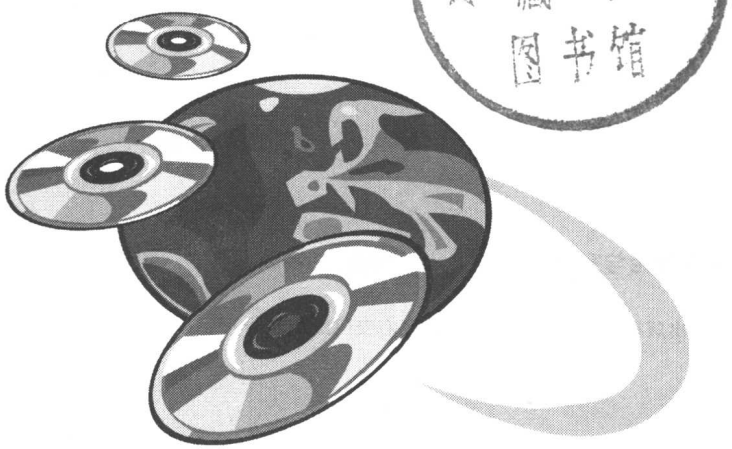
信息安全理论与实务

陈彦学　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE
文魁資訊股份有限公司

信息安全理论与实务

陈彦学 编著



中国铁道出版社
2001年·北京

（京）新登字 063 号

北京市版权局著作权合同登记号：01-2001-0458 号

版 权 声 明

图书在版编目（CIP）数据

信息安全理论与实务/陈彦学编著. —北京：中国铁道出版社，2001.3

ISBN 7-113-04093-4

Ⅰ.信… Ⅱ.陈… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2001)第 08002 号

书　　名：信息安全理论与实务
作　　者：陈彦学
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街 8 号）
策划编辑：严晓舟
特邀编辑：朱　静
封面设计：冯龙彬
印　　刷：北京市兴顺印刷厂
开　　本：787×1092　1/16　印张：16.5　字数：393 千
版　　本：2001 年 4 月第 1 版　　2001 年 4 月第 1 次印刷
印　　数：1～5000 册
书　　号：ISBN 7-113-04093-4/TP·521
定　　价：28.00 元

出版说明

在电子商务高速发展的今天，信息安全领域已倍受重视。本书会让你在最短的时间内获得信息安全领域中的一些专业知识。书中详细介绍了密码学的基本知识，及一些市面上常见的安全协议、标准内容，如：PKCS、SSL、X.509、LDAP 等。

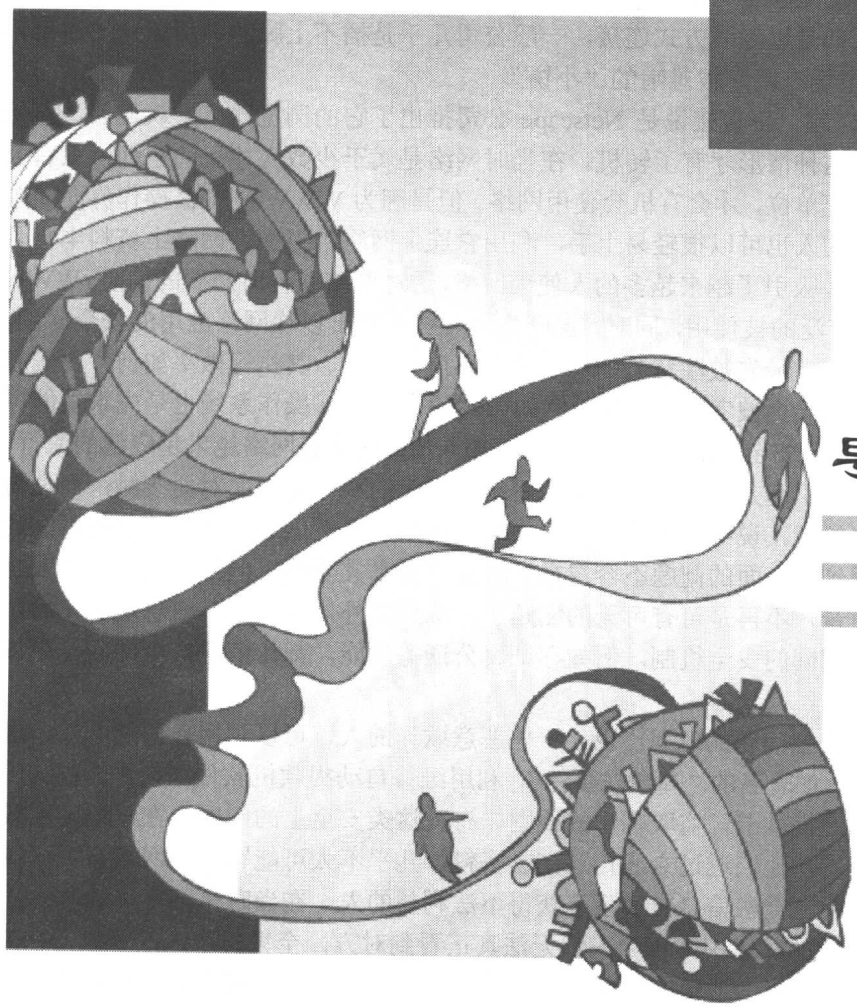
本书由台湾文魁资讯股份有限公司提供版权，经中国铁道出版社计算机图书项目中心审选，庄洪林、陈贤淑、廖康良、孟丽花、马婷儿、黄小红、安心、刘艺等同志完成了本书的整稿工作。

