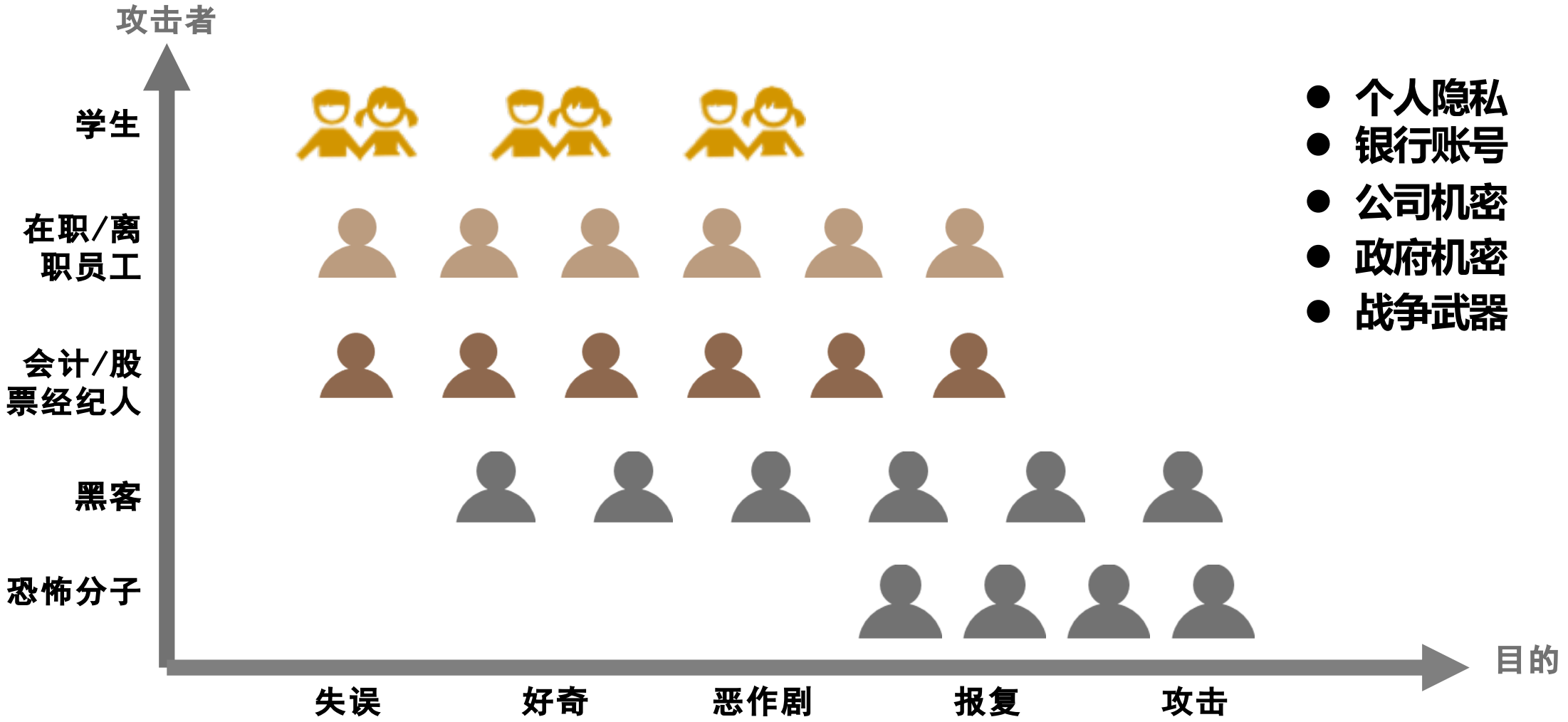
网络信息安全概述

网络应用面临的安全问题



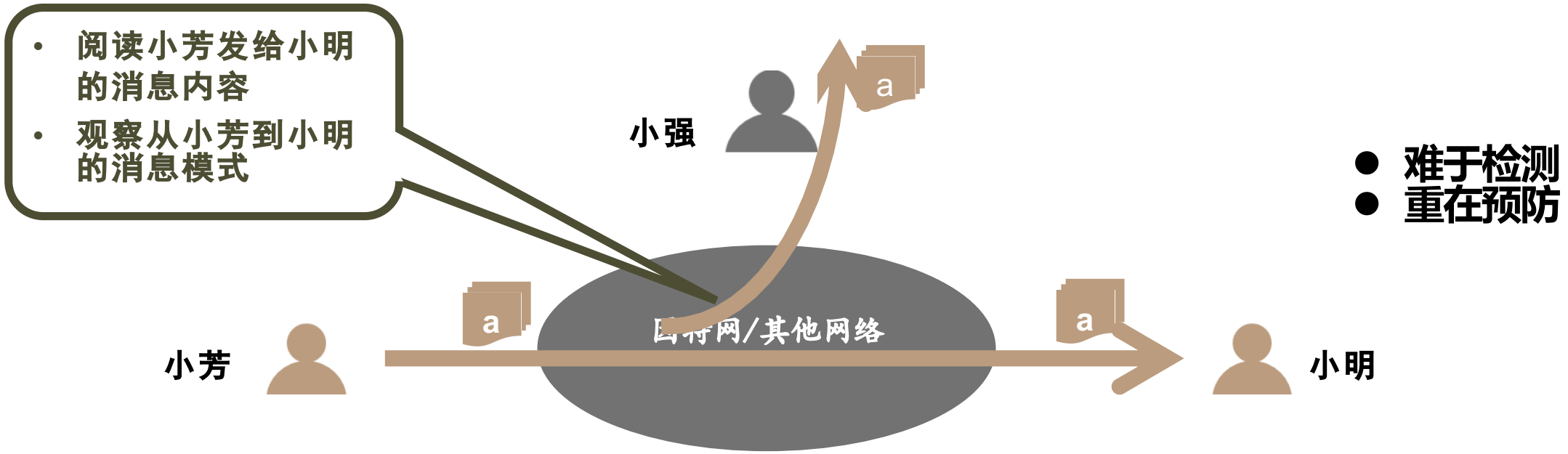
被动攻击

信息泄露：对传输中的明文进行窃听。

- wireshark
- Tcpdump
