国外计算机科学经典教材

THOMSON

Principles of Information Security

Second Edition

信息安全原理

(第2版)

(美) Michael E. Whitman 著
Herbert J. Mattord
齐立博 译

清华大学出版社

国外计算机科学经典教材

信息安全原理
(第2版)

(美) Michael E. Whitman 著
Herbert J. Mattord
齐立博 译

清华大学出版社
北 京

Michael E.Whitman，Herbert J. Mattord

Principles of Information Security，Second Edition

EISBN:0-619-21625-5

981-265-417-8

北京市版权局著作权合同登记号　图字：01-2005-3984

图书在版编目(CIP)数据

信息安全原理(第 2 版)/(美)威特曼(Whitman,M.E.)，(美)马特德(Mattord,H.J.) 著；齐立博 译. —北京：清华大学出版社，2006.3

书名原文：Principles of Information Security，Second Edition

(国外计算机科学经典教材)

ISBN 7-302-12493-0

Ⅰ.信… Ⅱ.①威… ②马… ③齐… Ⅲ.信息系统－安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2006)第 006652 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：曹　康
文稿编辑：于　平
封面设计：孔祥丰
版式设计：孔祥丰
印 刷 者：北京市清华园胶印厂
装 订 者：三河市李旗庄少明装订厂
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：27.75　**字数**：710 千字
版　　次：2006 年 3 月第 1 版　2006 年 3 月第1 次印刷
书　　号：ISBN 7-302-12493-0/TP・8011
印　　数：1～4000
定　　价：49.90 元

前　言

全球网络使世界各地的信息系统之间的互连变得越来越广泛，顺畅的通信和计算解决方案因而也变得更加重要，但诸如病毒、蠕虫攻击以及各种犯罪攻击事件的频繁出现，说明当前的信息技术十分薄弱，需要加强对这些系统的安全保护。

目前，各种机构对保护重要信息资产的需求正在不断增长。为了保护已有的系统和网络，企业必须招收一定数量的信息安全专业人员。企业还期望具有丰富经验和技巧的下一代专业人士能开发出更加安全的计算环境，参与和管理肯定会出现的、复杂的信息安全问题。为此，技术类的学生需要在大学教师的指导下，学习更高深的内容以及相关的技术材料，认识已有系统中存在的漏洞和薄弱部分，学习设计并开发将来所需的安全系统。

本书是一本阐述信息安全原理的优秀教材。目前有许多面向从业人员的、关于信息安全和保障的优秀出版物，但缺乏一本针对学生的、均衡地介绍安全管理和安全技术的教材。我们希望创作一本专门面向信息安全专业学生的教材来填补此空白。本书还解决了如何把信息安全作为一门学科来学习的问题。在开拓信息安全领域的过程中，人们发现，其他学科的学生和从业人员也需要学习本课程，例如信息系统、犯罪立法、政治学、会计信息系统等。这些领域未来的从业人员必须理解信息安全的基本原理，因为安全问题很可能影响他们的行业。因此，本书的基本原则为：现代机构内的信息安全是一个需要管理层来解决的问题，而不是仅通过技术就可解决的问题。换言之，机构的信息安全具有重要的经济效益，并对管理效果产生一定的影响。

0.1　方法

本书全面介绍了信息安全的整个领域，其中包括许多相关元素的背景，以及理解该领域所需的足够细节。本书包含了该学科的术语、简史，并概述了信息安全计划的管理模式。

下面是本书研究信息安全的一些特点：

信息系统安全专业人员资格认证的公共知识体系——因为本书作者是经过认证的信息系统安全专业人员(CISSP)，CISSP 的知识对本书的设计有一定的影响。虽然本书尽量避免成为一本 CISSP 学习指南类的书，但作者的背景导致了本书在介绍信息安全的知识时，在某种程度上结合了许多 CISSP 公共知识体系(CBK)。

章首场景——每章的开头都是一个小故事，讲述一个虚拟公司遇到某类现实世界常见的信息安全问题。每一章的最后都会简要复述这个小故事，并提出一些问题，让学生和老师讨论故事内容所隐含的根本问题。

相关资料和技术细节部分——这部分内容穿插在整本书中，重点讲述一些有趣的主题和详细的技术问题，让学生更深入地了解各种信息安全主题。

强化学习——在每章结尾提供了该章的小结、复习题和练习。这些内容便于学生在课堂外复习信息安全的内容。这些练习要求学生研究、分析和记录问题的答案，以巩固学习目标，并加深对本章内容的理解。

