网络与计算机安全丛书

信息安全
——系统的理论与技术

林代茂　编著

科学出版社
www.sciencep.com

网络与信息安全丛书

信息安全——系统的理论与技术

林代茂　编著

科学出版社
北京

内 容 简 介

作为广义信息理论的一部分，信息安全受到越来越多的关注。本书首先介绍了传统信息论的基本概念和重要定理，然后以系统和运动的观点，对信息安全的含义、性质、模型及处理思路进行了一般性的描述。书中把信息安全分为三种类型，并分别介绍了三类信息安全的相关技术（涉及密码学、信息隐藏及网络安全技术），最后简单地介绍了工作中常被忽视的问题，突出了信息安全是自然科学与社会科学之融合体的观点。

本书可作为信息安全专业研究生或高年级本科生的教学用书，也可供从事相关工作的人员阅读。

图书在版编目(CIP)数据

信息安全——系统的理论与技术/林代茂编著. —北京：科学出版社，2008

（网络与信息安全丛书）

ISBN 978-7-03-021208-5

Ⅰ. 信… Ⅱ. 林… Ⅲ. 信息安全——系统的理论与技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2008)第 031305 号

责任编辑：任 静 王志欣 / 责任校对：陈玉凤

责任印制：刘士平 / 封面设计：耕者工作室

科学出版社出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

新蕾印刷厂印刷

科学出版社发行 各地新华书店经销

*

2008 年 3 月第 一 版 开本：B5(720×1000)

2008 年 3 月第一次印刷 印张：20 1/2

印数：1—3 000 字数：397 000

定价：48.00 元

（如有印装质量问题，我社负责调换〈新欣〉）

前　言

几年前，本人有幸受聘为国际关系学院的客座教授，为信息安全专业的研究生讲授信息理论。这些年来，一直没有找到适用的教材，所以决定自己来编写讲稿。

讲授信息理论不能不提到香农信息论。香农信息论是通信专业的必修课程，原来讲授这门课程要结合通信技术特点，重点讨论编码方法以提高通信效率和准确性，很少谈到信息安全。另一方面，信息安全专业的学生除了应了解计算机网络的安全问题，也需要香农信息理论的指导，因此，把二者结合起来才是对信息理论课程的期望。这种结合是合理的，因为信息理论是一个外延广泛的概念，信息安全本应是信息理论的一部分。

根据作者在研究所多年的工作经验，宏观地思考了信息、信息安全和信息理论的内涵，觉得很有必要对这些内容进行梳理，形成比较系统的观点。只有这样，才能完成伟大的数学家华罗庚所说的“由厚到薄”的过程，只有这样，才有利于学生创造性地学习信息理论。

基于这种思想，本书做了如下的安排。首先在第一章介绍信息理论的发展历史与现状；第二章是信息安全的概述，我们把信息安全的含义进行了分解，分别用 A_1 类、A_2 类和 A_3 类安全表示信息自身安全、信息系统安全和不良信息的影响，于是发展多年的密码学、当前热点的信息隐藏和涉及千家万户的网络安全就不再是孤立的学科，而是存在内在联系的、同属一个范畴的内容。第三章至第九章讨论有关信息安全的各种技术。最后，第十章实践信息安全，是为开拓学生思路和针对人们往往忽视的具体问题而写的，可以当作讨论信息理论的一个回归。

本书可以作为信息安全专业研究生或者高年级本科生的教材，当然根据具体情况也可以略去某些章节，加 * 号的章节为可选章节。如果讲授全书内容，大约需要 80～100 个学时。

可能有些从事信息安全工作的实际工作者没有学过“随机过程”，他们可以略去第二章和第四、五章的部分内容。如果读者已经学过“随机过程”，那么阅读本书就不会有什么障碍了。

最后，感谢同仁段宏先生和白金茹女士，段宏仔细审阅了第六至十章的内容，并提出了不少宝贵意见，白金茹充实了 8.3 节的内容。也感谢我的学生们，他们和我的共同实践帮助我确定了本书的最后成形。

作 者

2007 年 11 月

于北京电子技术应用研究所

目　录

第一章 绪 论

1.1 信息的概念

研究信息及信息安全技术所面临的第一个问题是:什么是信息?

