# 信息安全的系统观

林代茂

（北京电子技术应用研究所，北京 100091）

[摘要] 给出了信息安全的三层涵义，指出信息安全学科是自然科学与社会科学的融合体。从社会工程角度给出系统的概念，从部件、接缝、人员、环境四方面探讨了系统与信息安全的关系，提出了信息安全设计的必要步骤，并以通信系统为例分析了影响信息安全的因素。

[关键词] 信息安全；安全系数；信息隐藏；接缝；威胁

[中图分类号] X913.4 [文献标识码] A [文章编号] 1009－1742(2007)08－0021－05

尽管信息安全术语在最近十几年才成为热门话题，但是信息安全的内容却早已进入人们的生活，密码技术、扩频通信、保密规定、甚至重要部门的门卫制度，都是影响信息安全的内容。不可否认，网络技术的发展大大促进了信息及信息安全技术的发展，并且形成了比较完整的体系，成为当前研究信息安全问题的主流。然而，计算机网络和其他应用场合的信息安全问题既有共性也有区别。笔者试图从系统的观点来审视信息安全的共性问题。

## 1 信息安全的涵义

多年来，人们一直在使用信息安全这个术语，却未必深究其涵义[1－3]。因此在谈论信息安全问题时，往往受到研究领域的限制而有一定的局限性。

信息安全的概念应该包含如下3层涵义：

信息自身的安全。诸如信息的保密性、完整性、可信性、可用性等，这不仅需要密码技术、信息隐藏技术、网络技术的支持，也需要管理与策略的维护。

信息系统的安全。信息从其产生到运用要经历存储、传输和处理等过程，这些过程的载体构成了信息系统。计算机网络是信息系统，程控机床是信息系统，重要文件的保管、传阅等也是信息系统。在考虑信息安全问题时，人们往往更多地关注计算机网络，而对其他信息系统重视不足，例如，对新诺卫星的干扰就是设计时没有从信息安全的角度充分考虑的结果。

某些信息的传播对社会的不良影响。不仅仅是因特网，其他信息系统也存在着同样的问题，例如广播系统、通信系统等。当然这也可以被看作是信息安全的反面问题，但是对从事信息安全工作的人们来说，其正、反两方面都是不可忽视的。

三个层次的划分是因为它们虽然都属信息安全问题，但是研究的内容和目的不同，要求的技术手段和措施不同。

根据对信息安全概念的理解，信息安全问题不仅是计算机网络必须面临和认真对待的问题，也是其他任何产生信息、存储信息、传播信息和运用信息的部门所共同面临的问题。在其他领域，人们积累了许多维护（或破坏）信息安全的方法与经验，成为早期网络安全工作者的有效借鉴。例如防火墙的概念就起源于保密部门的围墙与警卫。然而信息时代的情况更加复杂，仅仅沿用过去的思维已经不足以应付关于信息安全的挑战。

信息安全的问题涉及管理、策略和技术3个方面，和过去任一学科都不相同，它是自然科学与社会科学的融合体。这种融合是进入信息时代的一个重要特征。

[收稿日期] 2006－08－02；修回日期 2006－11－10

[作者简介] 林代茂（1945－），男，山东蓬莱市人，北京电子技术应用研究所研究员

## 2 系统的概念

由于上述原因，必须以系统的观点看待信息安全。这里所说的系统是传统系统概念的扩展，需要把自然科学与社会科学融合在一起加以考虑。

一般地说，系统是由若干部件、接缝和有关人员组成的，其中一些部件又由下一级的部件和接缝组成。这里的部件包括硬件设备、软件包；接缝是指所有部件的连接部分，包括软件、硬件的接口，包括人机界面，同时也包括系统与外部环境的交界；而有关人员主要指与系统运行法定有关的人员。

图1是上述系统概念的示意图，其中所有箭头处都表示接缝的存在，而图1中各部件的连接方式只是一个例子，实际上可能更复杂或更简单。

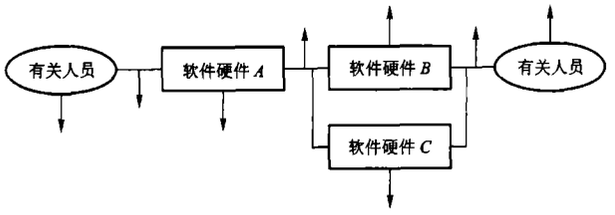


**图1 系统概念示意图**

**Fig. 1 Sketch of system concept**

虽然按照这样的定义有时会把问题复杂化，但是由于全面地考虑了所有的相关因素，将会避免许多信息安全事件的发生。如果习惯地把有关人员和接缝排除在外，许多信息安全事件的原因将被忽视。

