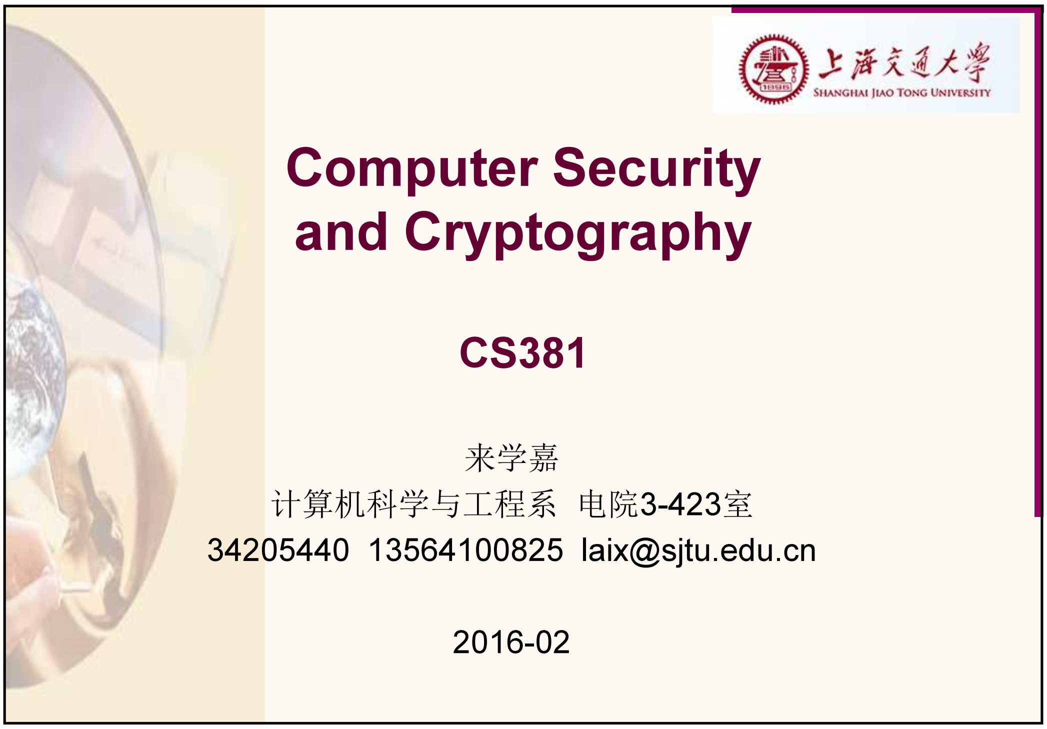
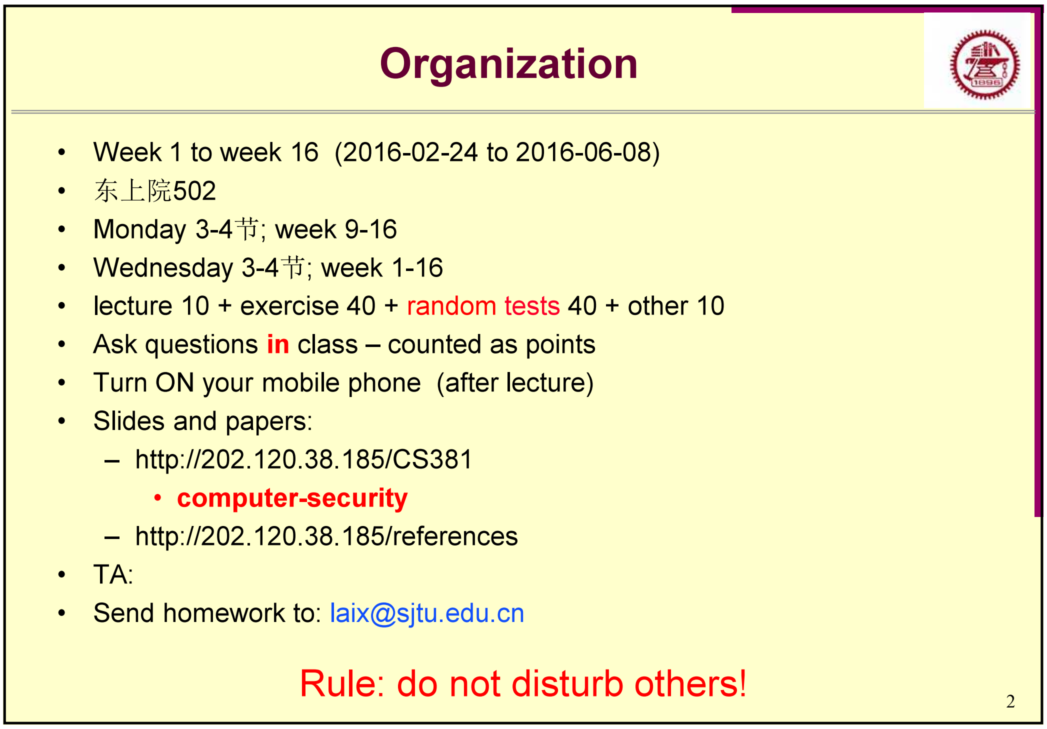


Computer Security and Cryptography

CS381

来学嘉
计算机科学与工程系 电院3-423室
34205440 13564100825 laix@sjtu.edu.cn

2016-02

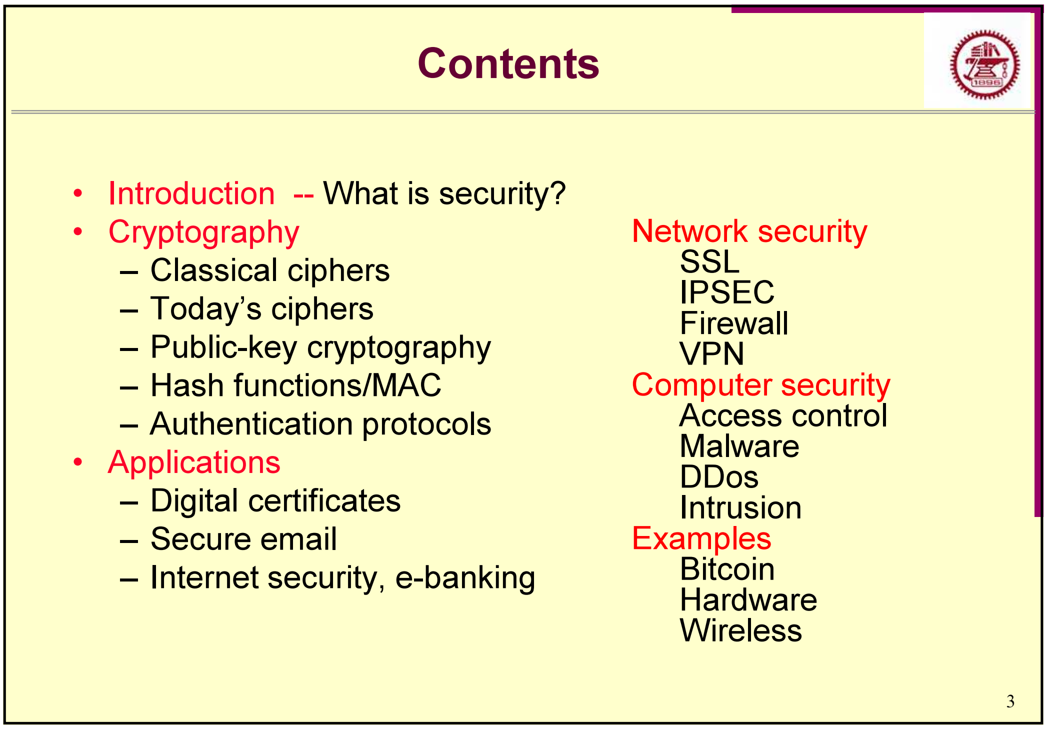


Organization

- Week 1 to week 16 (2016-02-24 to 2016-06-08)
- 东上院502
- Monday 3-4节; week 9-16
- Wednesday 3-4节; week 1-16
- lecture 10 + exercise 40 + random tests 40 + other 10
- Ask questions **in** class – counted as points
- Turn ON your mobile phone (after lecture)
- Slides and papers:
  - http://202.120.38.185/CS381
    - **computer-security**
  - http://202.120.38.185/references
- TA:
- Send homework to: laix@sjtu.edu.cn

Rule: do not disturb others!

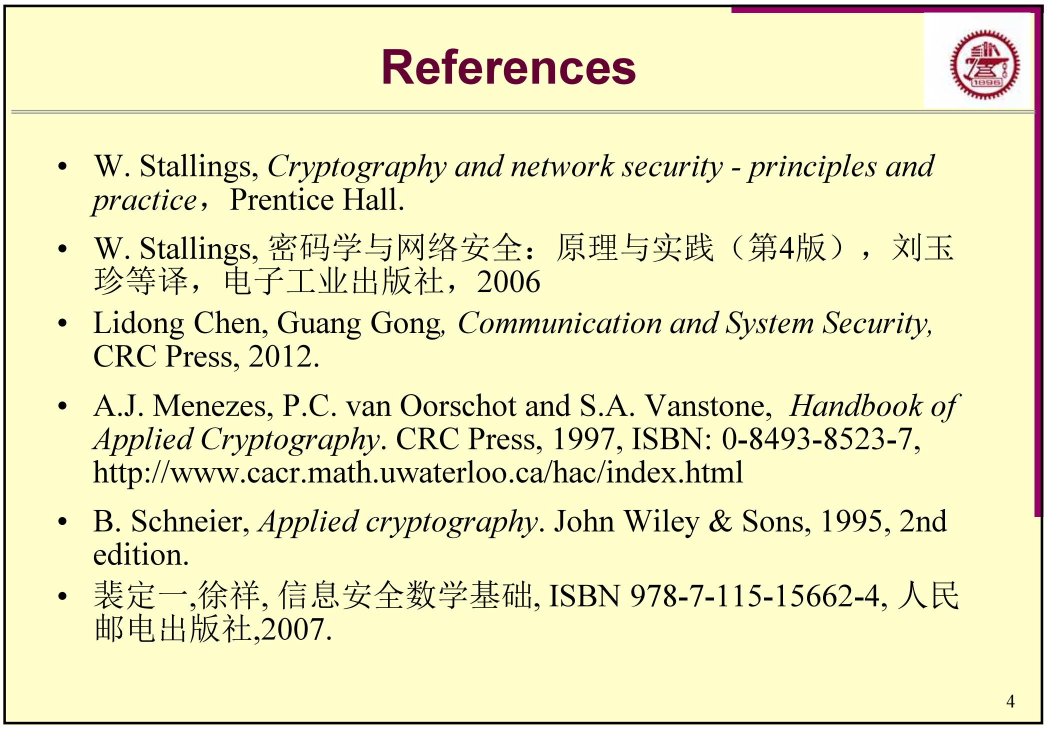
2



Contents

- Introduction -- What is security?
- Cryptography
  - Classical ciphers
  - Today's ciphers
  - Public-key cryptography
  - Hash functions/MAC
  - Authentication protocols
- Applications
  - Digital certificates
  - Secure email
  - Internet security, e-banking

