中山大學
SUN YAT-SEN UNIVERSITY

Module I. Fundamentals of Information Security

Chapter 1
Introduction to Information Security

Information Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- **1.1 Concept of Information Security**
  - Situation of Information Security
  - Definition of Information Security
  - History
  - Key Concepts
- **1.2 Computer System Security**
  - System Vulnerabilities
  - Operating System Security
  - Database Security
  - User Application Security

Outline

- **1.3 Information Security Service**
  - Basic Concepts
  - Authentication
  - Access Control
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation
- **1.4 Information Security Management, Audit and Protection**
  - Security Management
  - Security Audit
  - Levels of Information Security
- **1.5 Conclusion**

Outline

- **1.1 Concept of Information Security**
  - Situation of Information Security
  - Definition of Information Security
  - History
  - Key Concepts
- 1.2 Computer System Security
- 1.3 Information Security Service
- 1.4 Information Security Management, Audit and Protection
- 1.5 Conclusion

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CERT/CC
  - Computer Emergency Response Team/Coordination Center (美国计算机紧急事件响应小组协调中心)
  - http://www.cert.org
  - CERT Division/SEI/CMU
- CNCERT/CC
  - 中国国家计算机网络应急技术处理协调中心 (中国国家互联网应急中心)
  - http://www.cert.org.cn

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2016

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2016

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

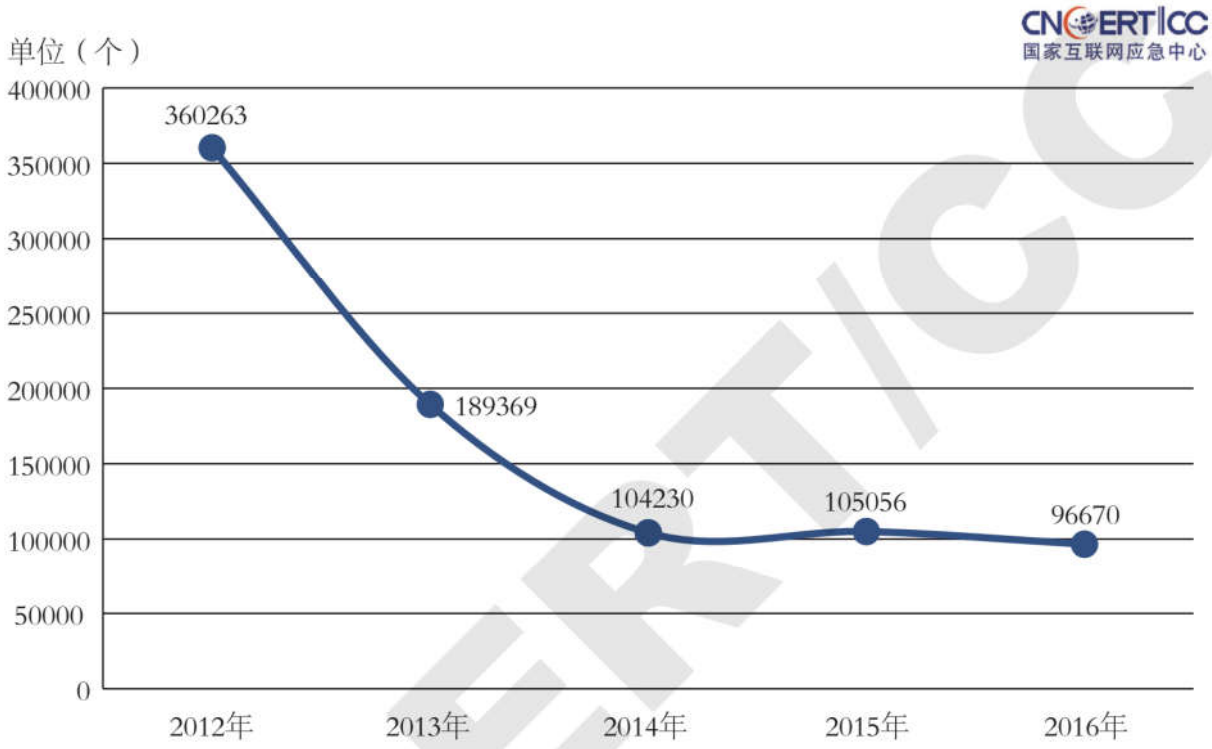


图1-1　2012-2016年木马和僵尸网络控制端数量对比（来源：CNCERT/CC）

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

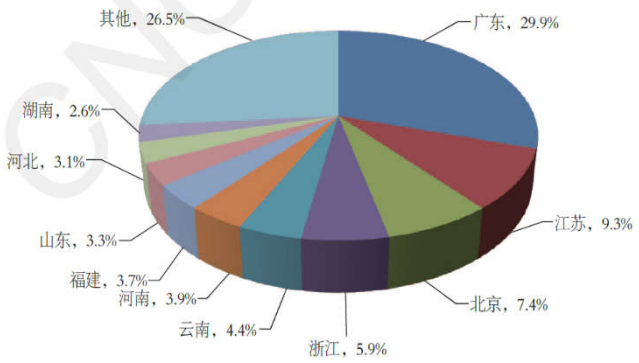
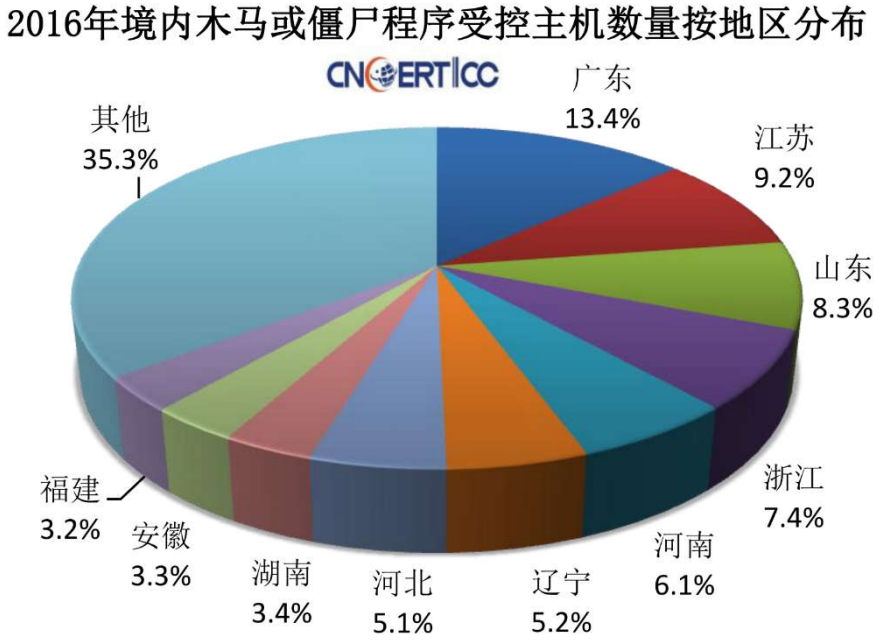