例如，移动通信的发展为人们的工作和生活带来极大的方便。通常，人们会把基站、用户终端和配套软件看成是完整的系统，因为它们的正常工作就能维持移动通信系统的运转。当考虑信息安全时问题并不是这样简单：虽然移动通信在正常进行，$A_1$，$A_3$ 类安全问题却照样可以发生。所以，应该按照上述的观点来构造系统，把有关人员也算作系统的一部分，并充分考虑系统中各部分的接缝。

在图2的示意图中，基站设备可能出现故障 $c$ 或遭到破坏 $j$、手机可能损坏 $b$ 或被窃取 $h$、通信人可能利用手机进行危害社会的活动 $a$、合法的通信内容可能被窃听 $i$，$j$，$k$、基站维护人员可能散布非法内容 $d$ 或者利用职务之便破坏信息安全 $l$、图谋不轨者可能设置虚假基站 $e$ 干扰或破坏正常通信 $m$ 等。

对于上述风险需要采取不同的对策，其中有技术支持，也有管理方法，任何一方面的偏废都可能导致难以估量的后果。例如，为了防止被恶意利用，国

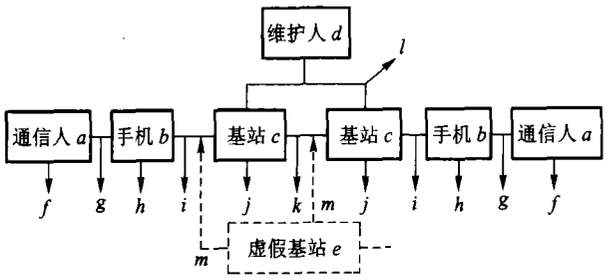


**图2 移动通信系统**

**Fig. 2 Mobile telephone system**

外在手机的销售和上网时采取了严格的登记制度，而我国却可以随意购买和联网，给不法分子创造了方便条件，使信息安全 $A_3$ 遇到了挑战，显然这是管理不到位的结果。

通过这个例子可以看到，上述信息系统的概念是有用的，它帮助人们对信息系统做出更加全面的分析，有目的地采取必要措施，防止信息安全事件的发生。

## 3 系统与信息安全

依据上述的系统概念，可以把产生信息安全问题的原因归结为4个方面：

1）*部件的可靠性* 它包括硬件故障、软件缺陷，此类问题可能导致系统瘫痪；

2）*接缝带来的风险* 接缝是外部干扰或攻击的窗口，也是不良信息的入口；

3）*有关人员的作用* 他们的忠诚度决定其是否是外部攻击的内应，其技术水平和防范能力决定其是否会成为系统崩溃的导火索；

4）*系统的物理环境* 它决定系统能否正常工作。

### 3.1 部件影响

各个部件以某种结构形式连接在一起，共同决定着信息系统的安全。

硬件故障和软件缺陷可能造成系统不能正常工作，甚至可能导致系统的瘫痪。可以说，硬件和软件的可靠性是影响 $A_1$ 和 $A_2$ 安全的常在因素。对于这类问题，主要靠严把质量关和经常性检查与及时修补来解决。

为了评价一个信息系统的安全程度，把系统正常工作而不发生安全问题的概率称为安全系数 $S$，则 $S$ 的定义域为[0，1]。相应地，也可以定义部件的安全系数。

为简单起见，首先假设系统中部件之间互不影响，任何一个部件的故障都将使系统安全遭到破坏，那么，无论这些部件是怎样连接的，整个系统的安全

系数都可以表示为

$$S = 1 - \sum_{K=0}^{N} \left[ \prod_{k=0}^{K} (1 - S_{ik}) \prod_{k=K+1}^{N} S_{ik} \right] = \prod_{i} S_i \tag{1}$$

