第1章 信息安全概述

翟健宏

综合楼709,86402573,zjh_hit@126.com

1.1 信息安全的理解

1.1.1 信息与信息安全

- 信息：事物运动的状态与方式
  - ISO给出的解释：“信息是通过施加于数据上的某些约定而赋予这些数据的特定含义”。
  - 通常我们可以把消息、信号、数据、情报和知识等都看作信息。信息本身是无形的，借助信息介质以多种形式存在或传播。
- 信息安全
  - ISO给出的定义：“在技术上和管理上为数据处理系统建立的安全保护，保护信息系统的硬件、软件及相关数据不因偶然或者恶意的原因遭到破坏、更改及泄露”。
  - 信息安全的目的：“确保以电磁信号为主要形式的、在计算机网络化系统中进行获取、处理、存储、传输和应用的信息内容在各个物理及逻辑区域中的安全存在，并不发生任何侵害行为”。

1.1 信息安全的理解

1.1.2 信息安全的发展阶段

- 信息安全发展：
  - 通信安全→ 信息安全→信息保障
- 通信安全（COMSEC）
  - 20世纪90年代以前，这一阶段的信息安全可以简单称为通信安全，主要目的是保障传递的信息安全，防止信源、信宿以外的对象查看信息。

1.1 信息安全的理解

1.1.2 信息安全的发展阶段

- 信息安全（INFOSEC）
  - 20世纪90年代以后，主要保证信息的机密性、完整性、可用性、可控性、不可否认性。
    - 机密性（Confidentiality）指信息只能为授权者使用而不泄漏给未经授权者的特性。
    - 完整性（Integrity）指保证信息在存储和传输过程中未经授权不能被改变的特性。
    - 可用性（Availability）指保证信息和信息系统随时为授权者提供服务的有效特性。
    - 可控性（Controllability）指授权实体可以控制信息系统和信息使用的特性。
    - 不可否认性（Non–Repudiation）指任何实体均无法否认其实施过的信息行为的特性，也称为抗抵赖性。

1.1 信息安全的理解

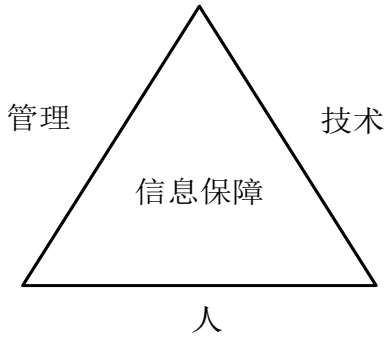
1.1.2 信息安全的发展阶段

- 信息保障(IA，Information Assurance)
  - 1996年美国人提出了信息保障：
    - 保护（Protect）、检测（Detect）、反应（React）、恢复（Restore）四个方面。
  - 我国也对信息保障给出了相关解释：
    - “信息保障是对信息和信息系统的安全属性及功能、效率进行保障的动态行为过程。它运用源于人、管理、技术等因素所形成的预警能力、保护能力、检测能力、反应能力、恢复能力和反击能力，在信息和系统生命周期全过程的各个状态下，保证信息内容、计算环境、边界与连接、网络基础设施的真实性、可用性、完整性、保密性、可控性、不可否认性等安全属性，从而保障应用服务的效率和效益，促进信息化的可持续健康发展。”。

1.1 信息安全的理解

1.1.2 信息安全的发展阶段

- 信息保障三大要素。
  - 人是信息保障的基础
  - 技术是信息保障的核心
  - 管理是信息保障的关键



- 信息安全不是一个孤立静止的概念，具有系统性、相对性和动态性。

1.2 信息安全威胁

1.2.1 信息安全威胁的基本类型

- **信息泄露**:信息被有意或无意泄露给某个非授权的实体。
- **信息伪造**:某个未授权的实体冒充其他实体发布信息，或者从事其他网络行为。
- **完整性破坏**:非法手段窃取信息的控制权，未经授权对信息进行修改、插入、删除等操作，使信息内容发生不应有的变化。
- **业务否决或拒绝服务**:攻击者通过对信息系统进行过量的、非法的访问操作使信息系统超载或崩溃，从而无法正常进行业务或提供服务。
- **未经授权访问**:某个未经授权的实体非法访问信息资源，或者授权实体超越其权限访问信息资源。

1.2 信息安全威胁

1.2.2 信息安全威胁的主要表现形式

- 攻击原始资料
  - 人员泄露,废弃的介质,窃取
- 破坏基础设施
  - 破坏电力系统,破坏通讯网络,破坏信息系统场所
- 攻击信息系统
  - 物理侵入,特洛伊木马,恶意访问,服务干扰,旁路控制,计算机病毒,
- 攻击信息传输
  - 窃听,业务流分析,重放,
- 恶意伪造
  - 业务欺骗,假冒,抵赖
- 自身失误
- 内部攻击

1.3 互联网的安全性

1.3.1 互联网的发展现状

- 1983年，ARPA和美国国防部通信局研制TCP/IP协议，该协议被做为其BSD UNIX的一部分。
- 1986年，NSF 利用Internet Protocol，连接5个科研教育服务机构，建立了NSFnet广域网。
- 1987年开始，中国四大网络CSTnet、CERNET、Chinanet、GBnet与Internet直连。
- 2007年底，我国互联网用户1.62亿，其中宽带上网用户达到1.22亿，中文网站89.8万个，IPv4地址总数9800多万个，国际出口带宽总量为368927 Mbps。

1.3 互联网的安全性

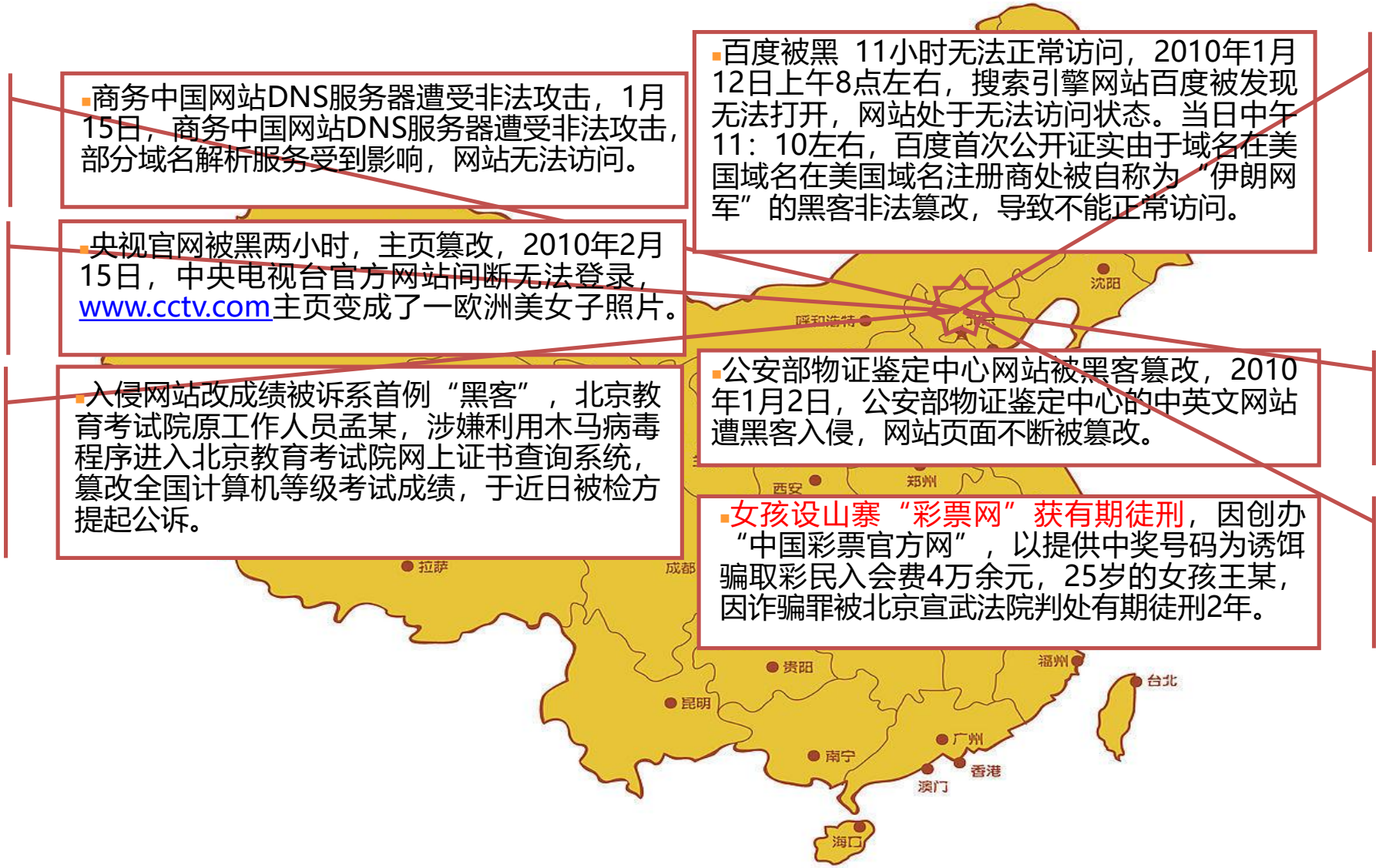
1.3.2 互联网的安全现状

- 2000年开始，病毒制造产业化操作，黑色产业链每年的整体利润预计高达数亿元。
- 窃取的个人资料
  - QQ密码、网游密码、银行账号、信用卡帐号,任何可以直接或间接转换成金钱的东西，都成为不法分子窃取的对象。
- CERT统计，
  - 在1988年安全事件6件，2001年5万件，2003年为13万7千多件，在2003年以后发生呈线性增长。
  - 据CCERT统计，2006年26476件，是2005年9112件的三倍。

安全事件

- 1988年著名的“Internet蠕虫事件”使得6000余台计算机的运行受到影响。
- 1998年2月份，黑客利用Solar Sunrise弱点入侵 美国防部网络，攻击相关系统超过500台计算机，而　　攻击者只是采用了中等复杂工具。
- 2000年春季黑客分布式拒绝服务攻击（DDOS）大型网站，导致大型ISP服务机构Yahoo网络服务瘫痪。
- 2001年5月的中美黑客大战。
- 2001年8月，“红色代码”蠕虫利用微软web服务器IIS 4.0或5.0中index服务的安全缺陷，攻破目的机器，并通过自动扫描感染方式传播蠕虫，已在互联网上大规模泛滥。
- 2003年，“冲击波”蠕虫的破坏力就更大，安全专家Bruce Schneier撰文分析认为，美国2003年8月份大停电与“冲击波蠕虫”相关。

国内信息安全事件（10年1-2月）



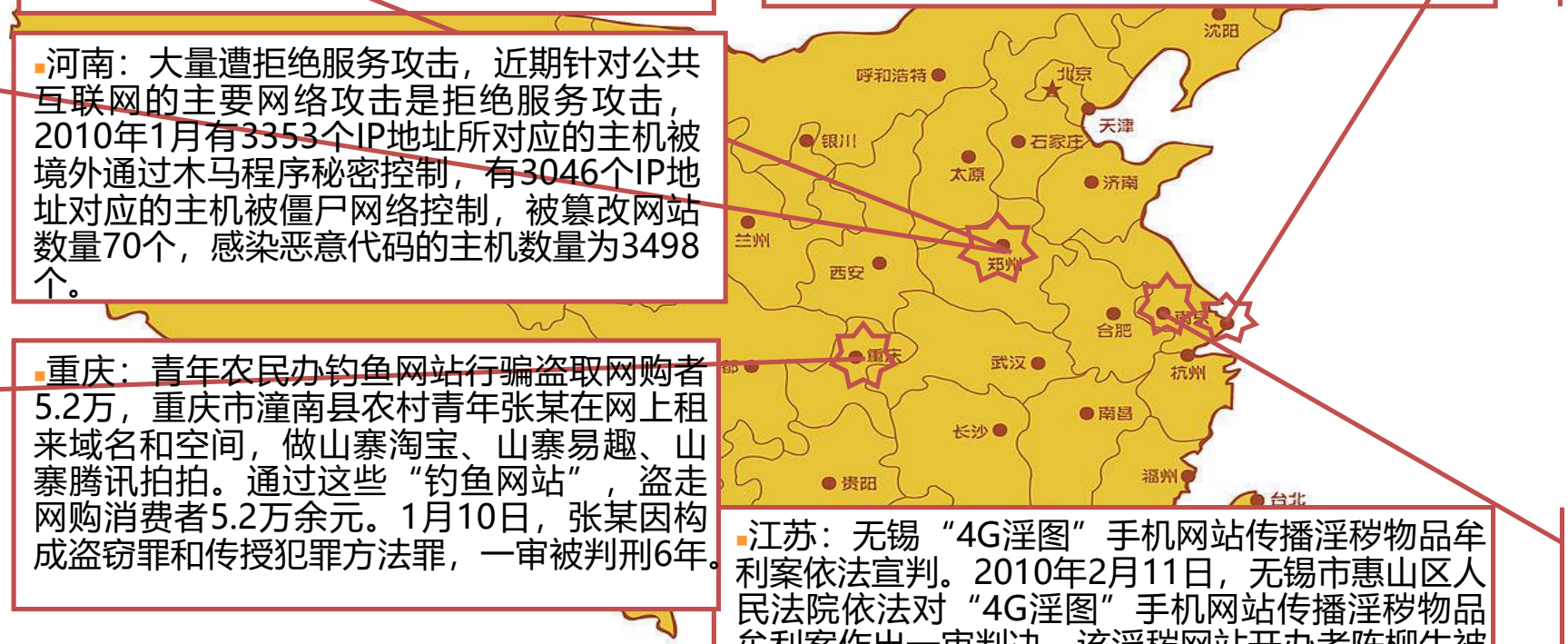
- 商务中国网站DNS服务器遭受非法攻击，1月15日，商务中国网站DNS服务器遭受非法攻击，部分域名解析服务受到影响，网站无法访问。
- 百度被黑 11小时无法正常访问，2010年1月12日上午8点左右，搜索引擎网站百度被发现无法打开，网站处于无法访问状态。当日中午11：10左右，百度首次公开证实由于域名在美国域名在美国域名注册商处被自称为“伊朗网军”的黑客非法篡改，导致不能正常访问。
- 央视官网被黑两小时，主页篡改，2010年2月15日，中央电视台官方网站间断无法登录，www.cctv.com主页变成了一欧洲美女子照片。
- 公安部物证鉴定中心网站被黑客篡改，2010年1月2日，公安部物证鉴定中心的中英文网站遭黑客入侵，网站页面不断被篡改。
- 入侵网站改成绩被诉系首例“黑客”，北京教育考试院原工作人员孟某，涉嫌利用木马病毒程序进入北京教育考试院网上证书查询系统，篡改全国计算机等级考试成绩，于近日被检方提起公诉。
- 女孩设山寨“彩票网”获有期徒刑，因创办“中国彩票官方网”，以提供中奖号码为诱饵骗取彩民入会费4万余元，25岁的女孩王某，因诈骗罪被北京宣武法院判处有期徒刑2年。

国内信息安全事件（10年1-2月）

- 河南：利用网络传播淫秽物品被判刑，2月5日，河南新乡市延津县人民法院对新乡市首例利用网络传播淫秽物品案作出一审判决，被告人肖某等11人分别被判处有期徒刑1年至拘役5个月缓刑1年不等。

- 上海：窃用他人账户套现 上海一网店店主被判7年，淘宝某店铺声称代人缴费后可打折收取账单金额，然而店铺卖家用来缴费的却是从不正当途径取得的他人银行账户内钱款。1月25日，上海一中院做出二审判决，认定网店店主犯信用卡诈骗罪。

- 河南：大量遭拒绝服务攻击，近期针对公共互联网的主要网络攻击是拒绝服务攻击，2010年1月有3353个IP地址所对应的主机被境外通过木马程序秘密控制，有3046个IP地址对应的主机被僵尸网络控制，被篡改网站数量70个，感染恶意代码的主机数量为3498个。



- 重庆：青年农民办钓鱼网站行骗盗取网购者5.2万，重庆市潼南县农村青年张某在网上租来域名和空间，做山寨淘宝、山寨易趣、山寨腾讯拍拍。通过这些“钓鱼网站”，盗走网购消费者5.2万余元。1月10日，张某因构成盗窃罪和传授犯罪方法罪，一审被判刑6年。

- 江苏：无锡“4G淫图”手机网站传播淫秽物品牟利案依法宣判。2010年2月11日，无锡市惠山区人民法院依法对“4G淫图”手机网站传播淫秽物品牟利案作出一审判决。该淫秽网站开办者陈柳生被判处有期徒刑11年。

国内信息安全事件（10年1-2月）

- 广东：黑客受雇潜入人事网篡改数据被判刑，黑客受雇潜入广东人事网篡改查询数据，为假证“转正”，并添加10多个虚假职称人员的资料。2010年1月26日，24岁的朱某因两次非法嵌入广东人事网上传并篡改数据，犯非法入侵计算机信息系统罪被越秀区法院判处有期徒刑1年零7个月。

- 厦门：不法分子开设网站炒股被刑拘，厦门不法分子开设“鸿龙国际”等十多个非法网站，以注册会员、发展下线、吸引会员参与模拟股票交易系统下单的方式进行网络赌博，庄家以抽取手续费的形式从中非法牟利。2月19日，厦门警方破获此案。

- 珠海：去昂过首例侵犯公民信息安全案例宣判，1月3日，被告人周某因非法出售公民个人信息资料被珠海市香洲人民法院以非法获取公民个人信息罪判处有期徒刑1年6个月，并处罚金。

- 深圳：“黄网”绑住科技公司网页，深圳南山高新区的一家科技公司网络服务器被黑客攻击，导致该公司负责维护的一些正规网站被点击时，会自动跳转到淫秽网站。南山警方一举破获此案。

- 香港：“兽兽门”传不雅视频 被黑客用来散布病毒，“中国第一车模兽兽”爆出的不良视频在网上大量传播，已被黑客用来散布病毒。很多用户通过QQ、MSN传播的“兽兽视频、兽兽视频全集.EXE”含有病毒，或者本身就是病毒，还有的黑客主动散播含毒的“兽兽视频下载网址”，用户中毒后会被窃取网游帐号、QQ密码等资料。

国内信息安全事件（10年1-2月）

- 湖北：湖北警方摧毁国内最大黑客培训网站，湖北警方近日成功摧毁国内规模最大的黑客培训网站“黑鹰安全网”，该网站招收会员逾18万人，向其提供木马程序，“传授”、“交流”非法控制他人计算机的“技巧”。

- 湖南：黑客篡改湖南通管局主页，1月29日，湖南省通信管理局网站被黑。黑客篡改主页，留言声称是因为几个月网站备案都未审批通过，所以不满而攻击。

安全趋势

1、集团化、产业化的趋势

- 产业链：病毒木马编写者 - 专业盗号人员 - 销售渠道 - 专业玩家
- 病毒不再安于破坏系统，销毁数据，而是更关注财产和隐私。
- 电子商务成为热点，针对网络银行的攻击也更加明显
- 2008年病毒会更加紧盯在线交易环节，从早期的虚拟价值盗窃转向直接金融犯罪。

2、“黑客”逐渐变成犯罪职业

- 财富的诱惑，使得黑客袭击不再是一种个人兴趣，而是越来越多的变成一种有组织的、利益驱使的职业犯罪
- 事例：拒绝服务相关的敲诈勒索和“网络钓鱼”。

安全趋势

3、恶意软件的转型

- 我国仍然是恶意软件最多的国家
- 恶意软件在行为上将有所改观，病毒化特征削弱，但手段更“高明”，包含更多的钓鱼欺骗元素

4. 网页挂马危害继续延续

- 服务器端系统资源和流量带宽资源大量损失
- 成为网络木马传播的“帮凶”
- 客户端的用户个人隐私受到威胁

安全趋势

5、利用应用软件漏洞的攻击将更为迅猛

- 新的漏洞出现要比设备制造商修补的速度更快
- 一些嵌入式系统中的漏洞难以修补
- 零日攻击现象日趋普遍

6、Web2.0的产品将受到挑战

- 以博客、论坛为首的web2.0产品将成为病毒和网络钓鱼的首要攻击目标
- 社区网站上带有社会工程学性质的欺骗往往超过安全软件所保护的范畴
- 自动邮件发送工具日趋成熟，垃圾邮件制造者正在将目标转向音频和视频垃圾邮件

安全趋势

- 7、无线网络、移动手机成为新的安全重灾区，消费者电子设备遭到攻击的可能性增大
  - 在无线网络中被传输的信息没有加密或者加密很弱，很容易被窃取、修改和插入，存在较严重的安全漏洞
  - 手机病毒利用普通短信、彩信、上网浏览、下载软件与铃声等方式传播，还将攻击范围扩大到移动网关、WAP服务器或其他的网络设备
  - 越来越多采用USB标准进行连接，并使用了更多存储设备和电脑外围产品

信息安全意义

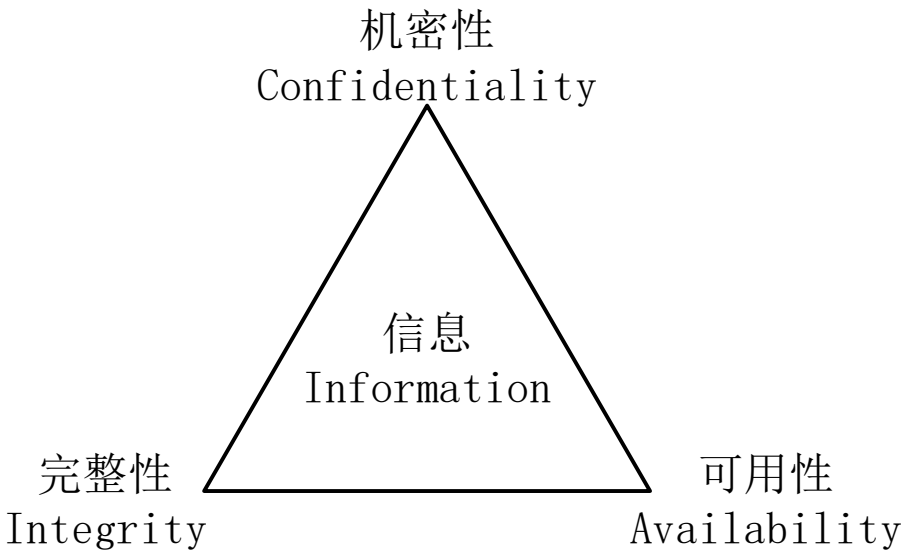
- 互联网安全不仅影响普通网民的信息和数据的安全性，而且严重的影响国家的健康发展。
  - 网络安全与政治
  - 网络安全与经济
  - 网络安全与军事
  - 网络安全与社会稳定

1.3.3 互联网的安全性分析

- 互联网的设计原始背景
- 网络传输的安全性
- 信息系统的安全性
  - 基础网络应用成为黑客及病毒的攻击重点。
  - 系统漏洞带来的安全问题异常突出。
  - Web程序安全漏洞愈演愈烈。
- 社会工程学攻击越来越多

1.4 信息安全体系结构

- **1.4.1 面向目标的知识体系结构**



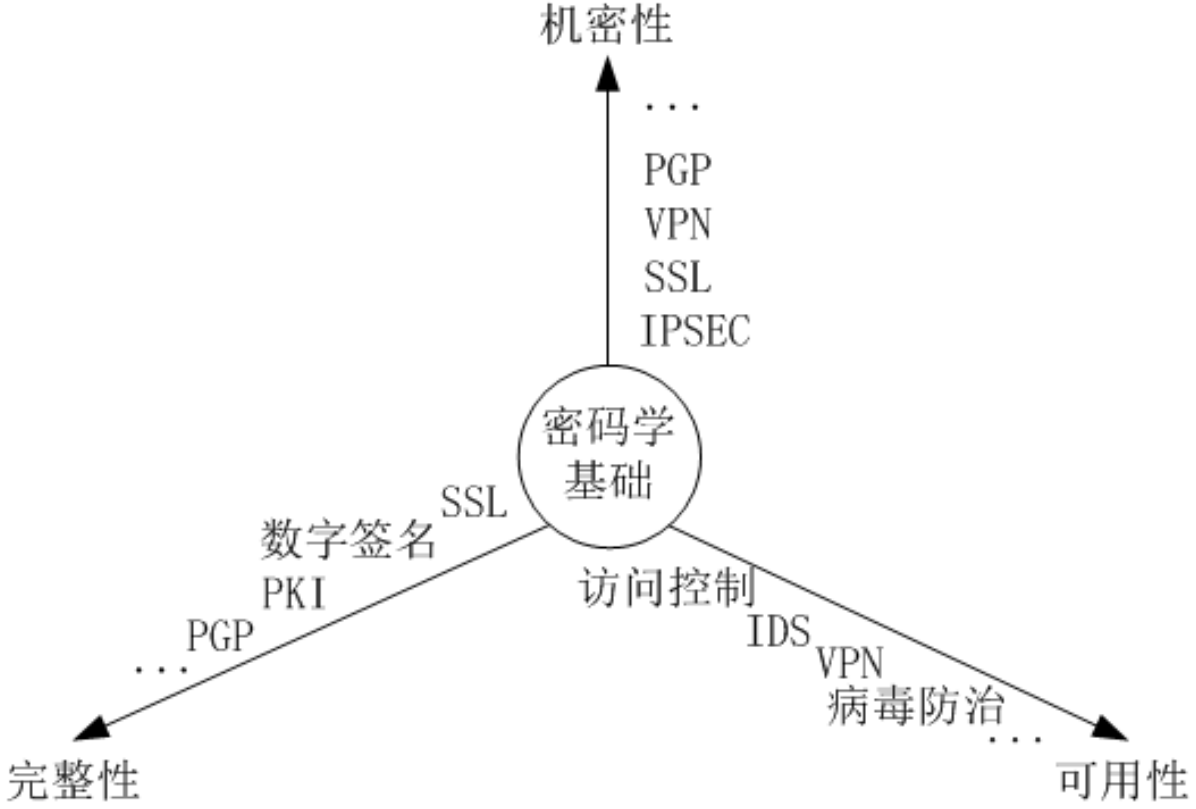
信息安全的三个基本目标（金三角）

CIA三元组

- CIA三元组是信息安全的三个最基本的目标
  - 机密性Confidentiality：指信息在存储、传输、使用过程中，不会泄漏给非授权用户或实体；
  - 完整性Integrity：指信息在存储、使用、传输过程中，不会被非授权用户篡改或防止授权用户对信息进行不恰当的篡改；
  - 可用性Availability：指确保授权用户或实体对信息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资源。
- DAD（Disclosure、Alteration、Destruction）是最普遍的三类风险

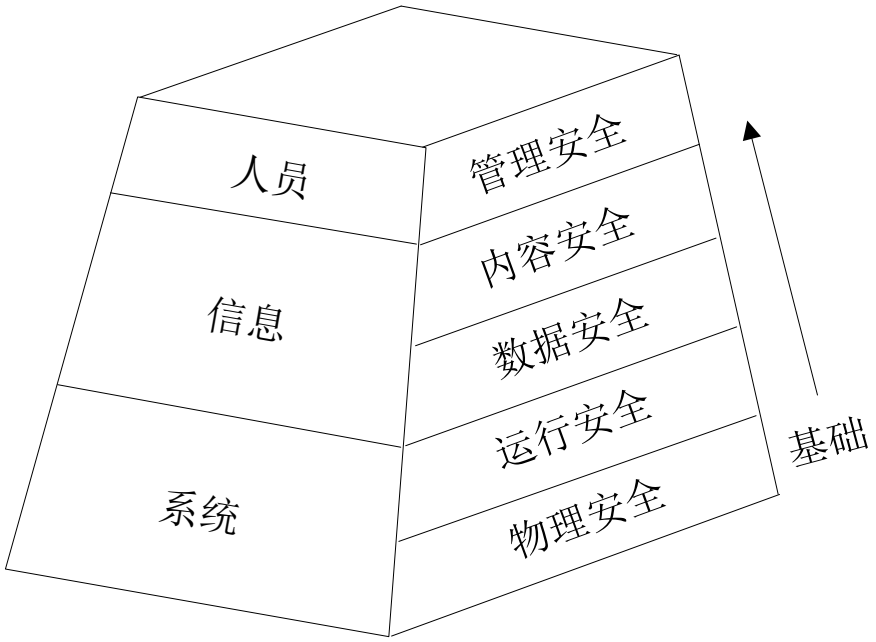
围绕CIA三元组展开的知识体系

- 密码学是三个信息安全目标的技术基础
- CIA技术存在着一定程度上的内容交叉



1.4.2 面向应用的层次型技术体系架构

- 信息系统基本要素
  - 人员、信息、系统
- 安全层次
  - 三个不同部分存在五个的安全层次与之对应
  - 每个层次均为其上层提供基础安全保证



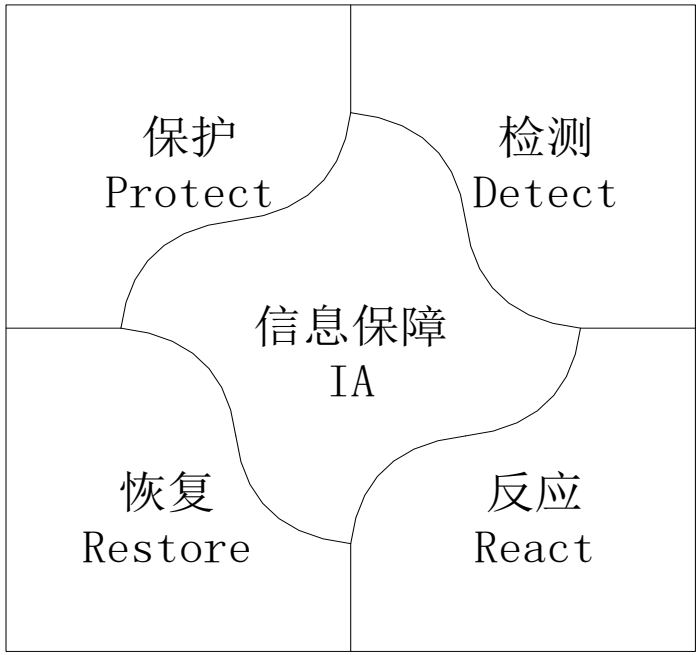
面向应用的层次型信息安全技术体系结构

安全层次

- 物理安全
  - 指对网络及信息系统物理装备的保护。
- 运行安全
  - 指对网络及信息系统的运行过程和运行状态的保护。
- 数据安全
  - 指对数据收集、存储、检索、传输等过程提供的保护，不被非法冒充、窃取、篡改、抵赖。
- 内容安全
  - 指依据信息内涵判断是否违反特定安全策略，采取相应的安全措施。
- 管理安全
  - 指通过针对人的信息行为的规范和约束，提供对信息的机密性、完整性、可用性以及可控性的保护。