图3-4 2015年境内木马或僵尸程序控制服务器IP地址按地区分布（来源：CNCERT/CC）



1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

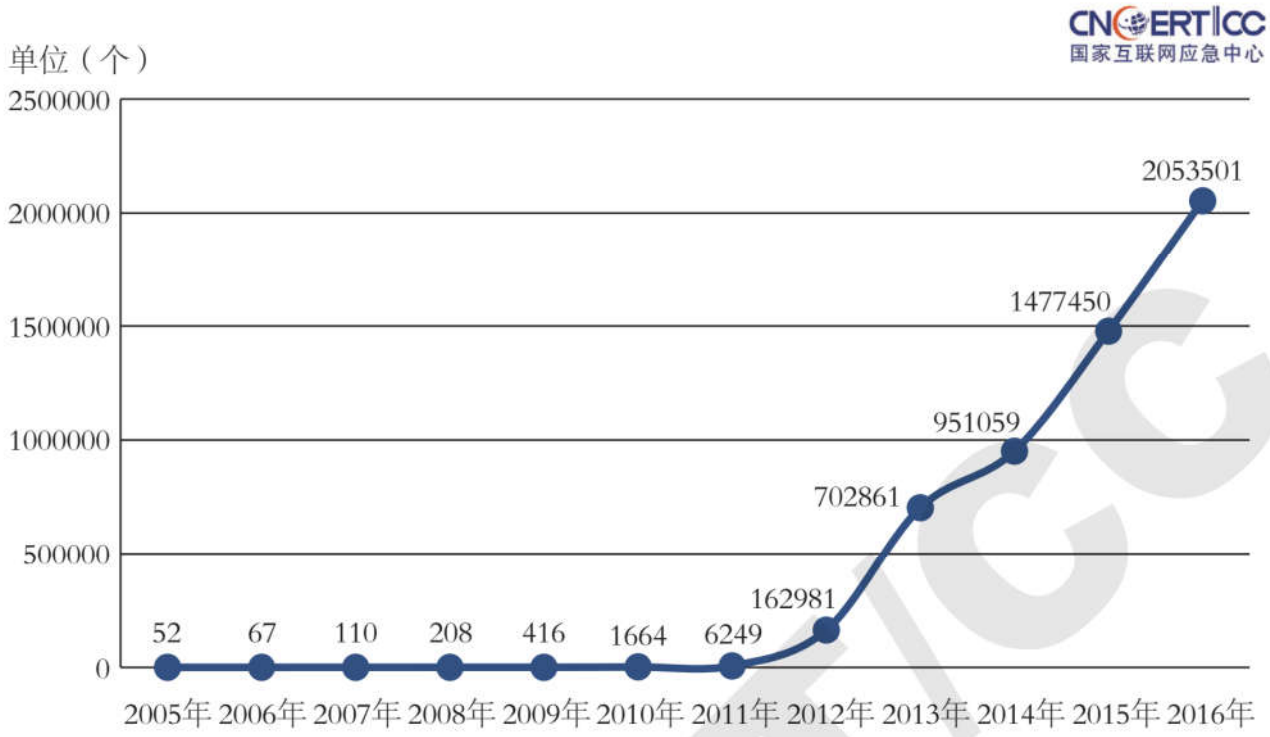


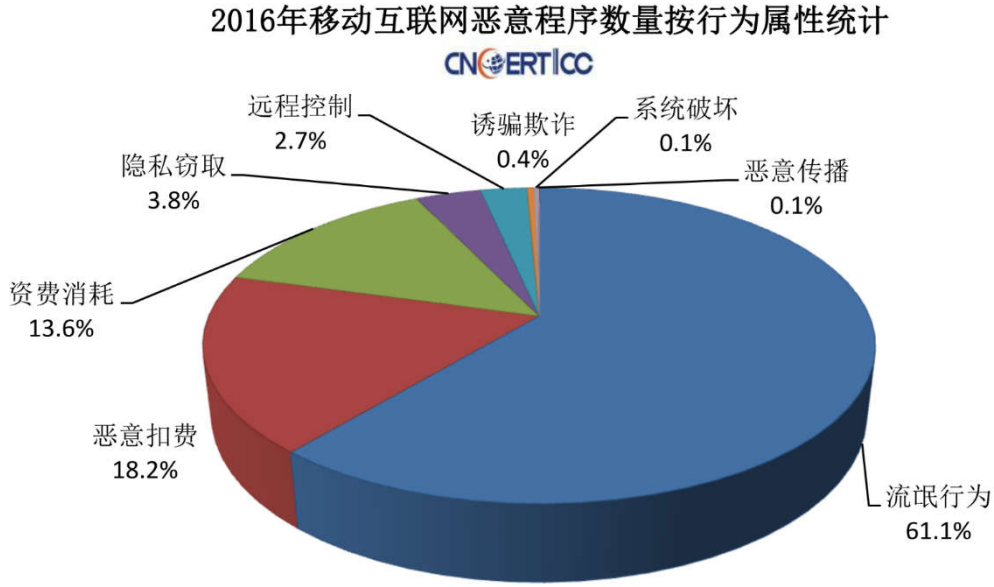
图1-3　2005-2016年移动互联网恶意程序走势（来源：CNCERT/CC）