中国铁道出版社

2001 年 4 月

目 录

1



导论

几年前，若是提到与信息安全相关的工作，往往会被联想到的可能你是军方人员，甚至联想到你是谍报员。因为早期信息安全的主要用途就是用在军方或是外交方面，从事在这方面工作的人，往往蒙上了一层神秘的色彩。记得自己当年刚出来找工作，投履历时提到在研究所是做信息安全方面的研究，几乎没人愿意雇用，因为没有需求，更甚者有一位初认识的朋友以为我是当警卫的。因为在当时民间的应用，除了金融界以外，根本不会很重视这方面的应用。当时唯一的认证中心(CA, Certification Authority)，是通关中心建立的，以目前的眼光看起来是很简陋的，但是在当时是个创举。即使在金融界的应用方面，信息安全几乎都是特定厂商的天下，而且都是以专线方式连接，一般公司几乎是插不上脚的，所以这“饼”不仅不是“大饼”，而是市场有限，很难啃的“小饼”。

但是自从 WWW 兴起，更直接说是 Netscape 公司推出了它的浏览器广受欢迎后，直接推动了因特网的流行，这种情形才有了转机。在当时网络是属于少数人才玩的东西，只有大专院校学生或是少数研究单位，才会有机会使用网络。但是因为 WWW 浏览器操作界面简单易学，即使不会计算机的人也可以很轻易上手，利用它连上网络，再加上网络上资料丰富且迅速、网页内容多采多姿，吸引了越来越多的人使用网络，透过网络获得所想要的信息。WWW 的兴起，使网络越来越广泛的被使用，同时，也产生出一些不同于以往网络应用的安全问题。

在一般计算机系统中，最先被注意到的问题是可不可以执行、其执行效率如何，而信息安全是计算机应用中最后一个被考虑的问题，例如微软的 windows 操作系统也是先求功能可以运行，再考虑效率，至于安全功能也是 NT 之后才加入的。而随着网络越来越广泛的流行，信息安全的问题才渐渐地引起人们的重视。因为网络上通信的双方无法面对面接触，而使得信息安全的问题渐渐地显现，说明白点就是很多人利用网络的特性做违法的事，获得不法的利益，让一般民众了解到这方面的问题不容忽视，虽然有点幸灾乐祸，但是也让吃信息安全饭的人有更大的说话声音，不再是可有可无的配角了。除此之外，在文件、信息电子化后，如何建立起与传统社会相同的安全机制，例如存证、公证等功能，都让信息安全的问题更加被重视。

由于以往对于信息安全问题的忽视，也让一些恶意欺诈的人，可以利用人们的无知，进行欺骗获取不法的利益。如著名的“郑金龙事件”，利用维修自动提款机软件之便，偷取的用户密码及相关资料，伪造提款卡，盗取客户的钱财。有关这类安全上的问题，在早期确实较不受重视，以金融界而言，他们透过专线传递交易资料，几乎不太可能有所谓网络窃听、重送的安全问题，可能运用这金融信息交换系统获得不法利益的人，在当时是寥寥可数。

但是在目前网络发达的环境中，每个人都无法真正看到对方，全凭每个人的识别码(ID)来识别通信的对象，对于网络上通信的对象几乎无法做很明确的认证，这个优点在于个人的隐私权可以受到充分的保护，但缺点就在于无法很明确的认证通信对方，导致很多人滥用这特性从事一些不法、欺骗的事。

