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
- 1.4 Information Security Management, Audit and Protection
- **1.5 Conclusion**

1.5 Conclusion

- The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure ...

— On War, *Carl Von Clausewitz*

- 孙子曰：昔之善战者，先为不可胜，以待敌之可胜；不可胜在己，可胜在敌。故善战者，能为不可胜，不能使敌之可胜。故曰：胜可知，而不可为。

不可胜者，守也；可胜者，攻也。守则不足，攻则有余。善守者，藏于九地之下；善攻者，动于九天之上，故能自保而全胜也。

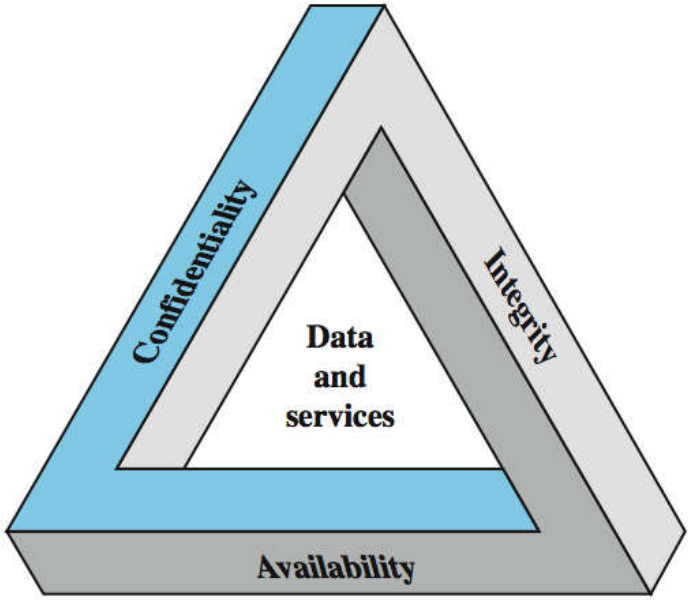
— 孙子兵法·军形篇

1.5 Conclusion

- **Standards Organizations**
  - National Institute of Standards & Technology (NIST)
  - Internet Society (ISOC)
  - International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
  - International Organization for Standardization (ISO)
  - International Electrotechnical Commission (IEC)
  - RSA Labs (de facto, 事实标准)
- **Computer Security**
  - 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)

1.5 Conclusion

- **Key Security Concepts**



1.5 Conclusion

- **Levels of Impact** – Low, Moderate, and High
  - **Low impact**
    - ✧ The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
    - ✧ A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might
      (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
      (ii) result in minor damage to organizational assets;
      (iii) result in minor financial loss; or
      (iv) result in minor harm to individuals.

1.5 Conclusion

- **Levels of Impact** – Low, Moderate, and High
  - **Moderate impact**
    - ✧ The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
    - ✧ A serious adverse effect means that, for example, the loss might
      (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
      (ii) result in significant damage to organizational assets;
      (iii) result in significant financial loss; or
      (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

1.5 Conclusion

- **Levels of Impact** – Low, Moderate, and High
  - **High impact**
    - ✧ The loss could be expected to have a severe or catastrophic (灾难性的) adverse effect on organizational operations, organizational assets, or individuals.
    - ✧ A severe or catastrophic adverse effect means that, for example, the loss might
      (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
      (ii) result in major damage to organizational assets;
      (iii) result in major financial loss; or
      (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

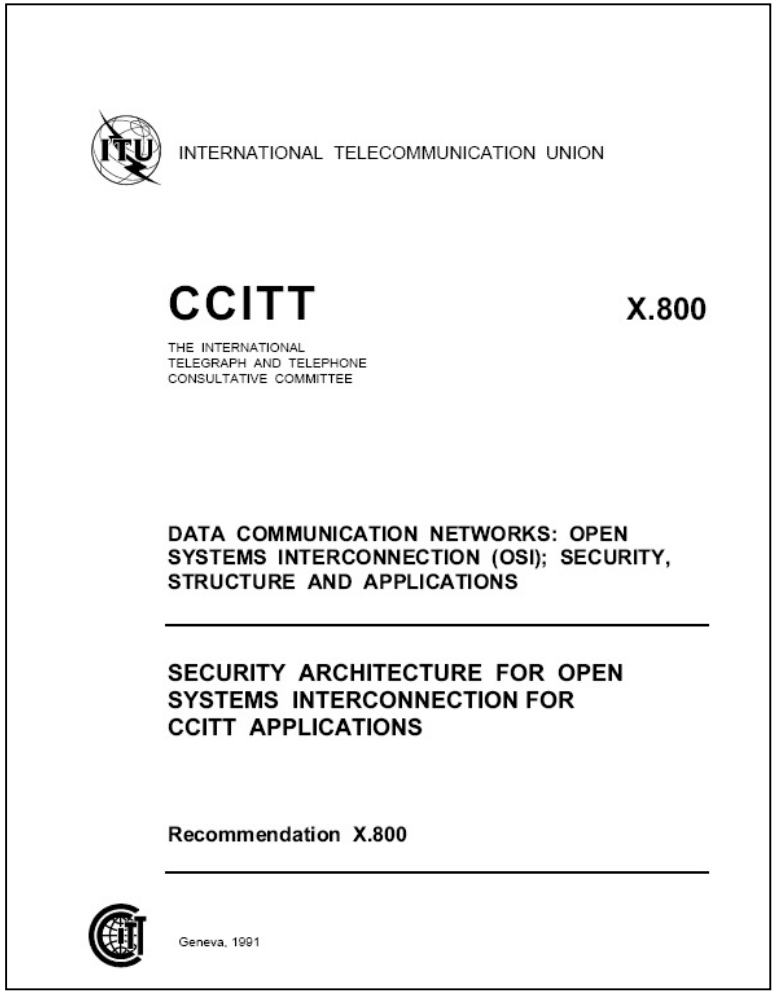
1.5 Conclusion

- **Computer Security Challenges**
  - the complexity
  - must consider potential attacks
  - procedures used counter-intuitive (非直观行为)
  - involve algorithms and secret infomation
  - must decide where to deploy mechanisms
  - battle of wits (斗智) between attacker / admin
  - not perceived (察觉) on benefit until fails
  - requires regular monitoring a process, not an event
  - too often an after-thought
  - regarded as impediment (碍事) to using system, “Unusable security is not secure”

1.5 Conclusion

- **OSI Security Architecture**
  - ITU-T X.800 “Security Architecture for OSI” (1991-1996)
    - ✧ defines a systematic way of defining and providing security requirements.
    - ✧ provides a useful, if abstract, overview of concepts we will study.

1.5 Conclusion



INTERNATIONAL TELECOMMUNICATION UNION

CCITT **X.800**

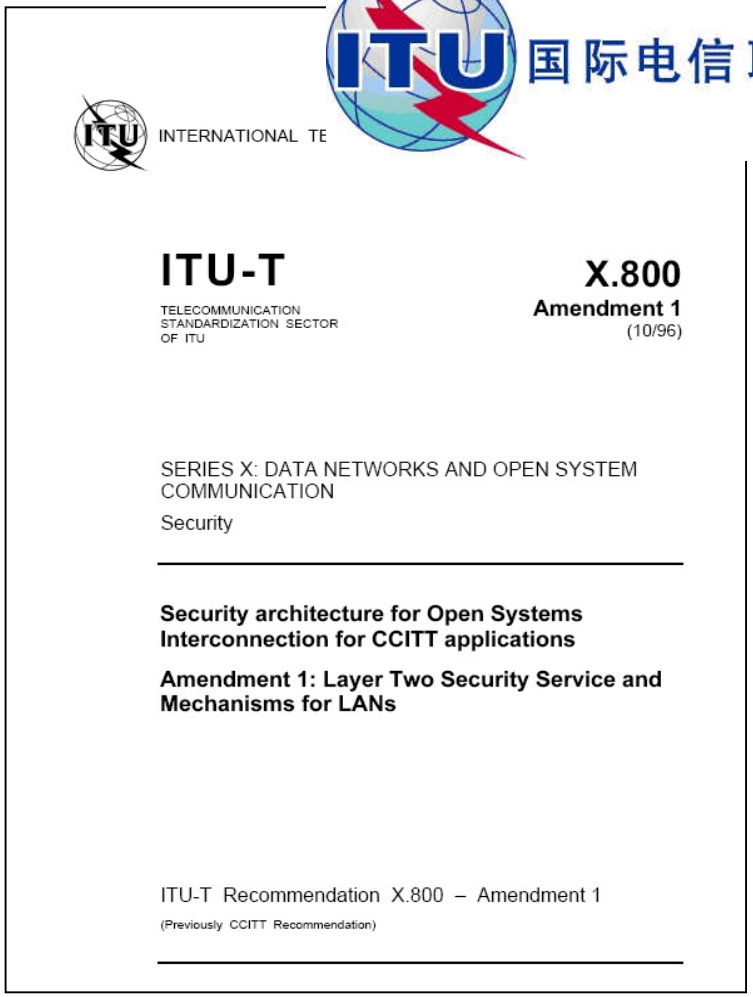
THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATIONS

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS

Recommendation X.800

Geneva, 1991



INTERNATIONAL TE

ITU-T **X.800**
Amendment 1
(10/96)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATION

Security

Security architecture for Open Systems Interconnection for CCITT applications

Amendment 1: Layer Two Security Service and Mechanisms for LANs

ITU-T Recommendation X.800 – Amendment 1

(Previously CCITT Recommendation)

1.5 Conclusion

- **OSI Security Architecture**
  - Series X: Data Networks and Open System Communication
    - ✧ **X.800** Security architecture for Open Systems Interconnection for CCITT applications
    - ✧ **X.802** Information technology - Lower layers security model
    - ✧ **X.803** Information technology - Open Systems Interconnection - Upper layers security model
    - ✧ **X.805** Security architecture for systems providing end-to-end communications

  - International Telephone and Telegraph Consultative Committee (CCITT, from French: Comité Consultatif International Téléphonique et Télégraphique 国际电话与电报顾问委员会) was created in 1956, and was renamed ITU-T (The ITU Telecommunication Standardization Sector) in 1993.

