中山大學
SUN YAT-SEN UNIVERSITY

Module I. Fundamentals of Information Security

Chapter 1
Introduction to Information Security

Web Security: Theory & Applications

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

Outline

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

1.3 Information Security Services

1.3.1 Basic Concept

- **Information Security Services**
  - Organizations frequently must evaluate, select, and employ a variety of Information security services in order to maintain and improve their overall Information security programs.
  - Information security services (e.g., security policy development, intrusion detection support, etc.) may be offered by an Information group internal to an organization, or by a growing group of vendors
  - 信息安全服务可以由机构内部设立的专门信息小组提供，也可采用外购的形式。

1.3 Information Security Services

1.3.1 Basic Concept

- **Information Security Services**
  - Information Security Service Categories

Management Service	Techniques and concerns normally addressed by management in the organization's computer security program. They focus on managing the computer security program and the risk within the organization.
Operational Service	Services focused on controls implemented and executed by people (as opposed to systems). They often require technical or specialized expertise and rely on management activities and technical controls.
Technical Services	Technical services focused on security controls a computer system executes. These services are dependent on the proper function of the system for effectiveness.

1.3 Information Security Services

1.3.1 Basic Concept

- **Information Security Services**
  - 信息安全服务
    - ✧ 信息安全服务指适应安全管理的需要，为企业、政府提供全面或部分信息安全解决方案的服务。信息安全服务应当提供包含从宏观的安全体系策略规划到具体的技术解决措施。
    - ✧ 目前，国内机构中的信息安全建设多数处在初级阶段，缺乏合理规划和管理机制。国内的信息安全服务商提供的安全服务体系一般包括信息安全评估、加固、运维、教育培训、风险管理等。用户购买安全服务的直接动机是应付当前的安全事件、满足管理层的意志或减轻来自内外的舆论压力，服务形式内容和现实需求之间存在较大落差。

1.3 Information Security Services

1.3.1 Basic Concept

- **Information Security Services**
  - 信息安全服务
    - ✧ 当前的信息安全服务主要在技术方面提供对用户的帮助，对管理机制的影响有限。用户普遍遇到的最大问题是自身资源不足，亦即“安全管理员”的缺位，其次是对基本管理体系探索的需求。
    - ✧ 从用户的角度看，信息安全服务能带来的实际好处包括：弥补用户人力的不足；弥补用户技术的不足；弥补用户信息的不足；弥补用户管理思想的不足。这些服务内容主要通过服务团队特别是一线人员传递到用户的手中，服务人员的技术技能和态度将直接决定用户的收益。
    - ✧ 信息安全产品服务包括解决方案设计、安装调试、人员培训、系统升级、再服务，具有相当长的持续周期。

1.3 Information Security Services

1.3.1 Basic Concept

- **Information Security Management Tools**
  - Two important tools are metrics and service agreements.
    - *Metrics*
      - Metrics (度量) are a management tool that facilitates decision-making and accountability through practical and relevant data collection, data analysis, and performance data reporting.
    - *Service agreements*
      - A service agreement serves as the agreement between the service provider and the organization requesting the service.

1.3 Information Security Services

1.3.2 Basic Issues

- **Authentication**
  - In computing, e-Business and information security is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

1.3 Information Security Services

1.3.2 Basic Issues

- **Authentication**
  - 认证通过某种特征识别方法确认用户 (如雇员、代理、软件过程等) 身份，从而确定其权限和服务。
  - 基本认证方法：
    ① 双重认证。采用两种 (或以上) 形式的验证方法，如令牌、智能卡和仿生装置 (视网膜或指纹扫描器)
    ② 数字证书。用于检验用户身份的电子文件。数字证书通过授权购买，提供更强的访问控制，并具有很高的安全性和可靠性
    ③ 智能卡
    ④ 安全电子交易协议 (SET)

1.3 Information Security Services

1.3.2 Basic Issues

- **Access Control**
  - Access control is a system that enables an authority to control access to areas and resources in a given physical facility or computer-based information system. An access control system, within the field of physical security, is generally seen as the second layer in the security of a physical structure.

1.3 Information Security Services

1.3.2 Basic Issues

- **Access Control**
  - 访问控制
    - ✧ 访问控制是针对越权使用资源的防御措施，阻止未被授权的人员使用资源 (硬件如：处理器、路由器、存储器；软件如：系统软件、应用程序；信息资源如：数据文档、系统文档；网络资源如：局域网、因特网；服务资源如：计算、通信、电源)。
  - 访问控制的基本目标
    - ✧ 防止对任何资源进行未授权的访问，从而使计算机系统在合法范围内使用；决定用户被允许的行为，也决定代表一定用户的程序被允许的行为。

1.3 Information Security Services

1.3.2 Basic Issues

- **Access Control**
  - 访问控制对 CIA 的作用
    - ✧ 访问控制对机密性、完整性起直接的作用。
    - ✧ 访问控制通过对以下信息行为的有效控制来实现可用性：
      - ① 颁发影响网络可用性的网络管理指令
      - ② 占用资源
      - ③ 获得可以用于拒绝服务攻击的信息

