

36 | HTTPS：让数据传输更安全

2019-10-26 李兵

《浏览器工作原理与实践》

课程介绍 >



讲述：李兵

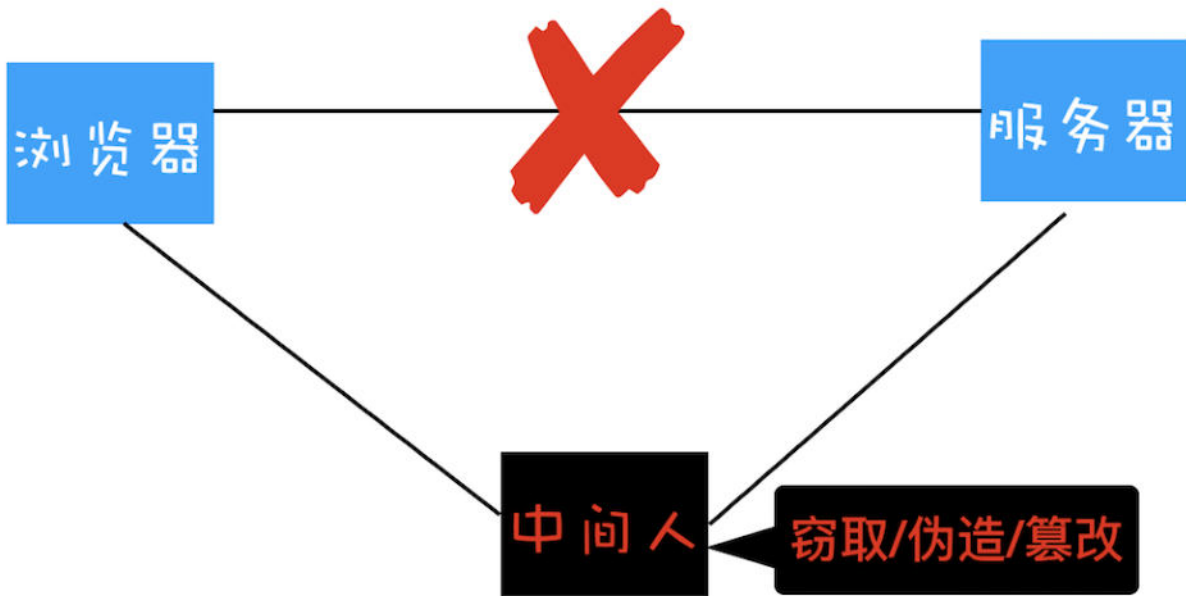
时长 15:39 大小 14.34M



浏览器安全主要划分为三大块内容：页面安全、系统安全和网络安全。前面我们用四篇文章介绍了页面安全和系统安全，也聊了浏览器和 Web 开发者是如何应对各种类型的攻击，本文是我们专栏的最后一篇，我们就接着来聊聊网络安全协议 HTTPS。

我们先从 HTTP 的明文传输的特性讲起，在上一个模块的三篇文章中我们分析过，起初设计 HTTP 协议的目的很单纯，就是为了传输超文本文件，那时候也没有太强的加密传输的数据需求，所以 HTTP 一直保持着明文传输数据的特征。但这样的话，在传输过程中的每一个环节，数据都有可能被窃取或者篡改，这也意味着你和服务器之间还可能有个中间人，你们在通信过程中的一切内容都在中间人的掌握中，如下图：





中间人攻击

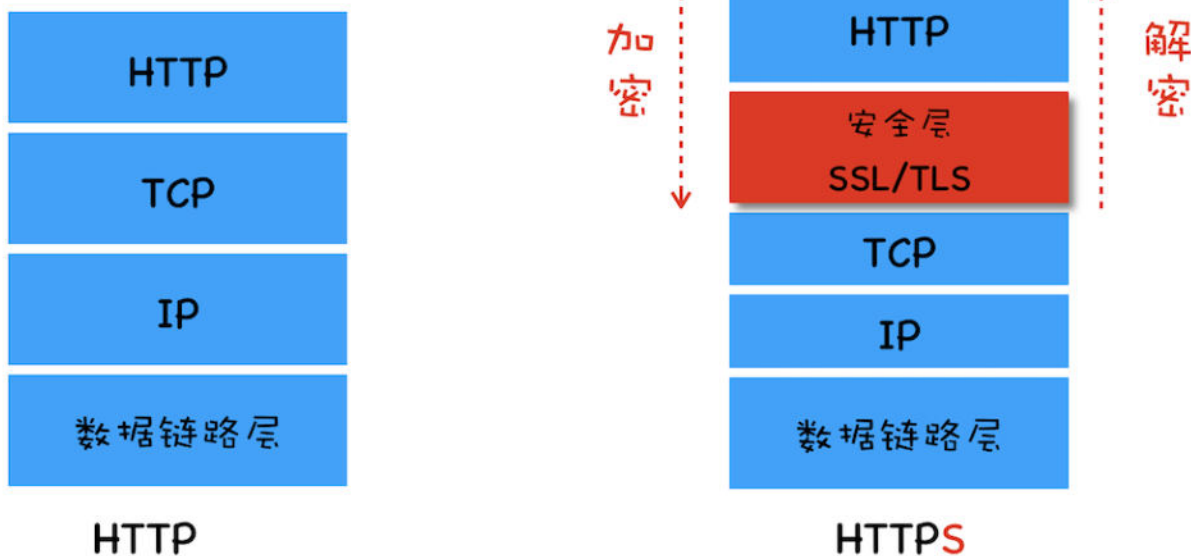
从上图可以看出，我们使用 HTTP 传输的内容很容易被中间人窃取、伪造和篡改，通常我们把这种攻击方式称为**中间人攻击**。

具体来讲，在将 HTTP 数据提交给 TCP 层之后，数据会经过用户电脑、WiFi 路由器、运营商和目标服务器，在这中间的每个环节中，数据都有可能被窃取或篡改。比如用户电脑被黑客安装了恶意软件，那么恶意软件就能抓取和篡改所发出的 HTTP 请求的内容。或者用户一不小心连接上了 WiFi 钓鱼路由器，那么数据也都能被黑客抓取或篡改。