第2版中的改动—— 第2版更流畅地论述了安全系统开发生命周期，并大大加强了有关安全技术的章节。另外，还修改了下述内容：

- 把技术控制的内容扩展为三章，其中包含防火墙、VPN(虚拟专用网)、入侵检测系统、密码系统、漏洞检测工具等。
- 把风险管理列为单独的一章，提供了解决该问题的一种更简明的方法，它是信息安全领域的核心。
- 把规划(包括安全计划蓝图、一般规划)、事故响应、灾难恢复和业务持续性计划合并为单独的一章，论述了这些复杂而相互关联的主题。

一般情况下，第2版的这些变化会使全书的内容更有条理，满足以信息安全学科为基础的课程的一般要求。这些变化还更新了许多主题的陈旧内容，确保本书的内容足以应对信息安全中各种不同的要素。

0.2 作者团队

本书由Michael Whitman和Herbert Mattord联合创作，结合了本研究领域内的理论知识以及商界的实际经验。

Michael Whitman博士，是经过认证的信息系统安全专业人员，是乔治亚州Kennesaw州立大学计算机科学和信息系统系的教授，他还是该大学信息系统专业的硕士生导师，以及信息安全教育的KSU中心(infosec.Kennesaw.edu)的导师。Whitman博士的主要研究领域有信息安全、公平可靠地使用策略、计算道德准则和信息系统研究方法等。目前他讲授信息安全、局域网和数据通信等大学课程和研究生课程。他还在其领域的顶级刊物“Information Systems Research”、“Communications of the ACM”、“Information and Management”、“Journal of International Business Studies”和“Journal of Computer Information Systems”等发表了一些文章。他是信息系统安全学会、计算机安全研究所、防火墙委员会、计算机学会和信息系统学会的成员，Whitman博士还与他人合著了*Management of Information Security*、*Readings and Cases in the Management of Information Security*和*The Hands-On Information Security Lab Manual*，这些图书都由Course Technology出版社出版。在Whitman博士开始其学术生涯之前，他是一名美军的装甲骑兵队军官。

Herbert Mattord是工商管理学硕士和CISSP。他曾经做过应用程序开发人员、数据库管理员、项目经理和信息安全专业人员。他在结束了24年的IT职业生涯之后，于2002年进入Kennesaw州立大学。Mattord教授是信息安全教育的KSU中心(infosec.Kennesaw.edu)的业务经理、信息安全与推广中心内的计算机科学与信息系统认证KSU部门的协调员。在IT从业期间，他已经是Kennesaw州立大学、乔治亚州玛丽埃塔市Southern Polytechnic州立大学、得克萨斯州奥斯丁市Austin Community大学以及得克萨斯州圣马科斯市Southwest Texas州立大学的副教授。目前他讲授信息安全、数据通信、局域网、数据库技术、项目管理、系统分析和设计以及信息资源管理与策略等课程。他曾是Georgia-Pacific公司信息技术安全联合部的经理。本书包含了他的诸多实践知识。Mattord教授还与其他人合著了*Management of Information Security*、*Readings and Cases in the Management of Information Security*和*The Hands-On Information Security Lab Manual*，这些图书都由Course Technology出版社出版。

0.3 本书结构

本书的结构遵循一种称为安全系统软件开发生命周期(或 SecSDLC)的模式。这个结构化方法可用于在几乎没有正式信息安全措施的企业中实现信息安全，也可以帮助改进已有的信息安全计划。SecSDLC 提供了坚实的基础架构，非常类似于在应用程序开发、软件工程、传统的系统分析与设计以及联网工程中使用的架构。本书使用这个结构化方法，提供了一条不超越主题的主线，此主线可指导教师和学生对信息安全领域的各个方面进行详细研究。为此，将本书分为 7 个部分、12 章。

第 I 部分——简介

第 1 章——信息安全简介

开篇章节讲述了理解信息安全各领域的基础内容。本部分定义关键术语，解释基本概念，并概述此领域的起源。

第 II 部分—— 安全调研阶段

第 2 章—— 安全需求

本章介绍商界对信息安全越来越感兴趣的原因。本章介绍了现代企业在信息安全领域的需求，强调并构建了第 1 章介绍的概念。一个原理性概念是：信息安全主要是一个管理问题，而不是技术问题。换言之，信息安全领域中的最佳实践过程是在考虑了商务需求后，才应用具体的技术。

