“十三五”
国家重点图书出版规划项目

龙芯中科
LOONGSON TECHNOLOGY
中国自主产权
芯片技术与应用丛书

龙芯

自主可信计算及应用

乐德广◉著
龙芯中科技术有限公司◉审校

信息安全 / 密码学 / 可信计算 / 可信度量技术 / 信任链技术 / 龙芯自主可控计算平台 / 龙芯自主可信计算平台 / 龙芯自主可信计算应用

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

★★★
★“十三五”★
国家重点图书出版规划项目

龙芯中科
LOONGSON TECHNOLOGY
中国自主产权
芯片技术与应用丛书

龙芯

自主可信计算及应用

乐德广◉著
龙芯中科技术有限公司◉审校

人民邮电出版社
北京

图书在版编目（CIP）数据

龙芯自主可信计算及应用 / 乐德广著. -- 北京 : 人民邮电出版社, 2018.12
（中国自主产权芯片技术与应用丛书）
ISBN 978-7-115-48216-7

Ⅰ. ①龙… Ⅱ. ①乐… Ⅲ. ①微处理器－系统设计 Ⅳ. ①TP332

中国版本图书馆CIP数据核字(2018)第058368号

内 容 提 要

本书主要介绍龙芯自主可信计算的研究背景、相关技术和具体应用。其中，第 1 章从信息安全的基础出发分析可信计算与信息安全的关系。第 2 章针对可信计算的密码支撑技术，介绍在可信计算中用到的相关密码算法。第 3 章到第 5 章分别介绍可信计算的体系结构及可信度量和信任链关键技术。第 6 章从国家安全的角度，重点介绍基于龙芯 CPU 处理器的自主可控计算平台的设计，包含硬件系统和配套的软件系统。第 7 章重点介绍基于龙芯国产 CPU 处理器和 TCM 可信密码模块的多层次自主可信计算体系结构。第 8 章重点介绍基于龙芯自主可信计算平台的文件可信存储和软件可信运行的安全应用，包括文件数据的可信加密和可信度量，以及软件的安全漏洞可信检测，从而确保软件的可信运行。

本书介绍的龙芯自主可信计算及其应用，在需要自主可信安全要求高的应用场合（如电子政务、航天航空、国防军事等）具有广阔的市场和应用前景。本书适合从事相关专业的科研和工程技术人员阅读，也可作为计算机、通信、信息安全、密码学等专业的教学参考书。

◆ 著　　乐德广
审　　校　龙芯中科技术有限公司
责任编辑　李永涛
责任印制　马振武

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：15.25
字数：302 千字　　2018 年 12 月第 1 版
印数：1－2 000 册　　2018 年 12 月河北第 1 次印刷

定价：69.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

INTRODUCTION

前言

计算机网络信息系统在我国的政治、经济、军事、文化等领域得到了广泛和深度的应用。没有信息化就没有现代化，信息已成为个人、企业乃至国家最为重要的资源，成为国家实力的象征。与此同时，其安全问题也日益突出和重要。防范高强度计算机网络信息系统的攻击，对世界各国都是一个难题。没有网络安全就没有国家安全，因此自主可信的计算机网络信息安全事关国家安全和社会稳定。本书从国家大力发展自主可信的安全战略需求出发，结合我国龙芯CPU自主计算技术和TCM国产可信计算技术，介绍具有完全自主知识产权的龙芯自主可信计算平台及其应用，从可信的物理安全、数据安全和软件安全3方面提升信息安全，对我国信息系统的自主可信安全建设具有重要的参考价值。