本书的内容就是介绍这些网络上的安全问题，业界针对这些问题所提出的一些解决方案，以及一些其它的相关知识及概念。

1.1 什么叫信息安全

信息安全不单单是指密码学及计算机的部分，它所包含的范围比你所知道的概念更广、更繁杂。以一个组织或公司为例，在工作上所定的各种作业规范都应可以包括在其中，如机密文件不得让没权限的人看到，或是机密文件携出公司，必须经过一定的审核程序、抽查员工是否有依照标准行事、密码不得写在明显的地方、甚至机器的放置地点是否有考虑到防止天然灾害、是否有定期备份等作业规范都在此范围之内。

在本书中后面内容中，基本上不着重于这类安全规范的制定，并不是这安全规范不重要，事实上大部分的安全问题并不是出在对计算机或网络的攻击，而是在内部管理上有瑕疵，让有心人士有可乘之机，前面所提的“郑金龙事件”就是一个最著名的例子。然而，这些安全规范必须因应各个组织、企业的特性不同而有所差别，基本上例如军事单位、一般政府机关、外交单位、高科技单位和传统产业，其着重要点必然是不相同，但是其根本精神是一样的，在本节中将简略地提出制定安全规范的重点。密码学大师 Shamir 在 1995 年国际密码学会议(Crypto'95)中，对于商业安全有十项建议，很值得参考。

1. 不要追求完美无缺的安全性。

没有绝对的安全，只有相对的安全。信息安全不是要做到滴水不漏的完美，而是根据系统的特性订出系统所需的安全度，否则太多的不合现实的限制，只会导致工作人员更多的反弹。

而真正合适的规范，是必须先评估自己所能承担的风险，将攻击的系统的成本提高到让想破解的人都认为不合乎成本，就不愿意花功夫去攻击你的系统，也就是“赔钱的生意没人做”的意思。

举例而言，军方及外交的资料当然是很机密的，在系统设计之时会想办法将攻击的成本尽量提高，甚至会用拉专线，不准使用一般的登录环境等比较繁杂的方式来规划系统，以减少被攻击的机会。而跨国大企业，若想利用因特网安全地传输公司内部信息，就会考虑使用 VPN 的方式，以保护数据传输的安全。至于一般的公司行号，可能就是使用 SSL 传资料，安全上虽不如 VPN 的强，但就成本及风险考虑上，也绰绰有余了。

2. 不要误以为问题解决了，但根本的问题仍然存在。

这个考虑很明显的，但是很容易受到种种因素影响，而未能真正实行，包括时间、主管的专业技能及其工作心态等，有时这点是很难做到的。

例如，早期著名的郑金龙利用职务之便，盗取金融卡的资料，并自己制作金融卡偷取客户的存款。这问题的根本不单是个人遵守的问题，而在于并未确实执行文件存取的规范，让程序设计师有权限阅读到他不该看的资料，这才是其根本的原因。若只是针对郑金龙个人处罚，就以为可以杀鸡儆猴，让以后的人不敢再做此事，无疑是缘木求鱼，还是会有人去作这种低风险高获利的事，简单的说就是“杀头的生意有人做”。若是根本的问题未解决，这种低风险，高获利的事一定会有人再继续做的。所以遇到问题，必须了解问题的原因所在，从根本来解决，而不是只处理目前的状况，就以为天下太平了。

3. 不要使用由下而上的策略解决问题。

在计算机系统中加入信息安全，所伴随的就是对使用者限制，造成一些不方便，若是让使用者由下往上地提出建议，当然是什么都不要限制最好。所以安全政策，必须是由上往下地推动，明白组织内需要的是什么之后，再大力推动。例如一般建议使用者的密码最好定期更换，而且每次的密码应该不一样，这样当然对于使用者造成很大的不便，若因应使用者的要求，密码永久有效，密码被有心人攻击的机会就大增，因为攻击者有很充裕的时间可以来破你的密码。

4. 不要过分地使用密码技术，反而造成使用者的不方便。

当计算机系统加入信息安全的技术时，必然会造成使用者许多的不便，就好像当你用惯了个人计算机，一旦使用工作站，居然要输入密码，有些文件还不能去存取，在使用习惯上一开始都不是很能适应。当然，加入更多的密码技术，会造成一些不便。但是换个观点来看，若是使用者界面做得不错，将使用者的不适应的感觉降低，适度地使用密码技术，未尝不是一件好事。