本章还介绍了企业面临的各种威胁，并给出对这些威胁进行分级的过程，以便在企业开始进行安全计划时利用相应的优先级。本章继续讲解上述威胁可能导致的各种攻击，以及它们对机构的信息系统产生的影响。本章结束部分进一步讨论了信息安全的重要原理，其中一些在第 1 章已经介绍过，如机密性、完整性、可用性、身份验证和标识、授权、责任和私密性。

第 3 章——信息安全中的法律、道德以及专业人员问题

除了 SecSDLC 调研过程的基本部分之外，本章对国家和国际条款中的现有法律、规章和公共道德进行了详细介绍，深刻阐述了商业交往中所遵循的规范。本章介绍了信息安全领域的几个重要法律，并详细描述了实现安全的人员必须遵守的计算机道德。不懂法律不是借口，但忽视法律(懂法但不守法)更危险。本章也介绍了现今企业中经常出现的几个法律和道德问题，以及可提升道德和法律责任的正规专业机构。

第 III 部分——安全分析

第 4 章——风险管理

在开始设计一个新的信息安全方案前，信息安全分析人员必须首先要理解企业的当前状况以及它和信息安全的关系。企业目前有正规的信息安全机制吗？它们的效率如何？企业给安全管理人员和终端用户发布了什么策略和过程？本章描述了标识威胁和资产，并评定其优先级的过程，以及标识当前可用于保护这些资产免受威胁的控制措施的过程，进而介绍了实施基本的信息安全评估的方式。本章还讨论了各种可利用的控制机制类型，并指明进行最初风险评估所涉及的步骤。本章把风险管理定义为识别、评估风险，并将其降低至可接受的程度、实现有效的控制措施以维持此风险级别的过程。最后讨论了风险分析和各种可行性分析。

第 IV 部分——逻辑设计

第 5 章——安全的规划

本章给出了许多被广泛接受的安全模型和基础框架，还介绍了最佳商务实践方案以及合理注意、谨慎处理的标准，并扼要介绍了安全策略的开发。本章详细描述了安全策略每一层次的主要组成内容、范围和目标对象，还解释了军队和私人的数据分类模式以及安全教育培训和意识(SETA)计划。本章论述了支持业务持续、灾难恢复和事故响应的规划过程，描述了在发生事故时机构的作用，以及机构需要外部法律执行部门的时机。

第 V 部分——物理设计

本部分的内容为信息系统专业的学生介绍信息安全领域中使用的技术控制。如果读者不熟悉联网技术和 TCP/IP 协议，可能会觉得第 6、7 和 8 章的内容比较难理解。如果读者不具备网络协议的基础知识，在学习本部分的内容之前，应先学习联网教材中有关 TCP/IP 协议的一两章内容。

第 6 章——安全技术：防火墙和 VPN

本章详细论述了如何配置和使用把企业和不安全的 Internet 隔离开来的技术。本章包含防火墙技术的许多定义和分类，以及可以部署防火墙的体系结构。接着讨论了与防火墙的正确配置和使用相关的规则。本章还阐述了远程拨号服务，以及为仍使用这种旧式技术的企业保护该访问点所必须的安全预防措施。之后介绍了过滤内容的能力和注意事项。最后讨论了通过虚拟专用网为授权用户提供远程访问权的技术。

第 7 章——安全技术：入侵检测、访问控制和其他安全工具

本章继续讨论安全技术，介绍入侵的概念，防止、检测、响应入侵和恢复到入侵前的状态的技术。阐述了入侵检测系统(IDS)的特定类型：主机 IDS、网络 IDS 和应用 IDS 及相应的配置和用法。本章继续论述专门的检测技术，将攻击者诱入诱骗系统(因而远离重要的系统)，或简单地把攻击者的入口指向这些诱骗的区域，这些区域称为蜜罐、蜜网或填充单元系统。本章还介绍跟踪系统，跟踪被诱入诱骗系统的攻击者的真实地址。之后详细论述重要的安全工具，信息安全专家可以使用这些工具检查企业系统的当前状态，标识出系统中已有的潜在薄弱区域或企业的整体安全态势中存在的潜在薄弱区域。最后讨论现代操作系统中广泛部署的访问控制设备，以及生物测定学中的新技术，对已有的实现方案提供强有力的身份验证。

