



原创

mm350670610

2010-04-29 15:44:00

 6991

 收藏 1

版权

文章标签：

[extension](#)[object](#)[ext](#)[string](#)[struct](#)[integer](#)

今天晚上打完球真累，没心思学习了，所以把这一阵学的OpenSSL的CRL大概总结一下。

CRL(Certificate Revocation List)，证书撤销列表，是在证书撤销时用的（好像是废话，晕）。当证书因为一些原因（比如，证书到期，证书私钥丢失等）会被CA吊销，CA为了让别人知道某个证书被吊销了，会定期发布一个CRL，CRL包含了在这个CRL发布时，被吊销的证书。客户端拿到这个CRL后，就可以知道哪些证书已经无效了。不过，CRL的发布是有一定的周期的，所以通过CRL的方法，客户端不能实时地检测某个证书是否有效。为了弥补CRL这个不足，现在一般都用 OCSP(Online Certificate Status Protocol)，在线证书状态协议。

CRL在的官方文档可以在RFC5280中看到。

CRL在OpenSSL中的表示是通过下面几个结构体完成的，结构体定义在文件x509.h中：

```
typedef struct X509_revoked_st
{
    //这个结构代表了一个被吊销的证书
    ASN1_INTEGER *serialNumber; //证书序列号
    ASN1_TIME *revocationDate; //被吊销的日期
    STACK_OF(X509_EXTENSION) /* optional */ *extensions;
    int sequence; /* load sequence */
} X509_REVOKED;

typedef struct X509_crl_info_st
{
    //CRL的信息
    ASN1_INTEGER *version; //CRL的版本号
    X509_ALGOR *sig_alg; //CRL所使用的签名算法
    X509_NAME *issuer; //CRL的发布者
    ASN1_TIME *lastUpdate; //CRL发布的日期
    ASN1_TIME *nextUpdate; //下一次发布CRL的日期
    STACK_OF(X509_REVOKED) *revoked; //被吊销的证书的序列
    STACK_OF(X509_EXTENSION) /* [0] */ *extensions;
    ASN1_ENCODING enc;
} X509_CRL_INFO;

struct X509_crl_st
{
    //CRL结构体
    /* actual signature */
    X509_CRL_INFO *crl;
    X509_ALGOR *sig_alg; //CRL所使用的签名算法，和结构X509_crl_info_st中sig_alg的值一样
    ASN1_BIT_STRING *signature; //CRL的签名
    int references;
} /* X509_CRL */;

在文件ossl_typ.h中有：
typedef struct X509_crl_st X509_CRL;

我们下面要操作的CRL就是X509_CRL。
```

- 1.生成一个空的CRL
- 调用函数**X509_CRL_new()**
- eg. X509_CRL *crl = X509_CRL_new();
- 2.设置CRL中各信息的值
- 调用函数**X509_CRL_set_XXX**，其中XXX可以是version, issuer, lastUpdate, nextUpdate。

分类专栏

Linux

1篇

```
3.给CRL签名
    调用X509_CRL_sign()
    eg. X509_CRL_sign(crl, pkey, EVP_md5());
    其中，pkey是一个EVP_PKEY型的指针变量。
4.给CRL中添加一个扩展项
    调用函数int X509_CRL_add1_ext_i2d(X509_CRL *x, int nid, void *value, int crit, unsigned long flags)
    这个函数自动为用户生成一个X509_EXTENSION结构体，定义如下：
typedef struct X509_extension_st
{
    ASN1_OBJECT *object;
    ASN1_BOOLEAN critical;
    ASN1_OCTET_STRING *value;
} X509_EXTENSION;
    参数x代表要操作的CRL，nid, value, crit分别是X509_EXTENSION中的object, value, critical，flag可以取下面的值：
#define X509V3_ADD_OP_MASK      0xfL
#define X509V3_ADD_DEFAULT      0L
#define X509V3_ADD_APPEND      1L
#define X509V3_ADD_REPLACE     2L
#define X509V3_ADD_REPLACE_EXISTING  3L
#define X509V3_ADD_KEEP_EXISTING  4L
#define X509V3_ADD_DELETE      5L
#define X509V3_ADD_SILENT      0x10
    一般用X509V3_ADD_DEFAULT就行了，也就是直接传0就OK了。
    需要注意的是，函数X509_CRL_add1_ext_i2d要求传入的value是一个ASN1_OCTET_STRING*型的。开始以为，是void*就可以传任何类型的指针，结果在函数X509_CRL_add1_ext_i2d运行时，会产生段错误。
    函数X509_CRL_add1_ext_i2d调用的主要的函数如下图:
```

int X509_CRL_add1_ext_i2d(X509_CRL *x, int nid, void *value, int crit, unsigned long flags)
| (在文件x509_ext.c中)
| 此函数的作用是，把nid, value, crit组合成一个X509_EXTENSION结构，
| 通过flags指示的动作加入到x中。

int X509V3_add1_i2d(STACK_OF(X509_EXTENSION) **x, int nid, void *value, int crit, unsigned long flags)
| (在文件v3_lib.c中)
| 此函数的作用是，通过调用X509V3_EXT_i2d把nid, value, crit组合成一个X509_EXTENSION结构，
| 通过flags指示的动作加入到x中。

