信息安全基础

Shandong Agricultural University College of Information Science and Engineering

山东农业大学信息学院

信息安全（Information Security，InfoSec）

- 指信息在产生、传输、处理和存储过程中不被泄露或破坏，确保信息的可用性、保密性、完整性、不可否认性，并保证信息系统的可靠性和可控性。
- 凡是涉及到信息的安全因素的技术和理论，都是信息安全所要研究的范畴，也是信息安全所要实现的目标。

早期的信息安全可通过物理和管理方法实现。

信息技术极大发挥作用是从计算机诞生后开始。从此，信息安全面临的威胁也就越来越复杂。

- 信息技术的技术支柱与信息安全的核心是什么？

- 信息技术的形成与发展有赖于复杂技术的结合：
  - 计算机技术
  - 多媒体技术
  - 通信与网络技术
  - 传感技术
  - 控制技术
- **可以说，计算机技术、通信技术是信息技术的两大支柱，而密码技术是信息安全的核心。而计算机安全和互联网安全两大范畴没有明确的界定。**

课程内容层次

引言：信息安全概述

一、密码学基础

二、网络安全应用

三、系统安全

信息安全概述

1 信息安全的CIA 三元组

2 OSI安全体系架构

- 请问如何实现一个安全的捎信过程？
  - 文字乱序（加密）
  - 隐藏暗号（防篡改）
  - 盖手印（真实性）
  - 沿途盖章（追溯）
  - 要在有限的时间内送达，可请一武士护送，保证信息可用性

1.信息安全的CIA 三元组

- 信息安全的目标：
  - 机密性（**Confidentiality**）—— 维持施加在数据访问和释放上的授权限制，确保信息在存储、使用、传输过程中可控，不会泄漏给非授权用户或实体。
  - 完整性（**Integrity**）—— 确保信息在存储、使用、传输过程中不会被非授权用户篡改，同时还要防止授权用户对系统及信息进行不恰当的篡改，保持信息内、外部表示的一致性。
  - 可用性（**Availability**）—— 确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

安全违规等级举例

美国国家标准与技术研究院（National Institute of Standards and Technology，NIST） 的联邦信息的安全分级标准与信息系统(FIPS199)指出了CIA三个安全目标，并给将安全违规分成三种等级。

违规等级 / 安全目标	低级	中级	高级
机密性	学生通信录信息	学生入学信息	学生成绩信息
完整性	民意测验信息	论坛注册用户信息	病人的过敏信息
可用性（成分和服务越关键，需要的可用性等级越高）	服务电话的自动应答程序（可转人工服务）	大学公共网站	为关键系统提供认证服务的系统（网通ppoe拨号）

- 人们认为在安全领域有必要对**CIA**补充或加强
  - 真实性：**authenticity**，可验证身份或来源
  - 责任性：可追溯性**Accountability**、不可抵赖性**Non-repudiation**

满足以上属性，就说明信息的使用符合安全要求。

计算机和网络安全实现起来往往比较复杂，因为面临种种困难：

- 安全往往是信息系统设计结束后的一种事后考虑；
- 攻击者的有利之处在于只要发现一个弱点就可以，而设计者需要考虑各种威胁，发现和堵住所有弱点；
- 符合安全的5个属性的安全机制和算法的设计会非常复杂，要决定这些机制的合适的使用场合，安全机制设计的安全性也不容易证明。
- 安全要求经常性检测，且在使用上有很多限制，所以在有效性和易用性上对信息应用是一种限制。
- ……

