登录

什么是会话密钥？会话密钥和 TLS 握手

TLS（过去称为“SSL”）协议同时使用非对称/公钥和对称加密，并且必须为每个通信会话生成用于对称加密的新密钥。这样的密钥称为“会话密钥”。

学习目标

阅读本文后，您将能够：

- 了解什么是会话，什么是密钥以及何时必须创建新的会话密钥
- 了解非对称和对称加密之间的区别
- 了解 SSL/TLS 加密协议如何同时使用两种加密方式

相关内容

复制文章链接

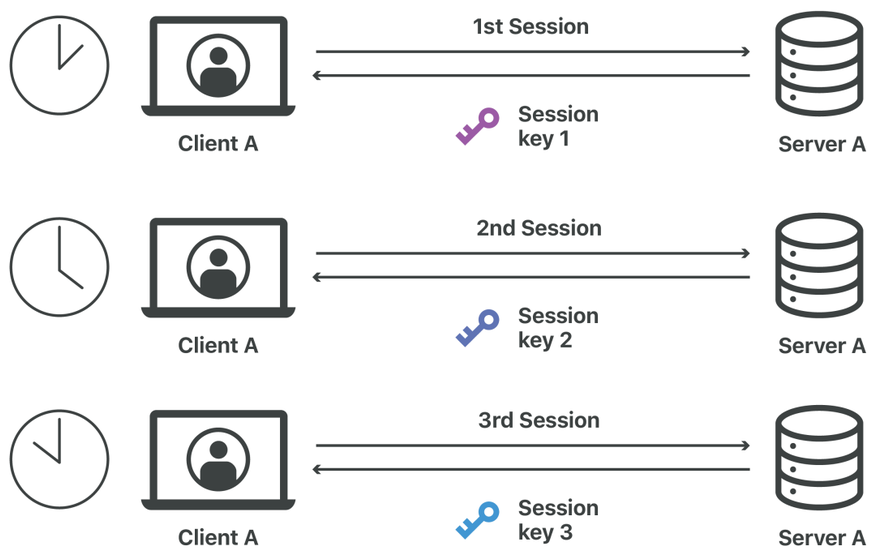
什么是会话密钥?

会话密钥是用于仅对单次通信会话进行加密的任何对称加密密钥。换句话说，它是一个临时密钥，只使用一次，仅在一个时间段内用于加密和解密双方之间发送的数据；双方之间的未来对话将使用不同的会话密钥进行加密。会话密钥就像每次登录时都会重置的密码一样。

在 TLS（过去称为“SSL”） 中，两个通信方（客户端和服务器）在任何通信会话最开始的 TLS 握手期间生成会话密钥。尽管 TLS 的官方 RFC 实际上并未将这些密钥称为“会话密钥”，但是从功能上讲，这就是它们的本质。

什么是会话?

会话本质上是两方之间的单个对话。会话通过网络进行，当两个设备相互确认并打开虚拟连接时即视为会话开始。当两个设备从对方获得所需的信息，发送“close_notify”消息并终止连接时，会话就结束了，这个过程就像两个人互相发短信，他们通过说“稍后再谈”来结束对话。连接也可能由于不活动而超时，例如发短信的两个人停止回复对方。



会话时间可以设定为固定的长短，也可以随两个通信方的持续对话而继续进行。如果是前者，则会话将在一定时间后到期；在 TLS 加密的情况下，这两个设备将必须交换信息并生成新的会话密钥以重新打开连接。

什么是加密密钥?

在密码学中，通常使用密钥（通常是一小段数据）来指代加密算法的特殊输入。最常用的密钥是用于数据加密的密钥；但是，存在用于不同目的的其他类型的密钥。

数据加密算法使用（秘密）密钥将消息转换为密文——即消息的加扰、不可读版本。可以使用解密密钥将密文恢复为原始消息。

在对称加密算法中，加密和解密密钥是相同的。因此，任何持有密钥的人都可以加密和解密数据，这就是人们常常使用术语“对称密钥”的原因。

相反，在非对称加密算法中（也称为公钥加密），存在两个密钥：一个是公共的，只能用于加密数据，另一个是私有的，仅用于解密密文。

HTTPS 使用对称还是非对称加密?

HTTPS 是 HTTP 与 TLS 协议的结合，它使用这两种类型的加密。所有通过 TLS 进行的通信都以 TLS 握手开始。非对称加密对于 TLS 握手的正常运转至关重要。

在 TLS 握手过程中，两个通信设备将建立会话密钥，这些密钥将用于其余会话的对称加密（除非设备选择在会话期间更新其密钥）。通常，这两个通信设备之一是客户端或者是诸如笔记本电脑或智能手机之类的用户设备，另一个是任何能托管网站的网页服务器。（如需更多信息，请参阅什么是客户端–服务器模型？）

在 TLS 握手中，客户端和服务器还会：

- 协商使用哪些加密算法（通过非对称加密安全地进行）
- 根据其 TLS 证书验证服务器的身份（使用非对称加密）

TLS 握手中的“主密钥”是什么？它与会话密钥有何关系？

主密钥是由客户端发送的一串随机数据、服务器发送的随机数据和另一串称为“预主密钥”的数据通过算法组合而成的。客户端和服务器各自拥有这三个消息，因此它们应该针对主密钥得出相同的结果。

然后，客户端和服务器使用主密钥计算几个会话密钥，仅在该会话中使用。它们最终应该得出相同的会话密钥。

详细了解 TLS 的工作原理：TLS 握手期间会发生什么？