X509_EXTENSION *X509V3_EXT_i2d(int ext_nid, int crit, void *ext_struct)
| (在文件v3_conf.c中)
| 此函数的作用是，把传入的三个参数组合成一个X509_EXTENSION结构，
| 这里的三个参数分别就是nid, crit, value

static X509_EXTENSION *do_ext_i2d(X509V3_EXT_METHOD *method, int ext_nid, int crit, void *ext_struct)
| (在文件v3_conf.c中)
| 这是一个内部函数，作用是通过method中的函数，把ext_struct转换成ASN1_OCTET_STRING，
| 然后调用X509_EXTENSION_create_by_NID生成一个X509_EXTENSION

X509_EXTENSION *X509_EXTENSION_create_by_NID(X509_EXTENSION **ex, int nid, int crit, ASN1_OCTET_STRING *data)
| (在文件x509_v3.c中)
| 此函数的作用是，把nid转换成ASN1_OBJECT，
| 并通过调用X509_EXTENSION_create_by_OBJ生成一个X509_EXTENSION

X509_EXTENSION *X509_EXTENSION_create_by_OBJ(X509_EXTENSION **ex, ASN1_OBJECT *obj, int crit, ASN1_OCTET_STRING *data)
| (在文件x509_v3.c中)

此函数的作用是，通过调用X509_EXTENSION_new, X509_EXTENSION_set_object, X509_EXTENSION_set_critical, X509_EXTENSION_set_data生成一个X509_EXTENSION

- 5.将CRL存入PEM格式文件
调用函数**PEM_write_X509_CRL()**
eg. PEM_write_X509_CRL(fp, crl);
这个函数是把CRL以PEM格式存入文件的。
- 6.从PEM格式文件中读取CRL
调用函数**PEM_read_X509_CRL()**
eg. PEM_read_X509_CRL(fp, crl, NULL, NULL);
其中，crl是一个指向X509_CRL的指针的指针。



mm350670610

关注



1



0



1



Openssl

qq_36428903的博客

188

软件升级，原来软件使用的**openssl**的版本是1.0.1，需要升级到1.1.0；结果编译出现这个错误，这个错误的原因是，在x509.h头文件里定义的X509_EXT...

Openssl crl命令

weixin_34060299的博客

101

一、简介 **crl**命令用于处理PME或DER格式的**CRL**文件 二、语法 **openssl crl** [-inform PEM|DER] [-outform PEM|DER] [-text] [-in filename] [-out filename] [...]



请发表有价值的评论， 博客评论不欢迎灌水，良好的社区氛围需大家一起维护。

抢沙发



评论

openssl crl 使用方法_weixin_34144450的博客

9-30

PEM格式的**CRL**文件的头部和底部一行如下: ---BEGIN X509 **CRL**--- ---END X509 **CRL**--- 实例: 请先参考CA一节来生成一个**CRL**文件,再做如下操作: **open...**

OpenSSL命令---CRL_VitalityShow(网络通讯)

9-27

crl工具,用于处理PME或DER格式的**CRL**文件。 用法: **openssl crl** [-inform PEM|DER] [-outform PEM|DER] [-text] [-in filename] [-out filename] [-hash] [-fing...

OpenSSL之CRL

weixin_34259232的博客

396

2019独角兽企业重金招聘Python工程师标准>>> ...

openssl 编程。证书制作

baidu_32526299的博客

512

首页博客学院下载GitChatTinyMind论坛问答商城VIP活动写博客发Chat登录注册么刚的专栏RSS订阅原**openssl**证书制作及编程2010年07月29日 19:56:00...

Openssl crl命令_weixin_30261095的博客

10-20

crl命令用于处理PME或DER格式的**CRL**文件 二、语法 **openssl crl** [-inform PEM|DER] [-outform PEM|DER] [-text] [-infilename] [-out filename] [-hash] [-fin...

openssl学习笔记_huawei_gj的专栏

10-23

OPENSSL X509证书验证 http://blog.chinaunix.net/uid-24709751-id-3527545.htmlx509_vfy.c http://www.verysource.com/code/713120_1/x509_vfy.c.htm...

openssl crl 使用方法

weixin_33929309的博客

379

用途： **crl**工具，用于处理PME或DER格式的**CRL**文件。 -inform arg:输入文件的格式。 DER是DER编码的**CRL**对象。 PEM（默认的格式）是base64编码的...

Linux学习笔记<二十五>——openssl服务

weixin_33749131的博客

37

openssl服务：SSL(Secure Sockets Layer)的开源实现，官方网站 www.openssl.org组成：libcrypto：通用加密库libssl：TLS/SSL的实现库基于会话的，...

OpenSSL学习笔记一:命令行_ZRXSLYG的博客

10-21

OpenSSL学习笔记一:命令行ZRXSLYG 2020-11-17 21:50:53 73 收藏 分类专栏: OPENSSL 版权 OPENSSL 专栏收录该内容 7 篇文章 0 订阅 订阅专栏 > ...

openssl生成证书链多级证书、证书吊销列表(CRL)_Joe's...