- **幸运的是，我们有了一套参照标准——OSI安全体系架构，先通过它对一些安全概念进行简要概览。**

2. OSI安全体系架构

系统定义了安全需求以及满足这些安全需求的方法。

→ 1）分析安全攻击**attack**，攻击决定了需求

→ 2）制定安全目标：安全服务**service**

→ 3）实现服务的具体安全机制**mechanism**

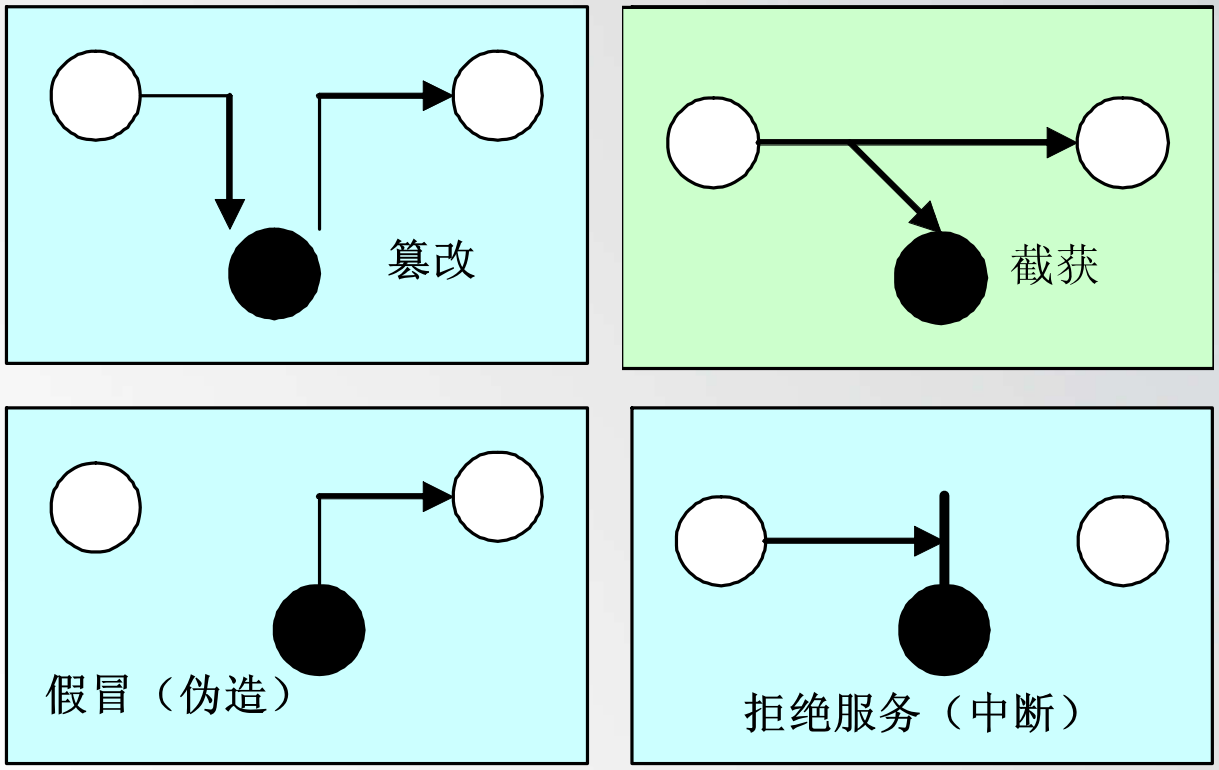
1）安全攻击attack

“防”前先要了解“攻”，最典型的划分安全攻击的方法：

- 被动攻击passive attack
  - 本质是窃听和监视数据传输，目标是获取传输的数据信息。两种形式
  - ①消息内容泄露攻击release of message content
  - ②流量分析攻击traffic analysis
- 主动攻击active attack
  - 改写数据、或添加错误数据等：

  ①改写modification of message、
  ②重放replay
  ③假冒masquerade
  ④拒绝服务denial of service

通信过程中的攻击举例



- 防范被动攻击：
  - 难以检测，重点是防范。如通信数据加密防止泄露，通信地点、频率、模式、信息等进行处理以使其流量分析中猜测到信息尽可能少。
- 防范主动攻击：
  - 主动攻击手段多种多样，完全防范不容易，但通过检测恢复攻击造成的损坏和延迟是可行的。检测的威慑力在一方面也起到一定的防范作用。

对付典型攻击可采用的服务

攻击	安全服务
假冒	•认证
入侵	•访问控制
非授权泄露	•保密性
篡改	•完整性
拒绝承认	•抗否认服务
拒绝服务	•认证、完整性

2）安全服务service

X.800定义的安全服务：由通信开放系统的协议层提供的（可见，OSI安全体系结构是在OSI协议体系结构内容上发展来的），并能确保系统或数据传输足够安全的服务。

X.800将安全服务分为5类和14种特定服务。

安全服务		功能目标	实例
认证服务	对等实体认证		身份证、盖公章
	数据源认证		
访问控制			口令
数据机密性	有连接机密性		加密信
	无连接机密性		
	选择域机密性		
	流量机密性		
数据完整性	无/带恢复的连接完整性		信用
	选择域无/有连接的完整性		
	无连接完整性		
不可抵赖性			双方签单的快递单

依赖于这些的可用性服务

安全服务的具体实现是通过划分在网络体系结构各协议层上的具体安全机制和一些通用系统安全机制共同实现的。

3）安全机制mechanism

- 用于协议层上的各种机制

① 加密　　注意层和加密算法的选择
② 数字签名
③ 访问控制　　安全访问策略、一组控制实体权限的规则
④ 数据完整性
⑤ 认证交换 添加鉴别信息，利用密码技术，使用实体的特征等
⑥ 流量填充 填充数据流冗余位干扰流量分析
⑦ 路由选择控制
⑧ 公证　　由可信第三方提供消息的完整性、源发性、可靠性的证明

