SSL安全问题及漏洞——安全小课堂第二十九期

京东安全应急响应中心 2016-10-14

安全小课堂第二十九期

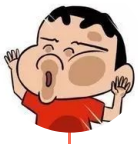
SSL是一个安全传输协议，其作用是身份验证，附带的是数据加密。通俗的来说就是用来加密传输服务器与网页之间的数据，在传输中保证数据的不被窃取，防止有人窥探你的敏感信息。本期我们来聊一聊SSL安全问题及漏洞。

本期邀请到
白帽子-Mend
知道创宇安全专家-城上
白帽子wAnyBug（ddy）
大家欢迎~

01

豌豆妹

什么是SSL？



小新

SSL =Secure Socket Layer，是一个安全传输协议，位于TCP/IP协议与各种应用层协议之间。它为Netscape所研发，用以保障在Internet上数据传输之安全，利用数据加密(Encryption)技术，可确保数据在网络上之传输过程中不会被截取。它已被广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输。SSL协议位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持。

02

豌豆妹

那能说说 SSL的重要性么？

哆啦A梦 

SSL还是灰常重要的，它的设计目的主要是提供以下服务：A、认证用户和服务器，确保数据发送到正确的客户机和服务器；B、加密数据以防止数据中途被窃取；C、维护数据的完整性，确保数据在传输过程中不被改变。从他提供的服务，就知道它的重要性了；D、不可否认服务，从技术上保证网站和用户对其行为的认可；E、公正服务，通过技术手段证明数据的有效性和正确性。

葫芦娃 

个人认为，SSL证书的作用是身份验证，附带的是数据加密。通俗的来说就是用来加密传输服务器与网页之间的数据，在传输中保证数据的不被窃取，防止有人窥探你的敏感信息。

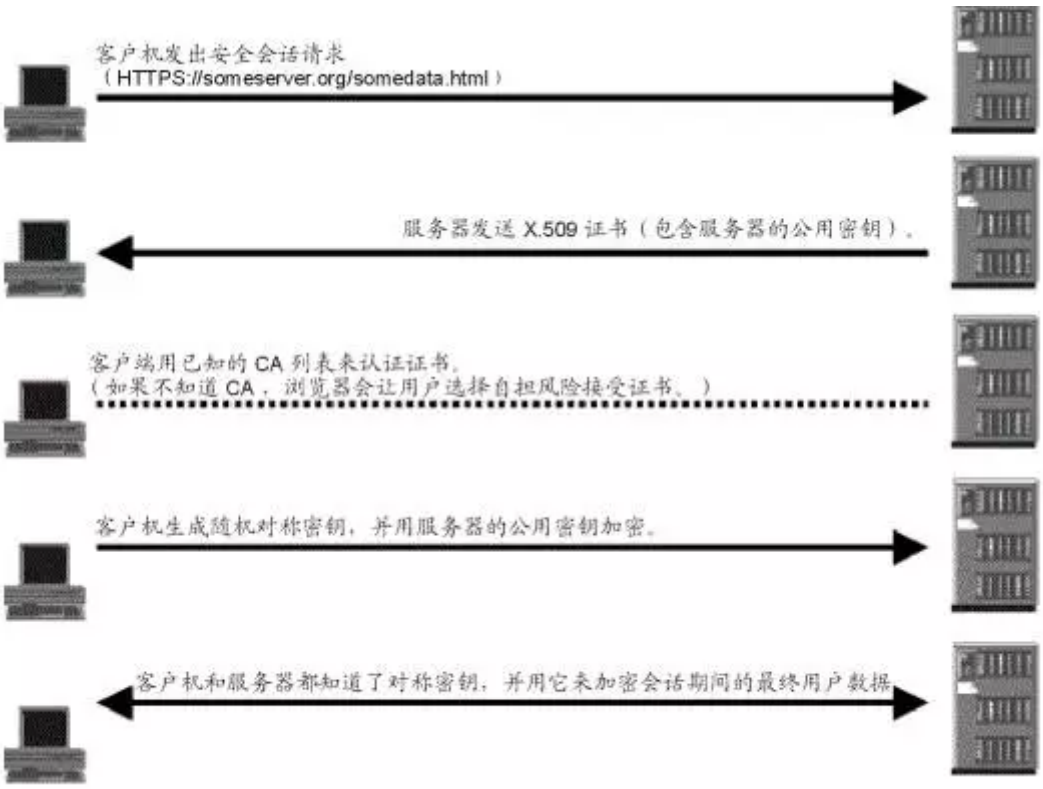
03

豌豆妹

SSL常见安全问题都有哪些呢？

小新 

安全问题就跟他的SSL工作原理有关了，先看下SSL握手的过程：



通过分析SSL握手过程，我们可以看到有 SSL的工作过程主要涉及客户端、服务器、CA证书服务器，大致来说，安全问题主要涉及CA证书服务器安全问题、服务器的私钥安全问题，以及经SSL代码实现的安全问题。

CA证书服务器安全问题主要是被爆破导致证书被窃取，CA证书服务器拒绝服务问题等。

服务器私钥安全问题，主要是私钥丢失的问题，比如猪队友把私钥放github上了。

SSL代码实现问题，主要是各种SSL实现库的问题吧，最经典的就是openSSL的漏洞。截至2016年10月1日，openSSL cve的数量已经达到255个。所以类似openSSL这种公共的加密库的安全应该持续关注， 该升级升级，该打补丁的打补丁。

04

豌豆妹

解决这些SSL常见安全问题的有效方法都有哪些呢？

小柴

除了对症下药，针对原来的错误配置进行修改，还有对已知的漏洞进行修复，并不能完全信任依靠SSL。

哆啦A梦

推荐下 libressl。针对证书服务的安全问题，建议最后在选择证书的时候，看看CA提供商的黑历史。开发者和公司要持续关注SSL爆出的安全问题，提高自身的安全意思，注意证书的保护。个人的话，需要提高保护自己敏感信息的意识，要注意非法证书，不要直接就点确认。

豌豆妹

开发者具体怎么注重SSL安全？

小新

其实最根本的就是要有使用SSL的意识，尤其是登录、输入密码，还有检验升级的地方。因为检验升级的地方不做SSL，可以挟持给用户下载一个含木马的安装包（安卓），或者诱导用户下载到其他的软件（安卓苹果）。
然后再谈技术层面的问题，首先要检验SSL证书，不要忽略SSL错误，服务端启用htst。注意保护SSL的私钥不要丢失，丢了要及时去CA申请注销/吊销这张证书。

豌豆妹

O(∩_∩)O哈！谢谢各位~本期的小课堂就告一段落哟~咱们下期见！有想知晓的安全话题，都可直接回复给我哦，我会尽量满足大家的需求呢！

微信公众号：jsrc_team
新浪官方微博：
京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