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 Concept of Information Security
- **1.2 Computer System Security**
  - System Vulnerabilities
  - Operating System Security
  - Database Security
  - User Application Security
- 1.3 Information Security Service
- 1.4 Information Security Management, Audit and Protection
- 1.5 Conclusion

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Computer Security**
  - NIST, 1995
    - ✧ The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Computer Security**
  - Orange Book, 1983
    - ✧ Trusted Computer System Evaluation Criteria (TCSEC), frequently referred to as the Orange Book, is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system.
    - ✧ TCSEC is used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information.
    - ✧ TCSEC is the centerpiece of the DoD Rainbow Series publications, initially issued in 1983 by the National Computer Security Center (NCSC), an arm of the National Security Agency, and then updated in 1985. TCSEC was eventually replaced by the Common Criteria international standard, originally published in 2005.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Computer Security**
  - Common Criteria (CC)
    - ✧ The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) in version 3.1, originated out of ITSEC, CTCPEC and TCSEC, is for computer security.
    - ✧ CC is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) in a Security Target (ST), and may be taken from Protection Profiles (PPs). Vendors can then implement and/or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims.
    - ✧ CC provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Computer Security**
  - The Evaluation Assurance Level (EAL)
    - ✧ The Evaluation Assurance Level (EAL1 through EAL7) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria security evaluation. The increasing assurance levels reflect added assurance requirements that must be met to achieve Common Criteria certification. The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented. The EAL level does not measure the security of the system itself, it simply states at what level the system was tested.
    - ✧ To achieve a particular EAL, the computer system must meet specific assurance requirements. Most of these requirements involve design documentation, design analysis, functional testing, or penetration testing. The higher EALs involve more detailed documentation, analysis, and testing than the lower ones.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Computer Security**
  - 计算机系统安全包含两重含义
    - ✧ 系统可靠安全性 (或称系统安全性 System Safety)
    - ✧ 系统保密安全性 (或称系统安全 System Security，本课程内容)
    - ✧ 可靠安全性和保密安全性的区别在于是否存在专业人员对系统的恶意侵害、攻击和破坏。
  - System Safety
    - ✧ 系统安全性是系统在运行中避免造成不可接受的风险的能力。
      - ◌ 风险如人身伤亡、设备损坏、财产重大损失、环境严重污染等。
  - System Security
    - ✧ 系统安全是系统在受到恶意攻击的情形下依然能够继续正确运行，并确保系统资源在授权范围内能够合法使用的能力。

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **System Vulnerability**
  - What’s vulnerability
    - ✧ A vulnerability (脆弱性) is a flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy (which allows an attacker to reduce a system's information assurance).
    - ✧ Vulnerability is the intersection of three elements
      - A system susceptibility (易感性) or flaw
      - Attacker’s access to the flaw
      - Attacker’s capability to exploit the flaw
    - ✧ The most vulnerable point in most information systems is the human user, operator, designer, or other human
      - Humans should be considered in their different roles as asset, threat, information resources.
      - Social engineering is an increasing security concern.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **System Vulnerability**
  - 什么是系统脆弱性
    - ✧ 系统脆弱性 (或系统安全漏洞) 指应用软件或操作系统软件在逻辑设计上的缺陷或错误，这些缺陷或错误能够被不法者利用，通过植入木马、病毒等方式来攻击或控制系统，窃取重要资料和信息，甚至破坏整个系统。
    - ✧ 安全漏洞可能广泛存在于系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙中。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都可能存在各自不同的安全漏洞。

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **System Vulnerability**
  - Vulnerability may originate from
    - ✧ Complexity
    - ✧ Familiarity
    - ✧ Connectivity
    - ✧ Password management flaws
    - ✧ Fundamental operating system design flaws
    - ✧ Internet website browsing
    - ✧ Software bugs
    - ✧ Unchecked user input
    - ✧ Not learning from past mistakes
    - ✧ … …

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **System Vulnerability**
  - 安全漏洞的根源可能是：
    - ✧ 恶意：在程序编写过程，编程人员为实现不可告人的目的，在程序代码的隐蔽处保留后门。
    - ✧ 能力：系统结构设计和程序实现过程受到设计人员的能力、经验和当时安全技术所限制造成的缺陷。
    - ✧ 硬件问题：程序设计无法弥补硬件的漏洞，硬件的问题通过软件系统呈现。