本书主要介绍龙芯自主可信计算的研究背景、相关理论技术和具体应用，分为8章，大致内容介绍如下。

- **第 1 章**：从信息安全的基础出发说明可信计算与信息安全的关系。
- **第 2 章**：针对可信计算的密码支撑技术，分别从对称密码体制、非对称密码体制和哈希密码体制 3 方面介绍密码学的研究现状和发展趋势，并介绍在可信计算中用到的相关密码算法。
- **第 3 章**：介绍可信计算的研究现状，包括可信计算的体系结构和主要技术，以及可信计算的相关组织。
- **第 4 章**：重点介绍可信度量技术，包括可信度量的模型，可信度量机制，IMA、PRIMA 和 DynIMA 可信度量技术。
- **第 5 章**：重点介绍信任链技术，包括基于无干扰理论和组合安全理论的信任链传递模型、TCG 信任链技术和 TPCM 信任链技术。
- **第 6 章**：从国家安全的角度说明了自主可控计算的发展现状，重点介绍基于龙芯国产 CPU 处理器的自主可控计算平台的设计，包含硬件系统和配套的软件系统。
- **第 7 章**：重点介绍基于龙芯国产 CPU 处理器和 TCM 可信密码模块的多层次自主可信计算体系结构，该自主可信计算体系结构具有积极防御和主动免疫的功能，可以从根本上对信息系统实施可信安全保护。

- **第 8 章：**重点介绍基于龙芯自主可信计算平台的文件可信存储和软件可信运行的安全应用，包括文件数据的可信加密和可信度量，以及软件的安全漏洞可信检测，从而确保软件的可信运行。

本书将自主可信安全基础、理论技术和应用相结合，深入浅出地介绍我国的自主可信安全现阶段的发展成果，可供从事相关专业的科研和工程技术人员阅读，也可作为计算机、通信、信息安全、密码学等专业的教学参考书。此外，本书也是一本我国自主可信安全知识的普及读物。

本书的编写工作得到了常熟理工学院学科建设项目和江苏省产学研前瞻性联合研究项目（项目编号：BY2016050-01）的资助，也得到了龚声蓉、陈华才、孙海勇、王叔君、成聪、陈卓等很多学者和同事的帮助和支持，在此对他们表示衷心的感谢。

最后，感谢康梅芳、张春娣等家人和朋友对我工作的支持和生活的照顾，没有你们的努力和付出，我就无法顺利完成本书的编写。

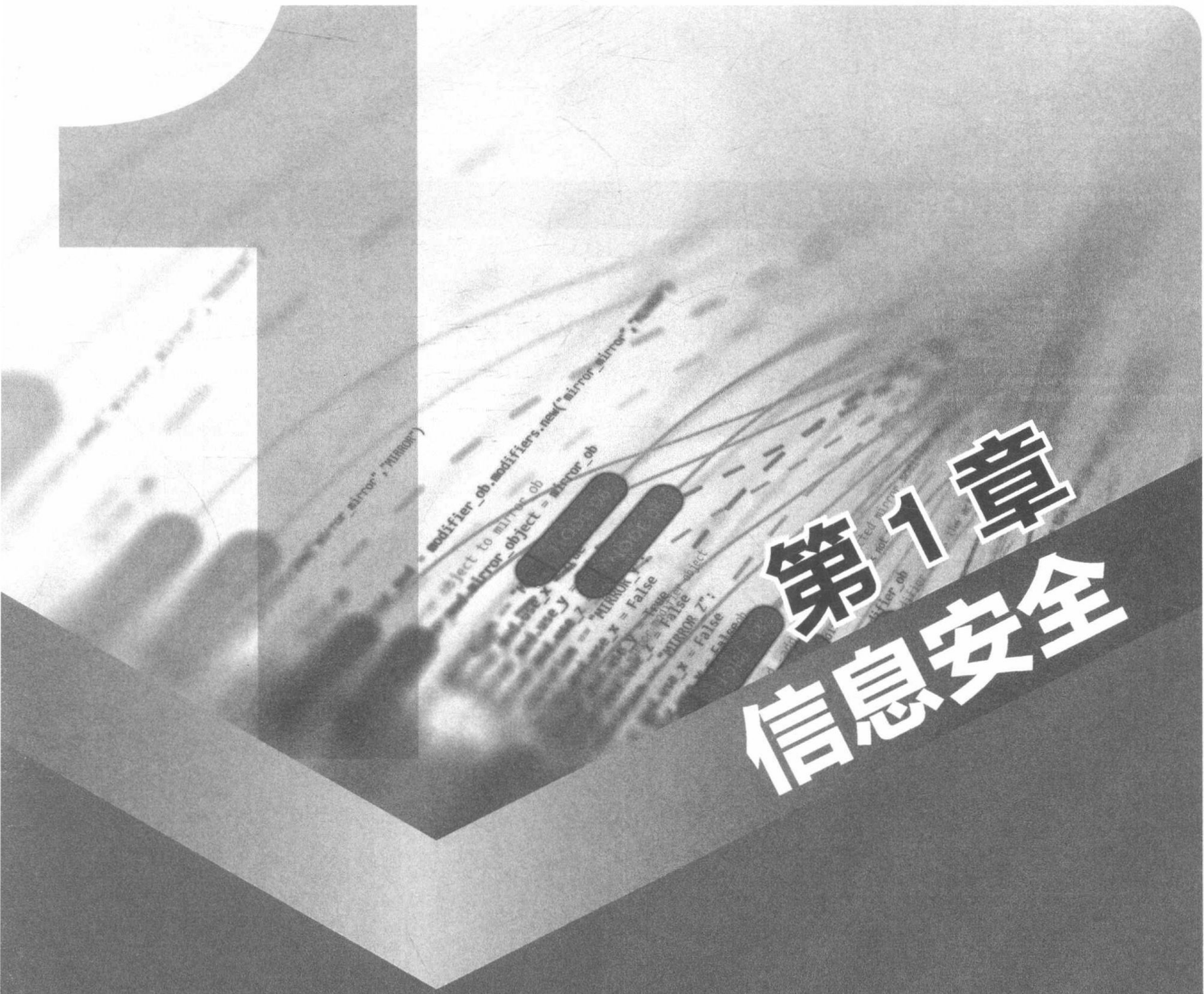
自主安全和可信计算技术的发展日新月异，新的需求和应用不断出现，作者水平有限，书中难免会有不妥、疏漏和错误之处，恳请读者理解和批评指正。