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

图4-1 2015年移动互联网恶意程序数量按行为属性统计（来源：CNCERT/CC）



1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

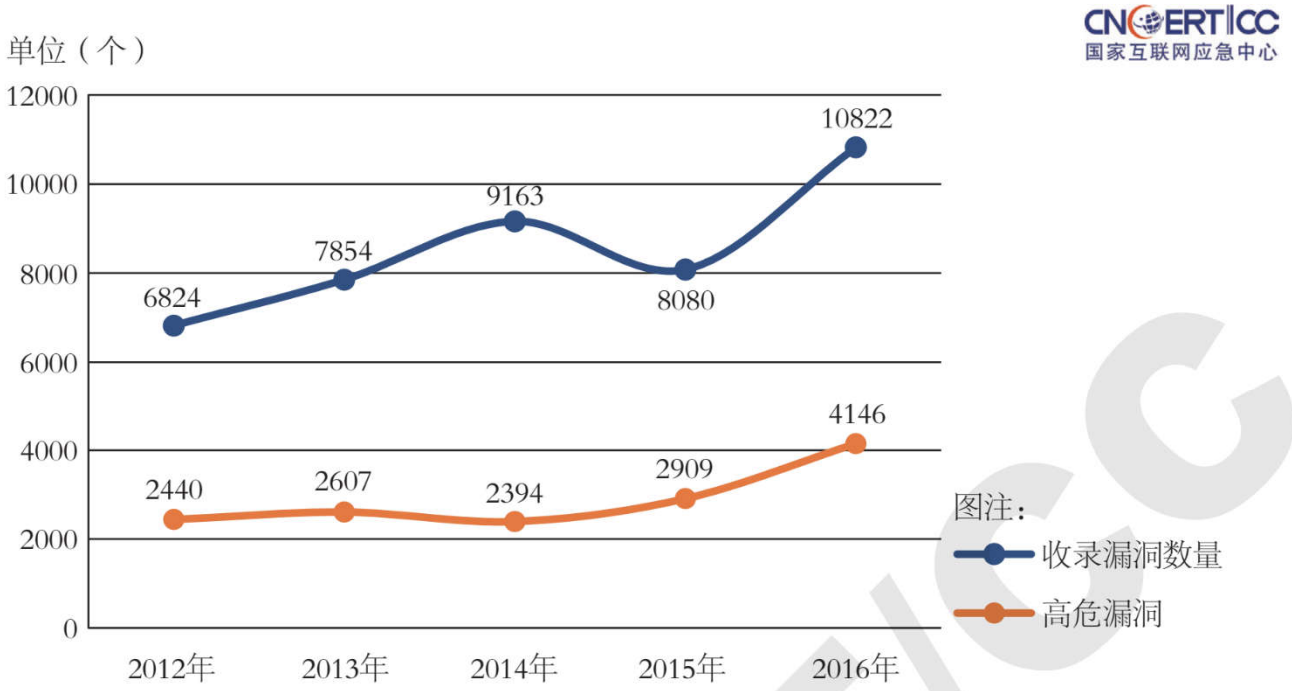
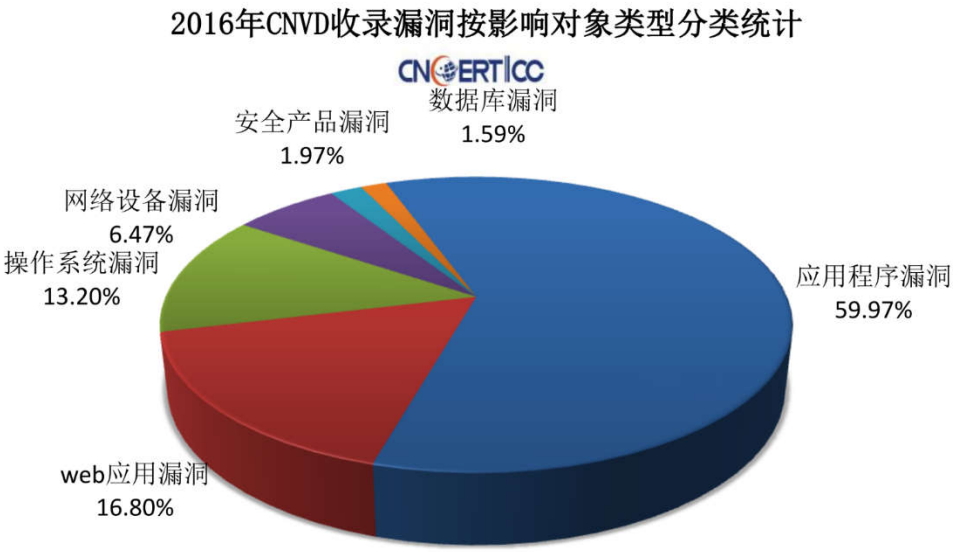


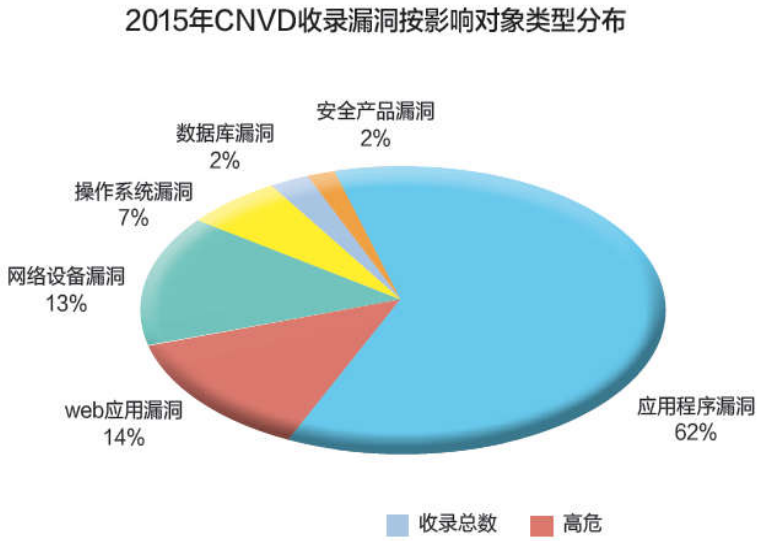
图1-6　2012-2016年CNVD收录的漏洞数量对比（来源：CNCERT/CC）