- SnifferPro
- windump/ snort/ NetXRay/

流量分析：通过分析密文获得消息模式等信息，来判断通信的性质等。

- **通信主机身份**
- **通信位置**
- **消息频度、消息长度等**



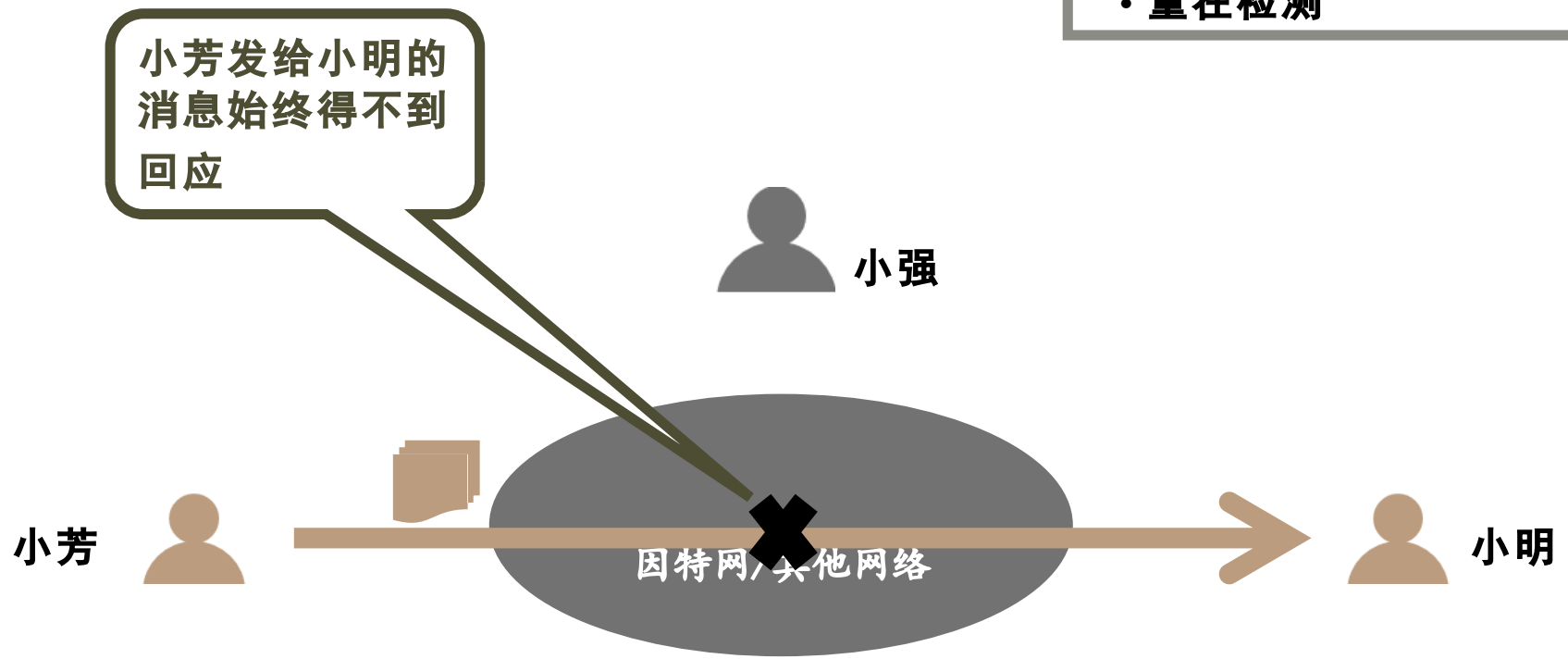
