HZ BOOKS
华章教育

计 算 机 科 学 丛 书

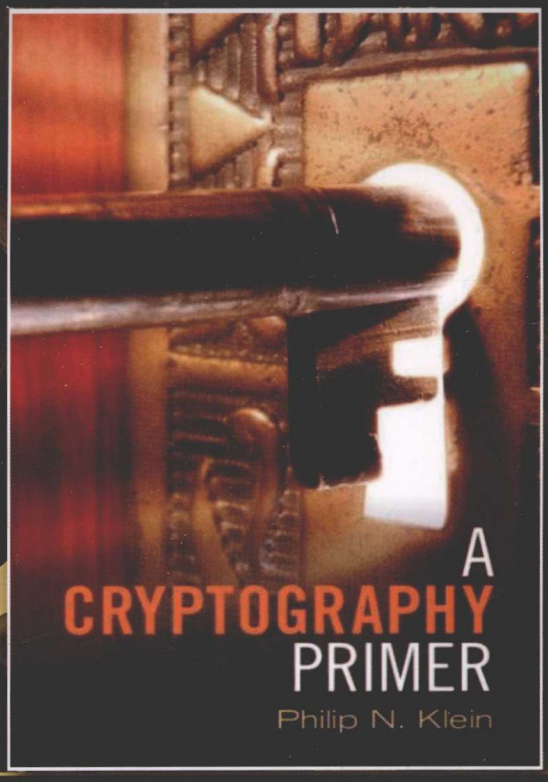
CAMBRIDGE

密码学基础教程

秘密与承诺

[美] 菲利普 N. 克莱因（Philip N. Klein）著
徐秋亮 蒋瀚 王皓 译

A Cryptography Primer
Secrets and Promises



机械工业出版社
China Machine Press

计 算 书

密码学基础教程

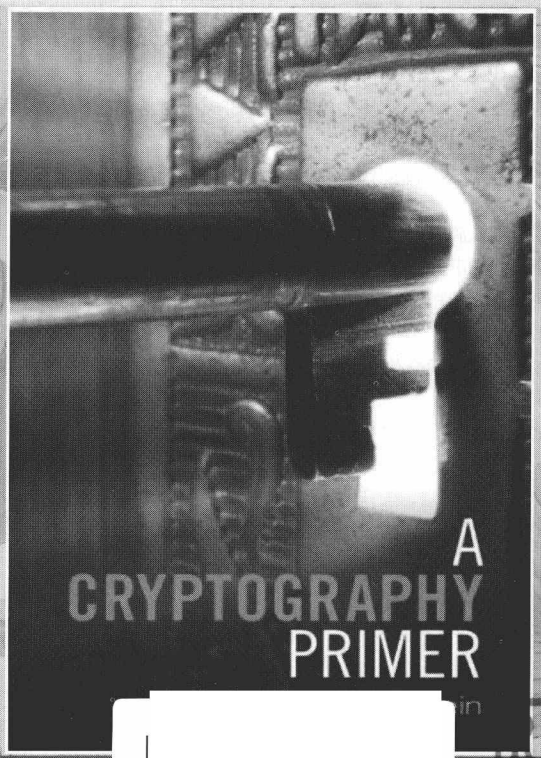
秘密与承诺

[美] 菲利普 N. 克莱因（Philip N. Klein）著

徐秋亮 蒋瀚 王皓 译

A Cryptography Primer

Secrets and Promises



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

密码学基础教程：秘密与承诺 /（美）菲利普 N. 克莱因（Philip N. Klein）著；徐秋亮，蒋瀚，王皓译 . —北京：机械工业出版社，2016.9
（计算机科学丛书）
书名原文：A Cryptography Primer：Secrets and Promises

ISBN 978-7-111-54436-4

I. 密… II. ① 菲… ② 徐… ③ 蒋… ④ 王… III. 密码－高等学校－教材 IV. TN918.1

中国版本图书馆 CIP 数据核字（2016）第 176191 号

本书版权登记号：图字：01-2016-3495

本书以通俗、直观的方式清晰阐述了现代密码学的基础知识，包括用来实现通信隐私性 / 机密性的保密算法（协议）及保证消息正确性、完整性、来源可靠性的数字签名协议，提供了一个易读、易学的关于现代密码学基本原理和数学知识的导引，通过浅显的例子和生动的语言让读者绕过晦涩的专业术语而直接看到密码技术的本质。

