计算机网络中的安全

早在1.6节我们就描述了某些非常盛行和危险的因特网攻击，包括恶意软件攻击、拒绝服务、嗅探、源伪装以及报文修改和删除。尽管我们已经学习了有关计算机网络的大量知识，但我们仍然没有考察如何使网络安全，使其免受那些攻击的威胁。在获得了新的计算机网络和因特网协议的专业知识后，我们现在将深入学习安全通信，特别是计算机网络能够防御那些令人厌恶的坏家伙的原理。

我们首先介绍一下Alice和Bob，这俩人要进行通信，并希望该通信过程是“安全”的。由于本书是一本网络教科书，因此Alice和Bob可以是两台需要安全地交换路由选择表的路由器，也可以是希望建立一个安全传输连接的客户和服务器，或者是两个交换安全电子邮件的电子邮件应用程序，所有这些学习案例都是在本章后面我们要考虑的。总之，Alice和Bob是安全领域中的两个众所周知的固定设备，也许因为使用Alice和Bob更为有趣，这与命名为“A”的普通实体需要安全地与命名为“B”的普通实体进行通信的作用是一样的。需要安全通信的例子通常包括不正当的情人关系、战时通信和商业事务往来；我们宁愿用第一个例子而不用后两个例子，并乐于使用Alice和Bob作为我们的发送方和接收方，并以第一种情况为背景来讨论问题。

我们说过Alice和Bob要进行通信并希望做到“安全”，那么此处的安全其确切含义是什么呢？如我们将看到的那样，安全性（像爱一样）是多姿多彩的东西；也就是说，安全性有许多方面。毫无疑问，Alice和Bob希望他们之间的通信内容对于窃听者是保密的。他们可能也想要确保当他们需要进行通信时，确实是在和对方在通信，还希望如果他们之间的通信被窃听者篡改时，他们能够检测到该通信已被这种篡改破坏。在本章的第一部分，我们将讨论能够加密通信的密码技术，鉴别正在与他通信的对方并确保报文完整性。

在本章的第二部分，我们将研究基本的密码学原则怎样能够被用于生成安全的网络协议。我们再次采用自顶向下方法，从应用层开始，将逐层（上面四层）研究安全协议。我们将研究如何加密电子邮件，如何加密一条TCP连接，如何在网络层提供覆盖式安全性，以及如何使无线LAN安全。在本章的第三部分，我们将考虑运行的安全性，这与保护机构网络免受攻击有关。特别是，我们将仔细观察防火墙和入侵检测系统是怎样加强机构网络的安全性的。

8.1 什么是网络安全

我们还是以要进行“安全”通信的情人Alice和Bob为例，开始我们的网络安全的研究。这确切地意味着什么呢？显然，Alice希望即使他们在一个不安全的媒体上进行通信，也只有Bob能够理解她所发送的报文，其中入侵者（入侵者名叫Trudy）能够在该媒体上截获从Alice向Bob传输的报文。Bob也需要确保从Alice接收到的报文确实是由Alice所发送，并且Alice要确保和她进行通信的人的确就是Bob。Alice和Bob还要确保他们报文的内容在传输过程中没有被篡改。他们首先也要确信他们能够通信（即无人能够拒绝他们