在 HTTP 协议栈中引入安全层

鉴于 HTTP 的明文传输使得传输过程毫无安全性可言，且制约了网上购物、在线转账等一系列场景应用，于是倒逼着我们要引入**加密方案**。

从 HTTP 协议栈层面来看，我们可以在 TCP 和 HTTP 之间插入一个安全层，所有经过安全层的数据都会被加密或者解密，你可以参考下图：



HTTP VS HTTPS

从图中我们可以看出 HTTPS 并非是一个新的协议，通常 HTTP 直接和 TCP 通信，HTTPS 则先和安全层通信，然后安全层再和 TCP 层通信。也就是说 HTTPS 所有的安全核心都在安全层，它不会影响到上面的 HTTP 协议，也不会影响到下面的 TCP/IP，因此要搞清楚 HTTPS 是如何工作的，就要弄清楚安全层是怎么工作的。

总的来说，安全层有两个主要的职责：**对发起 HTTP 请求的数据进行加密操作**和**对接收到 HTTP 的内容进行解密操作**。

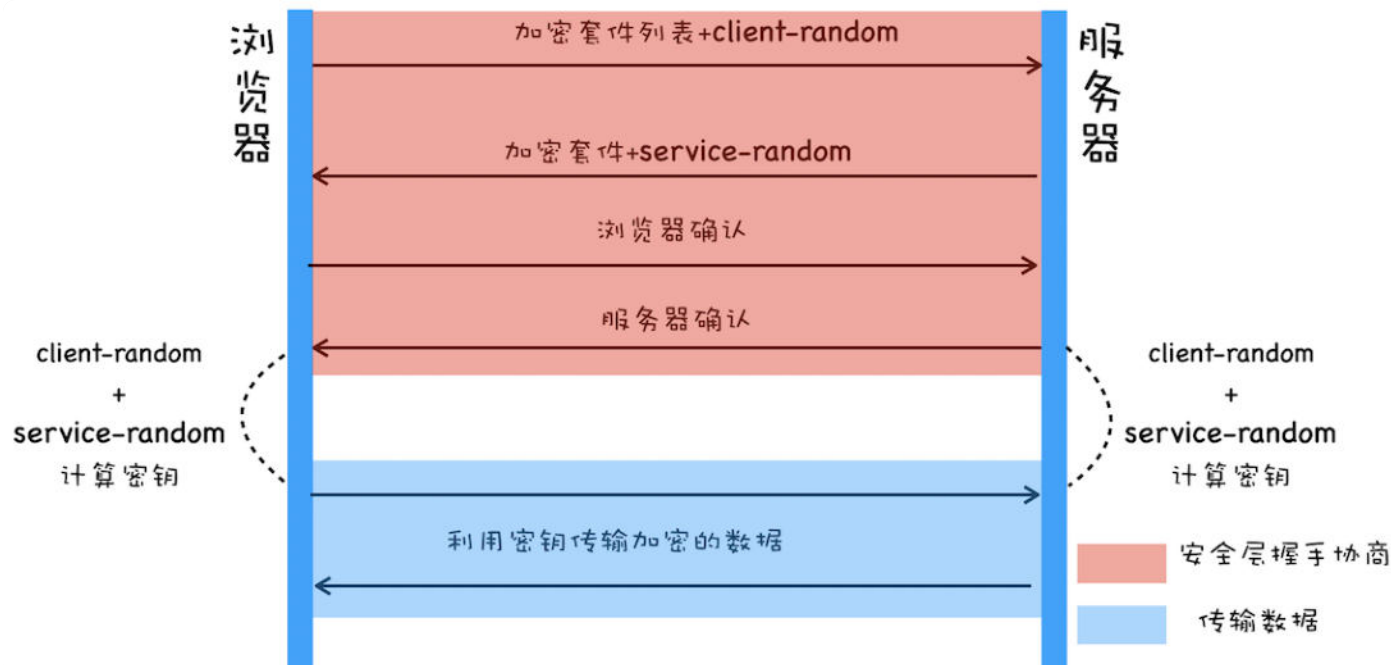
我们知道了安全层最重要的就是加解密，那么接下来我们就利用这个安全层，一步一步实现一个从简单到复杂的 HTTPS 协议。

第一版：使用对称加密

提到加密，最简单的方式是使用对称加密。所谓**对称加密**是指加密和解密都使用的是相同的密钥。

了解了对称加密，下面我们就使用对称加密来实现第一版的 HTTPS。

要在两台电脑上加解密同一个文件，我们至少需要知道加解密方式和密钥，因此，在 HTTPS 发送数据之前，浏览器和服务器之间需要协商加密方式和密钥，过程如下所示：



使用对称加密实现 HTTPS

通过上图我们可以看出，HTTPS 首先要协商加解密方式，这个过程就是 HTTPS 建立安全连接的过程。为了让加密的密钥更加难以破解，我们让服务器和客户端同时决定密钥，具体过程如下：

- 浏览器发送它所支持的加密套件列表和一个随机数 client-random，这里的**加密套件是指加密的方法**，加密套件列表就是指浏览器能支持多少种加密方法列表。
- 服务器会从加密套件列表选取一个加密套件，然后还会生成一个随机数 service-random，并将 service-random 和加密套件列表返回给浏览器。
- 最后浏览器和服务器分别返回确认消息。

这样浏览器端和服务器端都有相同的 client-random 和 service-random 了，然后它们再使用相同的方法将 client-random 和 service-random 混合起来生成一个密钥 master secret，有了密钥 master secret 和加密套件之后，双方就可以进行数据的加密传输了。

