OpenSSL C API：使用CRL进行证书链验证(示例代码)

2021-04-10

栏目: nginx ·

简介 这篇文章主要介绍了OpenSSL C API：使用CRL进行证书链验证(示例代码)以及相关的经验技巧，文章约1216字，浏览量474，点赞数5，值得参考！

我正在尝试对Windows可执行文件执行证书链验证，其中还包括使用OpenSSL 1.0.2 C API检查已撤销的证书。

我在本地存储了CRL文件，我想在验证期间加载它们（而不是通过具有它的证书从“CRL分发点”URL下载CRL）。

这是我加载单个CRL文件的简化示例（省略任何错误检查）：

```
X509_STORE *store = NULL;
X509_STORE_CTX *ctx = NULL;
X509_VERIFY_PARAM *params = NULL;

X509_CRL *crl = d2i_X509_CRL_fp(fc, NULL);  // fc is a file pointer to CRL file
X509_STORE_add_crl(store, crl);
X509_STORE_CTX_init(ctx, store, NULL, NULL);

params = X509_STORE_CTX_get0_param(ctx);
X509_VERIFY_PARAM_set_purpose(params, X509_PURPOSE_ANY);
X509_VERIFY_PARAM_set_flags(params, X509_V_FLAG_CRL_CHECK);  // only want to check end entity
X509_STORE_set1_param(store, params);

// assume p7 is properly initialized PKCS7*
// assume bio is properly initialized BIO*
int ret = PKCS7_verify(p7, p7->d.sign->cert, store, bio, NULL, 0);
```

上面的代码将返回错误的`ret == 0：unable to get certificate CRL`，根据我的理解，这意味着OpenSSL仍在尝试从证书本身搜索CRL，而不是使用我在本地加载的CRL。

实现这项任务的正确方法是什么？

答案

实际上上面的代码已经是正确的，以实现我执行CRL检查的目标。X509证书结构新手的一个潜在缺陷是，感兴趣的证书的“CRL分发点”URL包含在该证书本身内，而不是发行人的证书中。这是我的错误导致我提到的错误。我希望这可以帮助那些刚刚开始理解X509标准的人。

以上就是本文的全部内容，希望对大家的学习有所帮助，本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

相关文章

- 使用OpenSSL创建CA和申请证书(示例代码)
- Jmeter-如何在Jmeter中测试受客户端证书身份验证保护的api？
- openssl创建私有ca(示例代码)
- openssl的应用及私有CA相关内容
- Windows下使用OpenSSL生成证书并自签名记录(示例代码)
- openssl制作双向认证经过验证可行(示例代码)
- 使用openssl校验证书链(示例代码)
- openssl源码目录结构(示例代码)