数字签名的两种模式

我们都知道Android系统不会安装运行任何一款未经数字签名的apk程序，无论是在模拟器上还是在实际的物理设备上。所以我们会有一个疑问，为何在日常开发过程中我没有进行任何签名的操作，程序都会在模拟器和真机上运行？下面我们来讲讲

APK程序的两种模式：　调试模式(debug mode)和发布模式(release mode)

1. 调试模式(debug mode)：　在调试模式下，　ADT会自动的使用debug密钥为应用程序签名，因此我们可以直接运行程序。

debug密钥:　　一个名为debug.keystore的文件

存放位置：　C:\Users\Xiaopeng\.android\debug.keystore　　Xiaopeng对应替换为自己操作系统的用户名

两个风险：

debug签名的应用程序有这样两个风险：

1）debug签名的应用程序不能在Android Market上架销售，它会强制你使用自己的签名；

2）debug.keystore在不同的机器上所生成的可能都不一样，就意味着如果你换了机器进行apk版本升级，那么将会出现上面那种程序不能覆盖安装的问题。

不要小视这个问题，如果你开发的程序只有你自己使用，当然无所谓，卸载再安装就可以了。但要是你的软件有很多使用客户，这就是大问题了，就相当于软件不具备升级功能！

所以一定要有自己的数字证书来签名；

2. 发布模式(release mode)： **当要发布程序时，开发者就需要使用自己的数字证书给apk包签名**

使用自己的数字证书给APK签名的两种方法：

(1)通过DOS命令来对APK签名。
(2)使用ADT Export Wizard进行签名