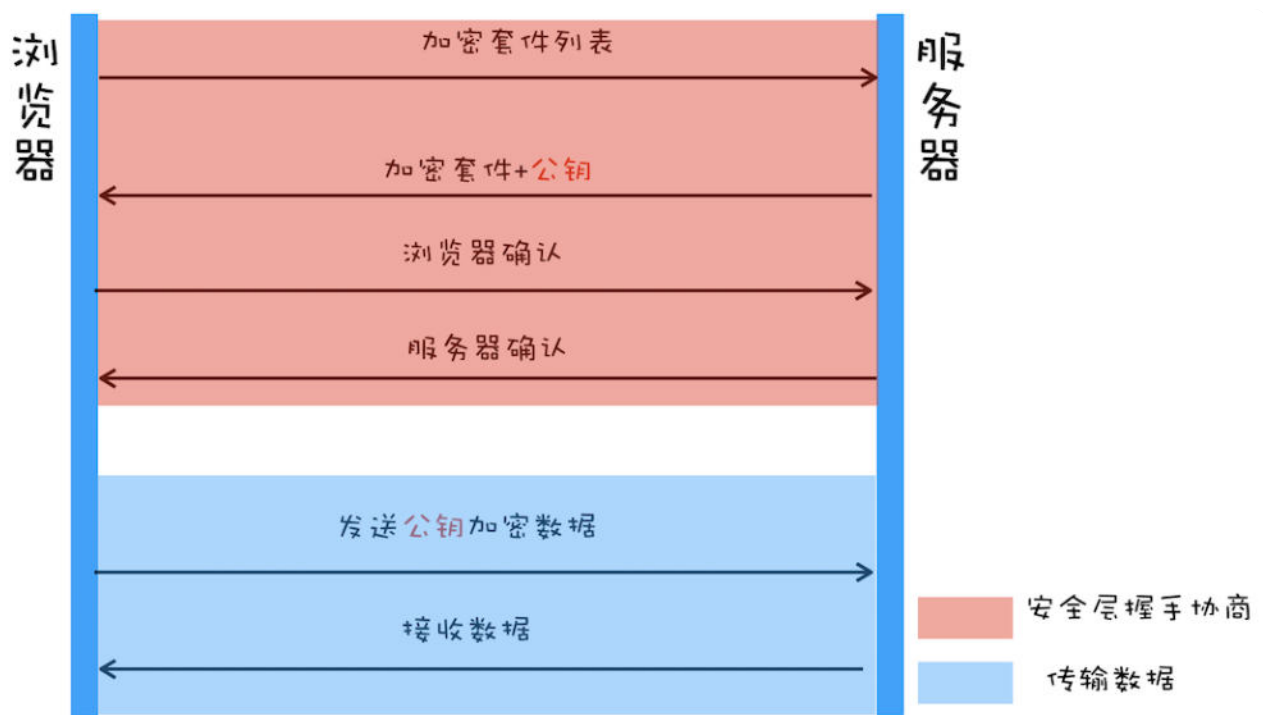
通过将对称加密应用在安全层上，我们实现了第一个版本的 HTTPS，虽然这个版本能够很好地工作，但是其中传输 client-random 和 service-random 的过程却是明文的，这意味着黑客也可以拿到协商的加密套件和双方的随机数，由于利用随机数合成密钥的算法是公开的，所以黑客拿到随机数之后，也可以合成密钥，这样数据依然可以被破解，那么黑客也就可以使用密钥来伪造或篡改数据了。

第二版：使用非对称加密

不过非对称加密能够解决这个问题，因此接下来我们就利用非对称加密来实现我们第二版的 HTTPS，不过在讨论具体的实现之前，我们先看看什么是非对称加密。

和对称加密只有一个密钥不同，非对称加密算法有 A、B 两把密钥，如果你用 A 密钥来加密，那么只能使用 B 密钥来解密；反过来，如果你要 B 密钥来加密，那么只能用 A 密钥来解密。

在 HTTPS 中，服务器会将其中的一个密钥通过明文的形式发送给浏览器，我们把这个密钥称为**公钥**，服务器自己留下的那个密钥称为**私钥**。顾名思义，**公钥是每个人都能获取到的，而私钥只有服务器才能知道，不对任何人公开**。下图是使用非对称加密改造的 HTTPS 协议：



非对称加密实现 HTTPS

根据该图，我们来分析下使用非对称加密的请求流程。

- 首先浏览器还是发送加密套件列表给服务器。
- 然后服务器会选择一个加密套件，不过和对称加密不同的是，使用非对称加密时服务器上需
要有用于浏览器加密的公钥和服务器解密 HTTP 数据的私钥，由于公钥是给浏览器加密使用的，因此服务器会将加密套件和公钥一道发送给浏览器。

- 最后就是浏览器和服务器返回确认消息。

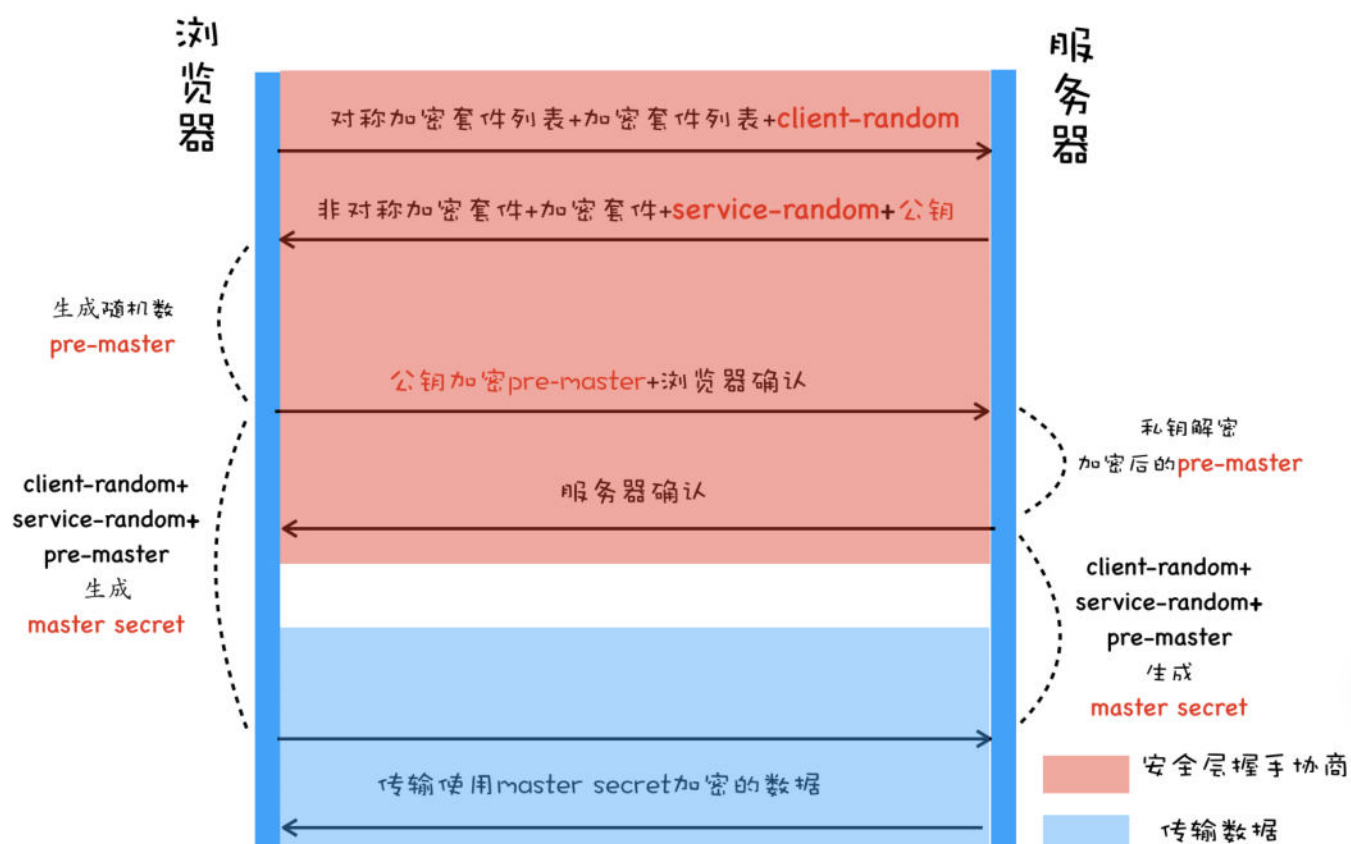
这样浏览器端就有了服务器的公钥，在浏览器端向服务器端发送数据时，就可以使用该公钥来加密数据。由于公钥加密的数据只有私钥才能解密，所以即便黑客截获了数据和公钥，他也是无法使用公钥来解密数据的。

