中山大學
SUN YAT-SEN UNIVERSITY

Module I. Fundamentals of Information Security

Chapter 1
Introduction to Information Security

Web Security: *Principles & Applications*

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

Outline

- **1.1 Concepts of Information Security**
  - Situation
  - Definition
  - 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 Concepts of Information Security**
  - Situation
  - Definition
  - 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 Concepts of Information Security

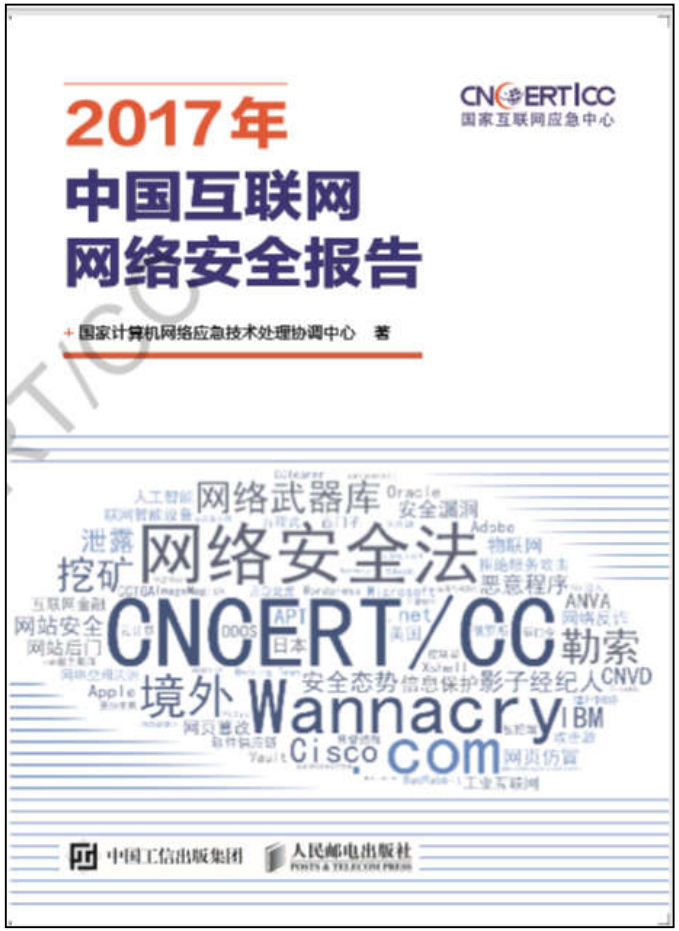
1.1.1 The Situation of Information Security

- 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 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Annual Report 2017



1.1 Concepts of Information Security

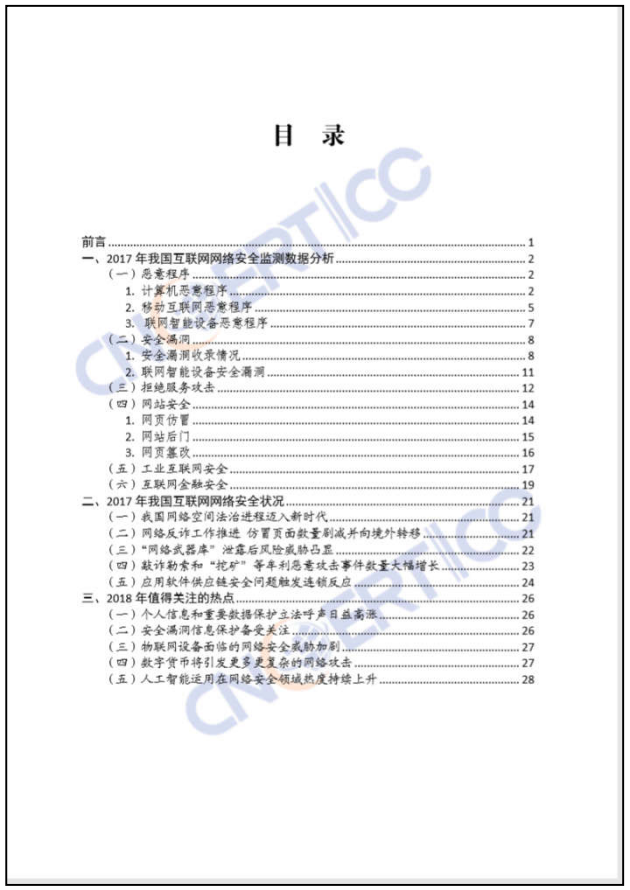
1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