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016





1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

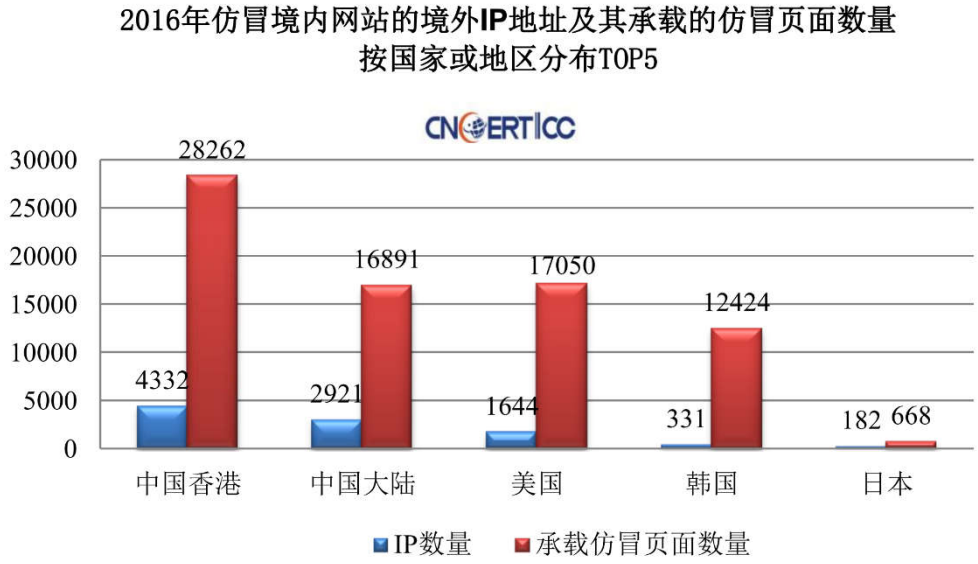
表1-1　2016年CNVD收录漏洞涉及的厂商情况统计（来源：CNCERT/CC）

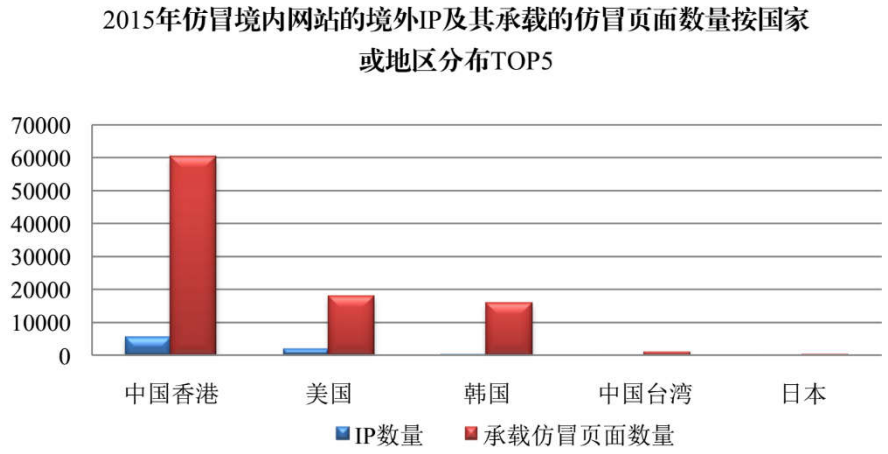
漏洞涉及产品	漏洞数量（个）	占全年收录数量百分比
Google	819	7.6%
Oracle	689	6.4%
Adobe	561	5.2%
Microsoft	522	4.8%
IBM	500	4.6%
Apple	439	4.1%
Cisco	356	3.3%
Wordpress	233	2.2%
Linux	218	2.0%
Mozilla	183	1.7 %
Huawei	155	1.4%
其他	6147	56.7%

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016





1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

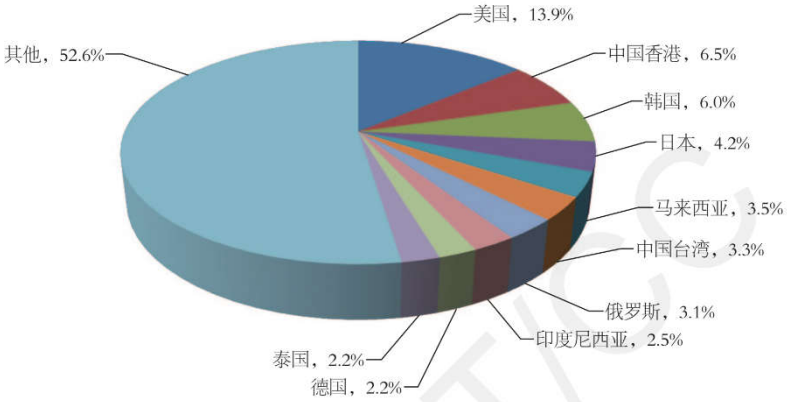
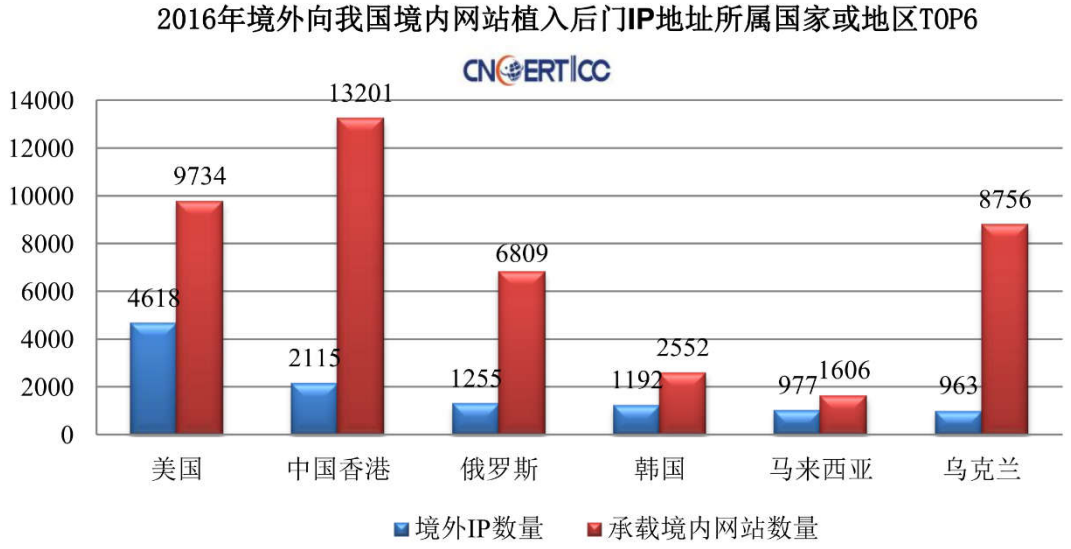