1.4.3 面向过程的信息安全保障体系

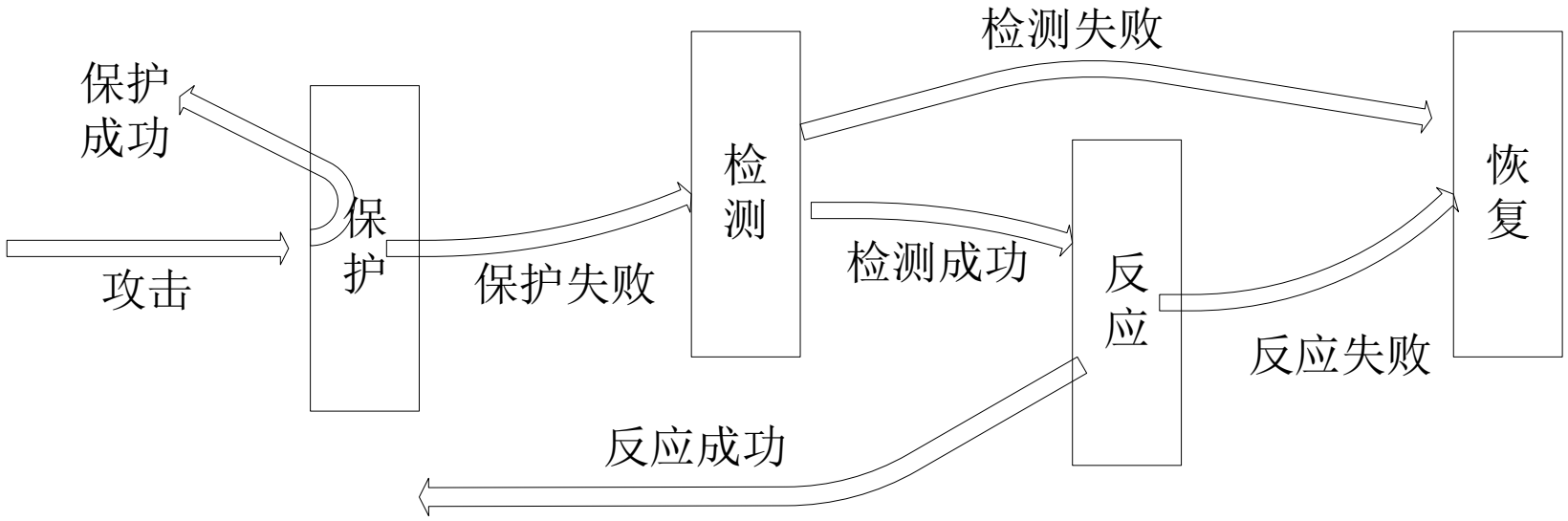
- 美国国防部提出的“信息安全保障体系”为诠释了安全保障的内涵。
- 信息安全保障体系包括四个部分内容，即PDRR。
  - 保护（Protect）
  - 检测（Detect）
  - 反应（React）
  - 恢复（Restore）



信息保障体系

1.4.3 面向过程的信息安全保障体系

- 信息安全保障是一个完整的动态过程，而保护、检测、反应和恢复可以看作信息安全保障四个子过程。

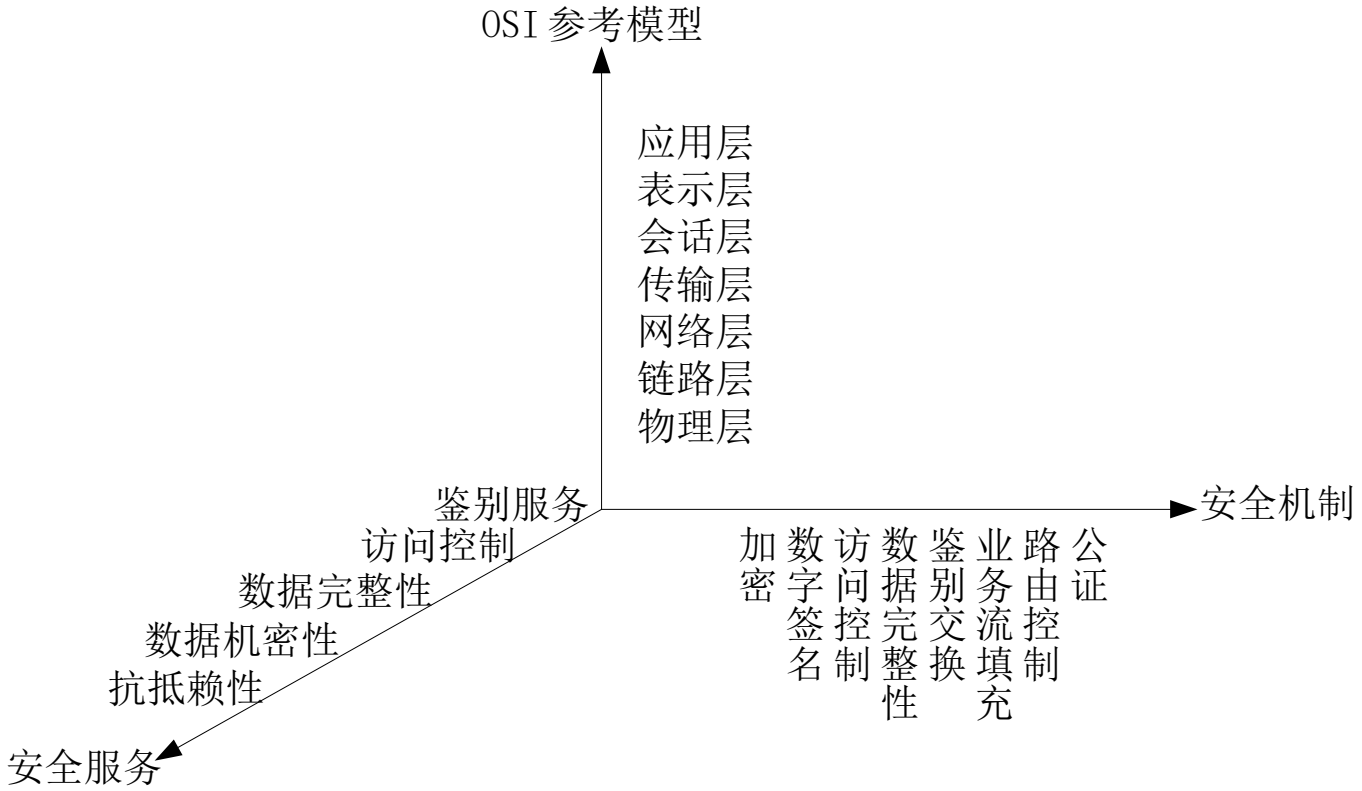


PDRR 模型安全保障动态过程示意图

1.4.4 OSI开放系统互连安全体系结构

– ISO7498-2（1989）

- 《信息处理系统、开放系统互连、基本参考模型—第2部分：安全体系结构》。描述的开放系统互联安全体系结构是一个普遍适用的安全体系结构。



ISO7498-2 安全体系结构三维图

安全服务（Security Service）

- **鉴别服务** 确保某个实体身份的可靠性。
- **访问控制** 确保只有经过授权的实体才能访问受保护的资源。
- **数据机密性** 确保只有经过授权的实体才能理解受保护的信息。
- **数据完整性** 防止对数据的未授权修改和破坏。
- **抗抵赖性** 用于防止对数据源以及数据提交的否认。

安全机制（Security Mechanism）

- **加密** 用于保护数据的机密性。
- **数字签名** 保证数据完整性及不可否认性的一种重要手段。
- **访问控制** 访问实体成功通过认证，访问控制对访问请求进行处理，查看是否具有访问所请求资源的权限，并做出相应的处理。
- **数据完整性** 用于保护数据免受未经授权的修改。
- **鉴别交换** 用于实现通信双方实体的身份鉴别。
- **业务流填充** 针对的是对网络流量进行分析攻击。
- **路由控制** **可以指定数据报文通过网络**的路径。路径上的节点都是可信任的
- **公证机制** 由第三方来确保数据完整性、数据源、时间及目的地的正确。

问题

① 怎么理解信息安全、机密性、完整性、可用性，举例说明；

② “信息安全是当今社会的亟待解决的重大问题”，你认为如何？

③ 你了解的密码学是什么样的？

④ 什么是对称密钥密码？用途；

⑤ 什么是公开密钥密码？用途；

⑥ 什么是散列函数（摘要函数）？用途；

第2章 密码学基础

翟健宏

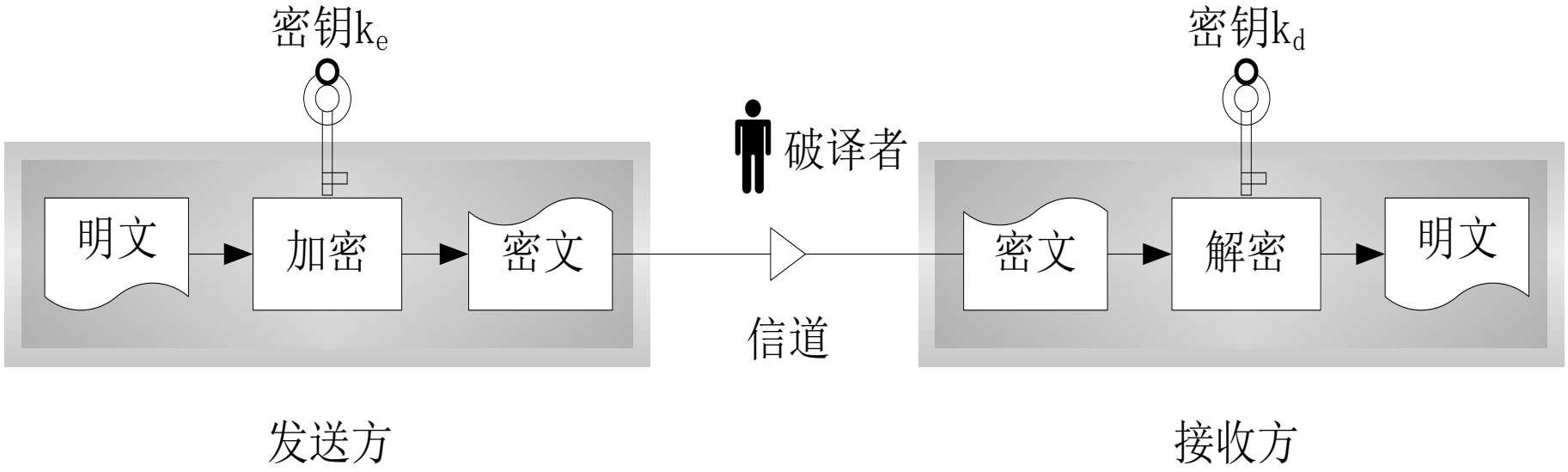
2.1 密码学基础知识

2.1.1 引言

- 解决数据的机密性、完整性、不可否认性以及身份识别等问题均需要以密码为基础
  - 密码技术是保障信息安全的核心基础。
- 密码学(Cryptography)包括密码编码学和密码分析学两部分。
  - 将密码变化的客观规律应用于编制密码用来保守通信秘密的，称为密码编码学；
  - 研究密码变化客观规律中的固有缺陷，并应用于破译密码以获取通信情报的，称为密码分析学。
- 历史
  - 宋代的曾公亮、丁度等编撰《武经总要》
  - 卡西斯基所著《密码和破译技术》
  - 1949年香农发表了《秘密体制的通信理论》

2.1.2 密码体制

- 消息在密码学中被称为明文（Plain Text）。
- 伪装消息以隐藏它的内容的过程称为加密(Encrypt)
- 被加密的消息称为密文(Cipher Text)
- 把密文转变为明文的过程称为解密(Decrypt)。



加密通信模型

2.1.2 密码体制

- 完整密码体制要包括如下五个要素
  - M是可能明文的有限集称为明文空间；
  - C是可能密文的有限集称为密文空间；
  - K是一切可能密钥构成的有限集称为密钥空间；
  - E为加密算法，对于任一密钥， 都能够有效地计算；
  - D为解密算法，对于任一密钥，都能够有效地计算。

- 密码体系必须满足如下特性：
  - 加密算法(Ek： M->C)和解密算法(Dk： C->M)满足:
    - **Dk(Ek(x))=x**, 这里x∈M；
  - 破译者不能在有效的时间内破解出密钥k或明文x。

2.1.3 密码的分类

- 依据密码体制的特点以及出现的时间分类：
  - 古典替换密码、对称密钥密码、公开密钥密码
- 依据处理数据的类型
  - 分组密码(block cipher)、序列密码(stream cipher)
- 密码分析也称为密码攻击，密码分析攻击主要包括：
  - 唯密文攻击、已知明文攻击、选择明文攻击、自适应选择明文攻击、选择密文攻击、选择密钥攻击

2.2 古典替换密码

2.2.1 简单代替密码

- 简单代替密码
  - 指将明文字母表M中的每个字母用密文字母表C中的相应字母来代替
  - 例如：移位密码、乘数密码、仿射密码等。
- 移位密码
  - 具体算法是将字母表的字母右移k个位置，并对字母表长度作模运算。
    - 每一个字母具有两个属性，本身代表的含义，可计算的位置序列值：
    - 加密函数：$E_k(m) = (m + k) \bmod q$；
    - 解密函数：$D_k(c) = (c - k) \bmod q$；

凯撒Caesar密码

- 凯撒密码体系的数学表示：
  - M=C={有序字母表}，q = 26，k = 3。
    - 其中q 为有序字母表的元素个数，本例采用英文字母表，q = 26。
  - 使用凯撒密码对明文字符串逐位加密结果如下：
    - 明文信息M = meet me after the toga party
    - 密文信息C = phhw ph diwho wkh wrjd sduwb

乘数密码

- 乘数密码
  - 将明文字母串逐位乘以密钥k并进行模运算。
  - 数学表达式:$E_k(m)=k * m \bmod q$, gcd (k, q) = 1。
    - gcd(k,q)=1表示k与q的最大公因子为1。
  - 算法描述：
    - M=C=Z/(26)，明文空间和密文空间同为英文字母表空间，包含26个元素；q=26；
    - K={k∈整数集 | 0<k<26，gcd(k,26)=1}，密钥为大于0小于26，与26互素的正整数；
    - $E_k(m) = k\ m \bmod q$。
    - $D_k^{-1}(c)=k^{-1}c \bmod q$，其中$k^{-1}$为k在模q下的乘法逆元。

密钥取值与乘法逆元

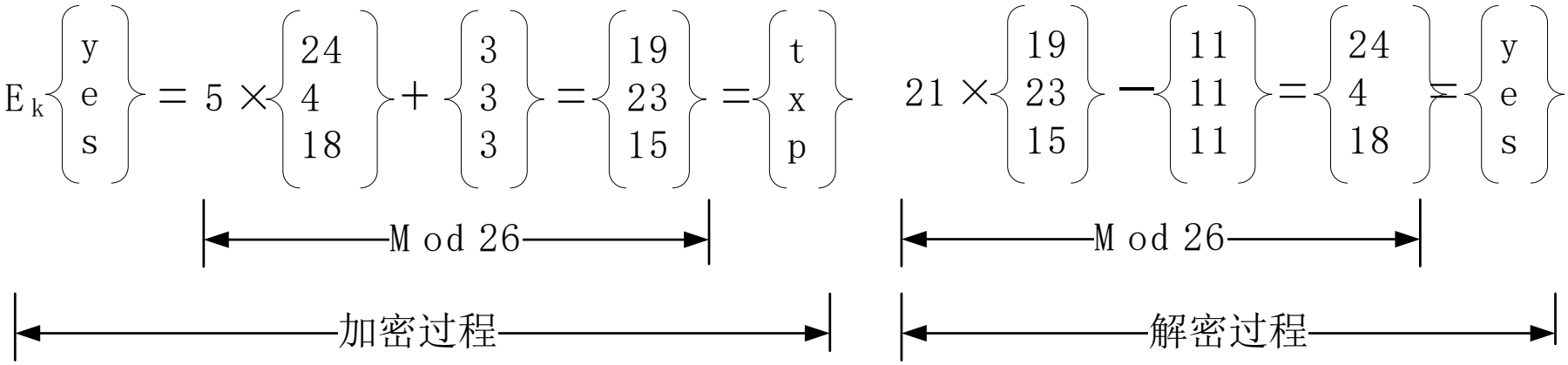
- 乘数密码的密钥k与26互素时，加密变换才是一一映射的，
  - k的选择有11种：3、5、7、9、11、15、17、19、21、23、25。K取1时没有意义。
- k^{-1}为k在模q下的乘法逆元，
  - 其定义为$k^{-1} * k \bmod q = 1$，
  - 可采用扩展的欧几里德算法。欧几里德算法又称辗转相除法，用于计算两个整数a和b的最大公约数。

仿射密码

- 仿射密码
  - 可以看作是移位密码和乘数密码的结合。
- 密码体制描述如下：
  - M=C=Z/(26)；q=26；
  - K={ $k_1,k_2 \in Z \mid 0< k_1,k_2<26$，$gcd(k_1,26)=1$}；
  - $E_k(m)=(k_1m+k_2) \bmod q$；
  - $D_k(c)= k_1^{-1}(c - k_2) \bmod q$，其中$k_1^{-1}$为$k_1$在模q下的乘法逆元。
- 密钥情况，k_1和k_2？

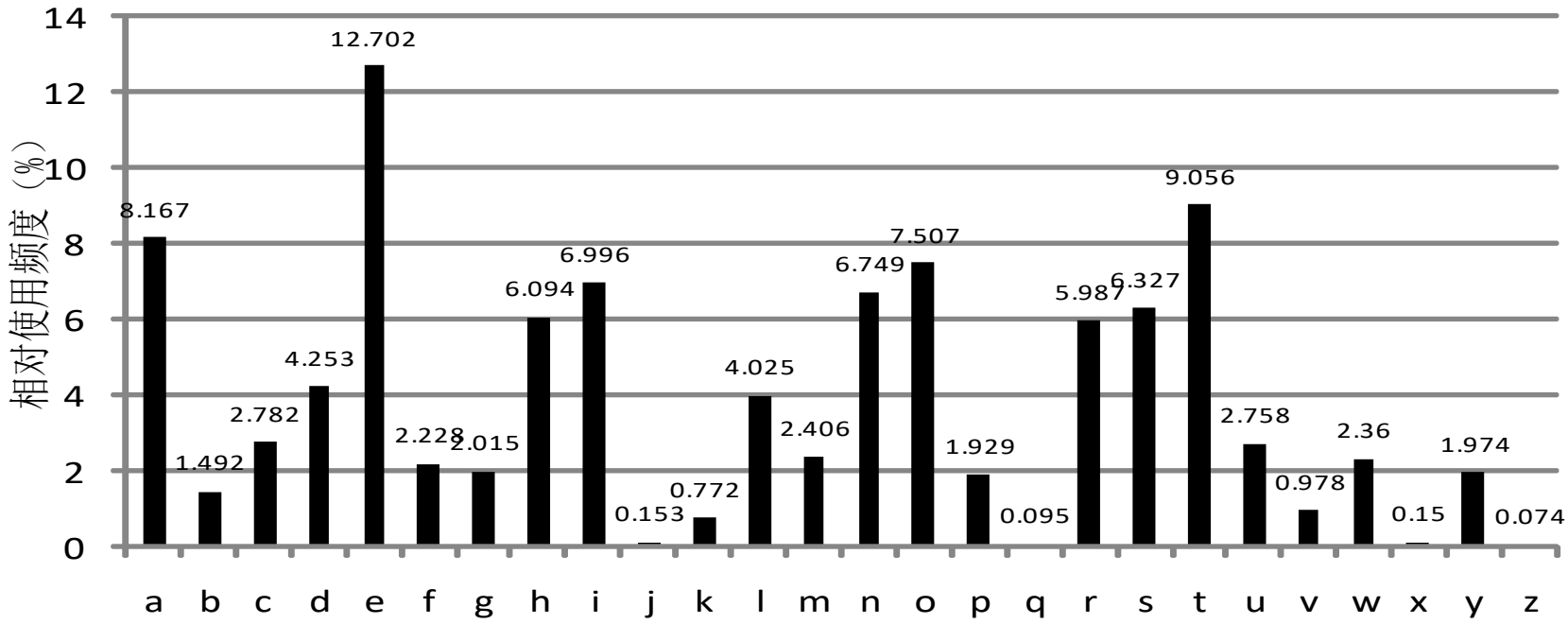
仿射密码事例

- 设k＝（5，3），注意到$5^{-1} \bmod 26=21$，
- 加密函数：
  - $E_k(x)=5x+3 \pmod{26}$，
- 解密函数：
  - $D_k(y)=21(y-3) \bmod 26 =21y-11 \pmod{26}$。
- 加密明文“yes”的加密与解密过程如下：



基于统计的密码分析

- 简单代替密码的加密是从明文字母到密文字母的一一映射
- 攻击者统计密文中字母的使用频度，比较正常英文字母的使用频度，进行匹配分析。
- 如果密文信息足够长，很容易对单表代替密码进行破译。



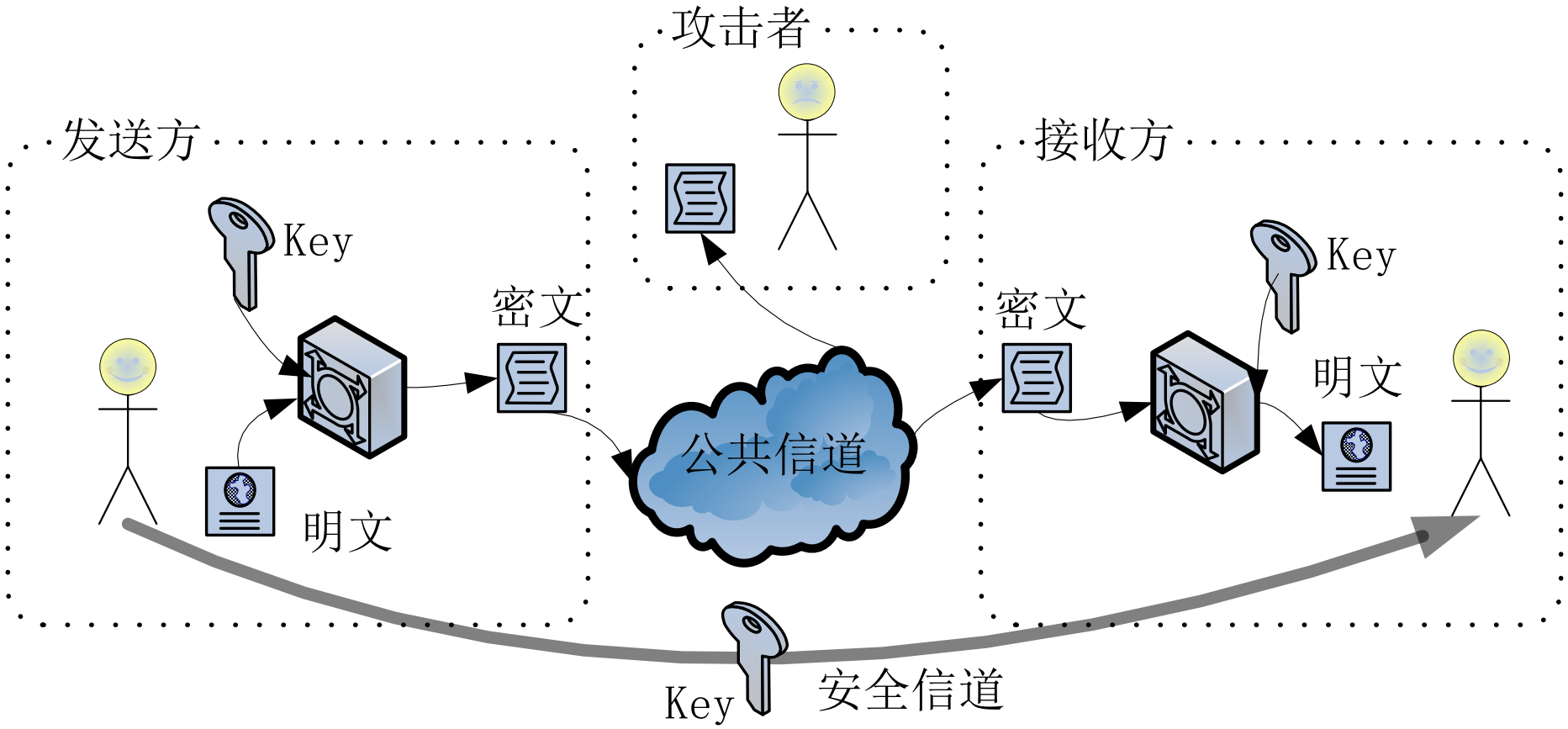
2.2.2多表代替密码

- 多表代替密码是以一系列代替表依次对明文消息的字母进行代替的加密方法。
- 多表代替密码使用从明文字母到密文字母的多个映射来隐藏单字母出现的频率分布。
- 每个映射是简单代替密码中的一对一映射
  - 若映射系列是非周期的无限序列，则相应的密码称为非周期多表代替密码。
- 非周期多表代替密码
  - 对每个明文字母都采用不同的代替表(或密钥)进行加密，称作一次一密密码。

维吉尼亚Vigenère密码

- 经典的多表代换密码有：
  - Vigenère、Beaufort、Running Key、Vernam和轮转机等密码。
- 维吉尼亚Vigenère密码
  - 是以移位代替为基础的周期多表代替密码。
  - 加密时每一个密钥被用来加密一个明文字母，当所有密钥使用完后，密钥又重新循环使用。
- 维吉尼亚Vigenère密码算法如下：
  - $E_k(m)=C_1 C_2 \ldots C_n$，其中$C_i=（m_i + k_i）\bmod 26$；
  - 密钥K可以通过周期性反复使用以至无穷。

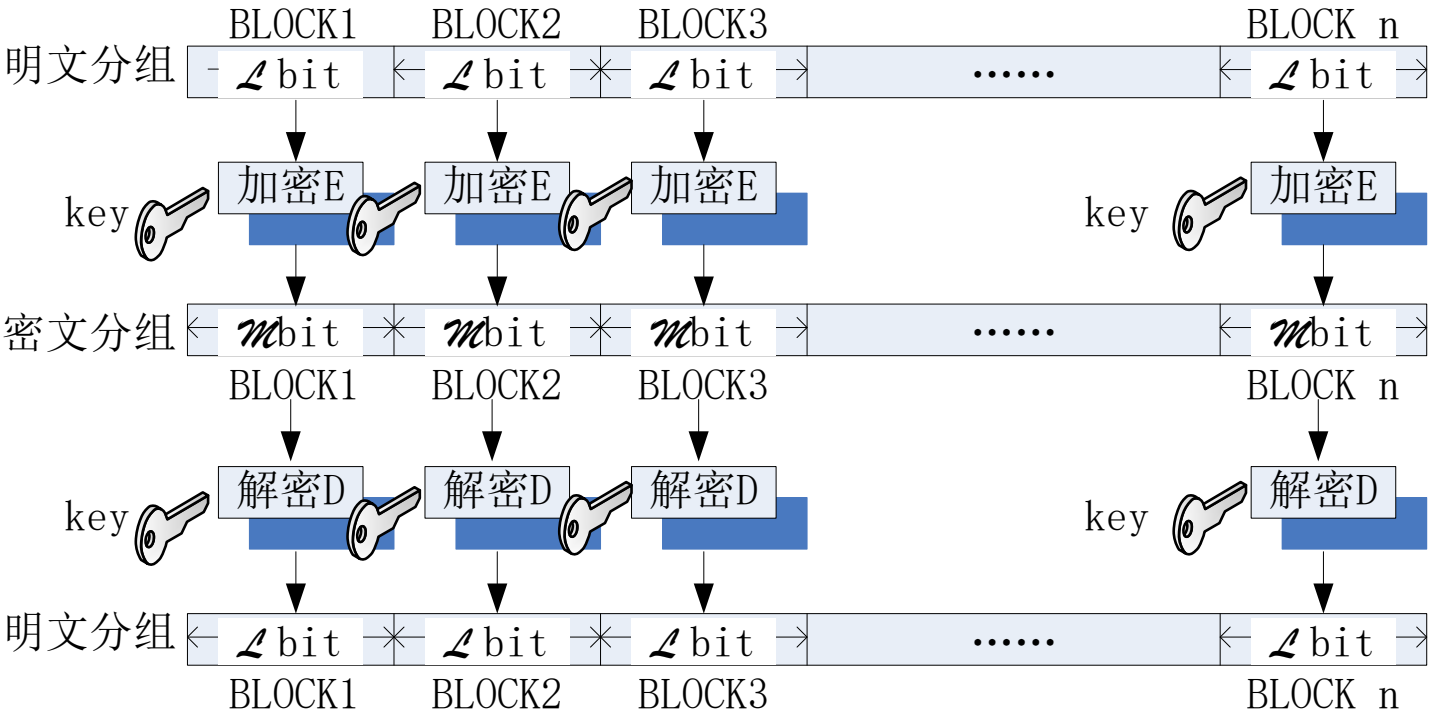
2.3 对称密钥密码



对称密钥密码的模型

2.3.1 对称密钥密码加密模式

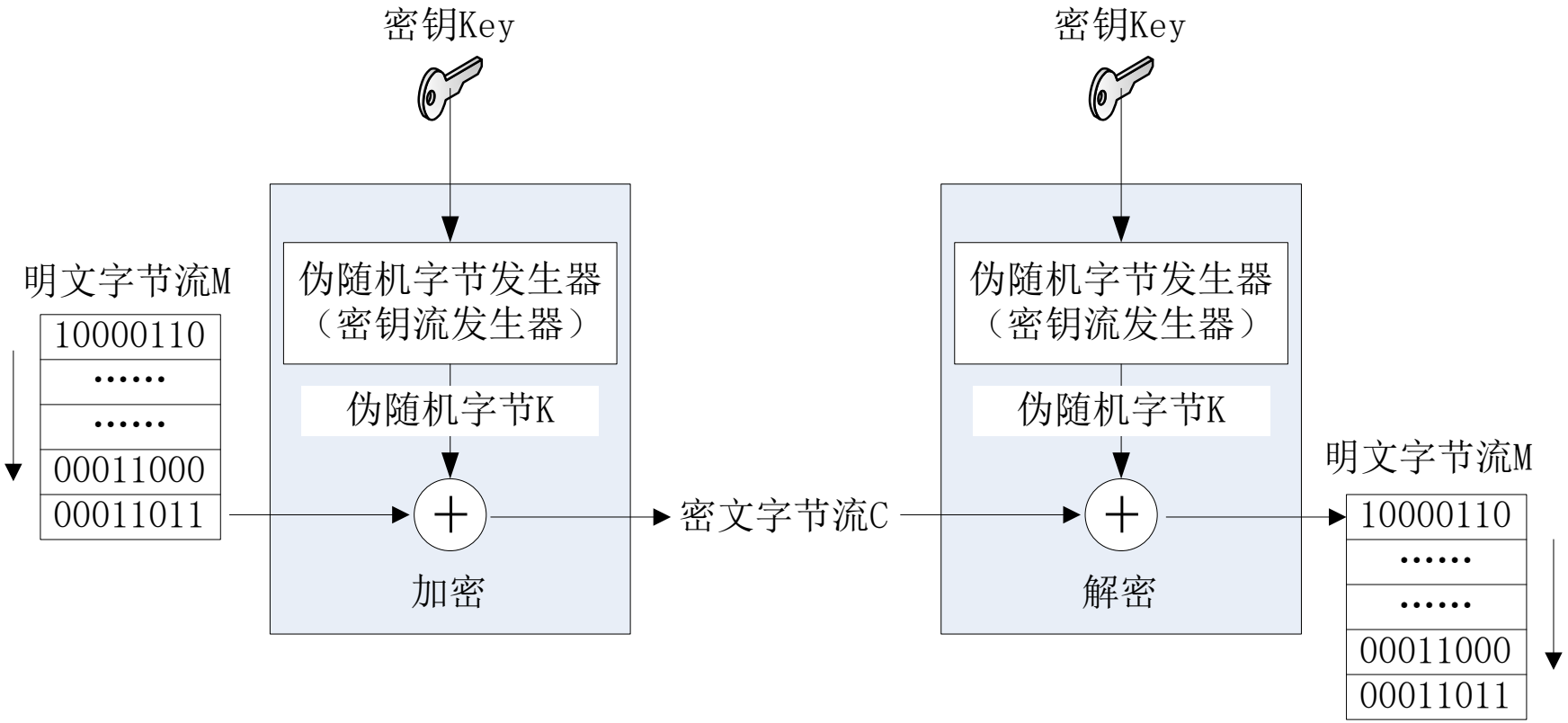
- 对称密码加密系统从工作方式上可分为：
  - 分组密码、序列密码
- 分组密码原理：
  - 明文消息分成若干固定长度的组，进行加密；解密亦然。