乐德广

2018 年 1 月于常熟

CONTENTS

目录



第1章 信息安全

随着社会的发展，人们对信息的需求和依赖日益增强。信息已成为个人、企业，乃至国家最为重要的经济、政治和军事战略资源。信息的获取、处理和安全保障能力成为一个国家综合实力的象征。目前，信息系统中存在信息泄漏、信息篡改、非法信息渗透和假冒等许多不安全因素，给个人、企业和组织造成巨大的经济损失，甚至危害社会稳定和国家安全。因此，信息系统的安全性显得越发重要，必须采取措施确保我国的信息安全。近年来，信息安全领域的发展十分迅速，取得了许多新的重要成果。信息安全理论与技术的内容十分广泛，这里主要介绍可信计算方面的研究和发展。本章首先从信息安全的定义、内容、缺陷、威胁和技术等方面进行概述；其次，基于 OSI 的 ISO/IEC 7498-2 标准，从安全服务和安全机制两方面介绍信息系统的安全体系结构；然后，对信息安全的保障、模型、层次模式、评估等方面进行研究；接着，介绍信息安全的相关标准和组织；最后，分析信息安全与可信计算的关系。

本章目标

了解信息安全的研究背景；明确信息安全的概念；了解信息安全所面临的威胁和攻击；了解信息安全的基本需求、目标和服务；掌握信息安全的解决方法。

1.1 信息安全概述

信息安全是一门涉及计算机技术、网络技术、通信技术、密码技术、软件技术、应用数学、数论、信息论等多种科学的综合性学科。本节从信息安全的定义、包含的内容、存在的缺陷、面临的威胁及发展的技术5方面对信息安全进行概述。

1.1.1 信息安全定义

随着计算机技术和网络通信技术应用的日益广泛，信息的数字化生存方式、空间、时间不断开拓，信息成为当今社会中不可或缺的基本要素。与此同时，信息所带来的安全问题日益突出，所面临的安全威胁日益严重，信息安全的内涵需要不断地延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为防御、检测、响应、恢复、控制、管理、评估等多方面的基础理论和实施技术。定义信息安全应考虑涵盖信息所涉及的全部内容，参照ISO国际标准化组织给出的计算机网络安全定义，认为信息安全是指为信息系统建立和采取的技术及管理的安全保护，即保护信息系统中的硬件、软件和数据信息资源，不因偶然或恶意的原因遭到破坏、更改、泄露，使信息系统连续可靠地正常运行，信息交换和共享服务正常有序不被中断。其中，信息系统是指由计算机及其相关和配套的设备、设施（包含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机交互系统。例如，互联网就是世界上最大的信息系统。典型的信息系统由硬件（包括计算机硬件和网络硬件）、系统软件（包括计算机系统软件和网络系统软件）和应用软件（包括由其处理、存储和传输的信息）3部分组成。信息安全的定义从信息的安全内容、安全缺陷和安全威胁等方面进行了高度概括。下面将对这些方面进行具体说明。

