c. 现在假设创建了共享密钥 S_1 和 S_2。使用时序图提供一个协议（尽可能简单并且不使用公开密钥密码），该协议允许 Alice 从 activist. com 请求一个 html 页面而不向 Proxy2 透露她的 IP 地址，并且不向 Proxy1 透露她正在访问哪个站点。你的图应当终止在一个 HTTP 请求到达 activist. com。

Wireshark 实验

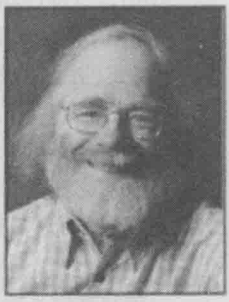
在这个实验中（与本书配套的 Web 站点有可用资源），我们研究安全套接层（SSL）协议。8.6 节讲过，使用 SSL 使得 TCP 连接更为安全，为了使因特网事务安全，实践中广泛应用了 SSL。在本实验中我们关注经 TCP 连接发送的 SSL 记录。我们将试图对每个记录定界和分类，目标是理解每个记录的工作原理和工作过程。我们研究各种 SSL 记录类型以及在 SSL 报文中的字段。通过分析你的主机与某电子商务服务器之间发送的 SSL 记录的踪迹来做这些事情。

IPsec 实验

在这个实验中（与本书配套的 Web 站点有可用资源），我们将探讨如何在 linux 装置之间创建 IPsec SA。你能够用两个普通的 linux 装置做该实验的第一部分，每个装置配有一块以太网适配器。但是对于实验的第二部分，你将需要 4 个 linux 装置，这些装置每个都具有两块以太网适配器。在该实验的第二部分，你将在隧道模式中使用 ESP 协议创建 IPsec SA。你做实验过程是：先人工创建 SA，然后让 IKE 创建 SA。

人物专访

Steven M. Bellovin 在位于新泽西州 Florham Park 的 AT&T 实验研究所的网络服务研究实验室工作多年后，成为了哥伦比亚大学的教师。他的研究重点是网络和安全，以及将两者有机结合起来。1995 年，因创立了 Usenet，即第一个连接两个或多个计算机并允许用户共享信息和参与讨论的新闻组交换网络，而被授予 Usenix 终生成就奖。Steven也是国家工程学会的当选成员。他获得了哥伦比亚大学的学士学位和位于 Chapel Hill 的北卡罗来纳大学的博士学位。



Steven M. Bellovin

- 什么原因使您决定专注于网络安全领域的研究？

听起来可能很奇怪，但是答案却很简单：只是因为感兴趣而已。我以前的背景是从事系统编程和系统管理，这很自然就发展到安全领域了。而且我一直对通信很感兴趣，这可以追溯到我还在上大学时，就兼职做系统编程方面的工作。

我在安全领域的工作持续受到两个因素的激励：一个是希望计算机有用，这意味着它们的功能不会被攻击者破坏，另一个是希望保护隐私。

- 当初您在研发 Usenet 时，您对它的愿景是什么？现在呢？

我们最初将它看作是一种能够在全国范围内讨论计算机科学和计算机编程的手段，考虑了用于事务管理和广告销售等目的的许多本地使用情况。事实上，我最初的预测是，每天从至多 50 ~ 100 个站点有 1 ~ 2 个报文。但是实际增长是与人相关的主题方面，包括（但不限于）人与计算机的相互作用。这么多年来，我喜欢的新闻组有 rec. woodworking 以及 sci. crypt。

在某种程度上，网络新闻已经被 Web 取代。如果现在要我再设计它的话，就会和那时的设计大不相同了。但是它仍然是沟通对某一主题感兴趣的大量读者的一种极好手段，而不必依赖特定的 Web 站点。

- 是否有人给过您专业上的启示和灵感？以什么样的方式呢？

Fred Brooks 教授对我的专业生涯影响重大。他是位于 Chapel Hill 的北卡罗来纳大学计算机科学系的创立者和原系主任，是研发 IBM S/360 和 OS/360 团队的管理者。他也是“The Mythical Man Mouth”