- 一些普适的安全机制：安全标签、事件检测、安全审计、安全恢复等

服务与实现机制对照表（理解掌握）

服务 \ 安全机制		加密	数字签名	访问控制策略	数据完整性	认证交换	流量填充	路由选择控制	公证
认证	实体认证	Y	Y			Y			
	数据源发认证	Y	Y						
访问控制				Y					
数据机密性	连接	Y						Y	
	无连接	Y						Y	
	选择字段	Y							
	流量	Y					Y	Y	
数据完整性	恢复、连接	Y			Y				
	无恢复、连接	Y			Y				
	字段、连接	Y			Y				
	无连接	Y	Y		Y				
	字段、无连接	Y	Y		Y				
不可抵赖性	不可否认发送过		Y		Y				Y
	不可否认接收过		Y		Y				Y
可用性					Y	Y			

回顾网络体系结构

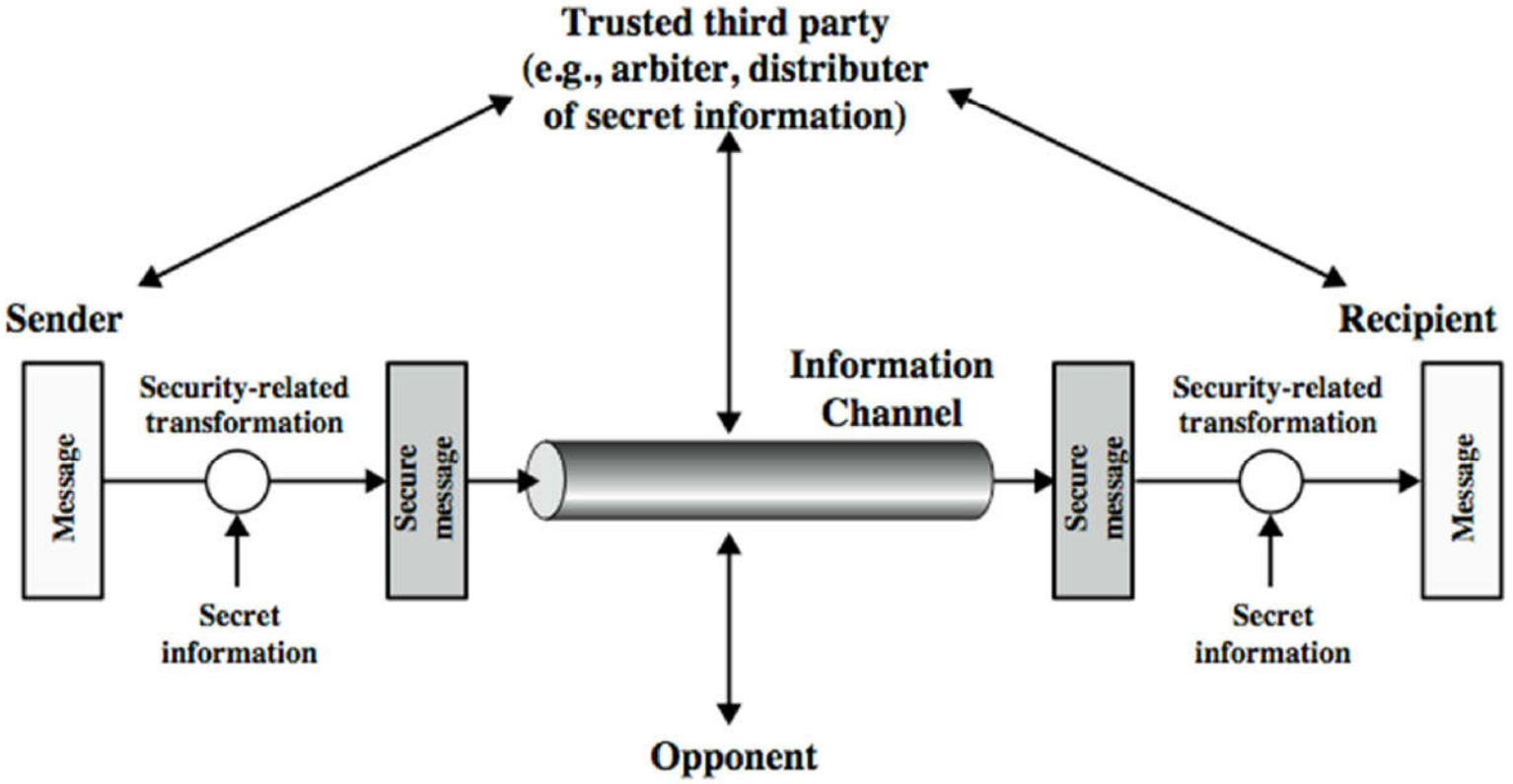
(一种抽象、逻辑上的概念)是计算机间实现相互通信的功能层，以及各层中的协议和层间接口的集合。

