PART 1

现代密码学概论

目录 CONTENTS

目录 CONTENTS

1.1 计算机安全的概念

计算机安全

- **计算机安全：对于一个自动化的信息系统，采取保护措施确保信息系统（包括硬件、软件、固件、信息和通信）资源的完整性、可用性和保密性。**

- **计算机安全的最核心三个关键目标为：保密性Confidentiality、完整性Integrity、可用性Availability，三者成为CIA三元组。**

计算机安全的三个指标

- （1）保密性
- 数据保密性：确保隐私或是秘密信息不向非授权者泄漏，也不被非授权者使用（获取到明文）
- 隐私性：确保个人能够控制或确定与其自身相关的那些信息可以被收集的、被保存的，这些信息可以由谁来公开或是向谁公开
- （2）完整性
- 数据完整性：确保信息和程序能够以特定和授权的方式改变
- 系统完整性：确保系统以一种正常方式来执行预定的功能，免于有意或是无意的非授权操纵
- （3）可用性
- 确保系统能够工作迅速，对授权用户不能拒绝服务

➢ **三元组体现了数据、信息和计算服务的基本安全目标。**

在某些安全领域另外两个概念

- （1）真实性
- 一个实体是真实性的、可被验证的和可被信任的特性。对于传输信息来说，信息和信息的来源都是正确的。也就是说能够验证那个用户是否是他声称的那个人，以及系统的每个输入是否均来自可信任的信源。
- （2）可追溯性
- 要求实体的行为可以位移的追溯到该实体，这一属性支持不可否认性、阻止、故障隔离、入侵检测和预防、时候恢复、以及法律诉讼。因为无法得到真正安全的系统，我们必须能够追查到对安全泄漏负有责任的一方。系统必须能保留他们的活动记录，以及允许时候审计分析，进而跟踪安全事件或解决争执。

1.2 OSI安全架构

OSI安全架构

- **安全架构**
  - 为了有效评价一个机构的安全需求；对各种安全产品和政策进行评估和选择
  - 以某种系统的方法来定义对安全的要求并刻画满足这些要求的措施
- ITU-T推荐X.800方案，即**OSI安全架构**
  - OSI：Open Systems Interconnection 开放式系统互联
  - 定义安全需求和提供安全需求的系统化方法。它为许多概念提供了一些有用的描述。

OSI安全架构

- OSI安全架构关注**安全攻击、安全服务和安全机制。**
  - **安全攻击**：
    - 任何危机信息系统安全的活动
  - **安全服务**：
    - 加强数据处理系统和信息传输的安全性的一种处理过程或通信服务。其目的是利用一种或多种安全机制进行反攻击。
  - **安全机制**：
    - 用来检测、阻止攻击，或者从攻击状态恢复到正常状态的过程，或实现该过程的设备