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Computer Security Terminology**
  - Adversary (Threat agent, 敌方)
    - ✧ An entity that attacks, or is a threat to, a system
  - Attack (攻击)
    - ✧ An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.
    - ✧ On one trait: "Deliberateness" (故意性是其特点)
  - Countermeasure (对策)
    - ✧ An action, device, procedure, or technique that reduce a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Computer Security Terminology**
  - Risk (风险)
    - ✧ An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
  - Security Policy (安全策略)
    - ✧ A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

1.2 Computer System Security

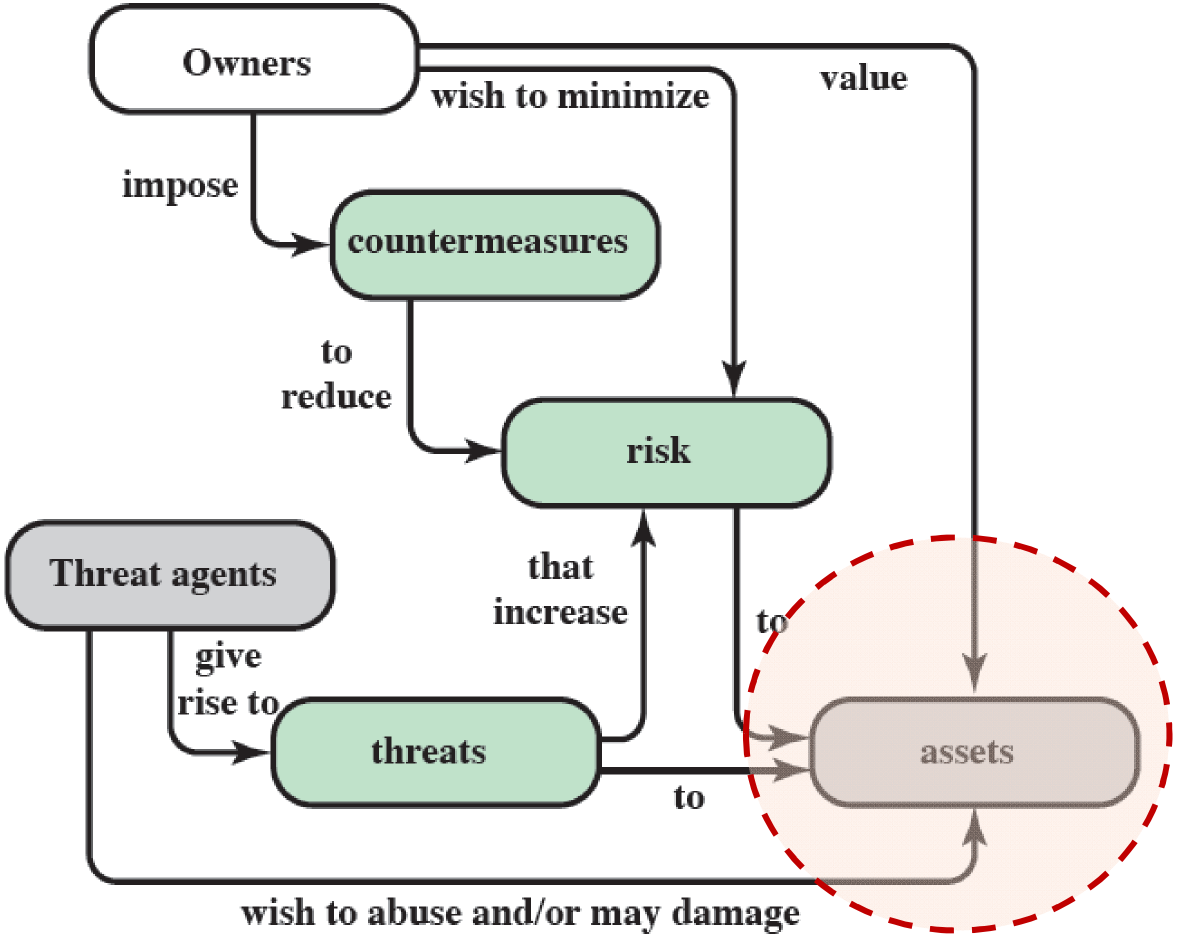
1.2.1 System Vulnerabilities

- **Computer Security Terminology**
  - System Resources (Asset, 信息资产)
    - ✧ Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component—hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.
  - Threat (威胁)
    - ✧ A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
    - ✧ A threat is a possible danger that might exploit a vulnerability.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Computer Security Concepts and Relationships**