1.1.2 信息安全的内容

在信息系统中，信息既有存储于计算节点（包括个人计算机、服务器、交换机、路由器和网关等设备）上的信息资源，即静态信息，又有在计算节点中运行或在计算节点间传播的信息，即动态信息。从静态的观点看，信息安全主要是解决特定计算机设备的数据存储安全问题。如果今天输入到计算机中的数据，任何一段时间之后仍保留在那里，完好如初并没有被非法读取，那么一般称这台计算机具有一定的数据存储安全性。从动态的观点看，如果处理信息的软件运行的效果和用户所期望的一样，那么该软件具有一定的运行安全性，我们就可以判定这台计算机是可信任的，或者说它是安全的。安全问题是一个动态的过程，不能用

僵硬和静止的观点去看待，不仅仅是计算机硬件存在形式的安全，还在于计算机软件特殊形式的安全特性。因为自然灾害和有运行故障或安全漏洞的软件同非法存取数据一样对计算机的安全性构成威胁。人为的有意或无意的操作、某种计算机病毒的发作和软件漏洞利用攻击、不可预知的系统故障和运行错误，都可能造成计算机中数据的泄漏或丢失。因此，信息安全的内容应包括物理安全、软件安全和数据安全3方面内容，如图1-1所示。

图 1-1　信息安全内容

一、物理安全

物理安全又称为硬件安全，是针对物理介质中产生的损坏、破坏和丢失等安全问题，实施安全保护方案以确保物理介质自身的安全性，以及物理介质中存储和传输的信息安全性，包括设备质量保证和备份等。其中，物理安全问题包括自然环境变化（如温度、湿度等环境变化）和自然灾害（如水灾、火灾、雷电、地震等环境事故）、物理损坏（如硬盘损坏、设备使用寿命到期、人为破坏等）、设备故障（如停电、断电等）、设备缺陷（如噪音和电磁干扰、电磁泄漏等）。面对各种物理安全问题，一方面要提高物理硬件系统的可靠性和防护措施；另一方面要通过安全意识的提高，安全制度的完善和安全操作的提倡等方式使用户和管理维护人员在物理层中实现对信息的保护。例如，针对自然环境变化，加强对物理系统所在环境的安全保护，在温度、湿度、空气洁净度、腐蚀度、虫害、振动和冲击等方面要有具体的要求和严格的标准。位置环境的选择，要注意其外部环境安全性、地质可靠性、场地抗电磁干扰性，避开强振动源和强噪声源，并避免设在建筑物高层和用水设备的下层或隔壁。针对自然灾难，构建分布式冗余存储和路由进行区域保护。针对物理损坏，可采用RAID磁盘阵列备份。针对电磁干扰和泄露，采用辐射防护。针对停电断电，采用UPS应急恢复等。物理安全是信息安全的最基本保障，是整个信息安全系统不可缺少和忽视的组成部分。

二、软件安全

软件安全是针对软件本身可能存在的安全问题，实施安全保护方案以确保软件自身的安全性。软件安全是信息安全的关键。信息系统中的软件包括操作系统、应用软件和网络通信协议，因此软件安全问题主要归结为操作系统的安全问题、应用软件的安全问题和网络通信协议的安全问题。现在的主流操作系统，如Windows、UNIX、Linux和Android等都存在很多安全漏洞。操作系统的安全漏洞也是信息不安全的主要原因。操作系统的安全漏洞根本是由操作系统体系结构的缺陷所引起，操作系统的程序可以进行动态连接，驱动程序和系统服务也都可以用打补丁的方式进行动态升级。这种通过补丁改进与升级的操作系统很难从根本上杜绝安全漏洞。此外，操作系统长期运行的许多守护进程也通常成为攻击者利用的手段。