- **难于检测**
- **重在预防**

主动攻击一

网络通信中断：攻击者有意中断他人在网络上的通信。

攻击特点

- 网络弱点多
- 难于预防
- 重在检测

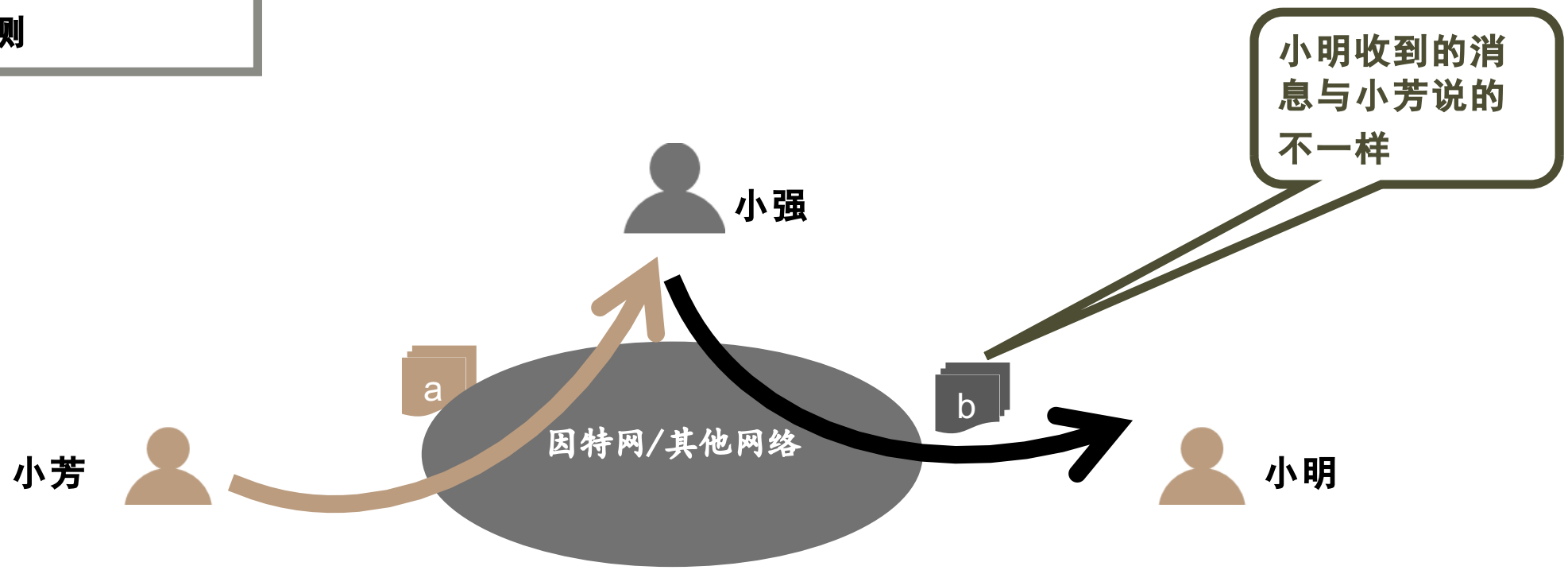


主动攻击之二