1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Threat Consequence**
  - Unauthorized Disclosure 泄露
    - ✧ Description
      - ◌ A circumstance or event whereby an entity gains access to data for which the entity is not authorized.
    - ✧ Threat to
      - ◌ Confidentiality
    - ✧ Action
      - ◌ *Exposure* 披露
        - Sensitive data are directly released to an unauthorized entity.
      - ◌ *Interception* 截听/拦截
        - An unauthorized entity directly accesses sensitive data travelling between authorized sources and destinations.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Threat Consequence**
  - Unauthorized Disclosure 泄露
    - Action
      - *Inference* 推测
        - A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by products of communications.
      - *Intrusion* 入侵
        - An unauthorized entity gains access to sensitive data by circumventing (规避) a system’s security protections.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Threat Consequence**
  - Deception 欺骗
    - Description
      - A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.
    - Threat to
      - Integrity
    - Action
      - *Masquerade* 伪装
        - An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.
      - *Falsification* 欺骗
        - An entity deceives an authorized entity by false data.
      - *Repudiation* 抵赖/否认
        - An entity deceives another by falsely denying responsibility for an act.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Threat Consequences**
  - Disruption 搅扰/破坏
    - ✧ Description
      - ○ A circumstance or event that interrupts or prevents the correct operation of system services and functions.
    - ✧ Threat to
      - ○ Integrity and Availability
    - ✧ Action
      - ○ *Incapacitation* 失效
        - A threat action that prevents or interrupts system operation by disabling a system component.
      - ○ *Corruption* 损毁/侵蚀, backdoor logic
        - A threat action that undesirably alters system operation by adversely modifying system functions or data.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Threat Consequences**
  - Disruption 搅扰/破坏
    - ✧ Action
      - ○ *Obstruction* 阻碍/堵塞
        - A threat action that interrupts delivery of system services by hindering (妨碍) system operation.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Threat Consequences**
  - Usurpation 篡夺
    - ✧ Description
      - A circumstance or event that result in control of system services or functions by an unauthorized entity.
    - ✧ Threat to
      - Integrity
    - ✧ Action
      - *Misappropriation* 盗用
        - An entity assumes unauthorized logical or physical control of a system resource.
      - *Misuse* 误用/不当使用
        - A threat action that causes a system component to perform a function or service that is detrimental (有害于) to system security.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Examples of Threats to CIA Triad**
  - Hardware
    - Availability
      - Equipment is stolen or disabled, thus denying service.
    - Confidentiality
      - An unencrypted CD or DVD is stolen.
  - Software
    - Availability
      - Programs are deleted, denying access to users.
    - Confidentiality
      - An unauthorized copy of software is made.
    - Integrity
      - A working program is modified, either to cause it to fail during execution or to cause it to do some untended task.

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Examples of Threats to CIA Triad**
  - Data
    - ✧ Availability
      - ◌ Files are deleted, denying access to users.
    - ✧ Confidentiality
      - ◌ An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.
    - ✧ Integrity
      - ◌ Existing files are modified or new files are fabricated (伪造).

1.2 Computer System Security

1.2.1 System Vulnerabilities

- **Examples of Threats to CIA Triad**
  - Communication Lines and Networks
    - Availability
      - Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.
    - Confidentiality
      - Messages are read. The traffic pattern of messages is observed.
    - Integrity
      - Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

1.2 Computer System Security

1.2.2 Operating System Security

- **Operating System Security**
  - Components
    - Process Isolation and Memory Management (进程隔离和内存管理)
    - User Rights Management (用户权限管理)
    - Reference Monitor (访问监控器)
    - TCB (trusted computing base 可信计算基)
      - Not TPM. TCB is the set of all hardware, firmware, and/or software components that are critical to its security, in the sense that vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system.
  - Purpose
    - OS security is to provide users with a secure software environment to process information
  - Trusted Operation Systems
    - Our works on TPM