分组密码工作原理示意图

序列密码（流密码）

- 通过伪随机数发生器产生性能优良的伪随机序列(密钥流)，用该序列加密明文消息流，得到密文序列；解密亦然。



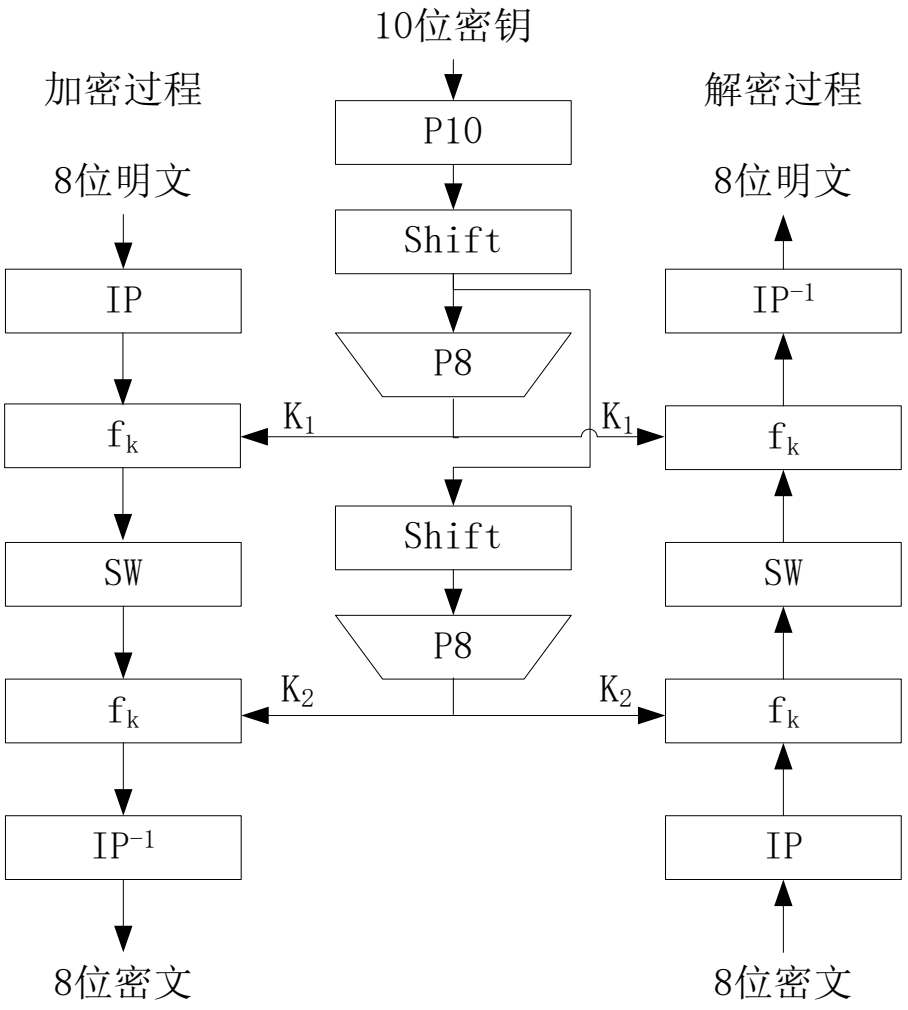
序列密码工作原理示意图

2.3.2 数据加密标准DES

- 1973年美国国家标准局NBS公开征集国家密码标准方案；
  - ① 算法必须提供高度的安全性；
  - ② 算法必须有详细的说明，并易于理解；
  - ③ 算法的安全性取决于密钥，不依赖于算法；
  - ④ 算法适用于所有用户；
  - ⑤ 算法适用于不同应用场合；
  - ⑥ 算法必须高效、经济；
  - ⑦ 算法必须能被证实有效；
  - ⑧ 算法必须是可出口的。
- 1974年NBS开始第二次征集时，IBM公司提交了算法LUCIFER。
  - 1977年LUCIFER被美国国家标准局NBS作为“数据加密标准 FIPS PUB 46”发布，简称为DES

S-DES

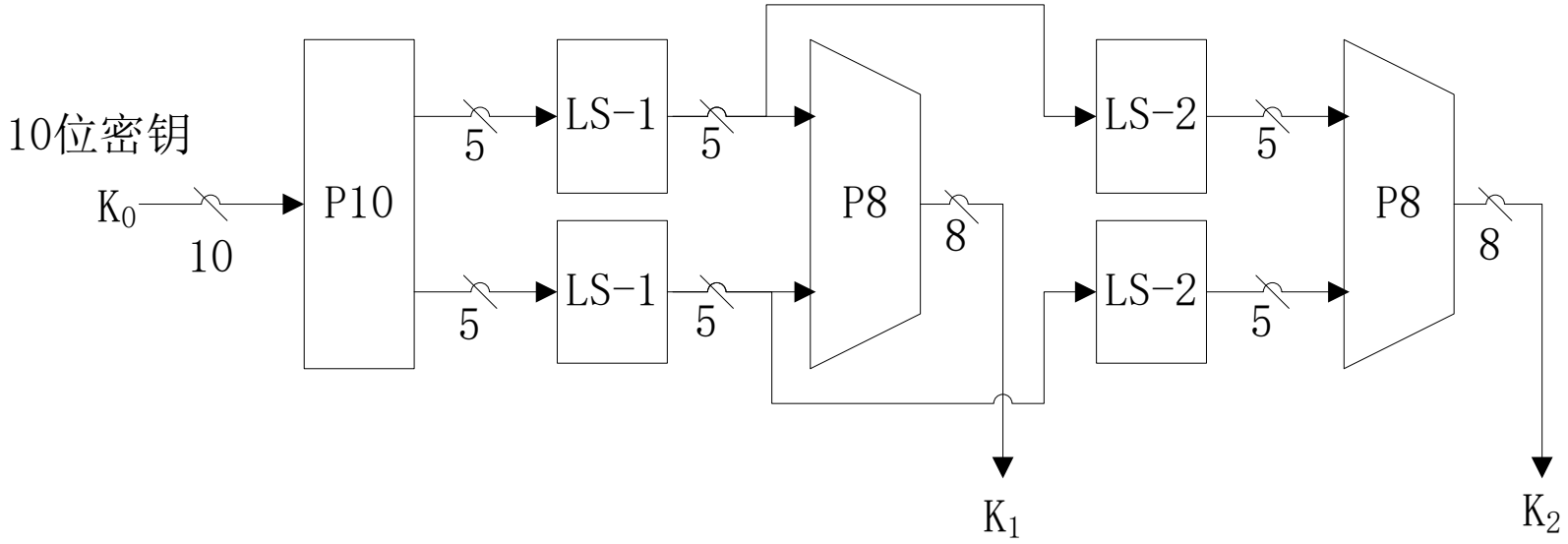
- S-DES加密算法
  - S-DES是由美国圣达卡拉大学的Edward Schaeffer教授提出的，主要用于教学，其设计思想和性质与DES一致，有关函数变换相对简化，具体参数要小得多。
  - 输入为一个8位的二进制明文组和一个10位的二进制密钥，输出为8位二进制密文组；
  - 解密与加密基本一致。
  - 加密:$IP^{-1}(f_{k2}(SW(f_{k1}(IP(明文)))))$
  - 解密: $IP^{-1}(f_{k1}(SW(f_{k2}(IP(密文)))))$



S-DES的体制

S-DES的密钥产生

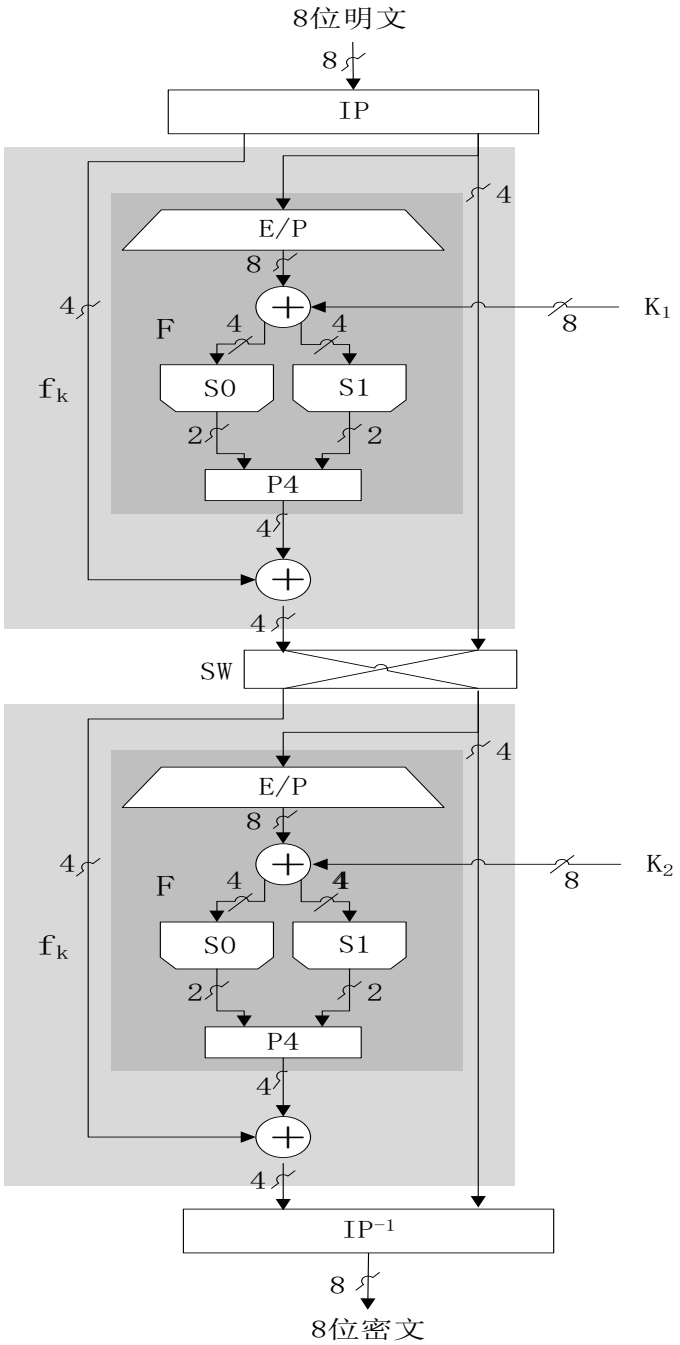
- P10=(3,5,2,7,4,10,1,9,8,6)
- 循环左移函数LS
- P8=(6,3,7,4,8,5,10,9)



S-DES的密钥产生

S-DES的加密变换过程

- IP=(2,6,3,1,4,8,5,7);
- IP^{-1}=(4,1,3,5,7,2,8,6)
- E/P=（4,1,2,3,2,3,4,1）
- “⊕”:按位异或运算;
- P4=（2,4,3,1）
- S盒函数
  - S0和S1为两个盒子函数，将输入作为索引查表，得到相应的系数作为输出。
- SW:将左4位和右4位交换。



S-DES的加密过程

S盒函数

S0=

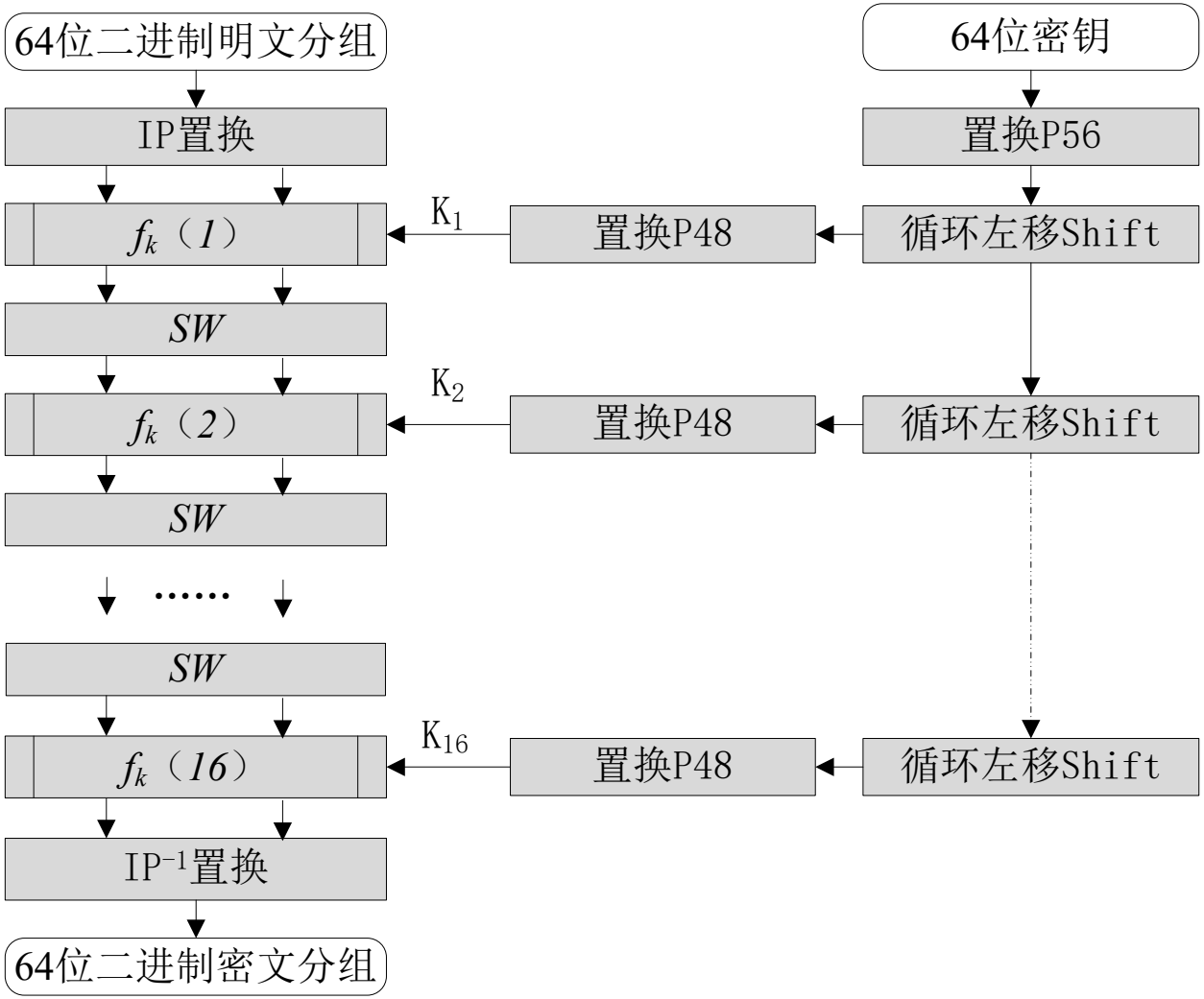
	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S1=

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

- S盒函数按下述规则运算：
  - 输入的第1位和第4位二进制数合并为一个两位二进制数，作为S盒的行号索引i；
  - 将第2位和第3位同样合并为一个两位二进制数，作为S盒的列号索引j，
  - 确定S盒矩阵中的一个系数（i，j）。
  - 此系数以两位二进制数形式作为S盒的输出。
  - 例如：
    - $L'=(l_0,l_1,l_2,l_3)=(0,1,0,0)$，　$(i,j)=(0,2)$
    - 在S0中确定系数3，则S0的输出为11B。

DES算法



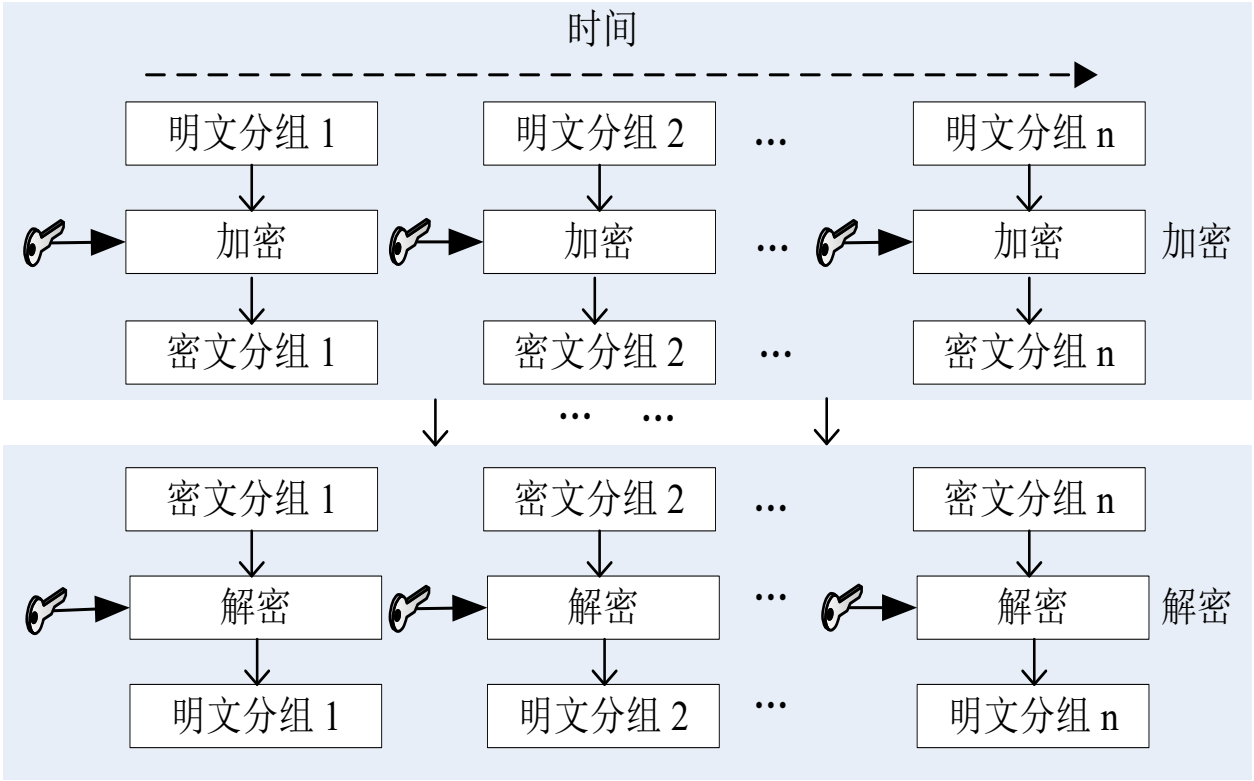
DES算法框图

DES的安全问题

- 1977年，耗资两千万美元建成一个专门计算机用于DES的破译，需要12个小时的破解才能得到结果。
- 1994年世界密码大会，M.Matsui提出线性分析方法，利用243个已知明文，成功破译DES，
- 1997年首届“向DES挑战”的竞技赛。罗克·维瑟用了96天时间破解了用DES加密的一段信息。
- 2000年1月19日，电子边疆基金会组织25万美元的DES解密机以22.5小时成功破解DES加密算法。
- DES的最近一次评估是在1994年，同时决定1998年12月以后，DES将不再作为联邦加密标准。