1.3 Information Security Services

1.3.2 Basic Issues

- **Confidentiality**
  - Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.
  - Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

1.3 Information Security Services

1.3.2 Basic Issues

- **Integrity**
  - In information security, integrity means that data cannot be modified undetectably.
  - Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

1.3 Information Security Services

1.3.2 Basic Issues

- **Integrity**
  - 数据完整性
    - ✧ 数据完整性是信息安全的三个基本要点之一，指在传输、存储信息或数据的过程中，确保信息或数据不被未授权篡改或在篡改后能够迅速被发现。在信息安全领域使用过程中，常常和保密性边界混淆。
    - ✧ 以普通 RSA 对数值信息加密为例，黑客或恶意用户在没有获得密钥破解密文的情况下，可以通过对密文进行线性运算，相应改变数值信息的值。例如交易金额为X元，通过对密文乘2，可以使交易金额成为2X (也称为可延展性 malleability)。为解决以上问题，通常需要使用数字签名或散列函数对密文进行保护。

1.3 Information Security Services

1.3.2 Basic Issues

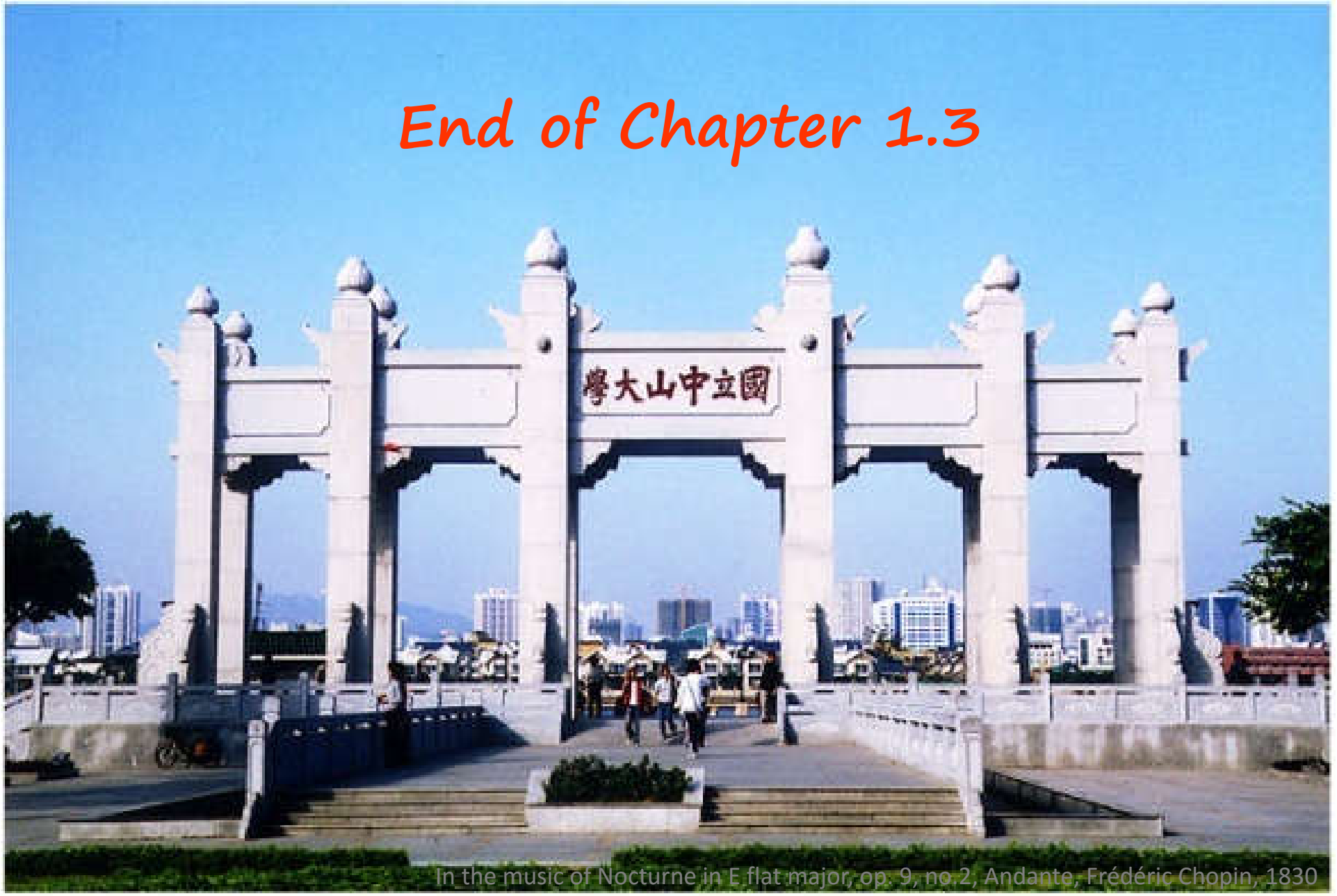
- **Availability**
  - For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

1.3 Information Security Services

1.3.2 Basic Issues

- **Non-repudiation**
  - In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.
  - Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

End of Chapter 1.3



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