2017 年我国互联网网络安全态势综述

国家计算机网络应急技术处理协调中心

2018 年 4 月



目 录

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

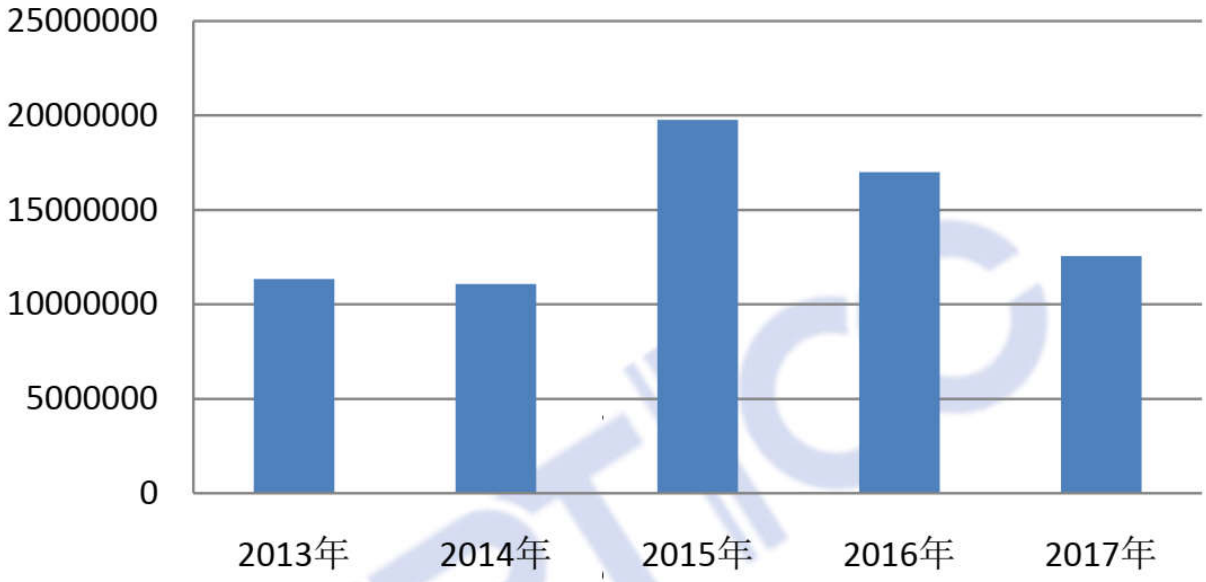


图 1 境内感染计算机恶意程序主机数量变化

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

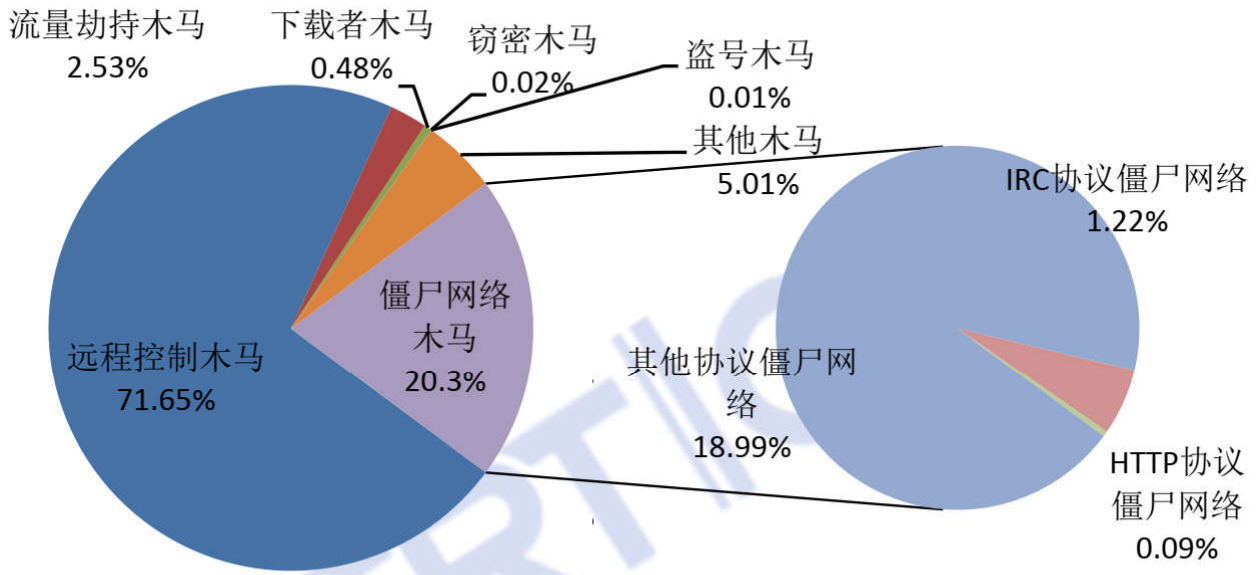


图 2 2017 年计算机恶意程序类型分布

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

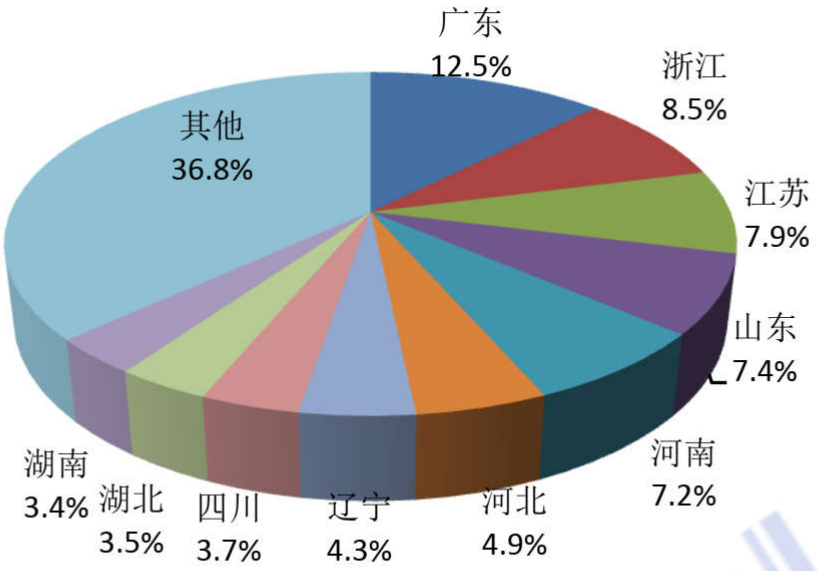


图 3 2017 年境内计算机恶意程序受控主机数量按地区分布

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

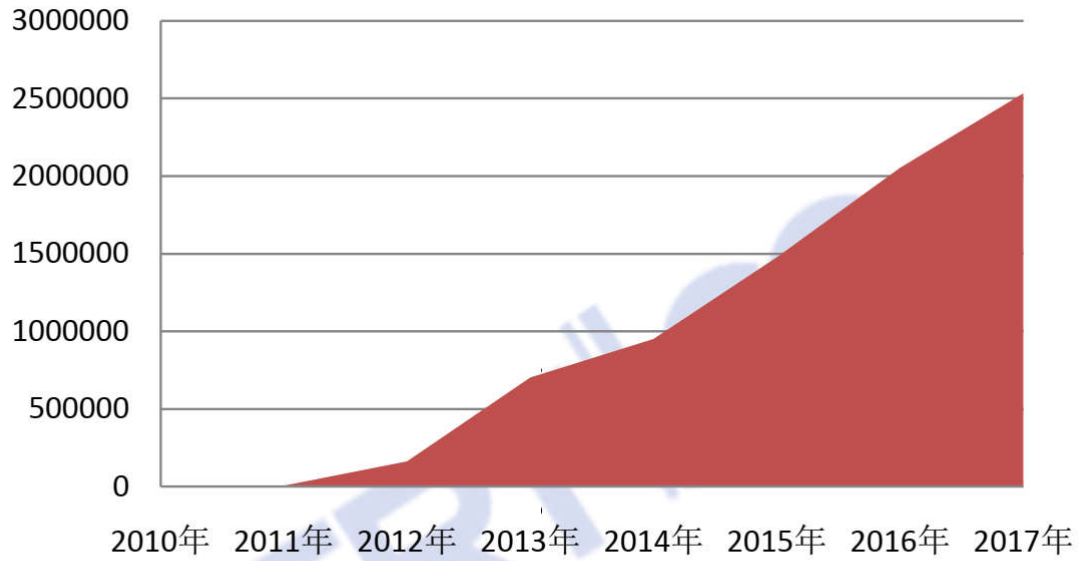


图 5 2010 年至 2017 年移动互联网恶意程序捕获数量走势

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

