北京大学 深圳研究生院
Peking University
Shenzhen Graduate School

Cryptography and Network Information Security

密码编码学与网络信息安全·

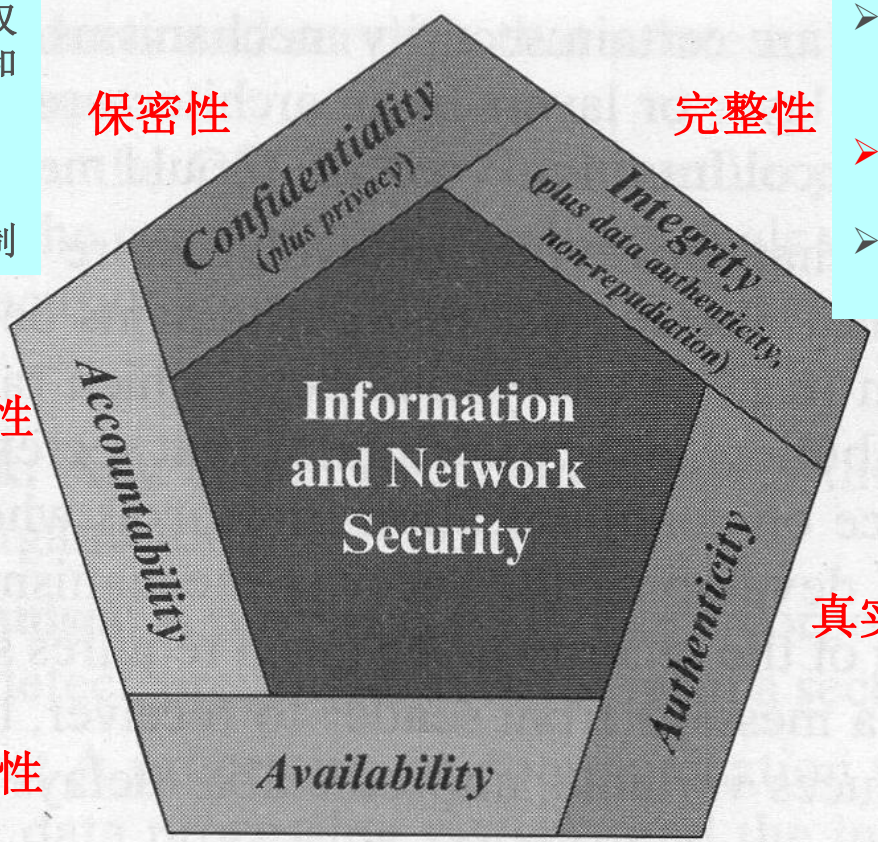
一． 信息安全引论

Introduction to Information Security

网络与信息安全基本概念

- 对信息访问和公开进行授权限制，包括保护个人隐私和秘密信息
- 保密性缺失：信息非授权泄露
- 解决方案：加密、访问控制

保密性



完整性

- 防止对信息不恰当修改或破坏，包括确保信息的不可否认性和真实
- 完整性缺失：对信息非授权修改和毁坏
- 解决方案：散列算法、数字签名、访问控制

- 确保实体的行动可被跟踪

可追溯性

- 确保对信息及时和可靠的访问和使用
- 可用性缺失：对信息和信息系统访问和使用中断
- 解决方案：防火墙、病毒扫描、安全OS

可用性

真实性

- 真实性是完整性概念的延伸
- 不仅仅具有完整性，而且文件的来源也已知

Essential Information and Network Security Objectives

标准化问题

International standards

ITU-T（International Telecommunication Union

Telecommunication Standardization Sector）

（国际电信联盟电信标准化机构） （Formerly CCITT）

http://www.itu.int

The Internet society

- Internet Engineering Task Force (IETF)，http://www.ietf.org
- Internet Architecture Board (IAB)
- Internet Engineering Steering Group (IESG)

NIST （National Institute of Standards and Technology）

直属美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及有关服务

ITU-T安全框构 - 推荐X.800方案

Data Communication Networks: Open Systems Interconnection (OSI); Security Structure And Applications

Security Architecture For Open Systems Interconnection For CCITT Applications

Recommendation X.800

Internet Engineering Task Force (IETF)

http://www.ietf.org

RFC (Request For Comments)-“请求注解”， Internet Society

RFC 2828 Internet Security Glossary互联网安全词汇（May 2000）

对安全下了明确的定义：

- **威协（Threat）：侵犯安全可能性，脆弱性的潜在危险。**
- **攻击（Attack）：智能威协对系统安全的攻击行为。**

Table 1.3 Threats and Attacks (RFC 2828)

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

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.

ITU-T X.800方案

OSI 开放式系统互联（Open Systems Interconnection ）安全框架

关注安全服务、机制和攻击。

为管理员提供安全组织方法。

保证系统和数据传输有足够的安全性。

X.800 VS RFC 2828

X.800 defines it as:

a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers

由协议层来保证的安全服务

RFC 2828 defines it as:

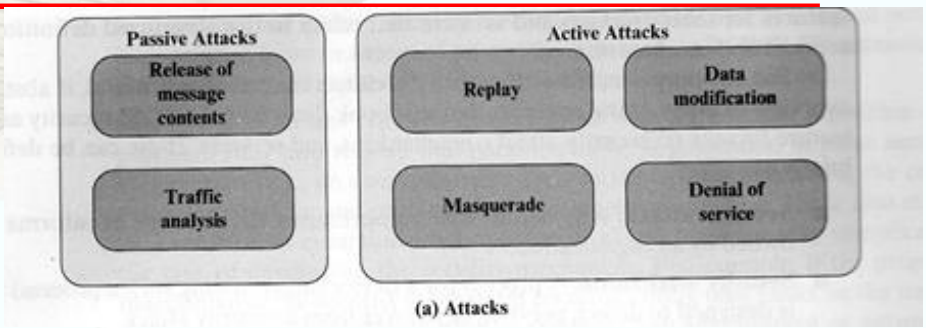
a processing or communication service provided by a system to give a specific kind of protection to system resources

由系统来保证的安全服务

安全攻击、机制和服务
Attacks, Mechanisms and Services

➢Security Attack

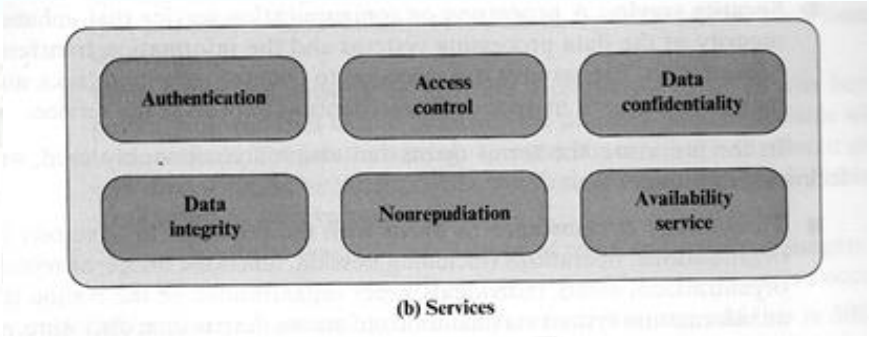
Any **action（行为）** that **compromises（危及）** the security of information.



(a) Attacks

➢Security Mechanism

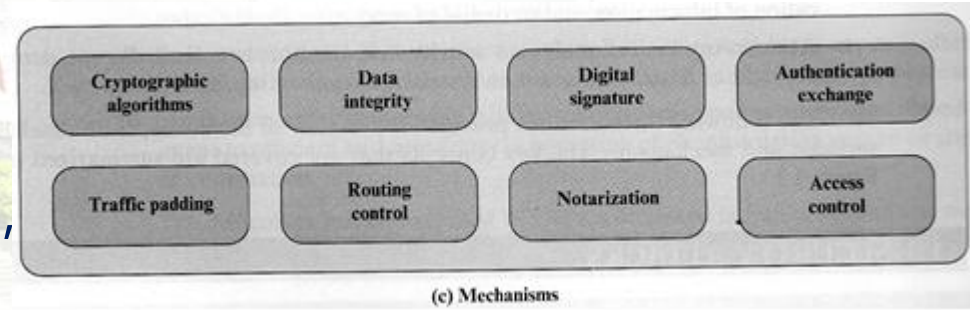
A mechanism that is designed to **detect（侦听）**, **prevent（防止）**, or **recover（恢复）** from a security attack.



(b) Services

➢ Security Service

A **service（服务）** that **enhances the security （增强安全性）** of data processing systems **（数据处理系统）** and information transfers **（信息传输）**, and makes use of one or **more security mechanisms（多种安全机制）**.