1.5 Conclusion

- **OSI Security Architecture**
  - Series X: Data Networks and Open System Communication
    - Information technology - Open Systems Interconnection - Security frameworks for open systems
      - **X.810** Overview
      - **X.811** Authentication framework
      - **X.812** Access control framework
      - **X.813** Non-repudiation framework
      - **X.814** Confidentiality framework
      - **X.815** Integrity framework
      - **X.816** Security audit and alarms framework

1.5 Conclusion

- **OSI Security Architecture**
  - Series X: Data Networks and Open System Communication
    - Information technology - Open Systems Interconnection - Generic upper layers security:
      - **X.830** Overview, models and notation
      - **X.831** Security Exchange Service Element (SESE) service definition
      - **X.832** Security Exchange Service Element (SESE) protocol specification
      - **X.833** Protecting transfer syntax specification
      - **X.834** Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma
      - **X.835** Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) proforma

1.5 Conclusion

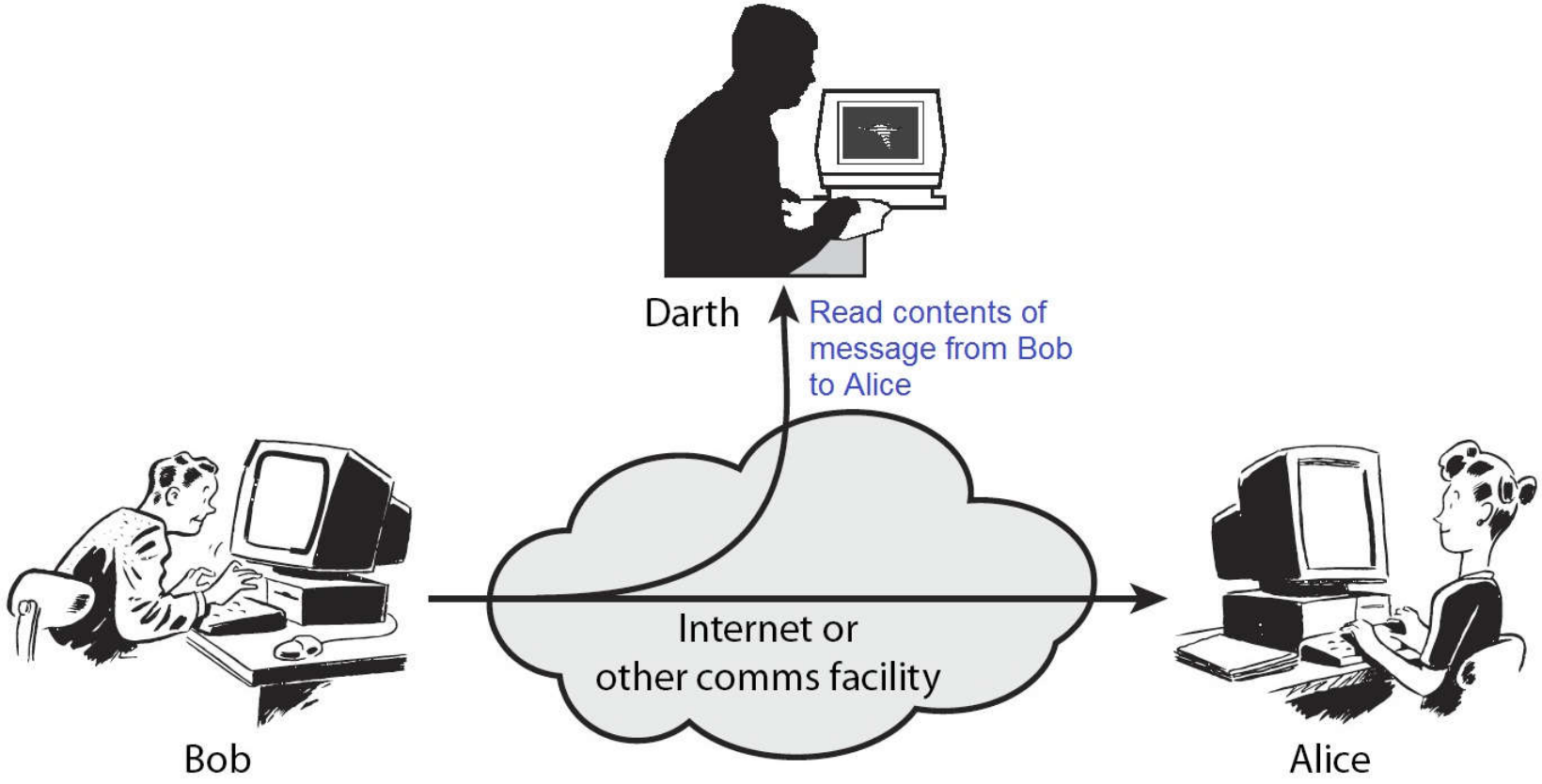
- **OSI Security Architecture**
  - Series X: Data Networks and Open System Communication
    - ✧ Information technology - Security techniques
      - ◌ **X.841** Security information objects for access control
      - ◌ **X.842** Guidelines for the use and management of trusted third party services
      - ◌ **X.843** Specification of TTP (Trusted Third Party) services to support the application of digital signatures
  - Ref. to ITU-T
    Data networks, open system communications and security:
    http://www.itu.int/rec/T-REC-X/en

1.5 Conclusion

- **Three Aspects** of information security
  - security attack
  - security mechanism (control)
  - security service
- **Note**
  - *vulnerability* – a way by which loss can happen
  - *threat* – a potential for violation of security
  - *attack* – an assault on system security, a deliberate attempt to evade security services
    - ✧ Passive attacks – focus on Prevention
      - ◌ Easy to stop; Hard to detect
    - ✧ Active attacks – focus on Detection and Recovery
      - ◌ Hard to stop; Easy to detect

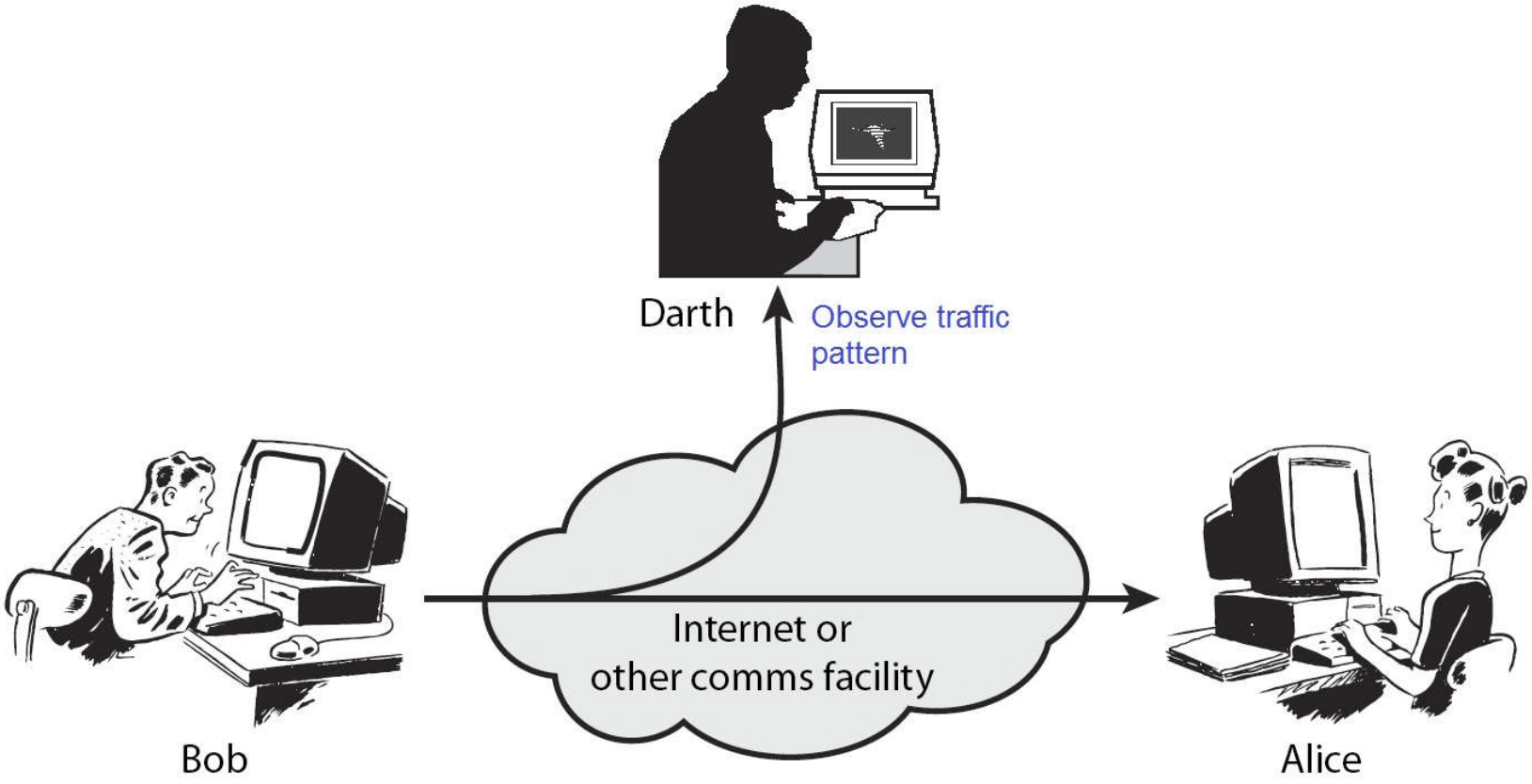
1.5 Conclusion

- **Example**
  - Passive Attack – Interception (窃听)