什么是适量运用，这就是取决于工作性质的特点，若是安全需求高的地点，如军方、外交单位，就会大量使用密码技术，可能每一次打个电话出去都需输入密码，或是插入一把钥匙，当然就会造成使用不便，但在一般学校单位，使用相同的设备，就未免太小题大作了。

这一点可以算是第三点的注意事项，不要为了建立一个超过你所需安全的环境，而牺牲掉使用者的便利，反而是得不偿失。

密码技术的提升，意味着另一层意义，攻击者虽然在这一点无法攻破，但是它们往往会从另一点攻击系统，在美国曾发生收集对手公司的垃圾，从这些丢弃的纸屑中，都会透露出这家公司的一些重要的信息。也就是说，安全必须是全面的考虑，不要只考虑密码技术的提升，却忽略了其它容易被攻击的漏洞。

5. 不要使用太复杂的方法。

简单的技术，不一定是代表不安全，复杂的技术不一定代表安全，反而可能产生新的漏洞，在学术上有很多这种例子。RSA 密码系统是一个很简单又实用的密码系统，加密与解密都是一条公式就解决了。一般相信它的安全度与分解因子困难问题是相当的，一堆人想要破它，但到目前为止，事实上并无人可以从根本破解 RSA 算法，只要加长密钥的长度，目前的破解法都还是无法有效的破解它。曾经有人提出一密码系统，宣称建立在分解因子及解离散对数的困难问题上，这想法很好，架在两种困难问题上安全度会比较好，但是后来被证明这方法根本未建立在这两个困难问题上，只是一个多项式时间可解的问题。

由上面的例子可以看出，往往太复杂的技术，可能伴随的是更多的漏洞，反而将系统导入更危险的地步。

6. 不要使用太昂贵的设备。

信息安全不是光靠设备、技术就可以安全无虞的，而且还得靠人员的配合。譬如，美国

国防部对于将密码贴在计算机上的人一律解雇。因为这是一种很坏的习惯，再贵的系统，只要你一干这种事，就大门尽开，攻击者不费吹灰之力，就可进入系统。

对于组织内信息安全制度的建立，往往比购买设备、考虑技术还重要。只要其中一个人心存不轨，或是不小心泄漏机密，往往会让一个花了很多心力系统的安全毁于一旦。

7. 不要使用单一防线策略。

这点的用意就很明显的，安全必须有配套的作法，不是只使用单一防线就可以防止的。就像工作站上，有密码认证的机制后，对于文件就必须有存取的控制。在敏感的系统上必须有相对的审计制度，以备有攻击迹象时，可以适时检测出来，或是事后可以找出入侵的轨迹。重要的机器如凭证管理中心签发凭证的机器，要放在有实体保护的地方，最好不要直接连上网络。甚至对于敏感、重要的资料，还得做最坏的打算，将资料定期备份，若发生攻击或是破坏事件时，可以将大部分的资料恢复过来，让损失减至最轻微。

8. 不要忽略了可能发生的“神秘攻击法”。

这点就很难防止了，当然身为系统管理者，对于一些信息安全的信息，必须时时去了解，别已经是在网络上传了半天的漏洞，系统公司或是网络上都出补丁了，居然变成你所管理系统的神秘攻击法。台湾地区政府机关网站曾经遭到过攻击，一般认为并不是很高级的技术，可能是那个家伙拿到一个攻击的软件，就找出一些可能有相关漏洞的网站一个一个去试，所以攻克了一些网站。一般若是在 CERT(网址为 http://www.cert.org/,在台湾地区也有一个 CERT 的网站在 http://www.cert.org.tw/)被公布的弱点，很快会在相关公司或组织网站获得补丁的软件，一切就看系统管理者用不用功了。

当然，应该重视审计的重要性，当你发现有奇怪的迹象时，应该追查其原因，不该把奇怪的现象当作是常态，很可能这奇怪的现象就是一个神秘攻击法。

9. 不要太过于依赖系统操作。

大多数的资料毁损，并不是由攻击者所造成的，而是使用者不慎使用，对资料做不正确的处理而导致的。相信每个玩计算机的人都有这样惨痛的经验，一不小心，辛苦一天的成果就完蛋了。所以玩计算机一阵子的人，都会有不断存盘的习惯，至少存盘前的东西还可以保持住，让受损减到最低。