Network security
SSL
IPSEC
Firewall
VPN
Computer security
Access control
Malware
DDos
Intrusion
Examples
Bitcoin
Hardware
Wireless



References

- W. Stallings, *Cryptography and network security - principles and practice*， Prentice Hall.
- W. Stallings, 密码学与网络安全：原理与实践（第4版），刘玉珍等译，电子工业出版社，2006
- Lidong Chen, Guang Gong, *Communication and System Security,* CRC Press, 2012.
- A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1997, ISBN: 0-8493-8523-7, http://www.cacr.math.uwaterloo.ca/hac/index.html
- B. Schneier, *Applied cryptography*. John Wiley & Sons, 1995, 2nd edition.
- 裴定一,徐祥, 信息安全数学基础, ISBN 978-7-115-15662-4, 人民邮电出版社,2007.

Security issues

- Need confidentiality
  - Data transmission
  - Credit card number
  - sensitive information
  - Oldest security
- Need authenticity
  - You got a message: “I am your friend UVW, need 1000 Yuan.
- Your shopping on internet
  - Is it secure?

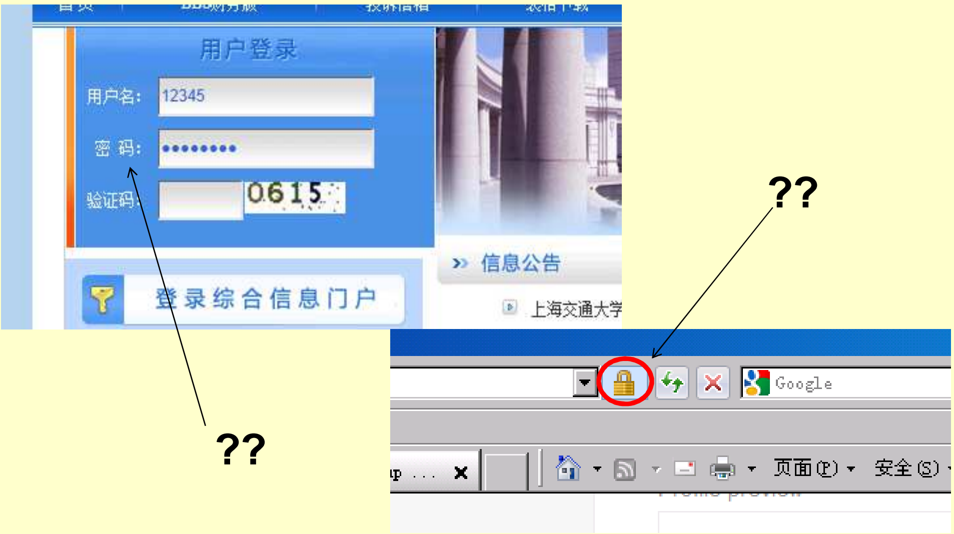
Authentication

- **虎符**:古代传达命令或调兵遣将所用的凭证。一符从中剖为两半,有关双方各执一半,使用时两半互相符合,表示命令验证可信。常作成虎形,故称“虎符”
- matching 2 pieces

implies authenticated

Today: we use Secure-ID, U盾

What are these?



用户登录

用户名: 12345

密 码: ••••••••

验证码: 0615

password

- Password
  - (A→B): Id = Alice
  - (B→A): proof?
  - (A→B): (<u>password</u>)
  - B: check (<u>password</u>)=stored password ?

    If yes, accept A as Alice.

- Bad practice: store password in plaintext. When server is hacked, then passwords leak (many cases)

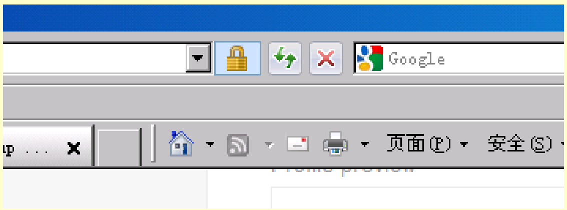
Password

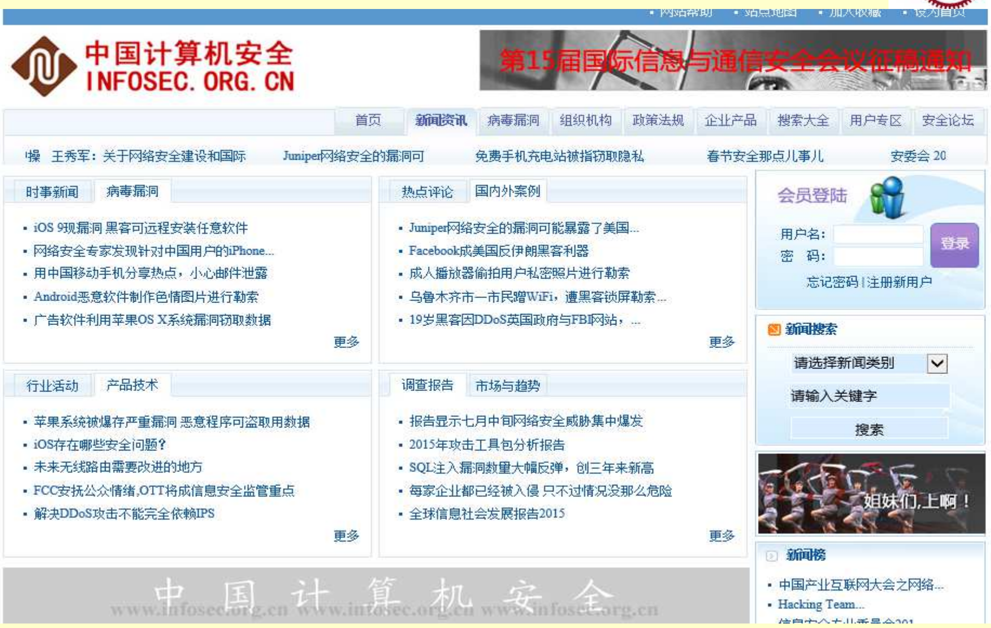
- Standard: store [userID, hash(password)]
  - Hash() is a one-way function
  - If attacker get hash(password), it’s not easy to computer password.
- As passwords are usually simple and easy to guess
  - Use 验证码 to prevent automatic password search
  - Use salt to prevent password guessing:

  hash(salt, password)

Password

- To prevent password leakage during transmission, the communication channel is encrypted by using https/SSL





• 网站帮助 • 站点地图 • 加入收藏 • 设为首页

中国计算机安全
INFOSEC. ORG. CN

第15届国际信息与通信安全会议征稿通知

首页 | 新闻资讯 | 病毒漏洞 | 组织机构 | 政策法规 | 企业产品 | 搜索大全 | 用户专区 | 安全论坛

操 王秀军：关于网络安全建设和国际 Juniper网络安全的漏洞可 免费手机充电站被指窃取隐私 春节安全那点儿事儿 安委会 20

时事新闻 | 病毒漏洞

- iOS 9现漏洞 黑客可远程安装任意软件
- 网络安全专家发现针对中国用户的iPhone...
- 用中国移动手机分享热点，小心邮件泄露
- Android恶意软件制作色情图片进行勒索
- 广告软件利用苹果OS X系统漏洞窃取数据

更多

热点评论 | 国内外案例

- Juniper网络安全的漏洞可能暴露了美国...
- Facebook成美国反伊朗黑客利器
- 成人播放器偷拍用户私密照片进行勒索
- 乌鲁木齐市一市民蹭WiFi，遭黑客锁屏勒索...
- 19岁黑客因DDoS英国政府与FBI网站，...