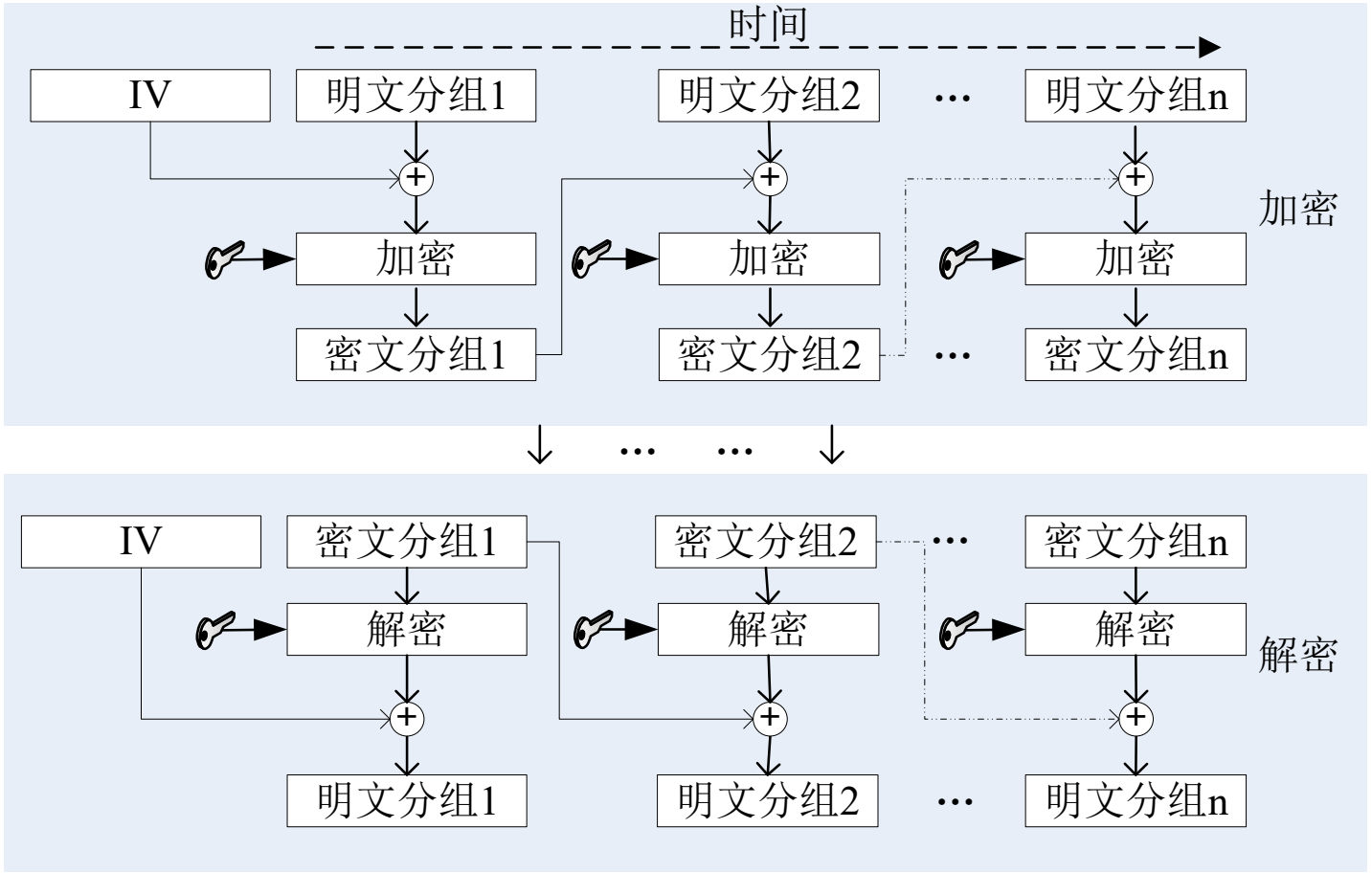
2.3.3 分组密码的工作模式

- 电子编码本模式（ECB）



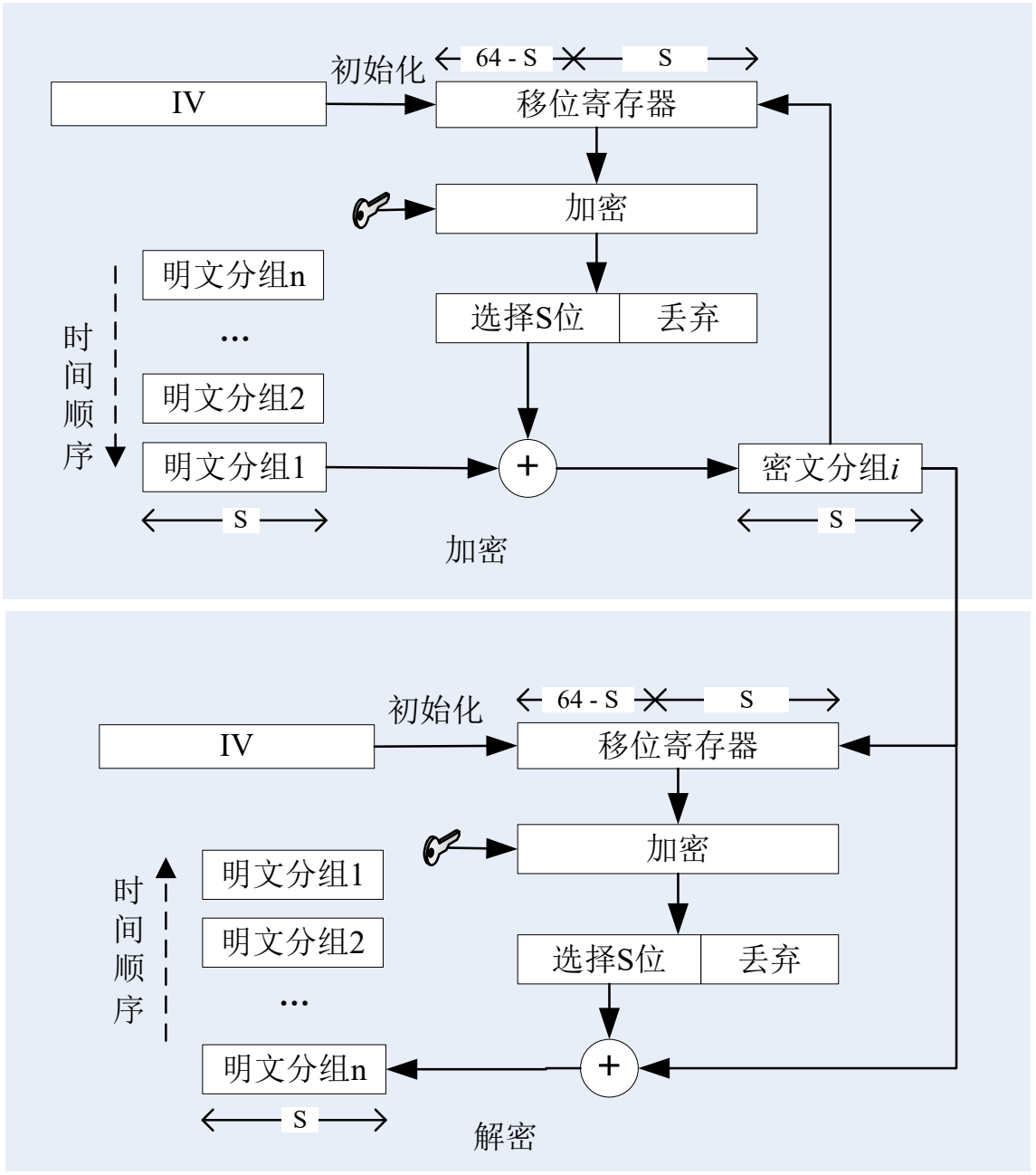
ECB工作模式

密码分组链接模式（CBC）



CBC工作模式

密码反馈模式（CFB）



CFB 工作模式

输出反馈模式（OFB）

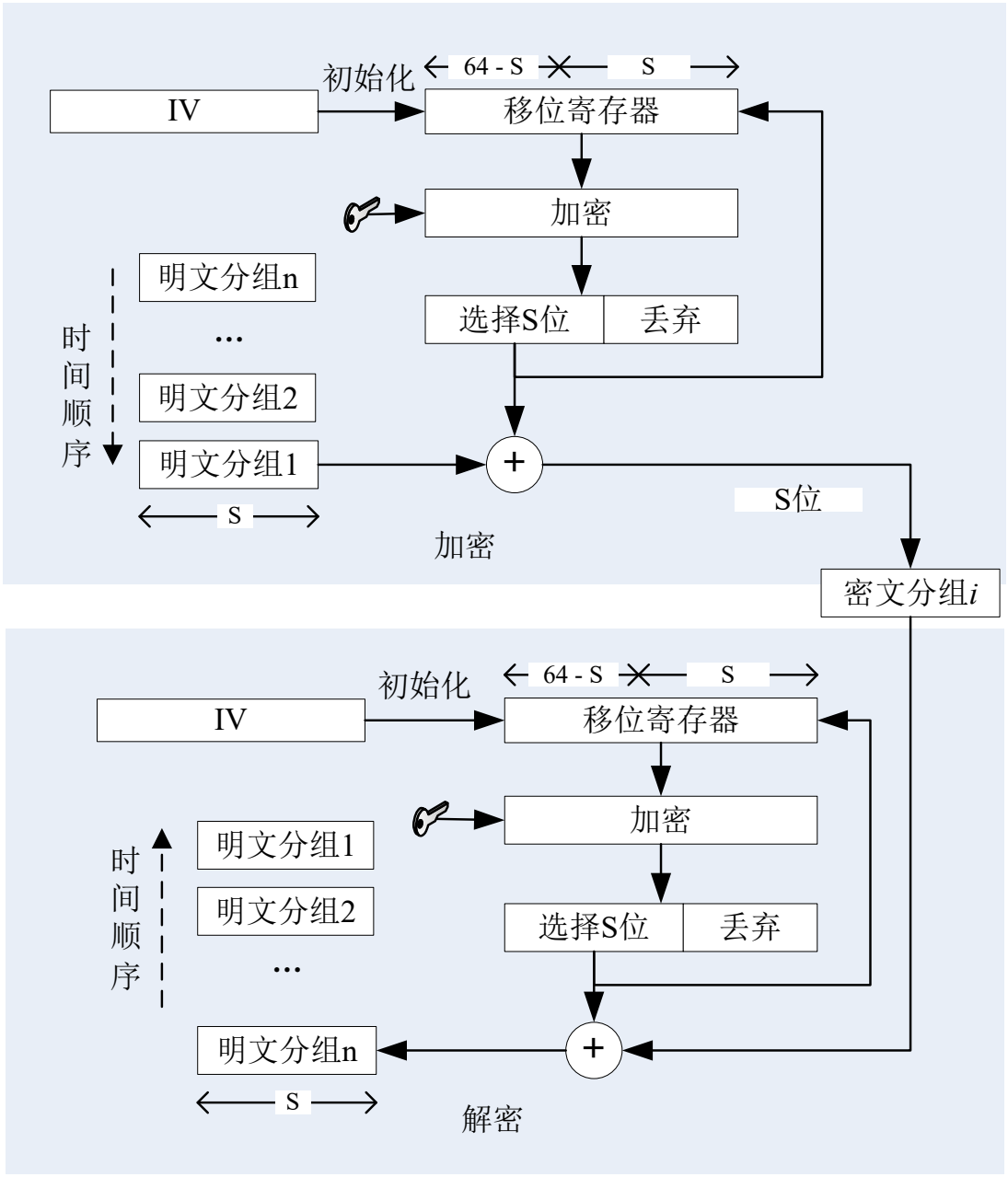


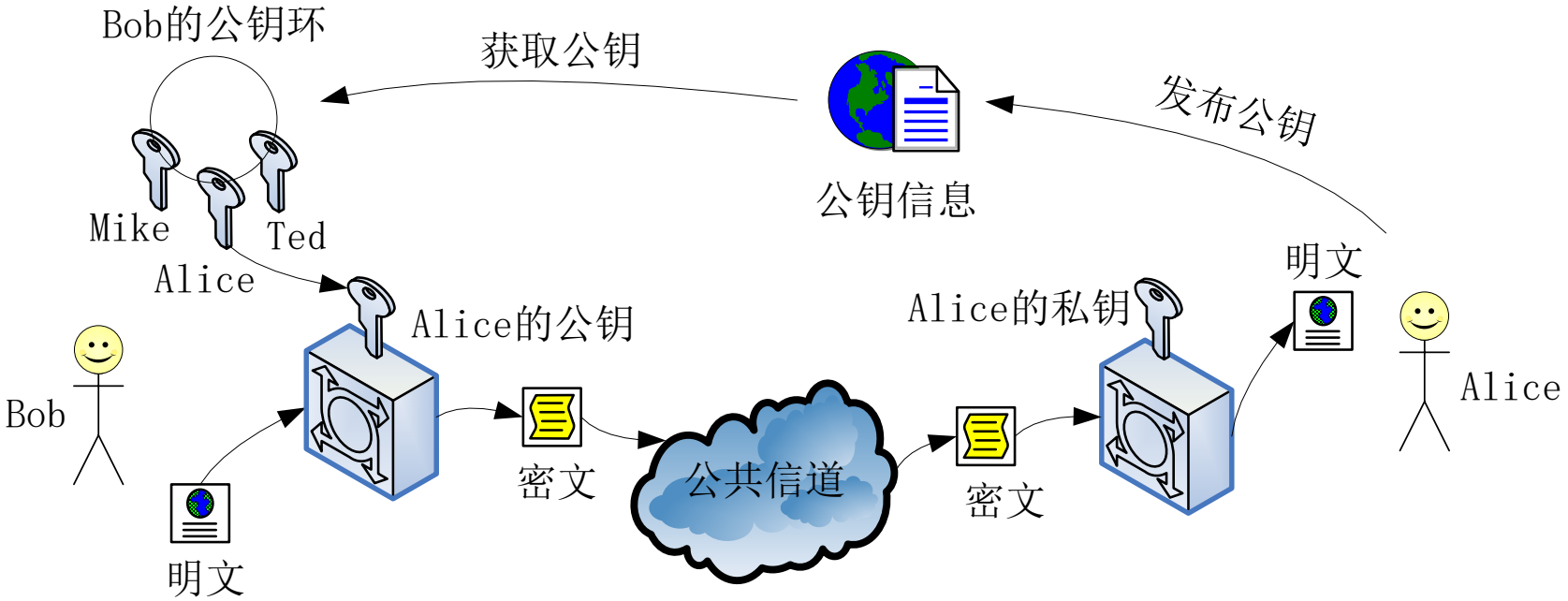
图 2.14 OFB 工作模式

2.3.4其他对称密码简介

- 三重DES
- RC5
- IDEA
- AES算法

2.4公开密钥密码

- 公开密钥密码又称非对称密钥密码或双密钥密码
  - 加密密钥和解密密钥为两个独立密钥。
  - 公开密钥密码的通信安全性取决于私钥的保密性。



公开密钥密码的模型

2.4.1 公开密钥理论基础

公开密钥密码的核心思想

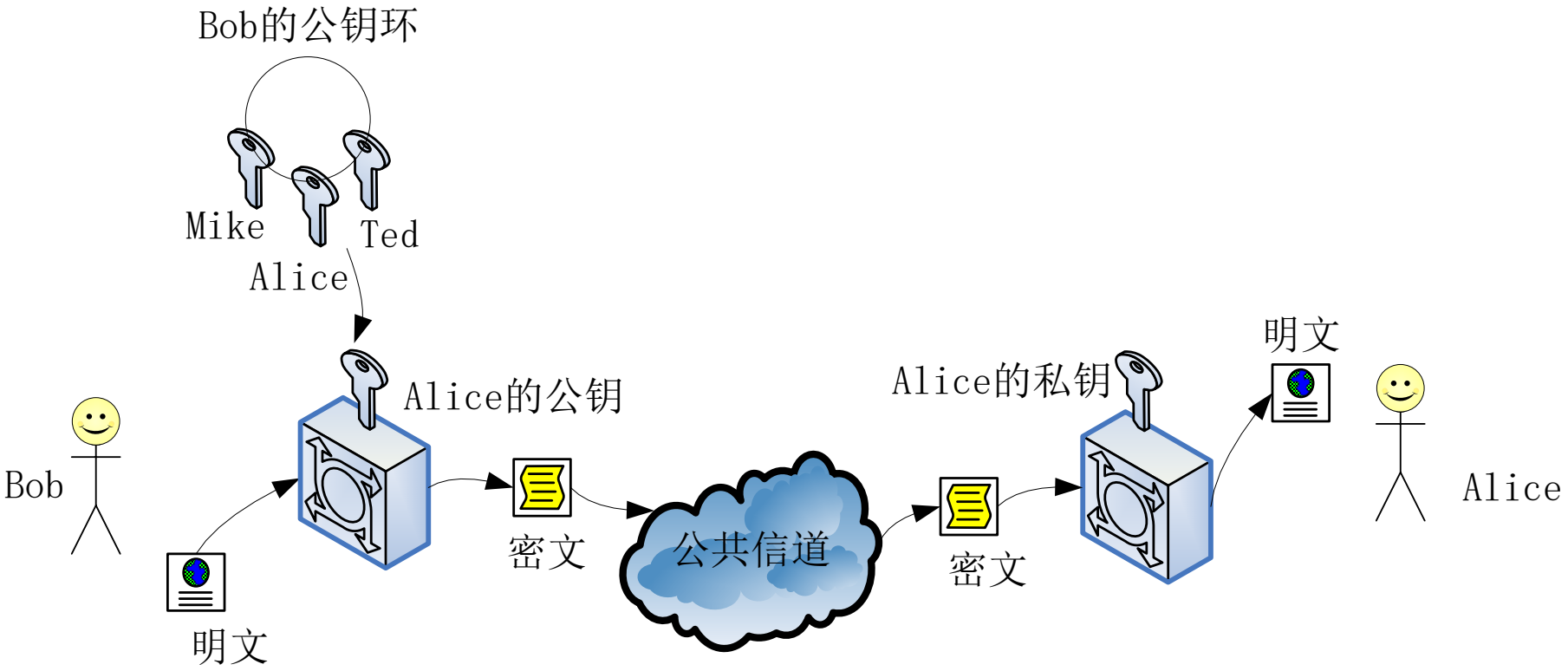
- 公开密钥密码是1976年由Whitfield Diffie和Martin Hellman在其“密码学新方向”一文中提出的。
- 单向陷门函数f(x)，必须满足以下三个条件。

① 给定x，计算y=f(x)是容易的；

② 给定y, 计算x使y=f(x)是困难的（所谓计算$x=f^{-1}(y)$困难是指计算上相当复杂已无实际意义）；

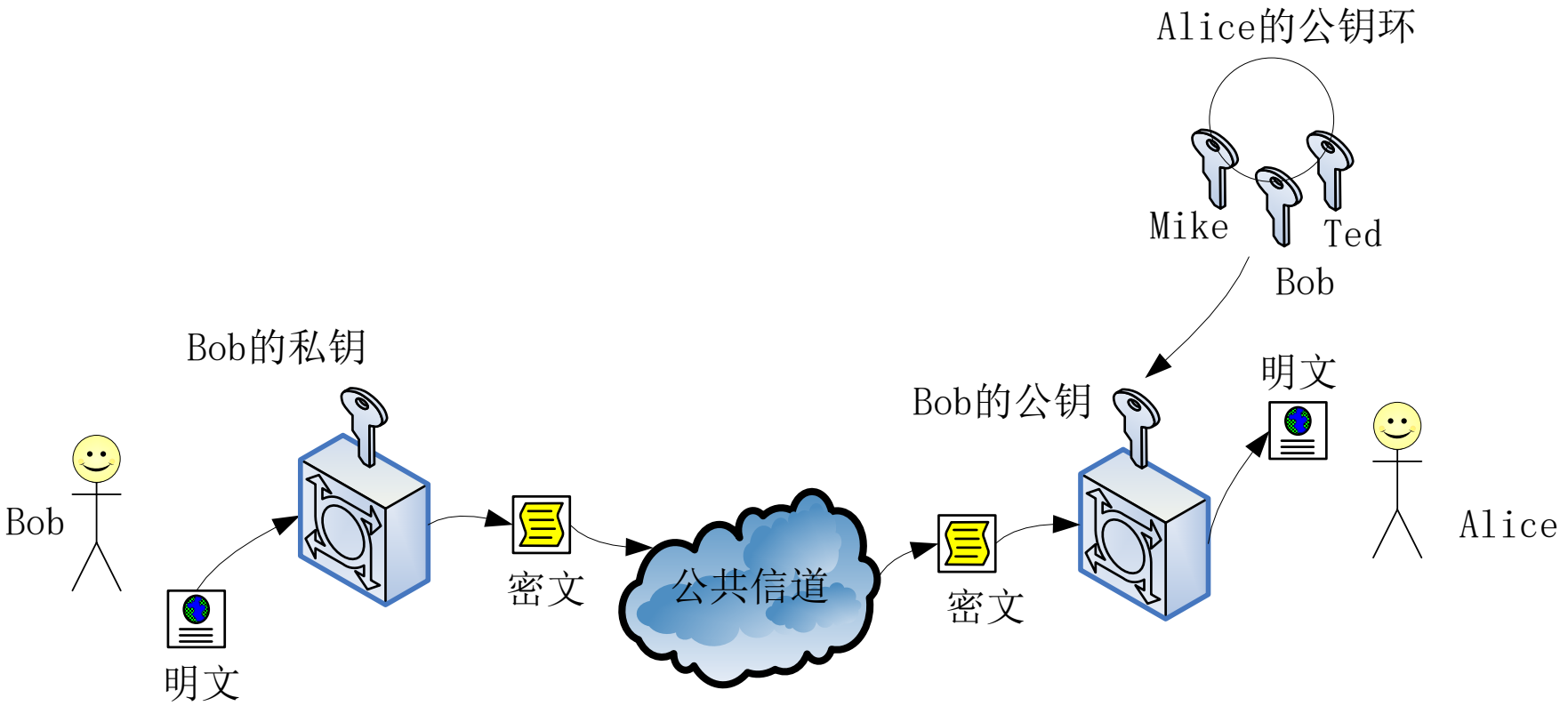
③ 存在δ，已知δ时对给定的任何y，若相应的x存在，则计算x使y=f(x)是容易的。

公开密钥的应用：加密模型



公开密钥密码的加密模型

公开密钥的应用：认证模型



公开密钥密码的认证模型

2.4.2 Diffie-Hellman密钥交换算法

- 数学知识
  - 原根
    - 素数p的原根（primitive root）的定义：如果a是素数p的原根，则数$a \bmod p, a^2 \bmod p, \ldots, a^{p-1} \bmod p$是不同的并且包含从1到p-1之间的所有整数的某种排列。对任意的整数b，可以找到唯一的幂i，满足$b \equiv a^i \bmod p$，且$1 \le i \le p-1$。
  - 注：“$b \equiv a \bmod p$”等价于“$b \bmod p = a \bmod p$”，称为“b与a模p同余”。

– 离散对数

- 若a是素数p的一个原根，则相对于任意整数b（b mod p≠0），必然存在唯一的整数i（1≤i≤p-1），使得$b \equiv a^i \bmod p$，i称为b的以a为基数且模p的幂指数，即离散对数。
- 对于函数$y \equiv g^x \bmod p$，其中，g为素数p的原根，y与x均为正整数，已知g、x、p，计算y是容易的；而已知y、g、p，计算x是困难的，即求解y的离散对数x。
- 注：离散对数的求解为数学界公认的困难问题。

Diffie-Hellman密钥交换算法

- Alice和Bob协商好一个大素数p，和大的整数g，1<g<p，g是p的原根。p和g无须保密，可为网络上的所有用户共享。当Alice和Bob要进行保密通信时，他们可以按如下步骤来做：
  ① Alice选取大的随机数x<p，并计算$Y=g^x \pmod P$；
  ② Bob选取大的随机数x′<p，并计算$Y'=g^{x'} \pmod P$；
  ③ Alice将Y传送给Bob，Bob将Y′传送给Alice；
  ④ Alice计算$K=(Y')^x \pmod P$，Bob计算$K'=(Y)^{x'} \pmod P$
- 显而易见$K=K'=g^{xx'} \pmod P$，即Alice和Bob已获得了相同的秘密值K。

2.4.3 RSA公开密钥算法

- 欧拉定理
  - 欧拉函数是欧拉定理的核心概念，其表述：对于一个正整数n，由小于n且和n互素的正整数构成的集合为Z_n，这个集合被称为n的完全余数集合。Z_n包含的元素个数记做$\phi(n)$，称为欧拉函数，其中$\phi(1)$被定义为1，但是并没有任何实质的意义。
  - 如果两个素数p和q，且$n = p \times q$，则$\phi(n) =(p-1)(q-1)$;
  - 欧拉定理的具体表述：正整数a与n互素，则$a^{\phi(n)} \equiv 1 \bmod n$。
- 推论：
  - 给定两个素数p和q，以及两个整数m、n，使得$n = p \times q$，且$0<m<n$，对于任意整数k下列关系成立，$\mathbf{m^{k\phi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n}$。

大整数因子分解

- 大整数因子分解问题：
  - 已知p、q为两个大素数，则求N=p×q是容易的，只需要一次乘法运算；但已知N是两个大素数的乘积，要求将N分解，则在计算上是困难的，其运行时间复杂程度接近于不可行。
- 算法时间复杂性：
  - 如果输入规模为n时，一个算法的运行时间复杂度为O(n)，称此算法为线性的；
  - 运行时间复杂度为$O(n^k)$，其中k为常量，称此算法为多项式的；
  - 若有某常量t和多项式h(n)，使算法的运行时间复杂度为$O(t^{h(n)})$，则称此算法为指数的。
- 一般说来，
  - 在线性时间和多项式时间内被认为是可解决的，比多项式时间更坏的，尤其是指数时间被认为是不可解决的。
  - 注：如果输入规模太小，即使很复杂的算法也会变得可行的。

RSA密码算法

- RSA密码体制：
  - 明文和密文均是0到n之间的整数，n通常为1024位二进制数或309位十进制数，
  - 明文空间P=密文空间C={x∈Z|0<x< n,Z为整数集合}。
- RSA密码的密钥生成具体步骤如下：

  ① 选择互异的素数p和q，计算n=pq，$\varphi(n) = (p - 1)(q - 1)$；

  ② 选择整数e，使$\gcd(\varphi(n),e) = 1$，且$1 < e < \varphi(n)$；

  ③ 计算d，$d \equiv e^{-1} \bmod \varphi(n)$，即d为模$\varphi(n)$下e的乘法逆元；
- 公钥Pk = { e, n }，私钥Sk = { d, n, p, q }
- 加密：$c = m^e \bmod n$；解密：$m = c^d \bmod n$。

RSA例

- p=101，q＝113，n=11413，φ(n)=100×112＝11200。
- e = 3533，求得$d \equiv e^{-1} \bmod 11200 \equiv 6597 \bmod 11200$，d = 6597。
- 公开n=11413和e=3533，
- 明文9726，计算$9726^{3533} \bmod 11413 = 5761$，发送密文5761。
- 密文5761时，用d＝6597进行解密，计算5761^{6597}（mod 11413)=9726。

RSA的安全性

- RSA是基于单向函数$e_k(x)=x^e(\mod n)$，求逆计算不可行。
- 解密的关键是了解陷门信息，即能够分解n=pq，知道φ(n)=(p-1)(q-1)，从而解出解密私钥d。
- 如果要求RSA是安全的，p与q必为足够大的素数;使分析者没有办法在多项式时间内将n分解出来。
- 模n的求幂运算
  - 著名的“平方-和-乘法”方法将计算$x^c \mod n$的模乘法的次数缩小到至多为2*l*，*l*是指数c二进制表示的位数。

2.4.4 其他公开密钥密码简介

- 基于大整数因子分解问题:
  - RSA密码、Rabin密码
- 基于有限域上的离散对数问题：
  - Differ-Hellman公钥交换体制、ElGamal密码
- 基于椭圆曲线上的离散对数问题：
  - Differ-Hellman公钥交换体制、ElGamal密码。

2.5 消息认证

- 2.5.1概述
  - 威胁信息完整性的行为主要包括：
    - 伪造：假冒他人的信息源向网络中发布消息；
    - 内容修改：对消息的内容进行插入、删除、变换和修改；
    - 顺序修改：对消息进行插入、删除或重组消息序列；
    - 时间修改：针对网络中的消息，实施延迟或重放；
    - 否认：接受者否认收到消息，发送者否认发送过消息。
  - 消息认证是保证信息完整性的重要措施
    - 其目的主要包括：
      - 证明：消息的信源和信宿的真实性；
      - 证明：消息内容是否曾受到偶然或有意的篡改，
      - 证明：消息的序号和时间性是否正确。

– 消息认证由具有认证功能的函数来实现的

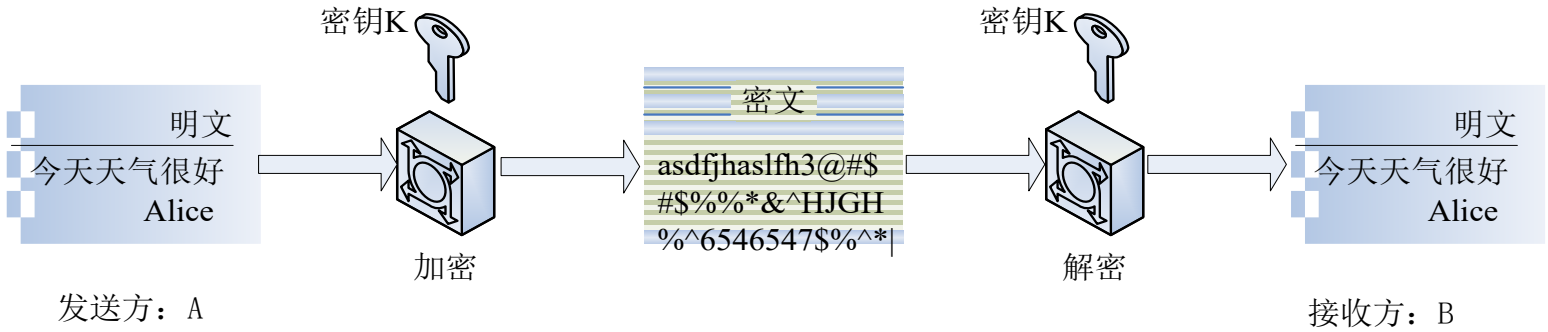
- 消息加密，用消息的完整密文作为消息的认证符；
- 消息认证码MAC（Message Authentication Code），也称密码校验和，使用密码对消息加密，生成固定长度的认证符；
- 消息编码，是针对信源消息的编码函数，使用编码抵抗针对消息的攻击。

2.5.2 认证函数

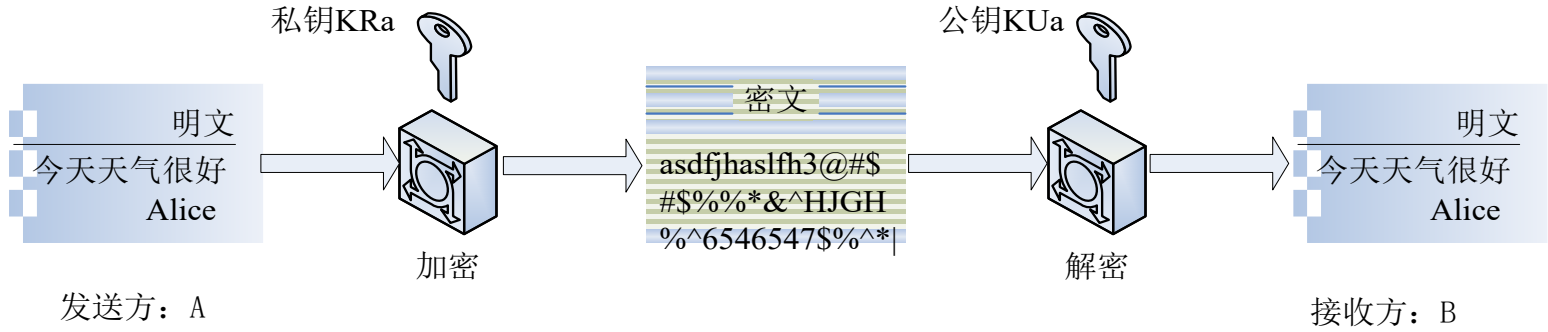
- 认证技术在功能上可以分为两层
  - 下层包含一个产生认证符的函数，认证符是一个用来认证消息的值；
  - 上层是以认证函数为原语，接收方可以通过认证函数来验证消息的真伪。

一、消息加密函数

- 对称密钥密码对消息加密，不仅具有机密性，同时也具有一定的可认证性;
- 公开密钥密码本身就提供认证功能，其具有的私钥加密、公钥解密以及反之亦然的特性;



（a）对称密钥密码：加密和认证



（b）公开密钥密码：认证

二、消息认证码

- 消息认证码MAC的基本思想：
  - 利用事先约定的密码，加密生成一个固定长度的短数据块MAC，并将MAC附加到消息之后，一起发送给接收者；
  - 接收者使用相同密码对消息原文进行加密得到新的MAC，比较新的MAC和随消息一同发来的MAC，如果相同则未受到篡改。

- 生成消息认证码的方法：
  - 基于加密函数的认证码和消息摘要（在散列函数中讨论）。
  - 消息认证符可以是整个64位的O_n，也可以是O_n最左边的M位

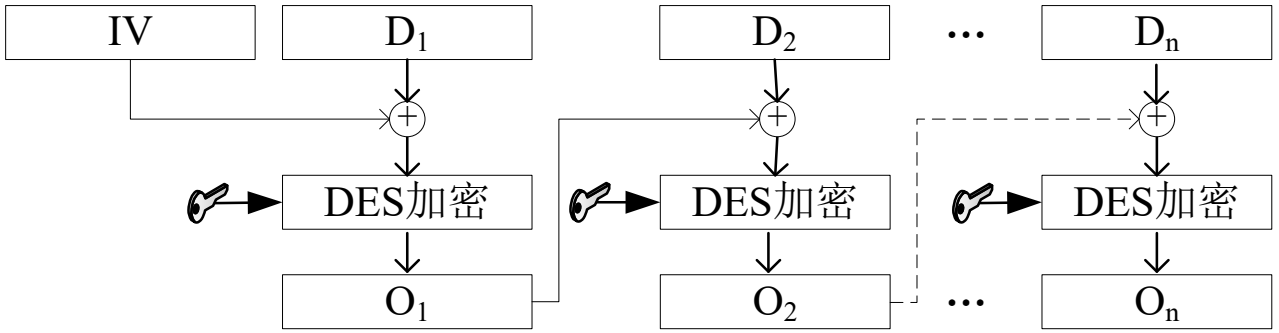


图2.19 基于DES的消息认证码

三、消息编码

- 消息编码认证的基本思想：
  - 引入冗余度，使通过信道传送的可能序列集M（编码集）大于消息集S（信源集）。
  - 发送方从M中选出用来代表消息的许用序列L_i，即对信息进行编码；
  - 接收方根据编码规则，进行解码，还原出发送方按此规则向他传来的消息。
  - 窜扰者不知道被选定的编码规则，因而所伪造的假码字多是M中的禁用序列，接收方将以很高的概率将其检测出来，并拒绝通过认证。

- 如果决定采用L_0，则以发送消息“00”代表信源“0”，发送消息“10”代表信源“1”。在子规则L_0下，消息“00”和“10”是合法的，而消息“01”和“11”在L_0之下不合法，收方将拒收这两个消息。

信源S / 编码 法则L	0	1	禁用序列
L_0	00	10	01，11
L_1	00	11	01，10
L_2	01	10	00，11
L_3	01	11	00，10

2.5.3 散列函数

- **散列函数（Hash Function）的目的**
  - 将任意长的消息映射成一个固定长度的散列值（hash值），也称为消息摘要。消息摘要可以作为认证符，完成消息认证。
- **散列函数的健壮性**
  - **弱无碰撞特性**
    - 散列函数h被称为是弱无碰撞的，是指在消息特定的明文空间X中，给定消息$x \in X$，在计算上几乎找不到不同于x的x'，$x' \in X$，使得$h(x)=h(x')$。
  - **强无碰撞特性**
    - 散列函数h被称为是强无碰撞的，是指在计算上难以找到与x相异的x'，满足$h(x)=h(x')$，x'可以不属于X。
  - **单向性**
    - 散列函数h被称为单向的，是指通过h的逆函数h^{-1}来求得散列值$h(x)$的消息原文x，在计算上不可行。

散列值的安全长度

- “生日悖论”
  - 如果一个房间里有23个或23个以上的人，那么至少有两个人的生日相同的概率要大于50%。对于60或者更多的人，这种概率要大于99%。
  - 不计特殊的闰年，计算房间里所有人的生日都不相同的概率，

① 第一个人不发生生日冲突的概率是 $\frac{365}{365}$ ，

② 第二个人不发生生日冲突的概率是 $1-\frac{1}{365}$ ，…，

③ 第n个人是 $1-\frac{n-1}{365}$ ，

④ 所有人生日都不冲突的概率是：

① E=1×($1-\frac{1}{365}$)×…×($1-\frac{n-2}{365}$)×($1-\frac{n-1}{365}$)，

⑤ 而发生冲突的概率P=1-E，当n=23时，P≈0.507；n=100时，P≈0.9999996。

散列值的安全长度

- 生日悖论对于散列函数的意义
  - n位长度的散列值，可能发生一次碰撞的测试次数不是2^n次，而是大约$2^{n/2}$次。
  - 一个40位的散列值将是不安全的，因为大约100万个随机散列值中将找到一个碰撞的概率为50%，
  - 消息摘要的长度不低于为128位。

MD5

- 1991年Rivest对MD4的进行改进升级，提出了MD5（Message Digest Algorithm 5）。
- MD5具有更高的安全性，目前被广泛使用。

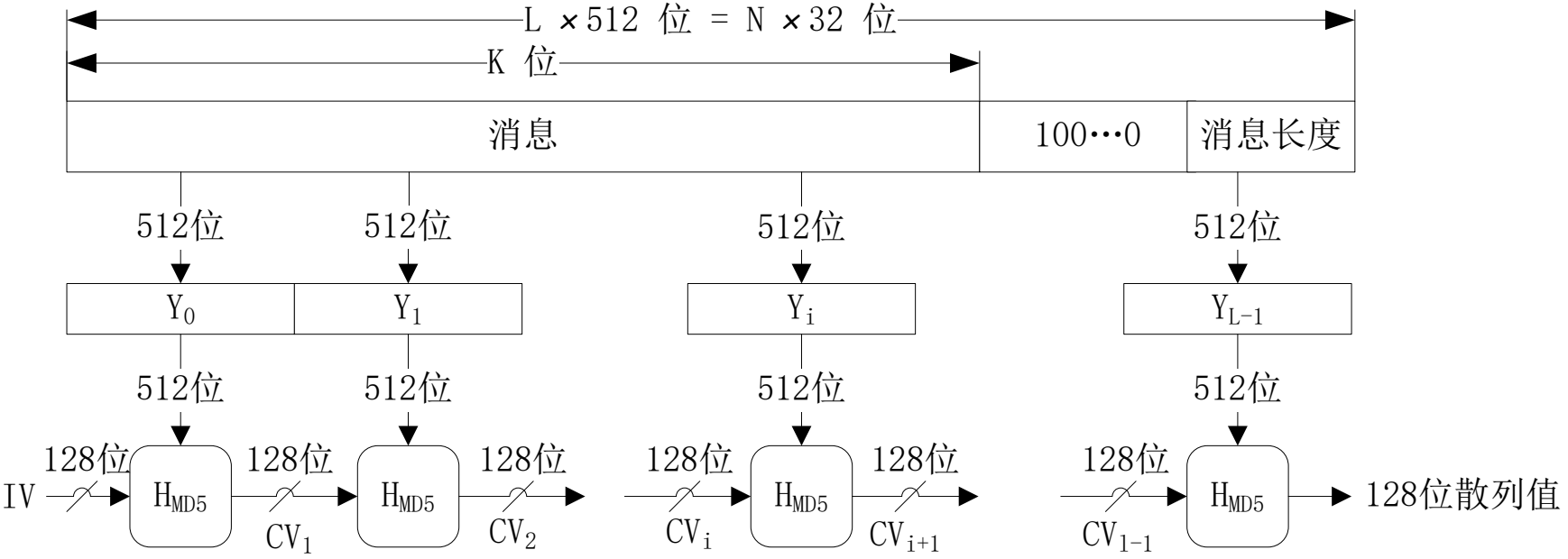
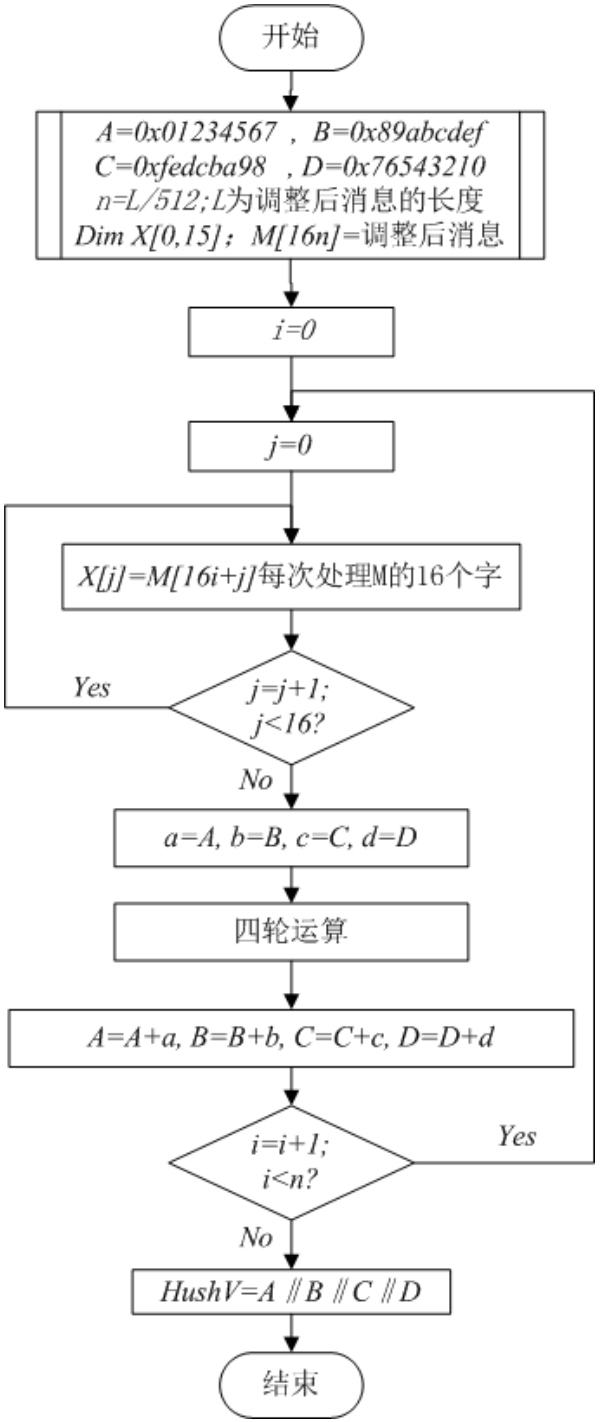


图2.20 MD5算法

MD5

- 四轮运算涉及四个函数：
  - E（X，Y，Z）=（X ∧ Y）∨（（¬X）∧ Z）
  - F（X，Y，Z）=（X ∧ Z）∨（Y ∧（¬Z））
  - G（X，Y，Z）= X ⊕ Y ⊕ Z
  - H（X，Y，Z）= Y ⊕（X ∨（¬Z））
- 四轮运算：
  - EE(a,b,c,d,M_j,s,t_i)： a = b + ((a+(E(b,c,d)+M_j+t_i)<<s)；
  - FF(a,b,c,d,M_j,s,t_i)： a = b + ((a+(F(b,c,d)+ M_j + t_i)<<s)；
  - GG(a,b,c,d,M_j,s,t_i) ： a = b + ((a+(G(b,c,d)+ M_j + t_i)<<s)；
  - HH(a,b,c,d, M_j,s,t_i) ： a = b + ((a+(H(b,c,d)+ M_j + t_i)<<s)；
- 得到常数t_i的计算方法是：
  - 整个四轮操作总共分为64步，在第i步中t_i是2^{32}×abs(sin(i))的整数部分，i的单位是弧度