这样的问题很难解决，不能完全信任系统的运作会很正常，决不会出错，减少损失方法很简单，就是定期备份，在系统不慎毁损的时候，还可以挽回大多数的资料，将损失减到最低。更严谨的系统可能还得备份多份，对于备份存放地的实体安全也得多加考虑。

另外就是对天灾的考虑，水灾、火灾、地震等天然灾害都是不可预期的，但对于资料的损毁都是毁灭性的，所以定期备份才可以减低资料损毁的损失，将损失降到最低。

10. 不要太过于依赖人员忠实。

这点就不用在多做解释了，一个组织中，人绝对是最难控制、管理的部分。根据统计大部分的计算机犯罪都是由内部的人所为的。所以对于比较敏感工作，不要完全相信他的忠诚，

放心让某一个人去执行，不如由制度面来管制，才是比较正常的作法。

至于该怎么做，这就不是本书的重点，可以推荐一本很好的参考书，O'REILLY 出的 Computer Crime(计算机犯罪)，作者以切身的工作经验，对于防止计算机犯罪的要点，做了很精辟的描述，很值得从事信息安全系统规划的工作人员参考。有关系统安全部分的问题，就在此打住了，有兴趣的读者，可以参考此书，相信一定可以给你更多的启示。

1.2 网络与信息安全

网络的广泛应用，可以说是今日信息安全应用的重要推动者，以台湾地区为例，在台湾地区“教育部”建造出第一条因特网，“学术网络(TANet)”之后，台湾地区正式加入了因特网的大家族中，大专院校众多的学生是最早的受益者，但此时的应用仍停留在系统安全及密码保护的阶段，并未真正地使用很多信息安全的技术来保护网络传输的资料。

而随着 WWW 的兴起，其浏览器界面简单及内容多样化的特性，让一般民众可以很容易使用网络，成为网络的使用者。随着因特网的进展，新的应用及商机不断的出现，诸如利用网络做电子商务、电子文件交换、以及信件传递等，让一般民众也可以享受网络的方便的特性。

网络兴起对于整个社会产生极大的影响，在正面的意义上它提供了便利、迅速的信息流通，但相对的在负面上也衍生出许多以前传统社会未有的问题。目前，在网络上几乎无法可管，电子化的资料在网络上流通，只要有一些特殊设备或软件，可以随意截取上面的信息，更甚者可以伪冒他人、传送错误的信息。由于这些网络安全问题，使得一些应用无法直接顺利推动，所以必须利用信息安全技术加以保护，以确保资料流通的信息安全。

因为因特网变得不是当初 ARPANET 时代简单的应用，而是有一堆不可控制的使用者在上面的媒体，这些人的行为无法控制，就像一颗颗不定时的炸弹，而网络信息流通快的特性，各种软件随处都是，有些软件可以根据系统的漏洞来攻击。只要有心去寻找，可以让一个计算机功力不高的人，轻松地成为破坏高手。所以每个使用者都可看作是一个个随时会爆炸的不定时炸弹。那么若要在网络上面推动一些应用，除了要考虑可行性的问题之外了，还必须考虑到种种信息安全问题，确保一般人甚至功力高的计算机高手，都不容易破解，造成危害。

应该做到何种程度的安全

所谓安全没有绝对的，只有相对的。所谓“相对的”意义在于安全不是要做到毫无缝隙、滴水不漏，而是让攻击者觉得攻击此系统的代价，远比他能获得的利益高，这样的话绝大部分的攻击者就不愿意做这种事。例如，Alice 要传一份机密资料给 Bob，最保险的做法就是自己亲自送，但是这样作的成本太高，而透过网络加密传送，若是采用 DES 加密，此信息可能被拦截下来，以目前的技术而言要破解已不是那么困难，那你就得评估你的加密成本与你的损失之间，取得平衡点。若只是一般的情书，又有何不可，这机密文件是 Alice 与 Bob 之间的机密，但是对别人来说，即使感兴趣，除非是钱太多的变态情敌或是外遇事件，一般人绝

不太可能花那么大的成本去破解这封情书。

一般而言，所谓安全要做到什么地步，是根据使用者所能接受的成本及攻击者可能获得最大利益的平衡点。以目前网络上常见的安全协议，SET(Secure Electronic Transaction)而言：SET 是让信用卡的持卡者可以在网络上做安全的信用卡交易，但是对于持卡者的保护却不是很周到。持卡者在这个协议中，若以严格的安全的观点来看几乎是很弱势，在整个交易结束后，并未获得任何已进行交易的证据，是一个纯以银行的观点设计的协议。或许是银行它有完整的审计制度，并且若有这类官司发生有损其声誉，一般除了银行内部的个人行为外，银行不太可能会发生这种欺诈行为。