更多

会员登陆

用户名：
密 码：
登录
忘记密码 | 注册新用户

新闻搜索

请选择新闻类别
请输入关键字
搜索

行业活动 | 产品技术

- 苹果系统被爆存严重漏洞 恶意程序可盗取用数据
- iOS存在哪些安全问题?
- 未来无线路由需要改进的地方
- FCC安抚公众情绪,OTT将成信息安全监管重点
- 解决DDoS攻击不能完全依赖IPS

更多

调查报告 | 市场与趋势

- 报告显示七月中旬网络安全威胁集中爆发
- 2015年攻击工具包分析报告
- SQL注入漏洞数量大幅反弹，创三年来新高
- 每家企业都已经被入侵 只不过情况没那么危险
- 全球信息社会发展报告2015

更多

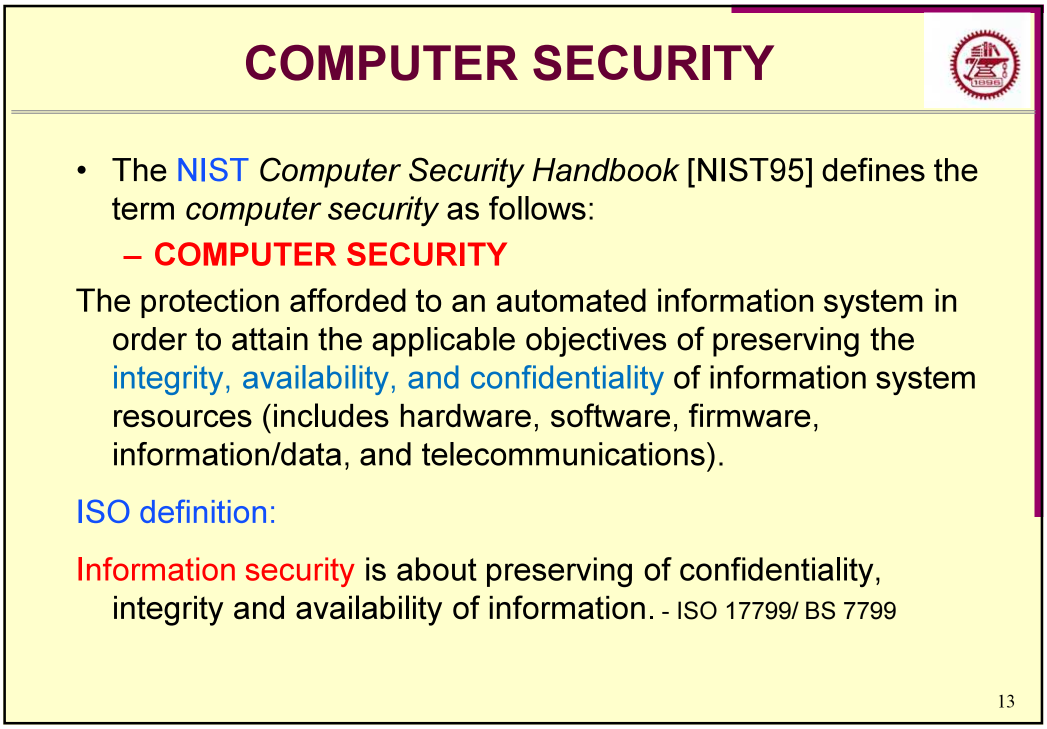
新闻榜

- 中国产业互联网大会之网络...
- Hacking Team...
- 信息安全专业委员会201

中 国 计 算 机 安 全
www.infosec.org.cn www.infosec.org.cn www.infosec.org.cn

Events

- Snowden
- Passwords leakage (CSDN, Walmart,RSA,携程..)
- Flame (most sophisticated attack)
- Heartbleed (big trouble caused by small mistake)
- Bitcoin (real use of cryptography)
- …..



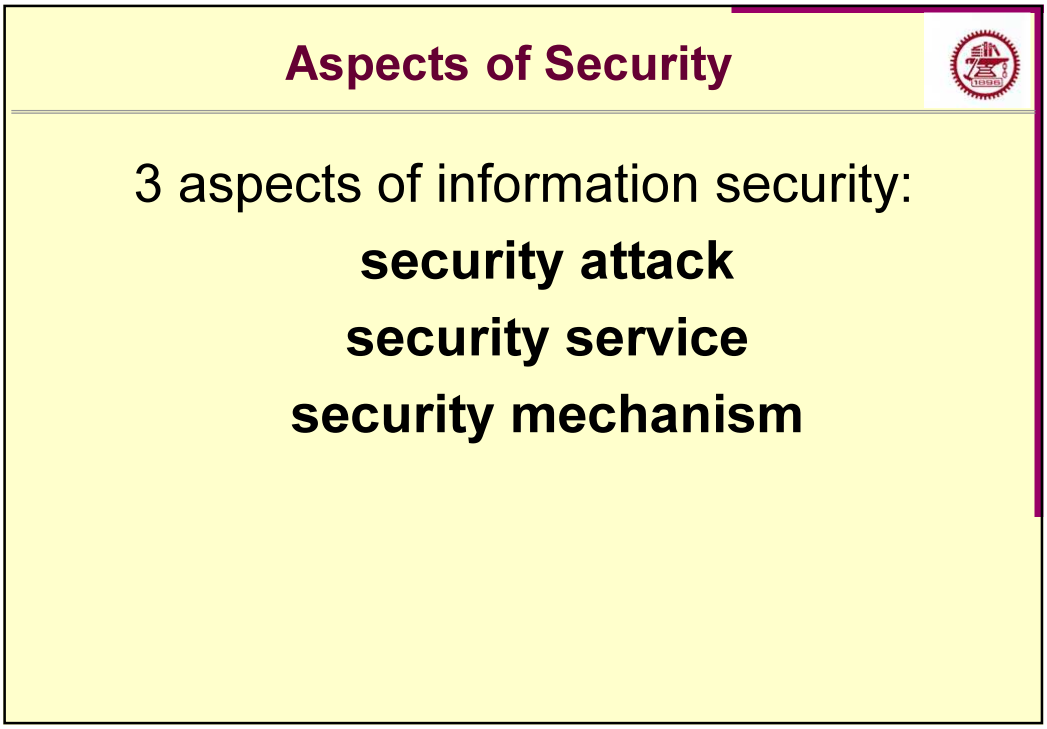
COMPUTER SECURITY

- The NIST *Computer Security Handbook* [NIST95] defines the term *computer security* as follows:
  - 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).

ISO definition:

Information security is about preserving of confidentiality, integrity and availability of information. - ISO 17799/ BS 7799



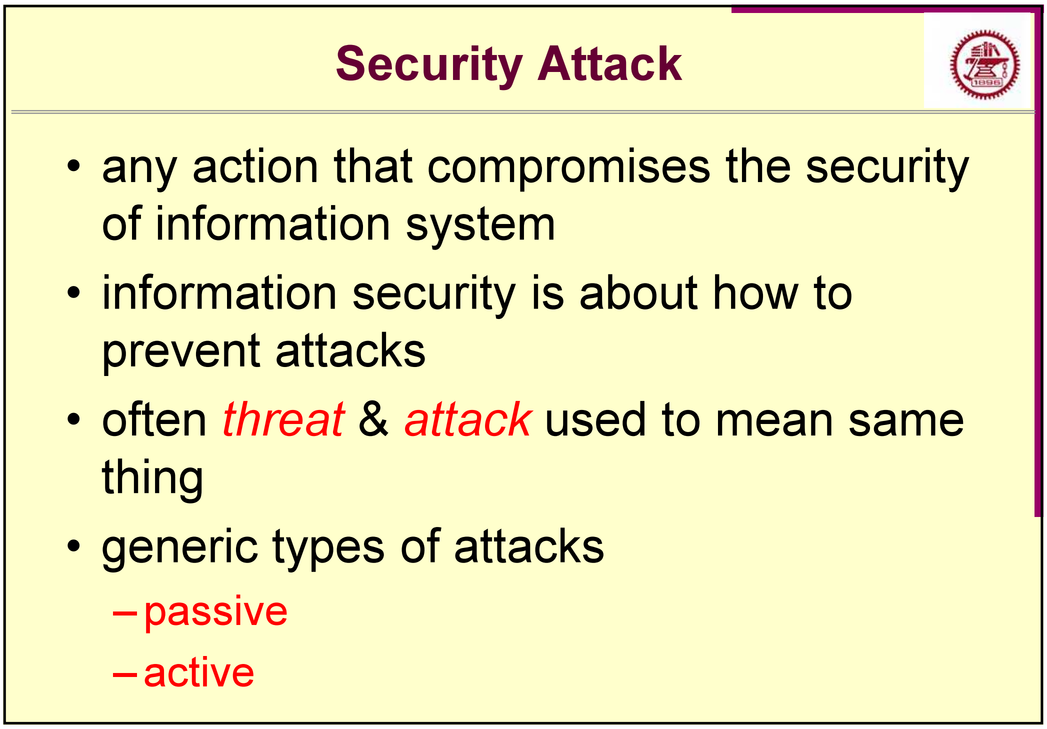
Aspects of Security

3 aspects of information security:

security attack

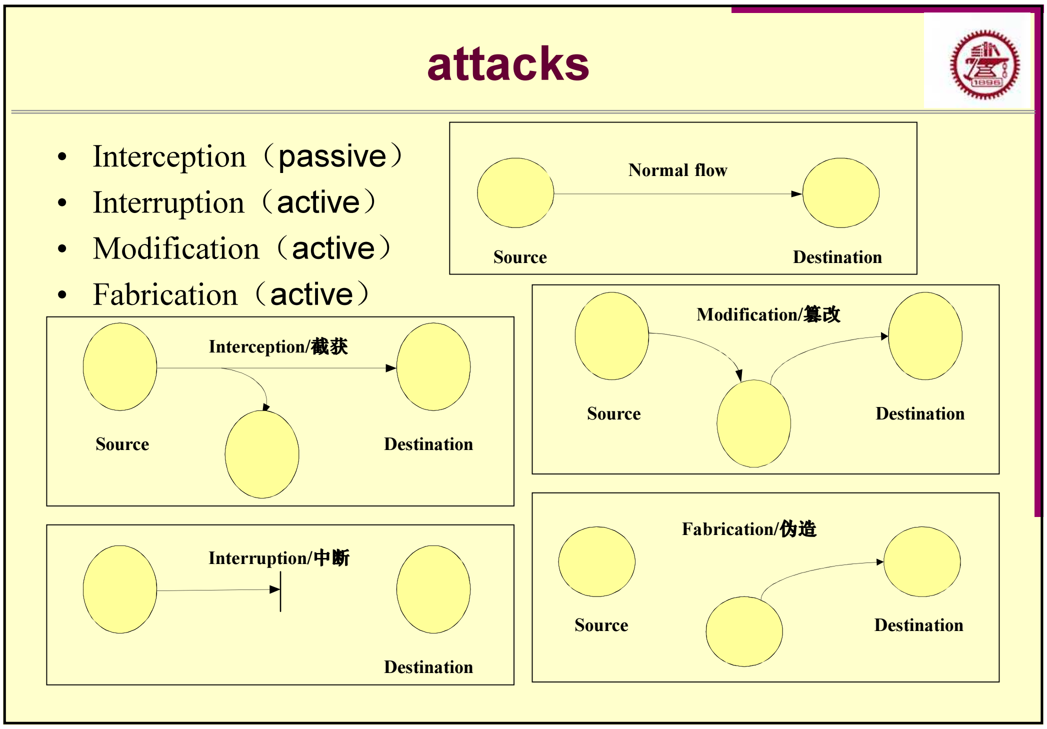
security service

security mechanism



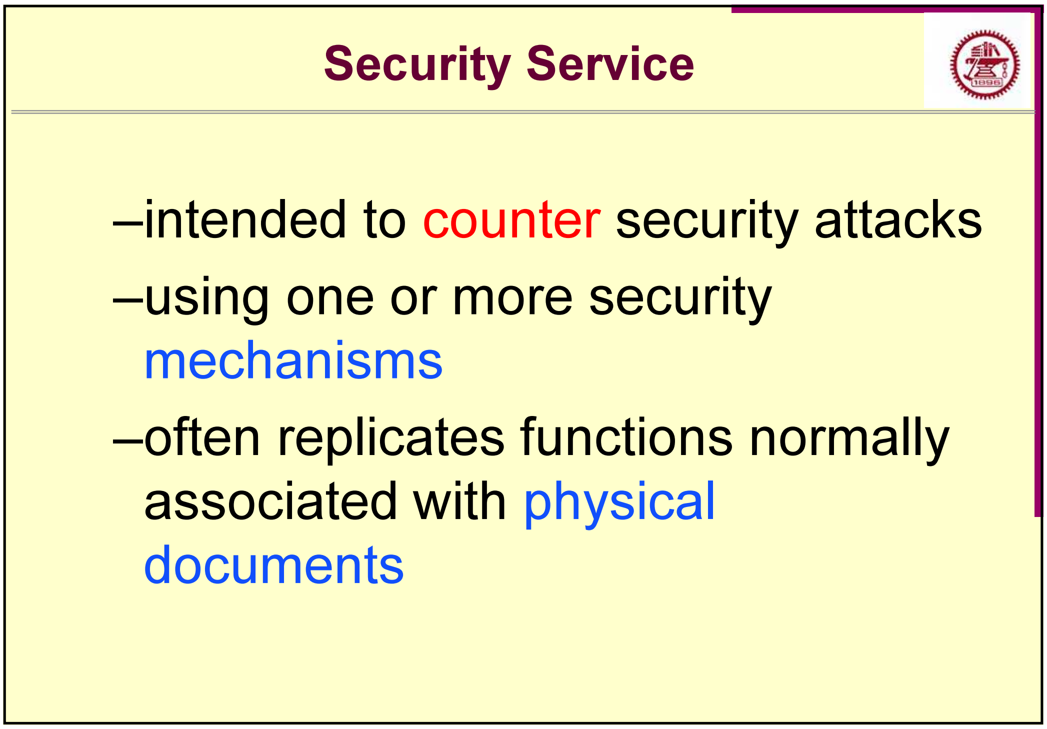
Security Attack

- any action that compromises the security of information system
- information security is about how to prevent attacks
- often *threat* & *attack* used to mean same thing
- generic types of attacks
  - passive
  - active



attacks

- Interception（passive）
- Interruption（active）
- Modification（active）
- Fabrication（active）

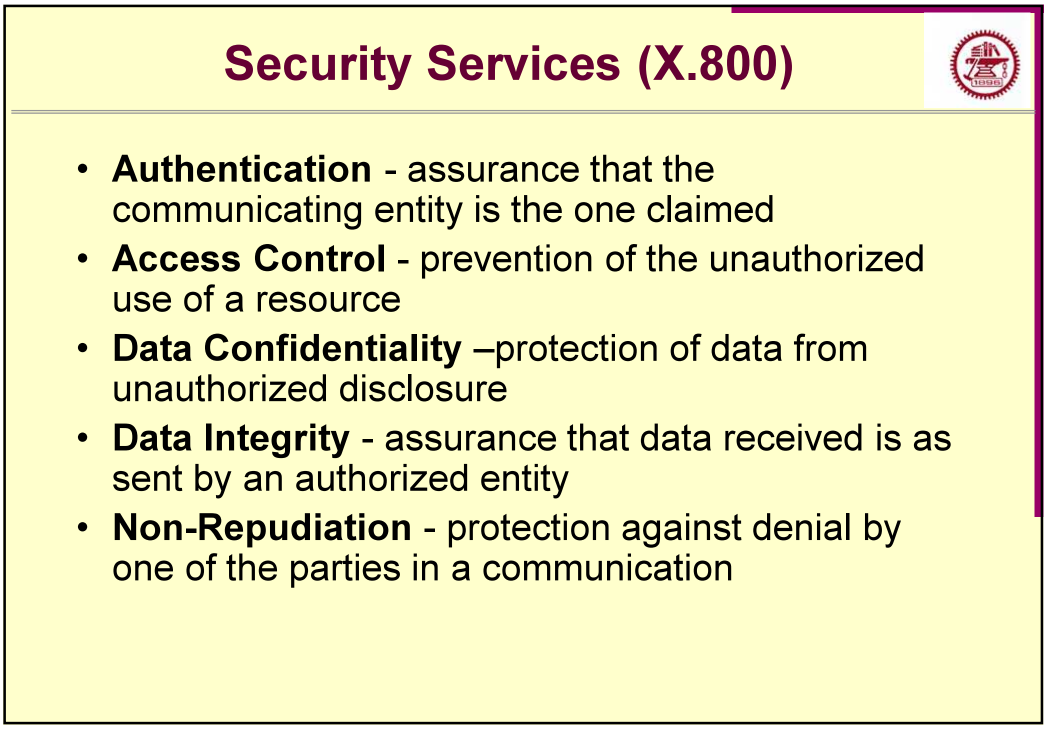


Security Service

–intended to counter security attacks

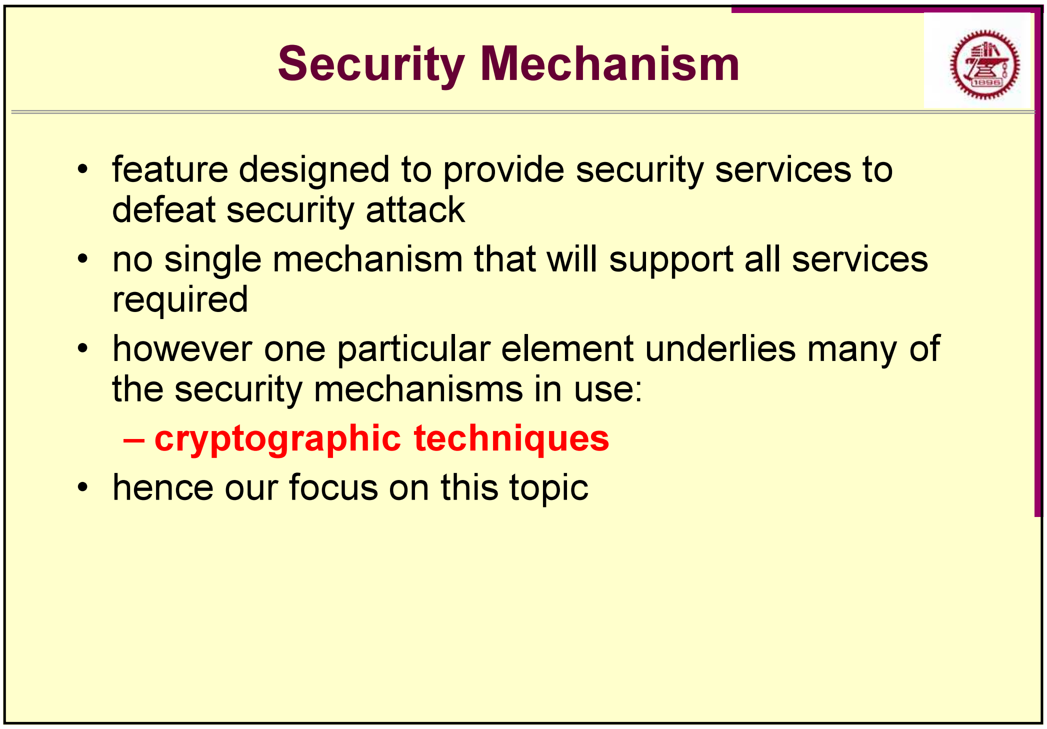
–using one or more security mechanisms

–often replicates functions normally associated with physical documents



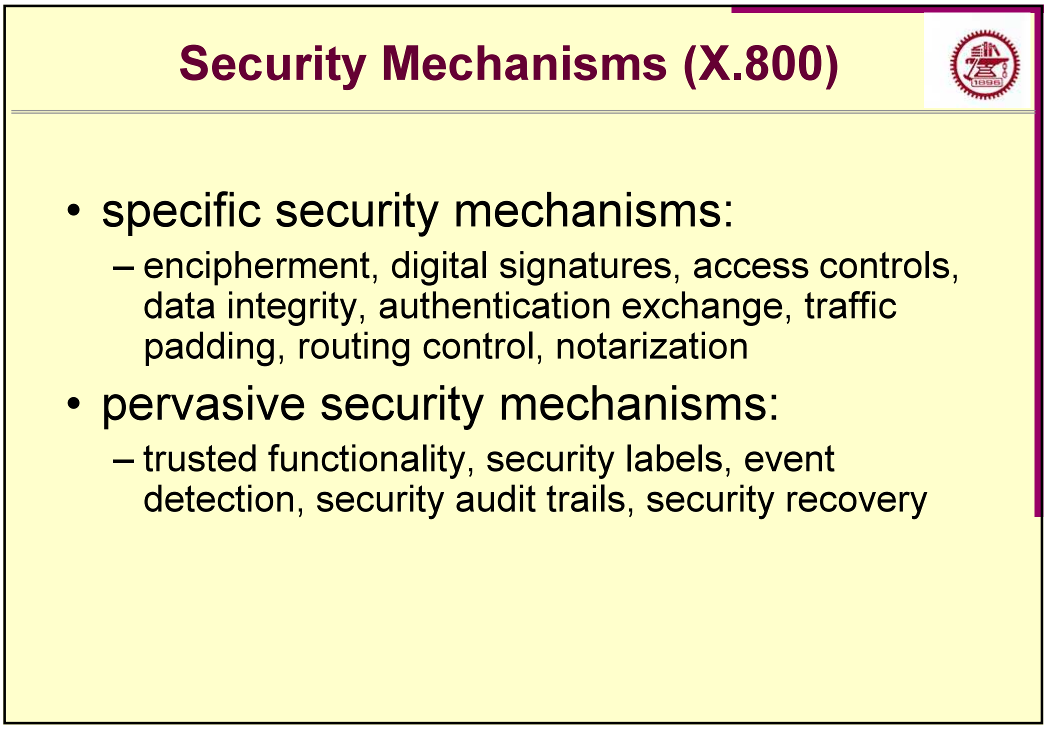
Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **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