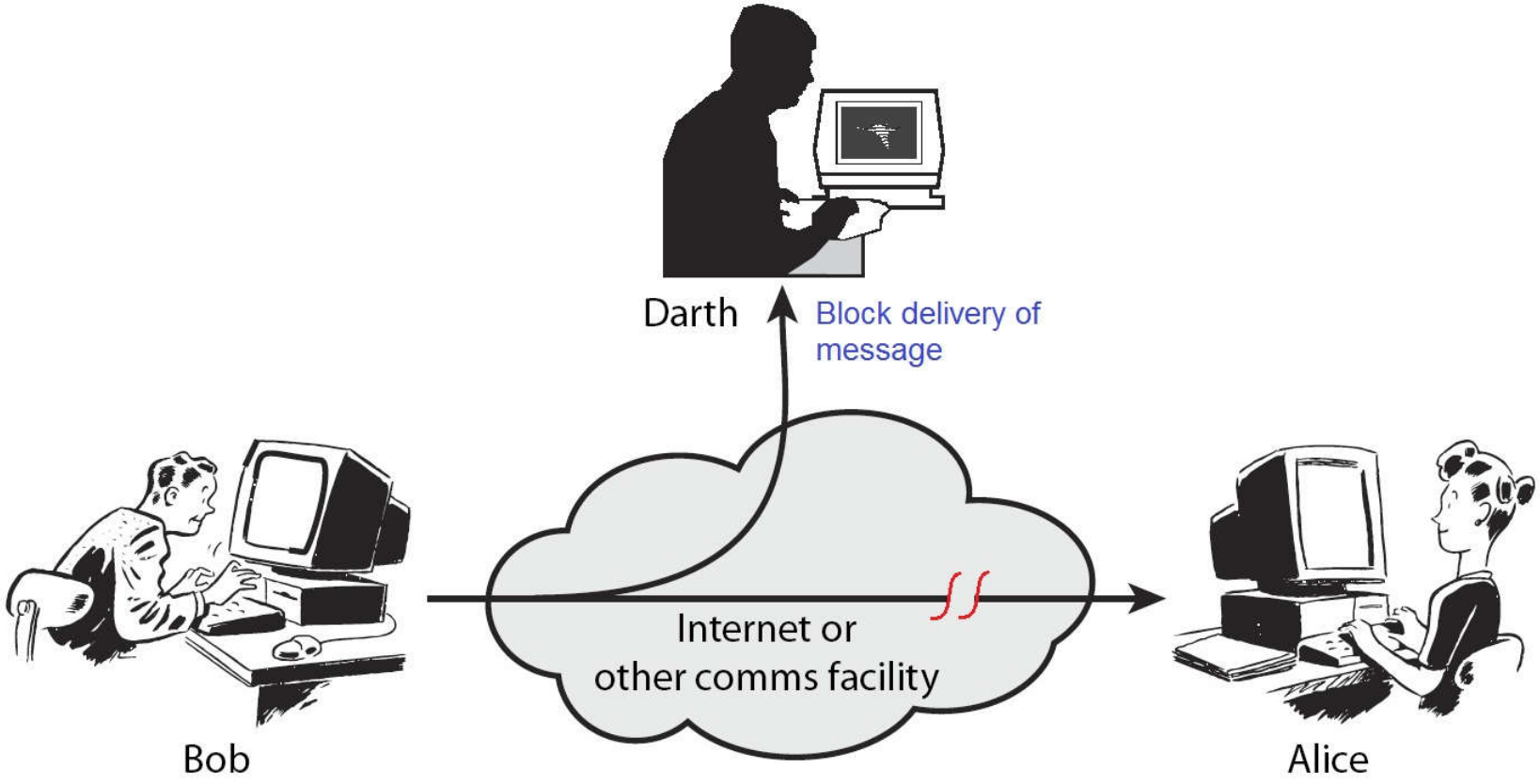
1.5 Conclusion

- **Example**
  - Passive Attack – Traffic Analysis (流量分析)



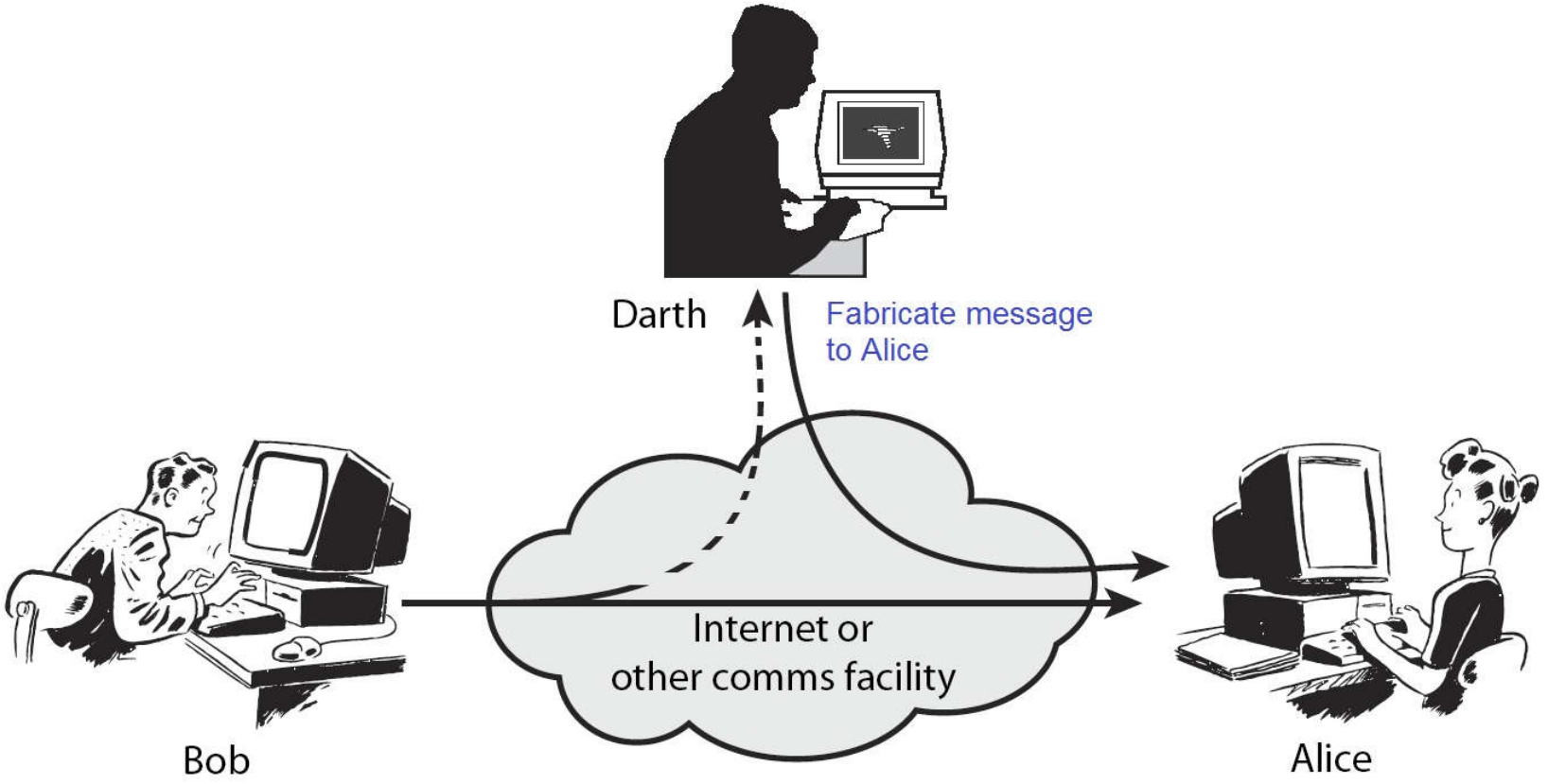
1.5 Conclusion

- **Example**
  - Active Attack – Interruption (截断)



