21 | 如何保证数据传输的安全（上）？

2019-08-31 李超

从0打造音视频直播系统 进入课程 >

讲述：李超
时长 12:14 大小 11.21M

数据安全越来越受到人们的重视，尤其是一些敏感数据，如重要的视频、音频等。在实现音视频通信的过程中，如果在网络上传输的音视频数据是未加密的，那么黑客就可以利用 Wireshark 等工具将它们录制下来，并很容易地将它们播放出来并泄漏出去。

如果这些音视频的内容涉及到股票交易或者其他一些更敏感的内容的话，很可能会造成不可挽回的损失。

对于浏览器更是如此，在全球至少有几亿用户在使用浏览器，这么大的用户量，如果通过浏览器进行音视频传输时，没有对音视频数据进行安全保护的话，那将会产生灾难性的后果。

既然数据安全这么重要，那接下来我将带你了解一下数据安全方面的相关概念。只有将这些基本概念搞清楚了，你才知道 WebRTC 是如何对数据进行防护的。

非对称加密

目前对于数据的安全保护多采用非对称加密，这一方法在我们的日常生活中被广泛应用。那**什么是非对称加密呢**？下面我就向你简要介绍一下。

在非对称加密中有两个特别重要的概念，即**公钥**与**私钥**。它们起到什么作用呢？这里我们可以结合一个具体的例子来了解一下它们的用处。

有一个人叫小 K，他有一把特制的锁，以及两把特制的钥匙——公钥和私钥。这把锁有个非常有意思的特点，那就是：**用公钥上了锁，只能用私钥打开；而用私钥上的锁，则只能公钥打开。**

这下好了，小 K 正好交了几个异性笔友，他们在书信往来的时候，难免有一些“小秘密”不想让别人知道。因此，小 K 多造了几把公钥，给每个笔友一把，当笔友给他写好的书信用公钥上了锁之后，就只能由小 K 打开，因为只有小 K 有私钥（公钥上的锁只有私钥可以打开），这样就保证了书信内容的安全。

从这个例子中，你可以看到小 K 的笔友使用公钥对内容进行了加密，只有小 K 可以用自己手中的私钥进行解密，这种对同一把锁使用不同钥匙进行加密 / 解密的方式称为**非对称加密**，而**对称加密**则使用的是同一把钥匙，这是它们两者之间的区别。

数字签名

了解了非对称加密，接下来你就可以很容易理解什么是**数字签名**了。

首先我们来讲一下数字签名是解决什么问题的。实际上，数字签名并不是为了防止数据内容被盗取的，而是解决如何能证明数据内容没有窜改的问题。为了让你更好地理解这个问题，我们还是结合具体的例子来说明吧。

还是以前面的小 K 为例，他觉得自己与多个异性交往太累了，并且看破红尘决定出家了。于是他写了一封公开信，告诉他的异性朋友这个决定。但小 K 的朋友们认为这太不可思议了，她们就猜测会不会是其他人冒充小 K 写的这封信呢！

那小 K 该如何证明这封公开信就是他自己写的呢？他想到了一个办法：将信中的内容做个 Hash 值（只要是同样的内容就会产生同样的 Hash 值），并用他的私钥将这个 Hash 值进行了加密。这样他的异性朋友就可以通过她们各自手里的公钥进行解密，然后将解密后的

Hash 值与自己计算的公开信的 Hash 值做对比（这里假设她们都是技术高手哈），发现 Hash 值是一样的，于是确认这封信真的是小 K 写的了。

数字签名实际上就是上面这样一个过程。在互联网上，很多信息都是公开的，但如何能证明这些公开的信息确实是发布人所写的呢？就是使用**数字签名**。

数字证书

实际上，在数字签名中我们是假设小 K 的朋友们手里的公钥都是真的公钥，如果这个假设条件成立的话，那整个流程运行就没有任何问题。但是否有可能她们手里的公钥是假的呢？这种情况还是存在很大可能性的。

那该如何避免这种情况发生呢？为了解决这个问题，**数字证书**就应运而生了。

小 K 的朋友们为了防止自己手里的公钥被冒充或是假的，就让小 K 去“公证处”（即证书授权中心）对他的公钥进行公证。“公证处”用自己的私钥对小 K 的公钥、身份证、地址、电话等信息做了加密，并生成了一个证书。

这样小 K 的朋友们就可以通过“公证处”的公钥及小 K 在“公证处”生成的证书拿到小 K 的公钥了，从此再也不怕公钥被假冒了。

到这里，从非对称加密，到数字签名，再到数字证书就形成了一整套安全机制。在这个安全机制的保护下，就没人可以非法获得你的隐私数据了。

X509

了解了互联网的整套安全机制之后，接下来我们再来看一下真实的证书都包括哪些内容。这里我们以 X509 为例。**X509 是一种最通用的公钥证书格式。**它是由国际电信联盟（ITU-T）制定的国际标准，主要包含了以下内容：