第 8 章——密码学

本章详细介绍了现代密码系统的基础知识、体系结构和实现方案。本章首先概述了现代密码系统的历史，在该历史中有重要作用的各种密码，还论述了组成密码系统的一些数学技术，包括散列函数。接着，比较传统的对称加密系统和现代的非对称加密系统，非对称系统是公共密钥加密系统的基础。然后，本章概述在安全通信中使用的、基于加密技术的协议，包括 SHTTP、SMIME、SET、SSH 和其他几个协议。之后讨论隐写术，这是一个新兴的技术，是隐藏信息的一种有效方式。最后讨论信息安全中专门针对加密系统的攻击。

第 9 章——物理安全

物理安全是信息安全过程中的一个重要环节，关注的是物理设施的管理，物理访问控制的实现以及环境控制的监督。本章讲解了现代企业在面对各种物理安全威胁时应特别注意的事项：设计一个安全的数据中心，评估警卫和看门狗的相对价值，分析火灾抑制和电力调节的技术问题等。

第 VI 部分——实现方案

第 10 章——实现安全

前面的章节介绍了企业设计信息安全计划的规则，本章介绍实现该设计所需的重要元素。本章主要实现了信息安全的靶心模型，讨论了企业是否应外购信息安全计划中的各种组件。此外，还讨论了变动的管理，程序的改进和业务持续性工作的额外计划等内容。

第 11 章——安全和人员

实现阶段的下一领域解决的是人员问题。本章介绍了人员的两个方面：安全人员和人员的安全。具体内容有：人员问题、专业人员安全证书以及雇佣政策的实现和实践。本章还讨论了信息安全政策与顾问、临时工和外部商务伙伴之间影响和被影响的方式。

第 VII 部分——维护和改进

第 12 章——信息安全维护

最后也是最重要的一部分是对维护和改进的讨论。本章介绍了对信息安全计划的实时技术性和管理性评估，企业必须执行该信息安全计划，才能维护其信息系统的安全。本章介绍了实时风险分析、风险评估和度量，这些都将保证风险管理计划的效率。最后考虑了用于建立和管理漏洞分析和渗透测试的实践。

0.4 教师资源

为支持本书内容，我们准备了许多教学工具，它们在多方面增强了课堂教学内容。请参阅书后的“教辅资料申请表”索取相关材料。

电子教师手册 ——教师手册包括使用本书的建议和策略，甚至还包括了讲座主题的提示。教师手册还包括每章结束处复习题的答案以及练习的建议方案。

图形文件——图形文件允许教师利用本书的图形创建自己的演示文稿。

PowerPoint 演示——本书的每一章都提供了相应的 Microsoft PowerPoint 幻灯片。它们可以用作课堂演示，让学生在网络上回顾每章的内容，或打印出来，分发给学生。教师还可以为在课堂上额外介绍的主题加入自己的幻灯片。

实验室手册 —— Course Technology 出版社出版了与本书和其他书配套的实验手册 *The Hands - On Information Security Lab Manual* (ISBN 0-619-21631-X)。该实验室手册提供了跟踪痕迹、枚举和防火墙配置等安全性强化练习，以及诸多作为实验室组件或课堂项目的练习和案例，作为本书的补充材料。要了解详细信息，请与 Course Technology 出版社的销售代理联系。

ExamView—— ExamView 是基于对象的测试需求的终极工具。它是一个功能强大的基于对象的试卷生成器，教师可从专门为 Course Technology 教材设计的试题库中创建书面的、基于 LAN 或基于 Web 的试卷。使用非常有效的 QuickTest Wizard 可以在不到 5 分钟的时间内利用 Course Technology 的试题库创建试卷，或重新定制自己的考试题。

目　录

第 1 章　信息安全简介

不要假想对手不会进行攻击；而应该关心自己是否已准备就绪。

—— Book of The Five Rings

对于 Amy 来说，这是她在 Sequential Label and Supply 公司诸多平常日子中的一天。她喜欢这份工作。接接电话，帮助办公室的人员解决一些 PC 问题，这不是很有趣，但很有挑战性，并且待遇非常丰厚。她的一些朋友在大公司工作，也有一些人就职于高科技公司，他们彼此之间都有联系。他们都认同技术工作是获得高薪的一种非常好的方式。

