文章编号 :1005-1228 (2011) 02-0030-03

一种基于 PKI 数字签名的电信设备许可证保护方法

杨志存[1],许希斌[2],李云洲[2],丁国鹏[2]

(1. 厦门大学信息科学与技术学院,福建 厦门 361005;
2. 清华大学信息技术研究院无线与移动通信技术研究中心,北京 100084)

摘 要 :基于软件的保护方式主要有注册码和许可证文件,文章介绍了将单向散列函数同公开密钥相结合实现数字签名的技术,提出了一种软件许可证生成、验证的许可系统,并基于 GNU 开源库 Libgcrypt 为电信设备实现许可证系统。与传统技术相比,该系统具有简单易用、安全可靠的特点。

关键词 :Libgcrypt 库 ;许可证文件 ;数字签名 ;签名校验 ;RSA
中图分类号 :TP309 文献标识码 :A

Implementation of License File Scheme Through Modified Digital Signature Scheme Based on PKI

YANG Zhi- cun[1],XU Xi- bing[2],LI Yun- zhou[2],DING Guo- peng[2]

(1.Communication Engineering,Xiamen University,Xiamen 361005,China
2.Wireless and Mobile Communication Technology R&D Center,Research Institute of Information Technology,
Tsinghua University,Beijing 100084)

Abstract :There are two main methods, i.e.License Key and License File in software copyrights protection area based on soft mode.This paper constructed digital signature adopting public key cryptography technique and Hashing,and then proposed a new license flie generation and validation system ,and also gave detailed design and implemention based on Libgcrypt which belongs to GNU. This system is easier and safer to use.

Key words: Libgcrypt; license file; digital signature; signature verification; RSA

现在越来越多的电信设备使用基于软件的许可证方式来实现版权保护，通过许可证文件对合法用户进行授权,设备在合法的许可证文件的控制下运行。许可证文件规定了哪些用户可以合法使用设备，以及使用设备的哪些功能。传统的许可证系统通过私钥生成数字签名并形成许可证文件，然后把许可证文件和公钥传输给合法的设备，设备通过公钥对许可证文件进行数字签名的校验。由于公钥需要由服务器传输给设备，可能被第三方窃取，通过高性能计算机分析破解可能得到对应的私钥，从而可以自行生成合法的许可证文件。本文在分析传统许可证系统的基础上，参考文献[1~2]设计了新的许可证系统,在许可证服务器侧和设备侧基于密钥生成参数独立地生成相同的密钥对,服务器通过密钥对中的私钥生成数字签名并形成许可证文件，设备通过密钥对中的公钥校验许可证文件。这样,由于不需要直接传输公钥,而是传输密钥对生成参数,密钥的安全性更高。

1 数字签名

1.1 公开密钥体制

公钥密码体制[3]也被称作非对称密码体制,它是现代密码学的一个重要分支,也是数字签名[4]技术的基础,现有的数字签名方案,大多数是建立在公钥密码学基础之上的。目前,比较成熟的公钥密码体制主要有两类 :一类是基于大整数因子分解问题的,其中最典型的代表是 RSA 体制；另一类是基于离散对数问题的,比如 EIGamal 公钥密码和影响比较大的椭圆曲线公钥密码。

RSA 算法 [5] 是 Rivest,Shamir 和 Adieman 于 1978 年在美国麻省理工学院研制出来的，RSA 算法的体制构造是基于数论的欧拉定理，其安全性依赖于大数因子分解的困难性。RSA 算法既可用于加密,也可以用

收稿日期 :2011- 02- 18
作者简介 :杨志存 (1986-) ,男,硕士研究生,研究方向 :无线移动通信 ;许希斌 (1968-) ,男,硕士生导师,研究员,研究方向 :无线移动通信和宽带无线传输技术。

于数字签名。RSA 算法流程如下：

选择两个不同的大素数[6-7]，计算乘积 $n=p\times q$ 和欧拉函数值 $\varphi(n)=(p-1)\times(q-1)$，然后随机选取一整数 $e\in Z$，满足 $1\le e\le\varphi(n)$ 且 $\gcd(e,\varphi(n))=1$，此时可求得 d 以满足 $ed\equiv 1 \bmod \varphi(n)$，则 $d\equiv e^{-1}\bmod\varphi(n)$。