攻击特点

- 网络弱点多
- 难于预防
- 重在检测

信息篡改：攻击者故意篡改网络上传送的报文。

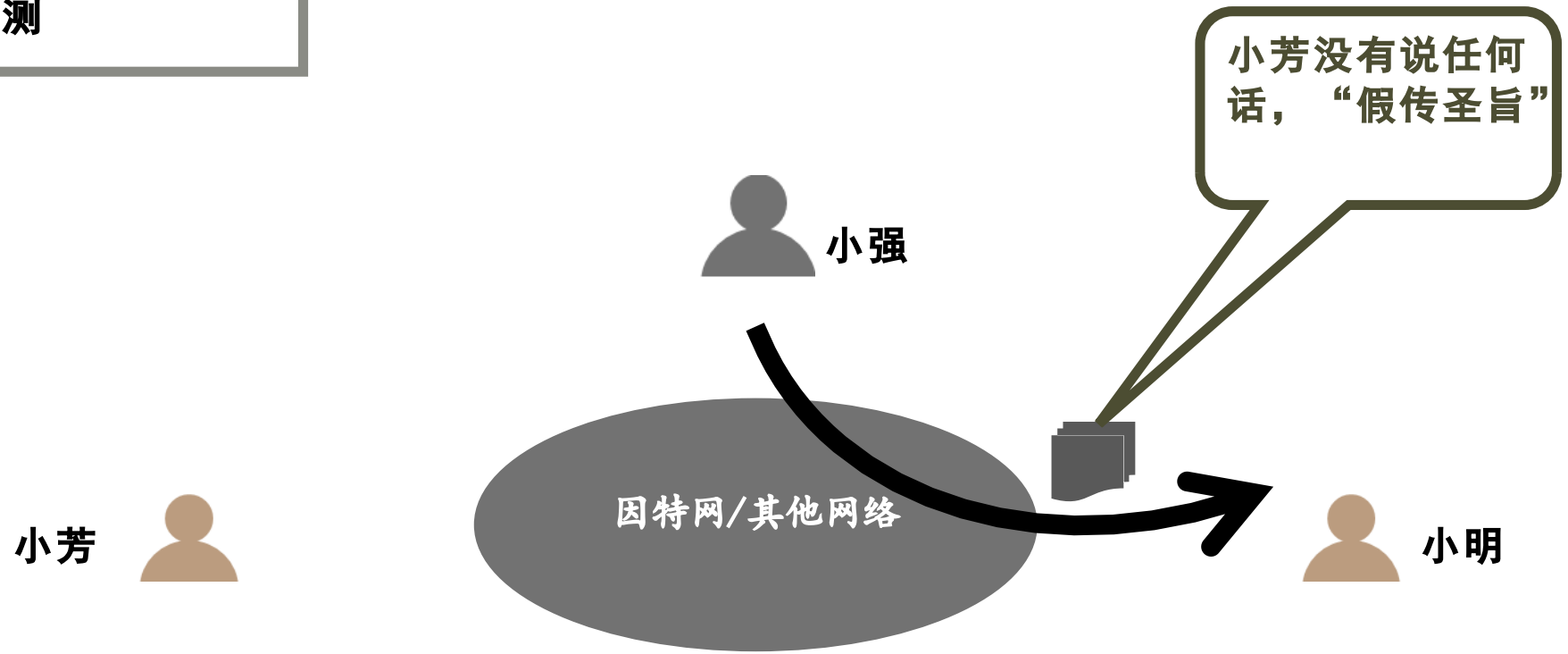


主动攻击之三

攻击特点

- 网络弱点多
- 难于预防
- 重在检测

伪造：攻击者伪造信息发送给接收者