电话响了。这对 Amy 不是一个大问题，毕竟这是她的工作。她每个小时要回 35 次这样的电话，每天大约 315 次，每两周中有 9 天都是这样。这次的电话开始时和平常一样，焦虑的用户希望 Amy 能帮助他摆脱困境。这个电话的信息显示在屏幕上：用户的姓名、电话号码、工作部门、他的办公室在公司中的位置以及过去接到过的所有电话。

“嗨，Bob”，她说，“上次电话里谈的那个文档格式化问题您解决了没有？”

“解决了，Amy，希望我们也能解决今天出现的问题。”

“那咱们来试试，Bob，告诉我具体情况。”

“好，我的 PC 现在很奇怪，”Bob 说，“我进入电子邮件程序运行屏幕，可鼠标和键盘都没有响应。”

“您尝试重启机器了吗，Bob？”

“当然，但窗口没有关闭，我必须关掉它。机器重启后，我打开电子邮件程序，可情况还跟以前一样——根本没有响应。其他部分则工作正常，但非常非常慢，甚至 Internet 浏览器都非常慢。”

“Bob，看来这个问题在电话里解决不了，我马上建档，尽快派技术人员过去。”

Amy 看了看墙上的 LED 计数器，此刻只派出了两个技术人员提供台式支持服务，而今天白班共有 4 个技术人员。

“不会等太久的，别着急，Bob。”

她挂断 Bob 的电话，把他遇到的情况记录到 ISIS(信息状态和问题系统)中。她把这个新生成的案例放到台式支持派出队列中，外面的台式支持小队是根据问题的类型来分组的，他们在几分钟内就会注意到 Bob 的问题。

过了一会儿，Amy 看到服务管理小队的高级经理 Charles Moody 正急冲冲地走向大堂，他正从办公室走向服务器房间的门口，后面跟着 3 个高级技术人员，他们看起来都很着急。在那个房间，公司的服务器处于一个受控制的环境里。

正在此时，Amy 的机器发出鸣响，告诉她收到一封新邮件。她朝下一看，机器还在不断地发出鸣响。单击信封图标，过了一会，邮件窗口打开了。在她的收件箱里有 47 封新邮件。打

开来自 Davey Martinez 的一封信，他在会计部门工作，与 Amy 很熟。主题行是："请看下面的内容"。正文内容："看看我们经理的薪水……"，还有一个 Amy 不认识的文件附件图标。但她知道 Davey 经常会发些很有趣和好笑的电子邮件。她双击了该图标。

PC 机上的沙漏指针图标显示了一秒钟，然后恢复为正常的指针。其他什么也没发生。她又单击下一个电子邮件消息图标，什么也没发生。这时电话又响了，她单击计算机桌面上的 ISIS 图标，激活电话管理软件，并激活了她的无线话筒。"您好，Sequential Label and Supply 公司技术支持，您有什么问题吗？"她不知道打电话的人是谁，因为 ISIS 还没有在 PC 屏幕上打开。

"您好，我是 Erin Williams"。

Amy 看了一眼屏幕，ISIS 还是没有打开。她看了看计数器屏幕，惊奇地发现打入的电话正疯一般地往上涨，就像秒表上的数字一样。Amy 从没见过一下子有这么多电话打进来。

"嗨，Erin，" Amy 说，"发生什么事了？"

"不知道"，Erin 回答，"麻烦大了。"这些电话和早些时候 Bob 的电话如出一辙，只是 Amy 没有把它们记录到 ISIS 中，而只能写到一个便笺上。她也没有派出台式支持小队。她看着计数器屏幕，已经黑屏了，根本没有数字。

然后她看见 Charile 从服务器房间跑到了大厅。他已不再是焦急，而是被吓坏了。

Amy 拿起了电话，希望能够和领导协商下一步该怎么做，但电话根本没有声音。

学习目的：

基于以上素材，您可以：

- 理解信息安全的定义。
- 了解计算机安全的历史，及其如何演变为信息安全。
- 理解本章给出的关键术语以及信息安全的重要概念。
- 概述安全系统开发生命周期的各个阶段。
- 理解机构里信息安全所涉及到的人员角色。

