第 17 章 总　结 17

恭喜你，一路完成了本书的学习！希望你在阅读时能像我写作时那样，收获一样多的乐趣。我们在书中讨论了这么多的TLS安全问题，那么我们到底面临着怎样的现状呢？TLS安全吗？还是说它有着无法修复的缺陷而注定要消亡？

与其他许多问题类似，答案完全取决于你对TLS的期望。如果与一些想象中的理想产品相比较，很容易指出TLS中的各种问题；TLS也确实存在很多问题，整个社区长期以来一直都在努力地修复完善。然而，安全协议的成功不能单纯地从技术性和安全性方面来衡量，更加重要的是在现实生活中的成功实践和实际效果。因此，尽管TLS并不完美，但每天仍有数十亿人使用它，这已经是一个巨大的成功。如果一定要在TLS生态系统中选出一个最大的问题，那就是我们还没有充分地使用加密，使用的时候也没有认真思考我们是否真的安全（想一想证书警告）。TLS的缺陷反而不是什么大问题。

我们一直在讨论TLS的安全性，这其实正是因为TLS非常成功，不然它早就被其他更好的产品取代了。不过，即使我们有机会使用其他产品来代替TLS，在经过多年的使用后，我们一样会碰到与TLS现状相同的情况。我清楚地意识到在全世界范围内不可能达到所谓完美的安全性。这个多样性的世界正在加强安全性方面缓慢前进，同时尽量避免对现状造成重大的破坏。你知道吗？这其实没什么大不了。这就是加入全球计算机网络的代价。

好消息是TLS正处在一个不断改善的良好阶段。多年前的某个时候，我们开始将更多注意力放在安全性上，尤其是加密环节。这一过程在2013年开始加速，因为随着用户使用越来越广泛，我们也不断地遭遇到大量安全问题。TLS工作小组正在忙于开发下一个协议版本。这一版本不会有（也不需要有）根本上的不同，但却会把我们的安全水平提高到一个更高的阶段。我会把这些新的内容写在这本书的未来版本中！