10-8

openssl x509 -in mycert.crt -out mycert.pem -outform PEM 1 吊销证书(作废证书) 首先 echo 00 > /etc/pki/CA/crlnumber 1 一般由于用户私钥泄露等情况...

单机使用Openssl搭建CA并生成证书和CRL (woindows、linux)

shuizhongmose的专栏

1171

参考文档：https://blog.csdn.net/miouqi/article/details/75268402 安装 windows去**openssl**官网下载安装包，然后将**openssl**的路径添加到环境变量PATH下...

Open***学习笔记——证书吊销及其他事项

weixin_33696822的博客

189

公司如果有一些其他需求，比如员工离职或者其他需求，可能需要对原来签发的客户端证书进行吊销，以免出现信息泄露等安全问题。如果config目录下...

OpenSSL学习笔记三:实操_ZRXSLYG的博客

10-21

https://www.openssl.org/docs/man1.1.1/man3/ 可以修改Key、IV、Nonce的最后一位,看加密后的密文是否修改 //man EVP_EncryptInit //DES in CBC, ECB...



mm350670610

码龄14年 暂无认证

16

原创

92万+

周排名

47万+

总排名

5万+

访问



等级

701

积分

9

粉丝

2

获赞

3

评论

7

收藏

私信

关注

搜博文文章



热门文章

配置Apache和OpenSSL 7349

OpenSSL学习笔记——CRL 6991

OpenSSL学习笔记——内存分配 6743

linux驱动模型学笔记——kobject&kset

Win32结构化异常处理(SEH)——异常处理程序(__try/__except)  3348

最新评论

配置Apache和OpenSSL
hyrtster: 1. Un-comment the below line: [code=plain] LoadModule socache_shmcb...
OpenSSL学习笔记——堆栈
mm350670610: 回复 NetCompactFramework
ork : BIO是SSL中对IO的一个抽象接口 , ...
OpenSSL学习笔记——堆栈
NetCompactFramework: 可以请教一下Stack和BIO的关系吗? 好像SSL进行IO操作用...

您愿意向朋友推荐“博客详情页”吗？



强烈不推荐 不推荐 一般般 推荐 强烈推荐

最新文章

linux驱动模型学笔记——字符设备号
linux驱动模型学笔记——kobject&kset
配置LAMP服务器

2010年 17篇

Open*****学习笔记**——部署安装

上一篇介绍了Open***部署前的环境准备，下面开始具体的部署安装。mkdir-p/opt/tools cd/opt/tools/ wgethttp://www.oberhumer.com/opensource/ldo...

选择验证**CRL**的最优算法

前提 拥有多个证书吊销列表**CRL**，给定一个证书，验证这个证书是否被吊销。 分析 目前想到有三个方法来实现。 循环所有**CRL**来验证证书 循环所...

数字证书**学习**笔记汇总

名词字典 **SSL**证书 **SSL**证书是数字证书的一种，类似于驾驶证、护照和营业执照的电子副本。因为配置在服务器上，也称为**SSL**服务器证书。 **SSL** 证书就...

Navicat连接数据库出现的错误和MySQL**学习**笔记

在Navicat Premium 15中连接数据库的时候，可能会出现如下错误： 出现此错误的原因是因为没有开启数据库服务 解决步骤： 一、桌面计算机图标右键...

Linux**学习**笔记<三十一>——https简单配置

假设实例如下：CA主机192.168.191.160Web服务器主机192.168.191.150，httpd配置沿用上一篇博文的CA自签署证书，传输给Web服务器，配置/etc/htt...

【博否安全】从加密算法到CA认证——数字认证技术**学习**笔记（一）

目录缩略词表数据加密技术非对称加密和数字签名1、非对称加密（公钥加密）2、数字签名与数字验签（私钥加密）证书的作用数字证书的格式1、证书...

最详细的 K8S **学习**笔记总结（2021最新版）

最新发布 民工哥的博文  1607

虽然 Docker 已经很强大了，但是在实际使用上还是有诸多不便，比如集群管理、资源调度、文件管理等等。那么在这样一个百花齐放的容器时代涌现出...

HTTP**学习**笔记（7）—— 确保WEB安全的HTTPS

qq_40118570的博文  105

第七章：确保WEB安全的HTTPS 引言 在HTTP请求中可能存在信息窃听身份伪装等问题 使用HTTPS通信机制可以有效防止这些问题 HTTP的缺点 缺点 内...

乱的**笔记**

weixin_34357962的博文  7977

链接：https://pan.baidu.com/s/1jBIX2OoWALMaLuMkx21H7w 提取码：mzI4 复制这段内容后打开百度网盘手机App，操作更方便哦如果看的不舒服可以上...

【课程**笔记**】快速上手Linux玩转典型应用——慕课网（Linux常用命令）

Cydiachencc的博文  956

标签（空格分隔）：Linux运维 **学习**笔记 1、软件操作命令：yum——软件包管理器 yum clean packages 2、服务器硬件资源、硬盘操作 内存：free -m ...

©2021 CSDN 皮肤主题: 大白 设计师:CSDN官方博客 返回首页