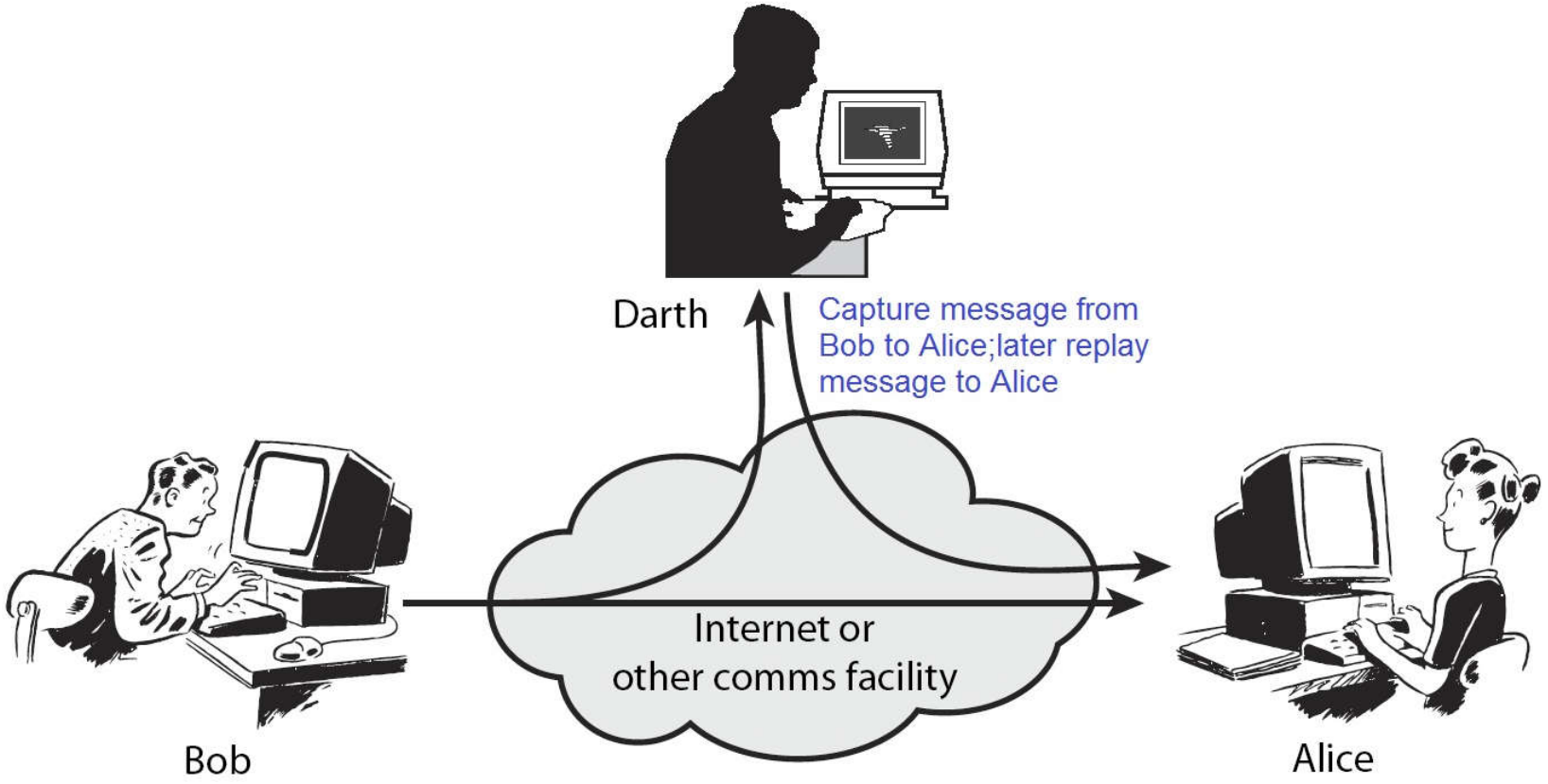
1.5 Conclusion

- **Example**
  - Active Attack – Fabrication (伪造)



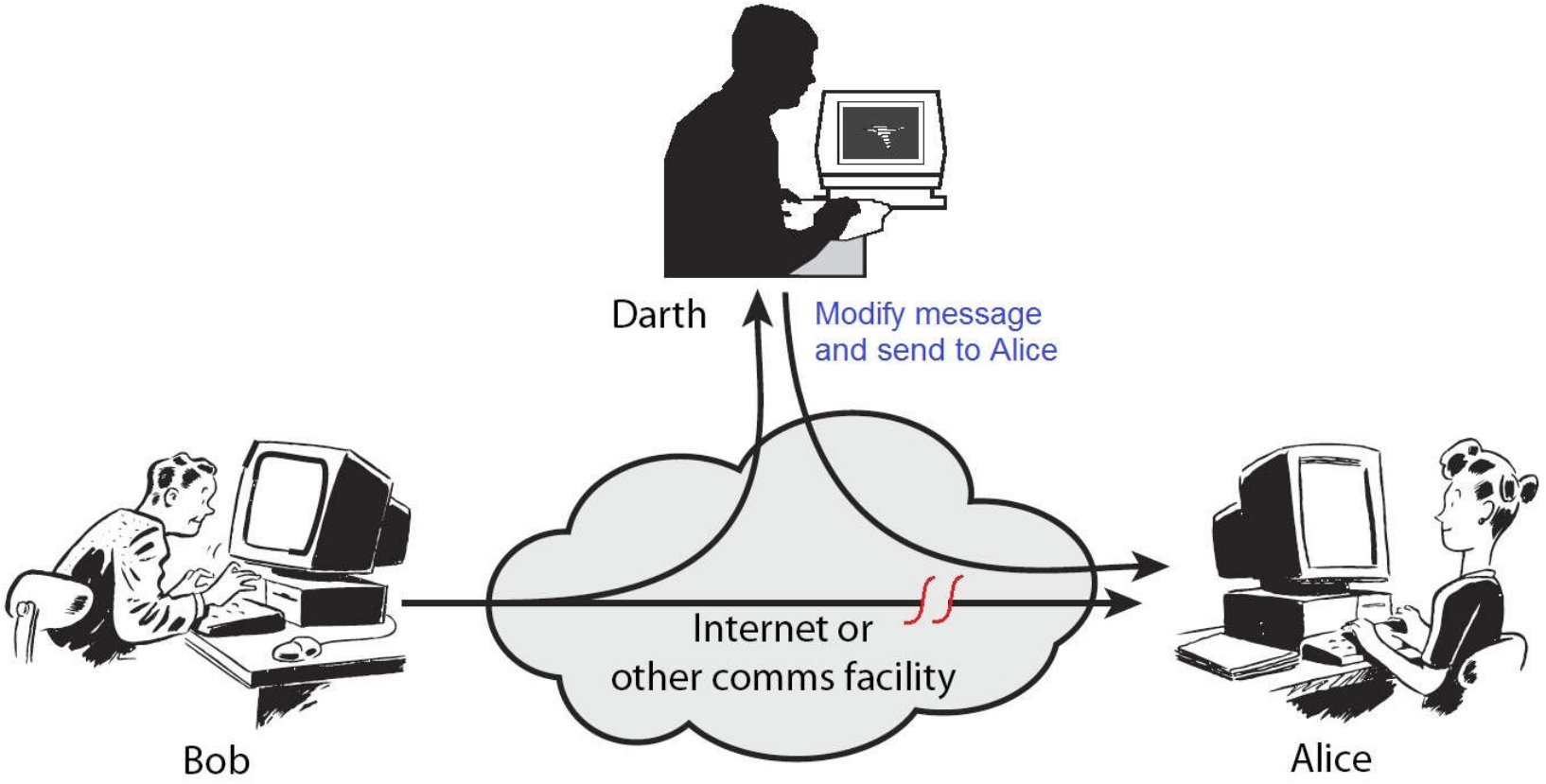
1.5 Conclusion

- **Example**
  - Active Attack – Replay (重放)



1.5 Conclusion

- **Example**
  - Active Attack – Modification/manipulation (篡改)



1.5 Conclusion

- **Attack Surface** (攻击截面)
  - The reachable and exploitable vulnerabilities in a system
    - Open ports
    - Services outside a firewall
    - An employee with access to sensitive info
    - . . .
  - The attack surface of a software environment is the sum of the different points (the “attack vectors”) where an unauthorized user (the “attacker”) can try to enter data to or extract data from an environment. (from Wikipedia)

1.5 Conclusion

- **Attack Surface**
  - The Attack Surface of an application is:
    - ✧ the sum of all paths for data/commands into and out of the application, and
    - ✧ the code that protects these paths (including resource connection and authentication, authorization, activity logging, data validation and encoding), and
    - ✧ all valuable data used in the application, including secrets and keys, intellectual property, critical business data, personal data, and
    - ✧ the code that protects these data (including encryption and checksums, access auditing, and data integrity and operational security controls).