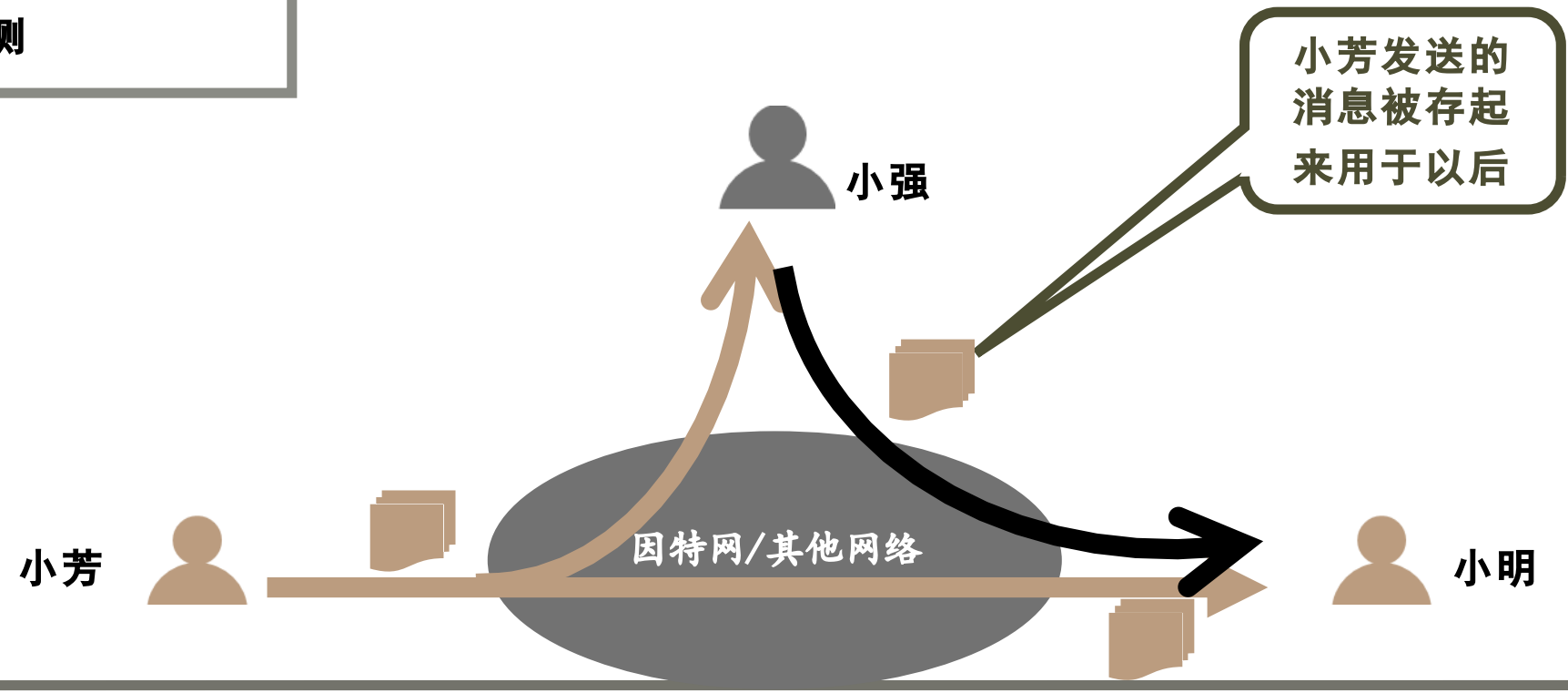


主动攻击之四

攻击特点

- 网络弱点多
- 难于预防
- 重在检测

重放：攻击者把截获的消息存起来，以后再发送给接收者



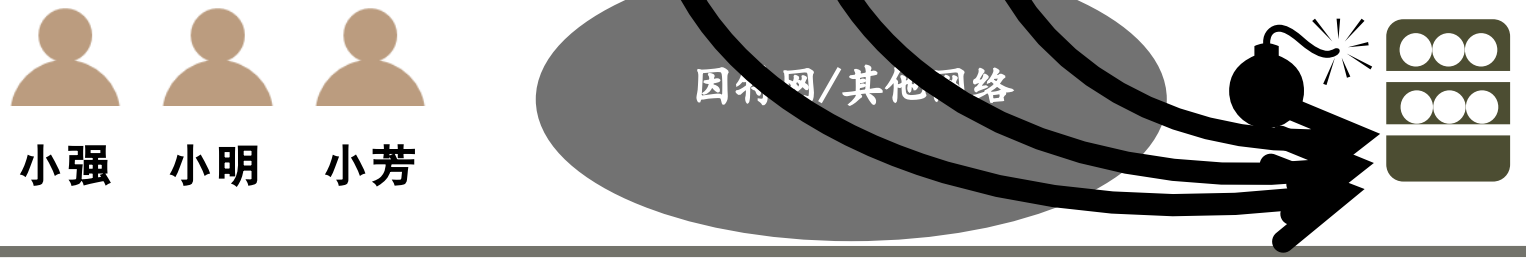
主动攻击之五

拒绝服务攻击（DoS）：计算机或网络无法提供正常的服务。

攻击特点

- 网络弱点多
- 难于预防
- 重在检测

- 攻击者删除某个连接上的所有报文，或者将双方或单方的所有报文加大延迟。
- 攻击者给服务器发送大量的服务请求（例如，SYN泛洪），导致服务性能下降甚至瘫痪。
- …