应用软件和操作系统一样由于安全漏洞的存在，运行时会出现非预期的行为，这种预期

之外的程序行为轻则会损害程序的预期功能，重则会导致程序崩溃，使其不能正常运行。更为严重的情况下，与安全相关的软件安全漏洞可以被攻击者利用，使程序主机遭受入侵，以至于造成如用户账号密码等私密数据信息的泄露。

TCP/IP是使用最为广泛的网络通信协议，由于TCP/IP自身的开放性特点，在最初的设计中，没有针对信息在网络通信过程引起的安全问题进行详细分析，从而产生许多在安全方面的设计缺陷。而TCP/IP协议的设计缺陷又引起了许多安全问题，如在FTP文件传输中没有对数据进行加密通信，导致信息的泄露。IP地址盗用和欺骗导致信息的伪造。ICMP、TCP SYN Flood等DoS攻击导致信息的中断。

因此，软件的安全性是指信息系统随时可用，信息系统运行过程中不出现故障，如果遇意外故障能够尽早恢复并尽量减少损失，保证信息的可靠性。其次，信息系统的管理者对信息系统有足够的控制和管理能力保证信息的可控性。另外，操作系统、网络通信协议和应用程序能够互相连接，协调运行，保证信息的互操作性。最后，检测信息系统运行中的安全漏洞，保证信息的可信性。

三、数据安全

数据安全是指信息自身的二进制数据安全性，包括信息的来源、去向，内容的真实无误确保信息的鉴别性，信息不被非法篡改和伪造确保信息的完整性，信息不会被非法泄露和扩散确保信息的保密性。此外，信息的发送者和接收者无法否认自己所做过的操作行为而保证信息的不可否认性。

1.1.3 信息安全的缺陷

安全性是信息的一个基本属性。影响信息安全的因素很多。本小节从信息系统的本质缺陷、内在缺陷及外在缺陷3方面说明出现信息不安全的主要原因。

一、本质缺陷

基于TCP/IP协议的互联网是世界上最大的信息系统。TCP/IP协议的标准化和开放性，使得互联网允许各种形式的通信网络和终端加入到互联网成为互联网的一个分子，并相互之间自由交换和共享信息。这种开放性大大降低了互联网的可控性和可信性，使它面临着各种安全威胁。此外，随着开放对象的多种多样，互联网规模的日益庞大，使整个互联网的软硬件系统都变得非常复杂。面对复杂的网络环境，其软硬件的设计也不可能尽善尽美，导致各种硬件缺陷、软件漏洞、协议设计缺陷的出现，这些也给信息安全带来了威胁。因此，开放性是互联网的最大特色和优点，同时也是信息安全的本质缺陷。如图1-2所示，如何既要保持互联网的开放性和灵活性，又要保证其信息的安全性是网络信息安全的重要目标。

二、内在缺陷

互联网信息系统自身主要由硬件系统、软件系统和通信协议3个基础部件构成，这些部件自身存在着内在的缺陷。这些缺陷也给互联网信息系统带来了安全方面的威胁和问题。

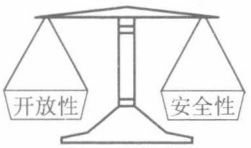


图 1-2　信息开放性与安全性

（1）硬件缺陷。

互联网的网络硬件系统自身存在物理属性缺陷和人的设计缺陷。例如，各种网络设备、通信终端和通信介质受到温度、湿度、静电、电磁场、闪电等自然因素及器件的物理老化的影响可能造成物理器件的失效、损坏或信息的泄漏。在无线通信系统中，数据信息在无线介质中以电磁波的形式在空中进行传播，存在电磁波泄露，并容易被截获的内在缺陷。此外，在硬件的设计和制造过程中，由于电路高度复杂，人的设计缺陷在所难免。例如，电路板焊点过密，造成电路短路，接插部件过多，容易出现接触不良故障等。