这样，得到公开密钥 {e，n}，私有密钥 {d，n}（p，q，$\varphi(n)$ 均需严格保密）

在 RSA 系统中，设 m 为明文且 m<n，c 为密文，则加密和解密算法如下：

加密算法　$c=E(m)\equiv m^e \pmod n$　　(1)

解密算法　$m=D(c)\equiv c^d \pmod n$　　(2)

RSA 数字签名 / 校验与加密 / 解密类似，一般对明文信息 m 先作 Hash 运算得摘要值 h（m），

数字签名　$s=(h(m))^d \bmod n$　　(3)

签名校验　$\overline{m}=s^e \bmod n$　　(4)

然后检查 $\overline{m}=h(m)$ 是否成立，即可鉴别签名是否正确。

1.2　单向散列函数（Hash 函数）

Hash 函数[8]也是密码学的一个基本工具，在数字签名、检验信息的完整性等有关方面有重要应用，Hash 函数的安全性直接关系到数字签名技术的安全性。Hash 函数是一个将不等长消息压缩为固定长度消息的确定性算法 h，它具有如下性质：

(1) 单向性质　任给消息 x，计算 h(x) 是容易的，而由 h(x)计算 x 是不可行的。

(2) 抗冲突性　要找两个不同的消息 x1，x2 使得 h(x1)=h(x2) 是计算上不可行（困难）的。

(3) 映射分布均匀性　在散列值 h(x) 中，0bit 和 1bit 的个数应该是相当的，且输入中 1 个 bit 位的变化，应导致散列值中一半以上的 bit 位发生变化。

总之，Hash 具有单向性，强抗碰撞性、初始值敏感性和计算快速性的特点。

2　改进的电信设备许可证系统

传统的许可证系统一般包括许可证服务器和客户端（实际加载许可证文件的设备），服务器主要是为不同的设备按照设备提供的信息产生密钥对，提取公钥 {e，n}和私钥 {d，n}，并通过私钥生成数字签名，形成许可证文件。将公钥、私钥、许可证保存在相应的数据库中，并维护密钥数据库和许可证数据库。服务器将公钥 {e，n}和许可证文件传输给设备，设备通过公钥 {e，n}来校验许可证文件的数字签名。

本电信设备许可证系统根据实际应用场景对传统的许可证系统做了改进，即在服务器侧和设备侧独立地产生密钥对，服务器和设备基于相同的密钥对生成参数产生相同的密钥对，服务器提取私钥 {d,n}，通过私钥生成数字签名并形成许可证文件；设备提取公钥 {e,n}，通过公钥校验许可证文件的数字签名。与传统的许可证系统相比，本文设计的许可证系统不直接传输公钥，而是传输密钥生成参数，有效地防止了第三方获得密钥并破解，提高了系统的安全性。具体做法是许可证服务器和设备都基于设备的唯一标识 ESN 和随机种子 RAND 值，来产生 RSA 密钥体制中的两个初始化素数 p，q，然后选取私钥 d（私钥 d 由 ESN 和 RAND 唯一确定），就产生相同的 e，即得到相同的公钥 {e，n}和私钥 {d,n}。服务器提取私钥 {d,n}，通过私钥生成数字签名并形成许可证文件；设备提取公钥 {e,n}，通过公钥校验许可证文件的签名。

2.1　服务器侧

电信设备的功能由若干个 Feature 功能项组成，图 1 为一个 Feature 的签名。首先为设备生成随机种子 RAND 值，并读取设备唯一标识 ESN，以 ESN 和 RANG 值产生初始化的 p、q，调用密钥生成函数，生成唯一的密钥对，从密钥对中提取私钥，通过提取的私钥对设备的 Feature 逐个生成数字签名，最终形成许可证文件，详细流程如图 1 所示：