Security Mechanism

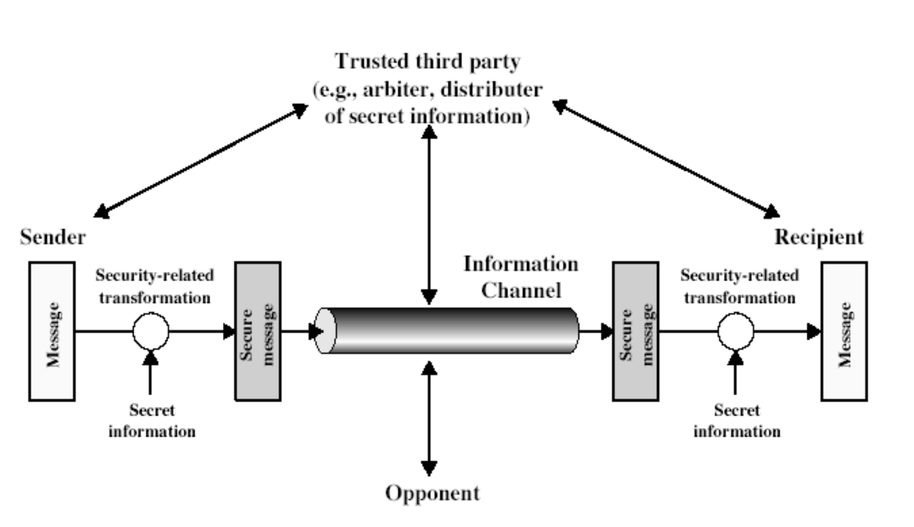
- feature designed to provide security services to defeat security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic



Security Mechanisms (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

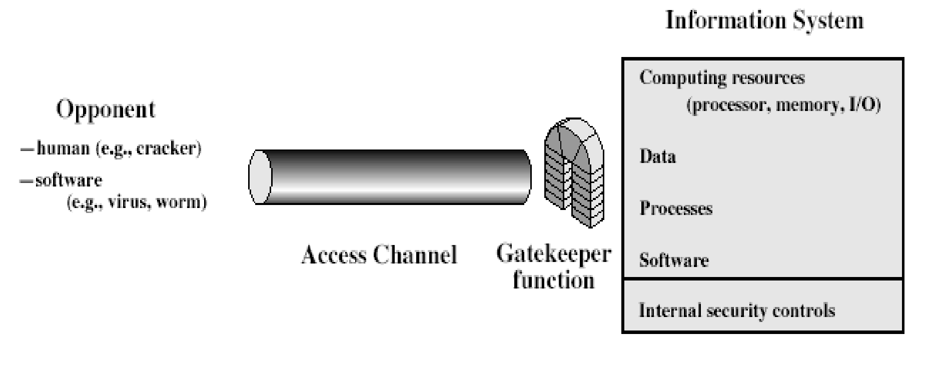
Model for Network Security



Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Access Security



This model considers the controlled access to information or resources on a computer system, in the presence of possible opponents.
Some cryptographic techniques are useful

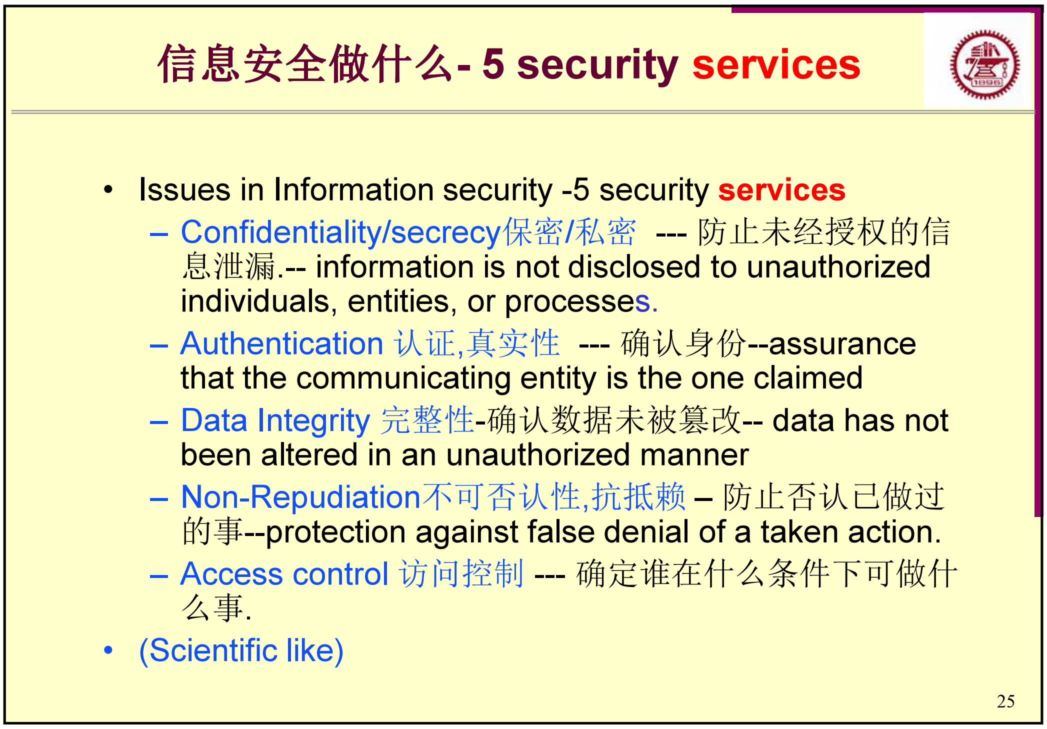
Definition of SECURITY

- NIST *Computer Security Handbook* [NIST95] definition:
  - 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).

- ISO definition:

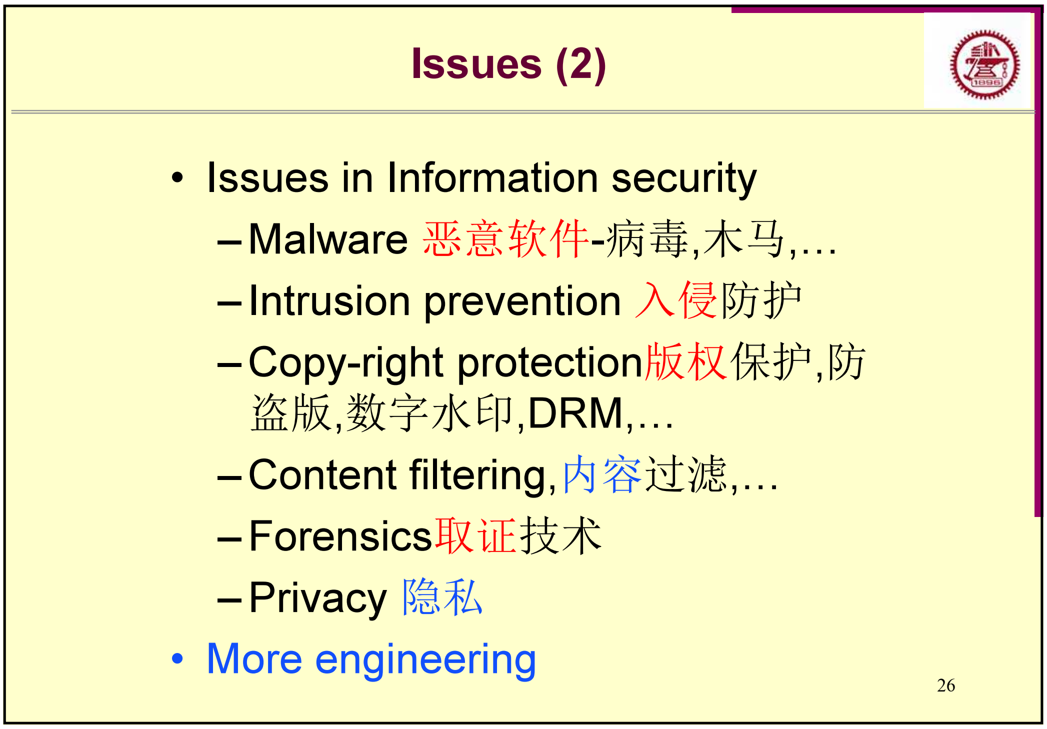
Information security is about preserving of confidentiality, integrity and availability of information. - ISO 17799/ BS 7799



信息安全做什么- 5 security services

- Issues in Information security -5 security **services**
  - Confidentiality/secrecy保密/私密 --- 防止未经授权的信息泄漏.-- information is not disclosed to unauthorized individuals, entities, or processes.
  - Authentication 认证,真实性 --- 确认身份--assurance that the communicating entity is the one claimed
  - Data Integrity 完整性-确认数据未被篡改-- data has not been altered in an unauthorized manner
  - Non-Repudiation不可否认性,抗抵赖 – 防止否认已做过的事--protection against false denial of a taken action.
  - Access control 访问控制 --- 确定谁在什么条件下可做什么事.
- (Scientific like)