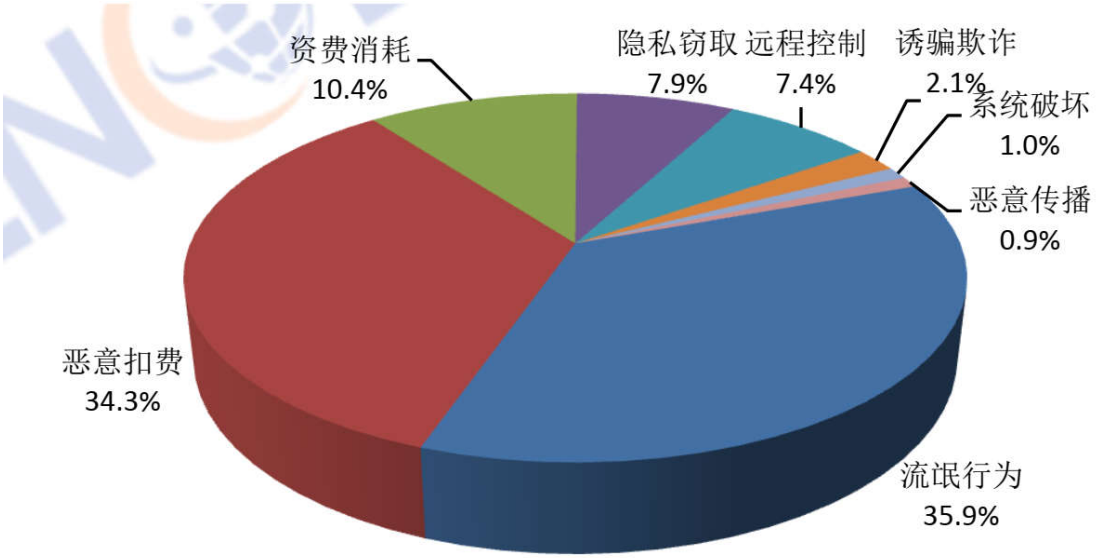


图 6 2017 年移动互联网恶意程序数量按行为属性统计

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

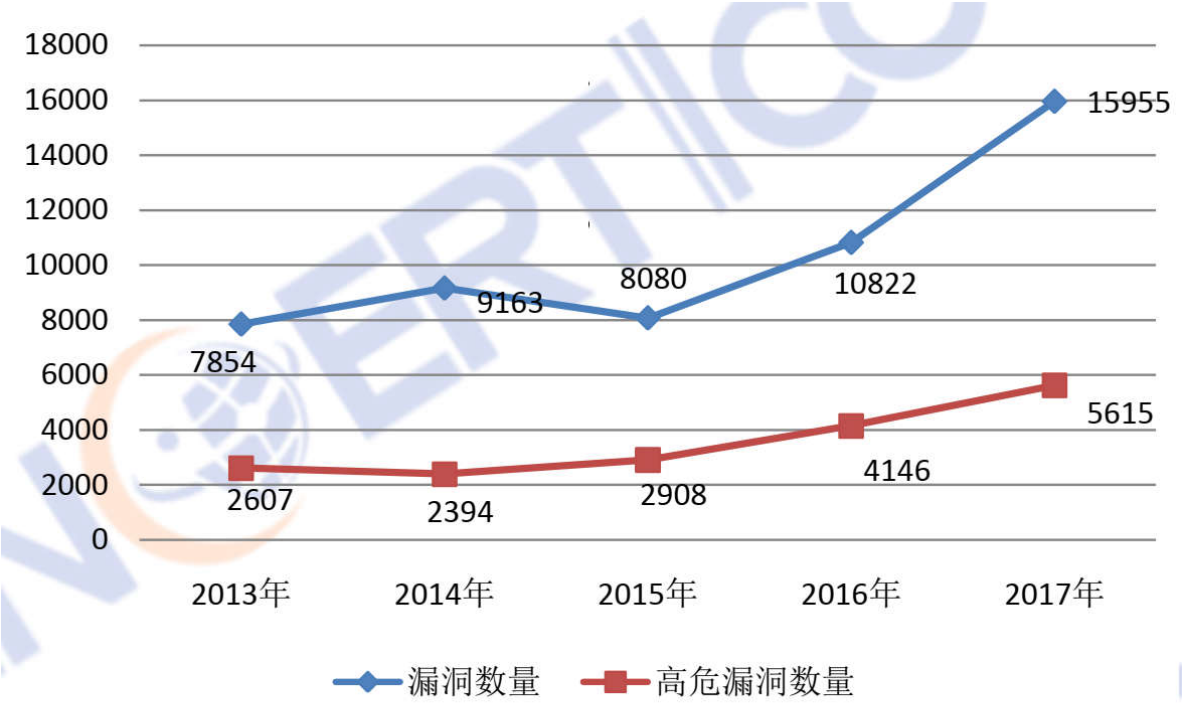


图 8 2013 年至 2017 年 CNVD 收录安全漏洞数量对比

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

表 2 2017 年 CNVD 收录漏洞涉及厂商情况统计

漏洞涉及厂商	漏洞数量（单位：个）	占全年收录数量百分比	环比
Google	1133	7.1%	38.3%
Oracle	775	4.9%	12.5%
Microsoft	674	4.2%	29.1%
IBM	574	3.6%	14.8%
Cisco	483	3.0%	36.7%
Apple	433	2.7%	-1.4%
WordPress	360	2.3%	54.5%
Adobe	350	2.2%	-37.6%
Huawei	296	1.9%	91.0%
ImageMagick	248	1.6%	/
Linux	228	1.4%	4.6%
其他	10401	65.2%	/