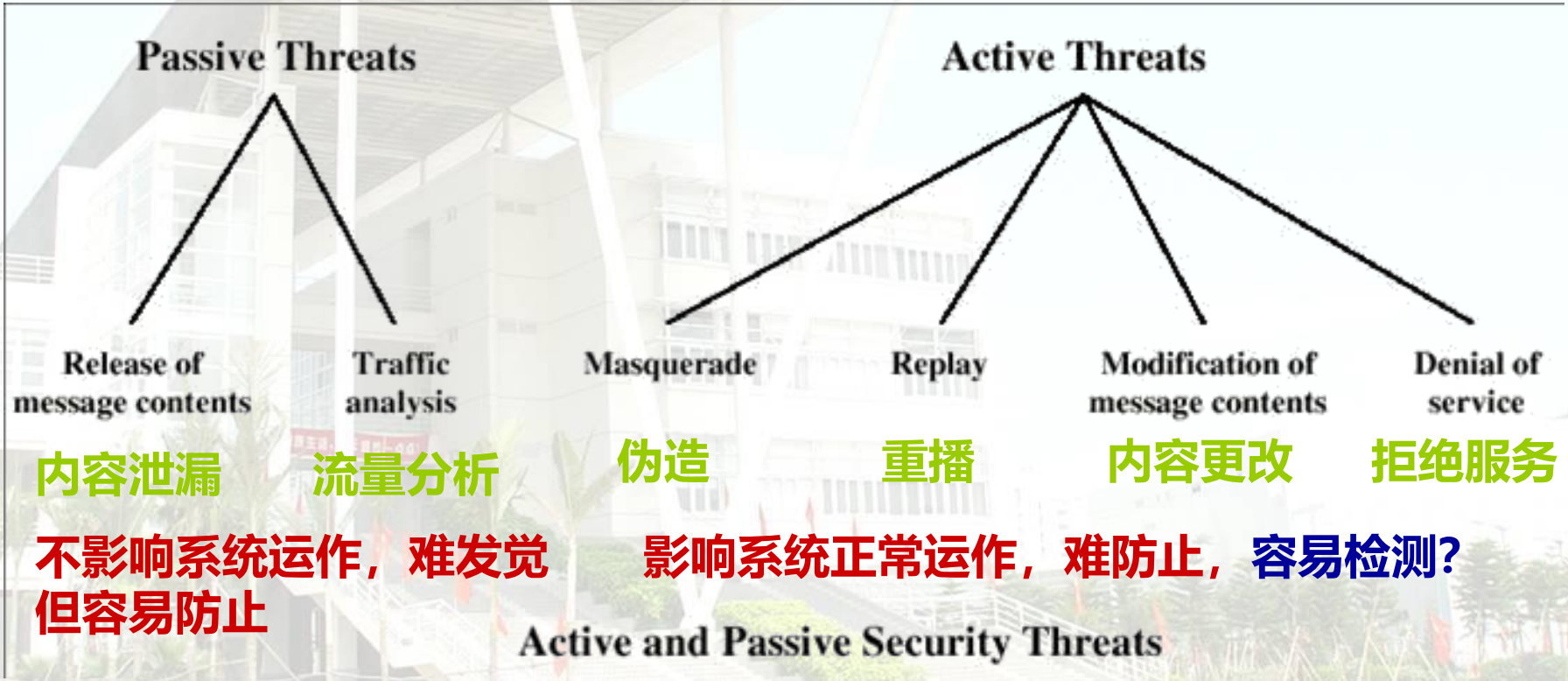


(c) Mechanisms

攻击方式

被动式

主动式



内容泄漏　流量分析

伪造　重播　内容更改　拒绝服务

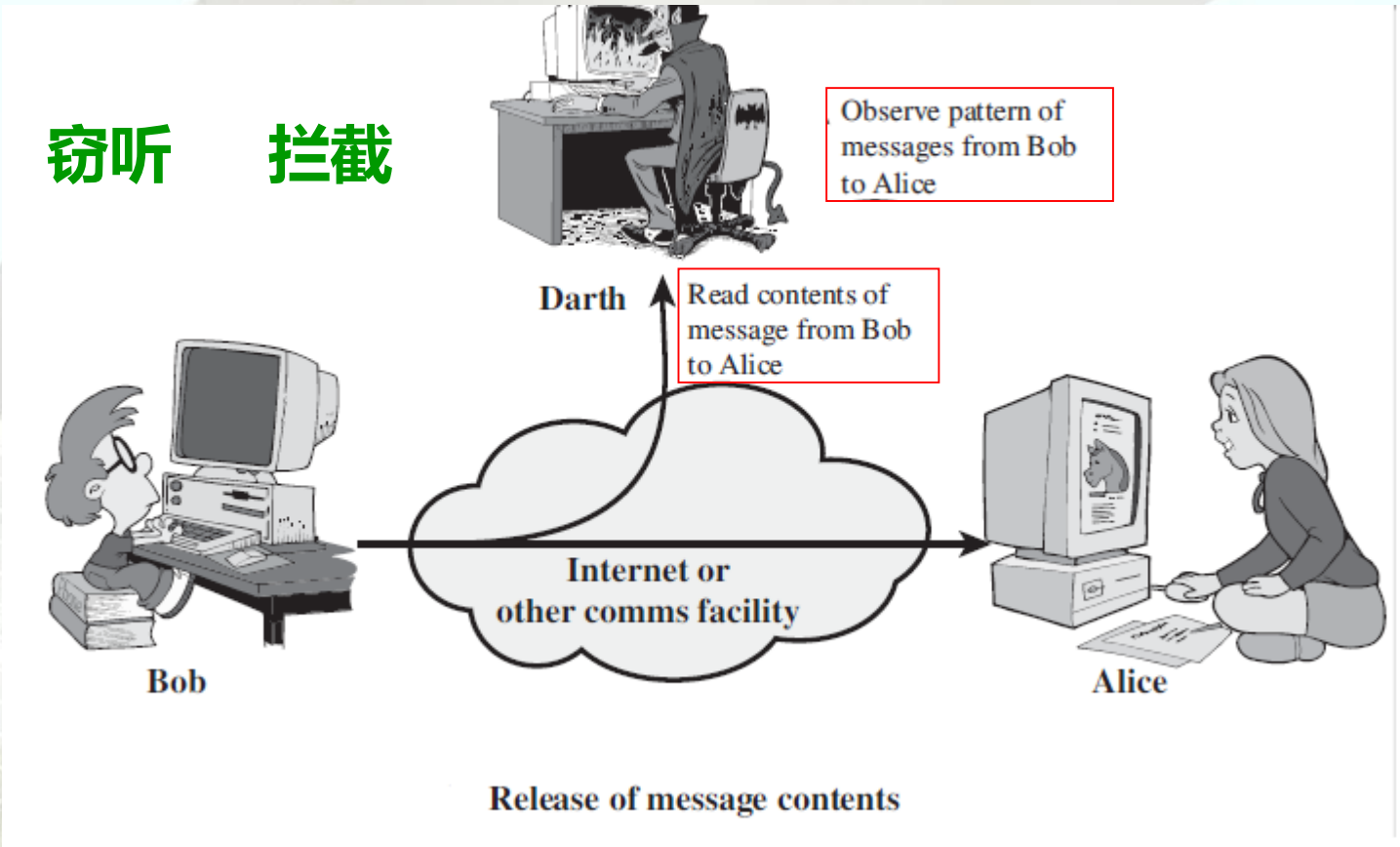
不影响系统运作，难发觉
但容易防止

影响系统正常运作，难防止，容易检测?