本书叙述清晰，简单易懂，适合作为高等院校计算机及相关专业本科生教材。

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：迟振春　　责任校对：董纪丽
印　　刷：北京诚信伟业印刷有限公司　　版　　次：2016 年 9 月第 1 版第 1 次印刷
开　　本：185mm × 260mm　1/16　　印　　张：10.75
书　　号：ISBN 978-7-111-54436-4　　定　　价：49.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

文艺复兴以来，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域取得了垄断性的优势；也正是这样的优势，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅擘划了研究的范畴，还揭示了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短的现状下，美国等发达国家在其计算机科学发展的几十年间积淀和发展的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起到积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章公司较早意识到“出版要为教育服务”。自 1998 年开始，我们就将工作重点放在了遴选、移译国外优秀教材上。经过多年的不懈努力，我们与 Pearson，McGraw-Hill，Elsevier，MIT，John Wiley & Sons，Cengage 等世界著名出版公司建立了良好的合作关系，从他们现有的数百种教材中甄选出 Andrew S. Tanenbaum，Bjarne Stroustrup，Brian W. Kernighan，Dennis Ritchie，Jim Gray，Afred V. Aho，John E. Hopcroft，Jeffrey D. Ullman，Abraham Silberschatz，William Stallings，Donald E. Knuth，John L. Hennessy，Larry L. Peterson 等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及珍藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力相助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专门为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近两百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍。其影印版“经典原版书库”作为姊妹篇也被越来越多实施双语教学的学校所采用。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因

素使我们的图书有了质量的保证。随着计算机科学与技术专业学科建设的不断完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都将步入一个新的阶段，我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。华章公司欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

华章网站：www.hzbook.com
电子邮件：hzjsj@hzbook.com
联系电话：（010）88379604
联系地址：北京市西城区百万庄南街1号
邮政编码：100037

华章科技图书出版中心

计算机信息网络已经成为人们社会生活的基础设施，人们对网络的依赖已经可以和水、电等基本生活必需品比肩，大量的生活信息、工作信息和社会信息在网络中高速传送、处理和应用，多维度地支撑着人们家庭及社会生活的方方面面，形成了人们生活的另一个“空间”，财产、身份、学历甚至整个社会关系都变成了信息网络空间中的一条条“记录”。但是，人们对信息网络的强烈依赖，也产生了另一方面的问题。存储于网络空间中的数据便于传输、处理、共享但可控性差。网络空间给人们带来便利的同时也带来了隐私信息泄露、商业信息泄密以及消息被篡改、不当使用、身份被假冒等多重风险，如果不能对信息进行很好的保护，将会造成不可估量的损失。

密码学是一门古老的学科，甚至可追溯到古埃及的法老时代。当然，最初的密码应用环境非常简单，是一种主要用于保证通信安全的技术或技巧，直到20世纪40年代香农创立信息论并以此研究保密系统开始，密码的设计和分析开始变为一种有理论基础、有科学方法的“科学”。而目前信息网络应用的普遍性和其中信息安全问题的广泛性，使得密码学不再是军事、外交、国防领域的专宠，而成为人们社会生活中时时处处依赖的信息安全保障必备工具，这也是从20世纪70年代以来密码学迅速发展的原因。密码学已经成为当今社会不可或缺的应用学科。

为了使网络使用者对密码学有一个初步了解，我们翻译了美国布朗大学 Philip N. Klein 教授编著的《A Cryptography Primer: Secrets and Promises》一书。与普通的密码学教程不同，这本书不以密码学的研究和应用为目的，而注重密码知识的普及。阅读该书几乎不需要任何专门知识，书中从最初步的概念、最易理解的例子、最简单的应用开始，深入浅出，层层递进，一直到密码学思想的实质。本书不追求表达的严谨性和方法的通用性，力求让读者理解密码学最本质的原理，是一本极具特色的入门书，通俗易懂而又极其深刻。译者在翻译该书的过程中深感获益，希望该书中文版的出版能够给希望了解密码学的中文读者带来帮助。