因此采用非对称加密，就能保证浏览器发送给服务器的数据是安全的了，这看上去似乎很完美，不过这种方式依然存在两个严重的问题。

- **第一个是非对称加密的效率太低。**这会严重影响到加解密数据的速度，进而影响到用户打开页面的速度。
- **第二个是无法保证服务器发送给浏览器的数据安全。**虽然浏览器端可以使用公钥来加密，但是服务器端只能采用私钥来加密，私钥加密只有公钥能解密，但黑客也是可以获取得到公钥的，这样就不能保证服务器端数据的安全了。

第三版：对称加密和非对称加密搭配使用

基于以上两点原因，我们最终选择了一个更加完美的方案，那就是在传输数据阶段依然使用对称加密，但是对称加密的密钥我们采用非对称加密来传输。下图就是改造后的版本：



从图中可以看出，改造后的流程是这样的：

- 首先浏览器向服务器发送对称加密套件列表、非对称加密套件列表和随机数 `client-random`；
- 服务器保存随机数 `client-random`，选择对称加密和非对称加密的套件，然后生成随机数 `service-random`，向浏览器发送选择的加密套件、`service-random` 和公钥；
- 浏览器保存公钥，并生成随机数 `pre-master`，然后利用公钥对 `pre-master` 加密，并向服务器发送加密后的数据；
- 最后服务器拿出自己的私钥，解密出 `pre-master` 数据，并返回确认消息。

到此为止，服务器和浏览器就有了共同的 `client-random`、`service-random` 和 `pre-master`，然后服务器和浏览器会使用这三组随机数生成**对称密钥**，因为服务器和浏览器使用同一套方法来生成密钥，所以最终生成的密钥也是相同的。

有了对称加密的密钥之后，双方就可以使用对称加密的方式来传输数据了。

需要特别注意的一点，`pre-master` 是经过公钥加密之后传输的，所以黑客无法获取到 `pre-master`，这样黑客就无法生成密钥，也就保证了黑客无法破解传输过程中的数据了。

第四版：添加数字证书

通过对称和非对称混合方式，我们完美地实现了数据的加密传输。不过这种方式依然存在着问题，比如我要打开极客时间的官网，但是黑客通过 DNS 劫持将极客时间官网的 IP 地址替换成了黑客的 IP 地址，这样我访问的其实是黑客的服务器了，黑客就可以在自己的服务器上实现公钥和私钥，而对浏览器来说，它完全不知道现在访问的是个黑客的站点。