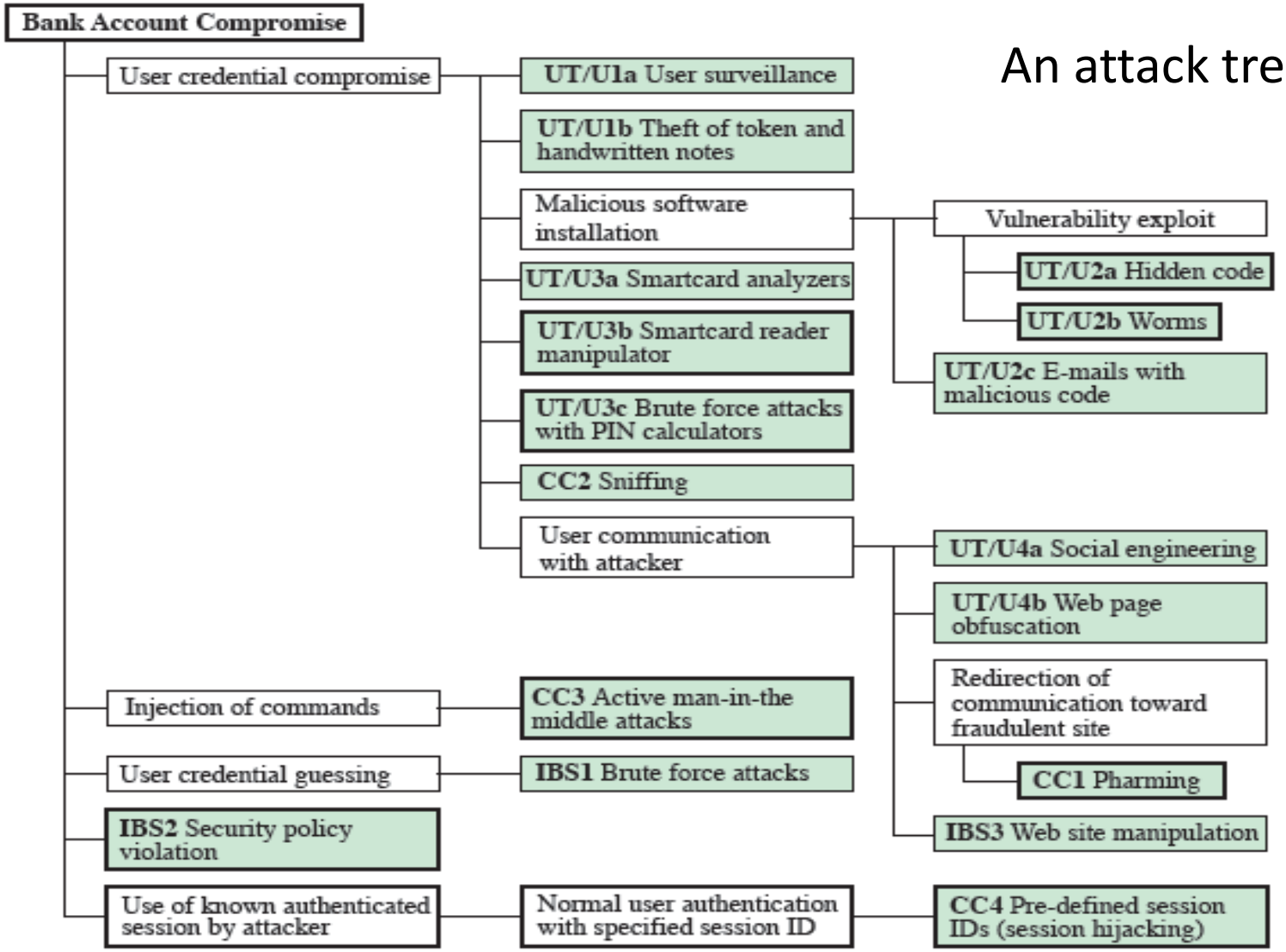
1.5 Conclusion

- **Attack Categories**
  - Network attack surface (i.e., network vulnerability).
  - Software attack surface (i.e., software vulnerabilities).
  - Human attack surface (e.g., social engineering).
- **Attack Analysis**
  - Assessing the scale and severity of threats (评估威胁的规模和严重程度).

1.5 Conclusion

- **Attack Trees**
  - A branching, hierarchical data structure that represents a set of potential vulnerabilities.
  - Objective: to effectively exploit the infomation available on attack patterns
    - ✧ published on CERT/CC or similar forums.
    - ✧ Security analysts can use the tree to guide design and strengthen countermeasures.

1.5 Conclusion



An attack tree

1.5 Conclusion

- **Security Service**
  - To enhance security of data processing systems and information transfers of an organization.
  - Intended to counter (对抗) security attacks.
  - Using one or more security mechanisms.
  - Often replicates functions normally associated with physical documents
    - ✧ which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed.
  - (通常用于重现一些与物理文档有关的属性，例如拥有签名和日期；防止泄露、窜改或毁坏；可用于公证或取证；可记录或授权)

1.5 Conclusion

- **Security Service** - X.800
  - Authentication - assurance that communicating entity is the one claimed
    - ✧ have both peer-entity & data origin authentication.
  - Access Control - prevention of the unauthorized use of a resource.
  - Data Confidentiality - protection of data from unauthorized disclosure.
  - Data Integrity - assurance that data received is as sent by an authorized entity.
  - Non-repudiation - protection against denial by one of the parties in a communication.
  - Availability - resource accessible/usable.

1.5 Conclusion

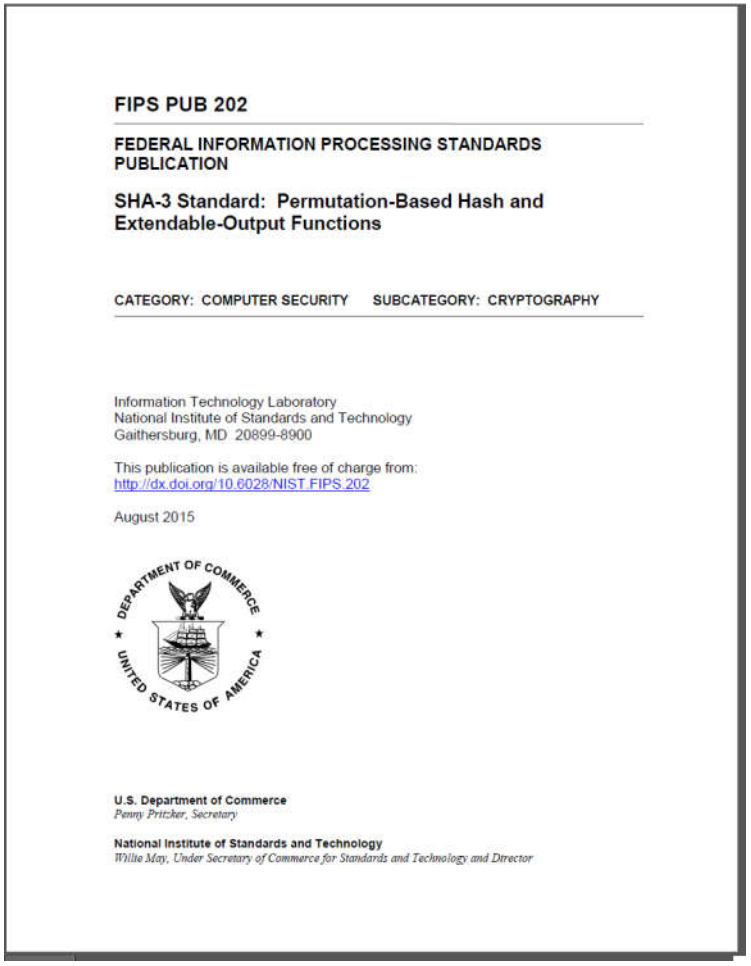
- **Security Mechanism**
  - aka **Control.**
  - feature designed to detect, prevent, or recover from a security attack.
  - no single mechanism that will support all services required.
  - however one particular element underlies many of the security mechanisms in use: *cryptographic techniques*

1.5 Conclusion

- **Security Mechanism -** X.800
  - specific security mechanisms:
    - ✧ encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization (公证机制).
  - pervasive (普适的) security mechanisms:
    - ✧ trusted functionality, security labels, event detection, security audit trails (追踪) , security recovery.

1.5 Conclusion

- **Security Functional Requirements** (NIST FIPS 202)
  - Federal Information Processing Standards, NIST 2015



FIPS PUB 202

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.FIPS.202

August 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

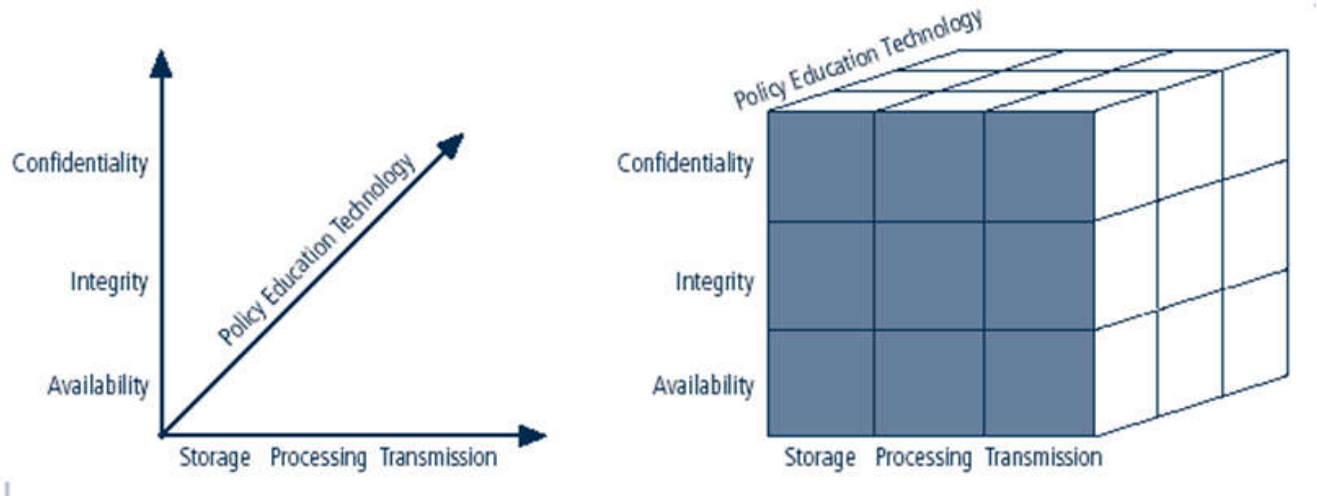
1.5 Conclusion

- **Security Functional Requirements** (NIST FIPS 202)
  - Federal Information Processing Standards, NIST 2015
  - Technical measures
    - ✧ Access control; identification & authentication; system & communication protection; system & information integrity.
  - Management controls and procedures
    - ✧ Awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition.
  - Overlapping technical and management
    - ✧ Configuration management; incident response; media protection.