Active and Passive Security Threats

Interception 被动式 Passive Attacks

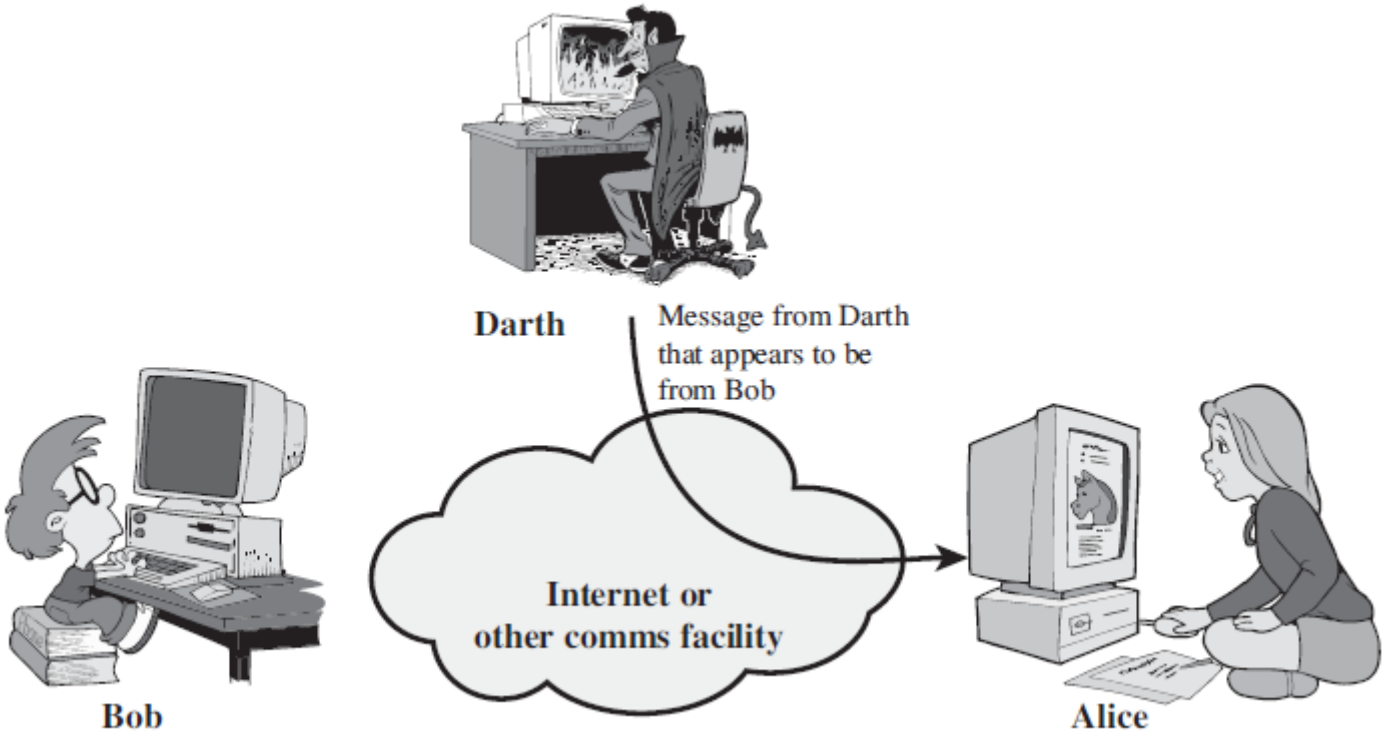
监视　　窃听　　拦截



an attack on confidentiality

非授权方介入系统的攻击，破坏保密性(confidentiality)
非授权方：可以是一个人，一个程序，一台机器
攻击：包括搭线窃听，文件或程序的不正当拷贝

伪造攻击



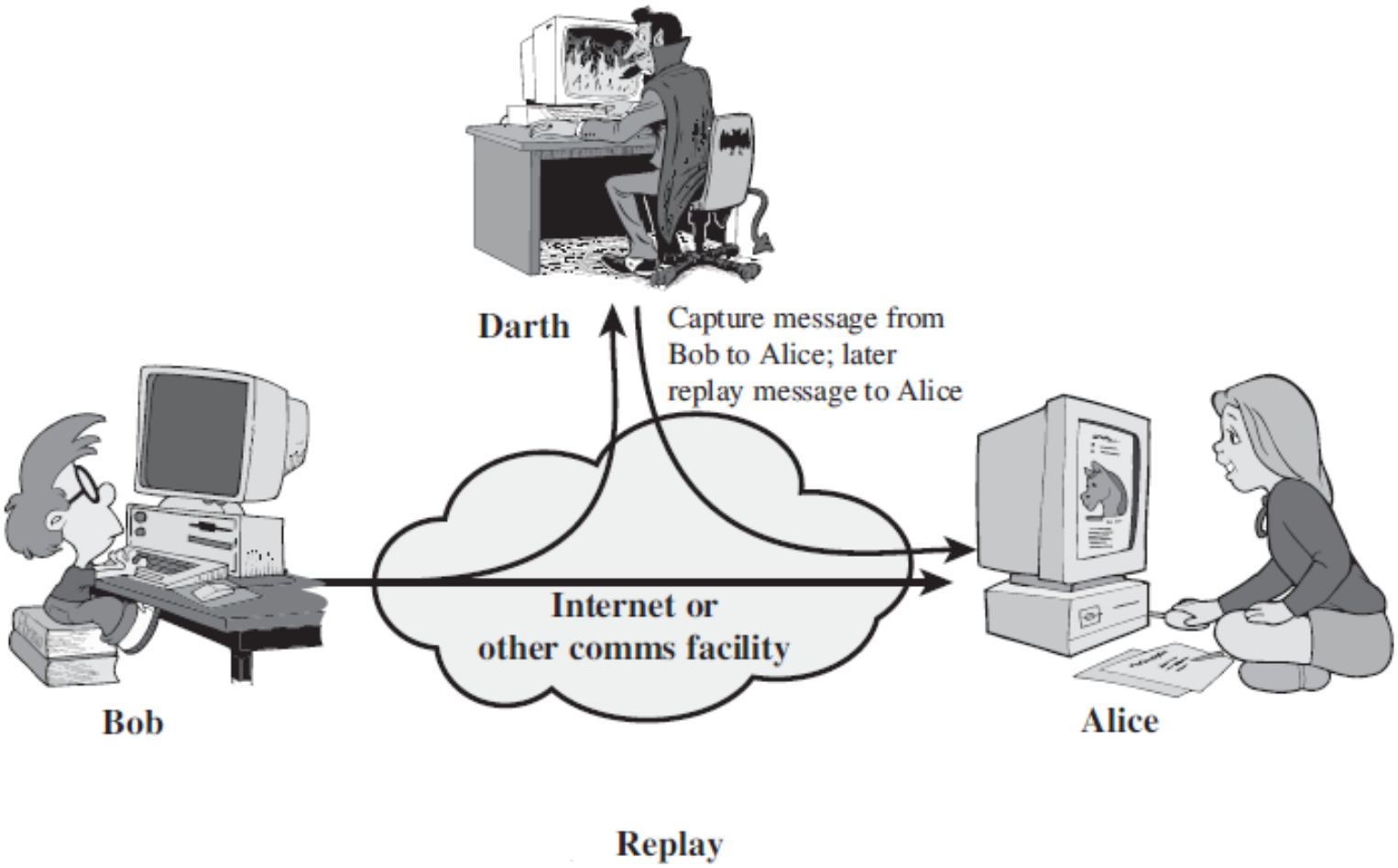
Masquerade: This is an attack on authenticity

非授权方将伪造的客体插入系统中，破坏真实性（authenticity）
攻击：包括网络中插入假信件，或者在文件中追加记录等

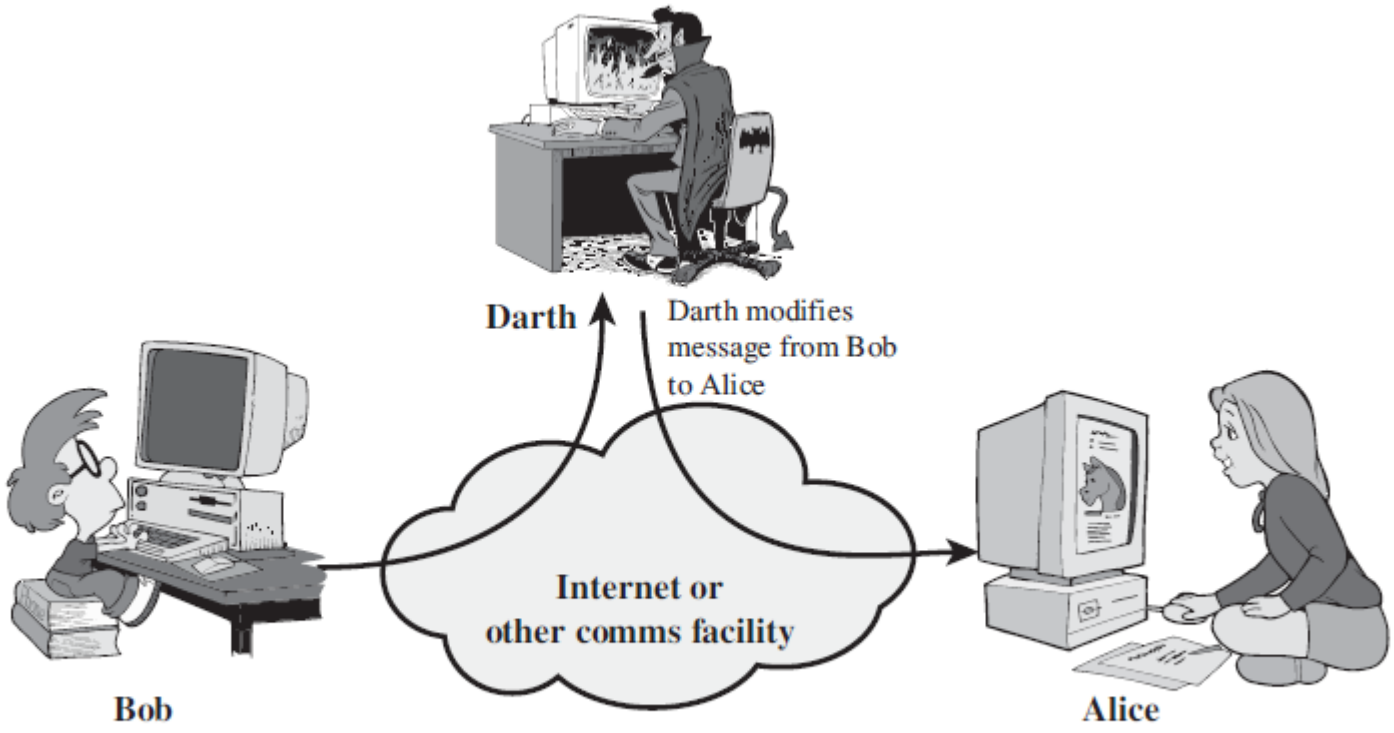
一个实体假装成另外一个实体。
在鉴别过程中，获取有效鉴别序列，以冒名重播的方式获得特权