所以当设计一套安全的应用系统时，并不是要做到滴水不漏，而是看系统的需求及应用范围，及其所能承受的风险，而来定义出此系统所需的功能，及需达到的功能。例如，前一阵子炒得很热的国民卡，若是真正执行时，因为是事关全体国民的身份资料，其系统设计的安全程度当然是必须很高，必须自安全规范到密码组件的实体安全，一直到软件程序代码的检查，做到很完备。但若只是一试验性质的系统，当然就不一定事事都有如此严格的标准把关，先以可行性为重点，对于安全可以只考虑较基本的安全问题，有些问题如密码组件实体安全部分，可以待试办完毕，后续的系统维护时再考虑这些问题。

如何达到安全的目标

首先必须了解你机器所在地点可能发生什么样的意外，最常见的意外灾害莫过于火灾，则设计之初就必须注重消防设备是否齐全、是否为防火材料、更严谨一点还必须看重要机器附近是否有特别的消防措施，这些很琐碎的问题都必须依据你的系统安全需求来评估考虑。当然还有水灾、风灾、地震等天然灾害必须考虑，虽然这些灾害的出现的频率不如火灾多，而且有些可以事先防范，但是只要稍有不慎，还是很容易引起不可弥补的损失，在建立之初若有余力，不妨也着力在这些方面。

有一项很无奈且好笑的报告，造成资料损毁近 50%~60%的原因居然是内部员工操作时不慎、疏忽所造成的，不过也是很符合现况。我个人经验而言，我所管理的 LINUX 机器，已经重装了好几次操作系统，有一次就是因为操作不慎，误删文件而造成不正常，改不回来之后，放弃之后、一气之下重装比较快。相信各位也有相同的经验，你文件中病毒的次数，绝没有自己错误动作的删除文件的机率大。对于这种状况，似乎防范再多、再好的系统，都无法杜绝这种错误的发生，唯有加强员工在职的训练，令员工时时互相规范、交换工作心得减少已知错误再犯的机会，应该可以减少这种问题的发生。

人员造成损失的其它原因还有，员工蓄意欺骗，前面那个郑金龙事件就是一例，1995 年的“国票事件”案，也是一例。这些都是员工刻意欺瞒，造成组织的金钱及名誉的损失。这样问题其实都是有迹可寻，以金融界为例，其作业流程制定得都是很明确，若是凡事按照这样步骤执行，根本不太可能发生所谓的“国票事件”，但是因为人员不足或是工作赶时间等原因，常会让某些人有特权，跳过这些标准作业程序直接处理事务，当这种事一多，久了甚至成为常态，那弊端就会由此而生。解决的方法必须多管齐下，例如主管不要长期授权给某个员工，做超越他职务的工作，尽量依照标准作业程序来执行业务。定期或不定期地审计业务，

让有心的员工不敢招摇，随意尝试，甚至在审计的过程中还可以找出若干弊端，进而制止一场灾难。

还有一类人也常造成组织的损失，就是心怀怨恨的员工，跟老板吵架之后心里不爽，暴力一点的直接 Format 硬盘，删除所有资料，或是离职前在系统中埋一颗定时炸弹，等离职后过一阵子爆发毁坏系统，这种行径也是很难证明与他有关，更狠的放一只“特洛伊木马”，将原公司的机密资料一点一点搬到新公司。凡此种种不胜枚举，这种状况似乎很难防止，或许作老板的人该谨慎行事一点，逼急了人，是可能会做出一些不理性的事。而除了个人修养及领导风格之外，审计也是一个很重要的工作。在审计的过程中，应有机制可以了解机器中的程序是否有异常的动作，或是否多了异常的文件，那些执行文件有被动过、或是文件加大了，这些工作都是很繁杂且无聊的，但是还是应该被认真考虑，才可以早期发现早期治疗，防止损失的发生。

