# HTTPS中证书链不完整的解决方案

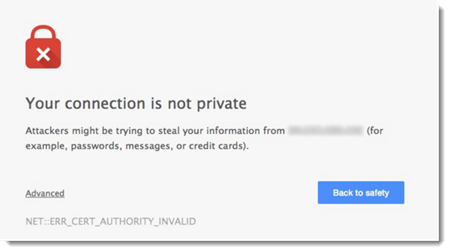
**问题背景**

最近在给服务器配置HTTPS，原因是运营商的恶心人的举动，我印象中以前也有运营商的劫持广告，但是都是很偶尔的情况，从2015年，几乎每次都会加上，京东淘宝的WebView也难以幸免。之前用的一直是一种Hack的方法，就是在页面中发现不属于自己的DOM就remove掉，但这终究治标不治本。

最终决定上HTTPS，由于我们买的是Wildcard证书，也就是子域名通配符的证书，\*.domain.com的形式。所以证书的申请、配置都非常顺利。

由于我们的业务要求在APP中嵌入WebView中打开Web页面，但在测试过程中却发现了一个问题，在Chrome中测试完全正常的https页面，在iOS的WebView中表现正常，但在Android中，不论是哪个版本的安卓系统，都不能正常打开页面，要么就是一片白，要么就是直接无法打开。

之后在Android自带的浏览器中测试，几乎所有的手机都出现下面这样的情况

[](http://www.tangzongchao.com/images/httpsCertificateChain1.png)  
[](http://www.tangzongchao.com/images/httpsCertificateChain2.png)  
[](http://www.tangzongchao.com/images/httpsCertificateChain3.png)

**证书链**

看来Andorid的WebView不能打开页面应该是与这有关，造成这个问题的主要原因是我们服务器配置证书的证书链不全造成的。

每个设备中都会存有一些默认的可信的根证书，但很多CA是不使用根证书进行签名的，而是使用中间层证书进行签名，因为这样做能更快的进行替换（这句可能不对，原文是 because these can be rotated more frequently）。

如果你的服务器上没有中间件证书，这样的结果就是你的服务器上只有你的网站的证书，客户端的浏览器里只有CA的根证书，这样就会导致证书信任链不全，才导致了上面那两个截图中的问题。这种中间层证书不全的问题多出现在移动端的浏览器上（就我目前看，iOS8 iOS9 都没有出现问题，Andorid各个版本都有这个问题）。

当你服务器上的证书中的信任链不全的情况下，浏览器会认为当前的链接是一个不安全的，会阻止页面的打开。

**解决方案**

说清楚了原因，解决问题就很简单了，只要把我们的证书链补全就可以了。

从SSL证书服务商那里，你获得的crt证书文件大概是这个样子的：

-----BEGIN CERTIFICATE-----

# 证书内容

-----END CERTIFICATE-----

在你补全中间层证书和根证书后，新的crt证书文件看起来是这样的：

-----BEGIN CERTIFICATE-----

# 证书内容 1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

# 证书内容 2

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

# 证书内容 3

-----END CERTIFICATE-----

这里包含了你的证书，以及从你的证书向上递归直至根证书的全部证书，这样就可以向浏览器证明你的链接是安全的。

补全证书链

比较方便的是使用这个在线的工具：

[https://certificatechain.io](https://certificatechain.io/)

进入这个网站，粘贴进你的证书（只包含你的用户证书），或者上传你的证书，他就会给出补全后的证书文件，你只需要粘贴回你的文件或者下载覆盖就可以了，然后在服务器上重新部署就可以解决问题。

由于这里只需要上传证书，所以是安全的，不需要担心不安全的问题。

如果不喜欢用在线的工具，可以使用下面这个本地的工具，PHP写的，在命令行中运行：

[Github ssl-certificate-chain-resolver](https://github.com/spatie/ssl-certificate-chain-resolver)

**结束语**

回到开头，https设计之初本是为了防止中间被人篡改一些核心数据，例如支付数据、交易数据等等。之前https证书的价格非常的昂贵，但这些年随着https证书价格的日趋平民化，越来越多的网站启用了https，究其原因大多数是为了对抗运营商的劫持。

我记得曾经看过一个视频，里边讲当初QQ的加好友的页面，也是一个Web页面套壳的设计，被某个地区的运营商劫持，甚至加入了某些不太好的内容。那么腾讯是怎么做的，做了个微信把运营商干掉。

虽然这只是个笑话，但真的希望运营商们能收敛一些这种行为，做好自己的角色。不要让我们把技术用到极致来对抗技术的发展。