重放攻击-Active Attacks

- 获取有效数据段以重播的方式获取对方信任



内容更改 攻击

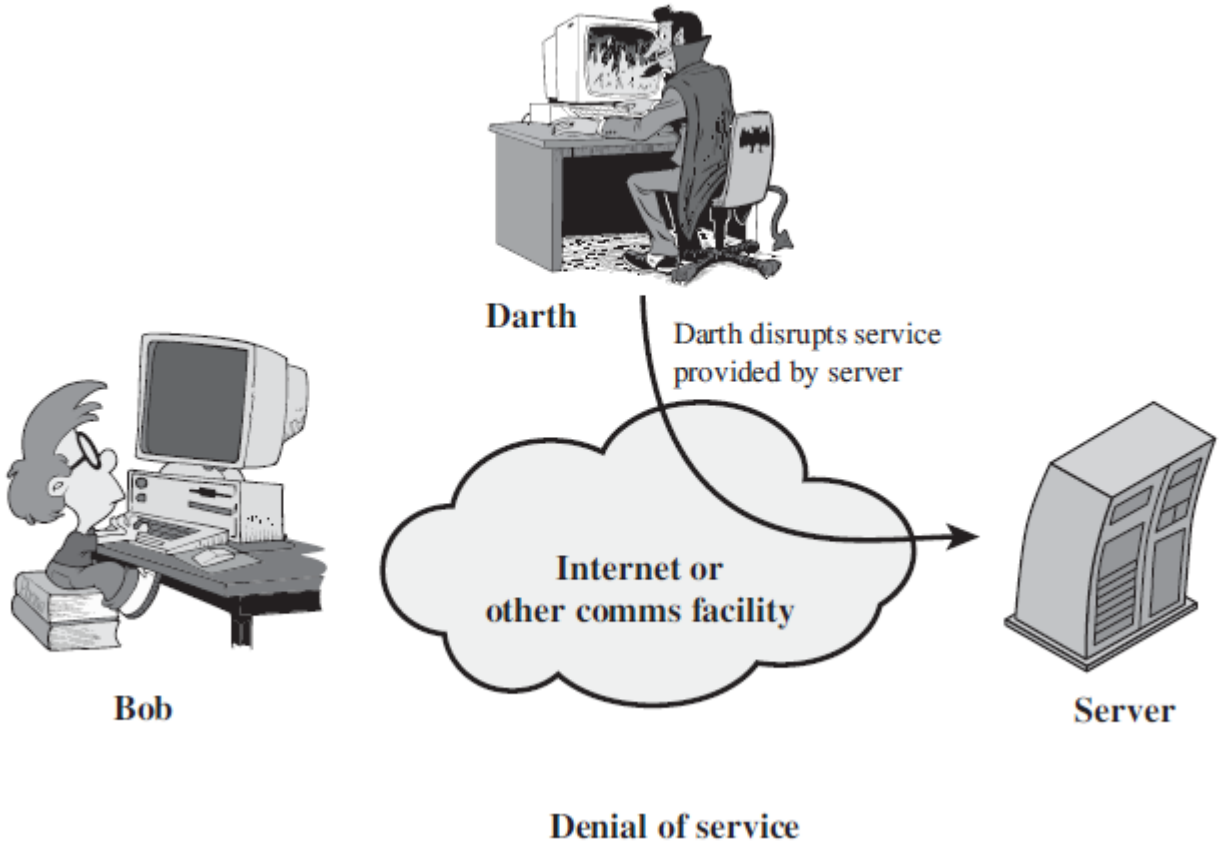


Modification: This is an attack on integrity

非授权方不仅介入系统而且在系统中‘瞎捣乱’的攻击，破坏完整性（integrity）

攻击：包括改变数据文件，改变程序使之不能正确执行，修改信件内容等

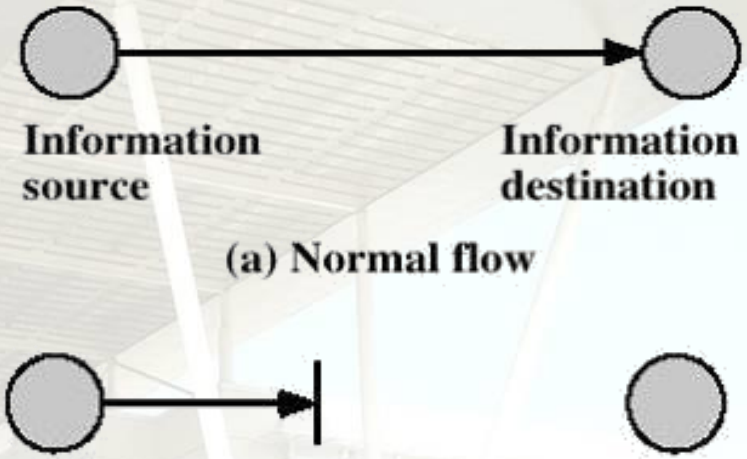
拒绝服务攻击



Denial of service

- 破坏设备的正常运行和管理
- 有针对性或特定目标
- 如抑制发往特定地址的所有信件
- 将整个网络扰乱，发送大量垃圾信件使网络过载，以降低系统性能

安全攻击(Security Attacks)



中断

- **Interruption**: This is an attack on availability

信息系统毁坏或不能使用的攻击，破坏可用性（availability）

如：硬件的毁坏，通信线路的切断，文件管理系统的瘫痪等

Table 1.2

安全攻击例子

1. Gain unauthorized access to information (i.e., violate secrecy or privacy).
2. Impersonate another user either to shift responsibility (i.e., liability) or else to use the other's license for the purpose of:
   a. originating fraudulent information,
   b. modifying legitimate information,
   c. using fraudulent identity to gain unauthorized access,
   d. fraudulently authorizing transactions or endorsing them.
3. Disavow responsibility or liability for information the cheater did originate.
4. Claim to have received from some other user information that the cheater created (i.e., fraudulent attribution of responsibility or liability).
5. Claim to have sent to a receiver (at a specified time) information that was not sent (or was sent at a different time).
6. Either disavow receipt of information that was in fact received, or claim a false time of receipt.
7. Enlarge cheater's legitimate license (for access, origination, distribution, etc.).
8. Modify (without authority to do so) the license of others (fraudulently enroll others, restrict or enlarge existing licenses, etc.).
9. Conceal the presence of some information (a covert communication) in other information (the overt communication).
10. Insert self into a communications link between other users as an active (undetected) relay point.
11. Learn who accesses which information (sources, files, etc.) and when the accesses are made even if the information itself remains concealed (e.g., a generalization of traffic analysis from communications channels to data bases, software, etc.).
12. Impeach an information integrity protocol by revealing information the cheater is supposed to (by the terms of the protocol) keep secret.
13. Pervert the function of software, typically by adding a covert function.
14. Cause others to violate a protocol by means of introducing incorrect information.
15. Undermine confidence in a protocol by causing apparent failures in the system.
16. Prevent communication among other users, in particular, surreptitious interference to cause authentic communication to be rejected as unauthentic.