1.3 安全攻击

- **安全攻击分为被动攻击和主动攻击。**
  - 被动攻击试图获取或利用系统的信息，但不影响系统资源。主动攻击则试图改变系统资源或影响系统运行。

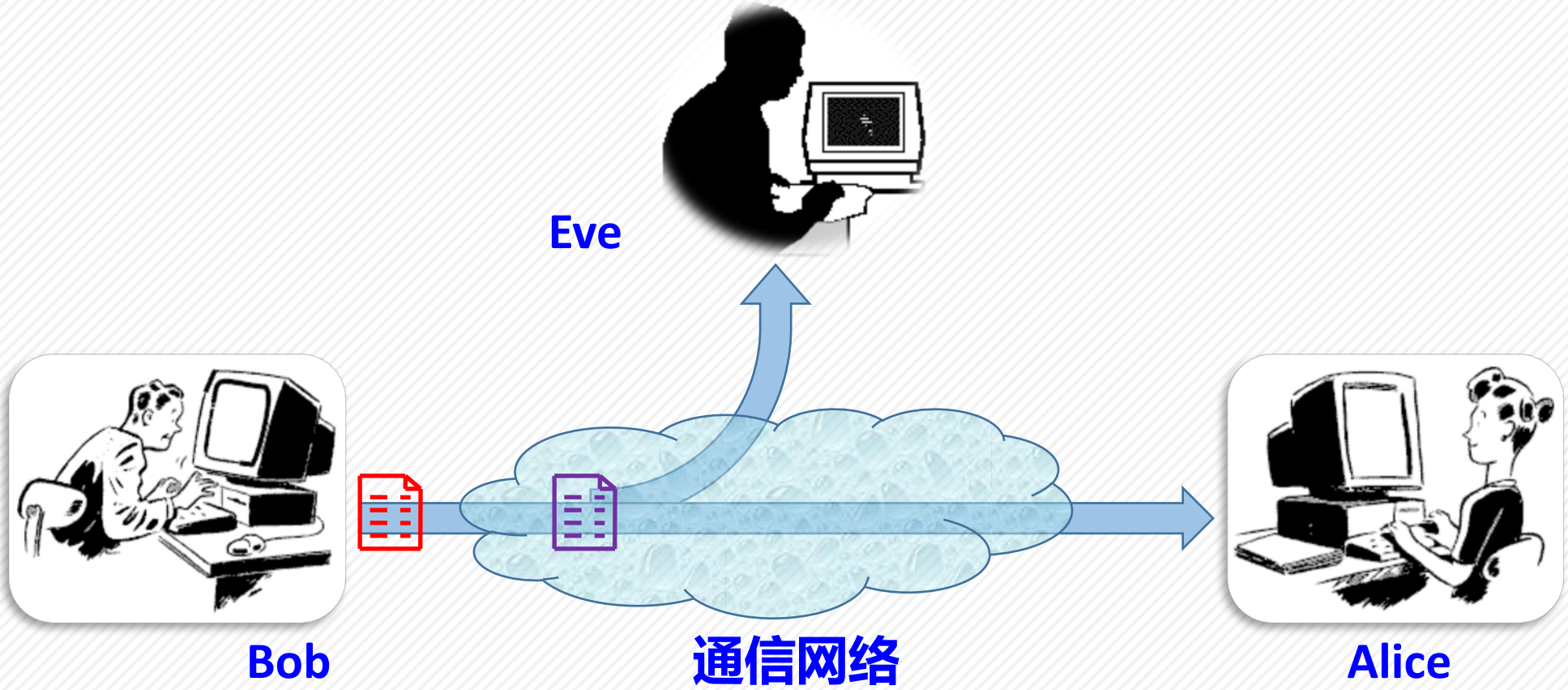
- **被动攻击的特性是对传输进行窃听和检测。攻击者的目标是获取传输的信息。**
  - 信息内容的泄漏和流量分析都属于被动攻击。

- 流量分析：当我们对信息进行加密，那么即使窃听到数据，也无法获取明文，但是仍然可以对这些数据进行分析，获得传输消息的频率和长度，以及通信主机的身份和位置，从而判断通信的某些心智。