对该书的编著者 Philip N. Klein 表示敬意。

译　者

2016年7月27日

前　言

A Cryptography Primer: Secrets and Promises

作为一个数论专家与和平主义者，G. H. Hardy 在其自传《一个数学家的致歉》中写道：

> ……令高斯以及少数数学家们欣慰的是，至少还有一种科学“数论”……能够远离人们的日常活动，它应当保持纯粹和优雅。

Hardy 的这本书于 1940 年出版，他当时正面临着职业生涯的结束。如果他能够延后 30 年再做出论断的话，或许他会得出截然不同的结论，因为数论成为一项与战争相关的重要技术（密码学——研究秘密编码的应用学科）的基础。

密码学的应用至少有数千年的历史。在印度圣经中，密码学被列为 64 项女人的技艺之一。其中一个著名的初等密码系统要归功于尤里乌斯·凯撒。许多逸闻趣事证实了多年以来密码学和密码分析学（即编码破解）在战争和外交博弈中的重要作用。例如，英国人曾截获并破译了由德国外交部发给墨西哥政府（经由大使）的齐默曼电报，在电报中德国许诺将得克萨斯州、新墨西哥州以及亚利桑那州划归给墨西哥作为其帮助对抗美国的回报，这促进了美国加入第一次世界大战的进程。密码分析学同时也在不那么重大的事件中发挥着作用，以下文字摘自 Casanova（1757）的自传：

> 五六周之后，她问我是否已经解密了这些手稿……我告诉她是的。
>
> “先生，恕我冒昧。没有密钥，这怎么可能呢?”
>
> “希望我告诉你密钥吗，夫人?”“如果这样的话告诉我吧。”
>
> 我告诉她密钥，这个密钥并不属于任何语言，然后看到她吃惊的表情。她告诉我说这是不可能的，因为她坚信她自己是唯一掌握这些密钥的人，她仅仅将这些密钥记在脑海中，从来没有写下来。
>
> 我本可以告诉她真相的——已被我掌握的与解密手稿同样的计算已经让我知道了密钥——但是一个邪恶的想法闪过心头，阻止我告诉她这一真相。我保持神秘使她深深地被我俘获，那天我主导了她的灵魂，肆意地散发着我的力量。

然而在信息时代，或许密码学最大的贡献还是在商业领域。一直以来，银行用密码学来保障电子传输的安全，分布在不同地域的公司用密码学来保证他们之间的通信不被工业谍报人员窃听。但是，或许最令人兴奋的应用在于，让素未谋

面并因此无法提前协商密钥的双方也能够安全地通信。随着互联网上的商业活动日渐繁荣，这种应用变得更加普及。幸运的是，现今的指数密钥交换协议和公钥密码学能够使这类应用成为现实。

Diffie 和 Hellman 在 1976 年提出了公钥密码学，其思想在于：有两个不同密钥，公开密钥用来加密消息，而私有密钥则用于解密；由一方秘密地生成这对密钥，他可以将加密密钥公开而不暴露用于解密的密钥。因而任何人都可以给密钥生成者发送加密的消息，而只有密钥生成者能够解密这一消息。Rivest、Shamir 和 Adleman 于 1978 年最先实现了这一思想。至于他们的方案有多么闻名于世，我们来看看下面这段摘自滑稽喜剧《山河之旅》中的对白吧：

> “杰伊，我不太熟悉计算机，对此知之甚少。我了解到这个密码是两个差不多 100 位的大素数相乘得到的，对吧?”
>
> “是的，很对。这被称为 RSA 密码系统。”
>
> “好吧，这一名字来源于 MIT 的 Rivest、Shamir 和 Adleman。我只知道这么多。我也知道即使是使用先进的计算机来破解，也需要花费无穷无尽的时间，”她回忆着，“两个 100 位的素数相乘得到的密钥差不多需要 38 亿年的时间来破解，对吧?”“完全正确。很明显，所有被窃取的信息都来自于从公司办公室到你家的电话线路上发生的窃听。假设只有麦克掌握解密密钥，如果他不将这一密钥分发给别人，那么是没人能够解密这一编码的。但是这一说法在逻辑上还有一点不严谨之处，”他边说边松了松深绿色的丝织领带，“Vee，这里比我想象的热好多啊，你介意我脱掉外套吗?”
>
> “当然不，你太客气了。”她说道……