通信网络的主要攻击方式

对设备攻击　　对服务攻击　　对信息攻击

既对服务器又对客户端

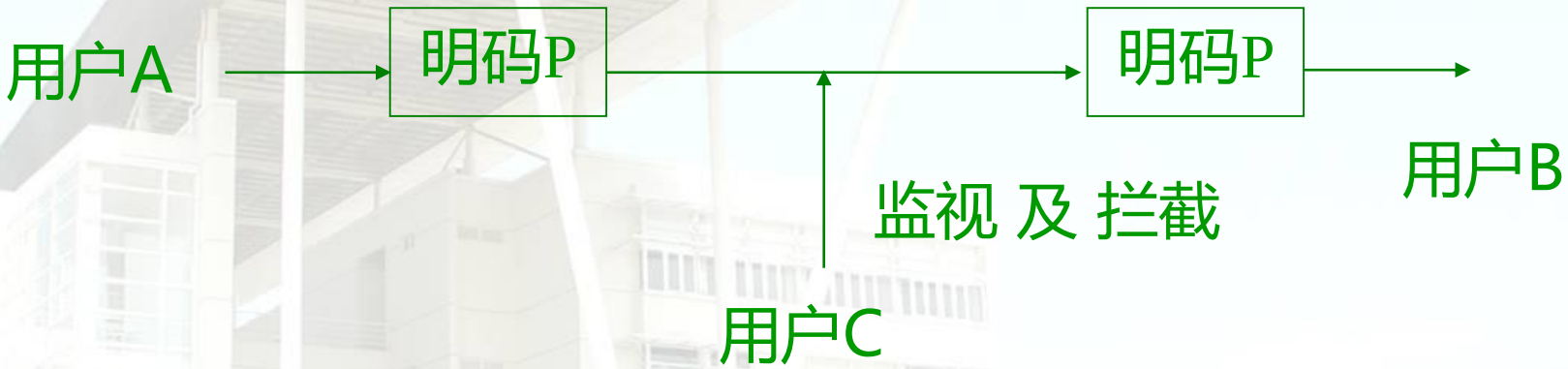
主动式

- 中间人攻击　　拒绝服务攻击 (DoS)
- 捏造　　克隆　　抵赖　　欺骗
- 篡改　　盗打　　重播　　重定向

被动式

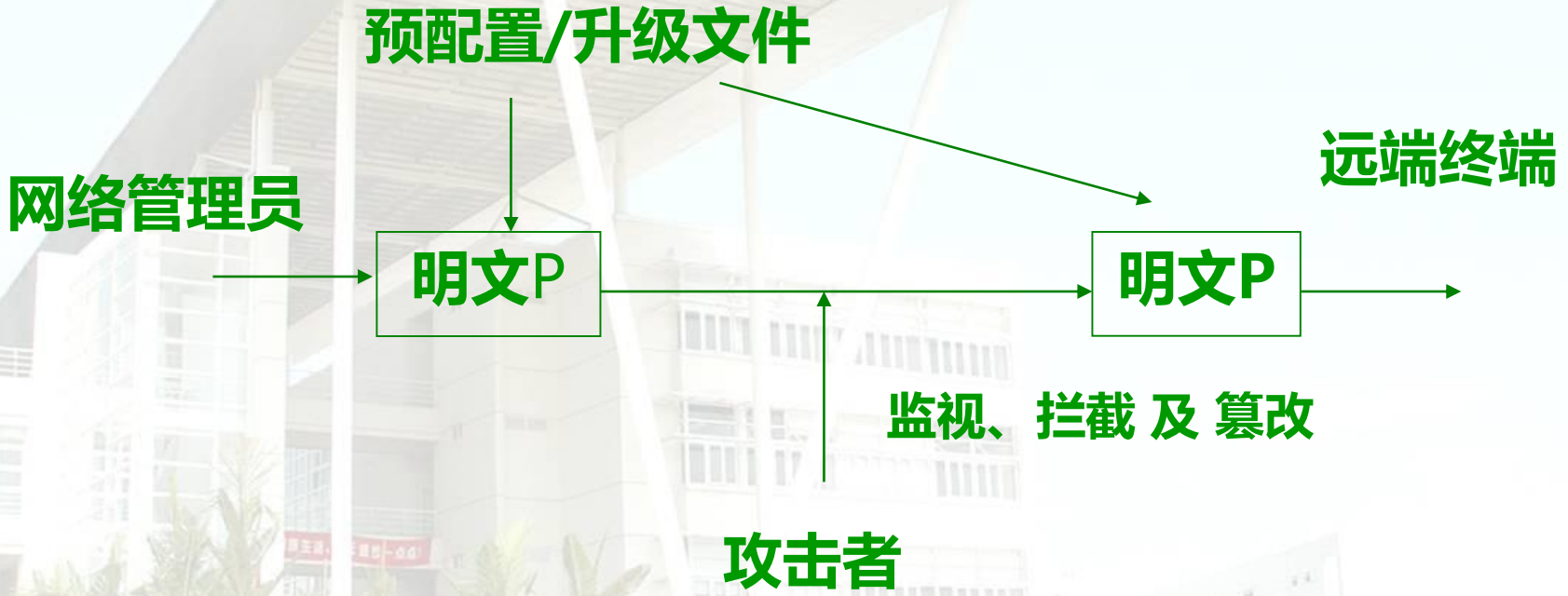
监视　　窃听　　拦截

VOIP常见的安全攻击例子 （一）



A给B打电话，C未经AB允许偷听。（非授权访问）

VOIP常见的安全攻击例子 （二）



Provisioning process

VOIP常见的安全攻击例子 （三）

Provisioning process

安全服务 （Security Services）

- 保密 Confidentiality (privacy)
- 认证 Authentication (who created or sent the data)
- 完整 Integrity (has not been altered)
- 不可抵赖 Non-repudiation (the order is final)
- 存取/接入控制 Access control (prevent misuse of resources)
- 可用 Availability (permanence, non-erasure)

prevent

Virus that deletes files

Denial of Service Attacks

ITU - T X.800分为五类14个特定服务

Security Services (X.800)

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

可靠安全网络通信应保证

保密性
完整性
真实性
可控性
可靠性
可用性

保密性

防止信息泄漏
防侦收
防辐射
信息加密
物理保密

连接保密（connection）
无连接保密（connectionless）
选定域保密 （selected field）
流量保密 （traffic）

用加密机制实现
目的：

- 密级文件经过加密可以公开存放和发送
- 实现多级控制需要
- 构建加密通道的需要，防止搭线窃听和冒名入侵

鉴别(认证)　Authentication

- 双方身份鉴别　　Mutual Authentication
- 单向身份鉴别　　例如 server Authentication
- 数据源鉴别　　data origin

- 消息鉴别（Message Authentication）：
  证实收到的消息来自可信的源点且未被篡改。
- 鉴别的函数：

(1)　消息加密函数(Message encryption)
用完整信息的密文作为对信息的鉴别

(2) 消息鉴别码MAC(Message Authentication Code)
公开函数+密钥产生固定长度的值作为鉴别标识

(3) 散列函数(Hash Function)
以一个变长的报文作为输入，产生一个定长的散列码，也称报文摘要，作为输出。

完整性及保障措施

保证信息的正确地生成、传输及存储

防止偶然 或蓄意地更改、伪造、乱序、插入、重播删除等破坏行为。

- 数据完整性-数据本身真实性的证明

- 完整性可以分为以下几类:
  - 带恢复的连接完整性
  - 不带恢复的连接完整性
  - 选择字段连接完整性
  - 无连接完整性
  - 选择字段无连接完整性

保障措施:

安全协议
纠错编码
密码校验
数字签名
鉴别

真实性及不可抵赖性

防止否认或抵赖曾经完成的操作或承诺

数据源鉴别

确认收方

可用性及可控性

可用性: 网络信息可访问及按需使用特性
可控性: 网络传播及内容控制

允许授权用户访问使用
身份识别确认
访问控制
业务流控制
路由选择控制
审计跟踪
网络管理: 升级及维护

- 防止对任何资源（如计算资源、通信资源或信息资源） 进行未授权的访问。在合法范围内使用;
- 未授权的访问包括：未经授权的使用、泄露、修改、销毁信息以及颁发指令等。
  - 非法用户进入系统。
  - 合法用户对系统资源的非法使用。

可靠性及措施

硬件可靠性
软件可靠性
人员可靠性
环境可靠性

可靠性测度　　抗毁性，生存性，有效性

措施:

提高设备质量，质量管理
备份，容错/纠错/自修复
网络结构及路由分配

安全措施 Methods of Defence

- **物理:** （Physical Controls ）:网络环境
- **政策:** （Policies）:政策法规
  管理 frequent changes of passwords
- **逻辑:** 安全及保密技术
  （ Encryption/authentication)
- **教育:** 普及教育

Methods of Defence

- 软件
  Software Controls
  - access limitations
  - in a data base,
  - in operating system (users)

- 硬件
  Hardware Controls
  - USB Key
  - simcard
  - smartcard
  - U 盾

安全机制 Security Mechanism

Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**Security Audit Trail** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
Traffic Padding The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.	
Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