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

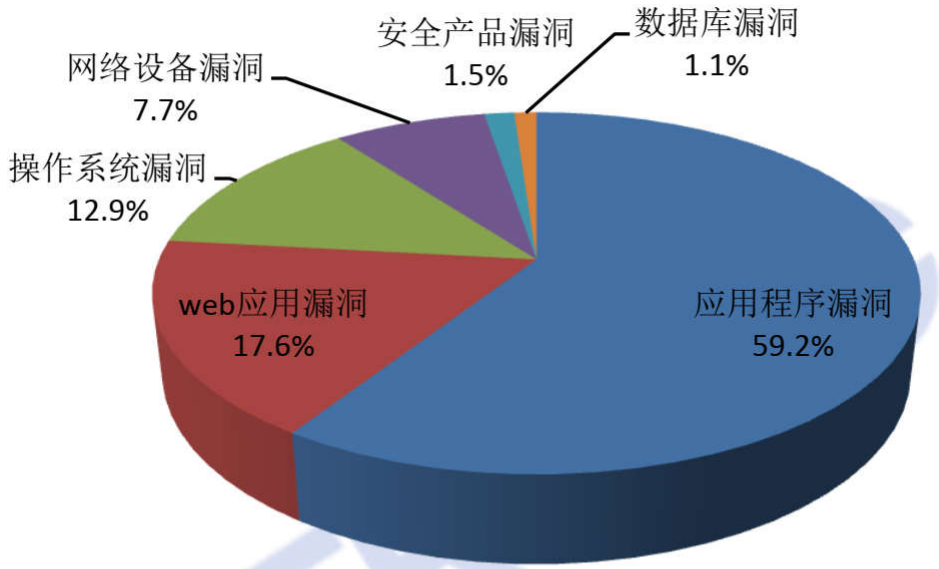


图 9 2017 年 CNVD 收录漏洞按影响对象类型分类统计

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

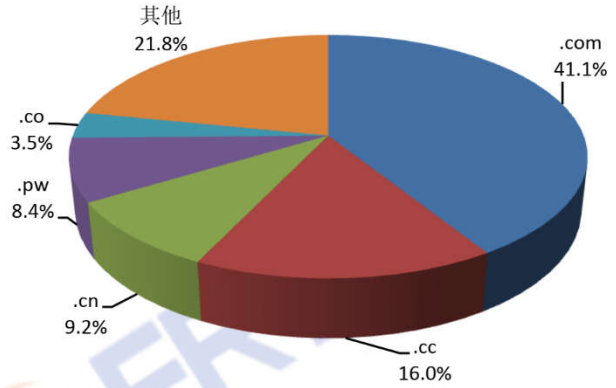


图 14 2017 年仿冒页面所用域名按顶级域分布

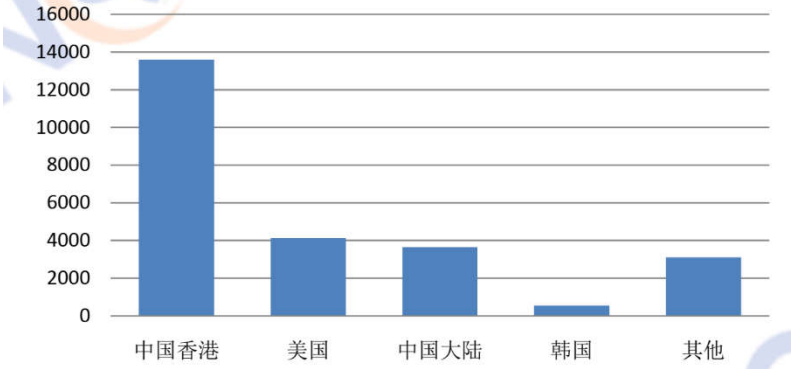


图 15 2017 年承载仿冒页面 IP 地址归属分布

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

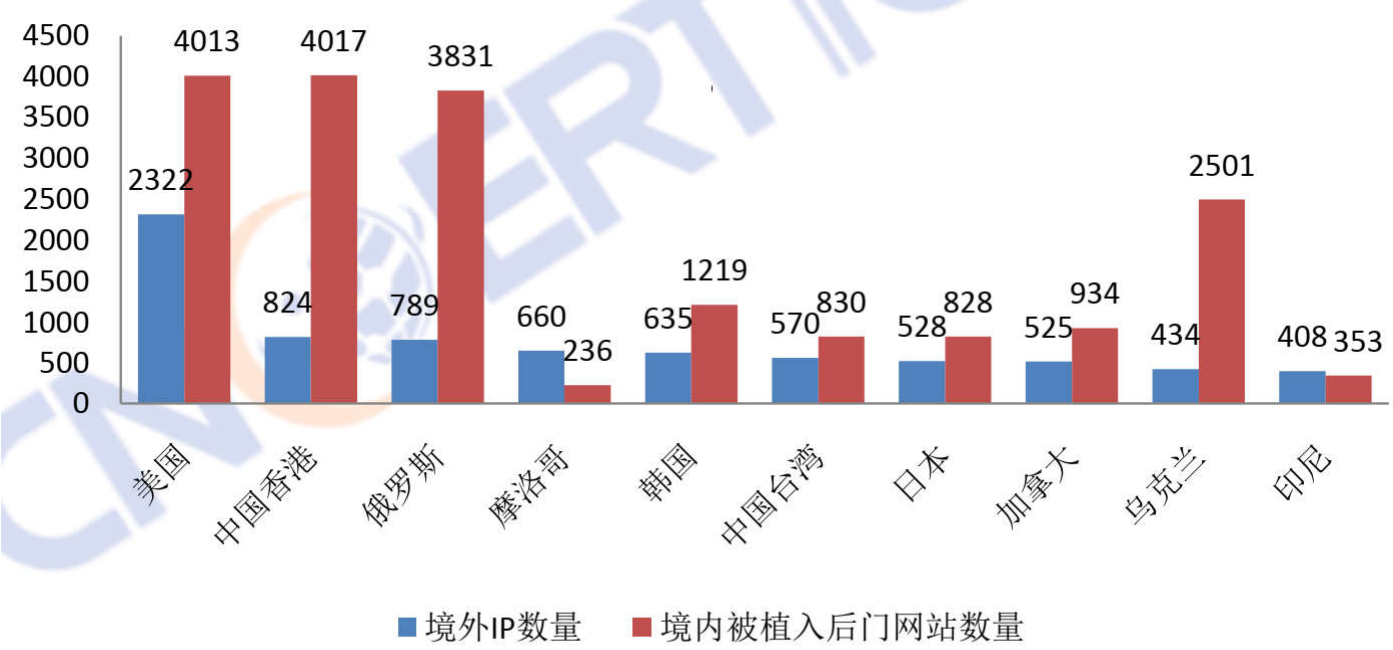


图 16 2017 年境外向我国境内网站植入后门 IP 地址所属国家或地区 TOP10

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

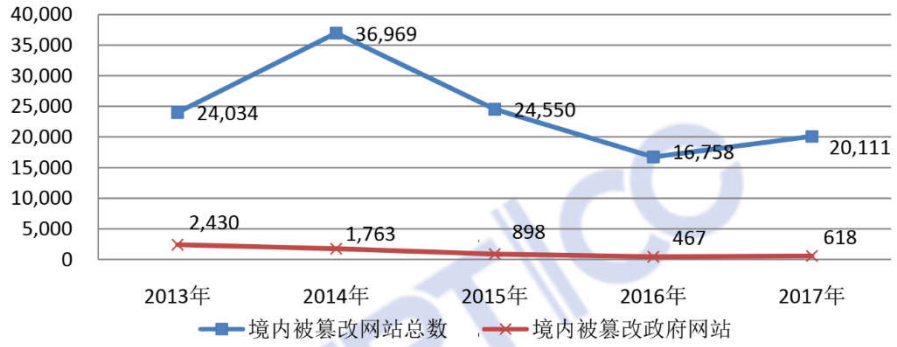


图 17 2013 年至 2017 年我国境内被篡改网站数量情况

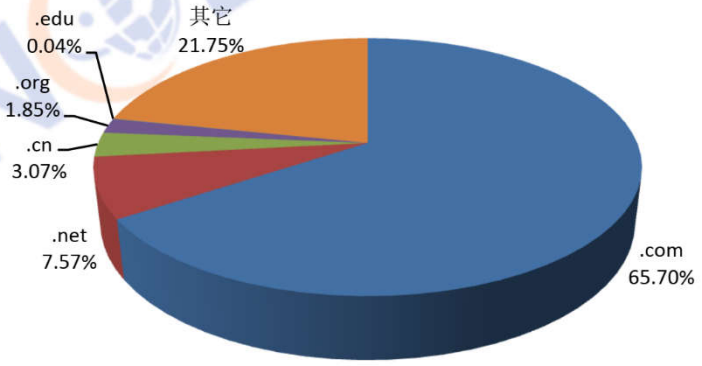


图 18 2017 年境内被篡改网站域名按顶级域分布

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

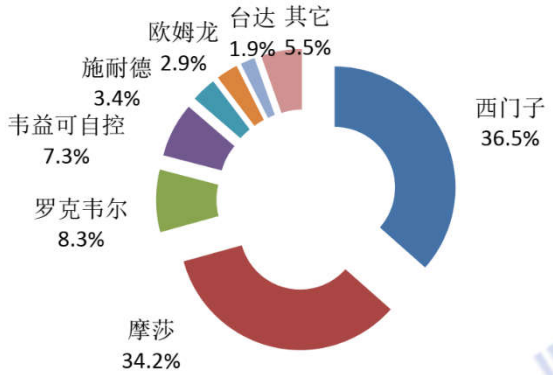


图 19 2017 年发现的联网工控设备厂商分布情况

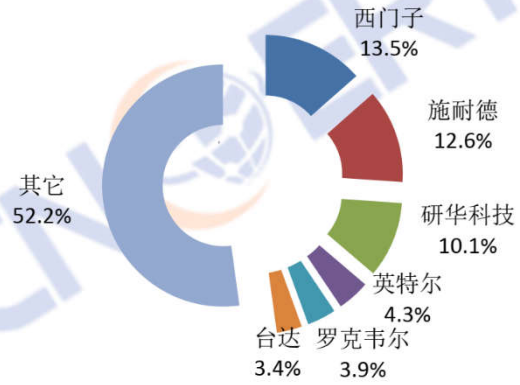


图 20 2017 年工控系统高危漏洞涉及厂商情况

1.1 Concepts of Information Security

1.1.1 The Situation of Information Security

- CNCERT/CC: Security Situation Report 2017

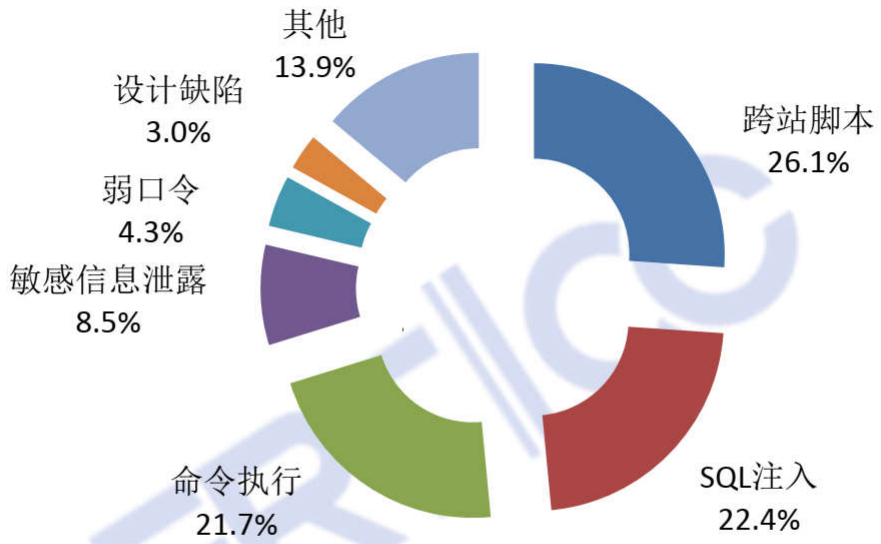


图 21 2017 年互联网金融网站高危漏洞类型分布

1.1 Concepts of Information Security

1.1.2 Definition of Information Security

- **Security**