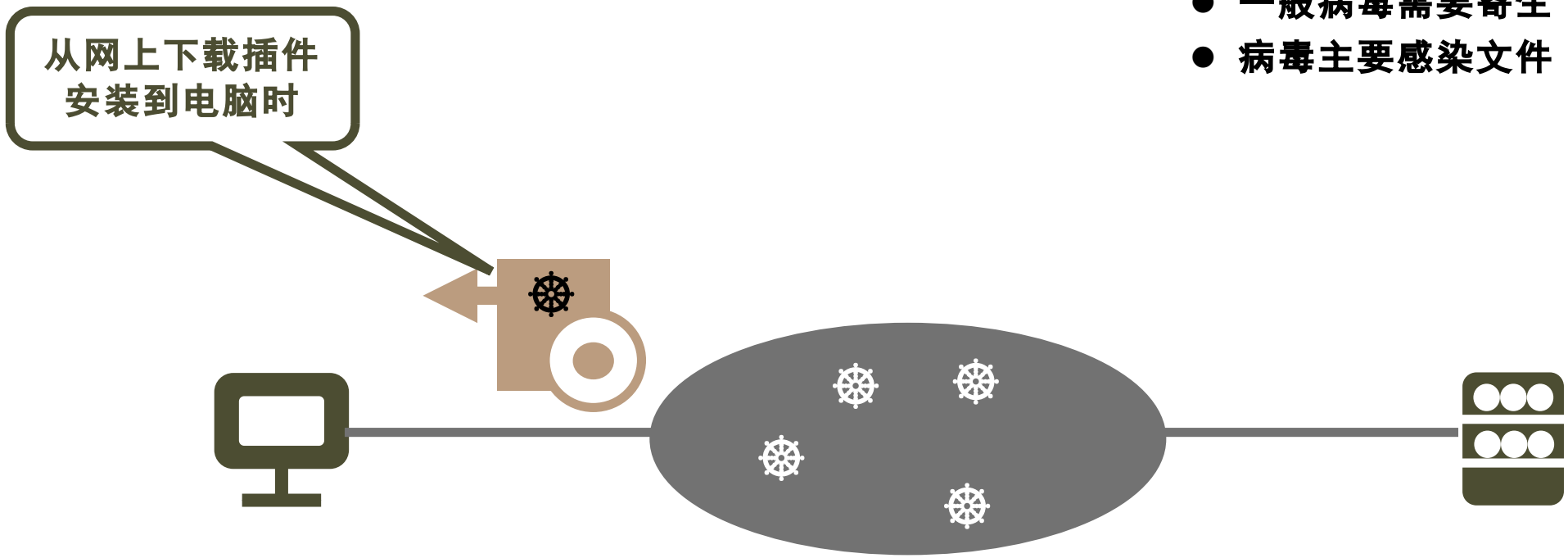


恶意程序——病毒

恶意程序：通常是指带有恶意攻击意图的一段程序。

计算机病毒：通过修改其他程序把自身复制进去的程序

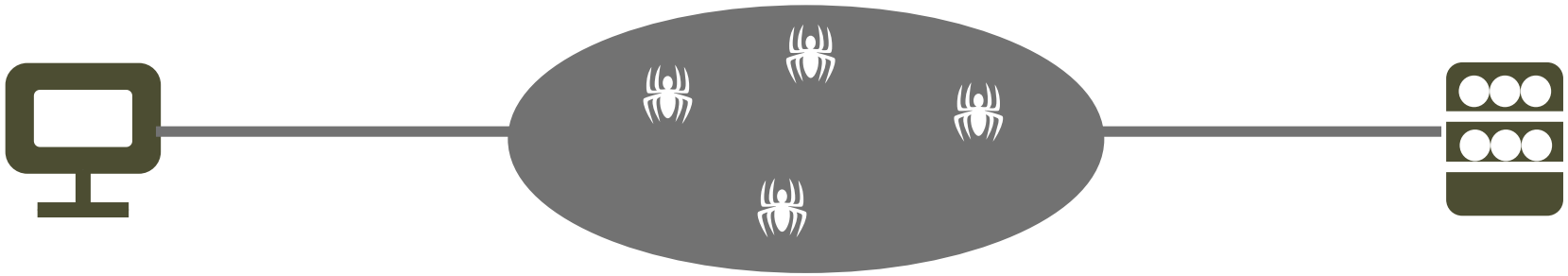
- **一般病毒需要寄生**
- **病毒主要感染文件**



恶意程序——蠕虫

计算机蠕虫：通过网络将自身从一个节点发送到另一个节点并启动运行的程序。