25



Issues (2)

- Issues in Information security
  - Malware 恶意软件-病毒,木马,…
  - Intrusion prevention 入侵防护
  - Copy-right protection版权保护,防盗版,数字水印,DRM,…
  - Content filtering,内容过滤,…
  - Forensics取证技术
  - Privacy 隐私
- More engineering

26

信息安全的定义？

- 信息安全在于保证信息的机密性、完整性、可用性三种属性不被破坏。
- 信息安全是一门涉及数学、物理等基础学科，计算机科学与技术、通信工程、 电子信息、网络技术等应用学科，法律、管理、心理学、伦理学、社会学等人文学科，因此，信息安全学科具有多学科交叉的特点。从信息安全技术应用的角度来讲，涉及到软件技术、信息安全技术、通信技术等，还与安全服务、安全管理以及公共信息安全等密切相关，因此，信息安全技术具有高度综合性的特点，信息安全技术的应用与管理密切相关。
- 信息安全学科是一门新兴的学科，它涉及通信学、计算机科学、信息学、密码学和数学等多个学科。以及许多技术，如信息加密技术、安全集成电路技术、安全管理和安全体系架构技术、安全评估和工程管理技术、电磁泄露防护技术、安全操作平台技术、信息侦测技术、计算机病毒防范技术、系统安全增强技术、安全审计和入侵检测、预警技术、内容分级监管技术和信息安全攻防技术等等。

What is information security?

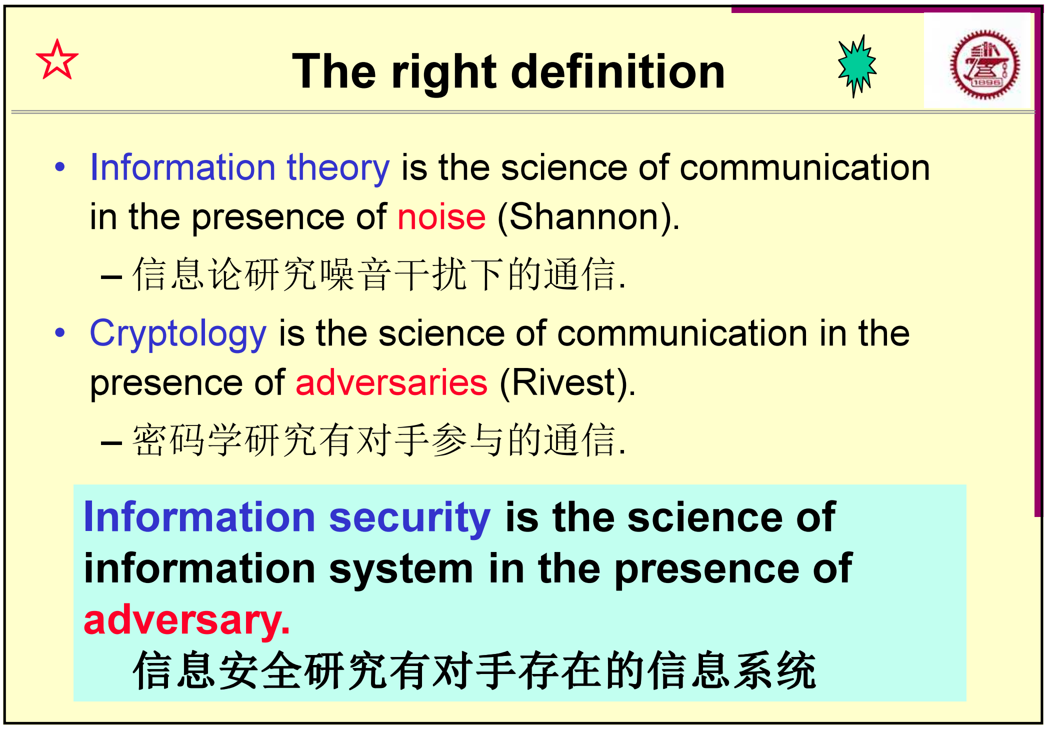
- There are many issues in information security, but what is information security?

The ISO definition:

Information security is about preserving of confidentiality, integrity and availability of information. - ISO 17799/ BS 7799

This definition is not satisfactory:

- cryptography (only a small part)
- +availability (beyond security)

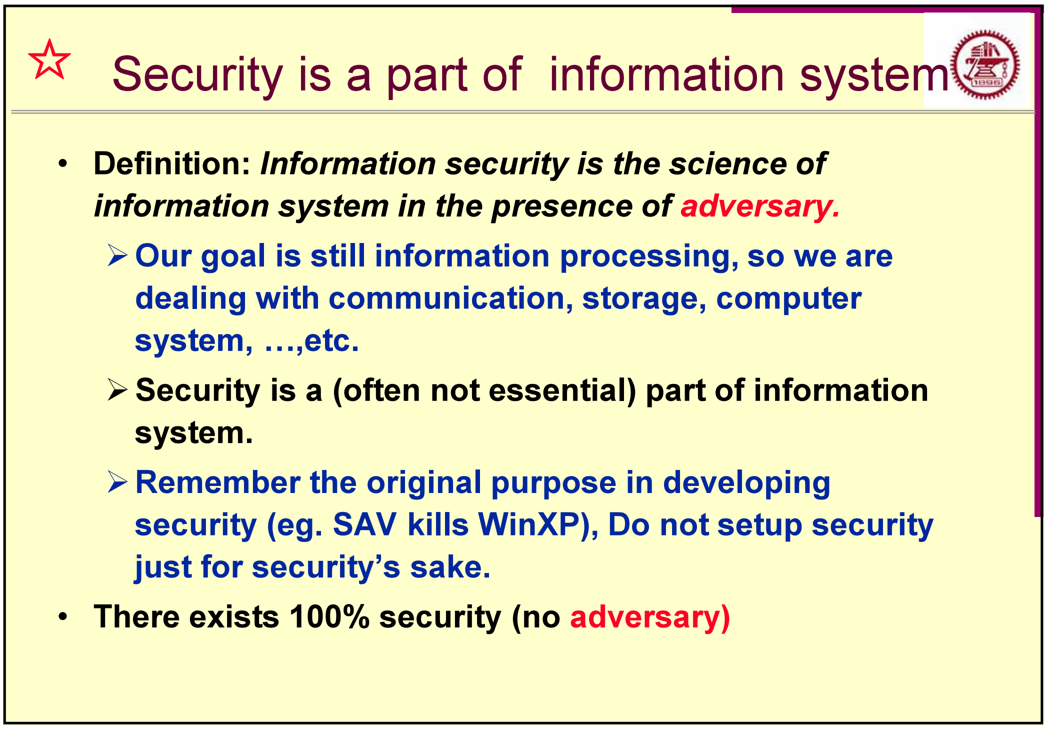


☆ The right definition

- Information theory is the science of communication in the presence of noise (Shannon).
  - 信息论研究噪音干扰下的通信.
- Cryptology is the science of communication in the presence of adversaries (Rivest).
  - 密码学研究有对手参与的通信.

Information security is the science of information system in the presence of adversary.

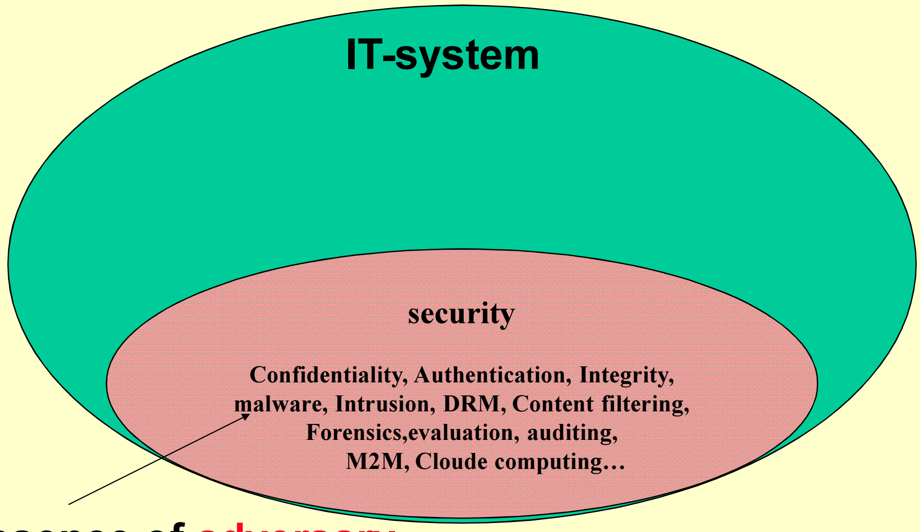
信息安全研究有对手存在的信息系统



☆ Security is a part of information system

- **Definition: *Information security is the science of information system in the presence of adversary.***
  - **Our goal is still information processing, so we are dealing with communication, storage, computer system, …,etc.**
  - **Security is a (often not essential) part of information system.**
  - **Remember the original purpose in developing security (eg. SAV kills WinXP), Do not setup security just for security's sake.**
- **There exists 100% security (no adversary)**