协议层实现

普通

安全机制 Security Mechanism

可逆： 加密解密 encryption and decryption

明码P → 加密 → 密码C → 解密 → 明码P

不可逆：

HASH
MAC
Digest,
Digital Signature

→ **Authentication**

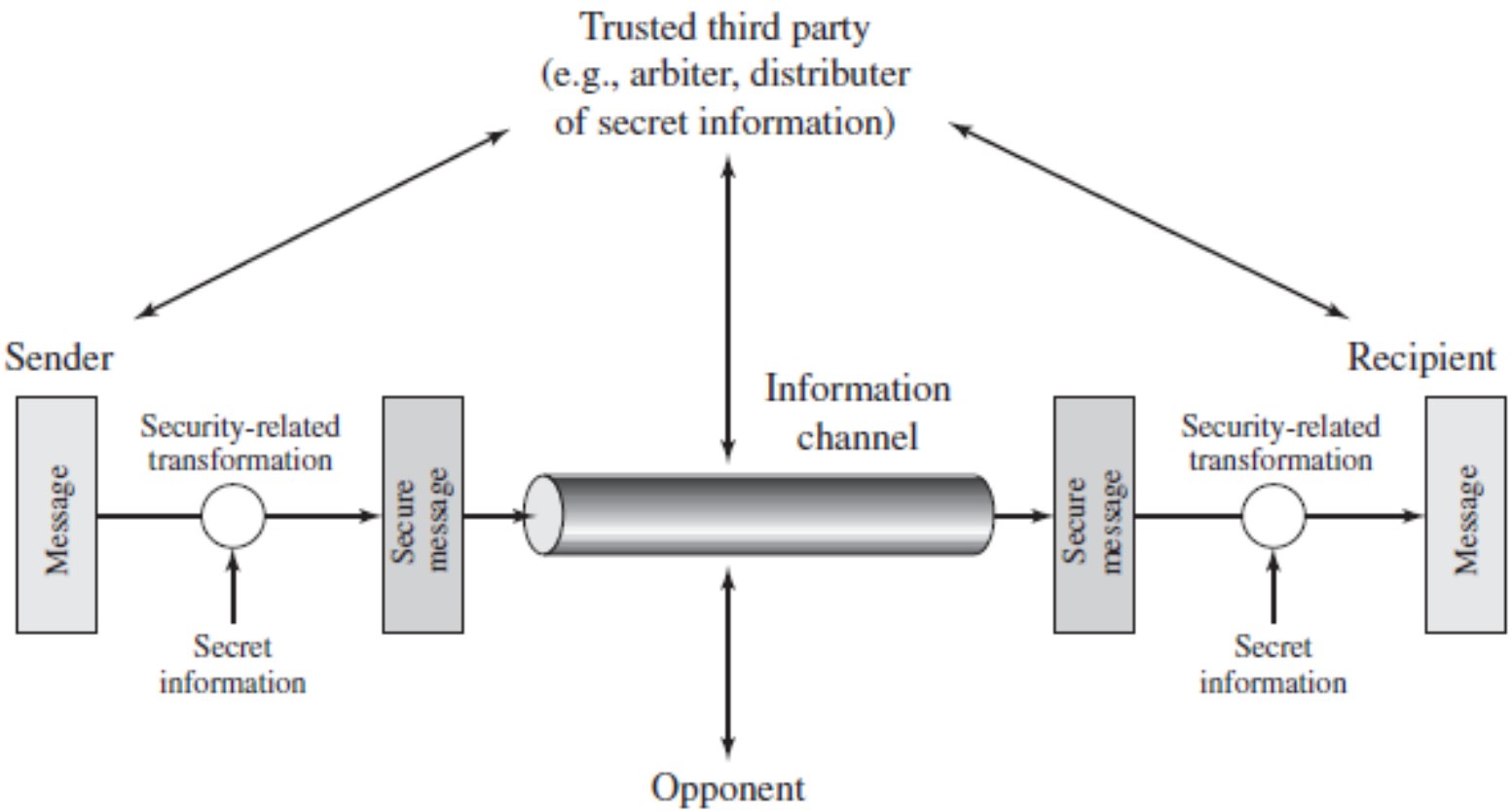
消息 → MD5 → 16 - byte 数据

安全服务和机制间的关系

Table 1.6 Relationship Between Security Services and Mechanisms

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

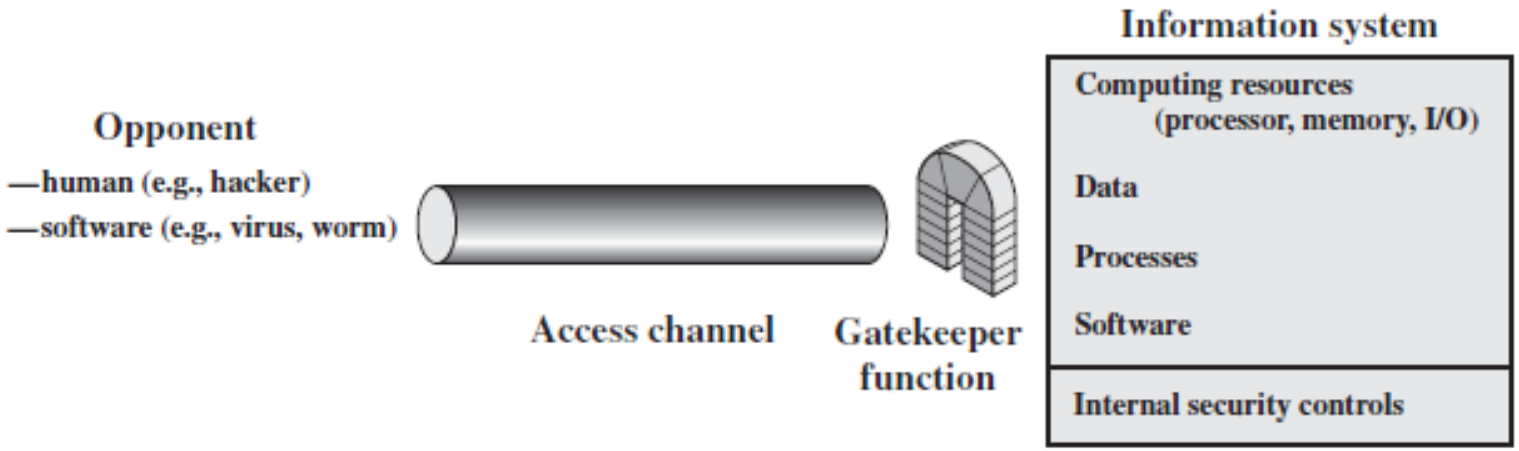
网络安全模型


Trusted third party
(e.g., arbiter, distributer
of secret information)
Sender
Recipient
Information
channel
Message
Security-related
transformation
Secure
message
Secret
information
Secure
message
Security-related
transformation
Message
Secret
information
Opponent

requires us to

- 加密算法设计：design a suitable algorithm for the security transformation
- 密钥产生：generate the secret information (keys) used by the algorithm
- 共享秘密分发：develop methods to distribute and share the secret information
- 通讯协议制定：specify a protocol enabling the principals to use the transformation and secret information for a security service

网络访问安全模型

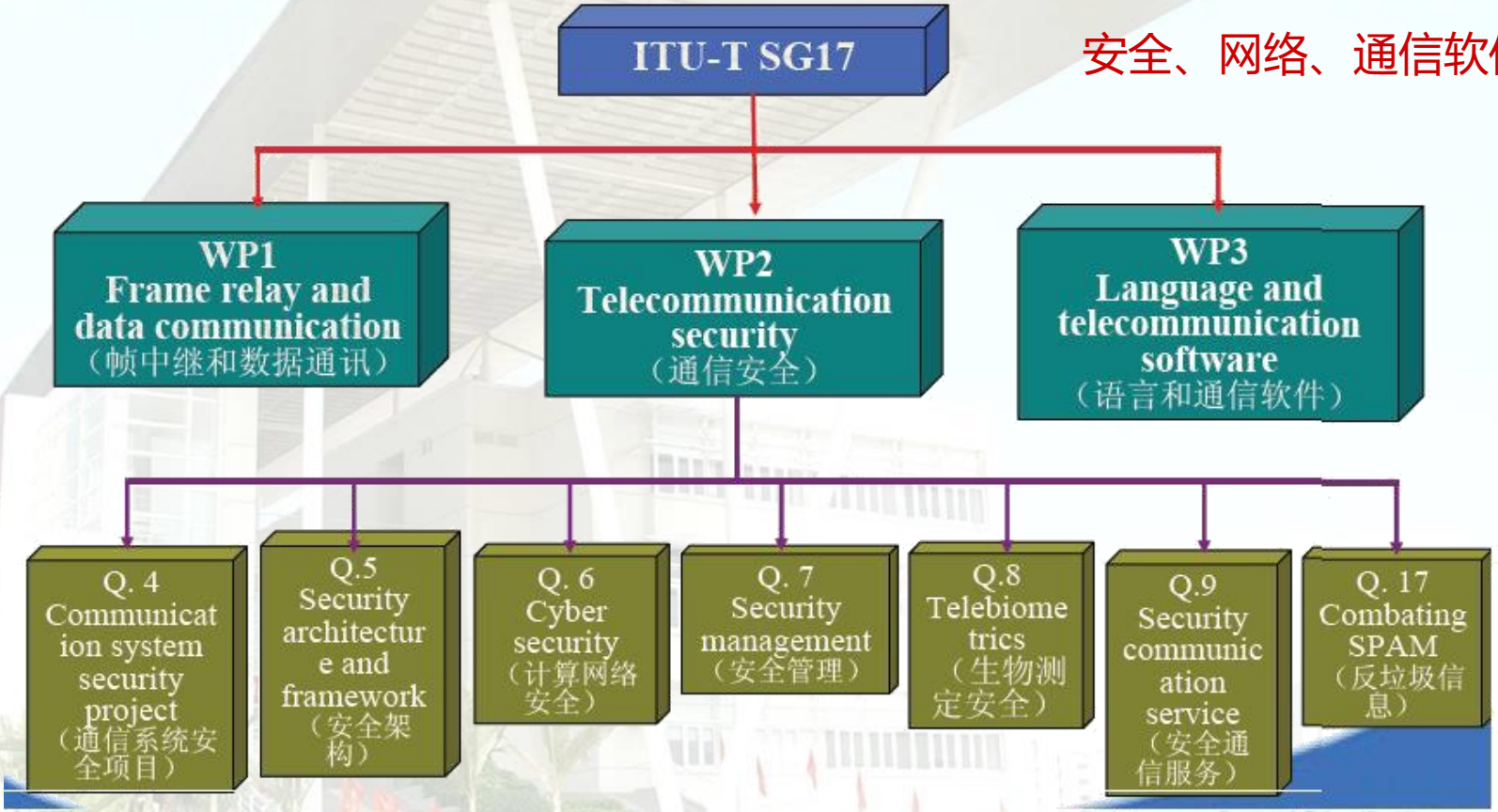


Network Access Security Model

requires us to:

- using the model
  - 门卫：select appropriate gatekeeper functions to identify users
  - 安全控制：implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems can be used to implement this model

ITU-T SG17
数据网络和电信软件研究组
通信安全研究与标准制定工作



组成课题：Q.G（通信安全项目）、Q.H（安全体系和框架）、Q.I（计算机安全）、Q.J（安全管理）、Q.K（远程生物识别）、Q.L（安全通信业务）和 Q17(反垃圾信息技术)。