- 被动攻击不涉及对数据的修改，因此很难察觉。通常采用加密的方式来阻止被动攻击。对于被动攻击重点是预防而非检测（很难检测出来）。

被动攻击——窃听、流量分析

- **窃听消息，分析消息模式**



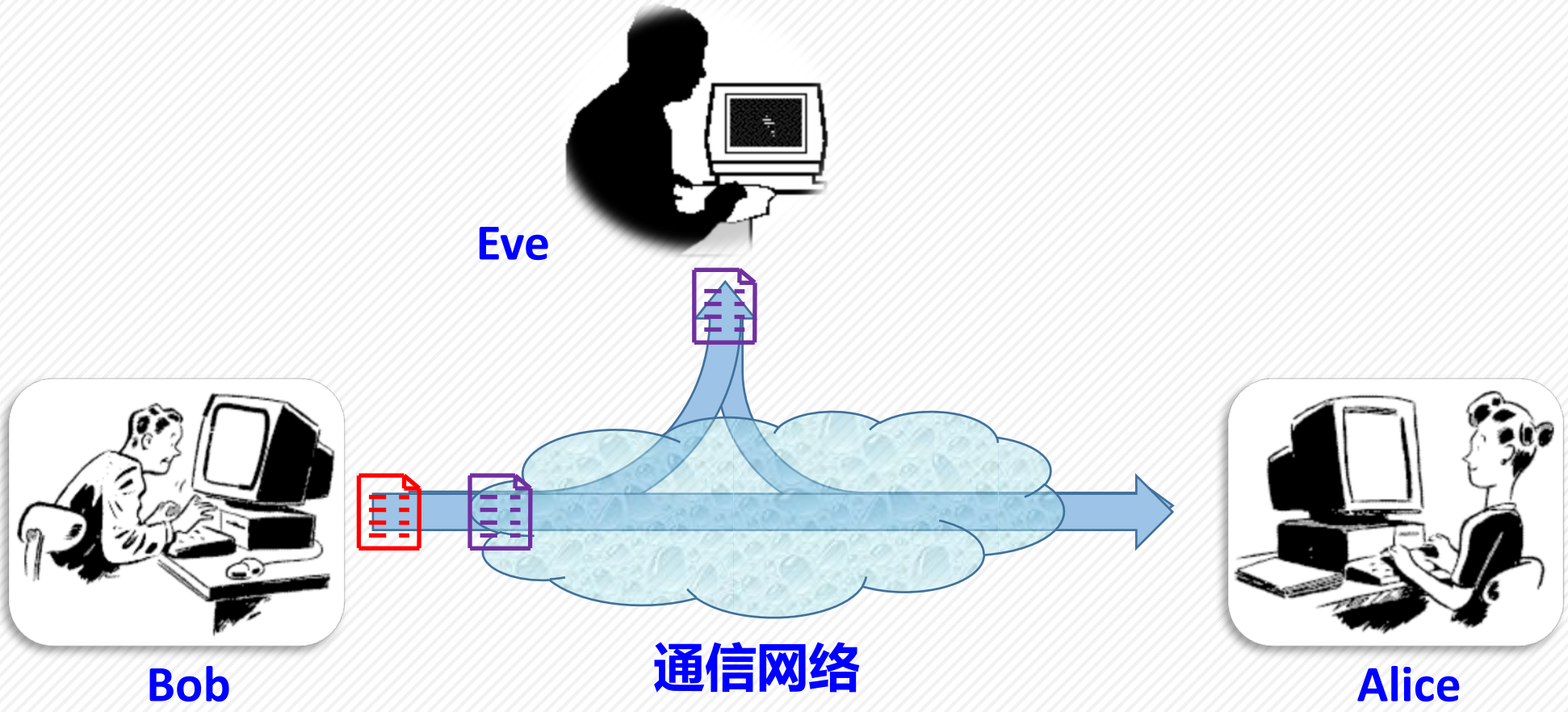
- 主动攻击包括对数据流的修改或伪造数据流分为：**伪装、重放、消息修改和拒绝服务**。
- **伪装**：指某实体假装为其他实体。伪装攻击还包含其他形式的主动攻击。例如，截获认证信息，在认证信息完成合法验证以后进行重放。无权限的实体就可以通过冒充有权限的实体获得额外的权限。
- **重放**：指攻击者未经授权将截获的信息再次重放。
- **消息修改**：值未经授权地修改合法消息的一部分，或延时消息的传输（没修改内容），或改变消息的顺序。
- **拒绝服务**：组织或禁止对通信设备的正常使用或是管理。针对具体的目标。拒绝服务的另一种形式是破坏整个网络，是网络是小，或是网络过载以降低其性能。