所以我们还需要服务器向浏览器提供证明“我就是我”，那怎么证明呢？

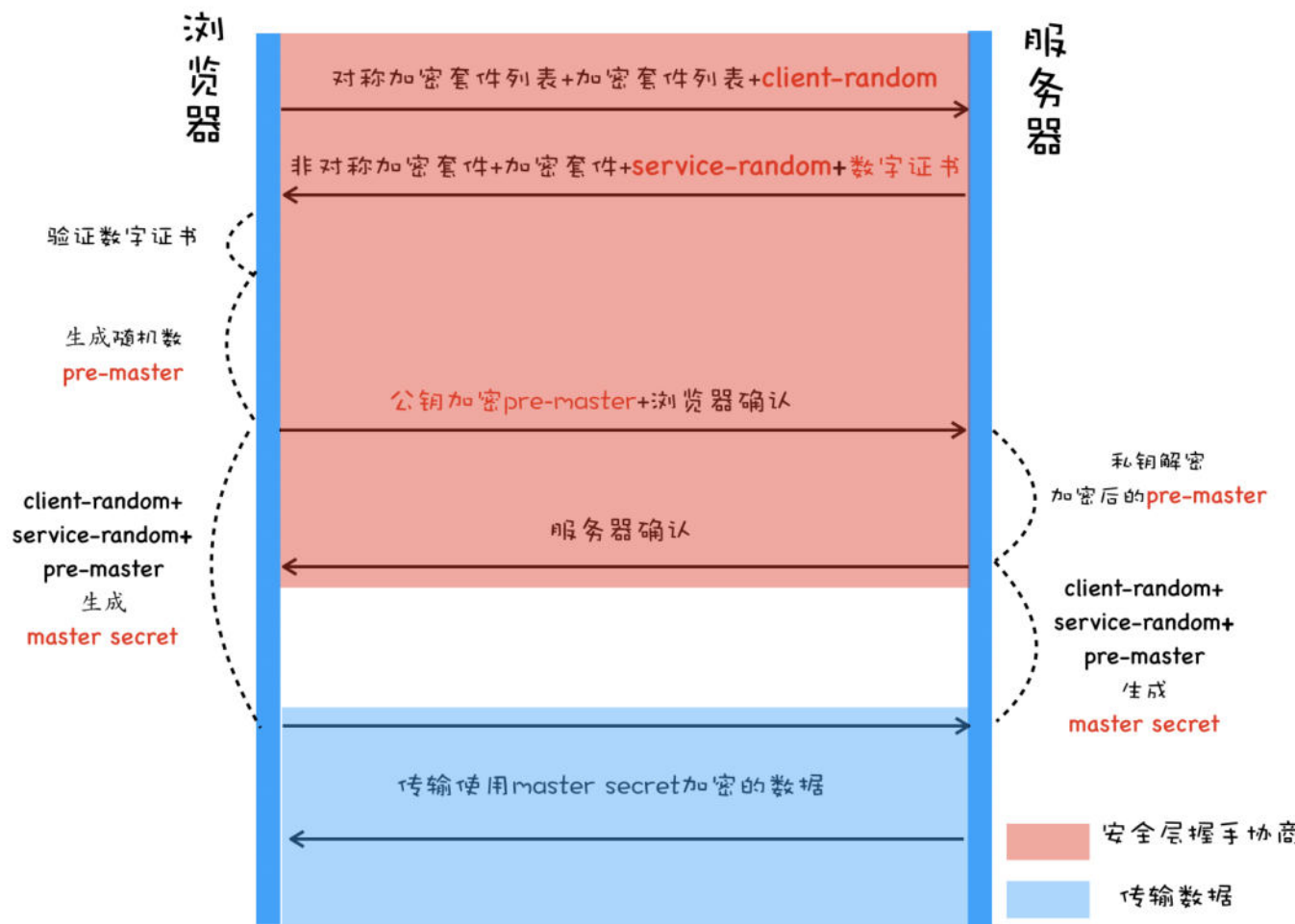
这里我们结合实际生活中的一个例子，比如你要买房子，首先你需要给房管局提交你买房的材料，包括银行流水、银行证明、身份证等，然后房管局工作人员在验证无误后，会发给你一本盖了章的房产证，房产证上包含了你的名字、身份证号、房产地址、实际面积、公摊面积等信息。

在这个例子中，你之所以能证明房子是你自己的，是因为引进了房管局这个**权威机构**，并通过这个权威机构给你颁发一个**证书**：房产证。

同理，极客时间要证明这个服务器就是极客时间的，也需要使用权威机构颁发的证书，这个权威机构称为 **CA (Certificate Authority)**，颁发的证书就称为**数字证书 (Digital Certificate)**。

对于浏览器来说，数字证书有两个作用：一个是通过数字证书向浏览器证明服务器的身份，另一个是数字证书里面包含了服务器公钥。

接下来我们看看含有数字证书的 HTTPS 的请求流程，你可以参考下图：



完整的 HTTPS 请求流程

相较于第三版的 HTTPS 协议，这里主要有两点改变：

1. 服务器没有直接返回公钥给浏览器，而是返回了数字证书，而公钥正是包含在数字证书中的；
2. 在浏览器端多了一个证书验证的操作，验证了证书之后，才继续后续流程。

通过引入数字证书，我们就实现了服务器的身份认证功能，这样即便黑客伪造了服务器，但是由于证书是没有办法伪造的，所以依然无法欺骗用户。

数字证书的申请和验证

通过上面四个版本的迭代，我们实现了目前的 HTTPS 架构。

在第四版的 HTTPS 中，我们提到过，有了数字证书，黑客就无法欺骗用户了，不过我们并没有解释清楚如何通过数字证书来证明用户身份，所以接下来我们再来把这个问题解释清楚。

如何申请数字证书

我们先来看看如何向 CA 申请证书。比如极客时间需要向某个 CA 去申请数字证书，通常的申请流程分以下几步：

- 首先极客时间需要准备一套私钥和公钥，私钥留着自己使用；
- 然后极客时间向 CA 机构提交公钥、公司、站点等信息并等待认证，这个认证过程可能是收费的；
- CA 通过线上、线下等多种渠道来验证极客时间所提供信息的真实性，如公司是否存在、企业是否合法、域名是否归属该企业等；
- 如信息审核通过，CA 会向极客时间签发认证的数字证书，包含了极客时间的公钥、组织信息、CA 的信息、有效时间、证书序列号等，这些信息都是明文的，同时包含一个 CA 生成的签名。

这样我们就完成了极客时间数字证书的申请过程。前面几步都很好理解，不过最后一步数字签名的过程还需要解释下：首先 CA 使用 **Hash 函数**来计算极客时间提交的明文信息，并得出**信息摘要**；然后 CA 再使用它的私钥对信息摘要进行加密，**加密后的密文就是 CA 颁给极客时间的数字签名**。这就相当于房管局在房产证上盖的章，这个章是可以去验证的，同样我们也可以通过数字签名来验证是否是该 CA 颁发的。

浏览器如何验证数字证书

有了 CA 签名过的数字证书，当浏览器向极客时间服务器发出请求时，服务器会返回数字证书给浏览器。

浏览器接收到数字证书之后，会对数字证书进行验证。首先浏览器读取证书中相关的明文信息，采用 CA 签名时相同的 Hash 函数来计算并得到**信息摘要 A**；然后再利用对应 CA 的公钥解密签名数据，得到**信息摘要 B**；对比信息摘要 A 和信息摘要 B，如果一致，则可以确认证书是合法的，即证明了这个服务器是极客时间的；同时浏览器还会验证证书相关的域名信息、有效时间等信息。

这时候相当于验证了 CA 是谁，但是这个 CA 可能比较小众，浏览器不知道该不该信任它，然后浏览器会继续查找给这个 CA 颁发证书的 CA，再以同样的方式验证它上级 CA 的可靠性。通常情况下，操作系统中会内置信任的顶级 CA 的证书信息（包含公钥），如果这个 CA 链中没有找到浏览器内置的顶级的 CA，证书也会被判定非法。