第一轮

- EE(a,b,c,d,M_j,s,t_i)： a = b + ((a+(E(b,c,d)+M_j+t_i)<<s)；

(1) EE(a,b,c,d,M_0,7,0xd76aa478) —》 a = b + ((a+(E(b,c,d)+M_0+0xd76aa478)<<7)；
(2) EE(d,a,b,c,M_1,12,0xe8c7b756)
(3) EE(c,d,a,b,M_2,17,0x242070db)
(4) EE(b,c,d,a,M_3,22,0xc1bdceee)
(5) EE(a,b,c,d,M_4,7,0xf57c0faf)
(6) EE(d,a,b,c,M_5,12,0x4787c62a)
(7) EE(c,d,a,b,M_6,17,0xa8304613)
(8) EE(b,c,d,a,M_7,22,0xfd469501)
(9) EE(a,b,c,d,M_8,7,0x698098d8)
(10)EE(d,a,b,c,M_9,12,0x8b44f7af)
(11)EE(c,d,a,b,M_{10},17,0xffff5bb1)
(12)EE(b,c,d,a,M_{11},22,0x895cd7be)
(13)EE(a,b,c,d,M_{12},7,0x6b901122)
(14)EE(d,a,b,c,M_{13},12,0xfd987193)
(15)EE(c,d,a,b,M_{14},17,0xa679438e)
(16)EE(b,c,d,a,M_{15},22,0x49b40821)

第二轮

- FF(a,b,c,d,M_j,s,t_i)： a = b + ((a+(F(b,c,d)+ M_j + t_i)<<s)

(1) FF(a,b,c,d,M_1,5,0xf61e2562) —》 a = b + ((a+(F(b,c,d)+M_1+0xf61e2562)<<5)；
(2) FF(d,a,b,c,M_6,9,0xc040b340)
(3) FF(c,d,a,b,M_{11},14,0x265e5a51)
(4) FF(b,c,d,a,M_0,20,0xe9b6c7aa)
(5) FF(a,b,c,d,M_5,5,0xd62f105d)
(6) FF(d,a,b,c,M_{10},9,0x02441453)
(7) FF(c,d,a,b,M_{15},14,0xd8a1e681)
(8) FF(b,c,d,a,M_4,20,0xe7d3fbc8)
(9) FF(a,b,c,d,M_9,5,0x21e1cde6)
(10)FF(d,a,b,c,M_{14},9,0xc33707d6)
(11)FF(c,d,a,b,M_3,14,0xf4d50d87)
(12)FF(b,c,d,a,M_8,20,0x455a14ed)
(13)FF(a,b,c,d,M_{13},5,0xa9e3e905)
(14)FF(d,a,b,c,M_2,9,0xfcefa3f8)
(15)FF(c,d,a,b,M_7,14,0x676f02d9)
(16)FF(b,c,d,a,M_{12},20,0x8d2a4c8a))

第三轮

- GG(a,b,c,d,M_j,s,t_i)： a = b + ((a+(G(b,c,d)+ M_j + t_i)<<s)；

(1) GG(a,b,c,d,M_5,4,0xEEfa3942) —》 a = b + ((a+(G(b,c,d)+M_5+0xEEfa3942)<<4)；
(2) GG(d,a,b,c,M_8,11,0x8771f681)
(3) GG(c,d,a,b,M_{11},16,0x6d9d6122)
(4) GG(b,c,d,a,M_{14},23,0xfde5380c)
(5) GG(a,b,c,d,M_1,4,0xa4beea44)
(6) GG(d,a,b,c,M_4,11,0x4bdecfa9)
(7) GG(c,d,a,b,M_7,16,0xf6bb4b60)
(8) GG(b,c,d,a,M_{10},23,0xbebfbc70)
(9) GG(a,b,c,d,M_{13},4,0x289b7ec6)
(10)GG(d,a,b,c,M_0,11,0xeaa127fa)
(11)GG(c,d,a,b,M_3,16,0xd4ef3085)
(12)GG(b,c,d,a,M_6,23,0x04881d05)
(13)GG(a,b,c,d,M_9,4,0xd9d4d039)
(14)GG(d,a,b,c,M_{12},11,0xe6db99e5)
(15)GG(c,d,a,b,M_{15},16,0x1fa27cf8)
(16)GG(b,c,d,a,M_2,23,0xc4ac5665)

第四轮

- HH(a,b,c,d, M_j,s,t_i)： a = b + ((a+(H(b,c,d)+ M_j + t_i)<<s)；

(1) HH(a,b,c,d,M_0,6,0xf4292244) —》 a = b + ((a+(H(b,c,d)+M_0+0xf4292244)<<6)；
(2) HH(d,a,b,c,M_7,10,0x432aEE97)
(3) HH(c,d,a,b,M_{14},15,0xab9423a7)
(4) HH(b,c,d,a,M_5,21,0xfc93a039)
(5) HH(a,b,c,d,M_{12},6,0x655b59c3)
(6) HH(d,a,b,c,M_3,10,0x8f0ccc92)
(7) HH(c,d,a,b,M_{10},15,0xEEeEE47d)
(8) HH(b,c,d,a,M_1,21,0x85845dd1)
(9) HH(a,b,c,d,M_8,6,0x6fa87e4f)
(10)HH(d,a,b,c,M_{15},10,0xfe2ce6e0)
(11)HH(c,d,a,b,M_6,15,0xa3014314)
(12)HH(b,c,d,a,M_{13},21,0x4e0811a1)
(13)HH(a,b,c,d,M_4,6,0xf7537e82)
(14)HH(d,a,b,c,M_{11},10,0xbd3af235)
(15)HH(c,d,a,b,M_2,15,0x2ad7d2bb)
(16)HH(b,c,d,a,M_9,21,0xeb86d391)

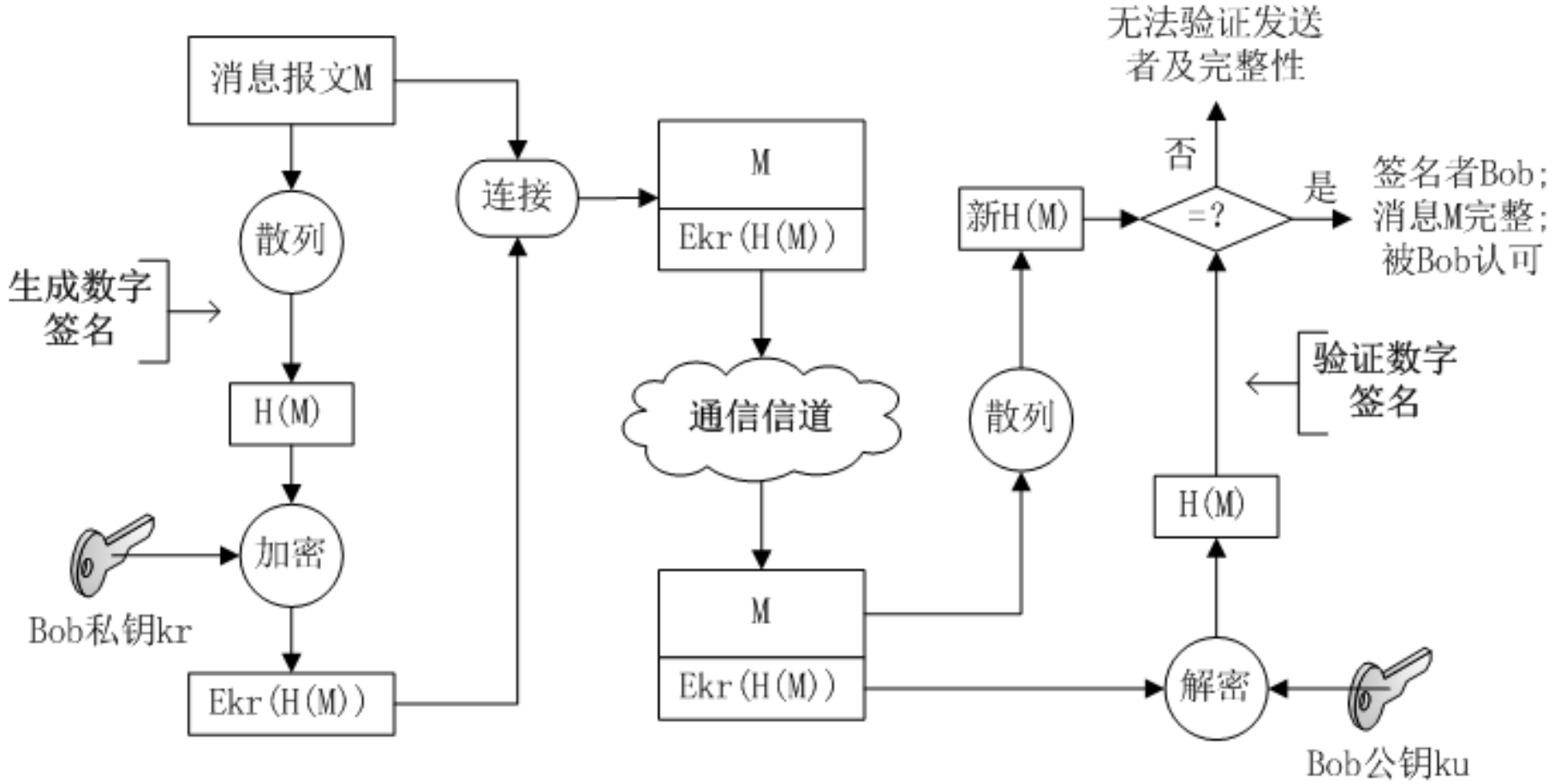
2.5.4 数字签名

- 数字签名： Digital Signature，
- 在ISO7498-2标准定义为
  - “附加在数据单元上的一些数据或是对数据单元所作的密码变换，这种数据或变换可以被数据单元的接收者用来确认数据单元来源和数据单元的完整性，并保护数据不会被人（例如接收者）伪造”。
- 美国电子签名标准对数字签名作了如下解释：
  - “数字签名是利用一套规则和一个参数对数据进行计算所得的结果，用此结果能够确认签名者的身份和数据的完整性”
- 一般来说，数字签名可以被理解为：
  - 通过某种密码运算生成一系列符号及代码，构成可以用来进行数据来源验证的数字信息。

- 从签名形式上分，数字签名有两种
  - 一种是对整个消息的签名，
  - 一种是对压缩消息的签名，
  - 它们都是附加在被签名消息之后或在某一特定位置上的一段数据信息。
- 数字签名主要目的
  - 保证收方能够确认或验证发方的签名，但不能伪造；发方发出签名消息后，不能否认所签发的消息。

- 设计数字签名必须满足下列条件：
  - 签名必须基于一个待签名信息的位串模板；
  - 签名必须使用某些对发送方来说是唯一的信息，以防止双方的伪造与否认；
  - 必须相对容易生成、识别和验证数字签名；
  - 伪造该数字签名在计算复杂性意义上具有不可行性
    - 既包括对一个已有的数字签名构造新的消息，也包括对一个给定消息伪造一个数字签名。

数字签名的生成及验证


消息报文M
散列
生成数字签名
H(M)
加密
Bob私钥kr
Ekr(H(M))
连接
M
Ekr(H(M))
通信信道
M
Ekr(H(M))
散列
新H(M)
无法验证发送者及完整性
否
=?
是
签名者Bob；消息M完整；被Bob认可
验证数字签名
H(M)
解密
Bob公钥ku

2.6 密码学新进展

- 1989年，英国数学家Matthews，基于混沌的加密技术混沌密码学
  - 混沌系统具有良好的伪随机特性、轨道的不可预测性、对初始状态及控制参数的敏感性等一系列特性，
  - 传统的密码算法敏感性依赖于密钥，而混沌映射依赖于初始条件和映射中的参数；
  - 传统的加密算法通过加密轮次来达到扰乱和扩散，混沌映射则通过迭代，将初始域扩散到整个相空间；
  - 传统加密算法定义在有限集上，而混沌映射定义在实数域内。

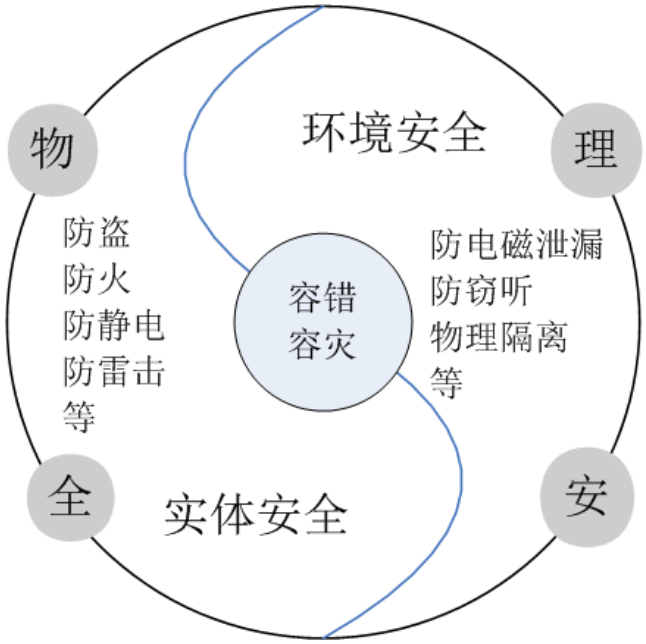
- 量子密码
  - 1970年威斯纳提出利用单量子态制造不可伪造的“电子钞票”，这个构想由于量子态的寿命太短而无法实现，
  - 1984年，IBM的贝内特和加拿大学者布拉萨德提出了第一个量子密码方案，由此迎来了量子密码学的新时期。
  - 量子密码体系采用量子态作为信息载体，经由量子通道在合法的用户之间传送密钥。
  - 量子密码的安全性由量子力学原理所保证，被称为是绝对安全的。
  - 所谓绝对安全是指即使在窃听者可能拥有极高的智商、可能采用最高明的窃听措施、可能使用最先进的测量手段，密钥的传送仍然是安全的，可见量子密码研究具有极其重大的意义。

- DNA计算
  - 1994年，Adleman等科学家进行了世界上首次DNA计算，解决了一个7节点有向汉密尔顿回路问题。
  - 由于DNA计算具有的信息处理的高并行性、超高容量的存储密度和超低的能量消耗等特点，非常适合用于攻击密码计算系统的不同部分，对传统的基于计算安全的密码体制提出了挑战。

第3章 物理安全

翟健宏

3.1 概述



- 物理安全:实体安全和环境安全
- 解决两个方面问题:
  - 对信息系统实体的保护;
  - 对可能造成信息泄漏的物理问题进行防范。
- 物理安全技术包括:
  - 防盗、防火、防静电、防雷击、防信息泄漏、物理隔离;
  - 基于物理环境的容灾技术和物理隔离技术也属于物理安全技术范畴。
- 物理安全是信息安全的必要前提
  - 如果不能保证信息系统的物理安全，其他一切安全内容均没有意义。

3.2 设备安全防护

3.2.1 防盗

- 计算机也是偷窃者的目标，计算机偷窃行为所造成的损失可能远远超过计算机本身的价值，
- （1）安全保护设备
  - 有源红外报警器、无源红外报警器和微波报警器等；
  - 计算机系统是否安装报警系统，安装什么样的报警系统，要根据系统的安全等级及计算机中心信息与设备的重要性来确定。
- （2）防盗技术
  - 在计算机系统和外部设备上加无法去除的标识；
  - 使用一种防盗接线板，一旦有人拔电源插头，就会报警；
  - 可以利用火灾报警系统，增加防盗报警功能；
  - 利用闭路电视系统对计算机中心的各部位进行监视保护等。

3.2.2 防火

- 火灾因素：
  - 电气原因、人为因素或外部火灾蔓延引起的
- 计算机机房的主要防火措施如下：
  - 计算机中心选址
  - 建筑物的耐火等级
  - 不间断供电系统或自备供电系统
  - 防雷设施与抗静电地板
  - 严禁存放腐蚀性物品和易燃易爆物品
  - 禁止吸烟和随意动火

3.2.3 防静电

- 静电产生：接触→电荷→转移→偶电层形成→电荷分离。
- 静电是一种电能，具有高电位、低电量、小电流和作用时间短的特点。
- 静电放电火花造成火灾，还能使大规模集成电损坏，这种损坏可能是不知不觉造成的。
- 静电防范：
  - 静电的泄漏和耗散、静电中和、静电屏蔽与接地、增湿等。防范静电的基本原则是“抑制或减少静电荷的产生，严格控制静电源”。

3.2.4 防雷击

- 雷电防范的主要措施是：
  - 根据电气及微电子设备的不同功能及不同受保护程序和所属保护层来确定防护要点做分类保护。
- 常见的防范措施主要包括：
  - 接闪
    - 让闪电能量按照人们设计的通道泄放到大地中去。
  - 接地
    - 让已经纳入防雷系统的闪电能量泄放入大地。
  - 分流
    - 一切从室外来的导线与接地线之间并联一种适当的避雷器，将闪电电流分流入地。
  - 屏蔽
    - 屏蔽就是用金属网、箔、壳、管等导体把需要保护的对象包围起来，阻隔闪电的脉冲电磁场从空间入侵的通道。

3.3 防信息泄露

3.3.1 电磁泄露

- 电磁干扰EMI（Electro Magnetic Interference）
  - 是指一切与有用信号无关的、不希望有的或对电器及电子设备产生不良影响的电磁发射。
- 防止EMI要从两个方面来考虑，
  - 减少电子设备的电磁发射；
  - 提高电子设备的电磁兼容性EMC。
- 电磁兼容性EMC（Electro Magnetic Compatibility）
  - 电子设备在自己正常工作时产生的电磁环境，与其它电子设备之间相互不影响的电磁特性。

TEMPEST

- TEMPEST技术（Transient Electromagnetic Pulse Emanation Standard）
  - 计算机信息泄漏安全防护技术，是一项综合性的技术，包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等项技术，涉及到多个学科领域。
  - 通常我们把输入、输出的信息数据信号及它们的变换称为核心红信号。
  - 那些可以造成核心红信号泄密的控制信号称为关键红信号，红信号的传输通道或单元电路称为红区。
  - 所谓的“TEMPEST”要解决的问题就是防止红信号发生电磁信息泄漏。

防电磁信息泄漏

- 主要包括三个层面，
  - 一是抑制电磁发射，采取各种措施减小“红区”电路电磁发射；
  - 二是屏蔽隔离，在其周围利用各种屏蔽材料使红信号电磁发射场衰减到足够小，使其不易被接收，甚至接收不到；
  - 三是相关干扰，采取各种措施使相关电磁发射泄漏即使被接收到也无法识别。

常用的防电磁泄漏的方法

- 屏蔽法（即空域法）
  - 屏蔽法主要用来屏蔽辐射及干扰信号。采用各种屏蔽材料和结构，合理地将辐射电磁场与接收器隔离开，使辐射电磁场在到达接收器时强度降低到最低限度，从而达到控制辐射的目的。
  - 空域防护是对空间辐射电磁场控制的最有效和最基本的方法，机房屏蔽室就是这种方法的典型例子。

- 频域法
  - 频域法主要解决正常的电磁发射受干扰问题。不论是辐射电磁场，还是传导的干扰电压和电流都具有一定的频谱，即由一定的频率成分组成。
  - 通过频域控制的方法来抑制电磁干扰辐射的影响，即利用系统的频率特性将需要的频率成分(信号、电源的工作交流频率)加以接收，而将干扰的频率加以剔除。
  - 频域法就是利用要接收的信号与干扰所占有的频域不同，对频域进行控制。

- 时域法
  - 与频域法相似，时域法也是用来回避干扰信号。
  - 当干扰非常强，不易受抑制、但又在一定时间内阵发存在时，通常采用时间回避方法，即信号的传输在时间上避开干扰。

3.3.2 窃听

- 窃听是指通过非法的手段获取未经授权的信息。
- 窃听技术
  - 指窃听行动所使用的窃听设备和窃听方法的总称。
- 防窃听
  - 指搜索发现窃听装置及对原始信息进行特殊处理，以达到消除窃听行为或使窃听者无法获得特定原始信息。
- 防窃听技术
  - 检测主要指主动检查是否存在窃听器，可以采用电缆加压技术、电磁辐射检测技术以及激光探测技术等；
  - 防御主要是采用基于密码编码技术对原始信息进行加密处理，确保信息即使被截获也无法还原出原始信息，另外电磁信号屏蔽也属于窃听防御技术。

3.4 物理隔离

- **3.4.1 物理隔离的理解**
  - 较早时描述的单词Physical Disconnection
  - 后来Physical Separation和Physical Isolation
  - 目前开始使用Physical Gap这个词汇，直译为物理隔离，意为通过制造物理的豁口，来达到物理隔离的目的。

对物理隔离的理解表现:

（1）阻断网络的直接连接

（2）阻断网络的Internet逻辑连接

（3）隔离设备的传输机制具有不可编程的特性

（4）任何数据都是通过两级移动代理的方式来完成，两级移动代理之间是物理隔离的。

（5）隔离设备具有审查的功能。

（6）隔离设备传输的原始数据，不具有攻击或对网络安全有害的特性

（7）强大的管理和控制功能。

（8）从隔离的内容看，隔离分为网络隔离和数据隔离。

3.4.2物理隔离与逻辑隔离

- 物理隔离与逻辑隔离有很大的区别，
  - 物理隔离的哲学是不安全就不连网,要绝对保证安全；
    - 物理隔离部件的安全功能应保证被隔离的计算机资源不能被访问（至少应包括硬盘、软盘和光盘），计算机数据不能被重用（至少应包括内存）。
  - 逻辑隔离的哲学是在保证网络正常使用下,尽可能安全
    - 逻辑隔离部件的安全功能应保证被隔离的计算机资源不能被访问，只能进行隔离器内外的原始应用数据交换。

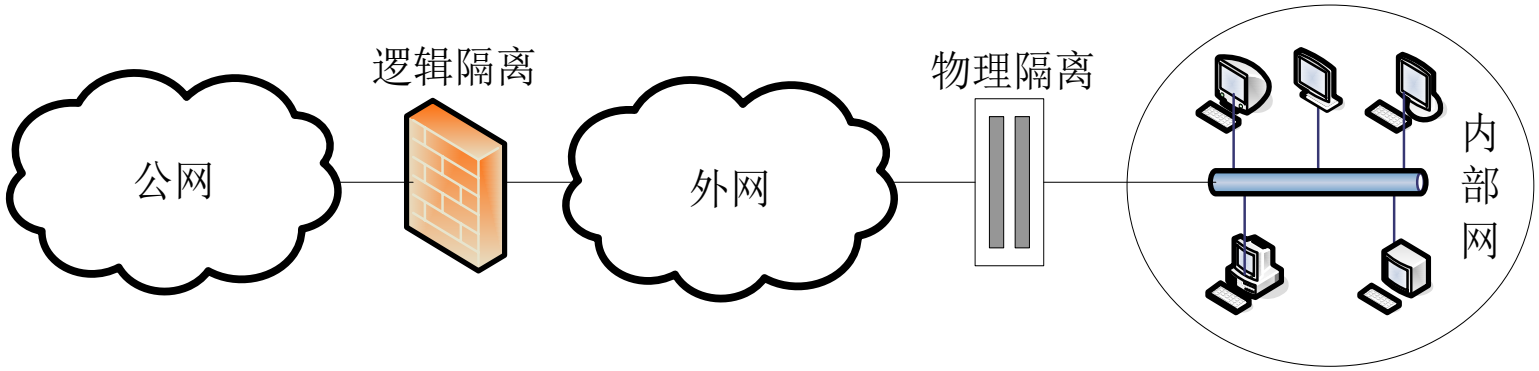


图3.2 企业网络的划分

3.4.3 网络物理隔离的基本形式

① 内外网络无连接，内网与外网之间任何时刻均不存在连接，是最安全的物理隔离形式。

② 客户端物理隔离，采用隔离卡使一台计算机既连接内网又连接外网，可以在不同网络上分时地工作，在保证内外网络隔离的同时节省资源、方便工作。

③ 网络设备端物理隔离，在网络设备处的物理隔离常常要与客户端的物理隔离相结合，它可以使客户端通过一条网线由远端切换器连接双网，实现一台工作站连接两个网络的目的。

④ 服务器端物理隔离，实现在服务器端的数据过滤和传输，使内外网之间同一时刻没有连线，能快速、分时地传递数据。

3.5 容错与容灾

3.5.1 容错

- 保证系统可靠性的三条途径
  - 避错是完善设计和制造，试图构造一个不会发生故障的系统，但这是不太现实的
  - 纠错做为避错的补充。一旦出现故障，可以通过检测、排除等方法来消除故障，再进行系统的恢复。
  - 容错是第三条途径。其基本思想是即使出现了错误，系统也可以执行一组规定的程序；

容错系统

① 高可用度系统：可用度用系统在某时刻可以运行的概率衡量。高可用度系统面向通用计算机系统，用于执行各种无法预测的用户程序，主要面向商业市场。

② 长寿命系统：长寿命系统在其生命期中不能进行人工维修，常用于航天系统。

③ 延迟维修系统：延迟维修系统也是一种容灾系统，用于航天、航空等领域，要求满足在一定阶段内不进行维修仍可保持运行。

④ 高性能系统：高性能系统对于故障（瞬间或永久）都非常敏感，因此应当具有瞬间故障的自动恢复能力，并且增加平均无故障时间。

⑤ 关键任务系统：关键任务系统出错可能危及人的生命或造成重大经济损失，要求处理正确无误，而且恢复故障时间要最短。

常用的数据容错技术

① 空闲设备：也称双件热备，就是备份两套相同的部件。当正常运行的部件出现故障时，原来空闲的一台立即替补。

② 镜像：镜像是把一份工作交给两个相同的部件同时执行，这样在一个部件出现故障时，另一个部件继续工作。

③ 复现：复现也称延迟镜像，与镜像一样需要两个系统，但是它把一个系统称为原系统，另一个成为辅助系统。辅助系统从原系统中接收数据，与原系统中的数据相比，辅助系统接收数据存在着一定延迟。

④ 负载均衡：负载均衡是指将一个任务分解成多个子任务，分配给不同的服务器执行，通过减少每个部件的工作量，增加系统的稳定性。

3.5.2 容灾

- 容灾的含义是对偶然事故的预防和恢复。
- 解决方案有两类
  - 对服务的维护和恢复；
  - 保护或恢复丢失的、被破坏的或被删除的信息。
- 灾难恢复策略
  （1）做最坏的打算
  （2）充分利用现有资源
  （3）既重视灾后恢复，也注意灾前措施
- 数据和系统的备份和还原
  - 是事故恢复能力的重要组成，
  - 数据备份越新、系统备份越完整的机构部门就越容易实现灾难恢复操作。

第4章 身份认证

翟健宏

4.1 概述

- 问题的提出
- 什么是身份认证？
  - 身份认证是证实用户的真实身份与其所声称的身份是否相符的过程。
  - 身份认证的依据应包含只有该用户所特有的、并可以验证的特定信息。
    - 用户所知道的或所掌握的信息（Something the user know），如密码、口令等；（基于口令的认证技术）
    - 用户所拥有的特定东西（Something the user possesses），如身份证、护照、密钥盘等；（基于密码学的认证技术）
    - 用户所具有的个人特征（Something the user is or How he behaves），如指纹、笔迹、声纹、虹膜、DNA等。（生物特征的认证技术）

身份认证的分类

- 根据认证条件的数目分类
  - 仅通过一个条件的相符合来证明一个人的身份，称之为单因子认证；
  - 通过两种不同条件来证明一个人的身份，称之为双因子认证；
  - 通过组合多种不同条件来证明一个人的身份，称之为多因子认证。
- 根据认证数据的状态来看，
  - **静态数据认证**:指用于识别用户身份的认证数据事先已产生并保存在特定的存储介质上；
  - **动态数据认证**:指用于识别用户身份的认证数据不断动态变化，每次认证使用不同的认证数据，即动态密码。

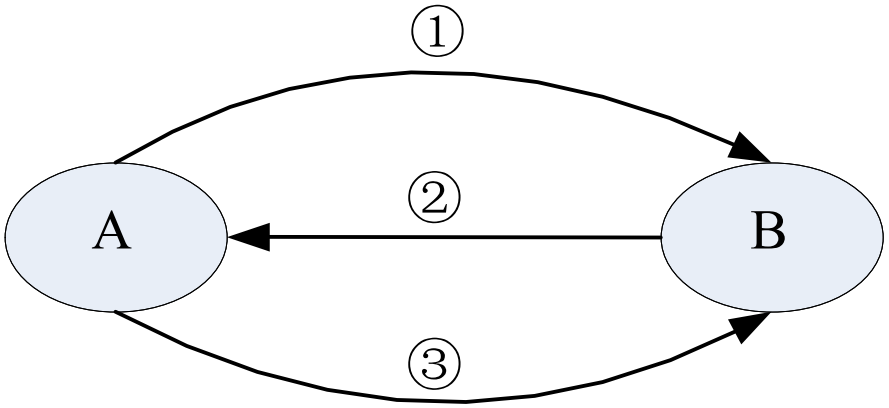
4.2 认证协议

- 以网络为背景的认证技术的核心基础是密码学，对称密码和公开密码是实现用户身份识别的主要技术。
- 实现认证必须要求示证方和验证方遵循一个特定的规则来实施认证，这个规则被称为认证协议。
- 认证过程的安全取决于认证协议的完整性和健壮性。

4.2.1 基于对称密钥的认证协议

- 基于对称密码体制下的认证
  - 示证方和验证方共享密钥，通过共享密钥来维系彼此的信任关系，实际上认证就是建立某种信任关系的过程。
  - 在只有少量用户的封闭式网络系统中，各用户之间的双人共享密钥的数量有限，可以采用挑战-应答方式来实现认证；
  - 对于规模较大的网络系统，一般采用密钥服务器的方式来实现认证，即依靠可信的第三方完成认证。

基于挑战-应答方式的认证协议



① A ⟶ B：IDa ‖ IDb

② B ⟶ A：Nb

③ A ⟶ B：$E_k(Nb)$

Needham-Schroeder认证协议

- 所有的使用者共同信任一个公正的第三方，此第三方被称为认证服务。
- 每个使用者需要在认证服务器AS(Authentication Server)上完成注册，
- AS保存每一个用户的信息并与每一个用户共享一个对称密钥。

Needham-Schroeder 协议描述

① A → KDC： $ID_A \| ID_B \| N_1$ ；

- A通知KDC要与B进行安全通信，N_1为临时值。

② KDC → A： EKa[Ks ‖ IDB ‖ N1 ‖ EKb[Ks ‖ IDA]] ；

③ A → B： EKb[Ks ‖ IDA] ；

- A转发KDC给B的内容。

④ B → A： EKs[N2] ；

- B用Ks加密挑战值N_2，发给A并等待A的回应认证信息。

⑤ A → B： EKs[f(N2)] ；

- A还原N_2后，根据事先的约定f(x)，计算$f(N_2)$，使用Ks加密后，回应B的挑战，完成认证，随后A和B使用Ks进行加密通讯。

Needham-Schroeder协议的漏洞

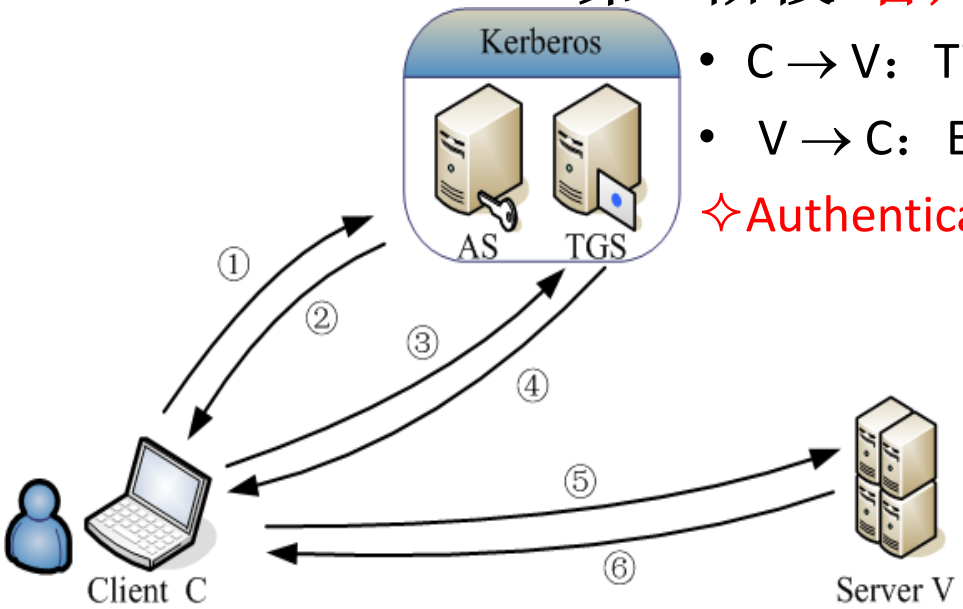
- 攻击方C已经掌握A和B之间通信的一个老的会话密钥
- C可以在第3步冒充A利用老的会话密钥欺骗B
  - 除非B记住所有以前使用的与A通信的会话密钥，否则B无法判断这是一个重放攻击。