  - Security
    - ✧ Security is freedom from, or resilience against, potential harm (or other unwanted coercive change) from external forces.
    - ✧ Security is “The quality or state of being secure — to be free from danger”．
  - Specialized areas of security in an organization
    - ✧ Physical security (物理安全)
    - ✧ Personal security (个人安全)
    - ✧ Operations security (运营安全)
    - ✧ Communications security (通信安全)
    - ✧ Network security (网络安全)
    - ✧ Information security (信息安全)

1.1 Concepts of Information Security

1.1.2 Definition of Information Security

- **Security**
  - Information Security
    - The importance or value of information comes from the characteristics it possesses
      - Availability, Accuracy, Authenticity, Confidentiality, Integrity, Utility, Possession.
    - Information security, shortened to ***InfoSec***, means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
    - From *Jim Anderson*:
      - Information security is a "well-informed sense of assurance that the information risks and controls are in balance."

1.1 Concepts of Information Security

1.1.2 Definition of Information Security

- **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。
    - ✧ 国际标准化组织 (ISO) 对于信息安全给出的定义是：为数据处理系统建立和采取的技术及管理保护，保护计算机硬件、软件、数据不因偶然及恶意的原因而遭到破坏、更改和泄漏。
      - ◌ 信息安全是指系统的硬件、软件及其信息受到保护，并持续正常地运行和服务。信息安全的实质是保护信息系统和信息资源免受各种威胁、干扰和破坏，即保证信息的安全性。主要目标是防止信息被非授权泄露、更改、破坏或被非法的系统辨识与控制，确保信息的保密性、完整性、可用性、可控性和可审查性 (信息安全5大特征)。

1.1 Concepts of Information Security

1.1.2 Definition of Information Security

- **Security**
  - Information Security
    - ✧ 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、防止未经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 Concepts of Information Security

1.1.2 Definition of Information Security

- **Security**
  - Information Security
    - ✧ 《中华人民共和国计算机信息系统安全保护条例》**第三条**：计算机信息系统的安全保护，应当保障计算机及其相关的配套设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统安全运行。(1984-2011)

1.1 Concepts of Information Security

1.1.2 Definition of Information Security

- **Security**
  - Information Security
    - ✧ "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2016)
      - ISO/IEC 27000:2016: Information technology — Security techniques — Information security management systems — Overview and vocabulary.
    - ✧ GB/T 29246-2017 /ISO/IEC 27000:2016，2018-07-01实施