另外，在申请和使用证书的过程中，还需要注意以下三点：

1. 申请数字证书是不需要提供私钥的，要确保私钥永远只能由服务器掌握；
2. 数字证书最核心的是 CA 使用它的私钥生成的数字签名；
3. 内置 CA 对应的证书称为根证书，根证书是最权威的机构，它们自己为自己签名，我们把这称为自签名证书。

总结

好了，今天就介绍到这里，下面我来总结下本文的主要内容。

由于 HTTP 的明文传输特性，在传输过程中的每一个环节，数据都有可能被窃取或者篡改，这倒逼着我们需要引入加密机制。于是我们在 HTTP 协议栈的 TCP 和 HTTP 层之间插入了一个安全层，负责数据的加密和解密操作。

我们使用对称加密实现了安全层，但是由于对称加密的密钥需要明文传输，所以我们又将对称加密改造成了非对称加密。但是非对称加密效率低且不能加密服务器到浏览器端的数据，于是我们又继续改在安全层，采用对称加密的方式加密传输数据和非对称加密的方式来传输密钥，这样我们就解决传输效率和两端数据安全传输的问题。



采用这种方式虽然能保证数据的安全传输，但是依然没办法证明服务器是可靠的，于是又引入了数字证书，数字证书是由 CA 签名过的，所以浏览器能够验证该证书的可靠性。

另外百看不如一试，我建议你自己亲手搭建一个 HTTPS 的站点，可以去 freeSSL 申请免费证书。链接我已经放在文中了：

- 中文： <https://freessl.cn/>
- 英文： <https://www.freessl.com/>


思考时间


今天留给你的作业：结合前面的文章以及本文，你来总结一下 HTTPS 的握手过程。

欢迎在留言区与我分享你的想法，也欢迎你在留言区记录你的思考过程。感谢阅读，如果你觉得这篇文章对你有帮助的话，也欢迎把它分享给更多的朋友。

分享给需要的人，Ta订阅超级会员，你将得 50 元

Ta单独购买本课程，你将得 20 元

 生成海报并分享

 赞 21  提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

[上一篇](#) 35 | 安全沙箱：页面和系统之间的隔离墙

[下一篇](#) 结束语 | 大道至简

JVM + NIO + Spring

各大厂面试题及知识点详解

限时免费 



精选留言 (49)

 写留言



成楠Peter

2019-10-26

我有一个地方不是很理解。CA的公钥，浏览器是怎么拿到的。是浏览器第一次请求服务器的时候，CA机构给浏览器的吗？求大神或者老师解答

作者回复：

我们先从证书类型开始：

我们知道CA是一个机构，它的职责是给一些公司或者个人颁发数字证书，在颁发证书之前，有一个重要的环节，就是审核申请者所提交资料的合法性和合规性。

不过申请者的类型有很多：

如果申请者是个人，CA只需要审核所域名的所有权就行了，审核域名所有权有很多方法，在常用的方法是让申请者在域名上放一个文件，然后CA验证该文件是否存在，即可证明该域名是否是申请者的。我们把这类数字证书称为DV，审核这种个人域名信息是最简单的，因此CA收取的费用也是最低的，有些CA甚至免费为个人颁发数字证书。

如果申请者是普通公司，那么CA除了验证域名的所有权之外，还需要验证公司公司的合法性，这类证书通常称为OV。由于需要验证公司的信息，所有需要额外的资料，而且审核过程也更加复杂，申



请OV证书的价格也更高，主要是由于验证公司的合法性是需要人工成本的。

如果申请者是一些金融机构、银行、电商平台等，所以还需额外的要验证一些经营资质是否合法合规，这类证书称为EV。申请EV的价格非常高，甚至达到好几万一年，因为需要人工验证更多的内容。

好了，我们了解了证书有很多种不同的类型，DV这种就可以自动审核，不过OV、EV这种类型的证书就需要人工验证了，而每个地方的验证方式又可能不同，比如你是一家美国本地的CA公司，要给中国的一些金融公司发放数字证书，这过程种验证证书就会遇到问题，因此就需要本地的CA机构，他们验证会更加容易。

因此，就全球就有很多家CA机构，然后就出现了一个问题，这些CA是怎么证明它自己是安全的？如果一个恶意的公司也成立了一个CA机构，然后给自己颁发证书，那么这就非常危险了，因此我们必须还要实现一个机制，让CA证明它自己是安全无公害的。

这就涉及到数字证书链了。

要讲数字证书链，就要了解我们的CA机构也是分两种类型的，中间CA(Intermediates CAs)和根CA(Root CAs)，通常申请者都是向中间CA去申请证书的，而根CA作用就是给中间CA做认证，通常，一个根CA会认证很多中间的CA，而这些中间CA又可以去认证其它的中间CA。

比如你可以在Chrome上打开极客时间的官网，然后点击地址栏前面的那把小锁，你就可以看到*.geekbang.org的证书是由中间CA GeoTrust RSA CA2018颁发的，而中间CA GeoTrust RSA CA2018又是由根CA DigiCert Global Root CA颁发的，所以这个证书链就是：*.geekbang.org--->GeoTrust RSA CA2018--->DigiCert Global Root CA。

因此浏览器验证极客时间的证书时，会先验证*.geekbang.org的证书，如果合法在验证中间CA的证书，如果中间CA也是合法的，那么浏览器会继续验证这个中间CA的根证书。

这时候问题又来了，怎么证明根证书是合法的？

浏览器的做法很简单，它会查找系统的根证书，如果这个根证书在操作系统里面，那么浏览器就认为这个根证书是合法的，如果验证的根证书不在操作系统里面，那么就是不合法的。

而操作系统里面这些内置的根证书也不是随便内置的，这些根CA都是通过WebTrust国际安全审计认证。

那么什么又是WebTrust认证？

WebTrust（网络信任）认证是电子认证服务行业中唯一的国际性认证标准，主要对互联网服务商的系统及业务运作的商业惯例和信息隐私，交易完整性和安全性。WebTrust认证是各大主流的浏览

器、微软等大厂商支持的标准，是规范CA机构运营服务的国际标准。在浏览器厂商根证书植入项目中，必要的条件就是要通过WebTrust认证，才能实现浏览器与数字证书的无缝嵌入。