  - NIST, National Institute of Standards and Technology, 美国国家标准与技术研究院
  - NBS (国家标准局), 1901 – NIST, 1988

1.5 Conclusion

- **NSTISSC Security Model**



  - NSTISSC: National Security Telecommunications and Information Systems Security Committee 美国国家安全通信与信息系统安全委员会

1.5 Conclusion

- **Fundamental Security Design Principles**
  - Despite years of research, it is still difficult to design systems that comprehensively prevent security flaws. But good practices for good design have been documented
    - ✧ analogous to software engineering (与软件工程类似), including economy of mechanism, fail-safe defaults, complete mediation, open design, separation of privileges, lease privilege, least common mechanism, psychological acceptability, isolation, encapsulation, modularity, layering, least astonishment.

1.5 Conclusion

- **Fundamental Security Design Principles**
  - Economy of mechanism
    - The design of security measures should be as simple as possible
      - Simpler to implement and to verify.
      - Fewer vulnerabilities.
  - Fail-safe default
    - Access decisions should be based on permissions; i.e., the default is lack of access.
  - Complete mediation (全面协调性)
    - Every access should checked against an access control system.
  - Open design
    - The design should be open rather than secret (e.g., encryption algorithms).
  - Separation of privilege
    - multiple privileges should be needed to do achieve access (or complete a task).

1.5 Conclusion

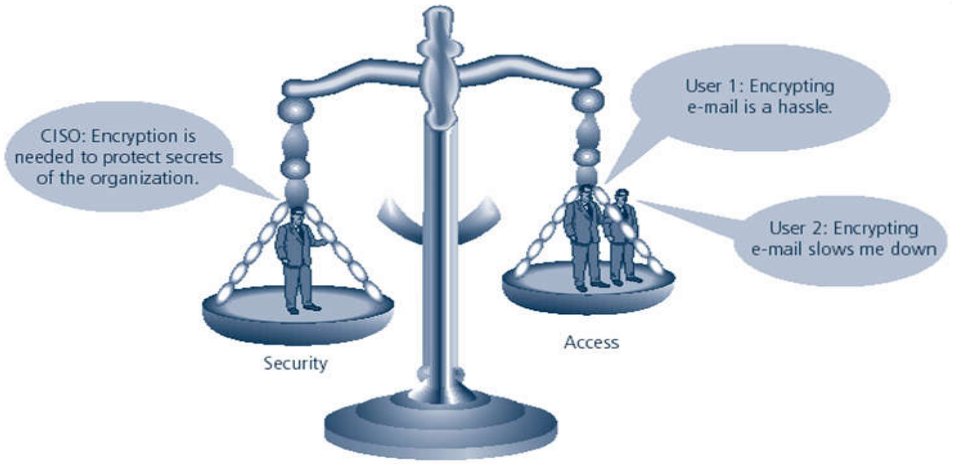
- **Fundamental Security Design Principles**
  - Least privilege
    - ✧ every user (process) should have the least privilege to perform a task.
  - Least common mechanism
    - ✧ a design should minimize the function shared by different users (providing mutual security; reduce deadlock).
  - Isolation
    - ✧ Public access should be isolated from critical resources (no connection between public and critical information).
    - ✧ Users files should be isolated from one another (except when desired).
    - ✧ Security mechanism should be isolated (i.e., preventing access to those mechanisms).

1.5 Conclusion

- **Fundamental Security Design Principles**
  - Psychological acceptability (心理可接受)
    - ✧ security mechanisms should not interfere unduly with the work of users.
  - Encapsulation (封装)
    - ✧ similar to object concepts (hide internal structures).
  - Modularity (模块化)
    - ✧ modular structure.
  - Layering (defense in depth)
    - ✧ use of multiple, overlapping protection approaches.
  - Least astonishment
    - ✧ a program or interface should always respond in a way that is least likely to astonish a user.
    - ✧ Aka the principle of least astonishment

1.5 Conclusion

- **Balancing Information Security and Access**
  - Impossible to obtain perfect security
    - ✧ it is a process, not an absolute
  - Security should be considered balance between protection and availability
  - To achieve balance, level of security must allow reasonable access, yet protect against threats

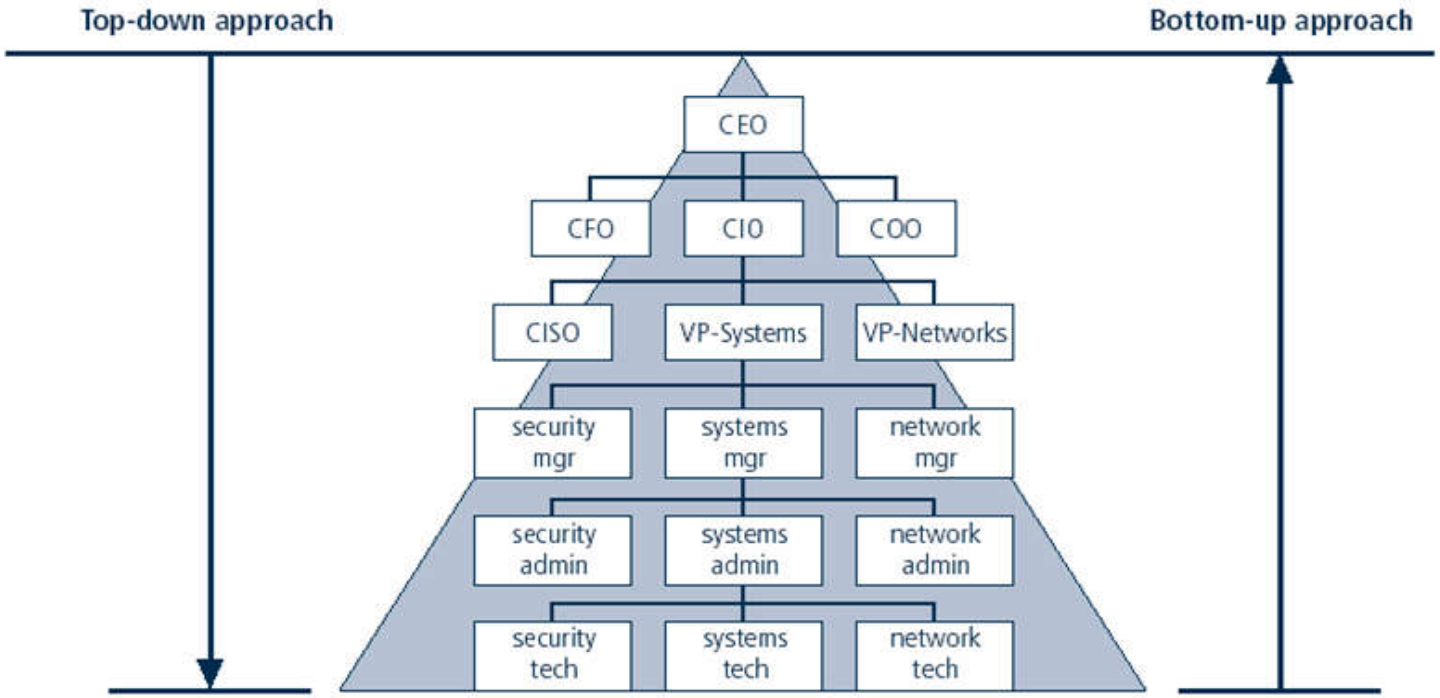


1.5 Conclusion

- **Information Security Implementation**
  - Bottom-Up Approach
    - ✧ Grassroots effort: systems administrators attempt to improve security of their systems.
    - ✧ Key advantage: technical expertise of individual administrators.
    - ✧ Seldom works (不太见效), as it lacks a number of critical features:
      - ◌ Participant support
      - ◌ Organizational staying power
  - Top-Down Approach
    - ✧ Initiated by upper management
      - ◌ Issue policy, procedures and processes.
      - ◌ Dictate goals and expected outcomes of project.
      - ◌ Determine accountability for each required action.
  - The most successful also involve formal development strategy referred to as systems development life cycle.

1.5 Conclusion

- **Information Security Implementation**
  - Bottom-Up & Top-Down Approach

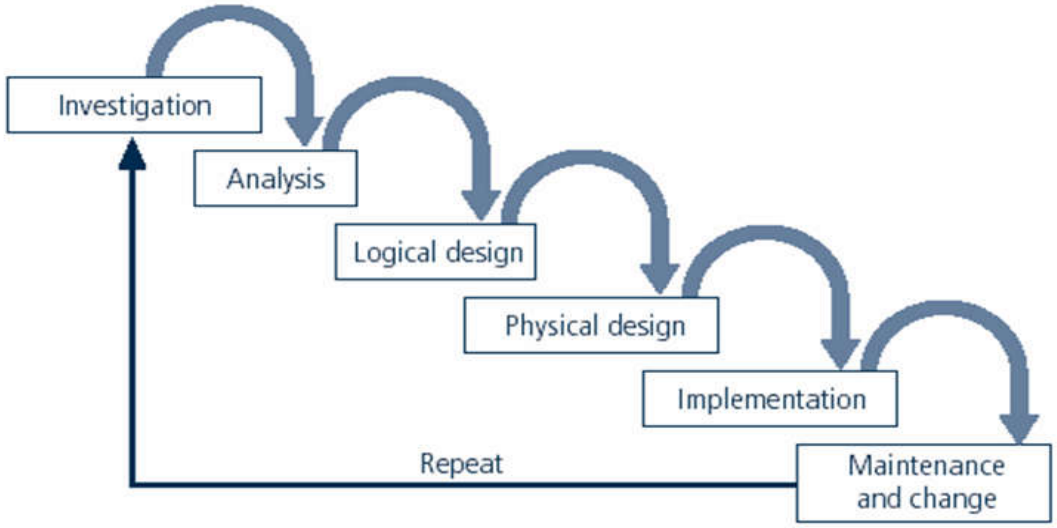


1.5 Conclusion

- **The Security Systems Development Life Cycle**
  - The Systems Development Life Cycle (SDLC)
    - ✧ Systems development life cycle (SDLC) is methodology and design for implementation of information security within an organization.
    - ✧ Methodology is formal approach to problem-solving based on structured sequence of procedures.
    - ✧ Using a methodology
      - ◌ ensures a rigorous process
      - ◌ avoids missing steps
    - ✧ Goal is creating a comprehensive security posture/program.
    - ✧ Traditional SDLC consists of six general phases.