图5-8 2015年向我国境内网站植入后门的境外IP地址按国家和地区分布
（来源：CNCERT/CC）



1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

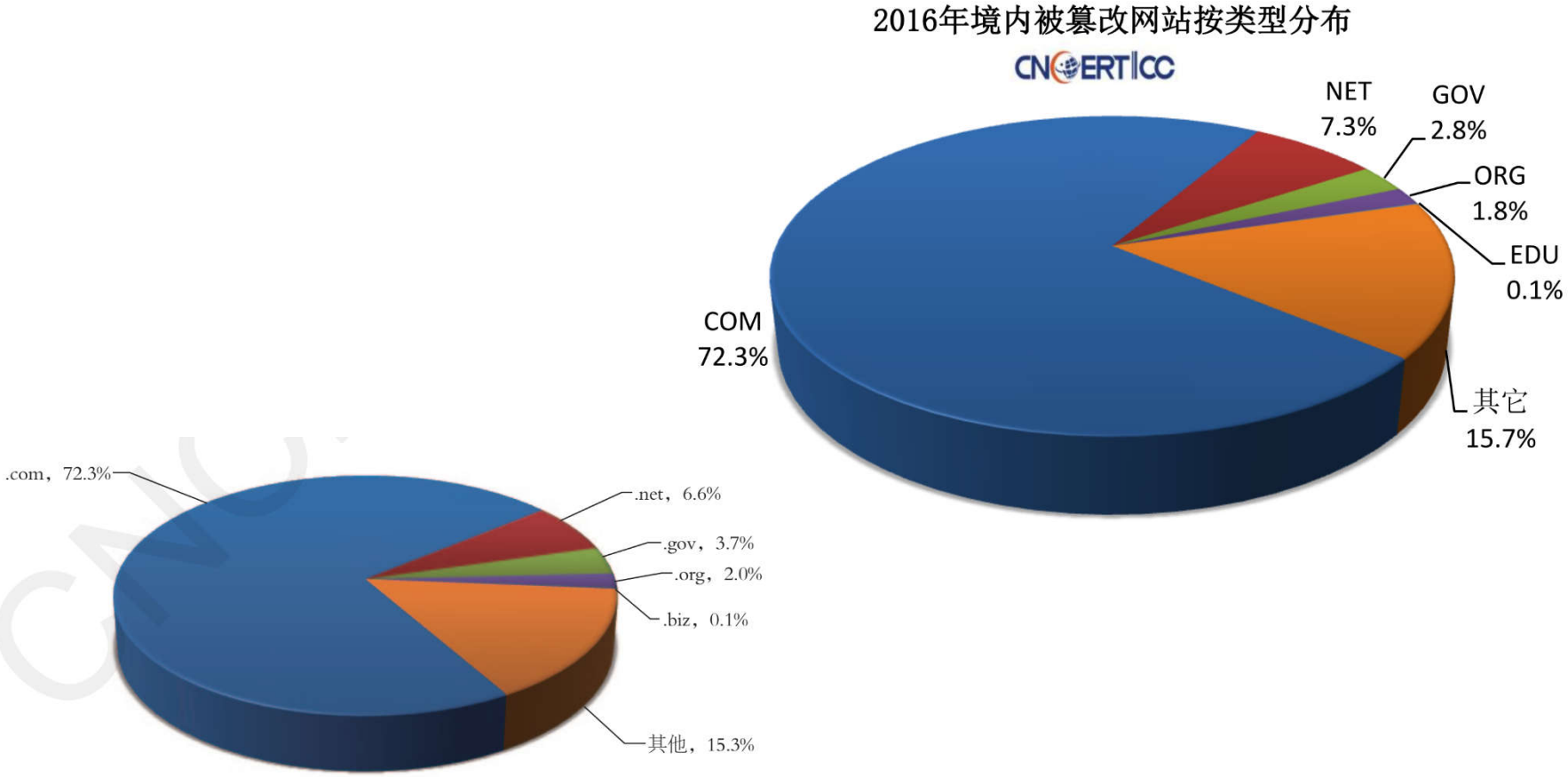


图5-2　2015年我国境内被篡改网站按域名类型分布（来源：CNCERT/CC）

1.1 Concept of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2016

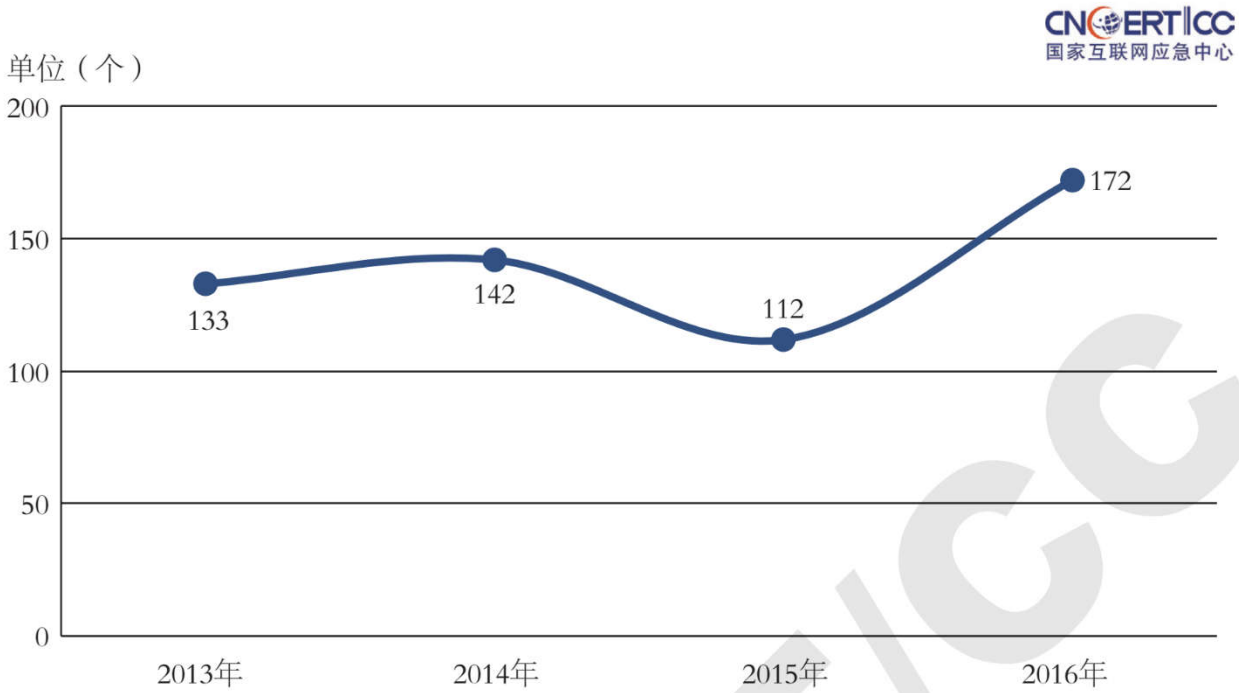


图1-11　2013-2016年CNVD收录的工业控制系统漏洞情况
（来源：CNCERT/CC）

1.1 Concept of Information Security

1.1.2 Definition of Information Security

- **Security**
  - Security: “The quality or state of being secure—to be free from danger”
  - Multiple layers of security in an organization
    - ✧ Physical security
    - ✧ Personal security
    - ✧ Operations security
    - ✧ Communications security
    - ✧ Network security
    - ✧ Information security

1.1 Concept of Information Security