目前通过WebTrust认证的根CA有 Comodo, geotrust, rapidssl, symantec, thawte, digicert 等。也就是说，这些根CA机构的根证书都内置在大操作系统中，只要能从数字证书链往上追溯到这几个根证书，浏览器会认为使用者的证书是合法的。

这也同时回答了你上面的问题。

共 9 条评论 >

👍 116



mfist

2019-10-26

1. 首先是tcp的三次握手建立连接
2. client发送random1+支持的加密算法集合 (clientHello)
3. server收到信息，返回选择一个加密算法+random2 (serverHello) + 证书+ 确认
4. client验证证书有效性，并用random1+random2生成pre-master通过服务器公钥加密 发送给server
5. server收到premaster，根据约定的加密算法对random1+random2+premaster (解密) 生成master-secret，然后发送预定成功
6. client收到生成同样的master-secret，对称加密密钥传输完毕

今日总结

浏览器安全主要包括页面安全、系统安全、传输安全三个部分。https主要保证传输过程的安全，从防止中间人窃取修改伪造的角度循序渐进的介绍了https的实现过程。

1. 对称加密传输 (协商密钥的过程容易被窃取)
2. 非对称加密传输 (服务端用私钥加密的内容，可以通过它的公钥进行解密)
3. 非对称加密交换密钥、对称加密传输内容 (DNS劫持 如何保证服务器是可信的)
4. 引入CA权威机构保证服务器可信性。

数字证书的申请过程：服务器生成一对公钥和私钥，私钥自己保存，通过公钥+企业+网站信息去CA机构申请证书。CA机构通过全方位的验证给这个网站颁发证书，证书内容包括企业信息、证书有效期、证书编号，以及自己私钥加密上述信息的摘要、网站的公钥。服务器就获得了CA的认证。

浏览器认证证书过程：浏览器从服务器拿到网站的证书，通过CA的公钥解密证书信息的摘要跟使用摘要算法计算企业信息等的摘要对比，如果一致则证明证书有效。如果证书CA是可靠的呢，通过给CA颁发证书的根CA验证，通常操作系统中包括顶级CA证书 (它们自己给自己签名称为自签名证书，我们自己生成证书也是自签名证书 只是它不是操作系统内置的)



作者回复: 这可以做标准参考答案了

共 9 条评论 >

👍 54

GY

2019-10-28

问了很多次，一直没有回复，想请问下老师，专栏中一直说的主线程和渲染引擎线程、js引擎线程之间有什么关系，渲染引擎和js引擎互斥，两个引擎是都运行在主线程中吗，这个主线程到底是什么啊？

作者回复: 首先，渲染进程有个主线程，DOM解析，样式计算，执行JavaScript，执行垃圾回收等等操作都是在这个主线程上执行的，

没有所谓的渲染引擎线程和js引擎线程的概念，你可以把渲染和执行JavaScript是一种功能，如果要执行这些功能的话，需要在一个线程上执行，在chrome中，他们都是执行在渲染进程的主线程上。

正是因为他们都是执行在同一个线程之上的，所以同一时刻只能运行一个功能，也就是你说的互斥。

不知道这样解释你明白没有，如果还有疑惑欢迎继续提问。

共 2 条评论 >

👍 24

蓝配鸡

2019-10-26

HTTPS握手过程：

1. 建立TCP链接
2. 获取服务器证书并检查证实真实性
3. 通过证书里服务器的公钥发送自己的公钥以及协商对称加密需要的信息给服务器.
4. 服务器返回协商结果
5. 双方生成对称密钥
6. 开始通信

第二步证明了服务器就是服务器，其实已经可以愉快的沟通了（通过非对称加密），后面交换对称加密信息的步骤其实可以算是优化吧？我记得是TLS1.2才引入的？

有个问题：

根证书是信任的根源，老师说它是被系统内核管理的并且自签名，那如果系统内核被黑了岂不是黑客就可以作假了？根证书是不是就是一个躺在内核中（用户无法访问到）的文件？有没有什么机制或者技术去发现根证书是假的？还是说等到用户出现损失之后系统级别的更新来去除对这个根CA的信任？

给李兵老师：

不知不觉最后一节了，本人由于工作原因对前端以及chrome需要加深理解。老师的专栏每天上下班的时候都会听，反复的听。



不管是内容，还是文字结构梳理，都不难发现老师花了大量的精力和时间去思考如何讲透某一个知识点。

老师对知识的颗粒度把握的很好，既不是泛泛而谈，又不会太细以至于难以理解。使得我对前端，以及chrome产生了浓厚的兴趣！虽然现在整个前端，或者chrome浏览器对我来说可能还是打着码的，但相比之前，我相信我已经看到一个大致轮廓了，今后一定会更花时间在前端领域中，把这些码去掉，成为前端大神！

表达能力可能有限...总而言之，谢谢老师🙏！虽然这是最后一篇了，但是如果老师想做几篇加餐，我想同学们也是很欢迎的😄

作者回复：只要拿到系统权限，就能随意安装根证书，这种我见过很多！

之前百度升级到https最后，很多劫持就是采用这种方式来干的，在操作系统安装假的根证书，然后劫持整个站点！

所以让黑客在你电脑上安装了根证书，https也会变得不安全了！

最后感谢你一路陪伴和提的问题，也让我能更好的改进专栏



👍 17



gigot

2019-11-05

感谢老师的干货输出，终于看完了，收获非常大。

看到很多同学对 client-random 和 service-random 生成 pre-master 比较迷惑，这里交换信息采用的是 ECDHE 算法，其实是浏览器生成了一对非对称密钥，其中私钥c，公钥即 client-random 发给服务器；而服务器也同理生成非对称密钥，其中私钥s，公钥即 service-random 发给浏览器。然后根据离散对数和椭圆曲线的数学基础，可以得出 $\text{pre-Master} = f(c, \text{service-random}, \text{client-random}) = f(s, \text{service-random}, \text{client-random})$ 。即根据不同私钥得出相同的密钥。而离散对数是非常难逆推破解的（计算量非常大），而形成保密

共 4 条评论 >

👍 8



成楠Peter

2019-10-26

这篇文章是我看过最好的https总结的文章，拆解很到位。

作者回复：👉



👍 7



Chris

2020-07-15

老师,

为什么要在ssl四次建立连接步骤中, 生成三次随机数, 我觉得最后一次的用服务器公钥加密的随机数pre-master就可以保证安全了啊。

共 1 条评论 >

👍 6



早起不吃虫

2019-10-26

老师好, 您前面说随机数加密算法是公开透明的, 后面又说利用 client-random 和 service-random 计算出来 pre-master, 然后利用公钥对 pre-master 加密, 并向服务器发送加密后的数据, 。 。这样的话, premaster不是也是可以计算出来了吗, 有必要用公钥加密吗?