1.5 Conclusion

- **The Security Systems Development Life Cycle**
  - The Systems Development Life Cycle (SDLC)



SDLC Waterfall Methodology

1.5 Conclusion

- **The Security Systems Development Life Cycle**
  - The Systems Development Life Cycle (SDLC)
    - Investigation
      - What problem is the system being developed to solve?
      - Objectives, constraints and scope of project are specified.
      - Preliminary cost-benefit analysis (成本收益分析) is developed.
      - At the end, feasibility analysis (可行性分析) is performed to assess economic, technical, and behavioral feasibilities of the process.
    - Analysis
      - Consists of assessments of the Organization, status of current systems, and capability to support proposed systems.
      - Analysts determine what new system is expected to do and how it will interact with existing systems.
      - Ends with documentation of findings and update of feasibility analysis.

1.5 Conclusion

- **The Security Systems Development Life Cycle**
  - The Systems Development Life Cycle (SDLC)
    - Logical Design
      - Main factor is business need; applications capable of providing needed services are selected.
      - Data support and structures capable of providing the needed inputs are identified.
      - Technologies to implement physical solution are determined.
      - Feasibility analysis performed at the end.
    - Physical Design
      - Technologies selected to support the alternatives identified and evaluated in the logical design.
      - Components evaluated on make-or-buy decision.
      - Feasibility analysis performed; entire solution presented to end-user representatives for approval.

1.5 Conclusion

- **The Security Systems Development Life Cycle**
  - The Systems Development Life Cycle (SDLC)
    - Implementation
      - Needed software created; components ordered, received, assembled, and tested.
      - Users trained and documentation created.
      - Feasibility analysis prepared; users presented with system for performance review and acceptance test.
    - Maintenance and Change
      - Consists of tasks necessary to support and modify system for remainder of its useful life.
      - Life cycle continues until the process begins again from the investigation phase.
      - When current system can no longer support the organization's mission, a new project is implemented.

1.5 Conclusion

- **The Security Systems Development Life Cycle**
  - The Security Systems Development Life Cycle (SecSDLC)
    - ✧ The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project.
    - ✧ Identification of specific threats and creating controls to counter them.
    - ✧ SecSDLC is a coherent program (连贯的过程) rather than a series of random, seemingly unconnected actions.

1.5 Conclusion

- **The Security Systems Development Life Cycle**
  - The Security Systems Development Life Cycle (SecSDLC)
    - Investigation
      - Identifies process, outcomes, goals, and constraints of the project
      - Begins with enterprise information security policy
      - Organizational feasibility analysis is performed
    - Analysis
      - Documents from investigation phase are studied
      - Analyzes existing security policies or programs, along with documented current threats and associated controls
      - Includes analysis of relevant legal issues that could impact design of the security solution
      - The risk management task begins

1.5 Conclusion

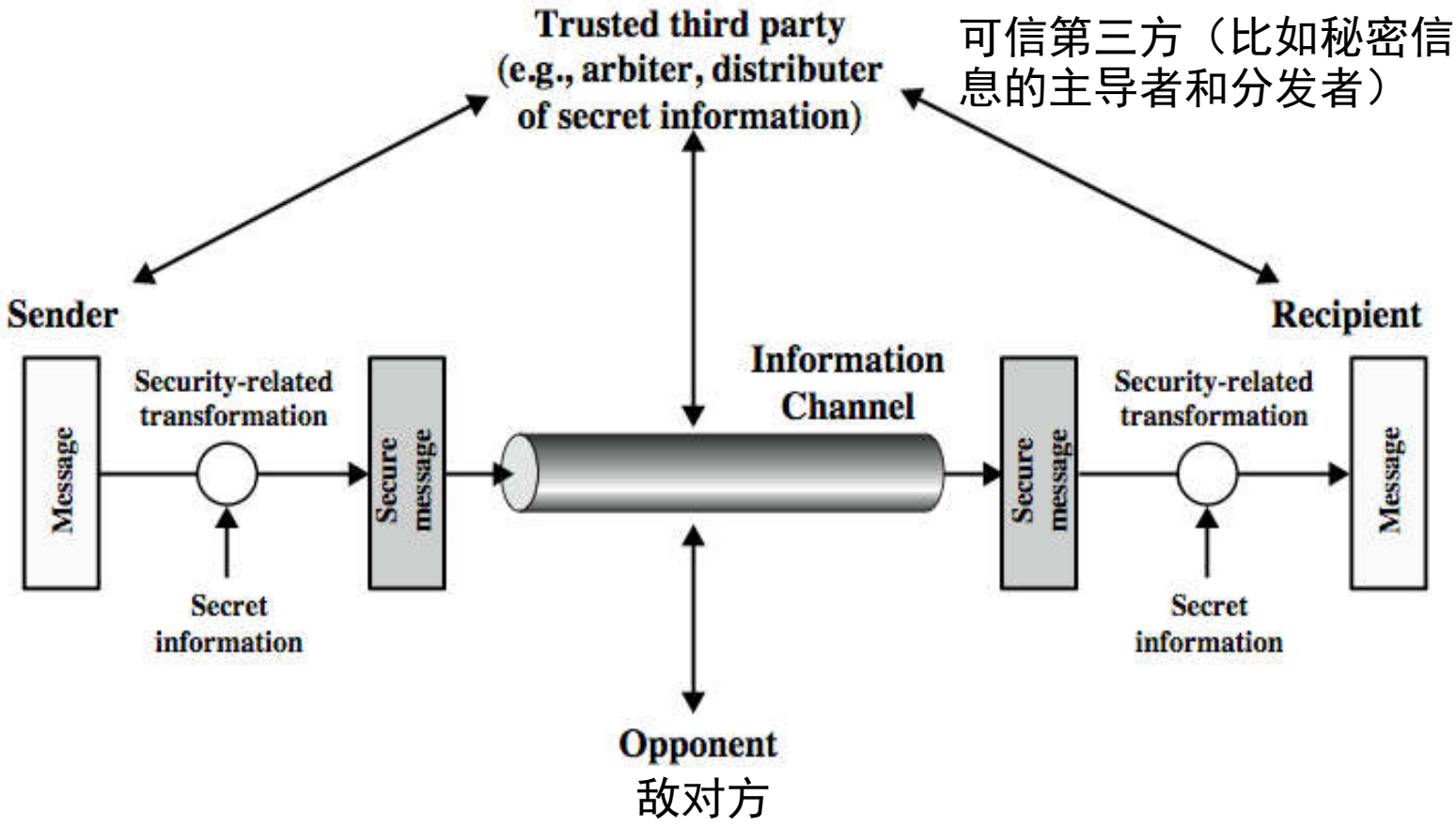
- **The Security Systems Development Life Cycle**
  - The Security Systems Development Life Cycle (SecSDLC)
    - ✧ Logical Design
      - ◌ Creates and develops blueprints for information security
      - ◌ Incident response actions planned:
        - Continuity planning
        - Incident response
        - Disaster recovery
      - ◌ Feasibility analysis to determine whether project should continue or be outsourced (外购/外包)
    - ✧ Physical Design
      - ◌ Needed security technology is evaluated, alternatives generated, and final design selected
      - ◌ At end of phase, feasibility study determines readiness (准备就绪) of organization for project

1.5 Conclusion

- **The Security Systems Development Life Cycle**
  - The Security Systems Development Life Cycle (SecSDLC)
    - Implementation
      - Security solutions are acquired, tested, implemented, and tested again
      - Personnel issues evaluated; specific training and education programs conducted
      - Entire tested package is presented to management for final approval
    - Maintenance and Change
      - Perhaps the most important phase, given the ever-changing threat environment
      - Often, reparation and restoration of information is a constant duel with an unseen adversary (与无形对手的持续的决战)
      - Information security profile of an organization requires constant adaptation as new threats emerge and old threats evolve (不断适应安全威胁的产生或进化)

