

互联网安全之数字签名、数字证书与PKI系统



作者 hi_xgb (/u/38c473816ca5) + 关注

2016.11.26 00:39* 字数 2458 阅读 892 评论 7 喜欢 17

(/u/38c473816ca5)



在现代社会，互联网已经渗透到人们日常生活的方方面面，娱乐、经济、社会关系等都离不开互联网的帮助。在这个背景下，互联网安全就显得十分重要，没有提供足够的安全保障，人们是不会如此依赖它的。幸运的是，在大牛们的努力下，很早以前就有一套安全体系来保障互联网信息的传递。下面我们一起来了解一下这套体系。

加密算法

首先我们需要了解一下加密相关的知识，加密可以分为**对称加密**和**非对称加密**。两者的主要区别就是是否使用同一个密钥，对称加密需要用同一个密钥。非对称加密不需要用同一个密钥，而是需要两个密钥：公开密钥（publickey）和私有密钥（privatekey），并且加密密钥和解密密钥是成对出现的。

对称加密

对称加密算法的特点是算法公开、计算量小、加密速度快、加密效率高。对称加密有很多种算法，由于它效率很高，所以被广泛使用在很多加密协议的核心当中。不足之处是，交易双方都使用同样钥匙，安全性得不到保证。常见的对称加密有 DES、AES 等。

非对称加密

非对称加密使用一对“私钥-公钥”，用私钥加密的内容只有对应公钥才能解开，反之亦然。非对称加密有以下特性：

- 对于一个公钥，有且只有一个对应的私钥。
- 公钥是公开的，并且不能通过公钥反推出私钥。
- 通过私钥加密的密文只能通过公钥能解密，通过公钥加密的密文也只能通过私钥能解密。



非对称加密不需要共享同一份密钥，安全性要比对称加密高，但由于算法强度比对称加密复杂，加解密的速度比对称加解密的速度要慢。常见的非对称加密有 RSA、ESA、ECC 等。

摘要算法

除了加密算法，摘要算法在互联网安全体系中也扮演了重要的角色。摘要算法有以下特性：

- 只要源文本不同，计算得到的结果，必然不同（或者说机会很少）。
- 无法从结果反推出源数据。

基于以上特性，我们一般使用摘要算法来校验原始内容是否被篡改。常见的摘要算法有 MD5、SHA 等。

Tips: 摘要算法不能算作加密算法，加密算法需要使用密钥加解密，但摘要算法无法根据结果反推出内容。另外 MD5 目前也不算安全了，例如彩虹表攻击 (<https://zh.wikipedia.org/wiki/%E5%BD%A9%E8%99%B9%E8%A1%A8>)。

具体例子

假设甲公司要给乙公司发送一份机密的文件，那么这次传输需要确保以下几点：

1. 文件内容不能被读取（加密）
2. 文件内容不能被篡改（数字签名）
3. 文件不能被掉包（数字证书）

加密

对称加密需要用同一份密钥，这一份密钥的约定就有被中途截获的可能。因此可以采用非对称加密算法加密对称密钥的方式来加密内容，也就是用乙的公钥加密对称密钥，并用这个对称密钥加密文件内容。

假设这份文件被黑客截获，但是黑客没有乙的私钥无法解出对称密钥，也就无法解密文件内容。但是这里有个风险，虽然黑客无法解密文件内容，但他可以自己生成一份密钥并用乙的公钥加密，再用这份密钥加密一份伪造的文件发给乙，这种情况下乙收到的就是被篡改的文件。

数字签名

上面提到乙有可能收到被篡改的文件，这个问题可以用数字签名的方式解决，数字签名就是用**摘要算法**提取出源文件的摘要并用私钥进行加密后的内容。针对上面那个问题，甲在发送文件时再附上源文件的数字签名。如果被黑客截取到加密后的文件和数字签名，黑客即使使用甲的公钥解出了文件摘要，由于摘要算法的特性黑客也无法还原出原始内容。但乙可以解密出文件内容再用同样的摘要算法提取出摘要来和数字签名里的摘要进行比对，摘要一致则说明文件没有被篡改过。

到目前为止还有一个风险就是乙无法确定自己用的公钥就是甲提供的，如果黑客将乙手里的甲的公钥替换成自己的并用自己的私钥生成数字签名，那么乙还是会受到被篡改的文件。

数字证书

数字证书的出现就是为了解决上述提到的问题，数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。



数字证书里一般会包含公钥、公钥拥有者名称、CA 的数字签名、有效期、授权中心名称、证书序列号等信息。

数字证书如何确保列出的用户就是公钥的拥有者呢？关键点是 CA 的数字签名，CA会用自己的私钥将证书内容的摘要进行加密。因为 CA 的公钥是公开的，任何人都可以用公钥解密出 CA 的数字签名的摘要，再用同样的摘要算法提取出证书的摘要和解密 CA 数字签名后的摘要比对，一致则说明这个证书没有被篡改过，可以信任。

PKI

PKI（Public Key Infrastructure）翻译过来就是公钥基础设施，可以理解为利用公钥技术为网络应用提供加密和数字签名等密码服务以及必需的密钥和证书管理体系。它是一个提供安全服务的基础设施，PKI 技术是信息安全技术的核心，同时也是电子商务的关键和基础技术。