1.2 Computer System Security

1.2.3 Database Security

- **Database Security**
  - Description
    - ✧ Database security concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability.
  - Security Requirement
    - ✧ Confidentiality
    - ✧ Auditability
    - ✧ Access Control
    - ✧ User Authentication
    - ✧ Availability

1.2 Computer System Security

1.2.3 Database Security

- **Database Security**
  - 数据库系统安全
    - ✧ 数据库完整性
      - ○ 物理上的数据库完整性 (预防数据物理损毁) 和逻辑上的数据库完整性 (保持数据的结构)。
    - ✧ 数据库元素完整性
      - ○ 包含在每个记录中的数据是准确的。
    - ✧ 用户认证
      - ○ 确保每个用户身份被正确识别 (鉴证)，既便于审计追踪，也为了限制对特定的数据进行访问。

1.2 Computer System Security

1.2.3 Database Security

- **Database Security**
  - 数据库系统安全
    - 访问控制
      - 用户只能访问获得授权许可的数据；
      - 不同的用户有不同的访问模式。
        - 读、写、修改、删除、加密、转移等等。
    - 可获取性
      - 即可用性。授权用户可以访问数据库以及所有被批准访问的数据。
    - 可审计性
      - 能够对数据的访问行为进行追踪。

1.2 Computer System Security

1.2.3 Database Security

- **Database Security**
  - 数据库系统安全的含义
    - 系统运行安全
      - 法律、政策的保护；
        - 如用户是否有合法权利，政策是否允许等。
      - 物理控制安全；
        - 如机房加锁等。
      - 硬件运行安全；
      - 操作系统安全；
        - 如数据文件是否保护等。
      - 灾害、故障恢复；
      - 死锁的避免和解除；
      - 电磁信息泄漏防止。

1.2 Computer System Security

1.2.3 Database Security

- **Database Security**
  - 数据库系统安全的含义
    - ✧ 系统信息安全
      - ○ 用户口令字鉴别；
      - ○ 用户存取权限控制；
      - ○ 数据存取权限、方式控制；
      - ○ 审计跟踪；
      - ○ 数据加密。

1.2 Computer System Security

1.2.4 User Application Security

- **User Application Security**
  - Description
    - ✧ Application security encompasses measures taken throughout the application's life-cycle to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application.
  - Components
    - ✧ Web security
    - ✧ Data security
    - ✧ Software security
      - ◌ Our works on code obfuscation

1.2 Computer System Security

1.2.4 User Application Security

- **User Application Security**
  - 用户应用安全/应用程序安全性
    - ✧ 密码技术已经可以较为有效地解决对传输和存储状态下的数据安全保护。目前对应用程序安全性的威胁已远远超出了通过协议和密码系统进行数据寻址的威胁。应用程序安全性解决方案除了要对传统的网络和数据实施安全保护之外，还必须对软件本身实施安全保护。应用程序安全性必须建立在对系统或网络中的每个点上所存在的潜在威胁的深入了解之上，因此给实际实施带来很大困难。

1.2 Computer System Security

1.2.4 User Application Security

- **User Application Security**
  - 应用程序安全性的构成
    - ✧ 应用程序安全性由网络安全性、数据安全性和软件安全保护三部分构成。
    - ✧ 网络安全性
      - ◌ 防范外部攻击，防止内部保留资源通过网络向外提供服务。传统的确保网络安生性的方法通常是使用防火墙、入侵检测系统和病毒扫描。
    - ✧ 数据安全性
      - ◌ 对应用程序本地使用的数据或在用户和服务器之间传输的数据加以保护。密码可以有效地保护传输和存储状态下的数据，确保数据的完整性和机密性，因此密码技术是确保数据安全性最主要的解决方案。