作者回复: 不好意思, 这个我写错了, 这个pre-master是随机生成的, 没有用到client-random和service-random。

内容已经改正了

共 3 条评论 >

👍 4



大前端洞见

2019-10-26

>虽然浏览器端可以使用公钥来加密, 但是服务器端只能采用私钥来加密, 私钥加密只有公钥能解密, 但黑客也是可以获取得到公钥的, 这样就不能保证服务器端数据的安全了。

老师, 这里不是很明白。浏览器使用公钥加密, 服务器端不是用私钥解密吗? 怎么你这里说“服务器端只能采用私钥来加密”呢?

作者回复: 这个要分开两部分来看:

- 1:浏览器发送数据给服务器
- 2:服务器发送数据给浏览器

浏览器发送数据给服务器时, 是采用服务器发送给浏览器的公钥加密的, 然后服务器可以拿它的私钥来解密。这个我们理解没问题的!

如果是服务器发送数据给浏览器, 由于浏览器只有服务器的公钥, 所以服务器只能用它的私钥来加密数据, 然后将加密的数据发送给浏览器, 浏览器使用公钥解密! 但是这个公钥是公开的, 所以服务器发送给浏览器的数据也就没有安全性可言了!

不知道这样解释你能明白吗?



共 2 条评论 >

👍 4



长草嘟嘟

2020-12-16

老师你好，原文中“首先浏览器读取证书中相关的明文信息，采用 CA 签名时相同的 Hash 函数来计算并得到信息摘要 A”，请问浏览器如何知道 CA 所用的是何种 HASH 函数。



👍 3



爱看书的蜗牛

2020-01-19

数字证书解决了DNS劫持的问题吗？并没有啊

共 3 条评论 >

👍 3



铭

2019-10-26

请问老师：

(1) 非对称加密部分，当浏览器的公钥给了服务器，服务器不就可以给浏览器安全传输数据了吗？

(2) 混合加密部分，“浏览器保存公钥，并利用 client-random 和 service-random 计算出来 pre-master”，经揣摩，pre-master是生成对称加密密钥的重要且唯一安全的参数，但是在浏览器端，计算出来的pre-master是安全的吗？因为考虑到client-random 和 service-random是可以被拦截的，是否pre-master可以在传输前就被知晓了？

(3) 混合加密方式有个漏洞，这种情况是服务器向浏览器发送公钥过程中被伪装篡改，导致浏览器不是与真正的“对话人”即服务器进行对话，因而出现了数字证书对公钥的身份进行公证。

作者回复：第一个问题：

通常浏览器是没有自己的证书的，也没有自己的公钥和私钥。

不过有一种情况，那就是服务器需要验证浏览器的身份，比如银行转账啥的，这种情况下，银行会给浏览器一个证书，通常是U盘的形式提供的，这种叫双向认证，不过不常见。

2:浏览器端计算pre-master是相对安全的，想攻破难度是非常高的，因为要攻击浏览器系统，做各种逆向，不是简单地截获下网络数据就行了。

3:公钥是和数字证书一起发动的，如果公钥改了，那么数字证书就会验证失败的，验证失败了浏览器也就不会继续下一步的请求了。





3



淡

2019-12-09

今天又读了两遍，收获很多，同时又产生了3个疑问：

- 1.“浏览器如何验证证书”这一节中提到“然后再利用对应 CA 的公钥解密签名数据，得到信息摘要 B”，这一步中CA的公钥怎么拿到的？我理解的浏览器收到的数字证书包含的公钥是服务器的公钥，这里公钥是不是要在验证过证书合法后才能得到CA的公钥？
- 2.文章说验证数字证书的CA是否合法的时候，当前的数字证书包含了完整的CA链？如果没有，当CA是个层级比较低的CA的时候（假设中间有3层），怎么判断中间CA是否是合法的？
- 3.“通常情况下，操作系统中会内置信任的顶级 CA 的证书信息（包含公钥），如果这个 CA 链中没有找到浏览器内置的顶级的 CA，证书也会被判定非法”，请问这里是操作系统内置证书还是浏览器内置证书？

共 8 条评论 >



2



影相随

2021-04-29

我有一个疑问，就是数字证书虽然不可以伪造，但是可不可以被劫持，比如中间人劫持了服务器返回的数字证书，然后把劫持到数字证书返回给浏览器，那浏览器拿到的数字证书依然可以验证通过呢？



1



Angus

2019-10-28

这是我在极客时间认真看完并总结的第一篇专栏，并且在最后将自己的网站升级了HTTPS。整体来说受益匪浅，后续还会反复查阅的，感谢！

作者回复: 🙏



1



填

2019-10-26

期待大佬以后有机会继续发布这么高质量的系列，很感谢这段时间的输出

作者回复: 🙏



1



一觉天明

2022-02-07



老师你好，第一步浏览器向服务器发送对称加密套件和非对称加密套件的时候是不是可以省掉那个随机数啊，感觉好像没啥用



电单车

2022-02-03

过年花了好几天时间一口气看完了，简直停不下来，写的真好，感谢



Yvan

2021-12-30

有一个问题，虽然黑客拿不到 pre-master，但他可以利用公钥伪造 pre-master 吧。浏览器和服务器是如何解决这种伪造的。

共 1 条评论 >



张宗智ZZZ

2021-12-11

我不太理解，CA证书是明文的，黑客也能获取到？那么黑客改了请求的IP地址，他只需要将获取到的这个证书保存起来发给浏览器，这时浏览器岂不是仍然不知道访问的正确与否？

共 1 条评论 >