（2）软件缺陷。

互联网的软件系统包括操作系统和应用软件，它们同样具有不可避免的安全缺陷。软件系统的缺陷来源于设计和软件工程实现中的问题。例如，在软件设计中的疏忽可能造成软件系统内部逻辑错误或留下安全漏洞。软件工程实现中缺乏规范化和模块化要求，将导致软件的安全等级达不到所声称的安全级别。此外，随着硬件能力的越来越强，操作系统和应用软件的规模越来越大，软件系统中的漏洞也不可避免的存在，如微软的Windows操作系统也存在各种各样的安全漏洞和后门，这也是信息安全的主要威胁之一。

（3）TCP/IP 缺陷。

TCP/IP作为互联网的标准通信协议，它最初的设计主要是考虑数据交换和资源共享，其架构设计并未考虑安全问题，缺乏相应的安全监督机制，因此存在严重的安全缺陷。首先，TCP/IP缺乏保密性。TCP/IP的设计原则就是保持简单，唯一的功能就是负责互连，尽可能把复杂的工作交给上层应用或终端去处理，所以设计TCP/IP时没有考虑数据传输过程中的数据加密，数据流的传输都是明文的，包括用户账号和口令等重要信息。因此，恶意用户可以截获含有账号和口令的数据分组从而进行攻击，这种明文传输方式无法保障信息的保密性和完整性。其次，TCP/IP协议使用IP地址作为网络节点的惟一标志，IP地址是一种分级结构地址，其包含了主机所在的网络拓扑信息，因此使用标准IP地址的网络拓扑对互联网来说是暴露的。当IP分组在网络节点间传递时，对任何人都是开放的，即其IP分组的源地址很容易被发现，因此攻击者根据IP地址信息可以构造出目标网络的轮廓。接着，TCP/IP协议缺乏用户身份鉴别机制。例如，TCP/IP协议缺乏对IP包中的源地址真实性的鉴定机制，因此，互联网上任何通信节点都可以产生一个带任意IP地址的IP包，从而假冒另一个通信节点的IP地址进行欺骗，所以IP地址很容易被伪造和更改。然后，TCP/IP缺乏路由协议鉴别认证机制，即在

网络层上缺乏对路由协议的安全认证机制，对路由信息缺乏鉴别与保护。因此，可以通过互联网利用路由信息修改网络传输路径，误导网络分组传输。再次，TCP/IP层次结构的脆弱性。由于TCP/IP应用层协议位于TCP/IP体系结构的最顶部，因此下层的安全缺陷必然导致应用层的安全出现漏洞甚至崩溃，而各种应用层协议（如DNS、FTP、SMTP等）本身也存在安全隐患。最后，TCP/IP协议存在安全漏洞。例如，TCP协议建立一个完整的TCP连接，需要经历3次握手过程，通过这个握手过程，双方需要协商一些参数，包括双方的初始发送顺序号、分配发送和接收缓冲区等。在客户/服务器模式的3次握手过程中，假如客户的IP地址是虚假的，就不可能到达，那么TCP就不可能完成该次连接的3次握手，使TCP连接处于半开状态。攻击者利用这一漏洞可以实现如TCP SYN Flooding的DoS拒绝服务攻击。TCP提供可靠连接是通过初始序列号的鉴别机制来实现的。在具体的协议实现中，初始序列号一般由随机发生器产生，但是很多操作系统（如UNIX）所产生的序列号不是真正随机的，而是一个具有一定规律、可猜测或计算的数字。对攻击者来说，猜出了初始序列号并掌握了目标IP地址后，就可以对目标实施IP Spoofing的欺骗攻击。UDP是一个无连接协议，极易受IP源路由和拒绝服务攻击。因此TCP/IP通信协议的不完善和漏洞，给各种不安全因素的入侵留下了隐患。

三、外在缺陷

互联网为人所服务，因此离不开人的参与交互。这必然会引起由于人的参与所带来的安全问题，称为外在缺陷。主要包括人为误操作和人为攻击。

（1）人为误操作。

互联网作为一个客体，要使它能工作和发挥功能，必须要有人的操作和管理。在人的操作和管理中，由于误操作和管理的欠缺也将引起信息安全威胁和问题。首先是安全管理方面的原因，管理者缺乏对信息安全的警惕性或对信息安全技术的了解，没有制定切实可行的信息安全策略和措施。例如，很多接入互联网的企业缺乏对信息安全的认识，管理上存在很多漏洞。很多企业只提供了接入互联网的通道，对网络上的不法行为缺乏基本的应对措施，这是造成信息安全问题的原因之一。其次，网络用户存在误操作，如数据的误删除等。对于来自用户的误操作，常规的信息安全产品基本无能为力，这类误操作行为需要网络信息审计、IDS等主要针对内部信息安全的安全产品来抵御。