PKI 既不是一个协议，也不是一个软件，它是一个标准，在这个标准之下发展出的为了实现安全基础服务目的的技术统称为 PKI。

PKI是一个标准，它包括一些基本的组件，不同的组件提供不同的服务，主要由一下几个组件组成：

- 认证中心 CA(证书签发)：CA 机构，又称为证书授证 (Certificate Authority) 中心，是 PKI 的"核心"，即数字证书的申请及签发机关，CA 必须具备权威性的特征，它负责管理 PKI 结构下的所有用户(包括各种应用程序)的证书，把用户的公钥和用户的其他信息捆绑在一起，在网上验证用户的身份，CA 还要负责用户证书的黑名单登记和黑名单发布。
- X.500目录服务器(证书保存)：X.500目录服务器用于"发布"用户的证书和黑名单信息，用户可通过标准的 LDAP 协议查询自己或其他人的证书和下载黑名单信息。
- 具有高强度密码算法(SSL)的安全 WWW 服务器(即配置了 HTTPS 的apache)：Secure socket layer(SSL)协议最初由 Netscape 企业发展，现已成为网络用来鉴别网站和网页浏览者身份，以及在浏览器使用者及网页服务器之间进行加密通讯的全球化标准。
- Web(安全通信平台)：Web 有 Web Client 端和 Web Server 端两部分，分别安装在客户端和服务端，通过具有高强度密码算法的 SSL 协议保证客户端和服务端数据的机密性、完整性、身份验证。
- 自开发安全应用系统：自开发安全应用系统是指各行业自开发的各种具体应用系统，例如银行、证券的应用系统等。

总结

数字签名和数字证书是两个不同的概念，理解的关键点是数字签名是内容提供方用自己的私钥对内容摘要（MD5、SHA）非对称加密，而数字证书的关键是 CA 用自己的私钥对证书内容的摘要非对称加密从而确保证书内的用户合法拥有证书里列出的公钥。

理解了这两个概念后再回头去看前面例子里的流程就很清楚了，后面有空再说明下 HTTPS 密钥协商的过程~

HTTPS 密钥协商过程参考这篇文章 (<http://www.jianshu.com/p/7158568e4867>)

参考资料



<http://www.enkichen.com/2016/04/12/certification-and-pki/>
(<http://www.enkichen.com/2016/04/12/certification-and-pki/>)
<https://my.oschina.net/dyyweb/blog/653631>
(<https://my.oschina.net/dyyweb/blog/653631>)
http://www.ruanyifeng.com/blog/2011/08/what_is_a_digital_signature.html
(http://www.ruanyifeng.com/blog/2011/08/what_is_a_digital_signature.html)

📖 日记本 (/nb/264532) 举报文章 © 著作权归作者所有



hi_xgb (/u/38c473816ca5)
写了 33413 字，被 683 人关注，获得了 1142 个喜欢
(/u/38c473816ca5)




+ 关注

iOS程序猿，探索世界中

如果觉得我的文章对您有用，请随意打赏。您的支持将鼓励我继续创作！


赞赏支持

🤍 喜欢 | 17




更多分享

(<http://cwb.assets.jianshu.io/notes/images/7219696>)



写下你的评论...


7条评论 只看作者 按喜欢排序 按时间正序 按时间倒序



股票三剑客战法 (/u/b0b361e562f0)
2楼 · 2016.11.26 11:10
(/u/b0b361e562f0)
当初我在一个软件编写公式时设置了密码9年了，早已经忘记其中的密码怎么破解，通过信股票分析软件

👍 赞

💬 回复



fhammer (/u/81a4f38eacf7)
3楼 · 2016.12.15 10:36
(/u/81a4f38eacf7)
数字签名的部分，甲持有公钥，作为数据发送方，已是持有私钥的，甲应该没有私钥，这时甲如何对发送内容摘要进行私钥加密生成数字签名？烦请解惑啊


👍 赞

💬 回复

hi_xgb (/u/38c473816ca5): @fhammer (/users/81a4f38eacf7) 你好，这个例子里假设双方事先已经交换过公钥了，这里甲是用自己的私钥加密文件摘要。如果没有事实先交换过公钥，那就需要用到数字证书，数字证书就是为了确保公钥的合法性，证书中包含公钥，CA认证通过后取出来的公钥就可以用来解密签名的摘要，再比对摘要是否一致来判断文件是否被篡改。

2016.12.15 11:02 💬 回复

✍️ 添加新评论



鼻毛长长 (/u/43b986cdcf7b)
4楼 · 2016.12.16 17:27
(/u/43b986cdcf7b)

+

🔖

🔗

假设这份文件被黑客截获，但是黑客没有乙的私钥无法解出对称密钥，也就无法解密文件内容。但是这里有个风险，虽然黑客无法解密文件内容，但他可以自己生成一份密钥并用乙的公钥加密，再用这份密钥加密一份伪造的文件发给乙，这种情况下乙收到的就是被篡改的文件。

乙不仅有私钥还有公钥？

👍 赞 💬 回复


hi_xgb (/u/38c473816ca5): @鼻毛长长 (/users/43b986cdf7b) 双方都有公钥和私钥

2016.12.16 18:31 💬 回复

鼻毛长长 (/u/43b986cdf7b): @hi_xgb (/users/38c473816ca5) 不是 服务端有私钥，客户端有公钥吗？

2016.12.17 11:02 💬 回复

✎ 添加新评论



乃铭 (/u/ad8fc6d2c588)
5楼 · 2017.03.28 14:35

(/u/ad8fc6d2c588)

写的很清楚，如果有图就更好了

👍 赞 💬 回复

被以下专题收入，发现更多相似内容

+

我的专题

互联网科技

IT共论

iOS学习
笔记

程序员

iOS
Dev...

首页投稿

工作

HTTP/操作...

+

🔖

🔗