我们的女主角 Vee 说道，RSA 的安全性是基于分解两个素数乘积的困难性，因此，它使得 Hardy 最喜欢的“纯”数学领域（数论）有了用武之地。这一密码系统（同大多数密码系统一样）的根基在于简单与困难的区别。生成一个公钥/私钥对就如同选择两个 100 位的素数并将它们相乘那么容易，而正如 Vee 所言，攻破这一系统（利用当前已知的方法）则需要大量的时间才能完成；这似乎需要用两个素数的乘积来确定这两个素数分别是什么，这一问题称为整数分解。尽管针对这一问题的研究有着持续的进展，但是无论如何，已知的算法的速度都还没有快到足以威胁 RSA 安全性的程度。下面引用一个更了解市场营销手段而不精通数论的人的一句话：

> 由于数字货币系统的隐私性和安全性都依赖于密码学，因此任何能

> 够攻破密码系统的数学或计算机科学的突破都会是一场灾难。而在数学方面最为显而易见的突破或许就是构建一个能够快速分解大整（素）数的方法。——比尔·盖茨，《未来之路》第一版，265 页
>
> （大整数分解是这样的问题，即已知一个数，求这个数是由哪些素数相乘得到的，如果这个数是一个素数，那么分解的结果就是它本身。）

但是 RSA 不仅仅用于加密。正如 Diffie 和 Hellman 意识到的那样，公钥密码学的另一个方面在于数字签名。使用类似于 RSA 的方式，公-私密钥对的生成者可以用私钥对文档产生一个签名。这是一个由文档产生的数字，拥有公钥的人都可以验证这一签名与文档是一致的（满足某种数学关系），而且只有拥有私钥的人才能够为文档产生合法的签名。因此一个文档的合法签名可以作为密钥生成者需要为此负责这一事实的强有力的证据。如果有人篡改了文档，那么篡改后的文档和签名不会再有相同的数学关系了，因此这一文档将会被视作无效。于是，数字签名可以用于互联网中传输的消息的认证，以此来防止潜在的消息篡改和伪造。它们可以用于创建不可伪造的证书，如电子版的信用卡或护照。它们也可以用于检测对计算机程序未经授权的篡改，如病毒的侵入等。

与此同时，其他保障计算机安全的技术也被陆续提出，包括对身份的安全认证（这与在电话中询问某电话号码、信用卡号码等信息以确认对方身份类似），对一个文档内容承诺但不泄露其信息的方法（对一个密封的信封的模拟），为一个文档打上时间标记的方法（对给自己邮寄一封信以得到带有时间的邮戳这一方法的模拟）。

计算科学对计算简单问题与计算困难问题进行了分类，而密码学技术正是构建于计算科学这一理论之上：在你拥有密钥的情况下，解密编码是容易的；而如果你没有密钥则不然。密码学正是对这种智慧追求的具体实现。

为了让更为广大的读者都能接触到这一饶有趣味的、令人兴奋的而且越来越重要的充满智力挑战性的领域，我开设了课程“秘密与承诺：数字安全导论”。我为这门课撰写了这本书作为教材。题目中“秘密”这个词表示用密码学的方法来实现私密通信；“承诺”这个词表示用数字签名来保证消息、文档或程序的有效性与完整性。本书旨在对现代密码学的基本理论和其所依赖的数学基础给出一个简介，而并非一部面向实践的、教你如何做的教材，即这本书不会指导读者如何用现代计算机程序（如网页浏览器和电子邮件系统）来实现数字安全。这些程序一直在更新换代，而且如果想在市场上占有一席之地，必须做到让它们的使用者无须了解这些软件所依赖的安全技术便可轻松使用。在本书中，我们要透过现象看到问题的本质，研究安全技术，探寻其之所以安全的原因。

对于一些基本的密码学方案，如 DES 和 SHA，其细节并没有启发作用，因而在本书中我们省略对其细节的讨论。其他一些基于初等数论的方案也能发挥与之相同的功能，尽管这些基于数论的方案效率低下难以实用，但是它们被认为是安全的，而且适合在这门课中讲解。因此为了最大限度地做到可读性与一致性，我们在实用性方面做出一定的牺牲与权衡，对于急切想了解 DES 细节的读者可以在其他教材中轻易地找到这些知识。

致谢

非常感谢 Sarah Finney、Peter Galea、Kevin Ingersoll 和 Mark Weaver 帮助我完成基于该书的课程。同样感谢国家科学基金对该课程建设的资助，感谢 Michael Yanagisawa 帮助书稿的校对，最后还要感谢 Alice、Bob、Eve 以及其他频繁出现在现代密码学文献中的角色。