在不同的时代,对于不同的研究对象,人们会定义不同的信息概念。我们可以从文献中查到几十个信息定义,其中最有影响的是由美国科学家香农(Shannon)和语言学家所定义的信息。

香农把问题限定在通信活动之中,因此他所定义的信息概念以通信模型为基础。

从人类原始的思想情感交流方式发展到现代通信技术,经历了漫长的历史过程。但是任何通信过程都符合一个基本的模型,即发送者发出的消息经过传输后被接收者所接收,正如图 1-1 所示。在这个最简单的通信模型中,信源是消息之源,通常指提供消息的人或设备,例如打电话时的说话人、广播节目的电视台等;信道是传递消息的通道,包括电缆、光纤,以及传输电磁波的空间等;而信宿则是指消息的接收者。

图 1-1 最简单的通信模型

信源发出的消息可能是符号、文字、图像或者声音,传送它们需要借助于载体,通过载体的传输完成消息的传递。对于电子通信来说,不可能使用物质载体,只能借助于能量载体,后者以电磁信号的形式完成携带消息的任务。接收者从收到的信号中检测出信源发出的原始消息。如果接收者早已知道这个消息,就失去了这次通信的意义,接收者感兴趣的是收到新消息,收到原来不知道的内容。在这个意义上,我们可以给出信息的一个定义。

定义 1.1 接收到的原来不知道的内容叫做信息。

这样定义的信息概念可以进行度量,它在通信技术发展过程中发挥了重要作用。《辞海》中对信息一词的解释显然受到上述影响:通信系统传输和处理的对象,泛指消息和信号的具体内容和意义,通常需通过处理和分析来提取。信息、物质和能量被称为系统的三大要素。信息的量值与信息的随机性有关,因此在接收

端无法预估消息或者信号中蕴涵的内容或意义，预估的可能性越小，信息量就越大。

然而在网络时代，通信效率和通信速率不再是人们关心的唯一问题，人们常说的信息概念也远远超出了上述定义。另一方面，对定义 1.1 的理解提出了一个问题，即当一个熟记小提琴协奏曲《梁祝》的人再次欣赏那优美乐章时，他是否收到了信息？

依据不同的基准会有不同的答案。如果把信息概念限定在“豆芽”的排列上，则没有收到信息，这反映在香农信息量 $H(X)=0$ 之中（见第二章）；如果把音色、音质，以及演奏者注入的情感这些乐谱无法表征的内容也看作是信息，则答案是肯定的。是啊，否则听音乐（也是一种通信过程）还有什么意义呢？

由于信源发出的消息总是以某种符号表示（文字、图像或者声音都是符号），因此在符号学理论和信息概念之间就有一种不可分割的关系。语言符号学的创始人之一莫里斯把语言分作三个方面：

（1）符号和对象之间的关系叫做符号过程的语义方面，有关研究叫语义学。

（2）符号和解释者之间的关系叫做符号过程的运用方面，有关研究叫语用学。

（3）符号相互之间的形式关系叫做符号过程的语形方面，有关研究叫语形学或句法学。

语用学、语法学和句法学之间的关系如图 1-2 所示。

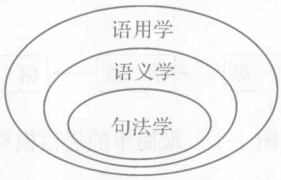

图 1-2　语言符号学的关系

有学者从类似的视角提出了的信息定义。

定义 1.2　消息中表达消息实质内容的部分叫做语义信息。

定义 1.3　消息中说明语义信息表现格式的部分叫做语法信息。

定义 1.4　语法信息和语义信息共同构成消息——本征信息。

这种类似于语言符号学的定义方法自有其积极意义。现代的通信技术中，接收到的消息既包含消息的实质内容，也包含与之有关的语法说明。例如我们传输一幅图像数据时，还必须带有这幅图像的格式，缺少了格式说明，接收端就很难得到应有的画面。似乎这种定义方法更适合网络时代的需求。然而，无论是语义信息、语法信息，还是本征信息，都没有直接指导信息技术的发展，即使在网络充分

