SSL 和 TSL
安全通信协议概要

Simon Horman aka Horms

horms@valinux.co.jp
horms@verge.net.au
horms@debian.org

February 22, 2012

摘要

SSL/TLS 被广泛用于在因特网上安全的传输数据，但是它不是一个具有魔力的解决方案，如果没有很好的理解协议是如何工作的和底层的技术，就无法更全面的使用 SSL/TLS，甚至更糟的是，很容易以不安全的方式使用 SSL/TLS。

这次演示将会解释 SSL/TLS 是如何工作的，从数据完整性，保密性和端点验证这些高层协议的讨论到组成 SSL/TLS 协议不同报文和最终保护链接安全的加密技术这些低层讨论。

本次面向的观众是对使用或者开发利用 SSL/TLS 保护数据传输安全应用程序的人。

目录

1 安全通信

安全套接字层协议（SSL）和传输层安全协议（TLS）目的是提供一种在网络两端安全通信的机制，使得两端无需进行端到断的控制，也避免了第三方窃听通信内容。因特网就是很好的例子。本质上，我们将会谈到连个方面，数据完整性和端点验证。

1.1 数据完整性