我国的一些标准工作现状

- GB/T 17901.1—2020《信息技术 安全技术 密钥管理 第1部分：框架》；
  中华人民共和国国家标准，（2020年第1号）

- GB/T 39205-2020《信息安全技术 轻量级鉴别与访问控制机制》；
  中华人民共和国国家标准，（2020年第21号）

- 可信计算密码支撑平台功能与接口规范”

- 宽带无线IP标准

WAPI（Wireless Authentication Privacy Infrastructure）无线鉴别和保密基础结构）

运营级WLAN技术标准体系

“无线城域网安全接入技术规范”，
“无线网状网技术规范”，
“无线局域网可视电话终端技术规范”，
“基于GB15629.11 系列国家标准的无线局域网与蜂窝网络互通技术 规范”，
“WAPI 移动终端设备测试技术规范”，
“GB 15629.11 系列国家标准扩展规范：会聚无线控制技术规范”
“无线局域网证书鉴别漫游 规范”
“WLAN与TD-SCDMA/WCDMA/CDMA互通技术要求”

例：运营级WLAN技术标准体系

运营级WLAN技术标准体系的规划前提：

- 对无线局域网网络产品的生产商、电信运营商、用户等开展广泛的调研
- 分析梳理高安全、可运营、易管理的WAPI扩展应用技术以及电信骨干网络的结构和业务流程
- 结合无线局域网技术的研发和应用需求的发展方向

运营级WLAN技术标准体系 (2)

运营级WLAN技术标准体系的设计原则：

- 对于已经成熟、满足无线局域网应用需求的标准可以直接或修改采用
- 对于无线局域网产品研发与应用有特殊需求、国内拥有先进技术成果和自主知识产权的领域
  - ✓以自主制定标准为主
  - ✓保持与已有标准最大程度的兼容、衔接

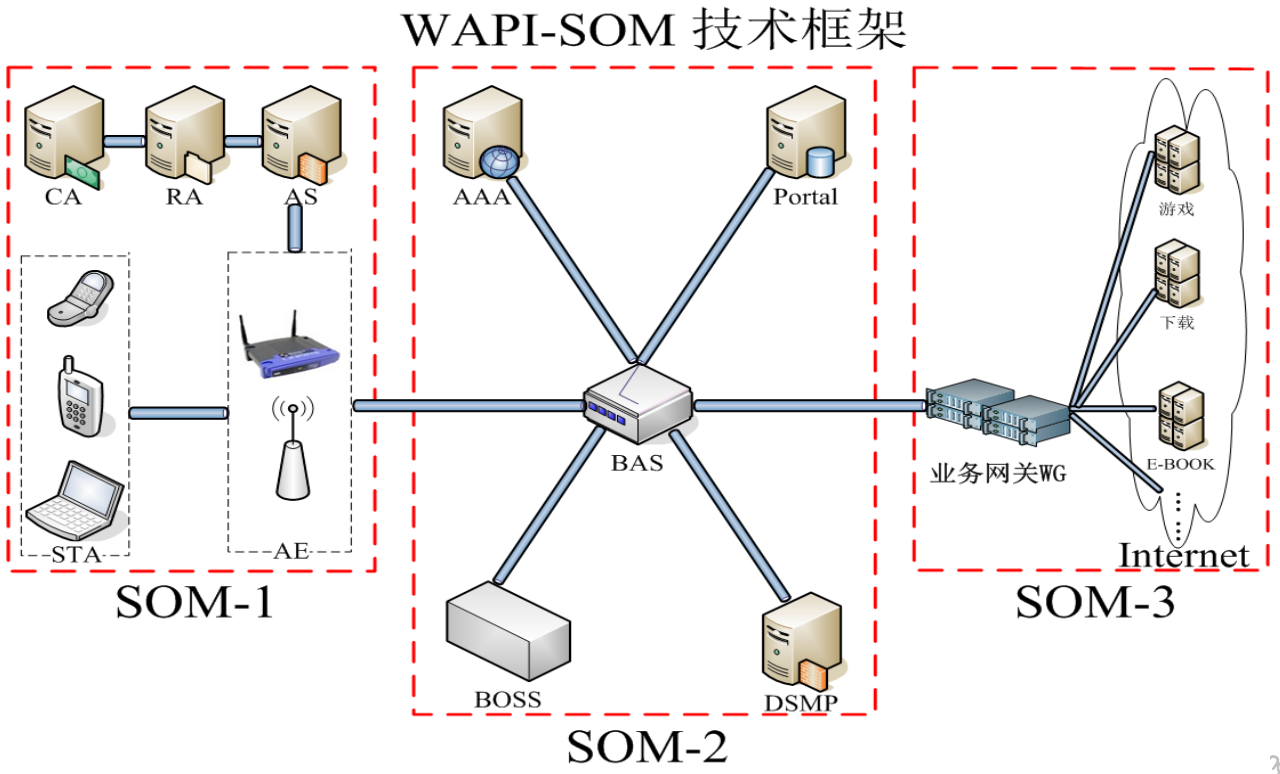
运营级WLAN技术标准体系综述(3)

运营级WLAN技术标准体系的覆盖范围：

- 无线局域网技术的标准集，尤其是
  - ✓ 支持使用WAPI技术的基础、产品、工程化、测试等相关标准
  - ✓ 应用于电信运营商网络的无线局域网技术相关标准

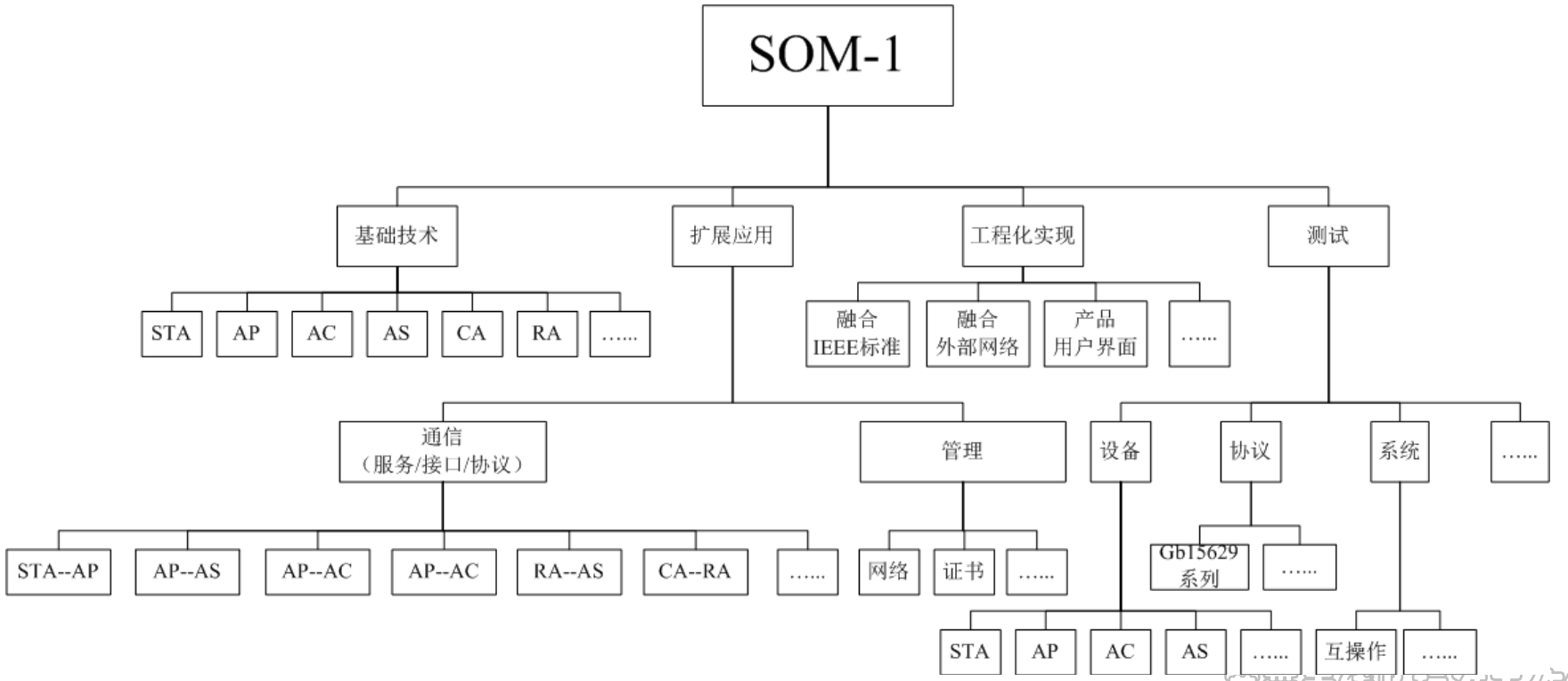
运营级WLAN技术标准体系架构(1)