版本号，目前的版本是 3。

证书持有人的公钥、算法（指明密钥属于哪种密码系统）的标识符和其他相关的密钥参数。

证书的序列号，是由 CA 给予每一个证书分配的唯一的数字型编号。

……

从中你可以看到，最关键的一点是通过 X509 证书你可以拿到“**证书持有人公钥**”，有了这个公钥你就可以对发布人发布的信息进行确认了。

在真实的场景中，你一般不会去直接处理数字证书，而是通过 OpenSSL 库进行处理，该库的功能特别强大，是专门用于处理数据安全的一套基础库，在下一篇文章中我们会对它做专门介绍。

5 种常见的加密算法及作用

介绍完数字签名、数字证书等相关概念后，下面我们再来学习一下几种常见的加密算法及其作用，了解它们的作用，对你后面学习 WebRTC 的数据安全有非常重要的意义。

1. MD5 算法

MD5 算法使用的是**哈希函数**，它一般用于对一段信息产生信息摘要，以防止数据内容被窜改。实际上，MD5 不能算是一种加密算法，而应该算作一种摘要算法。无论你输入多长的数据，MD5 算法都会输出长度为 128bits 的位串。

2. SHA1 算法

介绍完 MD5 后，我们再来看看 SHA1 算法。SHA1 和 MD5 的功能很类似，但相较而言，它**比 MD5 的安全性更强**。SHA1 算法会产生 160 位的消息摘要，一般应用于检查文件完整性以及数字签名等场景。

3. HMAC 算法

HMAC（Hash-based Message Authentication Code），使用 MD5、SHA1 算法，对密钥和输入消息进行操作，输出消息摘要。

HMAC 对发送方和接收方的 key 进行计算，并生成消息摘要，而其他人由于没有发送方或接收方的 key，所以无法计算出正确的哈希值，从而防止数据被窜改。

4. RSA 算法

RSA 是 1977 年由三位数学家 Rivest、Shamir 和 Adleman 设计的一种算法。RSA 就是以三位数学家名字的首字母组成的。RSA 算法是目前**最流行的非对称加密算法**。

5. ECC 算法

ECC 也是一种**非对称加密算法**，它的安全性比 RSA 更高，不过性能要差一些。

以上我们简要介绍了 5 种常见的加密算法，对于这些算法的具体实现不是本文的重点，本文的重点是让你对这些数据加密、安全等概念有一些了解，因为以后你研究 WebRTC 数据安全相关的源码时就会用到这些概念。

所以，弄清楚以上这些数据安全相关的概念，对你后面深入学习 WebRTC 具有重要的意义。

小结

在本文中，我向你介绍了非对称加密、公钥 / 私钥、数字签名、数字证书以及目前最通用的证书格式 X509，在文章的最后我还向你简要介绍了几种最常见的加密算法及作用。

由于数据安全涉及到的知识点特别多，所以本文更多的是向你介绍为了达到数据安全都用到了哪些方法，以及这些方法是因何而来的。

只有理解了这其中的道理，你在后面才能更好地理解 WebRTC 在数据安全方面的一些做法。其实，在学习任何新知识之前，我都很建议你按照这个思路去学习，也就是先了解其背后的原理或道理，然后再学习它的具体实现，这样可以让你的学习效率事半功倍。

而且依我的经验来看，越是比较难以理解或难以学习的知识，比如像 WebRTC 这种，就越应该按照这种方法来学习。倒是对于一些比较浅显的知识，反而通过实战和摸索的方式更有效果。

以上是我学习 WebRTC 的一点心得，你可以参考下，希望对你能有所帮助！

思考时间

今天你要思考的问题是：WebRTC 中使用的数据安全机制与 HTTPS 使用的安全机制是否是一样的呢？

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。

参考

以下是 X509 证书的详细内容，你可以了解下。

版本号：目前的版本是 3。

证书持有人的公钥、算法（指明密钥属于哪种密码系统）的标识符和其他相关的密钥参数。

证书的序列号：证书颁发机构给每一个证书分配的唯一的数字型编号。

主题信息：证书持有人唯一的标识符。

证书的有效期：证书的起始时间以及终止时间。

认证机构：证书的发布者。

发布者的数字签名：这是“认证中心”私钥生成的签名，以确保这个证书在发放之后没有被窜改过。

签名算法标识符：用来指定签署证书时所使用的签名算法。

上一篇　20 | 原来WebRTC还可以实时传输文件?

精选留言 (2)

写留言

君

2019-09-02

请问下老师webrtc多人视频，是不是每添加一路视频源就要创建一个RTCPeerConnection对象


许童童

2019-08-31

思考题：基本上是一样的，先用数字证书验证对方身份，然后通过非对称加密交换对称加密密钥，最后用对称加密进行通讯，保证数据的安全。

展开