

关于证书的那些事：自签名证书和私有CA签名证书等

SuperRoot

0.9032017.07.14 20:51:42李敏1.977阅读10,084

证书的三个作用 加密通信和身份验证(验证对方确实是对方声称的对象)和数据完整性(无法被修改,修改了会被知)

证书类型:

x509的证书编码格式有两种

1.PEM(Privacy-enhanced Electronic Mail) 是明文格式的 以 -----BEGIN CERTIFICATE-----开头, 已-----END CERTIFICATE-----结尾, 中间是经过base64编码的内容.apache需要的证书就是这类编码的证书 查看这类证书的信息的命令为: openssl x509 -noout -text -in server.pem

其次PEM就是把DER的内容进行了一次base64编码

2.DER 是二进制格式的证书 查看这类证书的信息的命令为: openssl x509 -noout -text -inform der -in server.der

扩展名:

.crt 证书文件, 可以是DER(二进制)编码的, 也可以是PEM(ASCII (Base64))编码的, 在类unix系统中比较常见

.cer 也是证书 常见于Windows系统 编码类型同样可以是DER或者PEM的, windows 下有工具可以转换crt到cer

.csr 证书签名请求 一般是生成请求以后发送给CA, 然后CA会给你签名并颁发证书

.key 一般公钥或者密钥都会用这种扩展名, 可以是DER编码的或者是PEM编码的 查看DER编码的(公钥或者密钥)的文件的命令为 openssl rsa -inform DER -noout -text -in xxx.key 查看PEM编码的(公钥或者密钥)的文件的命令为 openssl rsa -inform PEM -noout -text -in xxx.key

.p12 证书 包含一个X509证书和一个被密码保护的私钥

自签名证书和CA签名证书的区别

自签名的证书无法被吊销, CA签名的证书可以被吊销 能不能吊销证书的区别在于, 如果你的私钥被黑客获取, 如果证书不能被吊销, 则黑客可以伪装成你与用户进行通信

如果你的规划需要创建多个证书, 那么使用私有CA的方法比较合适, 因为只要给所有的客户端都安装了CA的证书, 那么该证书签名过的证书, 客户端都是信任的, 也就是安装一次就够了 如果你直接用自签名证书, 你需要给所有的客户端安装该证书才会被信任, 如果你需要第二个证书, 则还的挨个给所有的客户端安装证书2才会被信任。

****Linux下使用OpenSSL生成证书****

利用OpenSSL生成库和命令程序, 在生成的命令程序中包括对加/解密算法的测试.openssl程序.ca程序.利用openssl.ca可生成用于C/S模式的证书文件以及CA文件。

证书文件的生成步骤:

一、服务器端

1.生成服务器端的私钥(key文件):

openssl genrsa -des3 -out server.key 1024

运行时会提示输入密码,此密码用于加密key文件(参数des3是加密算法,也可以选用其他安全的算法),以后每当需读取此文件(通过openssl提供的命令或API)都需要输入口令.如果不要口令,则可用以下命令去除口令:

openssl rsa -in server.key -out server.key

生成无需密码的服务器私钥, 如果私钥是有密码的, 则每次启动web服务器都会要求你输入密码

2.生成服务器端证书签名请求文件(csr文件):

openssl req -new -key server.key -out server.csr

生成Certificate Signing Request(CSR).生成的csr文件交给CA签名后形成服务器自己的证书.屏幕上将有提示,依照其 提示一步一步输入要求的个人信息即可(如:Country,province,city,company等)。

```
root@localhost:~#openssl req -x509 -key server.key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
e is 65537 (010001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
root@localhost:~#openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a distinguished name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:Sh
Locality Name (eg, city) [Default: City]:Shanghai
Organization Name (eg, company) [Default: company Ltd]:local
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:localhost.localdomain
Email Address []:li
Please enter the following vector attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@localhost:~#openssl req -x509 -key server.key -out ca.crt
ca.crt: ca.key, server.csr, server.key
```