另外外部人员所产生的危害反倒比较没那么严重，目前的网络技术多可以很有效将这种问题控制在相当的程度之下。这些入侵方式比较常见的就是网络黑客(Hacker)的入侵，之所以有名就是他的效果很明显，前一阵的两岸网络攻防战，还有 1998 年印尼排华期间，中尼两国间的攻防战，都是很有名的案例。说真的，这些大多破坏一些防范不高的网站，说穿了就是让你破坏了都无所谓的网站，真正的资料倒未听说遭毁损，防火墙内的机器，倒没听说有被攻击的，当然啦，搞不好被攻击了放了只“木马”，还未被发现而已，只是目前未听说有什么损失而已。一般相信，真正的黑客，应该盗也有道，不应该随便就破坏人家的网站，搞这些的大多是找到几个软件，可以攻击某些机器，就洋洋得意随意攻击人家机器。不过防止此种攻击最佳的办法，还是找专业的厂商，他们将会提供完整的解决方案，防止这些问题，不是在这边三言两语可以说出道理来的，而且此部分内容属于很专业的技术，并非我专长还是不要班门弄斧，说错就丢脸了。

还有一种外部的攻击，就是如计算机病毒(Virus)及网虫(Worms)的恶意软件，这个大家就很熟悉了，玩计算机的人没中过几次病毒，似乎不可能的。其实，他的防止方法每个人都知道，但是做到的很少。装装防毒软件，定期更新病毒码，不要随便开莫名其妙的信，不要随便下载不明来路的游戏软件。反正，都是些老生常谈的话，每个人都知道，但是大部分的人都没有彻底做到。

最后，网络之间通信应该采用安全的通信协议及密码技术，说真的，这些技术倒不是最重要的关键，但是表现在网络使用者之前的就是这些东西。相信大部分的人都听过 SSL 或是 SET 等安全协议，但是很少人知道这些提供消费的网站内部安全控管执行得如何。基本上，安全的协议及密码技术是建立在前面所述的基本要项的基础上，使用安全协议及密码技术，以提供安全的网络上的服务，这样才可以赚到消费者的钱啦，也就是本书要说的重点，以下内容就是针对安全技术的要点略加说明。

1.3 安全系统的基本概念

讲到信息安全，最先联想到就是密码学，密码学不是新的学问，而是一门非常古老的学问，自古以来只要有人类，就有密码学，甚至你常常见到。简单的加密方法你也常见，例如

我以前常在不懂闽南语的外省朋友面前讲闽南语，骗他出丑，其实客家话对我而言就是一种加密了。稍微复杂的，就是将音变一变，在《天龙八部》小说中“慕容家”的方法就是一例。最复杂的方法，是以近代密码学加密技术加密信息，都属于密码学应用范围。以下就密码学中一些基本的概念，做一简单阐述。

对称密钥系统

因为近代的计算机技术大幅进步，古代简单的密码学技术已不足以应付应用计算机技术的攻击，所以近代发展的密码算法都与计算机技术的发展息息相关。以最常见的对称密钥加密技术 DES 而言，到目前为止并无任何攻击法可以彻底的破解它，而 DES 之所以会被认为不安全，都是因为是 DES 的密钥长度仅 56 位，而且计算机的软硬件技术进步神速，导致密钥太短很容易遭到暴力搜寻法的攻击，目前的破解速度已经过以往的几万年进步到几个小时内就可以破解。为了解决密钥长度太短的问题，而有所谓的 Triple-DES 的方法，重复做三次 DES 运算，将密钥的长度由 56 为原加长至 112 位或是 168 位；或有所谓 DESX 的方式将密钥长度加至 184 位。

在 1997 年，美国国家标准局(NIST, National Institute Standards And Technology)公开对世界征求可以取代 DES 的下一代密码标准，即所谓的 AES(Advanced Encryption Standard)(虽然这是国外的事，但是目前台湾地区凡事都是以美国马首是瞻，还是得小心听他说话，看他的眼色。)他征求 AES 的标准中，有一点是与 DES 不同的，即对称密钥的长度是可变动的，很明显可以看出目前如 DES 等比较强的密码算法，虽然并无很严重的安全漏洞，但是密钥长度是最可能被攻击的弱点。所以密钥长度可变动，一来可以容易延长密码算法的生命，一来可以让厂商出口合乎美国密码产品出口限制的产品。