- 运营级WLAN技术标准体系架构以运营级WLAN技术框架为基础（WAPI-SOM两网三层模型）



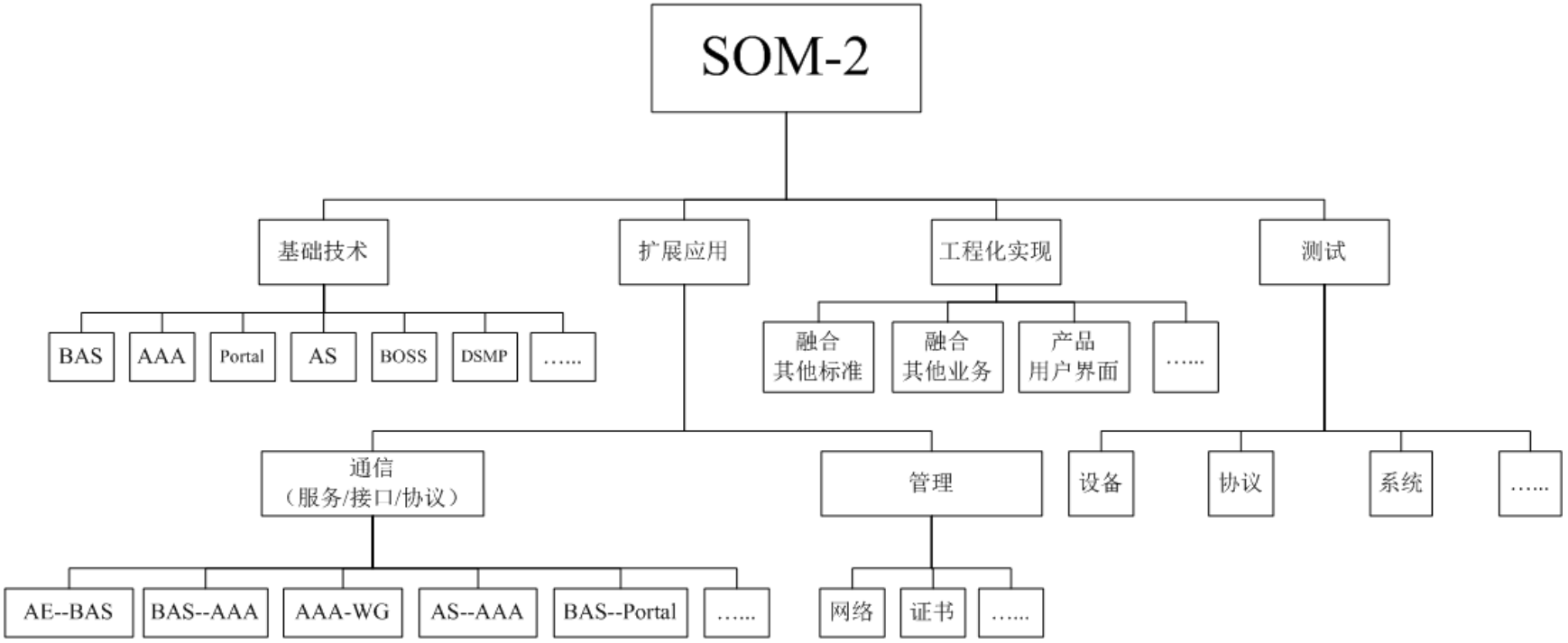
运营级WLAN技术标准体系架构(2)

- SOM-1类标准：合法终端接入合法无线局域网过程涉及到的系列标准。



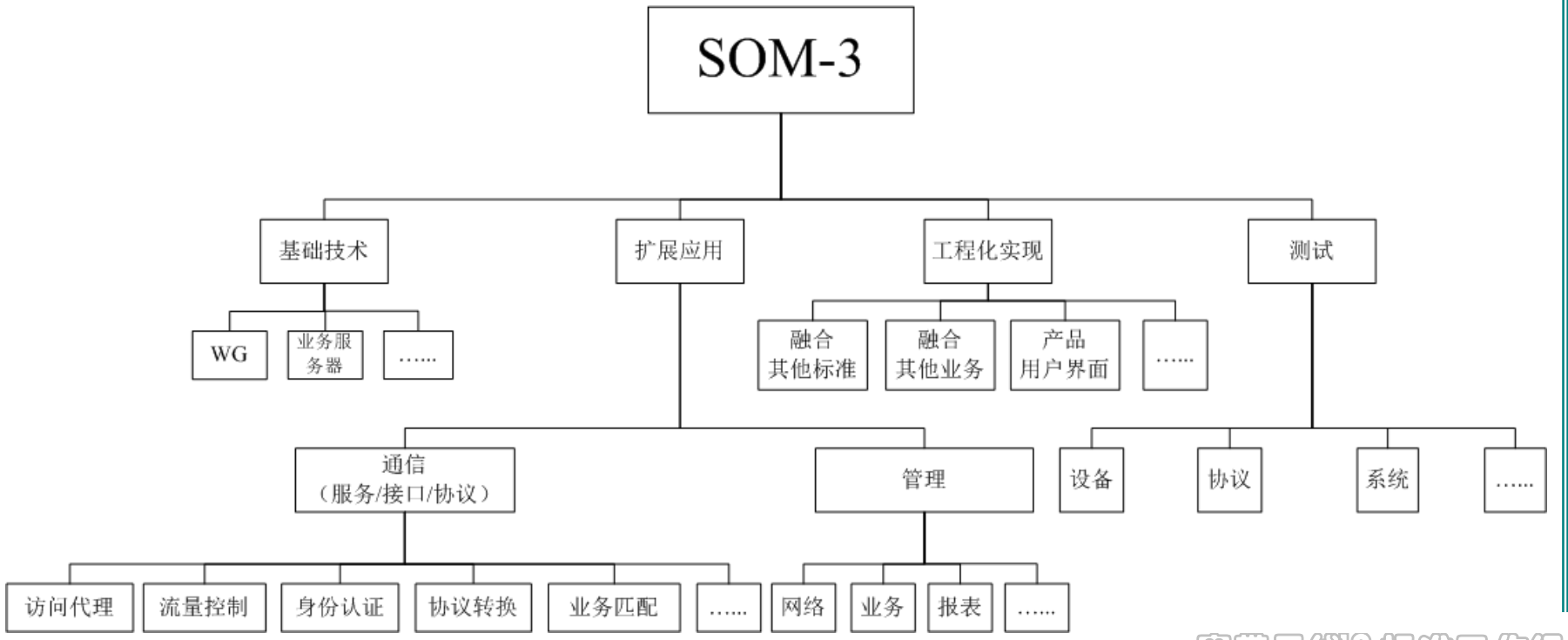
运营级WLAN技术标准体系架构(3)

- SOM-2类标准：从无线局域网接入的合法终端身份被电信核心网络利用和传递过程涉及到的系列标准。



运营级WLAN技术标准体系架构(4)

- SOM-3类标准：从无线局域网接入的合法终端身份经由电信核心网络与互联网业务绑定使用涉及到的系列标准。



RECOMMENDED READING AND WEB SITES

ANDR04 Andrews, M., and Whittaker, J. "Computer Security." *IEEE Security and Privacy*, September/October 2004.

BROW72 Browne, P. "Computer Security—A Survey." *ACM SIGMIS Database*, Fall 1972.

FRAS97 Fraser, B. *Site Security Handbook.* RFC 2196, September 1997.

LAMP04 Lampson, B. "Computer Security in the Real World," *Computer*, June 2004.

NIST95 National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800–12, October 1995.

NRC91 National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, D.C.: National Academy Press, 1991.

SALT75 Saltzer, J., and Schroeder, M. "The Protection of Information in Computer Systems." *Proceedings of the IEEE*, September 1975.

SCHN00 Schneier, B. *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley, 2000.

SHAN77 Shanker, K. "The Total Computer Security Problem: An Overview." *Computer*, June 1977.

STAL08 Stallings, W., and Brown, L. *Computer Security*. Upper Saddle River, NJ: Prentice Hall, 2008.

SUMM84 Summers, R. "An Overview of Computer Security." *IBM Systems Journal*, Vol. 23, No. 4, 1984.

WARE79 Ware, W., ed. *Security Controls for Computer Systems.* RAND Report 609–1. October 1979. http://www.rand.org/pubs/reports/R609-1/R609.1.html

Recommended Web Sites:

- **IETF Security Area:** Material related to Internet security standardization efforts.
- **The Cryptography FAQ:** Lengthy and worthwhile FAQ covering all aspects of cryptography.
- **Tom Dunigan's Security page:** An excellent list of pointers to cryptography and network security Web sites.
- **Peter Gutmann's home page:** Good collection of cryptography material.
- **Helgar Lipma's Cryptology Pointers:** Another excellent list of pointers to cryptography and network security Web sites.
- **Cryptology ePrint archive:** Provides rapid access to recent research in cryptology; consists of a collection of unrefereed papers.
- **IEEE Technical Committee on Security and Privacy:** Copies of their newsletter and information on IEEE-related activities.
- **Computer Security Resource Center:** Maintained by the National Institute of Standards and Technology (NIST); contains a broad range of information on security threats, technology, and standards.
- **Computer and Network Security Reference Index:** A good index to vendor and commercial products, FAQs, newsgroup archives, papers, and other Web sites.
- **Security Focus:** A wide variety of security information, with an emphasis on vendor products and end-user concerns.
- **SANS Institute:** Similar to Security Focus. Extensive collection of white papers.
- **Risks Digest:** Forum on risks to the public in computers and related systems.
- **Institute for Security and Open Methodologies:** An open, collaborative security research community. Lots of interesting information.
- **Center for Internet Security:** Provides freeware benchmark and scoring tools for evaluating security of operating systems, network devices, and applications. Includes case studies and technical papers.