1.1 Concepts of Information Security

1.1.2 Definition of Information Security

- **Security**
  - Information Security
    - ISO 信息安全管理体系标准族
      - ISO/IEC 27000 信息安全管理体系 概述和词汇 Overview and vocabulary
      - ISO/IEC 27001 信息安全管理体系 要求 Requirements
      - ISO/IEC 27002 信息安全控制实践指南
      - ISO/IEC 27003 信息安全管理体系实施指南
      - ISO/IEC 27004 信息安全管理 测量
      - ISO/IEC 27005 信息安全风险管理
      - ISO/IEC 27000 信息安全管理体系
      - 。 。 。

1.1 Concepts of Information Security

1.1.2 Definition of Information Security

- **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 Concepts of Information Security

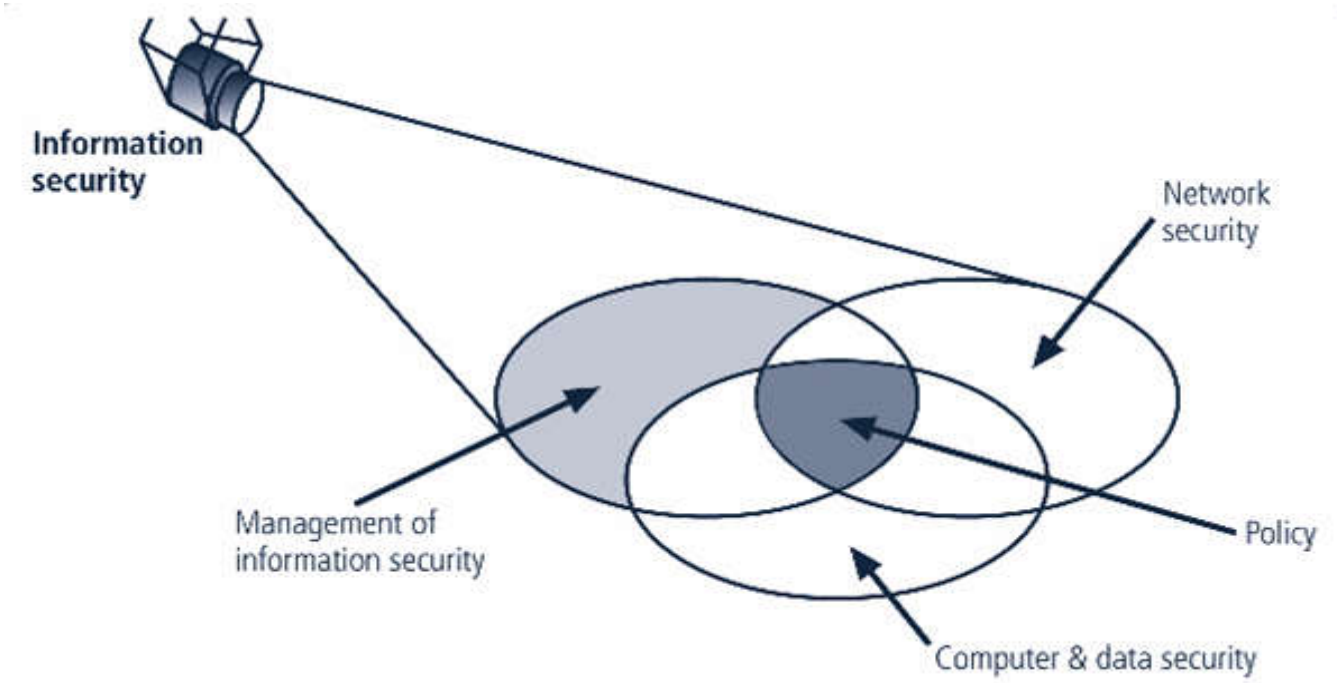
1.1.2 Definition of Information Security

- **Security**
  - InfoSec threats 信息安全威胁
    - ✧ 窃取 Steal：非法用户通过数据窃听的手段获得敏感信息。
    - ✧ 截取 Interception：非法用户首先获得信息，再将此信息发送给接收者。
    - ✧ 伪造 Forgery：将伪造的信息发送给接收者。
    - ✧ 篡改 Tampering：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 DoS：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 Repudiation：合法用户否认已经发生的行为。
    - ✧ 非授权访问 Unauthorized Access：未经系统授权而使用网络或计算机资源。
    - ✧ 传播病毒 Virus Transmission：通过网络传播计算机病毒。

1.1 Concepts of Information Security

1.1.2 Definition of Information Security

- **Security**
  - Components of InfoSec



1.1 Concepts of Information Security

1.1.3 History of Information Security

- **The origin of InfoSec**
  - Ancient and early modern times
    - ✧ 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 Concepts of Information Security

1.1.3 History of Information Security

- **The origin of InfoSec**
  - Deriving 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 Concepts of Information Security

1.1.3 History of Information Security

- **The development of InfoSec**
  - 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 Concepts of Information Security

1.1.3 History of Information Security

- **The development of InfoSec**
  - R-609
    - ✧ Information security began with Rand Report R-609 (paper that started the study of computer security)
      - ◌ The RAND Corporation (兰德公司) is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.
    - ✧ 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 Concepts of Information Security

1.1.3 History of Information Security

- **The development of InfoSec**
  - 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 Concepts 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 Concepts of Information Security

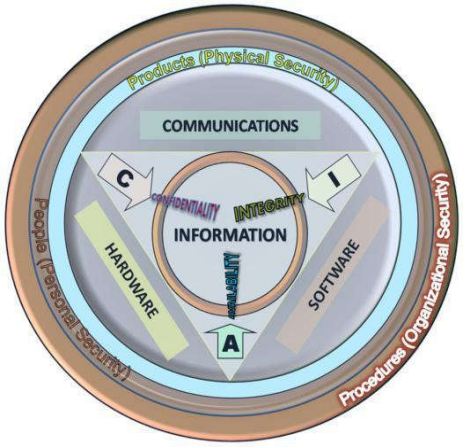
1.1.4 Key Concepts of Information Security

- **CIA triad**
  - The core principles of InfoSec
    - For over twenty years, information security has held **confidentiality**, **integrity** and **availability**, the **CIA** triad, to be the core principles of information security.
  - Confidentiality 保密性
    - Data confidentiality: assures that confidential information is not disclosed to unauthorized individuals
    - Privacy: concerns exist wherever sensitive information is collected, stored, used, destroyed or deleted – in digital form or otherwise.