NIST 自 1997 年公开征求 AES 以来目前共有 15 个算法投稿，在 1999 年 8 月份中，选出了 5 个候选算法，分别是 IBM 所提的 MARS、RSA 公司所提的 RC6、比利时 Joan Daemen 及 Vincent Rijmen 两位所提的 Rijndael，分属英国、以色列及挪威三国的 Ross Anderson、 Eli Biham 及 Lars Knudsen 所提的 Serpent 还有美国的 Bruce Schneier、 John Kelsey、 Doug Whiting、 David Wagner 、Chris Hall 及 Niels Ferguson,所提出的 Twofish。美国 NIST 已于 2000 年选出 Rijndael 算法，做为取代 DES 的下一代密码算法 AES。

公开密钥系统

相对于对称密钥系统的的公开密钥系统，因为美国政府并未介入为其制订标准，所以一直是百花争鸣的局面，各种新的算法不断的推出。公开密钥系统与对称密钥系统不同，公开密钥都是基于某些数学上的难解的困难问题，如分解因子、解离散对数或是迷袋问题等还无多项式时间解的困难问题上发展出来。目前在于学术领域上讨论的算法虽然很多，但基本上不脱离两个算法的范畴，一个就是最为业界所知道的 RSA 算法，另一个是 ElGamal 算法，更精确的说，是建立在两个困难问题上，分别是 RSA 的解分解因子问题及 ElGamal 的解离散对数问题(基于迷袋问题的算法，有其先天的弱点存在，几乎都是不安全的)。当然这只能

说是目前的主流，现阶段仍是有其它的算法在发展，如椭圆曲线，IEEE 在 P.1363 标准中已将椭圆曲线纳入。

公开密钥密码系统的作用有两种：第一种是传统上用来加密的用途；另一种就是目前很热门的数字签名。数字签名可以如同目前手签章或是印章的功能，用以证明数字文件的是已经某人认证过。当然，不论加密或是数字签名，都必须配合相当的体系才可以完成，也就是在后面会提到的公开密钥体系(PKI, Public Key Infrastructure)。

常见的密码系统

在目前的密码算法中，在公开密钥方面已由 Rivest、Shamir 及 Adleman 三位密码学先进所提的 RSA 的公开密钥系统及数字签名系统，最广为一般业界所使用。另外，近代公开密钥密码学的开山鼻祖 Diffie 及 Hellman，在其论文提出了公开密钥及数字签名的观念，在密码学中有其划时代的意义，但是在论文中并未能提出一个实际的公开密钥系统，不过在其论文中提出一个密钥交换系统，即一般所谓的 Diffie-Hellman 密钥交换安全协议，以证明其公开密钥的观念可行，此密钥交换协议也被很多厂商及安全标准所选用。另外，在密码学中另一位著名的人物 ElGamal，在其论文中提出不同于 RSA 的公开密钥系统及数字签名系统，在学术领域中由其所衍生的论文不输于 RSA 算法，但因为他没去开公司，所以在业界并未很受重视，但是一般认为美国的国家数字签名标准 DSA 是其变型，不过他后来去了 Netscape 公司，领导了一个团队，创造了著名的安全协议 SSL，也是在业界受到相当的重视，目前在台湾地区提到网络上的安全协议，就会令人直觉想到是 SSL。目前 SSL V3.0 已为 IETF 所接受，为 RFC 2246 的 TLS(Transport Layer Security)。

在对称密钥的算法方面，当然 DES 是最受重视的了，连今天我们所使用的自动提款机，都是采用 DES 作加密的，但是因为长度太短，DES 几乎遭到完全的破解，美国政府也已在征求下一代的对称密钥算法，前面提过，美国政府于 2000 年也选择了 Rijndael，作为新一代的加密标准。

在对称密钥系统中，除了前面所提的 DES 是属于区块式加密(Block Cipher)的算法，另外还有一类称之为串流式(Stream Cipher)，此类算法是由一种子(Seed)输入一虚拟随机数产生器(Pseudo Random Number Generator)，产生一系列的比特流(Bit Stream)，将此比特流与传输的信息做一简单的运算，如异或(XOR)，加密送出，此类算法目前有使用在个人通信设备的加解密。最有名的当然是手机中用的 A3、A8、A5 啦!另外军方及外交上也是常用此类算法加密。

密码模块

由算法再往上层发展，就是所谓的密码模块了，密码模块当然以硬件来做最佳，因为若是以软件来实现，碰到的第一个问题就是密钥要如何保管，若只是以密码加密密钥放在软盘上(就是后面会提到的 PKCS#5 所提出的方法)，不是一个万全之策，很容易遭到暴力搜寻法破解。若是能以一安全的密码模块来完成这些事情，会是一个比较好的解决方式。当然所谓