1.1 引言

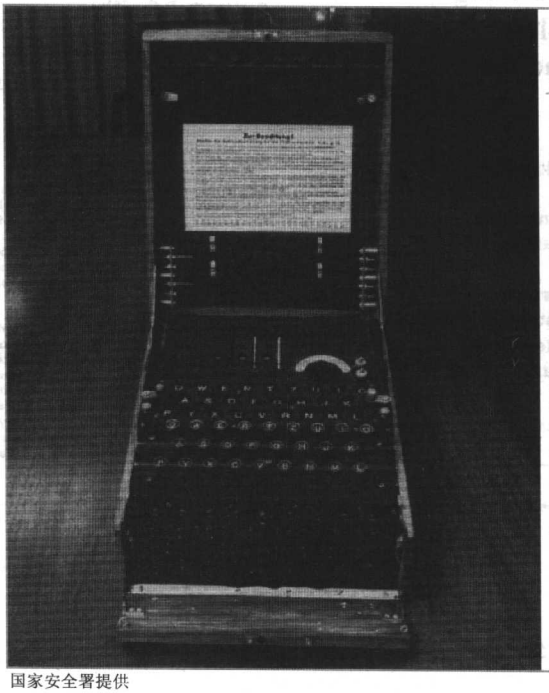
Inovant(世界最大的金融支付交易商务处理器)信息安全副主席 James Anderson 相信，当今企业的信息安全是一个为人所熟知的概念，它要在信息风险和控制之间保持平衡。

在本章开端的故事里，很明显 Sequential Label and Supply 公司的信息安全和控制未达到平衡。虽然 Amy 的工作是技术支持，她的责任就是解决技术问题，但她甚至没有想过公司当前的故障可能是病毒或蠕虫作祟的结果。管理也显得较为混乱，对这种情况没有什么应对措施。如果您处在 Amy 的位置，面对类似的状况，您会怎么做？采取什么对策？如果情况比这个简单的技术故障更为严重，您该怎么办？学习下面的章节，了解信息安全的更多内容，就能更好地回答这些问题。但在开始分析信息安全原理的细节之前，有必要先回顾一下该领域的起源。

1.2 信息安全发展史

信息安全起源于计算机安全。计算机安全就是确保硬件和软件的物理位置远离外部威胁。

在第二次世界大站期间开发了第一代大型机，主要是用来帮助分段计算代码(图 1-1)。从这些大型机付诸使用的那一刻起，就有了计算机安全的需求。人们采用多层安全措施来保护这些大型机，维护数据的完整性。例如，对重要军队位置的访问通过身份证件、密钥以及对授权人员的面部识别来加以控制。然而，随着维护国家安全的需求不断增长，计算机安全过程最终得到了更大的扩展，具有更复杂、技术更为高级的安全性。



德国代码机 Enigma 的早期版本在 1930 年第一次被 Poles 攻破。英国和美国在第二次世界大战期间攻破了更为复杂的后续版本。Enigma 不断增强的复杂版本，特别是 Enigma 的潜水艇或 Unterseeboot 版，在最终被攻破前曾使盟军大为苦恼。从加密传输中获得的信息可以用来预见德国军队的行动。“一些人问原因，如果我们二战期间还在读 Enigma，那我们就不会这么早地赢得这场战争。一些人还会问，如果我们二战期间还没破解它，那么我们现在也可能还没打赢这场战争呢。”