（2）人为攻击。

网络最终是为人服务的。当互联网为人们提供各种有价值的信息时，或者当网络中传输的信息具有价值的时候，不可避免地导致有人会非法获得这些信息资源（包括截取、修改甚至破坏这些信息等）的恶意行为，从而出现各种网络信息安全攻击。网络信息安全攻击的出现，给人们的社会、经济生活产生了破坏性影响，真正给信息的安全带来了巨大的威胁。

信息安全攻击是指损害信息系统及数据安全的任何行为，即攻击者（包括黑客和内部

人员等）利用目前信息系统的安全缺陷通过使用各种攻击方法非法进入本地或远程用户信息系统，非法获得、修改、删除系统的信息，以及在系统上添加、伪造信息等一系列过程的总称。信息安全攻击对信息安全造成极大的危害，并导致机密信息的泄漏。人为的恶意入侵和攻击是信息安全所面临的最大威胁。因此，下面将介绍信息安全攻击手段的种类，并列举常见的典型攻击方法。

根据攻击行为的不同，信息安全攻击分为被动攻击和主动攻击。其中，被动攻击是在不影响信息系统正常工作的情况下，进行截获、窃取、破解以获得重要机密信息。在被动攻击中，攻击者的目的只是获取信息，因此攻击者不会篡改信息或危害信息系统，信息系统可以不中断其正常运行。然而，攻击可能会危害信息的发送者或接收者，因此在信息发送者或接收者发现机密信息已经泄露之前，要发现这种攻击非常困难。主动攻击以各种方式有选择地破坏信息的有效性和完整性。主动攻击可能改变信息或危害信息系统。主动攻击通常易于探测但却难于防范，因为攻击者可以通过多种方法发起攻击。根据攻击方式、方法和手段的不同，信息安全攻击包括恶意程序和木马攻击、缓冲区溢出攻击、拒绝服务攻击、欺骗攻击、中间人攻击、重放攻击和扫描监听攻击等。

- 恶意程序和木马攻击。

恶意程序攻击是攻击者在信息系统中插入一组指令或程序代码破坏信息系统功能或破坏信息数据，影响信息系统使用。恶意程序能够通过文件复制、文件传送、文件执行等方式传播给其他计算机和整个互联网信息系统。图1-3显示了CNCERT/CC近年来捕获及通过厂商交换获得的移动互联网恶意程序样本数量统计。

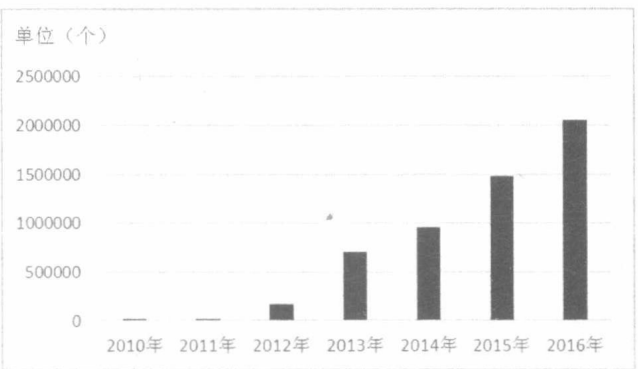


图 1-3　2010 ～ 2016 年移动互联网恶意程序样本数量对比（来源：CNCERT/CC）

从图1-3可以看出，大量涌现的恶意程序在移动互联网上极快地传播，对移动互联网安全带来了巨大灾难和安全问题，影响系统效率、破坏数据和阻塞网络等。木马和恶意程序一样也是一种蓄意设计的特殊程序，其一般分为客户端（Client）程序和服务器端（Server）程序。客户端是本地使用的各种命令的控制台程序，服务器端则是要给别人运行的程序，只有