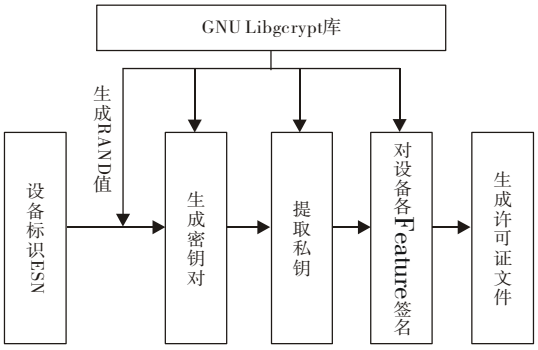

图 1　服务器生成许可证文件

具体到许可证文件中单个 Feature 的签名，流程如图 2 所示。首先对 Feature 明文作 Hash 摘要，然后用上述提取的私钥对摘要作签名，将签名信息 Sign 附在明文 Feature 之后，就完成了一个 Feature 的签名，依次可以对所有的 Features 签名，从而得到带有 RSA 数字签名的许可证文件。

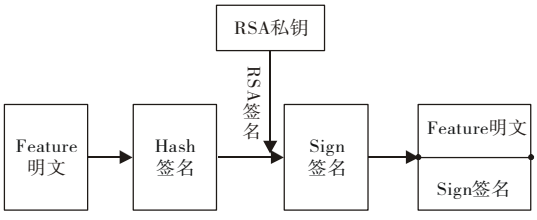

图 2　单个 Feature 的数字签名

2.2 设备侧

设备侧通过公钥实现对许可证文件的校验，是服务器侧许可证文件签名的逆过程，具有处理流程如图 3，其中，密钥对的产生及公钥的提取与服务器侧相同。

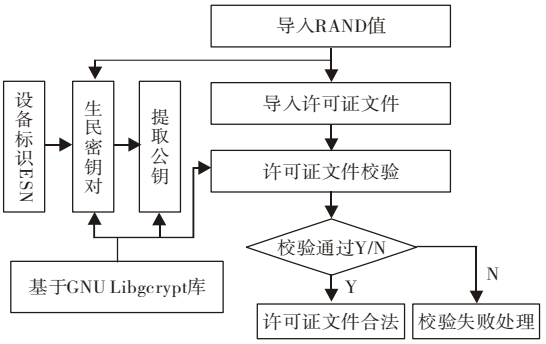

图 3 许可证文件的校验

首先设备导入从服务器接收到的随机种子 RAND 值并加载许可证文件，同时读取设备唯一标识 ESN，以 ESN 和 RANG 值作为输入产生初始化的 p、q，与服务器侧生成相同的密钥对并提取出公钥{e,n}，进入许可证文件校验模块，通过公钥{e,n}依次完成对各个 Feature 的校验。对于校验通过的 Feature，则激活对应的功能；对于校验失败的 Feature，则进入校验失败相应的处理（如：提示用户该 Feature 对应的功能校验失败，或及时付费或请求用户联系厂商等）。

具体到许可证文件中单个 Feature 签名的校验，流程如图 4 所示。首先对 Feature 明文作 Hash 变换，得到 Hash 摘要；同时用对应的 RSA 公钥校验 Feature 的签名，得到相应的 Hash 摘要。如果 Feature 明文得到的摘要和签名校验得到的摘要匹配，则校验通过，激活该 Feature 对应的功能；同样，如果摘要不匹配，则进行校验失败相关处理。

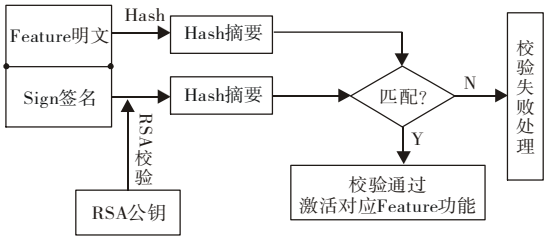

图 4 单个 Feature 签名的校验

3 许可证方法的实现

本文设计的电信设备许可证系统，可以在 Linux 平台上基于 Libgcrypt 来实现，Libgcrypt 是 GNU 的开源加密库，基于数据结构 MPI（multi_precision- integers）和 S 表达式（S_expressions）[9]，支持常见的对称密钥加密算法，公开密钥加密算法和 Hash 算法。