主动攻击——伪装

- 伪装Bob，欺骗Alice

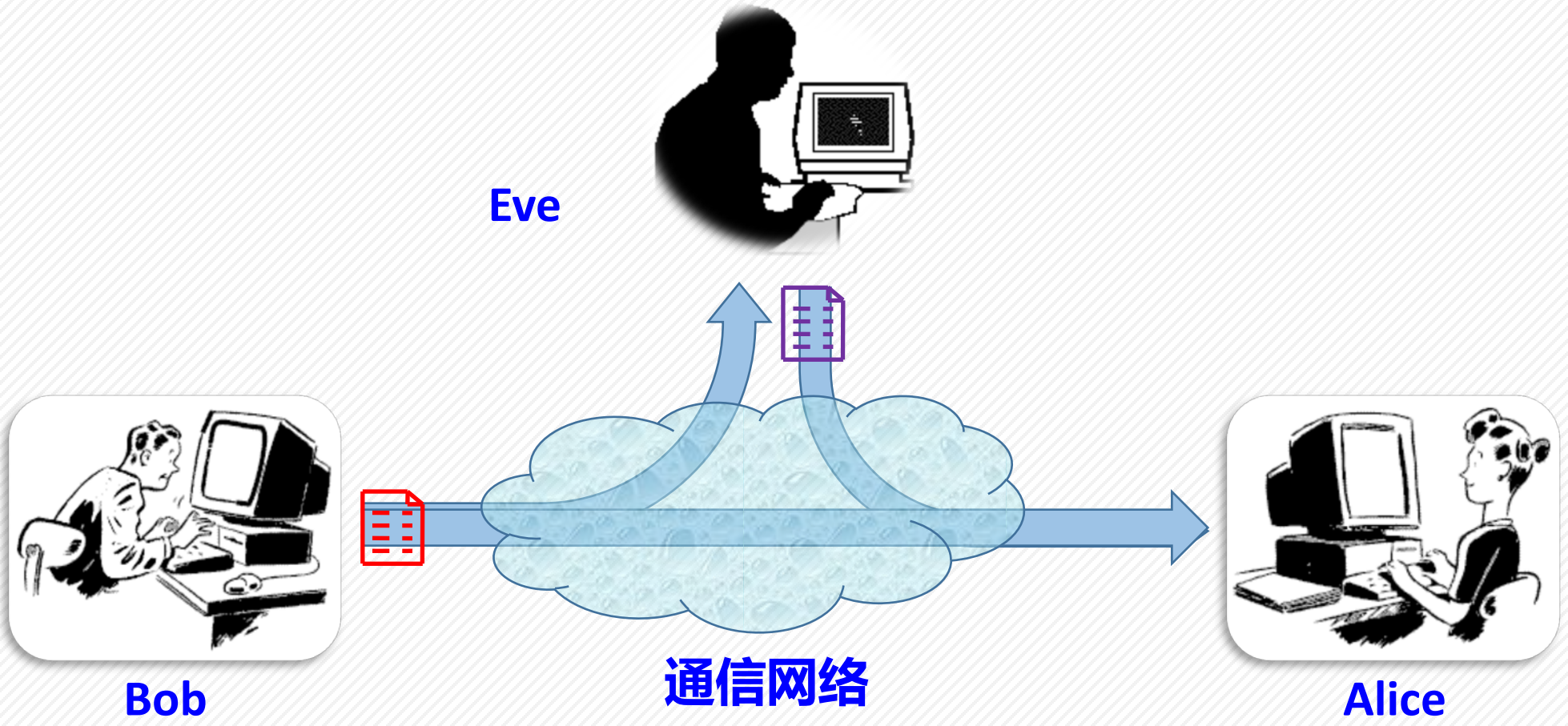
主动攻击——重放

- **窃听并记录消息，随后伪装成Bob重发给Alice**



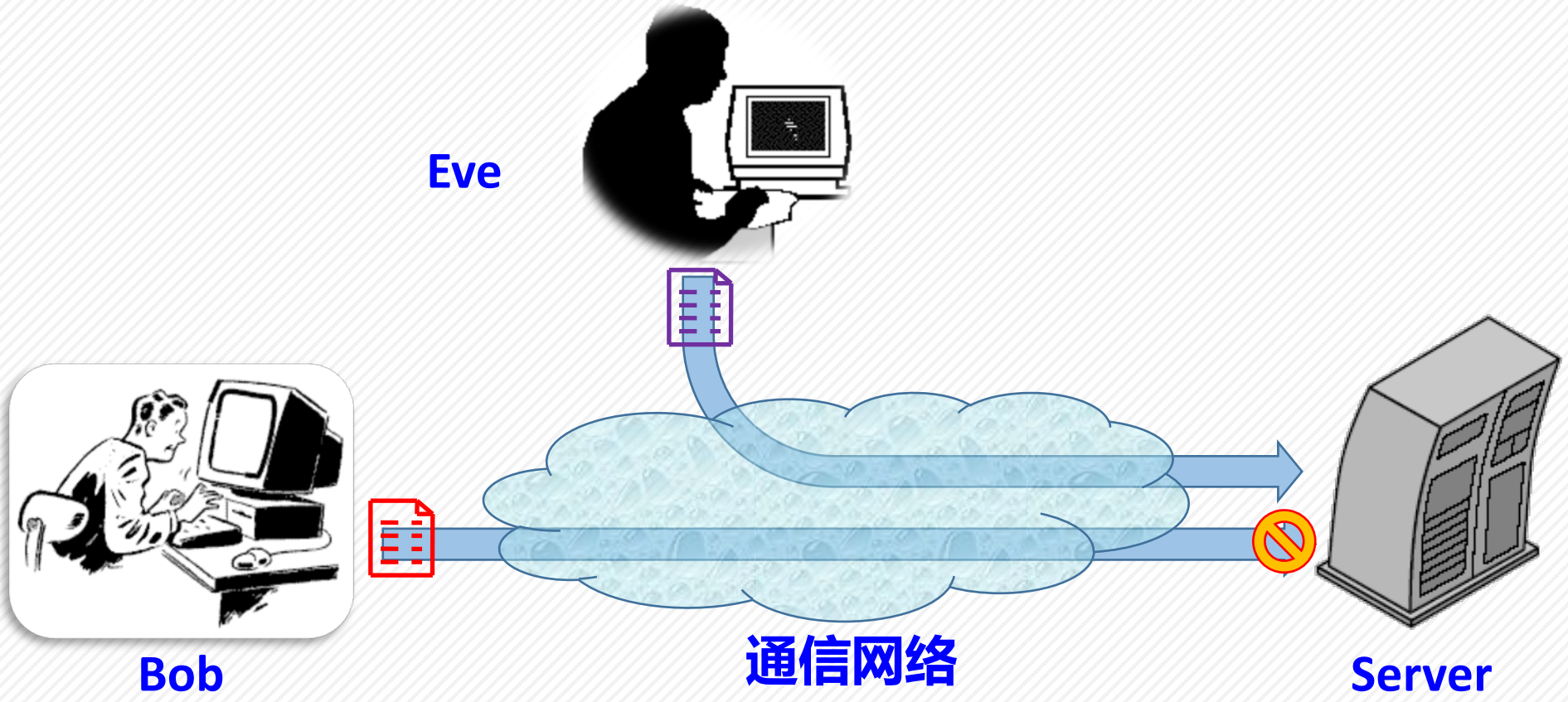
主动攻击——消息修改

- **截获Bob发出的消息，修改后再转发给Alice**



主动攻击——拒绝服务

- **阻塞、破坏服务器，使之无法相应客户请求**



1.4 安全服务

安全服务

- 增强数据处理系统和信息传输的安全性
- 记录安全攻击事件
- 使用一种或多种安全机制提供服务
- 复制与物理文档相关联的功能
  - 签名，记录日期
  - 防止泄露、篡改、破坏
  - 被证实或成为证据（通过公证，保证文档内容的有效性）
  - 被记录或许可（查看信息需要被记录，得到许可）

安全服务定义

- **X.800：**
  - **开放通信系统中协议层提供的服务，适当地保护系统和数据传输的安全。**
- **RFC 2828：**
  - **系统提供的处理或通信服务，为系统资源提供特别的保护。**

安全服务（X.800）

- **认证**
  - 确保实体身份，并保护不受第三方干扰
- **访问控制**
  - 防止资源的非授权使用
- **数据保密性**
  - 防止数据的非授权泄露
- **数据完整性**
  - 确保收到的数据与通信实体发送的数据相同
- **不可否认性**
  - 通信不可否认
- **有效性服务**
  - 确保系统或系统资源可以被授权实体按照规范访问、使用

1.5 安全机制

安全机制

- 被设计用来检测、防范安全攻击，或从安全攻击中恢复的特征
- 单一的机制不能满足所有需要的服务
- 许多安全机制都**以密码技术为基础**

安全机制（X.800）

- **特定安全机制**：
  - 在特定的协议层实现
  - 加密、数字签名、访问控制、数据完整性、交换认证、流量填充、路由控制、公证
- **普遍的安全机制**：
  - 不局限于任何安全服务或协议层
  - 可信功能、安全标签、事件检测、安全审计索引、安全恢复