- 协议(Protocol)：在某层上进行通信所使用的规则、标准或约定的集合。
- 各层协议按层次顺序排列而成的协议序列称为协议栈。

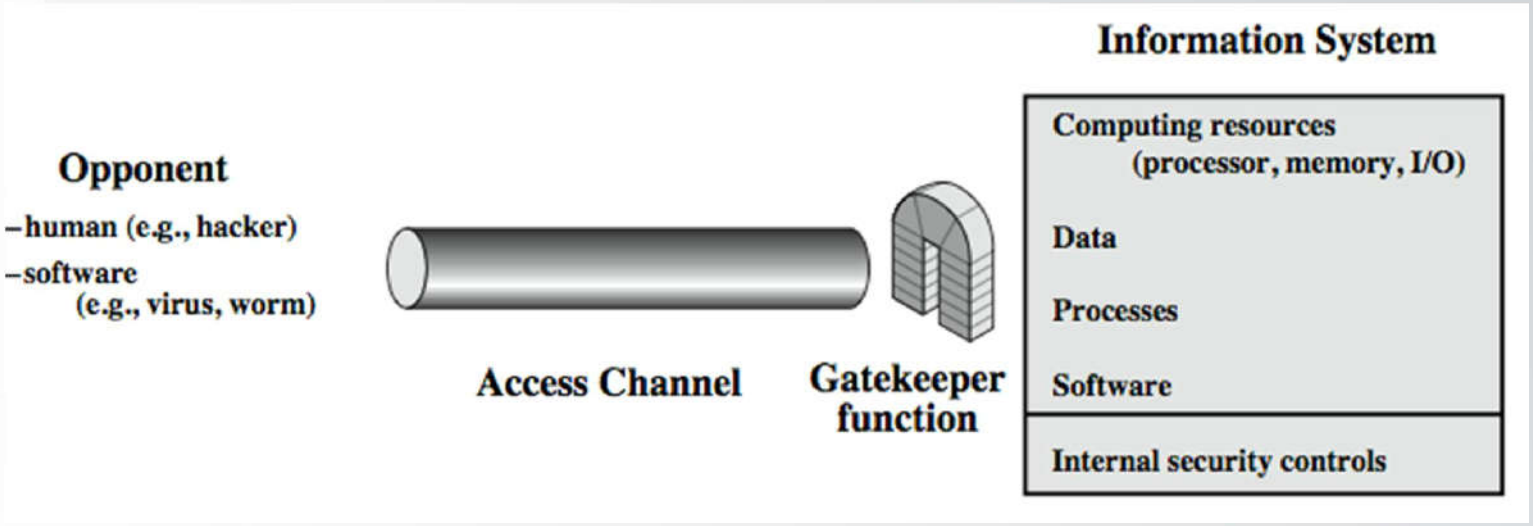
实现层与服务对照表（了解）

服务		实现层		OSI 参考模型
认证	实体认证	3、4、7	7	应用层
	数据源发认证	3、4、7	6	表示层
访问控制		3、4、7	5	会话层
数据机密性	连接	1-4、6、7	4	传输层
	无连接	2-4、6、7	3	网络层
	选择字段	7	2	数据链路层
	流量	1、6、7	1	物理层
数据完整性	恢复、连接	7		
	无恢复、连接	3、4、7		
	字段、连接	7		
	无连接	3、4、7		
	字段、无连接	3、4、7		
抗否认	不可否认发送过	7		
	不可否认接收过	7		

网络安全模型


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

网络访问安全模型


Information System
Opponent
–human (e.g., hacker)
–software
(e.g., virus, worm)
Computing resources
(processor, memory, I/O)
Data
Processes
Software
Internal security controls
Access Channel
Gatekeeper
function

信息系统安全防御策略

安全和灵活是矛盾的一体。
有时鱼与熊掌无法兼得。

- 最小特权原则
- 纵深防御
- 建立控制点
- 监测和消除薄弱连接
- 失效保护原则
- 普遍参与
- 防御多样化
- 简单化原则

思考与作业

作业：

1. 什么是OSI安全体系结构？
2. 被动和主动安全威胁有什么不同？
3. 列出并简要定义被动和主动安全攻击的分类。
4. 以填右表的形式将下述信息分别从机密性、完整性、可用性角度分配低、中、高等级。
   a) 一个网络服务器上的公众服务信息
   b) 一个管理极度敏感的法律强制调查信息
   c) 一个无关隐私的财政组织常规经营信息
   d) 一个包含敏感合同和常规管理信息的系统
5. 应对篡改和假冒攻击可采用什么安全机制进行应对？

	机密	完整	可用
高			
中			
低			

要求：每次作业一般在下周同一上课时间交