其中 $S_{ik}$ 是第 $ik$ 个部件的安全系数，$N$ 是系统所含部件的个数，$K$ 是出故障的部件数。

实际上某些部件可能是相互影响的，即一旦部件 $A$ 出现问题将导致其他部件（例如 $B$）的损坏，也就是说在 $A$ 损坏的条件下 $B$ 损坏的条件概率为 1，即 $P(B/A) = 1$。直观的感觉是这将降低整个系统的安全系数，通过下面的分析，事实并非如此。设有一个信息系统具有 3 个部件，各部件的安全系数分别为 0.9，0.8，0.85，计算系统的安全系数：

| 部件状况 | 系统安全系数 |
|---|---|
| $A$ 安全、$B$ 安全、$C$ 安全 | $0.9 \times 0.8 \times 0.85 = 0.612$， |
| $A$ 安全、$B$ 安全、$C$ 故障 | $0.9 \times 0.8 \times 0.15 = 0.108$， |
| $A$ 安全、$B$ 故障、$C$ 安全 | $0.9 \times 0.2 \times 0.85 = 0.153$， |
| $A$ 安全、$B$ 故障、$C$ 故障 | $0.9 \times 0.2 \times 0.15 = 0.027$， |
| $A$ 故障、$B$ 安全、$C$ 安全 | $0.1 \times 0 \times 0.85 = 0$， |
| $A$ 故障、$B$ 安全、$C$ 故障 | $0.1 \times 0 \times 0.15 = 0$， |
| $A$ 故障、$B$ 故障、$C$ 安全 | $0.1 \times 1.0 \times 0.85 = 0.085$， |
| $A$ 故障、$B$ 故障、$C$ 故障 | $0.1 \times 1.0 \times 0.15 = 0.015$。 |

上面列出了所有可能的情况下系统的安全系数，只有第一行才对应系统安全工作的情况，即该系统的安全系数是 0.612。可以看到，尽管部件 $B$ 的安全系数已经变为

$$S'_B = 1 - \{ S_A(1 - S_B) + (1 - S_A)P(B|A) \} = S_A S_B = 0.72,$$

系统的安全系数却仍然可以利用式（1）来计算。这个结果是可以理解的，因为对信息系统的安全评估是在系统正常工作情况下所作的，不能附加部件 $A$ 已损坏的前提。

实际问题更加复杂。首先，部件之间的相互影响虽然不改变系统的安全系数，却严重地影响安全事件所造成的损失。显然，如果由于部件 $A$ 的故障引起部件 $B$ 的损坏，则只修复 $A$ 而不修复 $B$，系统仍不能正常工作。

其次，某些部件对系统安全的影响可以忽略，另一些部件对系统安全却至关重要。例如一个通信系统的软件发生了小问题，虽然致使通信时间略有延误，但不影响通信的完成也不影响保密，而加密程序的损坏却可能使信息完全失去保密性。这说明不同部件对信息安全的权重不同。

为了考虑到安全权重的作用，对式（1）的计算结果作适当修改（由于部件的安全系数 $S_i$ 本身就是一个估计值，没有必要给出调整量的精确值）：如果最高权重部件的安全系数低于部件的平均安全系数，可以认为系统的安全系数比式（1）的结果更小，如果最高权重部件的安全系数高于部件的平均安全系数，可以认为系统的安全系数比式（1）的结果更大。

第三，对于有备份的容错系统，如果修复时间小于 2 次故障的间歇时间，则部件问题并不会影响整个系统的安全。

鉴于以上原因，部件对系统安全的影响主要考虑可靠性。实际上，对一个系统品质的评估包括性能、实现成本、安全、风险、恢复成本等诸多方面，不能期望用安全系数做全面的表征。

### 3.2 接缝影响

封闭系统消除了遭受外部攻击的可能性。如果没有部件问题（$A_2 = 0$），系统将是安全的（$A_1 = 0$，$A_3 = 0$）。

但是实际上并不存在封闭的系统。任何实际系统都与外部世界相联系，几乎所有的接缝都是对外开放的。接缝是系统受到外部干扰或攻击的窗口，也是不良信息的出入口，因此它将直接影响 $A_1$，$A_2$ 和 $A_3$ 安全。尽管不存在完全的封闭系统，但是在可能条件下减少系统的开放程度却是有用的，所谓的“对外保密”就是出于这种思想。

对于实际的也是开放的系统，接缝对信息安全的影响不宜用安全系数一类的指标衡量。有效的方法是考虑每个接缝可能受到哪些威胁，每种威胁的发生概率，一旦发生将产生的后果，然后权衡安全投入与风险损失，并做出善后的预案。

全面考虑可能受到的威胁并不困难，给出每种威胁的概率却是艰难的事情。对于同一种威胁，不同的评估专家可能会有不同看法，很难得到一致的结论。因此，要么采取多数原则综合专家组的意见，要么依赖于决策者的判断。