****注意: 前方高能预警 ! ! ! ! ****

最重要的是有一个common name, 可以写你的名字或者域名.如果为了https请求, 这个必须和域名吻合, 否则会引起浏览器警告。

二、客户端

1.对客户端也作同样的命令生成key及csr文件:

openssl genrsa -des3 -out client.key 1024

openssl req -new -key client.key -out client.csr

```
root@localhost:~#openssl req -x509 -key client.key 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
e is 65537 (010001)
Enter pass phrase for client.key:
Verifying - Enter pass phrase for client.key:
root@localhost:~#openssl req -new -key client.key -out client.csr
Enter pass phrase for client.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a distinguished name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:Shanghai
Locality Name (eg, city) [Default: City]:Shanghai
Organization Name (eg, company) [Default: company Ltd]:local
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:localhost.localdomain
Email Address []:li@localhost.localdomain
Please enter the following vector attributes
to be sent with your certificate request
A challenge password []:12345678
An optional company name []:local
root@localhost:~#openssl req -x509 -key client.key -out ca.crt
ca.crt: ca.key, client.csr, client.key, server.csr, server.key
```

三、生成CA证书文件

server.csr与client.csr文件必须有CA的签名才可形成证书。

1.首先生成CA的key文件:

openssl genrsa -des3 -out cakey 1024

2.生成CA自签名证书:

openssl req -new -x509 -key cakey -out ca.crt

可以加证书过期时间选项 "-days 365".

```
root@localhost:~#openssl genrsa -des3 -out cakey 1024
Generating RSA private key, 1024 bit long modulus
.....+++++
e is 65537 (010001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:
root@localhost:~#openssl req -new -x509 -key cakey -out ca.crt
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a distinguished name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:Shanghai
Locality Name (eg, city) [Default: City]:Shanghai
Organization Name (eg, company) [Default: company Ltd]:local
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:localhost.localdomain
Email Address []:li@localhost.localdomain
root@localhost:~#openssl req -x509 -key cakey -out ca.crt
ca.crt: ca.key
```

四、利用CA证书进行签名

方法一:

可以加证书的有效时间选项 "-days 365",也可以不加时间, 标识永久有效

openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey cakey -set_serial 01 -out server.crt

方法二:

用生成的CA证书为server.csr,client.csr文件签名,利用openssl中附带的CA.pl文件

1. 在提示输入已有的证书文件时,输入上面已生成的ca.crt证书文件:

ca.pl -newca

推荐阅读

Docker 开箱远程安全访问(0xxxx2376)

阅读 224

Http1.0、Http1.1和Http2.0以及Https

阅读 227

harbor容器镜像https

阅读 256

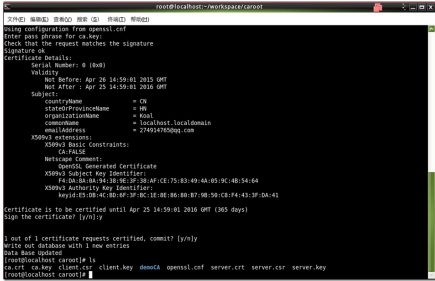
https 协议交互报文解析

阅读 288

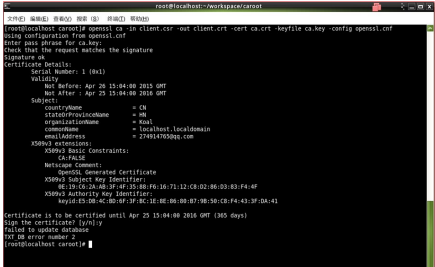
iOS 网络数据安全(防止抓包)

阅读 721

2.生成服务端证书文件
openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf



3.生成客户端证书文件
openssl ca -in client.csr -out client.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
必须保证openssl.cnf在当前目录下,这个文件可以在apps目录中找到.