1.2 Computer System Security

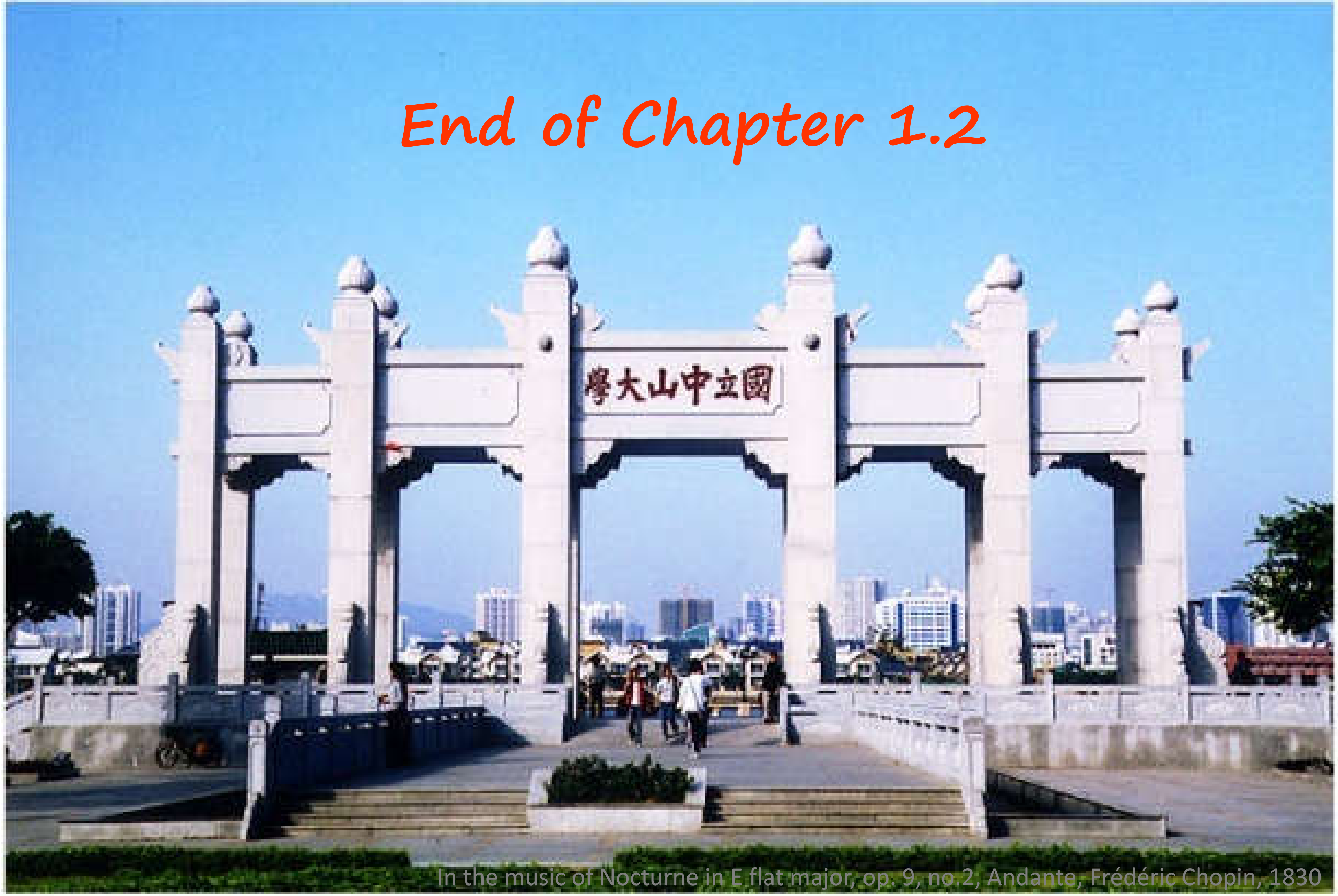
1.2.4 User Application Security

- **User Application Security**
  - 应用程序安全性的构成
    - ✧ 软件安全保护
      - ○ 对软件本身或软件所提供的服务加以保护以防止各类攻击，如防止对知识产权和许可内容的窃取，并确保软件的初始功能不被破坏。这一类的典型攻击包括逆向工程 (如反汇编、反编译、动态跟踪等)、篡改、非法复制等。

1.2 Computer System Security

1.2.5 Overall Strategies for Computer Security

- **An Overall Strategy for Providing Computer Security**
  - Policy (specs): what security schemes are supposed to do
    - ✧ Assets and their values
    - ✧ Potential threats
    - ✧ Ease of use vs. security
    - ✧ Cost of security vs. cost of failure/recovery
  - Implementation/mechanism: how to enforce
    - ✧ Prevention
    - ✧ Detection
    - ✧ Response
    - ✧ Recovery
  - Correctness/Assurance: does it really work
    - ✧ Validation/Review



End of Chapter 1.2

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