1.6 基本安全设计准则

安全设计准则

- 机制的经济性：指嵌入在硬件和软件中的安全机制赢设计的尽量简单、短小。设计越复杂，就弱点就难以被发现，漏洞也可能越多。（也是最难遵循的准则）
- 故障安全默认：指访问决策基于访问的条件。在安全机制的设计或实现中出现错误时，应拒绝访问许可。以便检测到错误。
- 完整的监察：必须检查访问机制中的每一个访问，不能依赖从缓存中检索得到的访问决策。也就是说应该实时的读取全权限
- 开放的设计：设计应该开放
- 权限分离：需要多个权限属性来访问一个受限资源时的准则。适用于任何需要将程序划分为多个部分，每个部分被授予不同的权限，减轻计算机收到攻击时的潜在损害

安全设计准则

海南大学 Hainan university

- 最小权限：每个进程和用户应该执行该任务所需要的最小权限集来进行操作。
- 最小共同机制：把不同用户共享的功能设计的最小，以便提供共同的安全性。
- 心理接受度：满足授权访问的用户需求的同时，不应该过度的干预用户的工作。
- 隔离
- 封装：基于面型对象的特定形式的隔离。
- 模块化：指将安全功能作为独立的模块开发，机制设计和实现的模块化。
- 分层：使用多个叠加的保护方法来保护信息系统的人员、技术和操作。任何一层失败，保护依然有效。
- 最小意外：程序或用户结构对意外事故的处理响应最小化。（也就是说，对用户透明的感觉）

1.7 攻击面与攻击树

攻击面与攻击树

- **攻击面是由系统中一系列可访问且可利用的漏洞组成。主要分为：**
  - **网络攻击面：指的是企业网络、广域网或是互联网。包含协议的漏洞及拒绝服务供给、终端通信链路等。**
  - **软件攻击面：设计应用程序、工具包或操作系统漏洞。**
  - **人类攻击面：主要是系统人员或是外部人员造成的漏洞。**

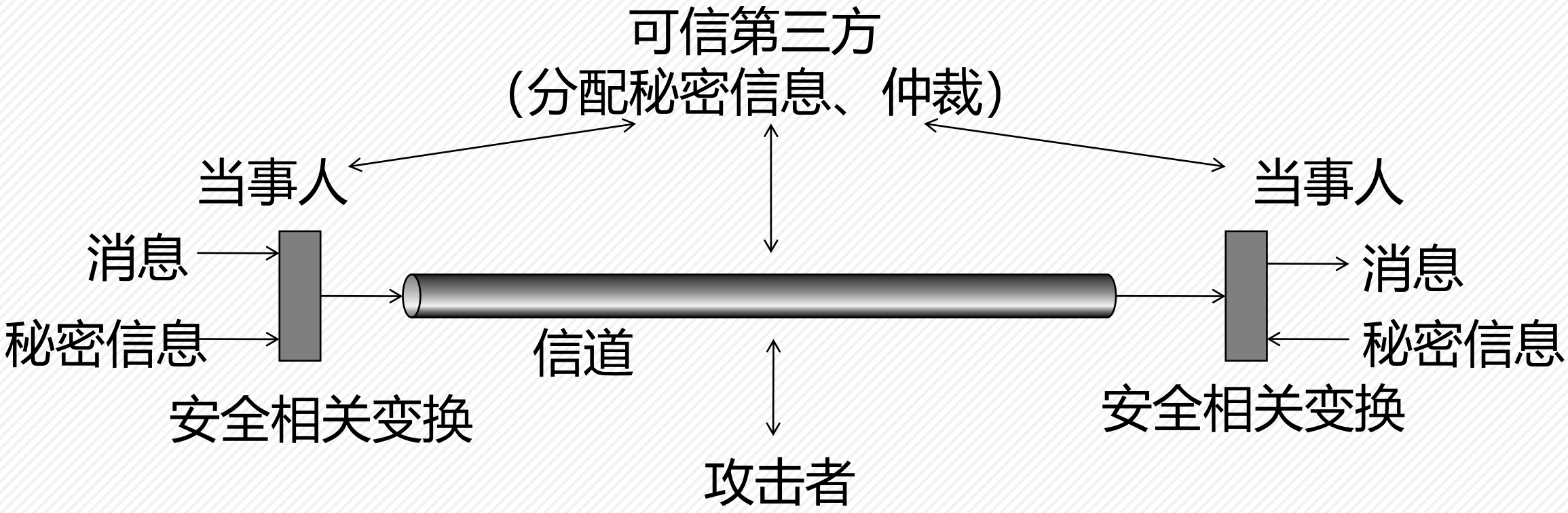
攻击面与攻击树

- **攻击树是采分支化、层次化表示利用安全漏洞的可能技术集合的一种数据结构。**
- **根节点：攻击目的。第二层是攻击的目标，再往下则是攻击的方式等。**
- **深度越深则越具体。因此叶节点是具体的攻击方式。**