普及的今天，也很难看到从符号学的信息定义出发导出的具有理论或实际意义的结果。

在人类社会迈进信息时代的今天，信息已经成为社会生产力的重要组成部分，人们不再只需要用信息理论研究通信问题，在信息的产生、存储、传输和应用过程中，都需要有信息理论的支持；人们也不再只重视传输效率和可靠性问题，许多关于信息的新问题，例如信息的完整性、有用性、安全性、时效性、可鉴别性等在现实的生产、生活中已经不可回避。因此，“什么是信息”这个问题重新摆在我们的面前。

那么，究竟应该如何定义信息才更符合实际需要？这样的信息具有什么性质？我们认为，把香农的信息概念加以泛化既有利于继承前人的贡献，又能适应当代科学发展的需要。

定义 1.5 关于客观事物的概念、属性、相互关联和运动规律的知识，以及客观事物属性的自我显现叫做信息。

这个定义包含两方面的内容：一是思维活动产生的结果，即所谓知识，知识的存储和传输就是信息的存储和传输；二是客观事物属性的自我显现，例如我们观察到蓝天下的田野，这个画面算不上什么知识，却是天空和田野属性的自我显现，观察的过程就是我们通过视觉系统接收信息的过程。关于第二方面的内容可以参考传统信息论创始人之一——维纳(Wiener)的信息定义：信息是人们在适应外部世界和控制外部世界的过程中，同外部世界进行交换内容的名称。

这个定义不强调原来是否知道，可以理解为香农信息论里所说的消息。在因特网上传输的海量信息中，有有用的信息，也有无用的修饰，对于那些无用的修饰，也要可靠地传输，不允许马塞克现象的出现；为提高网络传输效率，人们会采取限失真压缩办法，不一定要剔除消息中语义上的冗余；相互传送邮件时，斟酌字句去除信息冗余的情况也难于遇到。实际传输的比特率是对消息而言。

然而这个定义没有给出信息的定量标准。当我们说信息量的大小时，往往关注实际的比特数。在信息安全成为众所关心的议题时，这样的定义具有实际的意义。

1.2 信息的性质

和信息概念的定义一样，人们总结了许多条信息的性质，它们往往带有不同应用目的的影响，这是无可厚非的。但是，在从应用层面讨论之前，更应该从信息的物理属性方面观察，因为这方面的性质是更本质的东西。

性质 1.1 信息是普遍的客观存在。

按照定义 1.5，即使在人类创立知识以前，信息也已经客观存在。

性质 1.2 信息不守恒，即信息既可以消亡，也可以创生。

大脑的思维活动可以创生新的知识，这些知识属于新的信息内容；独版书籍或者存有某种数据的唯一光盘的销毁意味着有关信息的消亡。

性质 1.3 信息必须依赖于物质或能量而存在，依赖于物质或能量而传输，即不存在离开物质和能量而独立存在的信息，它必须以物质或能量作为载体。

性质 1.4 信息可以复制，从而可以分享。

不像物质和能量那样，信息可以无限复制，不同人可以同时拥有同一份信息。

性质 1.5 对信息的处理不会增加信息的原始内容。

这里所说的处理包括滤波、存储、传输等，滤波处理是对原始信息的修改，存储和传输是对信息的转移，在此过程中增加的所有内容都不是原始的信息。例如从 BMP 图像转换成 JPG 图像(可以归为滤波处理)，且不说图像细节的丢失，JPG 格式的语法说明就不是原来的内容；模糊图像处理的结果本来就含在原来的信息之中；接收端收到的信息不可能多于信源发出的信息，而且只有在接收灵敏度和感觉灵敏度都达到一定水平时，二者才可能相等。