3.1 公钥 / 私钥对的生成及提取

GNU 的 Libgcrypt 库是随机生成密钥对的，主要是 p、q 是选取随机的。本文设计的许可证许可系统要求许可证服务器和设备生成相同的密钥对，因此需要修改 Libgcrypt 库密钥生成部分。通过 ESN 和 RANG 值分别初始化 p、q，同时密钥对中的私钥 d 也由 ESN 和 RANG 值唯一确定。

创建存放密钥对的 S 表达式 gcry_sexp_new（&key_spec,"（genkey（rsa（nbits 4:1024））",0,1）；

调用密钥生成函数 gcry_pk_genkey（&key, key_spec）；将生成的密钥对按照 key_spec 设定的格式存放在 S 表达式变量 key 中。

提取公钥 {e,n}：由函数 pub_key = gcry_sexp_find_token（key,"public- key",0）实现。如图 5 所示：

```
(public-key
 (rsa
  (n #00D408F0D668AF7BF7ED255003D2536B2E4D1AC87DD650FC9A4209D373FFE7AF24201211F5
9C736C6705E4C53E2420EC7B4BD47FD5E82791DB2FF58D9206D67D11B73BDC10246DAAC20332A692
91CA23986BD0D744633C9A48C5F55B3849DD678ED32ADFE1E08522728CD847F3D2538FF7794C7759
7D41F331EBA79242961C5C6F#)
  (e #010001#)
 )
)
```

图 5 从密钥对中提取公钥{e,n}

提取私钥{d,n}：由函数 gcry_sexp_find_token（key, "private- key",0）实现。如图 6 所示：

```
(private-key
 (rsa
  (n #00D408F0D668AF7BF7ED255003D2536B2E4D1AC87DD650FC9A4209D373FFE7AF24201211F5
9C736C6705E4C53E2420EC7B4BD47FD5E82791DB2FF58D9206D67D11B73BDC10246DAAC20332A692
91CA23986BD0D744633C9A48C5F55B3849DD678ED32ADFE1E08522728CD847F3D2538FF7794C7759
7D41F331EBA79242961C5C6F#)
  (d #3496C519009CE99BDBC3301DDF8C7FCD0DE89D28937631DCBAAAE62362695D1801DBE2D9B23
C312F358685DAD646B900BA28AA16C2DE8C689BD12E39A80BCA9070CBB4D8E2248FFA78DE0DAD594
EBF3AB72BD1962AB9B8A5A6B6D281A0B7F1727F9B3D7875FF4AAB929A98067CB549EA403084744300
0F0A63E187FCC0028BC10D#)
 )
)
```

图 6 从密钥对中提取私钥{d,n}

3.2 Hash 摘要

genhash(char *ch)函数依次调用 Libgcrypt 库的以下函数 gcry_md_open（），gcry_md_enable（），gcry_md_write（），gcry_md_read（），gcry_md_close（）实现对 Feature 的 Hash 摘要。

将 Feature 生成的 Hash 摘要写进 S 表达式，如图 7 所示：

```
(data
 (flags pkcs1)
 (hash sha256 #85F16E0EE7E6DDAC1B052A30C0357D028BD665E09D423A16CE451FC6FF867914#
)
```

图 7 Feature 生成的 Hash 摘要

由函数 gcry_sexp_build（&data,NULL,"（data（flags pkcs1）（hash sha256 %s））",ch）实现。

3.3 签名生成及校验

利用提取的私钥{d,n}对 Hash 值进行加密，得到签名 Sign 信息，如图 8 所示：

（下转第 54 页）

控制的感受和认识，关于 AUTHORWARE 软件对 midi 音乐的控制最重要的理念就是应该根据不同的 midi 音乐播放要求去制定合理且简洁的控制方法，在这一过程中，制作者应该熟练掌握 AUTHORWARE 软件中声音的基本控制功能，在此基础上再系统地对一些音频控制函数加以理解，并在实践中不断地进行实验和运用，在不断总结的基础上就一定能在自身的课件开发中把 MIDI 音乐用好。

参考文献：

[1] 刘丽华，刘世普.Authorware 中声音的处理技术[J].河北大学学报（自然科学版），2001（3）:325- 327.