Kerberos

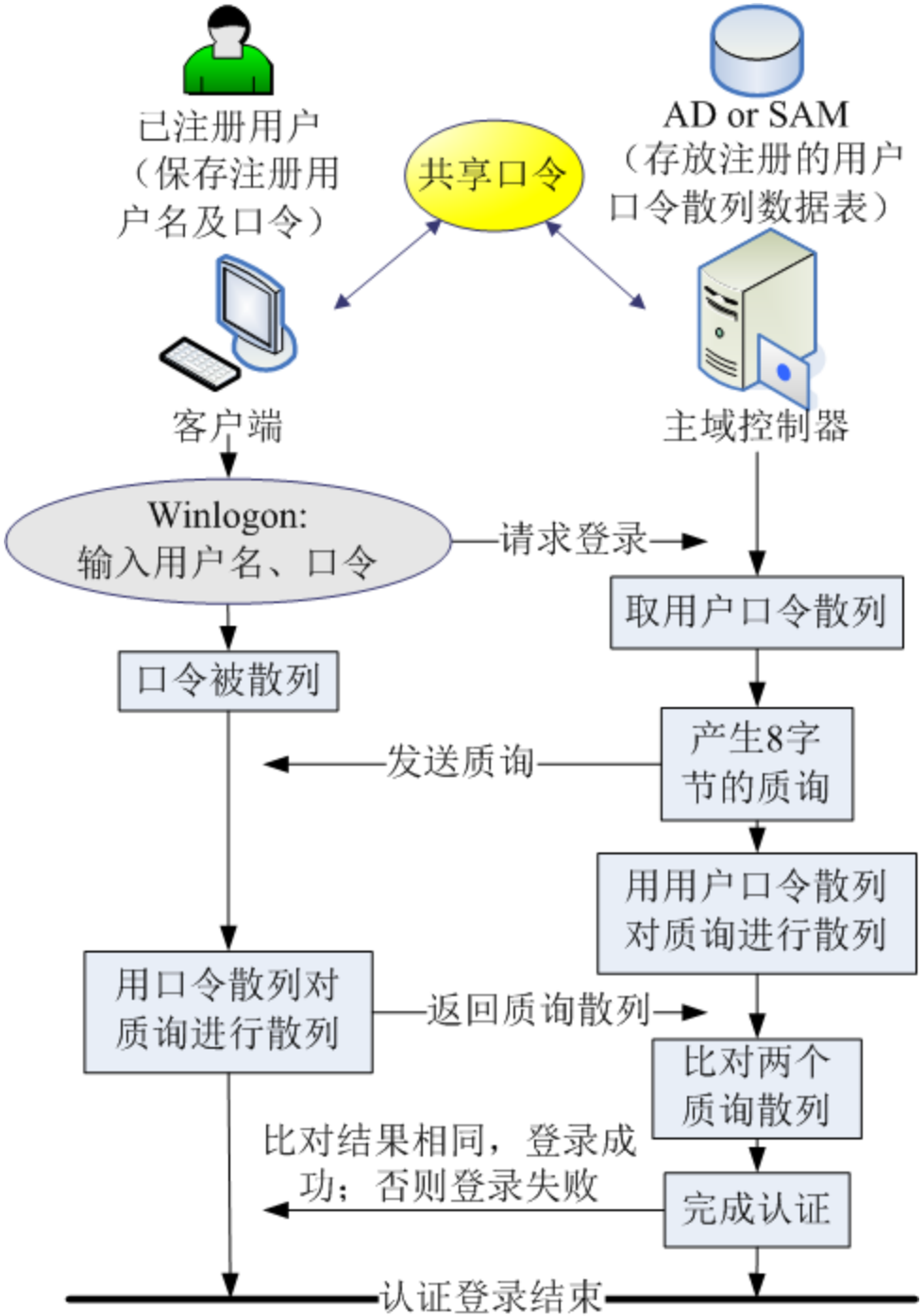
- Kerberos的设计目标是通过使用对称密钥系统为客户机/服务器应用程序提供强大的第三方认证服务。
  - 每个用户或应用服务器与Kerberos分享一个对称密钥。
  - Kerberos由两个部分组成，
    - 认证服务器AS（Authentication Server）和票据授予服务器TGS（Ticket Granting Server）。
  - 允许一个用户通过交换加密消息在整个网络上与另一个用户或应用服务器互相证明身份，Kerberos给通讯双方提供对称密钥。
  - 票据Ticket是客户端用于证明自己身份。
    - AS负责签发访问TGS服务器的票据，TGS负责签发访问其它应用服务器的票据。

协议内容

- 第一阶段 身份验证服务交换
  - C → AS： $ID_C \| ID_{tgs} \| TS_1$
  - AS → C： $E_{KC}[K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}]$
  - ✧ $Ticket_{tgs} = E_{Ktgs}[K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2]$
- 第二阶段 票据授予服务交换
  - C → TGS： $ID_V \| Ticket_{tgs} \| Authenticator_c$
  - TGS → C： $E_{Kc,tgs}[K_{c,v} \| ID_v \| TS_4 \| Ticket_v]$
  - ✧ $Authenticator_c = E_{Kc,tgs}[ID_c \| Ad_c \| TS_3]$。
  - ✧ $Ticket_v = E_{KV}[K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4]$；
- 第三阶段 客户与服务器身份验证交换
  - C → V： $Ticket_v \| Authenticator_c$
  - V → C： $E_{Kc,v}[TS_5+1]$ (for mutual authentication)
  - ✧ $Authenticator_c = E_{Kc,v}[ID_c \| AD_c \| TS_5]$



Windows系统的安全认证



4.2.2 基于公开密钥的认证协议

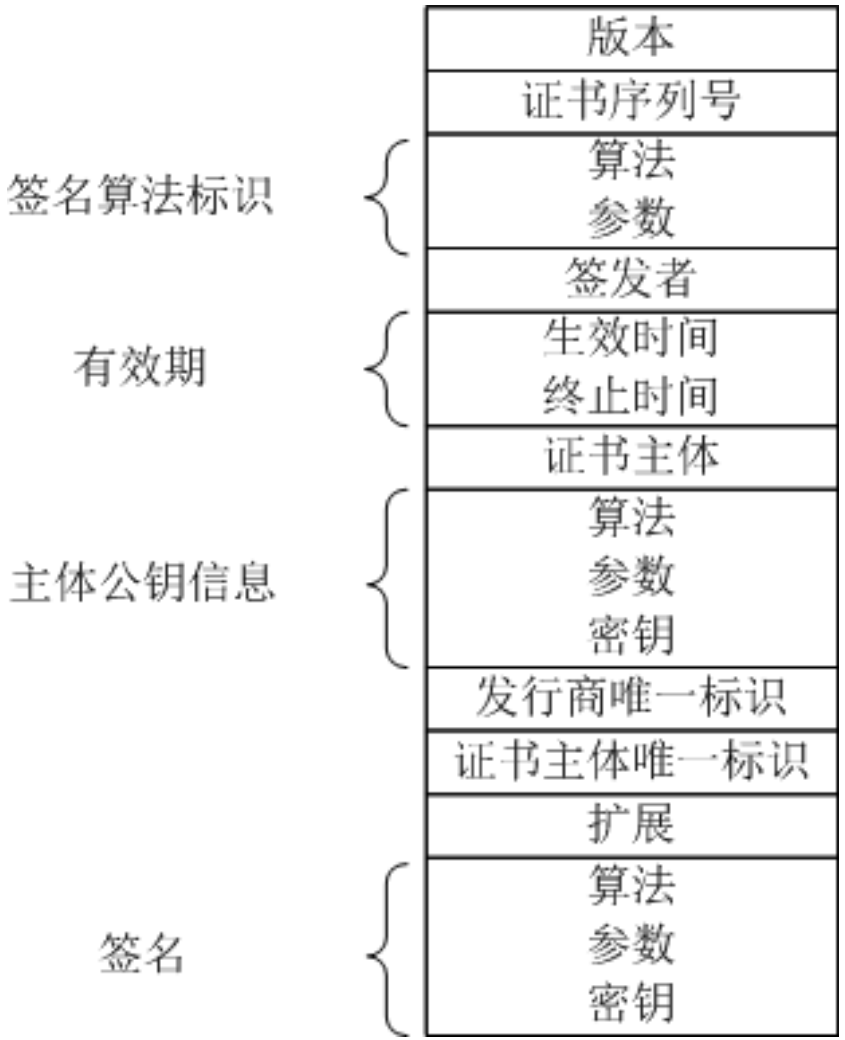
- 基于公开密钥体制下的认证协议通常有两种认证方式，
  - 方式一是实体A需要认证实体B，A发送一个明文挑战消息（也称挑战因子，通常是随机数）给B，B接收到挑战后，用自己的私钥对挑战明文消息加密，称为签名；B将签名信息发送给A，A使用B的公钥来解密签名消息，称为验证签名，以此来确定B是否具有合法身份。
  - 方式二是实体A将挑战因子用实体B的公钥加密后发送给B，B收到后是用自己的私钥解密还原出挑战因子，并将挑战因子明文发还给A，A可以根据挑战因子内容的真伪来核实B的身份。

Needham-Schroeder公钥认证

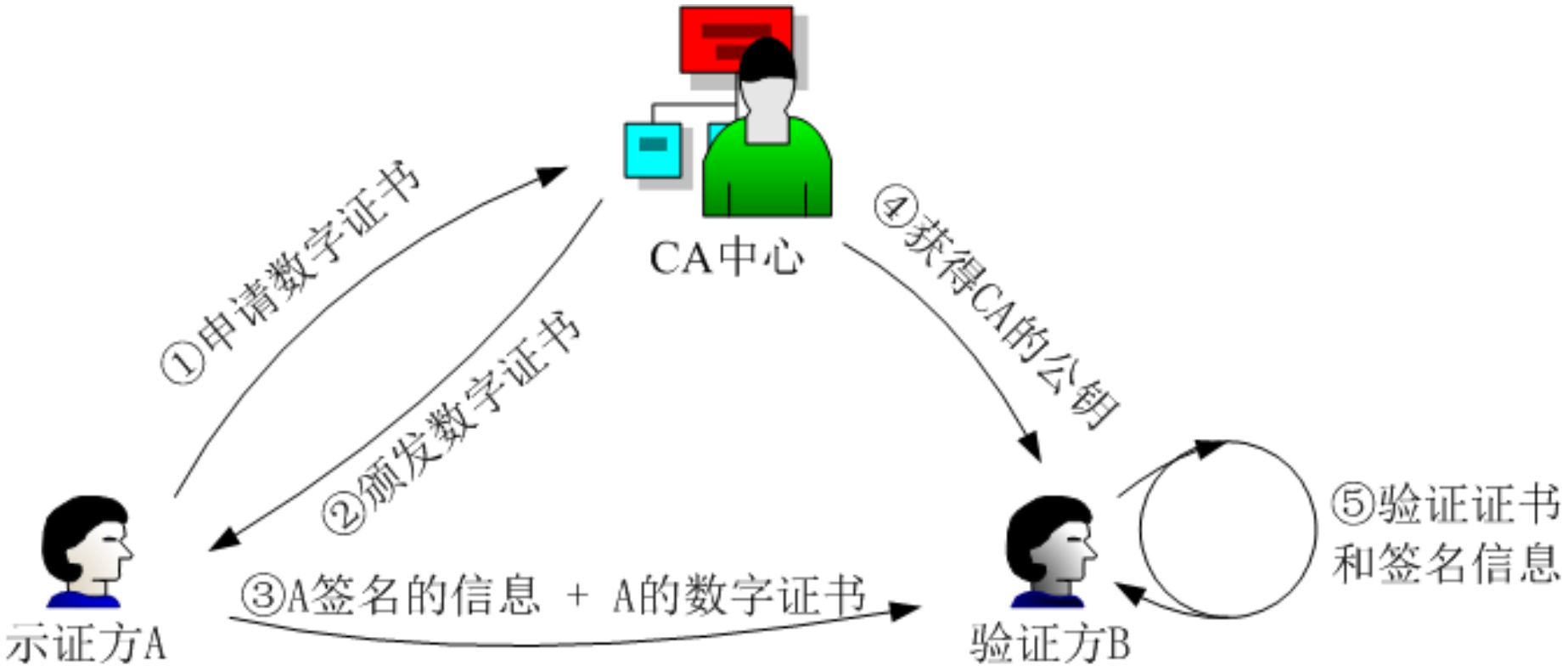
- ① A → B：$E_{KUb}[ID_a \| R_a]$；
  - A使用B的公钥加密A的标识ID_a和挑战R_a，确保只有B才能使用私钥解密。
- ② B → A：$E_{KUa}[R_a \| R_b]$；
  - B使用A的公钥加密A的挑战R_a和B的挑战R_b，发送给A，确保只有A才能使用其私钥解密。
- ③ A → B：$E_{KUb}[R_b]$；
  - A还原出R_b后，再使用B的公钥加密R_b，作为验证应答信息发送给B。

基于CA数字证书的认证协议

- 数字证书是一个经过权威的、可信赖的、公正的第三方机构（CA认证中心）签名的包含拥有者信息及公开密钥的文件。
- CA：Certificate Authority



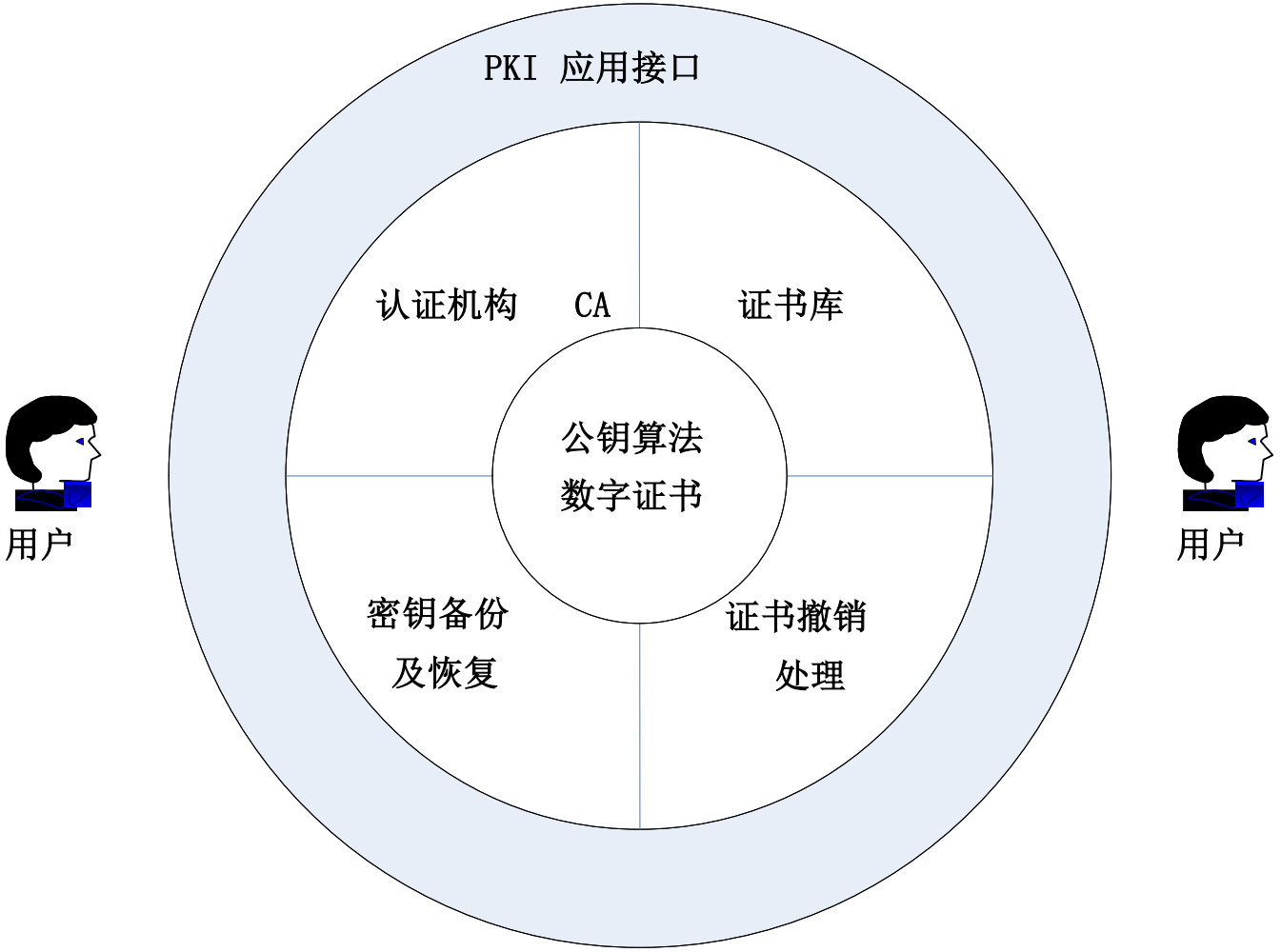
基于数字证书进行身份认证的过程



4.3 公钥基础设施PKI

- PKI是一种遵循一定标准的密钥管理基础平台，为所有网络应用提供加密和数字签名等密码服务所必需的密钥和证书管理。
  - PKI就是利用公钥理论和技术建立的提供安全服务的基础设施。
  - 用户可利用PKI平台提供的服务进行安全的电子交易、通信和互联网上的各种活动。

4.3.1 PKI体系结构



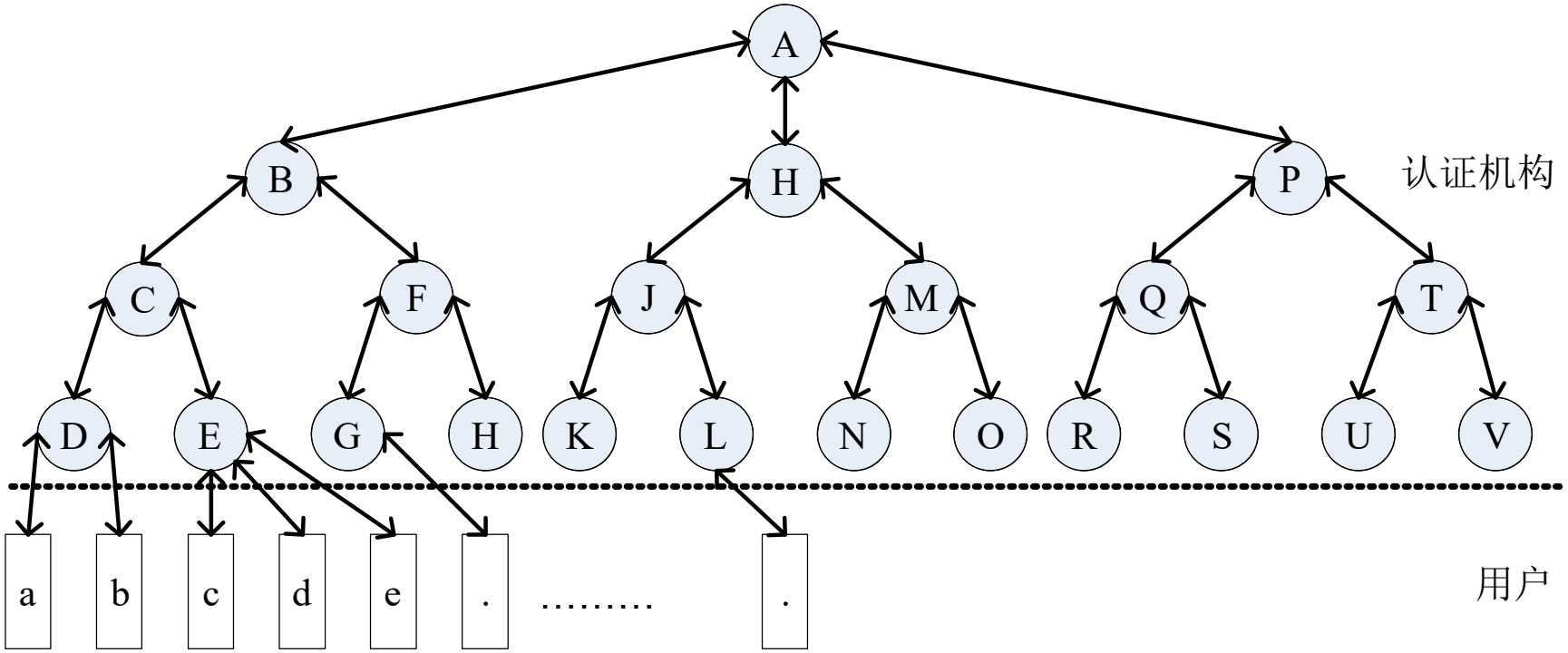
4.3.2 基于X.509的PKI系统

- X.509是国际电信联盟-电信（ITU-T）部分标准和国际标准化组织（ISO）的证书格式标准。
- X.509的主要作用
  - 确定了公钥证书结构的基准
    - X.509 V3证书包括一组按预定义顺序排列的强制字段，还有可选扩展字段，即使在强制字段中，X.509证书也具有很大的灵活性，因为它为大多数字段提供了多种编码方案。

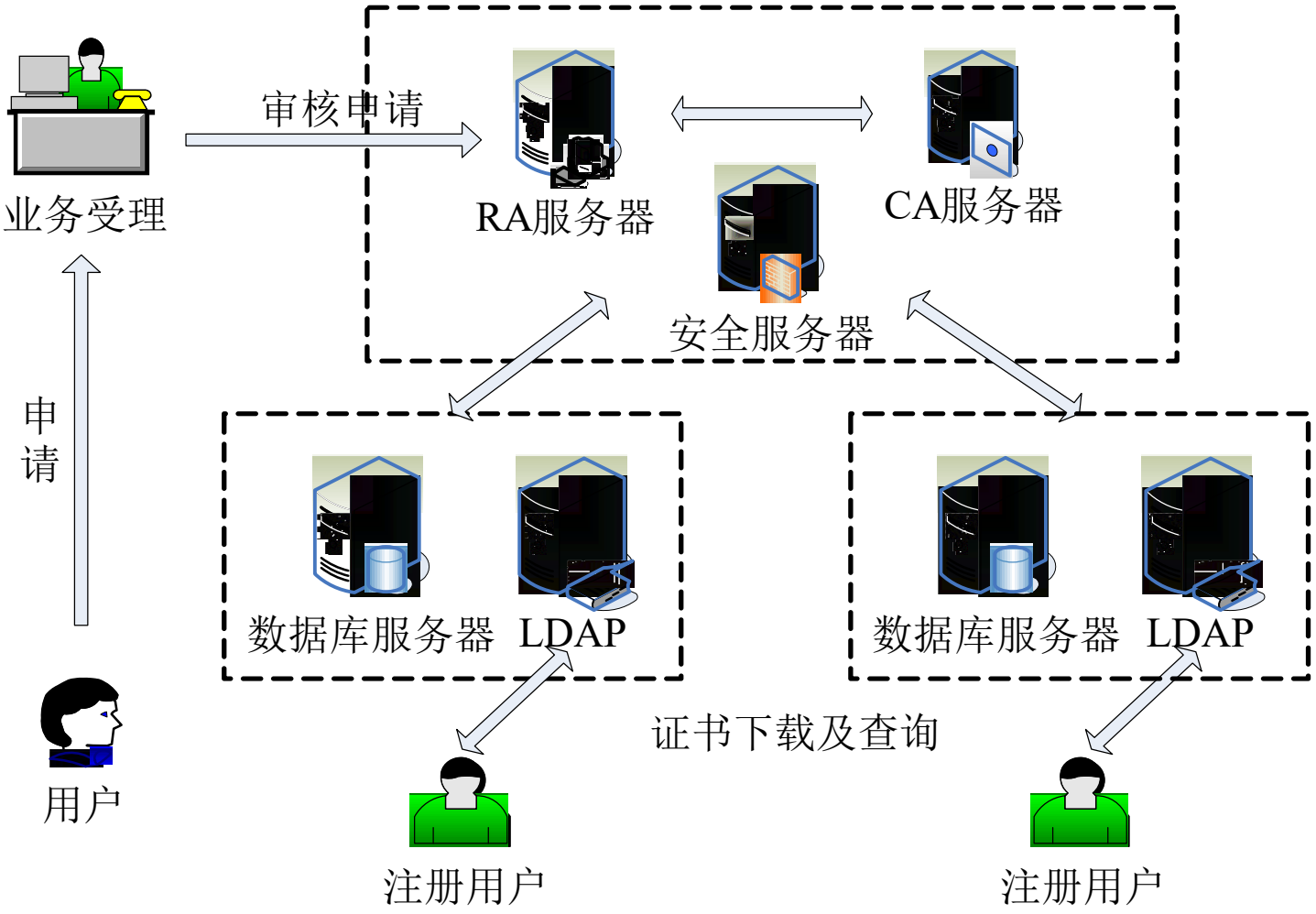
X.509的CA目录的层次结构

用户a的证书链可以使用下面的形式表达：

KR_A《CA_B》KR_B《CA_C》KR_C《CA_D》KR_D《CA_a》



一个典型的PKI模型


审核申请
业务受理
RA服务器
CA服务器
安全服务器
申请
数据库服务器
LDAP
数据库服务器
LDAP
证书下载及查询
用户
注册用户
注册用户

PKI系统功能

- 接收验证用户数字证书的申请；
- 确定是否接受用户数字证书的申请；
- 向申请者颁发（或拒绝颁发）数字证书；
- 接收、处理用户的数字证书更新请求；
- 接收用户数字证书的查询、撤销；
- 产生和发布证书的有效期；
- 数字证书的归档；
- 密钥归档；
- 历史数据归档。

问题

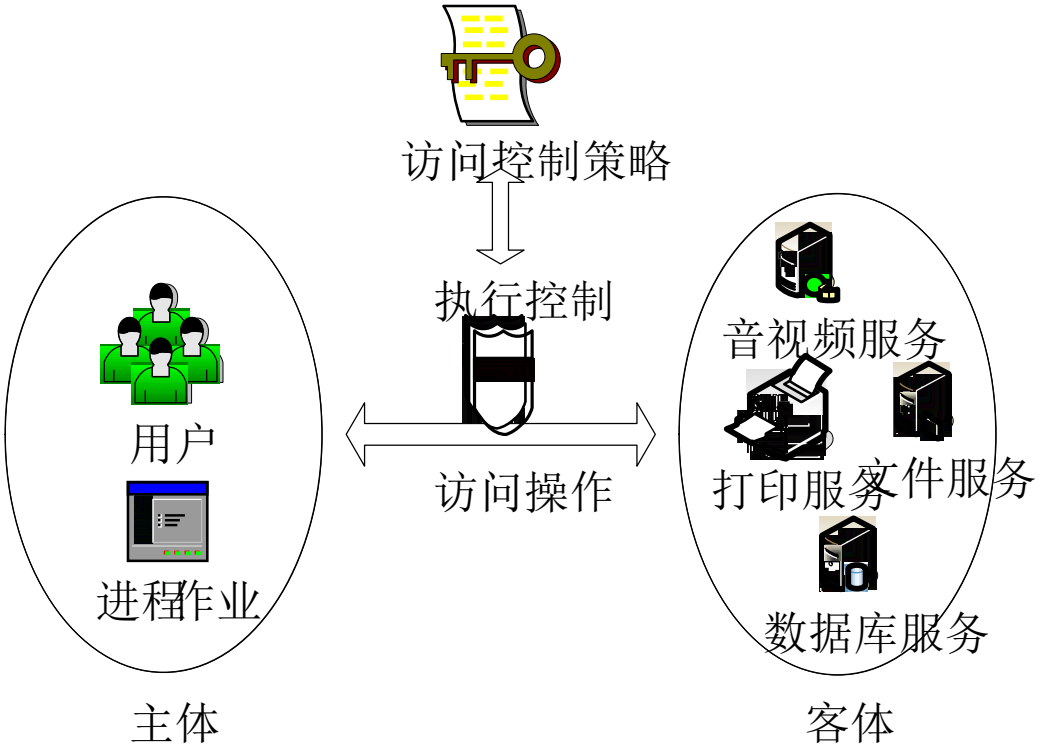
1. 什么是“挑战应答方式”认证和needham对称密钥认证协议的区别？模仿needham设计一个三方通讯认证协议。
2. 什么是Kerberos认证协议，讲解详细过程。
3. Windows系统的网络认证是如何实现的？
4. 什么是数字证书，如何使用数字证书进行身份认证？
5. 什么是PKI，它包含那些主要功能，如何工作？
6. 什么是证书链，X.509是如何实现证书认证的？
7. 设计一个基于PKI应用。举例说明。

第5章 访问控制

翟健宏

5.1 概述

- 身份认证：识别“用户是谁”的问题
- 访问控制：管理用户对资源的访问



访问控制的基本组成元素

- 主体(Subject)：是指提出访问请求的实体，是动作的发起者，但不一定是动作的执行者。主体可以是用户或其它代理用户行为的实体（如进程、作业和程序等）。
- 客体(Object)：是指可以接受主体访问的被动实体。客体的内涵很广泛，凡是可以被操作的信息、资源、对象都可以认为是客体。
- 访问控制策略（Access Control Policy）：是指主体对客体的操作行为和约束条件的关联集合。简单地讲，访问控制策略是主体对客体的访问规则集合，这个规则集合可以直接决定主体是否可以对客体实施的特定的操作。

5.2 访问控制模型

- 1985年美国军方提出可信计算机系统评估准则TCSEC，其中描述了两种著名的访问控制模型：
  - 自主访问控制DAC(Discretionary Access Control)
  - 强制访问控制MAC(Mandatory Access Control)
- 1992年美国国家标准与技术研究所(NIST)的David Ferraiolo和Rick Kuhn提出一个模型
  - 基于角色的访问控制RBAC（Role Based Access Control）模型