Security in IT system

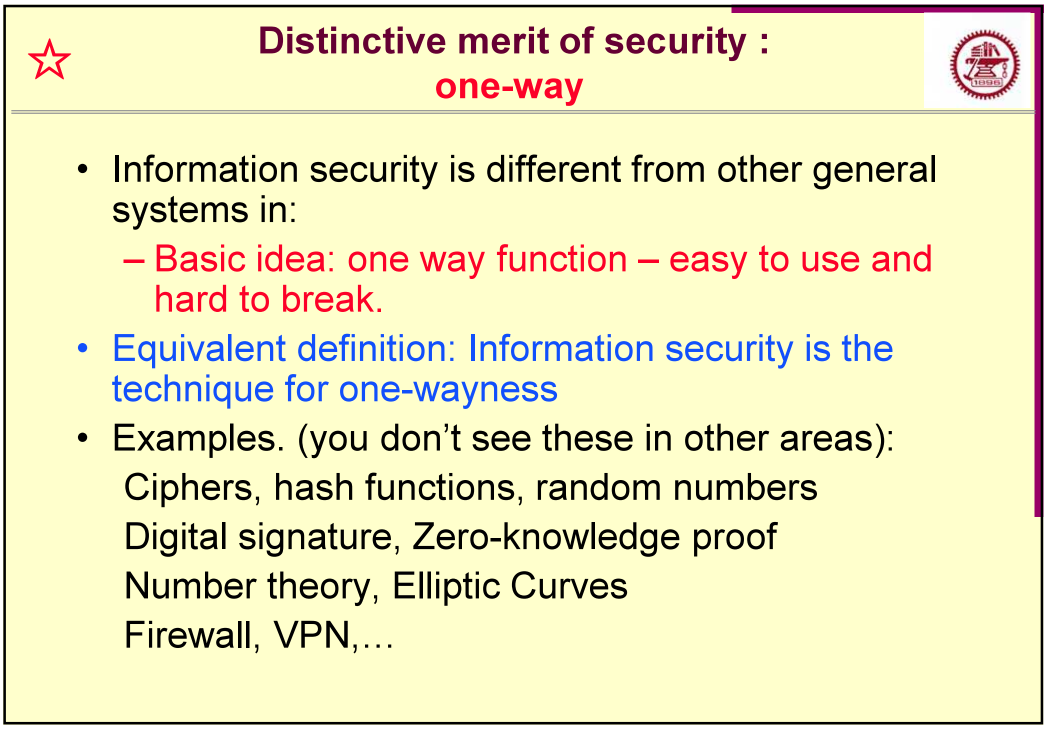


IT-system
security
Confidentiality, Authentication, Integrity,
malware, Intrusion, DRM, Content filtering,
Forensics,evaluation, auditing,
M2M, Cloude computing…

presence of adversary

Remark 2. Security is becoming necessary

- **Security is becoming necessary** because the presence of adversary – is increasing:
- IT-techniques is spreading in our life
- The threshold for making damage is getting lower
- Outside enemy and Insider, even ourselves
- Attacks become organized actions, not only individual activity: virus-crime-APT



☆ Distinctive merit of security : one-way

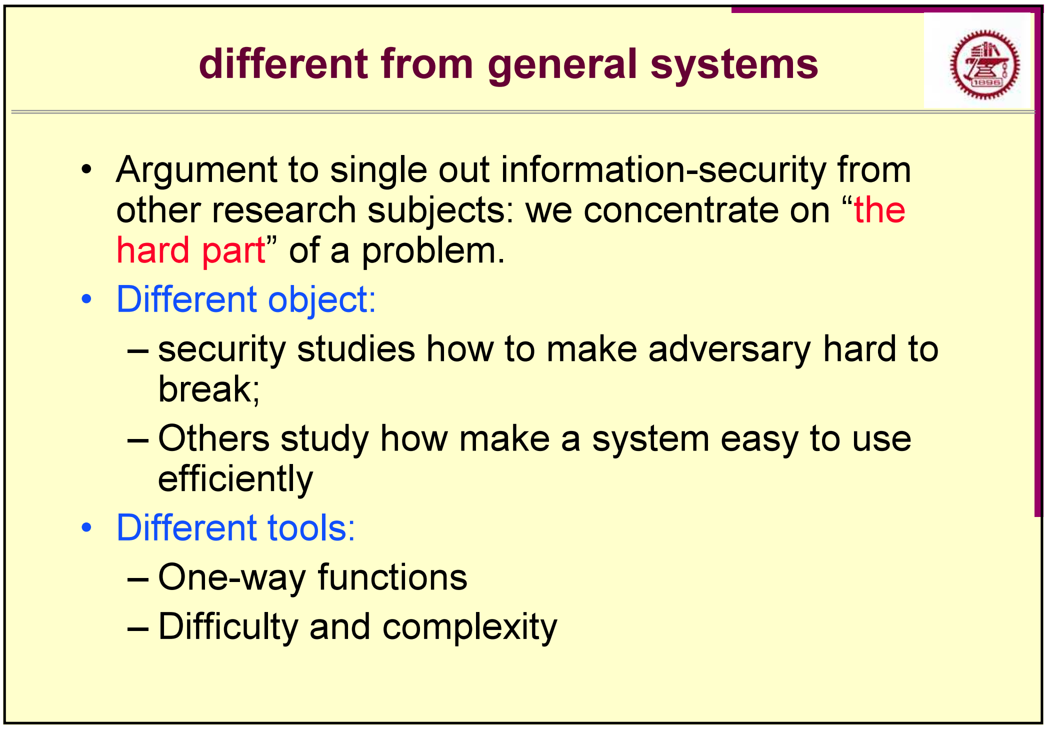
- Information security is different from other general systems in:
  - Basic idea: one way function – easy to use and hard to break.
- Equivalent definition: Information security is the technique for one-wayness
- Examples. (you don't see these in other areas):

  Ciphers, hash functions, random numbers

  Digital signature, Zero-knowledge proof

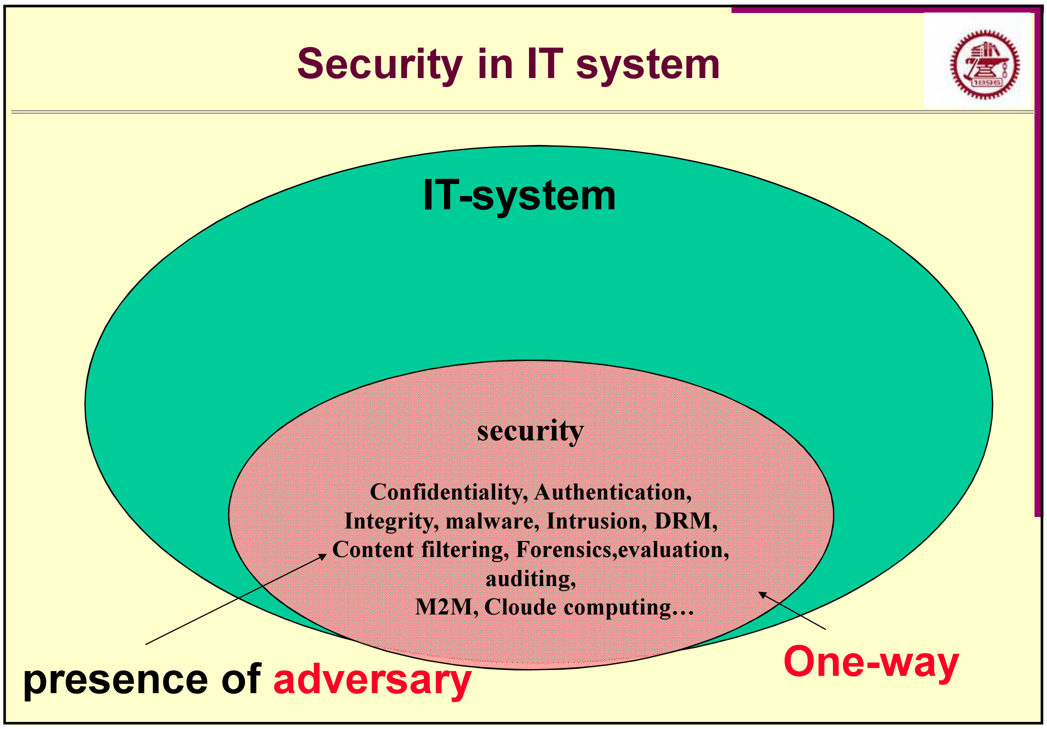
  Number theory, Elliptic Curves

  Firewall, VPN,…



different from general systems

- Argument to single out information-security from other research subjects: we concentrate on "the hard part" of a problem.
- Different object:
  - security studies how to make adversary hard to break;
  - Others study how make a system easy to use efficiently
- Different tools:
  - One-way functions
  - Difficulty and complexity



Security in IT system

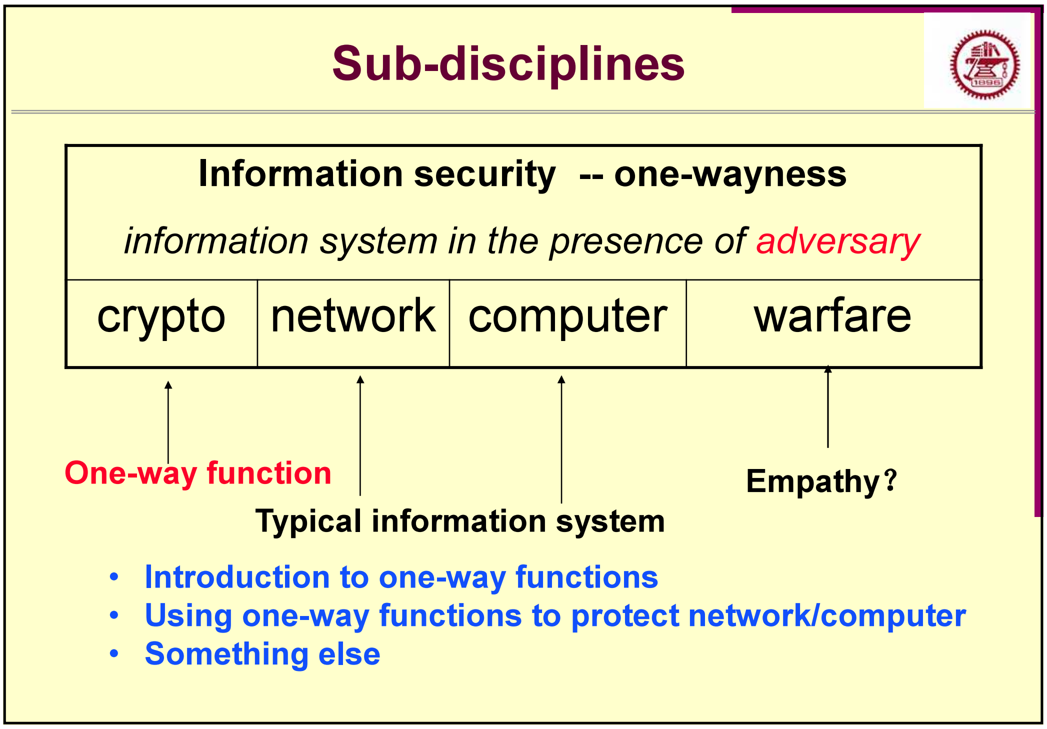
IT-system

security

Confidentiality, Authentication, Integrity, malware, Intrusion, DRM, Content filtering, Forensics,evaluation, auditing, M2M, Cloude computing…

