关于身份验证：如何在客户端完全禁用SSL会话恢复?

authentication openssl session ssl

How to disable SSL session resumption on client side completely?

我正在使用OpenSSL 1.0.2g。 在我的客户端中，我想完全禁用SSL会话恢复(出于测试目的)。

创建SSL_CTX之后，我会在连接之前执行以下操作：

```
SSL_CTX_set_session_cache_mode(ctx, SSL_SESS_CACHE_OFF);
SSL_CTX_set_options(ctx, SSL_OP_NO_TICKET);
```

但是我在流量捕获中看到的是-我的客户端总是通过发送非空会话ID来进行会话重用。 服务器确实接受它。

如何完全禁用SSL会话恢复?

更多扩展的代码段：

```
SSL_CTX *ctx = NULL;
ctx = SSL_CTX_new(SSLv23_client_method())
SSL_CTX_set_session_cache_mode(ctx, SSL_SESS_CACHE_OFF);
SSL_CTX_set_options(ctx, SSL_OP_NO_TICKET);
SSL_CTX_set_verify(ctx, SSL_VERIFY_NONE, NULL);
SSL_CTX_set_verify_depth(ctx, 0);
SSL_CTX_set_mode(ctx, SSL_MODE_AUTO_RETRY);
```

我做错什么了吗? 是否缺少任何必需的步骤?

相关讨论

您正在设置自动重试：

```
SSL_CTX_set_mode(ctx, SSL_MODE_AUTO_RETRY);
```

根据文档：

> SSL_MODE_AUTO_RETRY
>
> Never bother the application with retries if the transport is blocking. If a renegotiation take place during normal operation, a SSL_read or SSL_write would return with -1 and indicate the need to retry with SSL_ERROR_WANT_READ. In a non-blocking environment applications must be prepared to handle incomplete read/write operations. In a blocking environment, applications are not always prepared to deal with read/write operations returning without success report. The flag SSL_MODE_AUTO_RETRY will cause read/write operations to only return after the handshake and successful completion.

这意味着自动重新协商将以静默方式进行，而不会意识到使用OpenSSL库的应用程序。请参阅 `SSL_write()` 的文档：

> If the underlying BIO is blocking, SSL_write() will only return, once the write operation has been finished or an error occurred, except when a renegotiation take place, in which case a SSL_ERROR_WANT_READ may occur. This behaviour can be controlled with the SSL_MODE_AUTO_RETRY flag of the SSL_CTX_set_mode call.

这种"无声的"重新协商可以解释您观察到的行为，如果这样，不使用 `SSL_MODE_AUTO_RETRY` 可能会解决您的问题。

在我看来，OpenSSL是一种极其复杂的工具，其许多选项的行为记录不足。对于一个太相关的示例，该怎么做，"可以通过SSL_CTX_set_mode调用的SSL_MODE_AUTO_RETRY标志来控制此行为。"控制如何？暗示使用 `SSL_MODE_AUTO_RETRY` 允许静默重新协商并因此进行会话重用，但是从未明确声明。

同样，`SSL_CTX_set_session_cache_mode()` 的许多选项之一可能是相关的：

> In order to reuse a session, a client must send the session's id to the server. It can only send exactly one id. The server then either agrees to reuse the session or it starts a full handshake (to create a new session).
>
> A server will lookup up the session in its internal session storage. If the session is not found in internal storage or lookups for the internal storage have been deactivated (SSL_SESS_CACHE_NO_INTERNAL_LOOKUP), the server will try the external storage if available.

所以呢

> SSL_SESS_CACHE_OFF
>
> No session caching for client or server takes place.

禁用内部缓存的使用？对我而言，这意味着事实并非如此。

相关讨论

> Am I doing anything wrong?

我认为您在查看路况时一定做错了什么，或者代码中有很重要的部分没有显示。默认情况下，客户端根本不会恢复任何会话，这仅仅是因为它不知道应该恢复哪个会话。从SSL_CTX_set_session_cache_mode的文档中：

> SSL_SESS_CACHE_CLIENT
> ... As there is no reliable way for the OpenSSL library to know whether a session should b

e reused or which session to choose (due to the abstract BIO layer the SSL engine does not have details about the connection), the application must select the session to be reused by using the SSL_set_session function...

Copyright © 码农家园 联系：ddyu2x@gmail.com