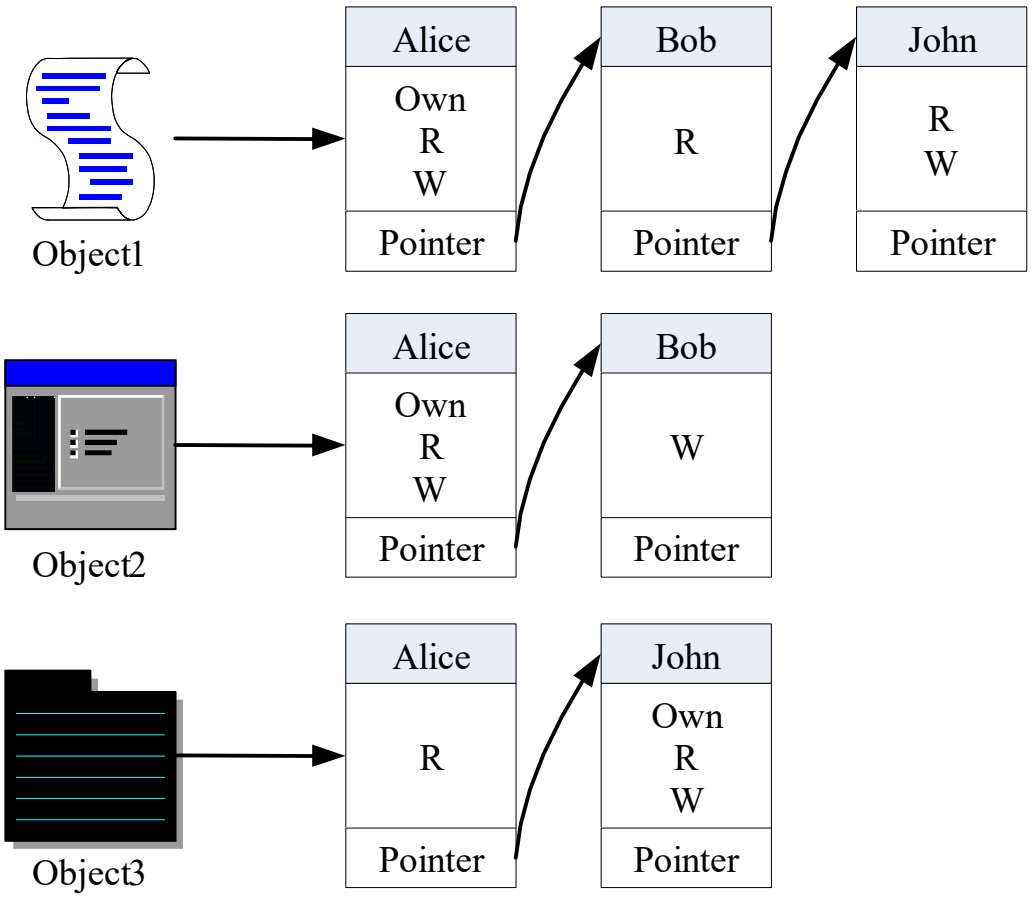
5.2.1 自主访问控制

- 自主访问控制DAC模型
  - 根据自主访问控制策略建立的一种模型，
  - 允许合法用户以用户或用户组的身份来访问系统控制策略许可的客体，同时阻止非授权用户访问客体。
  - 某些用户还可以自主地把自己所拥有的客体的访问权限授予其它用户。
- UNIX、LINUX以及Windows NT等操作系统都提供自主访问控制的功能。

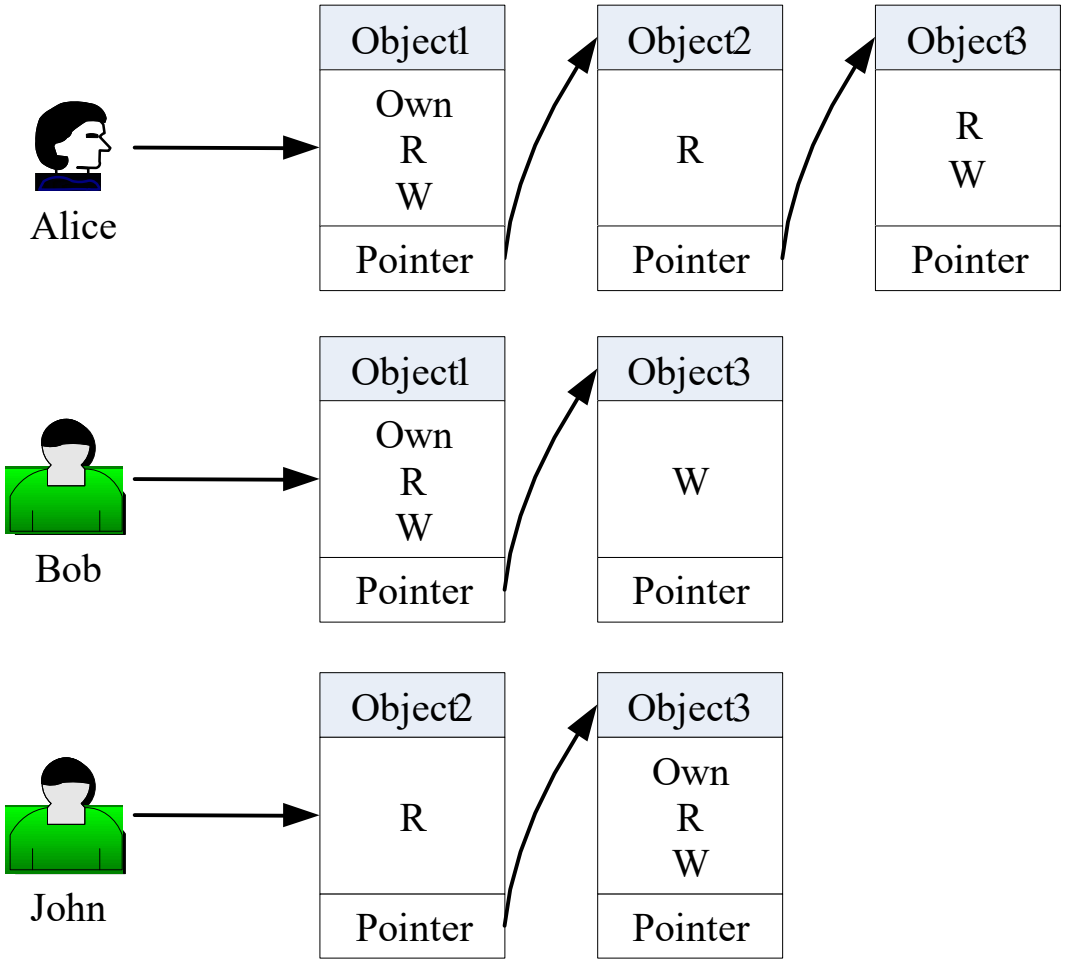
访问权限信息存储

- 特权用户为普通用户分配的访问权限信息的形式
  - 访问控制表ACL（Access Control Lists）
  - 访问控制能力表ACCL（Access Control Capability Lists）
  - 访问控制矩阵ACM（Access Control Matrix）

访问控制表ACL


Alice
Own
R
W
Pointer
Bob
R
Pointer
John
R
W
Pointer
Object1
Alice
Own
R
W
Pointer
Bob
W
Pointer
Object2
Alice
R
Pointer
John
Own
R
W
Pointer
Object3

访问控制能力表ACCL



访问控制矩阵ACM

主体 \ 客体	Object1	Object2	Object3
Alice	Own，R，W	R	R，W
Bob	R	Own，R，W	
John	R，W		Own，R，W

5.2.2 强制访问控制

- 强制访问控制MAC是一种多级访问控制策略
  - 系统事先给访问主体和受控客体分配不同的安全级别属性。
  - 在实施访问控制时，系统先对访问主体和受控客体的安全级别属性进行比较，再决定访问主体能否访问该受控客体。
- MAC模型形式化描述
  - 主体集S和客体集O
  - 安全类SC(x) = < L，C >
    - L为有层次的安全级别Level
    - C为无层次的安全范畴Category

访问的四种形式

- 向下读（RD，Read Down）：
  - 主体安全级别高于客体信息资源的安全级别时，即SC(s)≥SC(o)，允许读操作； Bell-LaPadula
- 向上读（RU，Read Up）：
  - 主体安全级别低于客体信息资源的安全级别时，即SC(s)≤SC(o)，允许读操作； Biba
- 向下写（WD，Write Down）：
  - SC(s)≥SC(o)时，允许写操作； Biba
- 向上写（WU，Write Up）：
  - SC(s)≤SC(o)时，允许写操作。 Bell-LaPadula

MAC信息流安全控制

主体 \ 客体	TS	C	S	U
TS	R/W	R	R	R
C	W	R/W	R	R
S	W	W	R/W	R
U	W	W	W	R/W

High ↓ ↓ ↓ Low

5.2.3 基于角色的访问控制

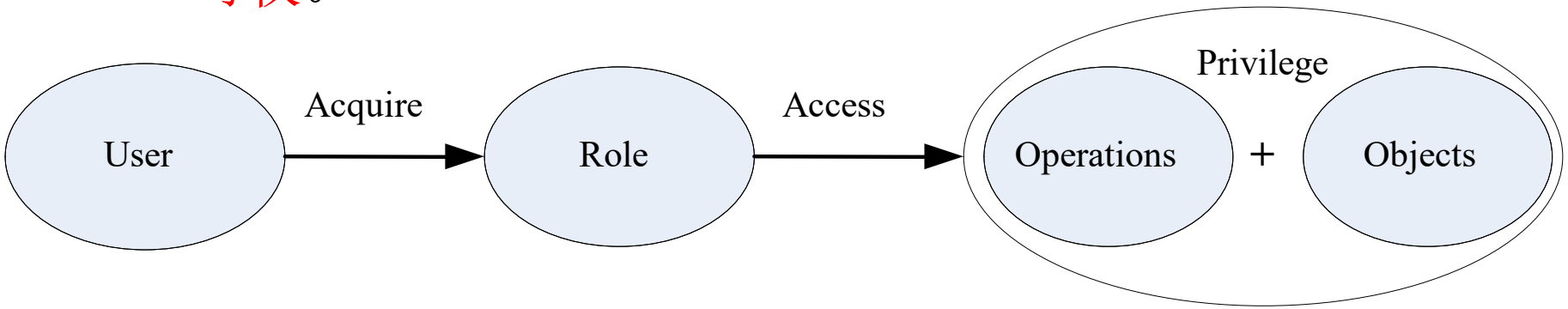
- Group的概念，一般认为Group是具有某些相同特质的用户集合。
- 在UNIX操作系统中Group可以被看成是拥有相同访问权限的用户集合，
  - 定义用户组时会为该组赋予相应的访问权限。
  - 如果一个用户加入了该组，则该用户即具有了该用户组的访问权限
  - 角色Role的概念，可以这样理解一个角色是一个与特定工作活动相关联的行为与责任的集合

角色Role的理解

- 一个角色是一个与特定工作活动相关联的行为与责任的集合。
  - Role不是用户的集合，也就与组Group不同。
  - 当将一个角色与一个组绑定，则这个组就拥有了该角色拥有的特定工作的行为能力和责任。
  - 组Group和用户User都可以看成是角色分配的单位和载体。
  - 而一个角色Role可以看成具有某种能力或某些属性的主体的一个抽象。

引入角色Role的目的

- Role的目的：
  - 为了隔离User与Privilege。
  - Role作为一个用户与权限的代理层，所有的授权应该给予Role而不是直接给User或Group。
  - RBAC模型的基本思想是将访问权限分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。



例子

- 在一个公司里，用户角色可以定义为经理、会计、出纳员和审计员，具体的权限如下：
  - 经理：允许查询公司的经营状况和财务信息，但不允许修改具体财务信息，必要时可以根据财务凭证支付或收取现金，并编制银行账和现金帐；
  - 会计：允许根据实际情况编制各种财务凭证及账簿，但不包括银行账和现金帐；
  - 出纳员：允许根据财务凭证支付或收取现金，并编制银行账和现金帐；
  - 审计员：允许查询审查公司的经营状况和财务信息，但不允许修改任何账目。

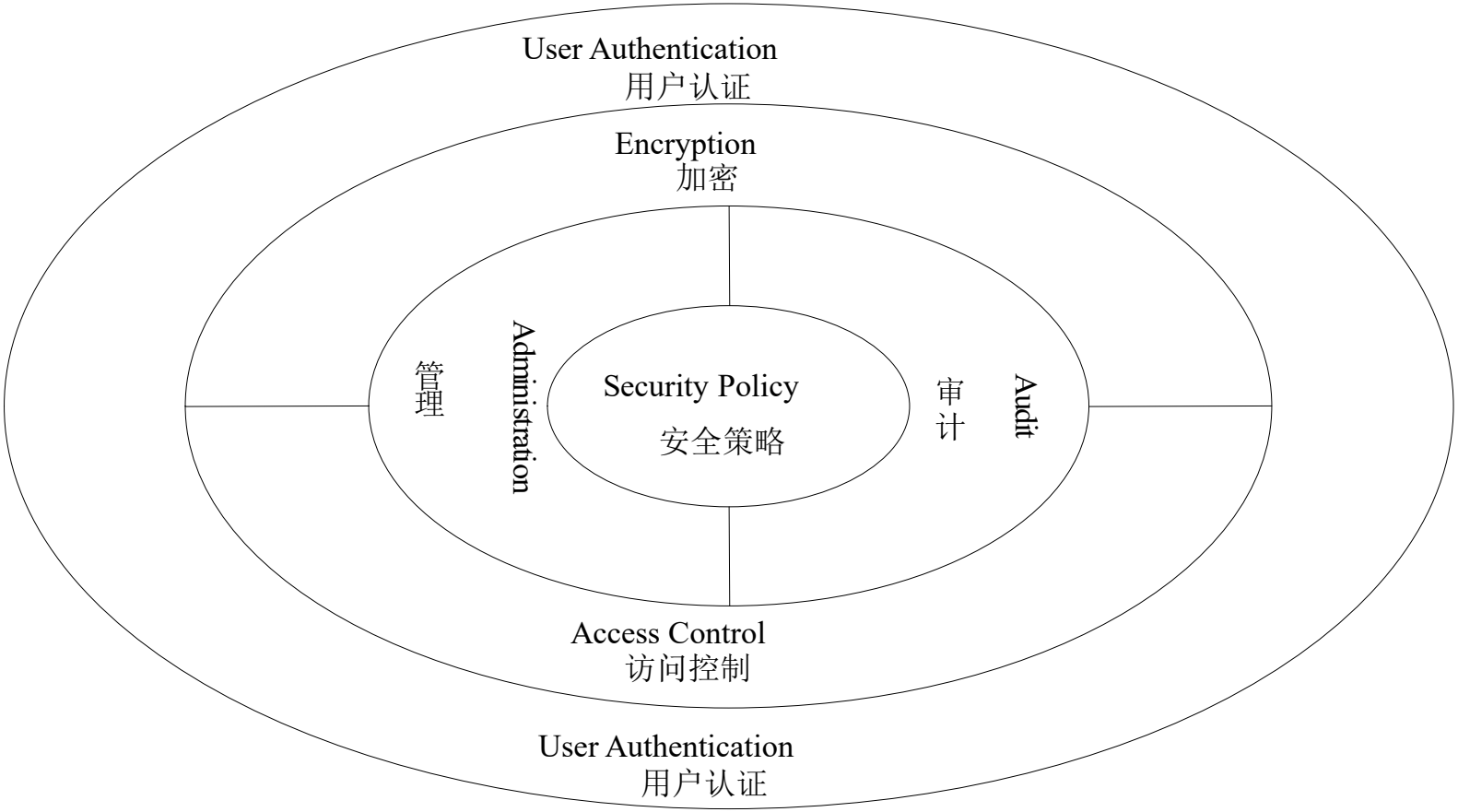
- RBAC的策略陈述易于被非技术的组织策略者理解，既具有基于身份策略的特征，也具有基于规则策略的特征。
- 在基于组或角色的访问控制中，一个用户可能不只是一个组或角色的成员，有时又可能有所限制。
- 例如经理可以充当出纳员的角色，但不能负责会计工作，即各角色之间存在相容和相斥的关系。

制定访问控制策略的三个基本原则

- 最小特权原则
  - 是指主体执行操作时，按照主体所需权利的最小化原则分配给主体权力。
  - 最小特权原则的优点是最大限度地限制了主体实施授权行为，可以避免来自突发事件和错误操作带来的危险。
- 最小泄漏原则：
  - 是指主体执行任务时，按照主体所需要知道信息的最小化原则分配给主体访问权限。
- 多级安全策略：
  - 是指主体和客体间的数据流方向必须受到安全等级的约束。多级安全策略的优点是避免敏感信息的扩散。
  - 对于具有安全级别的信息资源，只有安全级别比它高的主体才能够对其访问。

5.3 Windows系统的安全管理

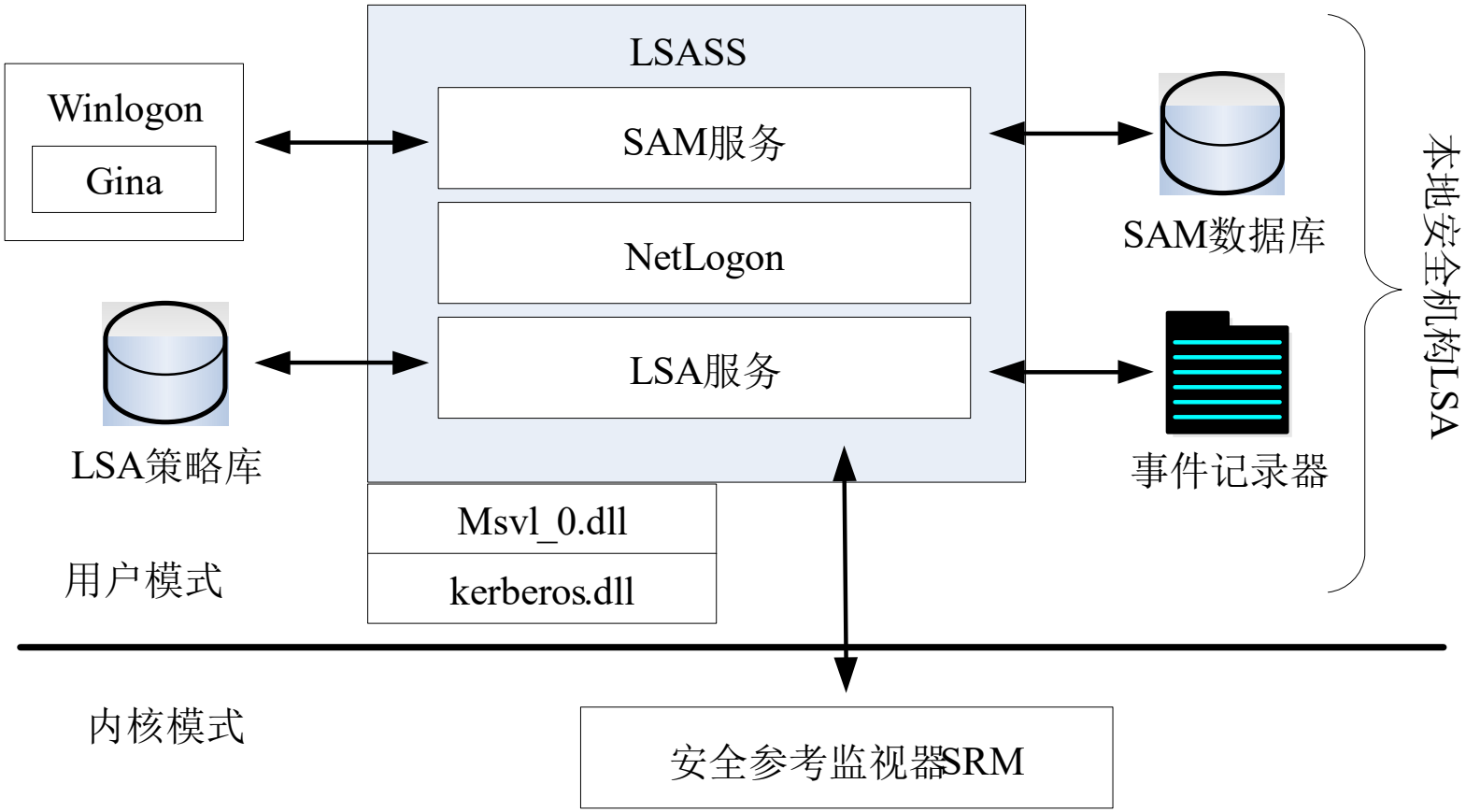
- **5.3.1 Windows系统安全体系结构**



安全主体

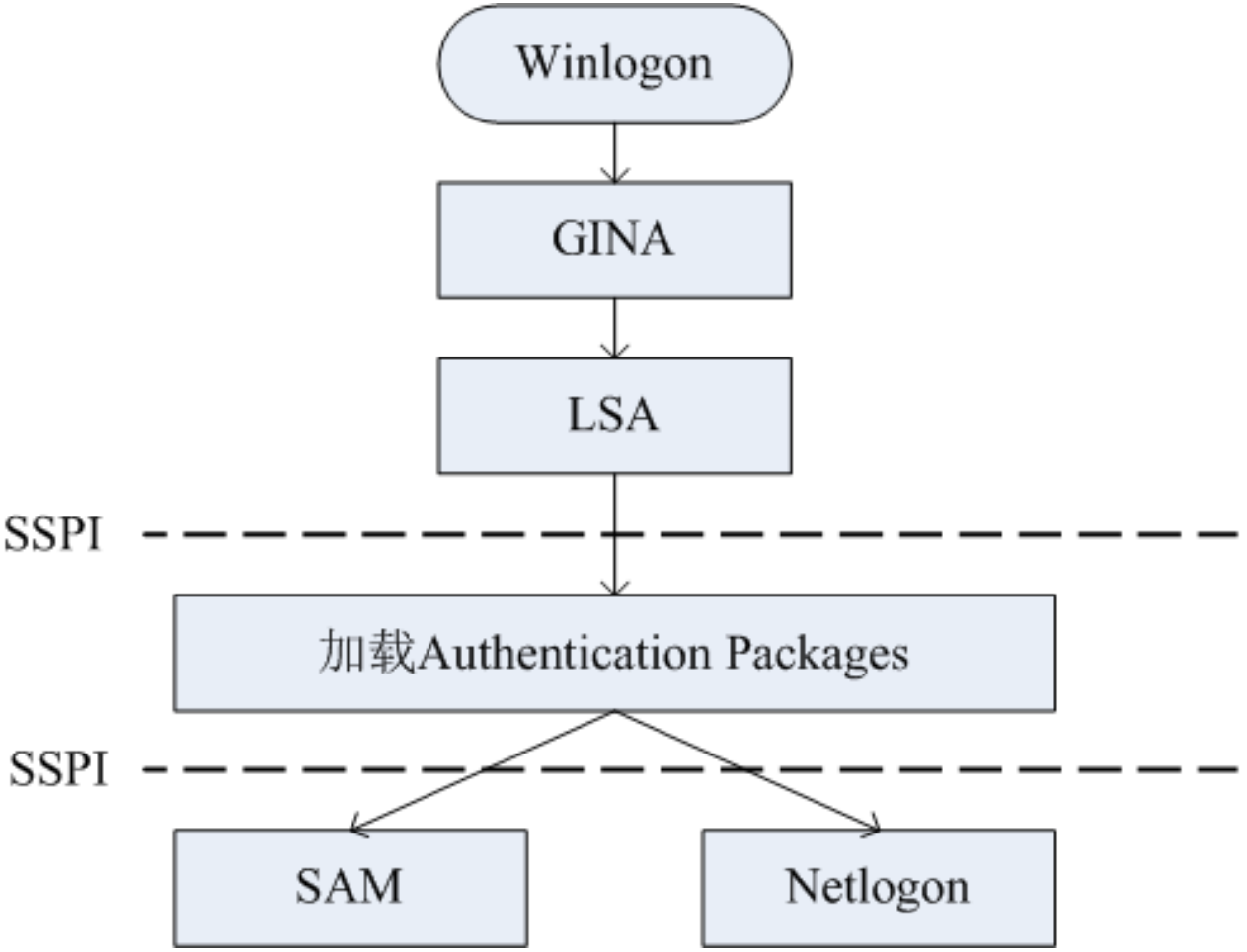
- Windows系统的安全性主要围绕安全主体展开，保护其安全性。
- 安全主体主要包括用户、组、计算机以及域等。
  - 用户是Windows系统中操作计算机资源的主体，每个用户必须先行加入Windows系统，并被指定唯一的账户，
  - 组是用户账户集合的一种容器，同时组也被赋予了一定的访问权限，放到一个组中的所有账户都会继承这些权限；
  - 计算机是指一台独立计算机的全部主体和客体资源的集合，也是Windows系统管理的独立单元；
  - 域是使用域控制器(DC, Domain Controller)进行集中管理的网络，域控制器是共享的域信息的安全存储仓库，同时也作为域用户认证的中央控制机构。

安全子系统



Windows安全子系统

Windows登录认证流程



5.3.2 Windows系统的访问控制

- 访问控制模块的组成
  - 访问令牌（Access Token）和安全描述符（Security Descriptor），它们分别被访问者和被访问者持有。通过访问令牌和安全描述符的内容，Windows可以确定持有令牌的访问者能否访问持有安全描述符的对象。
- 访问控制的基本控制单元“账户”。
  - 账户是一种参考上下文(context)，是一个具有特定约束条件的容器，也可以理解为背景环境。
  - 操作系统在这个上下文描述符上运行该账户的大部分代码。
  - 那些在登录之前就运行的代码（例如服务）运行在一个账户（特殊的本地系统账户SYSTEM）的上下文中。

安全标识符SID

- Windows中的每个账户或账户组都有一个安全标识符SID（Security Identity）
  - Administrator、Users等账户或者账户组在Windows内部均使用SID来标识的。
  - 每个SID在同一个系统中都是唯一的。
    - 例如S-1-5-21-1507001333-1204550764-1011284298-500就是一个完整的SID。
    - 第一个数字（本例中的1）是修订版本编号，
    - 第二个数字是标识符颁发机构代码（Windows 2000为5）
    - 4个子颁发机构代码
    - 相对标识符RID（Relative Identifier） RID 500代表Administrator账户，RID 501是Guest账户。从1000开始的RID代表用户账户