1.1.2 Definition of Information Security

- **Information Security**
  - Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
  - Information security: a “well-informed sense of assurance that the information risks and controls are in balance.”

    - Jim Anderson

1.1 Concept of Information Security

1.1.2 Definition of Information Security

- **Information Security**
  - 信息安全指保护信息和信息系统免受未经授权的访问、使用、披露、破坏、修改、审阅、检查/探测、记录或销毁。
    - ✧ 一般认为，信息安全主要包括以下五方面的内容：信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。
    - ✧ 信息安全的根本目的是使内部信息不受外部威胁，因此信息通常要加密；为保障信息安全，要求有信息源认证和访问控制；还要排除非法软件驻留和非法操作的可能性。
  - 信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

1.1 Concept of Information Security

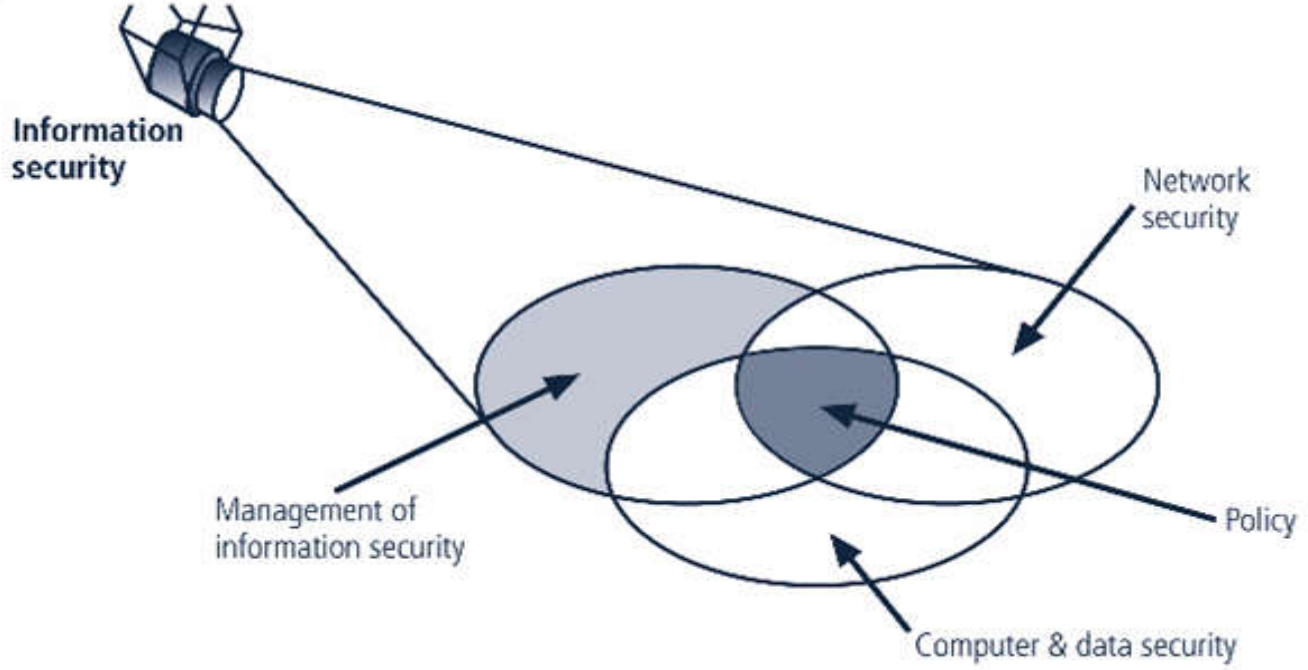
1.1.2 Definition of Information Security

