Q OpenSSL C API CRL检查

c api ssl openssl certificate 2014-10-06 60 views 2 likes

2

我正在尝试使用OpenSSL C API编写CertificatePathValidation测试。我目前停留在测试撤销中间(ca-)证书。有两种测试用例:1. EndCert被吊销，并且2. SubCACert被吊销。我的代码的一部分:OpenSSL C API CRL检查

```
FILE* fl = NULL;
int i;
for(i=0; i<crl_count; i++){
    fl = fopen(pem_crl_files[i],"r");
    x509 = PEM_read_X509_CRL(fl, NULL,0,NULL);
    X509_STORE_add_crl(store, x509);
    fclose(fl);
}
X509_STORE_set_flags(store, X509_V_FLAG_CRL_CHECK);
```

所以现在当我使用X509_V_FLAG_CRL_CHECK标志，测试用例1的工作了罚款，测试案例2失败(返回证书是有效的)。如果我使用X509_V_FLAG_CRL_CHECK_ALL标志，则情况1和2都会失败。有谁知道我错过了什么？

来源

2014-10-06 guest123

A 回答

4

的这个设置的行为是略有不同的文档建议:

- X509_V_FLAG_CRL_CHECK使CRL检查。如果此选项关闭，则不会执行检查。
- 如果X509_V_FLAG_CRL_CHECK_ALL是*也是*设置整个链会被检查，否则只有叶证书。

这意味着您需要同时设置 `X509_V_FLAG_CRL_CHECK|X509_V_FLAG_CRL_CHECK_ALL` 。

从OpenSSL的1.0.1e，文件加密/ X509/x509_vfy.c相关的代码:

```
669 static int check_revocation(X509_STORE_CTX *ctx)
670   {
671   int i, last, ok;
672   if (!(ctx->param->flags & X509_V_FLAG_CRL_CHECK))
673     return 1;
674   if (ctx->param->flags & X509_V_FLAG_CRL_CHECK_ALL)
675     last = sk_X509_num(ctx->chain) - 1;
```

正如你可以看到它会跳过行672673全吊销检查，如果没有设置X509_V_FLAG_CRL_CHECK。

来源

2014-10-06 15:32:10

相关文章

1. Openssl crl命令
2. openssl漏洞检查
3. openssl C函数总结，
4. Openssl中的Libcrypto API
5. openssl 检查证书是否过时
6. openssl
7. OpenSSL编程
8. OpenSSL

每日一句

每一个你不满意的现在，都有一个你没有努力的曾经。

最新问题

1. 操作无法完成。（NSXMLParserErrorDomain错误26.）- Three20 XML解析器
2. 在VBScript中使用输出参数调用SQL存储过程
3. WPF标签设计
4. 锁定按钮同时AJAX调用
5. LendingClub.com API内部服务器在二级市场上购买票据的错误
6. TCP/IP数据包中的端口号
7. 模拟Angular 2中的长响应
8. 如何在QSplitter中设置QTreeView的初始大小？
9. 打印响应部分完成Python的异步事件循环，同时还完成任务的响应
10. 如何结合3正则表达式？

相关问题

1. Openssl crl命令
2. openssl漏洞检查
3. openssl C函数总结，
4. Openssl中的Libcrypto API
5. openssl 检查证书是否过时
6. openssl
7. OpenSSL编程
8. OpenSSL
9. day3-selinux+openssl
10. openssl API网络通讯

9. day3-selinux+openssl
10. openssl API网络通讯
11. 检查C++中的内存泄漏-经过工具来检查
12. 使用 OpenSSL API 进行安全编程
13. 清理c盘检查
14. C/C++内存检查原理
15. CRL校验与OCSP套封
16. openssl命令使用
17. openssl生成证书链多级证书、证书吊销列表（CRL）
18. Java 错别字检查接口 API
19. 开源C++/C代码检查工具
20. valgrind检查C/C++内存泄漏
21. 转 C# 使用openssl
22. 使用 openssl 生成证书
23. OpenSSL生成
24. openssl的简介
25. Openssl create Cert
26. Android Native C/C++ 使用OpenSSL EVP接口
27. Nginx 健康检查
28. Centos7下的Openssl和CA
29. openssl实现证书申请
30. openssl aes api 记录 [二] - windows 下使用openssl问题记录