1.8 网络安全模型

网络安全模型

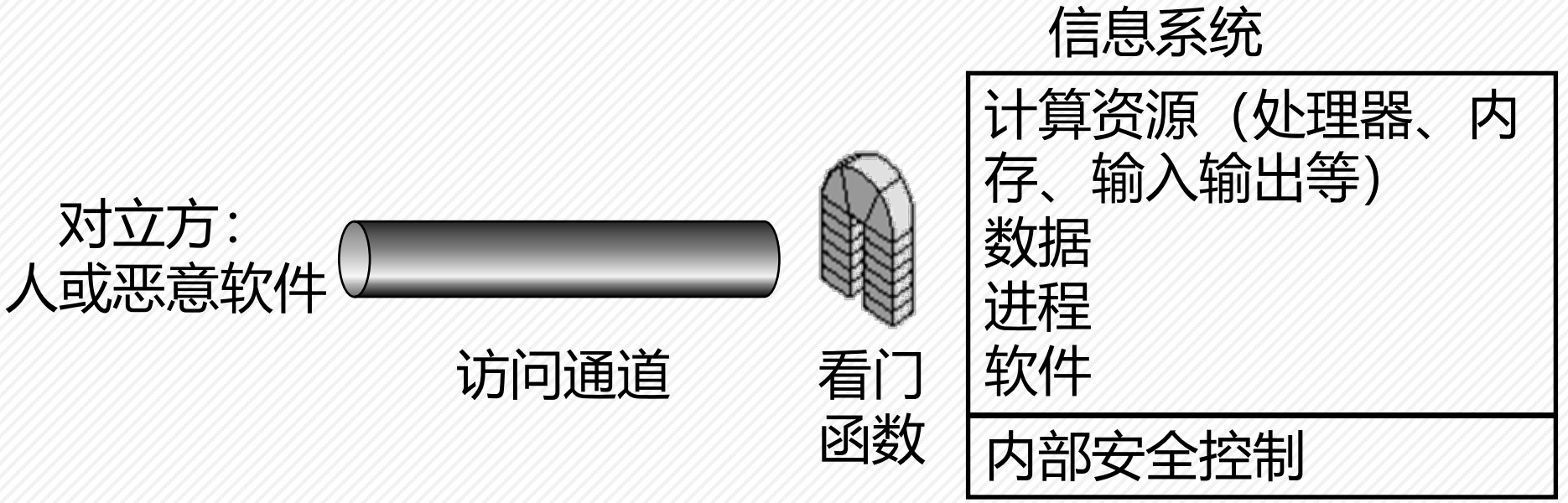
- **所有提供安全的技术都具备：**
  - **对待发送信息进行安全相关变换**
  - **两个当事人共享一些秘密信息，而对手对此一无所知**



网络安全模型

- 使用网络安全模型需要：
  - 设计适当的安全相关**变换算法**
  - 产生算法所需的**秘密信息**（密钥）
  - 设计**分发、共享**秘密信息的方案
  - 指定**协议**，该协议利用安全变换和秘密信息实现安全服务

网络安全模型



- **使用网络访问安全模型需要：**
  - **选择合适的看门函数识别用户**
  - **实现安全控制，确保仅授权用户可以使用指定信息或资源**
- **可信计算机系统有助于实现此模型**

信息系统的安全性

- **保密性**：信息不泄露给未经授权的人
- **数据完整性**：信息在传输过程中不被篡改
- **实体认证**：确认实体所声称的身份
- **消息认证**：确认消息源
- **可用性**：授权者能使用信息和信息系统
- **访问控制**：限制用户所能访问的资源，方式是授权
- **可控性**：对信息和信息系统实施安全监控管理
- **收据与确认**：告知已经收到信息或服务
- **不可否认性**：实体不能否认自己的行为


海南大学
Hainan university