信息的物理性质反映了信息的本质特征，决定了达到某种应用目标的可能性。

从应用角度阐述的信息性质决定了信息技术的发展方向。

从信息安全的角度看，人们关心的是信息的安全性、完整性、有用性、时效性、可鉴别性等。秘密信息的保密、音像产品的非法复制牵涉到信息的安全性问题，网络路由的复杂性决定了能否保证信息的完整性，信息的真实和时效意义是信息有用性的体现，保密性、真实性和不可抵赖是可鉴别性的动因，等等。

有些书上为信息归纳了十几条性质，其中有些基于香农的信息定义，有些从应用层面考虑，例如：①新颖性。接收者收到信息之前，对其内容是不知道的，所以信息是新知识、新内容。②有益性。信息是能使认识某一事物的未知性或不确定性减少的有用知识。③可测性。信息是可度量的，信息量的大小有差别。④相对性。不同的接收者所得到的信息量不同。⑤可加工性。信息可以产生、消失、携带、存储和处理。⑥转移性。信息可以在时间上或在空间中从一点转移到另一点。⑦变换性。信息是可变换的，它可以由不同的载体和不同的方法来载荷。⑧有序性。信息可以用来消除系统的不定性，增加系统的有序性。⑨动态性。一切活的信息都随时间而变化，因此信息也是有时效、有寿命的。

这些甚至更多的性质，对信息安全的研究实际意义不大，倒是还有些更加深入的内容值得我们思考，例如用不同的语气讲同样的话表示不同的意思，“言外之意”、“字里行间”等都反映了信息的复杂性质。为了避免这些深层次因素的影响，我们不打算用包罗万象的概念来讨论信息，只局限在消息的层面上讨论问题。

1.3 信息理论的发展

信息理论是信息科学的基础，强调用数学语言描述信息科学中的共性问题和解决方案。到目前为止，信息理论一直处在发展之中，新的研究成果可能仅局限于某个应用领域，也有可能具有广泛的意义。有人把信息理论划分为狭义信息论、一般信息论和广义信息论三个层次，以说明其涵盖范围的不同。

狭义信息论又称香农信息论，主要总结了香农的研究成果，在信息可度量的基础上，研究如何有效、可靠地传递信息，重点是各种编码技术。它是通信问题的理论提升。

香农分别于 1948 年和 1949 年发表了两篇著名文章：*The Mathematical Theory of Communication* 和 *Communication in the Presence of Noise*。这两篇文章讨论了信息的度量、特征、传输速率、信道容量以及干扰的影响等问题，用概率测度和数理统计方法系统地阐述了通信的基本问题，奠定了信息科学的基础，对通信技术的发展做出了重大贡献。尽管在此之前，奈奎斯特(Nyquist)已于 1924 年解释了信号带宽和信息率间的关系，但是其影响远不如香农这两篇文章的作用。

一般信息论除了香农对信息科学的贡献以外，还包括其他人的研究成果，特别是美国科学家维纳的微弱信号检测理论。他在与香农的同一时期出版了两本名著：*Extrapolation, Interpolation and Smoothing of Stationary Time Series* 和 *Control Theory*，讨论微弱信号的检测问题，形成信息理论的另一个分支。

信号检测可以分为确知信号检测和具有随机参量的信号检测，重点研究如何从干扰中提取信息。一般信息论的研究包括噪声理论、信号的滤波与预测、统计检测与估计理论、调制理论、信号处理与设计理论等，它是广义通信问题的理论提升。

香农和维纳的研究成果为通信和控制理论与技术的发展做出了开创性的贡献，可以名副其实地称为信息理论的创始人。但是由于通信技术对人类的影响更大，信息科学的理论成果与通信技术联系更多，所以人们倾向于把香农叫做信息论的创始人。

现代信息科学涉及范围非常广泛，除了传统的感测技术、通信技术、控制技术、智能技术等以外，还涉及经济学、心理学、语言学、社会学等其他领域，特别是近年来发展迅猛的信息安全技术，显然也应该属于信息科学的范畴，摈弃信息安全的信息理论是不完整的信息理论。信息安全问题是自然科学和社会科学的融合体，广义信息理论不仅要讨论客观问题，也要涉及人的主观因素，不仅要研究自然科学问题，也要研究与之关联的社会科学问题。广义信息论的研究需要更一般