目 录

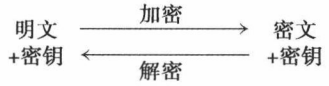
A Cryptography Primer: Secrets and Promises

第1章
A Cryptography Primer: Secrets and Promises

引　论

1.1　加密与解密

我们最熟悉的密码学用途是隐藏一个消息或文档的内容，*密码系统*（cryptosystem）就是能够实现这一功能的系统。它包括两个部分：加密方法和解密方法。未经变换的、可读的消息或文档称为*明文*，经过变换的、一般不可读的形式称为*密文*（密码系统“cryptosystem”在英文中也被称为“cypher”，或者拼写为“cipher”）。



加密（encryption）是将明文转化为密文的过程。加密方法需要两个输入：明文和密钥。类似地，解密方法也需要两个输入：密文和密钥，并输出明文。

在传统的密码系统中，加密和解密使用相同的密钥，这样的系统被称为*对称密钥密码系统*（symmetric-key cryptosystem）。如果 Alice 想要发送一条加密消息给 Bob，双方都必须知道所使用的密钥。（这一点与*公钥密码系统*不同。在一个公钥密码系统中，有两个不同的密钥，一个用于加密，另一个用于解密。我们将在后面讨论公钥密码系统。）如果 Alice 和 Bob 希望他们的通信内容是保密的，就必须保证密钥的秘密性，因为对于任意窃听者而言，如果他知道密钥并截取了密文，就可以确定明文消息。

我们在这里假设每个潜在的窃听者都知道加密和解密的方法，在本书 1.4 节中将要详细讨论这个假设。这个假设在方法论上是现代密码学的基础，我们将这条假设贯穿于全书。简单地讲，*我们总是假设每个潜在的攻击者了解你所使用密码系统的每个细节*。

密码分析（cryptanalysis）是试图攻破密码系统的过程，窃听者采用密码分析的方法来发掘 Alice 发送给 Bob 消息的内容。在 1.6 节中，我们简述窃听者可

能采取的几种不同类型的攻击方法，但是密码分析的细节知识超出了本书讨论的范围。

1.2 信道、安全与不安全

我们常常使用各种不同的通信媒介，如电话网络、无线电波、有线电视网络、计算机局域网、互联网和印刷媒体等。银行通过一个网络将他们的自动取款机连接到中心计算机和另一个网络以实现电子资金转账；寻呼服务使用有线和无线通信的结合；而某些卫星和地球之间的通信则使用微波。我时常使用计算机内存在现在的我和将来的我之间通信；当我使用电话的时候，在我的声音到达听筒之前，声音穿过了空气；而在拨号的行为中，我是与电话系统进行通信。

我们希望将数字安全的概念应用于所有这些通信媒介中，为了达成这一目的，我们从纷繁复杂的差异中抽象出一个单一的、通用的术语——信道。信道是通信双方之间的媒介（我喜欢想象成连接两个铁罐的绳）。

当然，大多数通信媒介允许两方以上的实体间相互通信，然而在大多数情况下，认为信道连接两方在概念上就足够了，因为如果有多方参与的话，我们可以认为存在多条信道。

一个人将一个特定通信媒介（比如电话网络）看作是安全的或者是不安全的是根据他自己的观点而定的。比如说，在通常情况下，我们认为电话网络是相当安全的，然而，每年都有数以百计的政府窃听和监听命令被批准，而每一个命令都会导致平均数千段通话处于被窃听之中。

出于学习密码学的目的，我们将简单地宣称一个信道是安全的或是不安全的。如果存在第三方（窃听者）可以截取（窃听）信道中传输的消息，我们认为该信道是不安全的。在某些情况下，窃听者甚至可能篡改从发送方到接收方的消息。

安全信道是指不会受到窃听与干预的信道。当然，人们更感兴趣的是将密码学应用于不安全信道。幸运的是（或者不幸的是，取决于你怎么看），在我们的现实生活中不安全信道比比皆是。在本小节剩余部分，我们将对三种通信媒介描述某些导致其不安全的特征。这些只是作为例子，毋庸置疑，读者也可以在其他通信媒介中找到不安全的因素，包括本节开头提到的各种通信媒介。