由于某些威胁确属小概率事件，几乎不可能发生，即使发生也不会造成致命的伤害，在安全投入远大于可能损失的情况下，对其不以为然是明智的。然而，对某些小概率事件却不得不给以足够的重视，因为它所产生的后果是极其严重的。例如银行数据库遭受攻击属于小概率事件，但是一旦被攻击的后果是难以估量的，这时应该不惜维护安全的成本。

一个不能忽视的问题是对计算机网络的攻击，包括篡改网页、施放病毒等等。注意到几乎所有这

些攻击都在利用系统软件的缺陷,同时也都来自于系统接缝,因此需要从部件与接缝两方面进行考虑(防火墙隔离与软件补钉等措施)。

### 3.3 人员影响

人员问题相当复杂,是引起 $A_1$, $A_2$ 和 $A_3$ 三类信息安全问题的重要因素,甚至可能成为至关重要的因素,要么是造成信息安全事件的导火索,要么成为维护信息安全的英雄。

对于信息系统的维护和使用人员来说,缺乏防范意识会忽视外部攻击的进程,防范能力不足会给攻击者更多成功的机会,有意或无意泄露的一些数据,则会成为信息系统遭受攻击的利器。从而带来较大的安全隐患,像鲍勃和艾丽丝那样进行隐蔽通信的人员[4],则可能将自己送上法庭。

另一方面,信息系统可能遭受硬件或环境破坏、软件入侵等攻击,像温迪那样的检察人员还会采取监视等其他方法。无论哪一种攻击方法,只要信息系统存在隐患,就有被彻底颠覆的可能。

人员的作用充分显示出社会科学对信息安全的重大影响。有人在研究人与信息系统的关系的基础上,建立了所谓的"社会工程学",一些网迷在互传通过欺骗手段获取敏感数据的方法。社会科学与自然科学相互融合的研究工作已经提到有社会责任感的人们的研究日程。

为了消除不利影响,必须加强管理工作。管理者要从上述的系统观点着眼,全面考虑各方面的影响,采取合法有力的策略,通过制定必要的法规和采取先进的技术措施,杜绝信息安全事件的发生。

### 3.4 外部环境影响

外部环境主要指能否保证信息系统正常运行的条件,例如水电供应、温度湿度环境、震动等级、天灾人祸、电磁辐射干扰等。为此,有时准备了备份供电系统或者 UPS 电源,有时采用空调以至净化系统,加装防静电地板,屏蔽系统,甚至采取一定的防震措施。然而在许多部门,人们并不是在分析以后才做出决策,因而造成资金的浪费。例如,在地震频发地区不能不考虑震动影响,在相对稳定的地理环境中为此做出的投入将是极大的浪费。

有些因素看起来关系不大,一旦出现问题也会极大地影响信息安全,诸如交通阻断、资金短缺等。

## 4 实现信息安全的系统思考

根据功能需要设计系统、根据安全目标完善系统是构建信息系统的必要步骤。假设有一个信息系统已经完成功能设计,现在要对其采取安全措施以实现信息安全,应该按照系统的观点(图 3),分别考虑部件、接缝、人员和环境 4 个方面。很明显,这牵涉到管理、策略、技术 3 个方面,其中一些考虑需要有技术背景但却非技术性工作。如果管理人员把信息安全的责任全部放在技术人员身上,不在管理方面做实质性的工作,则必然存在安全隐患。

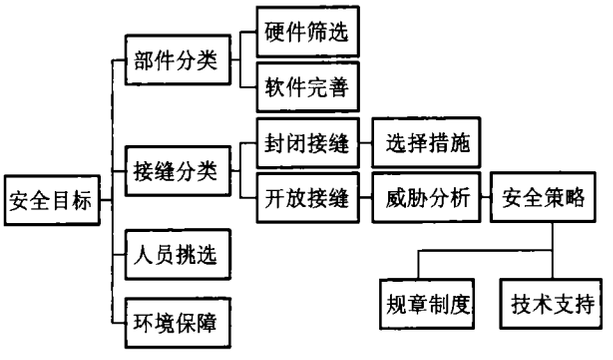


**图 3 信息安全设计步骤**

**Fig. 3 Design process of information safety**

另一方面,由于信息安全问题往往表现为攻守双方的对抗,而各方的策略和技术又在不断发展,所以信息安全是一个动态概念。如果维护信息安全的策略和技术停滞不前,安全程度将随着攻击能力的增强而下降,如果没有新的攻击方法,安全程度将随着防护手段的提高而提高。