presence of adversary

One-way



Sub-disciplines

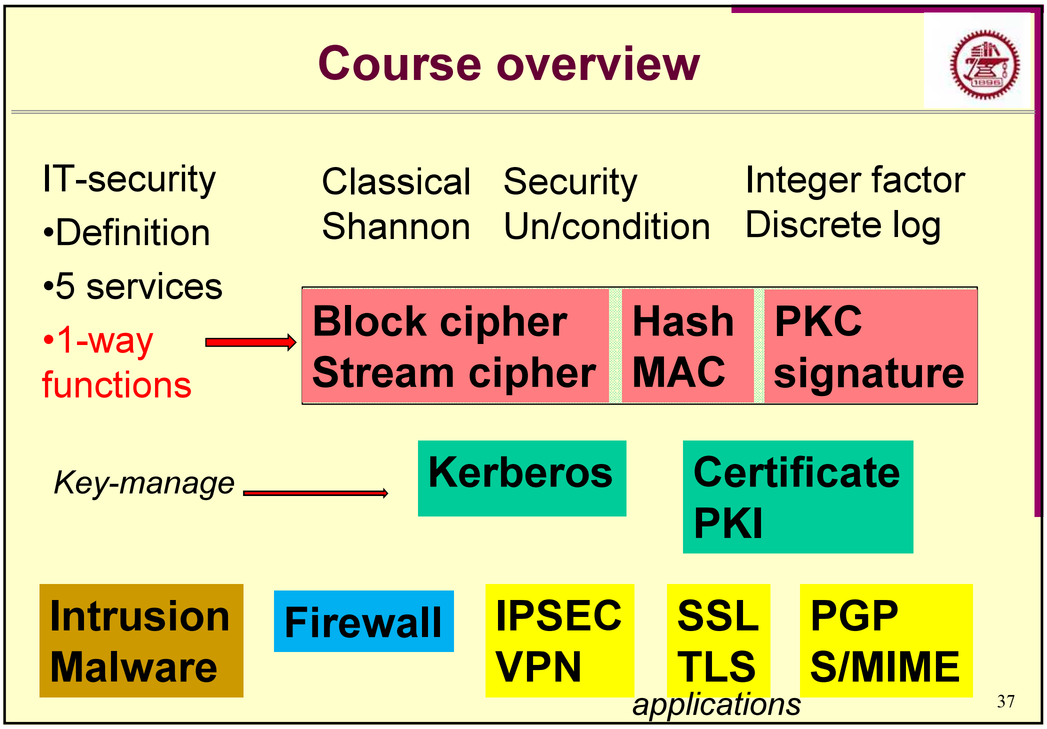
Information security -- one-wayness *information system in the presence of adversary*			
crypto	network	computer	warfare

One-way function

Typical information system

Empathy?

- Introduction to one-way functions
- Using one-way functions to protect network/computer
- Something else



Course overview

IT-security
- Definition
- 5 services
- 1-way functions

Classical
Shannon

Security
Un/condition

Integer factor
Discrete log

Block cipher
Stream cipher

Hash
MAC

PKC
signature

Key-manage

Kerberos

Certificate
PKI

Intrusion
Malware

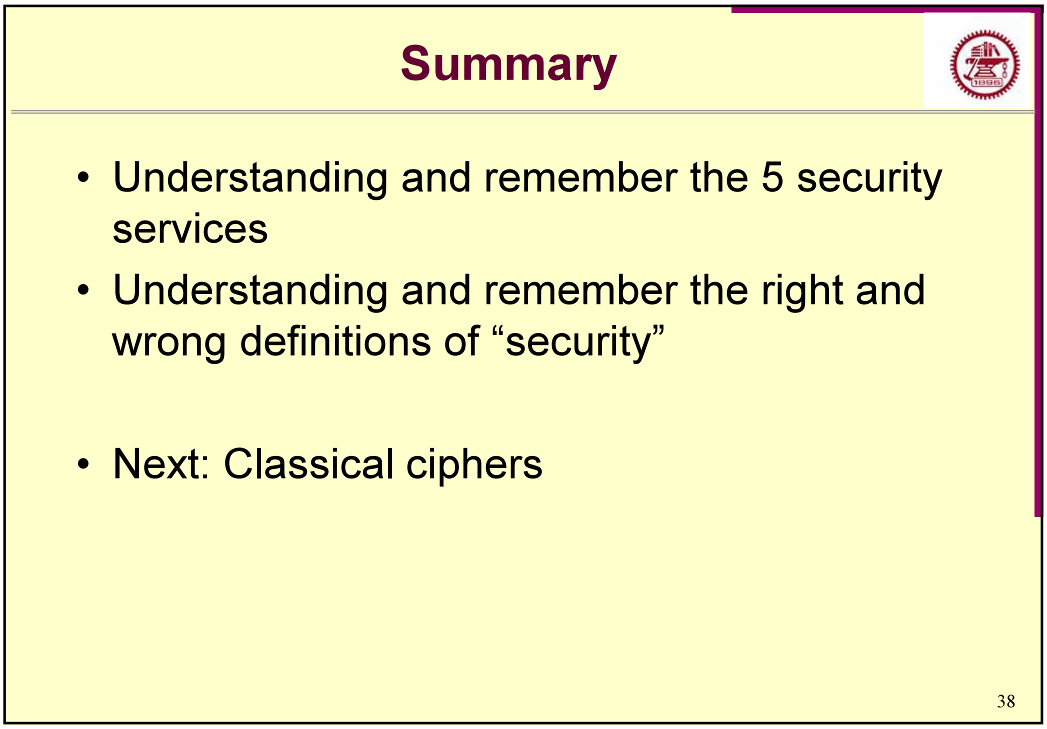
Firewall

IPSEC
VPN

SSL
TLS

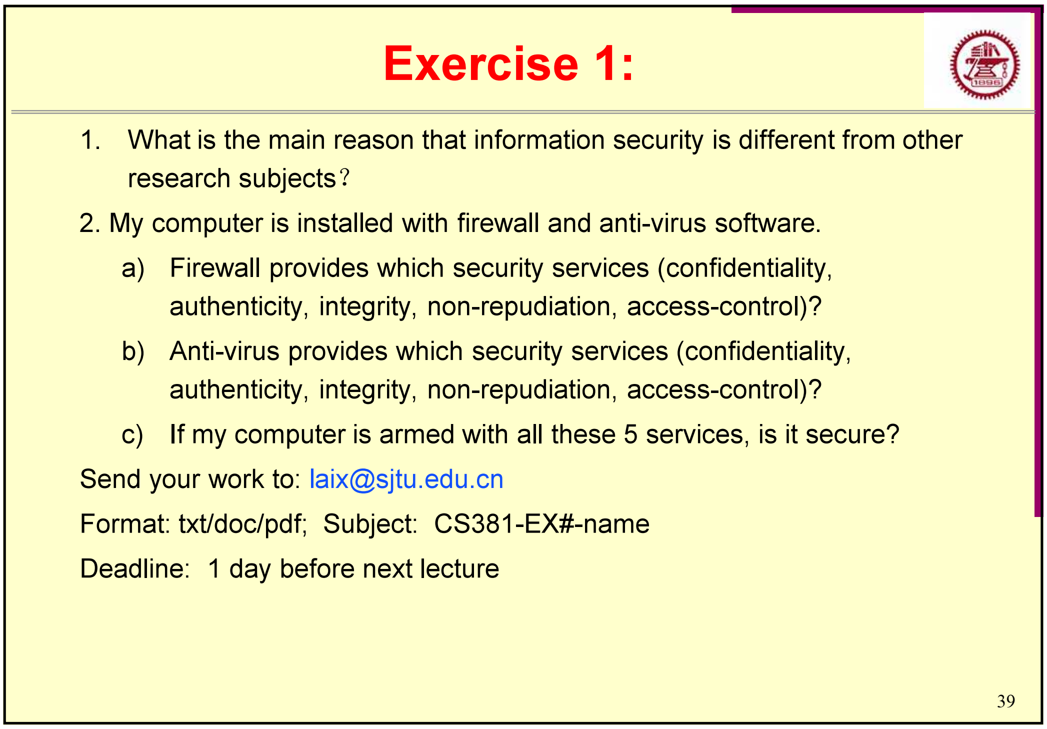
PGP
S/MIME

applications



Summary

- Understanding and remember the 5 security services
- Understanding and remember the right and wrong definitions of “security”
- Next: Classical ciphers



Exercise 1:

1. What is the main reason that information security is different from other research subjects？

2. My computer is installed with firewall and anti-virus software.
   a) Firewall provides which security services (confidentiality, authenticity, integrity, non-repudiation, access-control)?
   b) Anti-virus provides which security services (confidentiality, authenticity, integrity, non-repudiation, access-control)?
   c) If my computer is armed with all these 5 services, is it secure?

Send your work to: laix@sjtu.edu.cn

Format: txt/doc/pdf; Subject: CS381-EX#-name

Deadline: 1 day before next lecture