1.5 Conclusion

- **Example**
  - Model for Network Security

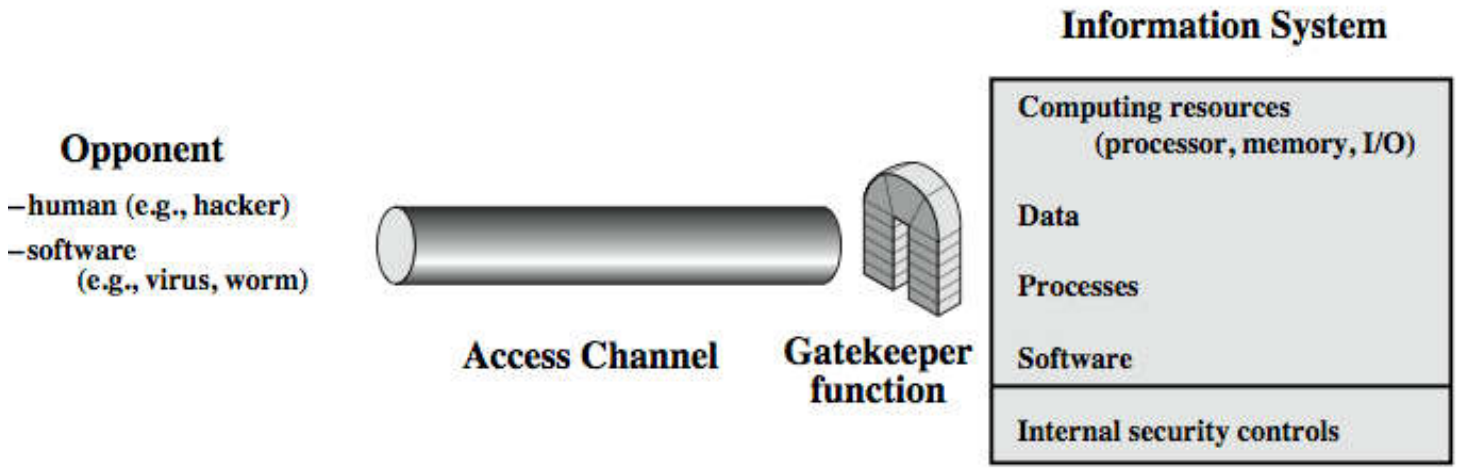


1.5 Conclusion

- **Example**
  - Model for Network Security
    - ✧ We need to
      - ◌ design a suitable algorithm for the security transformation
      - ◌ generate the secret information (keys) used by the algorithm
      - ◌ develop methods to distribute and share the secret information
      - ◌ specify a protocol enabling the principals (当事人) to use the transformation and secret information for a security service

1.5 Conclusion

- **Example**
  - Model for Network Access Security



1.5 Conclusion

- **Example**
  - Model for Network Access Security
    - ✧ We need to
      - ◌ select appropriate gatekeeper functions to identify users
      - ◌ implement security controls to ensure only authorised users access designated information or resources
      - ◌ Note that the model does not include monitoring of system for successful penetration
        - monitoring of authorized users for misuse
        - audit logging for forensic (法定) uses, etc.

References

1. William Stallings, Computer Security – Principles and Practice, Pearson 2008.
2. GBT 1999-2008
3. ITU-T, Recommendation X.800, 1991-1996
4. http://www.itu.int/rec/T-REC-X/en
5. http://en.wikipedia.org/wiki/Information_security
6. http://en.wikipedia.org/wiki/Information_security_management
7. http://en.wikipedia.org/wiki/Information_security_management_system
8. http://en.wikipedia.org/wiki/Information_security_audit

信息安全等级保护标准体系

- **通用基础**
  - 信息安全技术 信息系统安全等级保护实施指南
  - 信息安全技术 信息系统安全等级基本模型
  - 信息安全技术 信息系统安全等级基本配置
- **系统定级**
  - GB/T 22240-2008 信息安全技术 信息系统安全等级保护 定级指南
- **安全建设**
  - GB 17859-1999 计算机信息系统 安全保护等级划分准则
  - GB/T 22239-2008 信息安全技术 信息系统安全等级保护 基本要求
  - GB/T 20269-2006 信息安全技术 信息系统安全管理要求
  - GB/T 20270-2006 信息安全技术 网络基础安全技术要求
  - GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
  - GB/T 20272-2006 信息安全技术 操作系统安全技术要求
  - GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求
  - GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法
  - GB/T 20276-2006 信息安全技术 智能卡嵌入式软件安全技术要求（EAL4增强级）
  - GB/T 20277-2006 信息安全技术 网络和终端设备隔离部件测试评价方法
  - GB/T 20278-2006 信息安全技术 网络脆弱性扫描产品技术要求

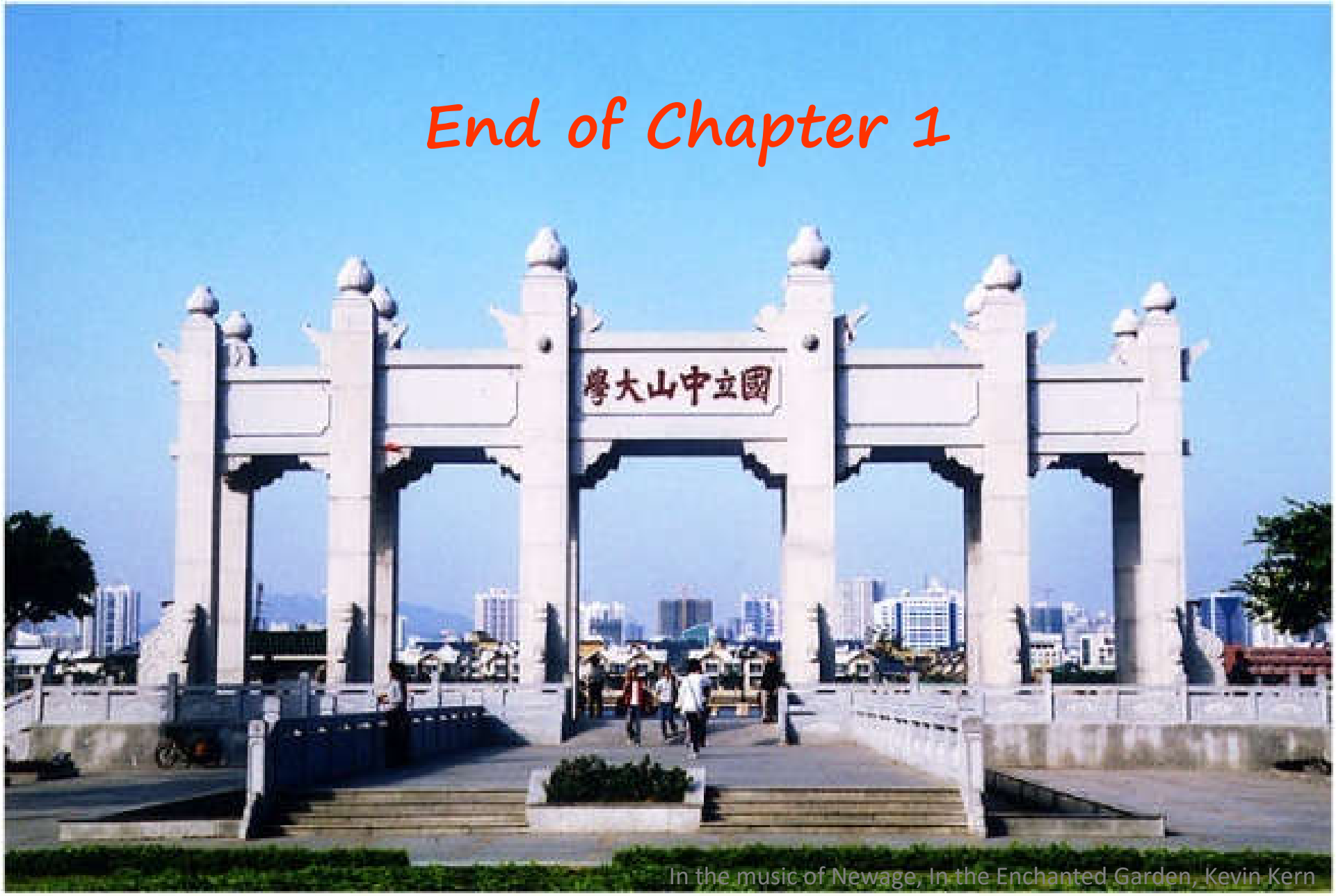
信息安全等级保护标准体系

- **安全建设**
  - GB/T 20279-2006 信息安全技术 网络和终端设备隔离部件安全技术要求
  - GB/T 20280-2006 信息安全技术 网络脆弱性扫描产品测试评价方法
  - GB/T 20281-2006 信息安全技术 防火墙技术要求和测试评价方法
  - GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求
  - GB/T 20945-2007 信息安全技术 信息系统安全审计产品技术要求和测试评价方法
  - GB/T 20979-2007 信息安全技术 虹膜识别系统技术要求
  - GB/T 21028-2007 信息安全技术 服务器安全技术要求
  - GB/T 21050-2007 信息安全技术 网络交换机安全技术要求（评估保证级3）
  - GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求
  - GB/T 18018-2007 信息安全技术 路由器安全技术要求
  - 信息安全技术 信息系统等级保护产品使用等级划分准则
  - 信息安全技术 检测评估机构服务资质等级划分准则
- **等级测评**
  - 信息安全技术 信息系统安全等级保护测评要求
  - 信息安全技术 信息系统安全等级保护测评过程指南

信息安全等级保护标准体系

- **运行维护**
  - GB/Z 20985-2007 信息安全技术 信息安全事件管理指南
  - GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南
  - GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
  - 信息安全技术 网络设备安全配置指南
  - 信息安全技术 操作系统安全配置指南
  - 信息安全技术 防火墙安全配置指南
  - 信息安全技术 补丁与脆弱性管理指南
- **风险评估标准**
  - GB/T 20984-2007《信息安全技术 信息安全风险评估规范》
  - GB/T 18336《信息技术 安全技术 信息技术安全性评估准则》
  - GB 17859－1999《计算机信息系统安全保护等级划分准则》
  - GB/T 19716－2005《信息技术 信息安全管理适用规则》
  - GB/T22080-2008《信息技术 安全技术 信息安全管理体系要求》
  - GB/T22081-2008《信息技术 安全技术 信息安全管理实用规则》/ISO27002
  - GB/T 20274《信息系统安全保障评估框架》

End of Chapter 1



In the music of Newage, In the Enchanted Garden, Kevin Kern