- **Information Security**
  - 信息安全威胁
    - ✧ 窃取：非法用户通过数据窃听的手段获得敏感信息。
    - ✧ 截取：非法用户首先获得信息，再将此信息发送给接收者。
    - ✧ 伪造：将伪造的信息发送给接收者。
    - ✧ 篡改：非法用户对合法用户之间的通讯信息进行修改，再发送给接收者。
    - ✧ 拒绝服务攻击：攻击服务系统，造成系统瘫痪，阻止合法用户获得服务。
    - ✧ 行为否认：合法用户否认已经发生的行为。
    - ✧ 非授权访问：未经系统授权而使用网络或计算机资源。
    - ✧ 传播病毒：通过网络传播计算机病毒。

1.1 Concept of Information Security

1.1.2 Definition of Information Security

- **Information Security**
  - Components of information security



1.1 Concept of Information Security

1.1.2 Definition of Information Security

- **Information Security**
  - 信息安全覆盖范围广泛，从国家事务的机密安全，到防范商业企业机密泄露、防范青少年对不良信息的浏览、防止个人信息泄露等。
  - 网络环境下的信息安全体系是保证信息安全的关键，其中包括了计算机安全操作系统、安全协议、安全机制 (如数字签名、信息认证、数据加密) 等，其中任何一个安全漏洞都可能对全局安全造成威胁。
  - 信息安全服务至少应该包括支持信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

1.1 Concept of Information Security

1.1.2 Definition of Information Security

- **Information Security, Computer Security and Information Assurance**
  - Similarities
    - ✧ Protecting the **Confidentiality**, **Integrity** and **Availability** of information
  - Differences
    - ✧ The approach to the subject
    - ✧ The methodologies used
    - ✧ The areas of concentration

1.1 Concept of Information Security

1.1.3 History of Information Security

- Since the early days of writing, heads of state and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering.
- Julius Caesar (July 100 – 15 March, 44 BC) is credited with the invention of the Caesar cipher which was created in order to prevent his secret messages from being read should a message fall into the wrong hands.
- World War II brought about many advancements in information security and marked the beginning of the professional field of information security.

1.1 Concept of Information Security

1.1.3 History of Information Security

- Originated from computer security
  - Began immediately after the first mainframes were developed
  - Groups developing code-breaking computations during World War II created the first modern computers
  - Physical controls to limit access to sensitive military locations to authorized personnel
  - Rudimentary in defending against physical theft, espionage, and sabotage (初步用于防范物理盗窃、间谍活动和蓄意破坏)

1.1 Concept of Information Security

1.1.3 History of Information Security

- The 1960s
  - Advanced Research Procurement Agency (ARPA, 高级研究项目局) began to examine feasibility of redundant networked communications
  - Larry Roberts developed ARPANET from its inception
- The 1970s and 80s
  - ARPANET grew in popularity as did its potential for misuse
  - Fundamental problems with ARPANET security were identified
    - ✧ No safety procedures for dial-up connections to ARPANET
    - ✧ Non-existent user identification and authorization to system
  - Late 1970s: microprocessor expanded computing capabilities and security threats

1.1 Concept of Information Security

1.1.3 History of Information Security

- R-609
  - Information security began with Rand Report R-609 (paper that started the study of computer security)
  - Scope of computer security grew from physical security to include:
    - ✧ Safety of data
    - ✧ Limiting unauthorized access to data
    - ✧ Involvement of personnel from multiple levels of an organization

1.1 Concept of Information Security

1.1.3 History of Information Security

- The 1990s
  - Networks of computers became more common; so too did the need to interconnect networks
  - Internet became first manifestation of a global network of networks
  - In early Internet deployments, security was treated as a low priority
- The Present
  - The Internet brings millions of computer networks into communication with each other—many of them unsecured
  - Ability to secure a computer's data influenced by the security of every computer to which it is connected – the security of networks

1.1 Concept of Information Security

1.1.3 History of Information Security

- 信息安全的发展历史
  - 自从人类有了书写文字，国家和军队首脑已经认识到使用一些技巧来保证通信的机密以及获知其是否被篡改是非常有必要的。通常认为凯撒在公元前50年发明了凯撒密码，它被用来防止秘密的消息落入错误的人手中时被读取。
  - 第二次世界大战使得信息安全研究取得了许多进展，并且标志着其开始成为一门专业的学科。
  - 20世纪末以来通信、计算机硬件和软件以及数据加密领域发展迅速。在因特网上快速增长的电子数据处理和电子商务应用，全社会形态对计算机及网络的高度依赖，以及技术、行为和后果日趋严重的数据侵略事件，形成对保护计算机及其数据存储、加工和传输的信息安全的迫切需求。

1.1 Concept of Information Security

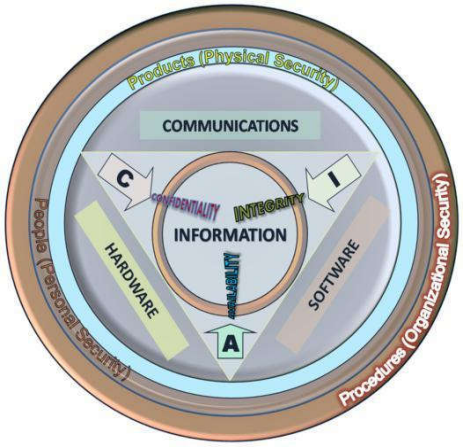
1.1.4 Key Concepts of Information Security

- The value of information comes from the characteristics it possesses
  - Availability, Accuracy, Authenticity, Confidentiality, Integrity, Utility, Possession
- **CIA** triad
  - For over twenty years, information security has held **confidentiality**, **integrity** and **availability**, the **CIA** triad, to be the core principles of information security.
  - Confidentiality
    - ✧ Data confidentiality: Assures that confidential information is not disclosed to unauthorized individuals
    - ✧ Privacy: Assures that individual control or influence what information may be collected and stored