1.2.1　互联网

当今密码学最显而易见的应用都涉及互联网，原因如下。首先，互联网在某种程度上是由计算机组成的，而计算机擅长处理密码学相关任务。其次，互联网是使先前未曾熟识的各方实现自主通信的完美媒介。最后，也是最重要的，互联网的特殊结构使得它需要一套安全防护机制。在互联网中，计算机极少与其他计算机直接相连，当你使用位于罗德岛卧室中的计算机发送一条消息到父母位于加利福尼亚的计算机时，你的这条消息将会经过很多中间计算机，每台中间计算机都会尽力将消息向前转发给更为靠近目的地的另一台计算机，同时存在一套机制检测这条消息是否最终找到正确路线。中间计算机在转发这条消息之前，可能存储这条消息的副本，或者将其篡改后再转发。然而，在系统中没有任何措施阻止它们这么做。一台流氓计算机甚至并不转发这条消息，却返回一条报文显示你的原始消息已经完成了传递。（当然，情况并不像这种描述那样可怕，因为报文的传递路径经常是不可预测的，你的消息通常被分成许多片，每一片会沿着不同的路径被转发，而且，大多数路径上的中间节点计算机可能并非恶意。）

一个更为严峻的情形出现在远程登录中。如果你在加利福尼亚的一台计算机上有一个账户，通过一个叫作“远程登录”（telnet）的程序，你可以在罗德岛的电脑登录这台在加利福尼亚的计算机。当然，加利福尼亚的计算机将向你发送一条消息，要求你输入登录口令。当你提供了口令之后，这条口令会穿过罗德岛与加利福尼亚之间的所有中间计算机。任何一台中间计算机都可以存储你在加利福尼亚这台计算机的地址、你的用户名和你的口令，随后，他们就获得了登录你账户的权限。有证据表明，有数万条用户口令被流氓计算机用这种方式所截获。

由于互联网被广泛用于商业目的，因此面临的威胁日益增加。假设你在做出一个商业决定之前，用网页浏览器获取最新的股票信息，有可能（尽管不都是这样）你的商业对手已经建立了一台计算机来代替他真实的设备，伪造了你正在搜集的股票数据。假设你要下载喜欢的电脑游戏公司的演示程序，有可能一台流氓计算机会截取浏览器发出的请求，并发送给你一个经过篡改的、感染了病毒的版本。最后，假设你正在浏览一个在线书店的网页，网站提供了一个方法以加密你的信用卡号，而你也将信用卡号提供给了这个网站。但是事实

上，你所浏览的网页可能根本就不是这个在线书店，而是在一台流氓计算机上伪造的页面。

1.2.2 局域网

不仅仅像从加利福尼亚到罗德岛这样的远距离通信存在安全隐患，连接你的电脑与服务器（用于存储程序以及提供邮件服务等）的局域网也可能是不安全的，接入网络的流氓计算机可能会侵入你的通信（使用一种被称之为“数据包嗅探器”（packet-sniffer）的软件），甚至注入经过篡改的数据。

1.2.3 移动电话

当然，移动电话利用空中电波进行通信，因而可能被窃听，如美国众议院议长纽特·金里奇在1997年1月发现其电话遭受窃听。不仅通话会遭受窃听威胁，当一个呼叫被发起时，移动电话会传输一个账号用于收费，这同样是危险的。1995年，移动电信业遭受了约四亿五千万美元的诈骗损失[⊖]，其中大部分归咎于手机“克隆”，即犯罪分子截获手机账号，并将这个账号植入另一个手机中，因此便“克隆”了原来的手机。用新的手机打电话，将会被计费到原来的手机。

移动电信业界正在采取措施，通过加入安全特性来防止诈骗。然而，旧的通信标准难以废弃，更进一步地，正如1.3节中将要讨论的那样，引入的安全机制也没有被充分证明。

即使一个用户并不在使用手机，安全威胁依然存在。当一个手机漫游的时候，它将会向系统注册位置变动情况，这些信息的传输可以被截获，并被用来帮助确定这个手机（从而也是其机主）的位置。联邦调查局要求建立标准，强制要求手机能够为警方提供机主的位置信息[⊜]。

1.3 隐匿式安全

考虑以下场景：

- 在第二次世界大战期间，美国军方在太平洋战区雇佣印第安纳瓦霍人来

⊖ 来自：贝尔大西洋公司，http://www.ba.com/nr/95/may/freddie.html。
⊜ 执法中的通信技术支持，参见 http://www.epic.org/ privacy/wiretap。