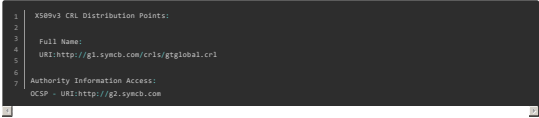
五、可能出现的错误
错误1:
error loading the config file 'openssl.cnf'
解决方法
find -name "openssl.c"
cp /usr/local/ssl/openssl.cnf ./
错误2:



解决方法
touch demoCA/serial
echo "00" > demoCA/serial

三 查看信息
openssl rsa -noout -text -in server.key 查看私钥信息
openssl req -noout -text -in server.csr 查看签名请求信息
openssl rsa -noout -text -in ca.key 查看ca的私钥信息
openssl x509 -noout -text -in ca.crt 查看证书信息
openssl crl -text -in xx.crl 查看一个证书吊销列表信息
openssl x509 -purpose -in cacert.pem 查看一个证书的例外信息
openssl rsa -in key.pem -pubout -out pubkey.pem 从一个私钥里面提取出公钥
openssl rsa -noout -text -pubin -in apache.pub 查看一个公钥的信息
openssl verify -CAfile 指定CA文件路径 apache.crt 验证一个证书是否是某一个CA签发
openssl s_client -connect 192.168.20.51:443 模拟一个ssl客户端访问ssl服务器 如果服务端要求客户端提供证书 则在加上 -cert 和 -key参数 比如 openssl s_client -connect 192.168.20.51:443 -cert client.crt -key clientkey
openssl pkcs12 -in path.p12 -out newfile.crt.pem -clerts -nokeys Mp12文件里面提取证书openssl pkcs12 -in path.p12 -out newfile.key.pem -nocerts -nodes Mp12文件里面提取私钥

现代浏览器检查一个证书是否仍然有效 两种方法 OCSP (Online Certificate Status Protocol, 在线证书状态协议) 和Crl (Certificate Revoke List, 证书吊销列表)
这些信息在CA的证书里面应该得有, 否则浏览器无法检查由该CA签过的证书是否还继续有效 (这句话属于猜测)
可以试一下导出给京东或者淘宝签名的CA证书 并用openssl x509 -noout -text -in ca.crt 查看一下, 就能看到这两类信息京东的证书是由GeoTrustSSL进行签名的, 导出GeoTrustSSL CA的证书 然后查看该CA的信息其中有一段信息是这样



这里说明了它的证书吊销列表地址和OSCP协议地址有兴趣的可以试试给淘宝签名的CA的证书信息

对巴证书吊销列表 各浏览器的行为可以参考一下两个地址
<http://news.netcraft.com/archives/2013/05/13/how-certificate-revocation-doesnt-work-in-practice.html>
<https://www.trustwave.com/Resources/SpiderLabs-Blog/Defective-By-Design---Certificate-Revocation-Behavior-In-Modern-Browsers/>

相关参考信息链接

<http://blog.csdn.net/sdcxyz/article/details/47220129>
<http://www.linuxidc.com/Linux/2015-05/117034.htm>

11人点赞

日记本

更多精彩内容,就在简书APP

“小礼物走一走,来简书关注我”
赞赏支持

还没有人赞赏,支持一下

SuperRoot 网络安全小白, 慢慢学习中
总资产2 共写了2.1W字 获得37个赞 共23个粉丝

关注

推荐阅读
半自动化创建CA和申请证书
1 概述 本文之所以称为半自动化, 是因为证书的申请并非日常工作, 只是一段时间才需要申请, 同时, 在创建证书和办法证...

更多精彩内容>

ghbsunny 阅读 1,459 评论 0 赞 1

openssl的证书格式转换

openssl的证书格式转换 证书转换 PKCS 全称是 Public-Key Cryptography Stan...

五大RobertWu翻译 阅读 8,194 评论 1 赞 3

每颗人间烟火全都美丽了我

人体的细胞全部更新一次的周期大约是6-7年。从现在起7年以后，你就是个崭新的自己。在23岁结束前谈了李英来的《七年...

— iPhonebook 阅读 158 评论 1 赞 1

席的重生, 摩西减肥蜕变记

我是来自青田幸福一号的王秋平,认识我的人都叫我摩西.原先我青田这边的工业区开了一家手机店,日复一日,年复一...

减肥帝摩西 阅读 212 评论 12 赞 6



十月雪中有感

雪飞寒天犹未信, 总叹神贫惜日巧。在再时光东流水, 功业可有建丝毫。2012.10.23

森森 阅读 75 评论 0 赞 0



写下你的评论...

评论1 赞11 ...