1.1 Concepts of Information Security

1.1.4 Key Concepts of Information Security

- **CIA triad**
  - Integrity 完整性
    - ✧ 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 可用性
    - ✧ Assure that systems works promptly and service is not denied to authorized users.



1.1 Concepts of Information Security

1.1.4 Key Concepts of Information Security

- **Other concepts to a complete security picture**
  - Authenticity 认证性
    - ✧ 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 可审计性
    - ✧ Generates the requirement for actions of an entity to be traced uniquely to that individual to support non-repudiation, deference, fault isolation, etc.
  - Non-repudiation 不可抵赖性
    - ✧ Services that provide proof of the integrity and origin of data, or an authentication that can be said to be genuine with high confidence.
  - Reliability 可靠性
  - ref. to Sec.1.3.2

1.1 Concepts of Information Security

1.1.4 Key Concepts of Information Security

- 一些术语的解释
  - 真实性
    - ✧ 判断信息的真实来源，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。

1.1 Concepts of Information Security

1.1.4 Key Concepts of Information Security

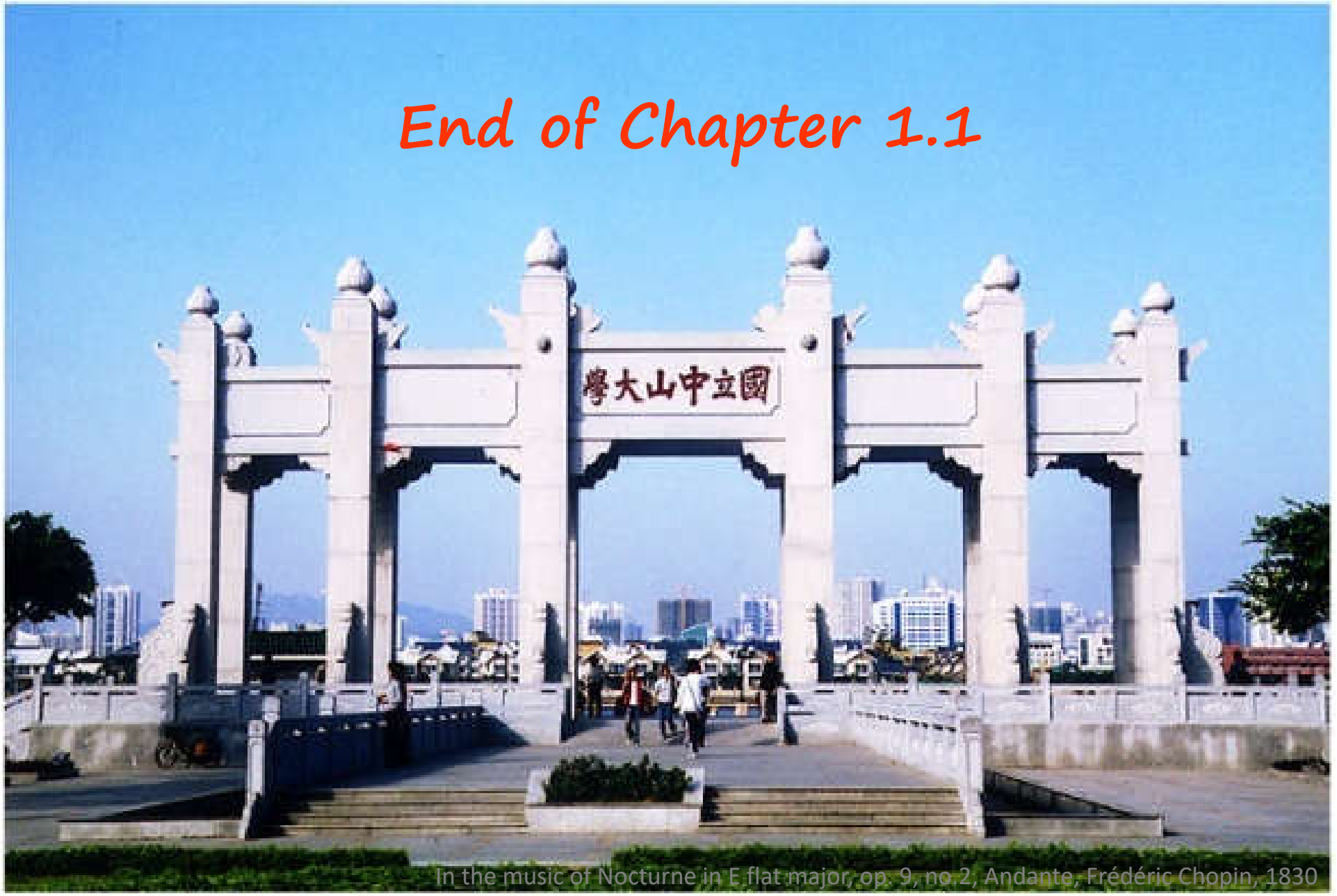
- 一些术语的解释
  - 可控制性
    - ✧ 对信息的传播及内容具有控制能力。
  - 可审查性/可审计性
    - ✧ 对出现的网络安全问题提供调查的依据和手段。

1.1 Concepts 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