1.1 Concept of Information Security

1.1.4 Key Concepts of Information Security

- **CIA** triad
  - Integrity
    - ✧ Data integrity: assures that information and programs are changed only in a specified and authorized manner
    - ✧ System integrity: assures that a system performs its operations in unimpaired (未受损害) manner
  - Availability
    - ✧ Assure that systems works promptly and service is not denied to authorized users



1.1 Concept of Information Security

1.1.4 Key Concepts of Information Security

- Other concepts to a complete security picture
  - Authenticity
    - ✧ The property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator
  - Accountability
    - ✧ Generates the requirement for actions of an entity to be traced uniquely to that individual to support nonrepudiation, deference, fault isolation, etc
  - ref. to Sec.1.3.2

1.1 Concept of Information Security

1.1.4 Key Concepts of Information Security

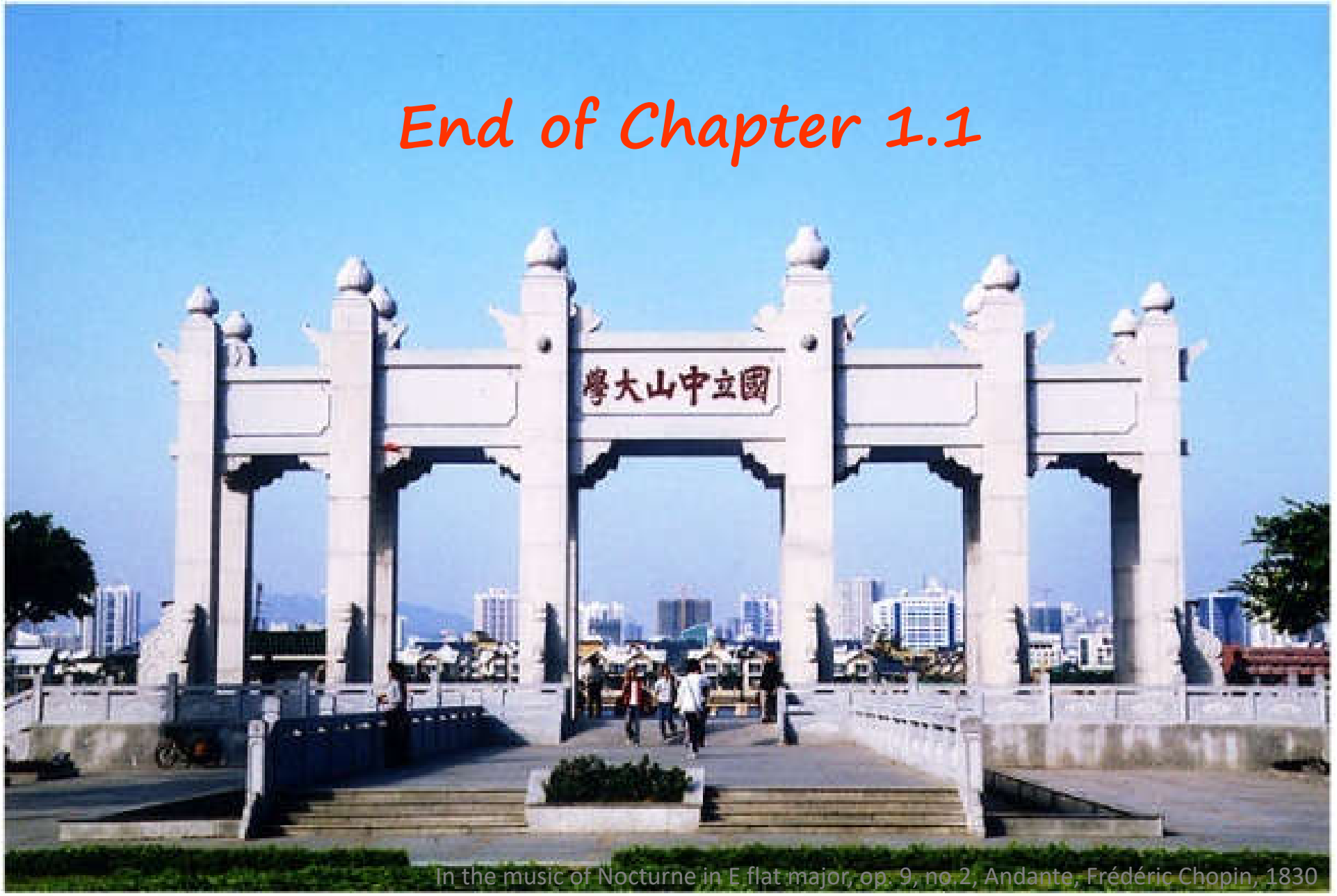
- 信息安全的主要概念
  - 计算机安全、信息安全以及信息保障等学科是和许多专业的组织一起出现的。他们都持有共同的目标，即确保信息系统的安全和可靠，包括
    - ✧ 真实性：判断信息的来源，能对伪造来源的信息予以鉴别
    - ✧ 保密性：保证机密信息不被窃听，或机密信息的真实含义不被窃听者了解
    - ✧ 完整性：保证数据的一致性，防止数据被非法用户篡改
    - ✧ 可用性：保证合法用户对信息和资源的使用不会被不正当地拒绝
    - ✧ 不可抵赖性：建立有效的责任机制，防止用户否认其行为
    - ✧ 可控制性：对信息的传播及内容具有控制能力
    - ✧ 可审查性：对出现的网络安全问题提供调查的依据和手段

1.1 Concept of Information Security

1.1.4 Key Concepts of Information Security

- Levels of security breach impact (安全事件的影响级别)
  - Low
    - ✧ The loss will have a limited impact, e.g., a degradation (恶化) in mission or minor damage or minor financial loss or minor harm.
  - Moderate
    - ✧ The loss has a serious effect, e.g., significance degradation on mission or significant harm to individuals but no loss of life or threatening injuries.
  - High
    - ✧ The loss has severe or catastrophic (惨重的) adverse effect on operations, organizational assets or on individuals (e.g., loss of life)

End of Chapter 1.1



In the music of Nocturne in E flat major, op. 9, no.2, Andante, Frédéric Chopin, 1830