[2] 赵伟.Authorware 多媒体课件中的音乐控制设计[J].丹东纺专学报，2004（4）:37－39.

[3] 朱卫锋.Authorware 中的声音控制[J].计算机时代，2001（3）:43－44.

[4] 李学梅.多媒体课件中的声音控制技术——以 Authorware 为例[J].邵阳师范高等专科学校学报，2000（5）:58－59.

[5] 董全德.AUTHORWARE 声音控制[J].黄山学院学报，2005（3）:75- 76.

（上接第 32 页）

```
(sig-val
 (rsa
  (s #40693ACA400A71ADD07168F624E380E95ECD6B8429E2171845CF1CDF8510D133111D54AEE6
DF13E86F4672A7D590A69C3A5275963205290A068FFCC4AABF993537B02E81A645E6827D85CB159B
0112CE9ECOA1#)
  )
 )
```

图 8 RSA 对 Feature 的签名

由函数 gcry_pk_sign（&sig，data，sec_key）实现。

设备在使用许可证文件时，对签名进行校验，首先对 Feature 明文作摘要变换，得到摘要值 h（m），流程如 4.2 节所示，并将 Feature 生成的 Hash 摘要 h（m）写进 S 表达式 data。

校验通过 gcry_pk_verify（sig，data，pub_key）；实现，利用提取的公钥{e，n}对签名 Sign 解密得到摘要值 $\overline{m}$，然后检查 $\overline{m}$=h（m）是否成立。

4 分析及结论

本文设计的许可证方法，在传统的许可证方法上加以改进，不直接传输密钥，而是传输密钥生成参数 ESN 和 RANG 值，密钥更隐蔽、更安全。服务器和设备基于密钥生成参数独立地产生相同的密钥对。设备标识 ESN 一般选取设备的硬件编号，如硬盘序列号、网卡 MAC 地址及系统处理器型号等，为保密起见，还可以将设备标识 ESN 通过哈希算法生成固定长度的摘要值 h（ESN）作为 ESN，这样安全性更高；随机种子 RAND 值由许可证服务器随机产生，与设备一一对应，与许可证文件一起传给设备。

ESN 和 RAND 值与密钥的双重绑定提高了系统的安全性，可以更有效地防止非法伪造或篡改许可证文件，如果结合软件自检测防篡改技术[10]及反跟踪技术，还可以进一步提高系统安全性，保护知识产权。

参考文献：

[1] 张杰.一种密钥传递及数字签名的方法[P]. 中国专利: CN1255002，2000- 05- 31.

[2] 孙吉平，韩勇.一种安全地生成密钥对和传送公钥或证书申请文件的方法[P]. 中国专利: CN101170407, 2008- 04- 30.

[3] Carlisle Adams Steve Lloyd.公开密钥基础设施——概念、标准和实施[M].冯国登，译.北京:人民邮电出版社.

[4] W.Diffe rand M.Hellman,New directions in cryptography[J].IEEE Trans. Information Theory,1976,22,pp.644- 654.

[5] RIVEST R J, SHAMIR A L. A method for obtaining digital signature and public key cryptosystem[J]. Communications of the ACM, 1978, 21（2）: 120- 126.

[6] 张宏，刘晓霞，张若岩. RSA 公钥密码体制中安全大素数的生成[J].计算机技术与发展，2008，（09）:132- 134.

[7] 游新娥，田华娟.一种快速的强素数生成方法[J].通信技术，2009（02）:323- 325.

[8] LAMPORT L. Password authentication with insecure communication[J]. Communications of the ACM，1981，24（11）:770- 772.

[9] http://people.csail.mit.edu/rivest/sexp.html[EB- OL].

[10] 沈海波，史毓达.计算机软件的防篡改技术.现代计算机，2005，205（2）:45- 48.