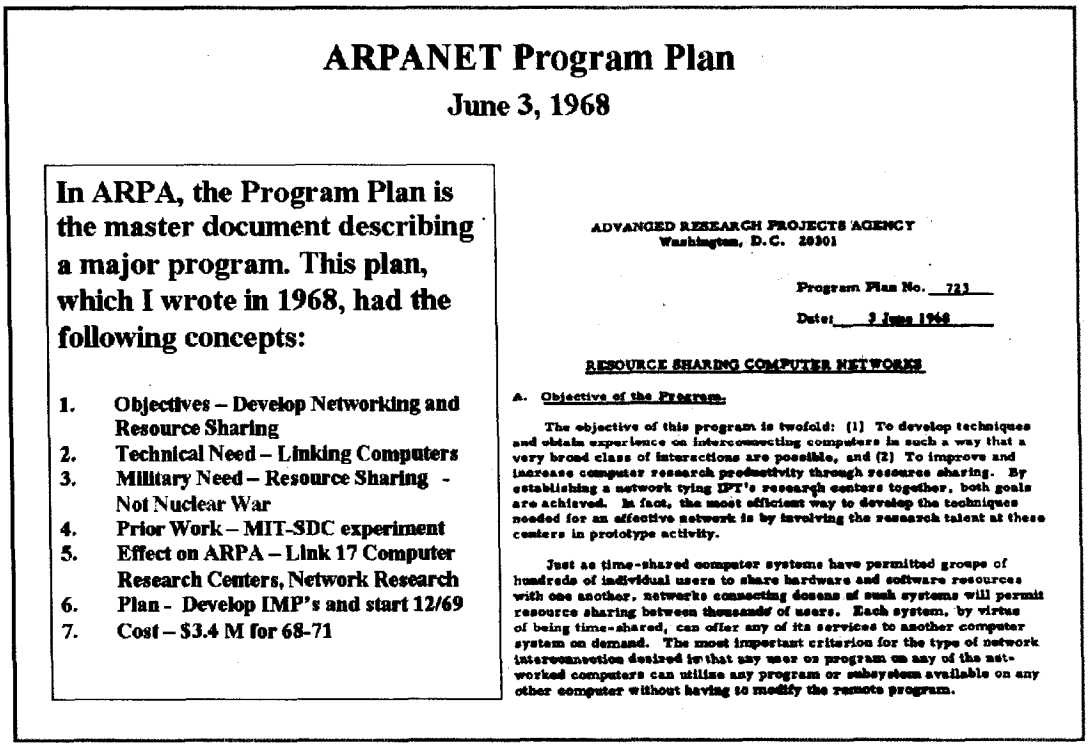
国家安全署提供

图 1-1　Enigma[1]

刚开始时，信息安全没有什么发展，主要由一些简单的文档分类模式组成，那时并没有针对计算机或操作系统的应用分类项目，因为那时安全的主要威胁是偷盗物理设备，对系统产品搞间谍活动和破坏。第一个非物理的文档安全问题出现在 20 世纪 60 年代早期：一个系统管理员对 MOTD(message of the day，消息日志)文件进行操作，同时另一个管理员编辑其密码文件。有一个软件故障混合了这两个文件，结果每个输出文件都打印出整个密码文件[2]。

1.2.1　20 世纪 60 年代

在冷战期间，人们使用许多大型机来完成更为复杂和高级的工作。此时，很有必要找到一种方式，使这些大型机互相通信，且通信过程要比在计算机中心之间互相邮递磁带简便得多。按此需求，(美国国防部)高级研究计划署(ARPA)开始考察设计一个冗余的、联网通信的系统的可行性，以保障军队交换信息。Internet 的奠基人 Larry Roberts 开发了这个项目。该项目命名为 ARPANET，它是当今 Internet 的雏形(ARPANET 项目规划[3]的摘录见图 1-2)。



ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. **Objectives – Develop Networking and Resource Sharing**
2. **Technical Need – Linking Computers**
3. **Military Need – Resource Sharing - Not Nuclear War**
4. **Prior Work – MIT-SDC experiment**
5. **Effect on ARPA – Link 17 Computer Research Centers, Network Research**
6. **Plan - Develop IMP's and start 12/69**
7. **Cost – $3.4 M for 68-71**

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 9 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Lawrence Roberts 博士提供

图 1-2　ARPANET 项目规划[3]

1.2.2　20 世纪 70 年代和 80 年代

在接下来的 10 年里，ARPANET 开始流行并投入使用，但其误用的趋势也在上升。1973 年 12 月，Ethernet(最流行的网络协议之一)的开发人员 Robert M."Bob"Metcalfe 指出，ARPANET 安全存在几个基本问题。各种远程用户站点没有足够的控制权和防护措施来保护数据免受未授权远程用户的访问。其他的问题包括：密码结构和格式非常脆弱；拨号连接的过程不安全；系统没有用户验证和授权。电话号码分布广泛，而且公开发布在电话亭的墙上，这使黑客很容易访问 ARPANET。因为计算机安全危害的范围很广，也非常频繁，而且 ARPANET 上的主机和用户数呈爆炸性增长，所以网络安全就变成网络不安全了[4]。1978 年，发表了一个著名的研究报告"保护性分析：最终报告"。它通过考察 ARPA 承担的一个项目，发现了操作系统安全的缺陷。表 1-1 按照时间顺序给出它和其他计算机安全重要研究的概况。

表 1-1　早期计算机安全的重要工作

日　期	文　档
1968	Maurice Wilkes 在"分时计算机系统"一文中讨论密码安全
1973	Schell、Downey 和 Popek 在"设计安全的军事计算机系统的初步设想"一文中提出检验军事系统时附加安全的必要性[5]
1975	在 *Federal Register* 中 FIPS(Federal Information Processing Standards，联邦信息处理标准)检验 DES(数字加密标准)