## 5 通信中的信息安全举例

为了进一步阐述上述观点,以通信中的信息安全问题为例加以说明。

可以把通信过程分为公开通信、保密通信和隐蔽通信三种情况。所谓公开通信泛指通信内容可以公开,不担心被截获、窃听的通信方式;保密通信指通过加密操作,使截获者不能了解通信内容的通信方式;隐蔽通信指通过技术或非技术手段,使第三者不能发现或证实通信在秘密进行的通信方式。

公开通信的信息安全问题,主要表现在保证相关人员的忠诚尽职、信息系统的正常运行、防止从系统接缝侵入的干扰和破坏。保密通信的信息安全问题,则除了要保证相关人员的忠诚尽职、信息系统的正常运行、防止从系统接缝的侵入(窃取密码本或密钥等)以外,还要保证加密强度。以下仅以隐蔽通信为例,对信息安全做一较为详细的分析。

在信息隐藏技术领域,几乎没有人不知道著名的监狱问题[4]:鲍勃和艾丽丝要进行隐蔽通信,而他们

的通信内容必须经过狱警温迪的检查，所以他们采用信息隐藏技术以蒙蔽温迪。鲍勃、艾丽丝和信件构成系统的部件，他们书写、阅读的过程形成了两个接缝，而温迪的检查是该系统的第三个接缝，因此这个系统由三个部件和三个接缝组成。信息安全事件可能发生在任一部件和接缝之中：鲍勃和艾丽丝可能已经出卖对方，信息隐藏的信件可能出现破绽，书写和阅读过程可能被别人发现，温迪可能掌握相当高的发现秘密的水平，等等。如果只注重信息隐藏技术而忽视了其他问题，这个信息系统必然是不安全的。

一般地说，隐蔽通信既要保证信息的畅通，又要防止通信内容被他人得知，同时还要隐蔽通信者的身份。在隐蔽通信中，信息自身的安全和信息系统的安全是等价的（$A_1 \Leftrightarrow A_2$），即如果温迪发现了隐藏的信息，鲍勃和艾丽丝必将受到惩罚；如果二人之一向温迪透露了真情则隐藏的信息也将暴露无疑。

假设鲍勃和艾丽丝不掌握信息隐藏技术，他们同样可以进行隐蔽通信：秘密进行无线保密通信或使用扩频技术、利用放风时间将信息放在约定地点等，只要温迪不能发现他们的通信设备、没有发现藏密地点、没有检测到他们发射的信号，或者即使检测到通信信号却不能确定系鲍勃或艾丽丝所为，隐蔽通信都可以安全进行。用上述系统观点的话来说，即要充分考虑部件（设备可靠工作）、接缝（设备和通信过程的隐蔽）、人员（不自我暴露）和环境条件（电源等）。总之，无论从鲍勃通信系统的信息安全还是从温迪的信息检测来看，都是技术与策略的结合。

## 6 结论

信息安全的重要性在信息时代尤为突出，它不仅需要自然科学所能提供的思想方法和技术支撑，也需要人们在社会科学中的管理经验，信息安全科学是自然科学与社会科学相互融合的社会工程。

解决实际的信息安全问题应该具有系统的观点，全面分析面临的安全威胁，根据应用需要确定安全目标，找到正确对策，利用相关技术并制定必要措施。笔者从系统的观点对信息安全进行了初步探讨，以具体实例证明解决信息安全问题是一个社会工程。

**参考文献**


[1] 吴世忠，陈晓华，李鹤田，等. 信息安全测评认证——理论与实践[M]. 北京：中国科学技术大学出版社，北京：中电电子出版社，2006

[2] Schneier B. Secrets and Lies: Security in a Networked World [M]. 吴世忠，马 芳译，北京：机械工业出版社，2001

[3] 杨义先，钮心忻. 网络安全理论与技术[M]. 北京：人民邮电出版社，2003

[4] 汪小帆，戴跃伟，茅耀斌. 信息隐藏技术——方法与应用[M]. 北京：机械工业出版社，2001. 35～37


# The System Standpoint on Information Safety


Lin Daimao

(*Beijing Institute of Electronic Technology Application, Beijing 100091, China*)



[**Abstract**] The meanings in three layers on information safety are given. It is proposed that all management, strategy and technology are necessary to implement information safety, because the science of information safety is the merger of natural and social sciences. The concept of information system which includes elements, boundary, working condition and relevant people is proposed. The relation between the system and information safety is analyzed, and an example about information safety in communication is given. The procedure of safety designing is suggested.



[**Key words**] information safety; security factor; information hiding; boundary; threat