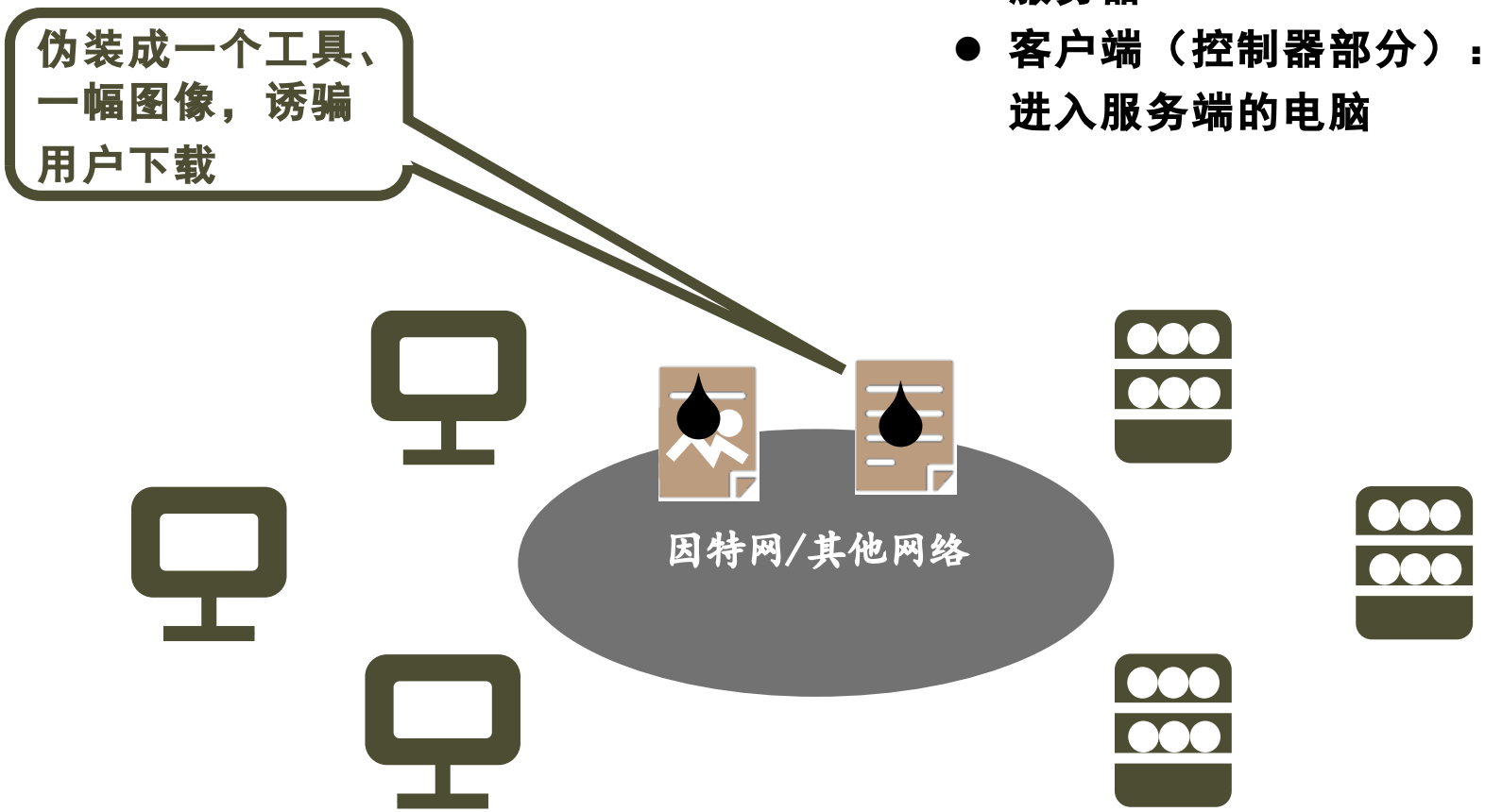
- 病毒传染主要针对计算机内文件系统
- 蠕虫传染目标是互联网内的所有计算机



恶意程序——特洛伊木马

特洛伊木马：实际功能超出所声称功能的程序。

- 服务端（服务器部分）：植入对方电脑的服务器
- 客户端（控制器部分）：黑客利用客户端进入服务端的电脑



恶意程序——逻辑炸弹

逻辑炸弹：当运行环境满足特定条件时执行特殊功能的程序。

- 逻辑炸弹强调破坏作用本身
- 实施破坏的程序不具有传染性
- 在运行环境满足特定条件时被触发