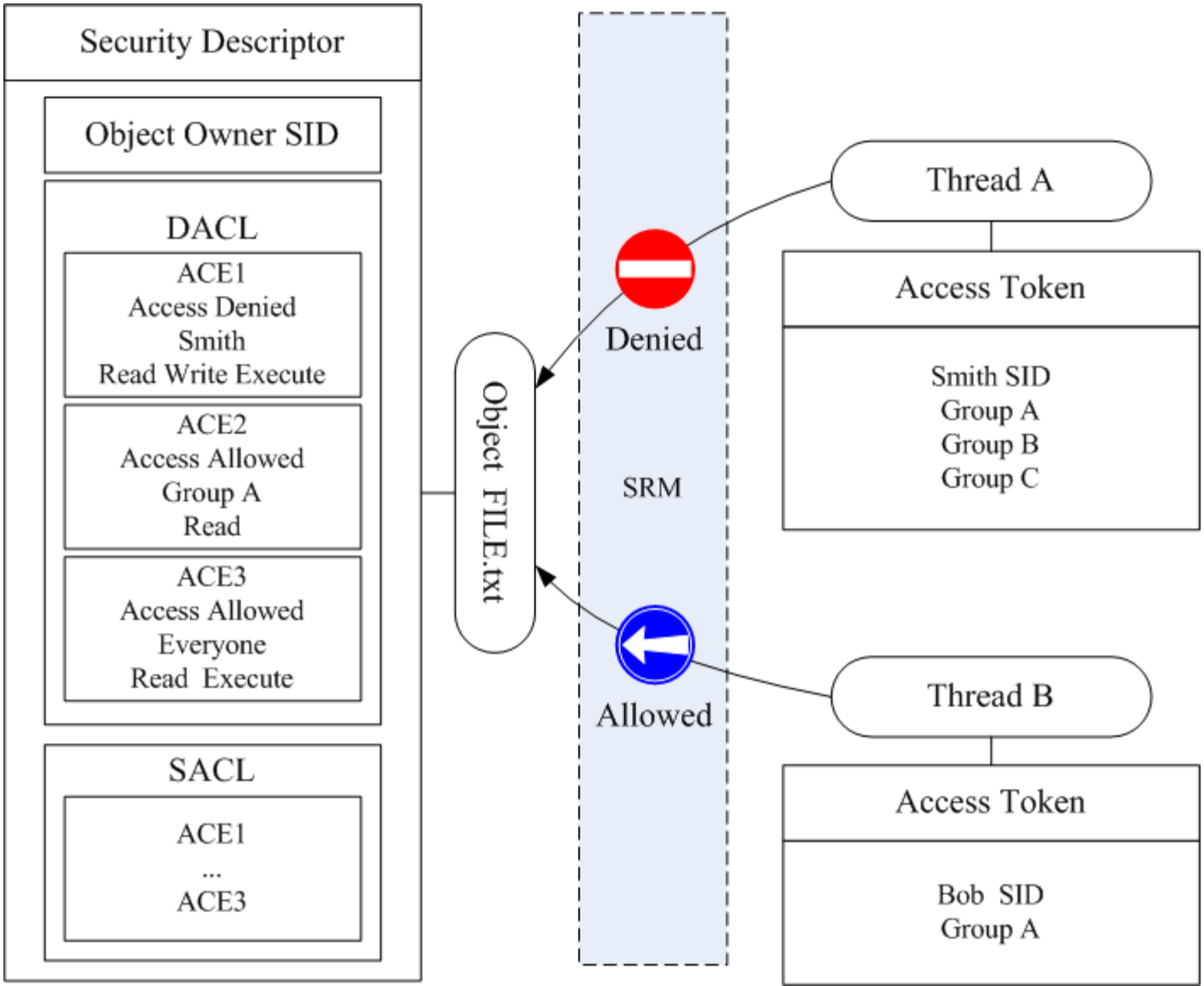
访问令牌

- 每个访问令牌都与特定的Windows账户相关联，访问令牌包含该帐户的SID、所属组的SID以及帐户的特权信息。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\>whoami /all
[User]   = "Smith\Administrator"  S-1-5-21-2000478354-842925246-1202660629-500
[Group 1] = " Smith \None"  S-1-5-21-2000478354-842925246-1202660629-513
[Group 2] = "Everyone"  S-1-1-0
[Group 3] = " Smith \Debugger Users"  S-1-5-21-2000478354-842925246-
1202660629-1004
[Group  4] = "BUILTIN\Administrators"  S-1-5-32-544
[Group  5] = "BUILTIN\Users"  S-1-5-32-545
[Group  6] = "NT AUTHORITY\INTERACTIVE"  S-1-5-4
[Group  7] = "NT AUTHORITY\Authenticated Users"  S-1-5-11
[Group  8] = "LOCAL"  S-1-2-0
```

- Microsoft Windows [版本 6.1.7600]
- 版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
- C:\Users\zjh>whoami
- zjh-pc\zjh
- C:\Users\zjh>whoami/all
- 用户信息
- ----------------
- 用户名 SID
- ========== ==
- zjh-pc\zjh S-1-5-21-868672325-3564177769-4166673043-1000
- 组信息
- -----------------
- 组名 类型 SID 属性
- ==================================== ====== ================================
- Everyone 已知组 S-1-1-0
- 必需的组, 启用于默认, 启用的组
- zjh-PC\Debugger Users 别名 S-1-5-21-868672325-3564177769-4166
- 673043-1001 必需的组, 启用于默认, 启用的组
- BUILTIN\Administrators 别名 S-1-5-32-544
- 只用于拒绝的组
- BUILTIN\Users 别名 S-1-5-32-545
- 必需的组, 启用于默认, 启用的组
- NT AUTHORITY\INTERACTIVE 已知组 S-1-5-4
- 必需的组, 启用于默认, 启用的组
- 控制台登录 已知组 S-1-2-1
- 必需的组, 启用于默认, 启用的组
- NT AUTHORITY\Authenticated Users 已知组 S-1-5-11
- 必需的组, 启用于默认, 启用的组
- NT AUTHORITY\This Organization 已知组 S-1-5-15
- 必需的组, 启用于默认, 启用的组
- LOCAL 已知组 S-1-2-0
- 必需的组, 启用于默认, 启用的组
- NT AUTHORITY\NTLM Authentication 已知组 S-1-5-64-10
- 必需的组, 启用于默认, 启用的组
- Mandatory Label\Medium Mandatory Level 标签 S-1-16-8192
- 必需的组, 启用于默认, 启用的组
- 特权信息
- ----------------------
- 特权名 描述 状态
- ============================= ==================== ======
- SeShutdownPrivilege 关闭系统 已禁用
- SeChangeNotifyPrivilege 绕过遍历检查 已启用
- SeUndockPrivilege 从扩展坞上取下计算机 已禁用
- SeIncreaseWorkingSetPrivilege 增加进程工作集 已禁用
- SeTimeZonePrivilege 更改时区 已禁用

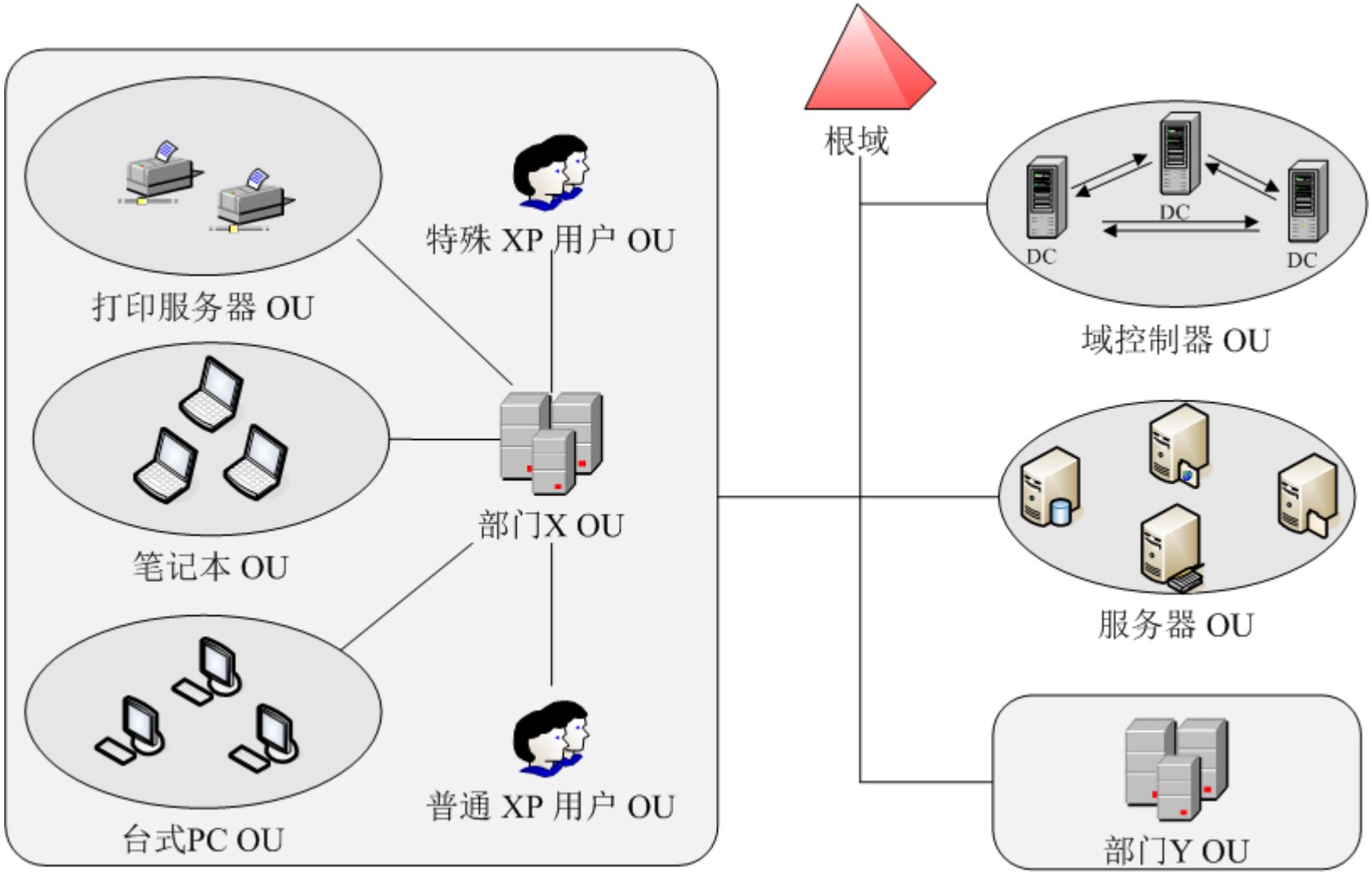
Window 访问控制


Security Descriptor
Object Owner SID
DACL
ACE1
Access Denied
Smith
Read Write Execute
ACE2
Access Allowed
Group A
Read
ACE3
Access Allowed
Everyone
Read Execute
SACL
ACE1
...
ACE3
Object FILE.txt
Denied
SRM
Allowed
Thread A
Access Token
Smith SID
Group A
Group B
Group C
Thread B
Access Token
Bob SID
Group A

5.3.3 活动目录与组策略

- 活动目录AD（Active Directory）是一个面向网络对象管理的综合目录服务。
- 网络对象包括用户、用户组、计算机、打印机、应用服务器、域、组织单元（OU）以及安全策略等。
- AD 提供的是各种网络对象的索引集合，也可以看作是数据存储的视图，
- 将分散的网络对象有效地组织起来，建立网络对象索引目录，并存储在活动目录的数据库内。

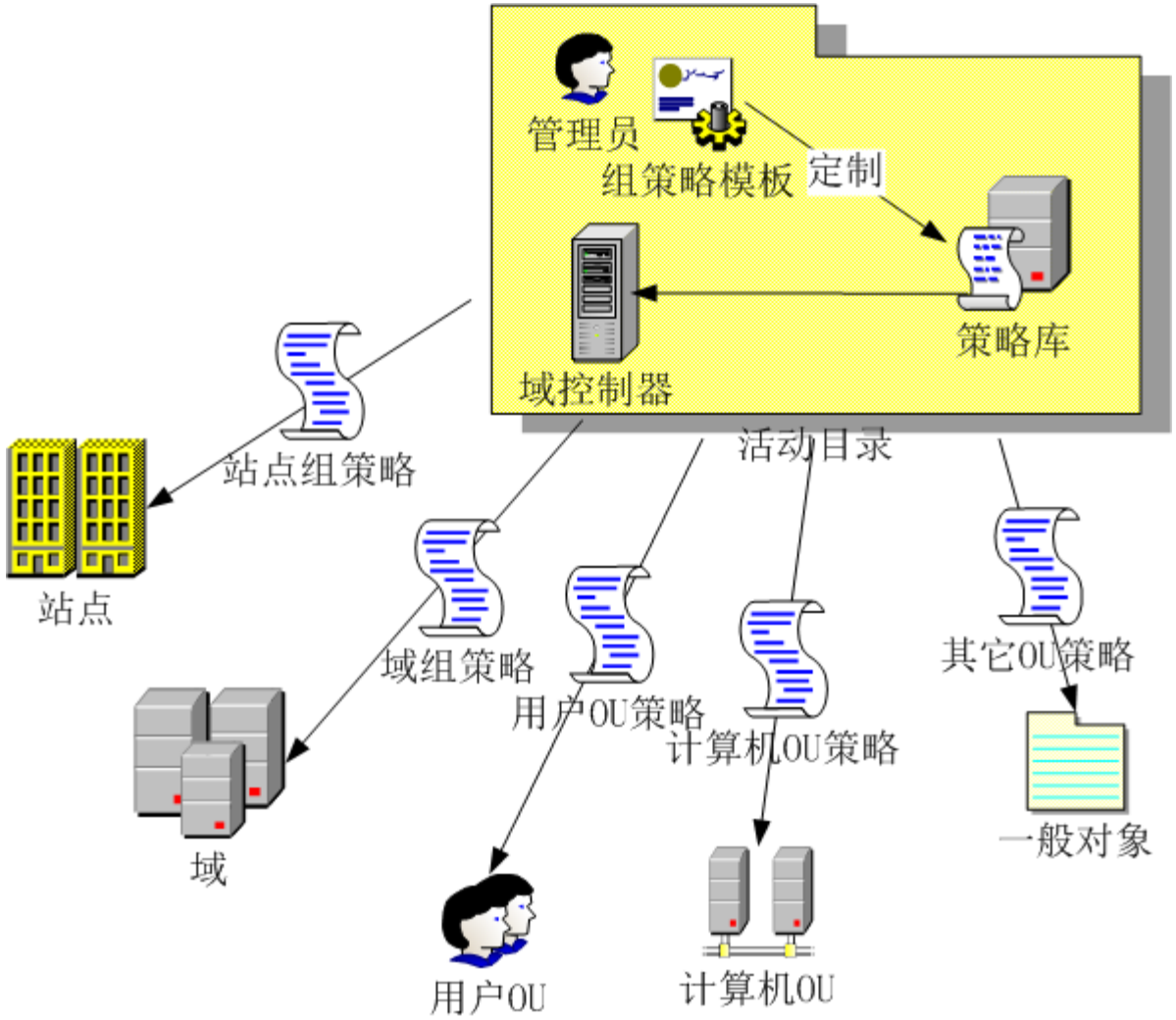
活动目录AD的管理划分



组策略GP

- 活动目录AD是Windows网络中重要的安全管理平台，组策略GP（Group Policy）是其安全性的重要体现。
- 组策略可以理解为依据特定的用户或计算机的安全需求定制的安全配置规则。
  - 管理员针对每个组织单元OU定制不同的组策略，并将这些组策略存储在活动目录的相关数据库内，可以强制推送到客户端实施组策略。
- 活动目录AD可以使用组策略命令来通知和改变已经登录的用户的组策略，并执行相关安全配置。

组策略工作流程


管理员
组策略模板
定制
策略库
域控制器
活动目录
站点组策略
站点
域组策略
用户OU策略
计算机OU策略
其它OU策略
域
用户OU
计算机OU
一般对象

组策略的实施

- 注册表是Windows系统中保存系统应用软件配置的数据库。
- 很多配置都是可以自定义设置的，但这些配置发布在注册表的各个角落，如果是手工配置，可想是多么困难和繁琐。
- 组策略可以将系统中重要的配置功能汇集成一个配置集合，管理人员通过配置并实施组策略，达到直接管理计算机的目的。
- 简单点说，实施组策略就是修改注册表中的相关配置。

组策略和活动目录AD配合

- 组策略分为基于活动目录的和基于本地计算机的两种：
  - AD组策略存储在域控制器上活动目录AD的数据库中，它的定制实施由域管理员来执行；而本地组策略存放在本地计算机内，由本地管理员来定制实施。
  - AD组策略实施的对象是整个组织单元OU；本地组策略只负责本地计算机。
- 组策略和活动目录AD配合
  - 组策略部署在OU、站点或域的范围内，也可以部署在本地计算机上。部署在本地计算机时，组策略不能发挥其全部功能，只有和AD配合，组策略才可以发挥出全部潜力。

组策略的主要工作

① 部署软件

② 设置用户权力

③ 软件限制策略

- 管理员可以通过配置组策略，限制某个用户只能运行特定的程序或执行特定的任务。

④ 控制系统设置：

- 允许管理员统一部署网络用户的Windows服务。

⑤ 设置登录、注销、关机、开机脚本。

⑥ 通用桌面控制

⑦ 安全策略

⑧ 重定向文件夹

⑨ 基于注册表的策略设置

第6章 网络威胁

翟健宏

6.1 概述

- 威胁：用威力逼迫恫吓使人屈服。
- 网络威胁：是网络安全受到威胁、存在着危险。
- 随着互联网的不断发展，网络安全威胁也呈现了一种新的趋势，
  - 最初的病毒，比如“CIH”、“大麻”等传统病毒
  - 逐渐发展为包括特洛伊木马、后门程序、流氓软件、间谍软件、广告软件、网络钓鱼、垃圾邮件等等，
  - 目前的网络威胁往往是集多种特征于一体的混合型威胁。

网络威胁的三个阶段

- 第一阶段（1998年以前）网络威胁主要来源于传统的计算机病毒，其特征是通过媒介复制进行传染，以攻击破坏个人电脑为目的；
- 第二阶段（大致在1998年以后）网络威胁主要以蠕虫病毒和黑客攻击为主，其表现为蠕虫病毒通过网络大面积爆发及黑客攻击一些服务网站；
- 第三阶段（2005年以来）网络威胁多样化，多数以偷窃资料、控制利用主机等手段谋取经济利益为目的。

网络威胁分类

- 从攻击发起者的角度来看，
  - 一类是主动攻击型威胁，如网络监听和黑客攻击等，这些威胁都是对方人为通过网络通信连接进行的；
  - 另一类就是被动型威胁，一般是用户通过某种途径访问了不当的信息而受到的攻击。
- 依据攻击手段及破坏方式进行分类
  - 第一类是以传统病毒、蠕虫、木马等为代表的计算机病毒；
  - 第二类是以黑客攻击为代表的网络入侵；
  - 第三类以间谍软件、广告软件、网络钓鱼软件为代表的欺骗类威胁。

6.2 计算机病毒

- **6.2.1 病毒概述**
  - 1949年约翰·冯·诺依曼《自我繁衍的自动机理论》中从理论上论证了当今计算机病毒的存在论。
  - 20世纪60年代初，美国贝尔实验室的三位程序员编写了一个名为“磁芯大战”的游戏
  - 1983年，美国南加州大学的弗雷德·科恩博士研制出一种在运行过程中可以复制自身的破坏性程序，第一次验证了计算机病毒的存在。
  - 1984年弗雷德·科恩《计算机病毒：原理和实验》。
  - 1986年Brain病毒，世界上流行的第一个病毒。
  - 1988年罗伯特·塔潘·莫里斯（美国前国家安全局首席科学家罗伯特·莫里斯的儿子）编写Morris蠕虫。

计算机病毒定义

- 《中华人民共和国计算机信息系统安全保护条例》中明确定义：
  - 病毒是指“编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

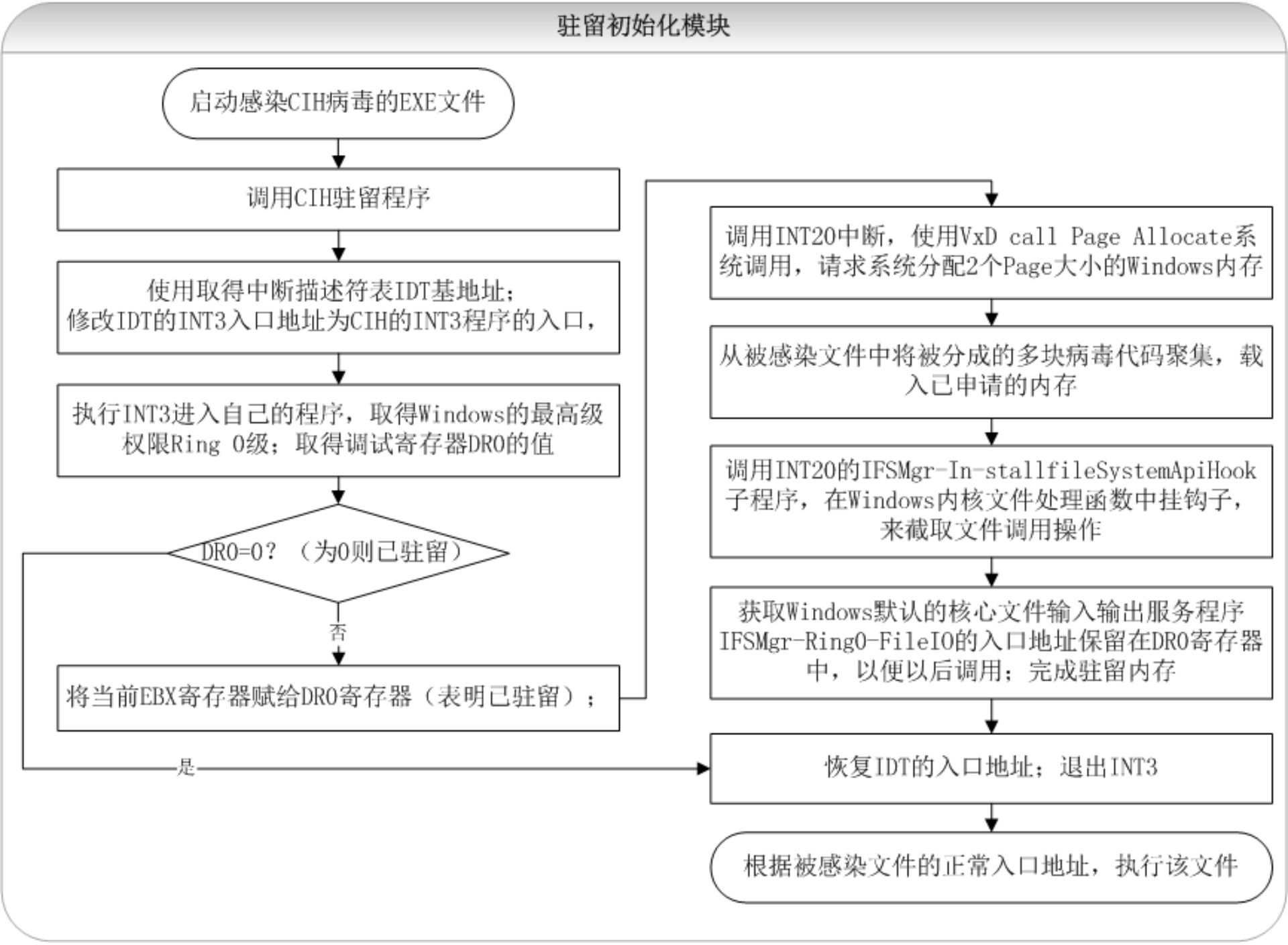
- 计算机病毒特征
  （1）非授权性
  （2）寄生性
  （3）传染性
  （4）潜伏性
  （5）破坏性
  （6）触发性

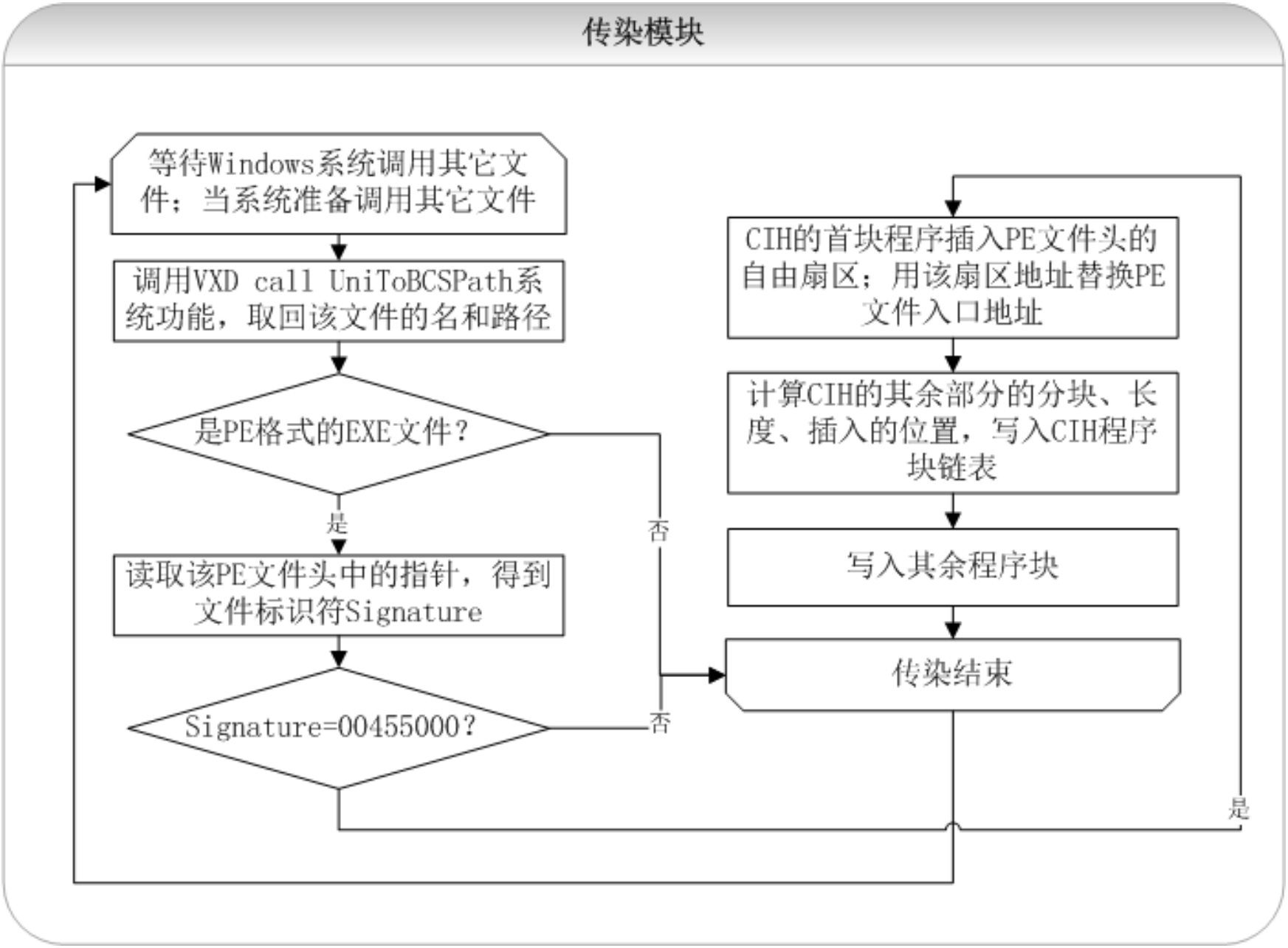
- 计算机病毒发展新的趋势
  ① 无国界
  ② 多样化
  ③ 破坏性更强
  ④ 智能化
  ⑤ 更加隐蔽化

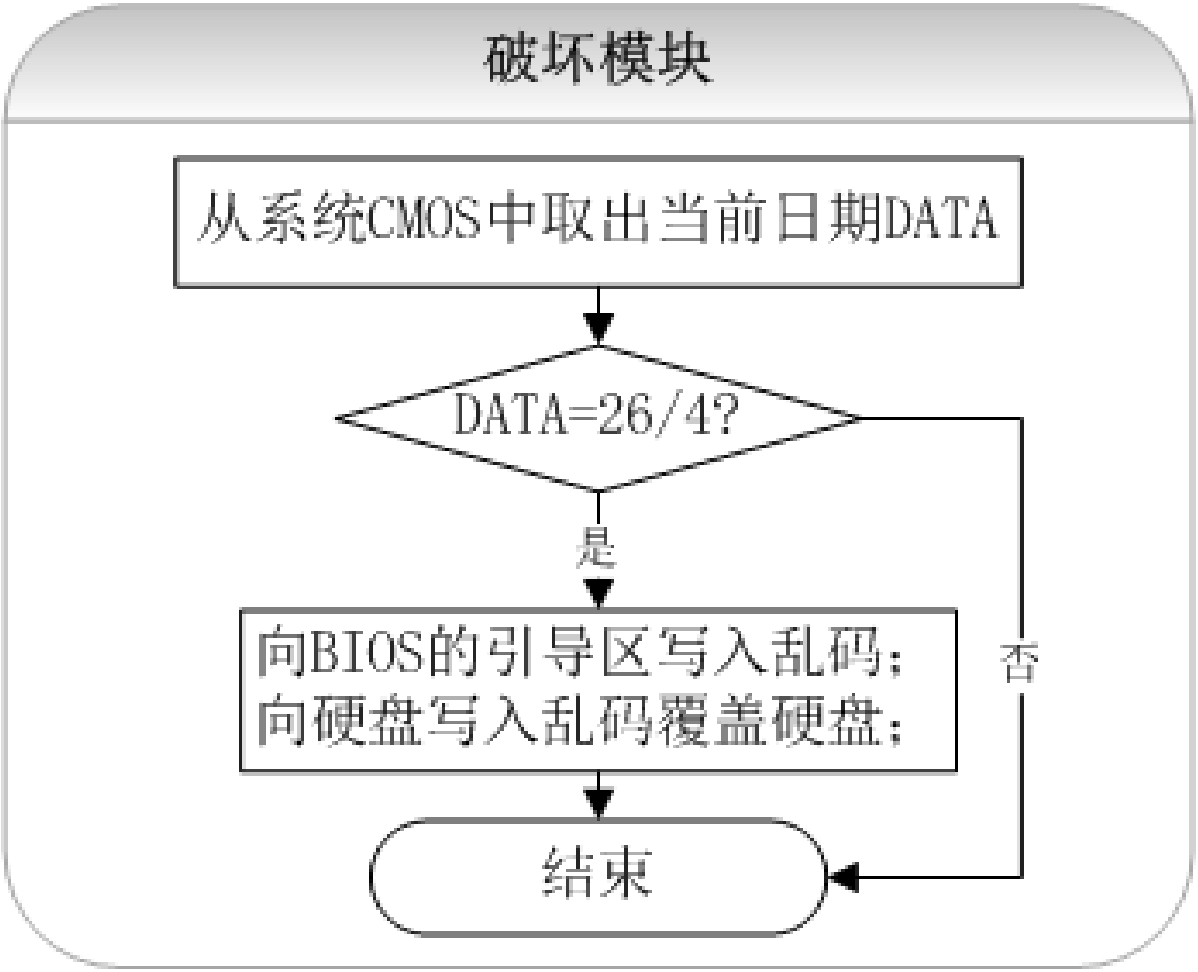
- 计算算机病毒可以根据其工作原理和传播方式划分成
  ① 传统病毒
  ② 蠕虫病毒
  ③ 木马

6.2.2 传统病毒

- 传统病毒的代表
  - 巴基斯坦智囊（Brain）、大麻、磁盘杀手（DISK KILLER）、CIH等。
- 传统病毒一般有三个主要模块组成，包括启动模块、传染模块和破坏模块。
- CIH
  - 感染Windows95/98环境下PE格式的EXE文件（第一例）
  - 病毒发作时直接攻击和破坏计算机硬件系统。
  - 该病毒通过文件复制进行传播。
  - 计算机开机后，运行了带病毒的文件，其病毒就驻留在Wnidows核心内存里，
  - 组成：初始化驻留模块、传染模块和破坏模块。


驻留初始化模块
启动感染CIH病毒的EXE文件
调用CIH驻留程序
使用取得中断描述符表IDT基地址；
修改IDT的INT3入口地址为CIH的INT3程序的入口，
执行INT3进入自己的程序，取得Windows的最高级权限Ring 0级；取得调试寄存器DR0的值
DR0=0？（为0则已驻留）
否
将当前EBX寄存器赋给DR0寄存器（表明已驻留）；
是
调用INT20中断，使用VxD call Page Allocate系统调用，请求系统分配2个Page大小的Windows内存
从被感染文件中将被分成的多块病毒代码聚集，载入已申请的内存
调用INT20的IFSMgr-In-stallfileSystemApiHook子程序，在Windows内核文件处理函数中挂钩子，来截取文件调用操作
获取Windows默认的核心文件输入输出服务程序IFSMgr-Ring0-FileIO的入口地址保留在DR0寄存器中，以便以后调用；完成驻留内存
恢复IDT的入口地址；退出INT3
根据被感染文件的正常入口地址，执行该文件


传染模块
等待Windows系统调用其它文件；当系统准备调用其它文件
调用VXD call UniToBCSPath系统功能，取回该文件的名和路径
是PE格式的EXE文件？
是
否
读取该PE文件头中的指针，得到文件标识符Signature
Signature=00455000?
否
CIH的首块程序插入PE文件头的自由扇区；用该扇区地址替换PE文件入口地址
计算CIH的其余部分的分块、长度、插入的位置，写入CIH程序块链表
写入其余程序块
传染结束
是


破坏模块
从系统CMOS中取出当前日期DATA
DATA=26/4?
是
否
向BIOS的引导区写入乱码；
向硬盘写入乱码覆盖硬盘；
结束

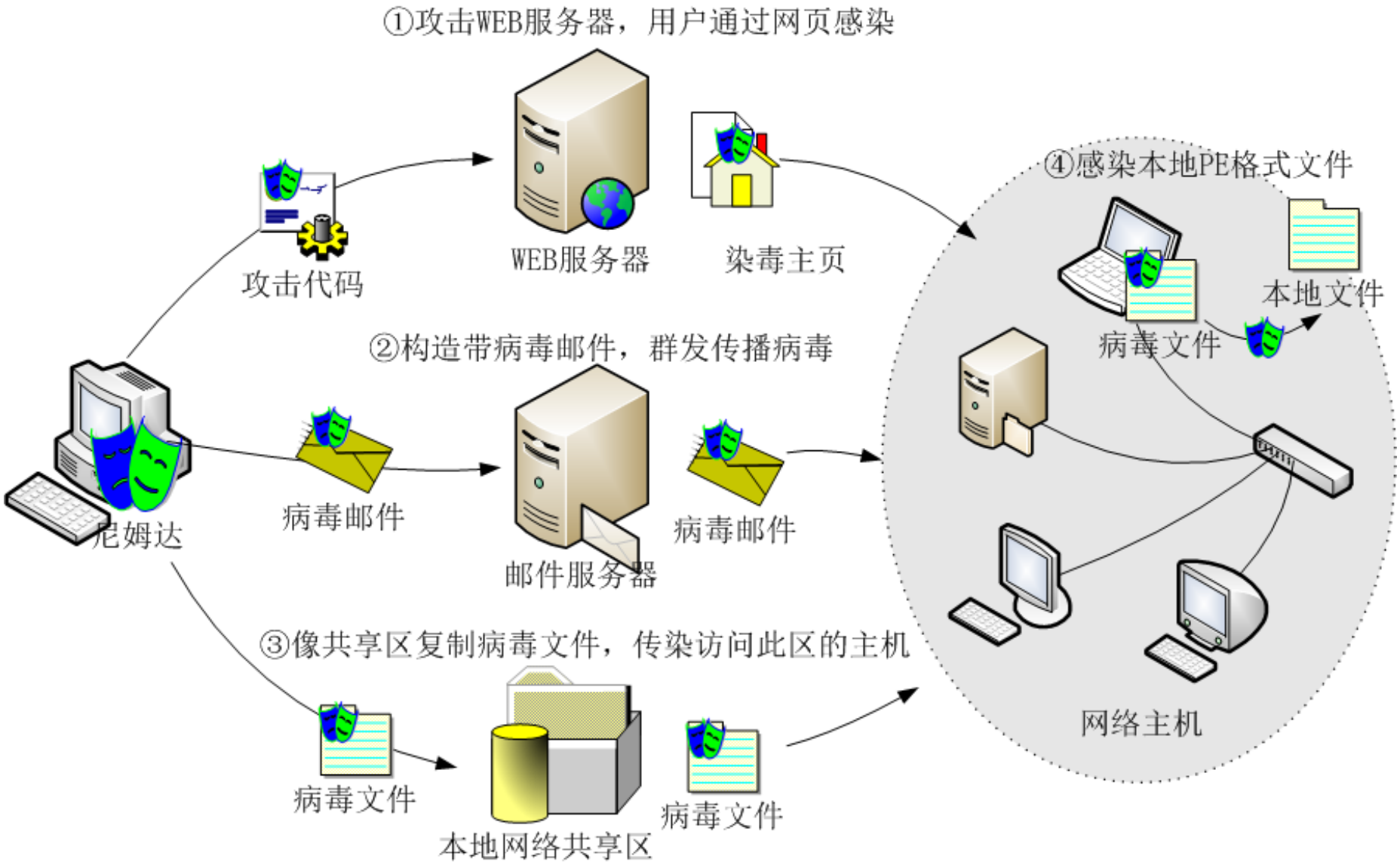
6.2.3蠕虫病毒

- 蠕虫与传统病毒的区别：
  - 传统病毒是需要的寄生的，通过感染其它文件进行传播。
  - 蠕虫病毒一般不需要寄生在宿主文件中，传播途径主要包括局域网内的共享文件夹、电子邮件、网络中的恶意网页和大量存在着漏洞的服务器等。
  - 可以说蠕虫病毒是以计算机为载体，以网络为攻击对象。
- 蠕虫病毒能够利用漏洞，分为软件漏洞和人为缺陷
  - 软件漏洞主要指程序员由于习惯不规范、错误理解或想当然，在软件中留下存在安全隐患的代码
  - 人为缺陷主要指的是计算机用户的疏忽，这就是所谓的社会工程学（Social Engineering）问题。

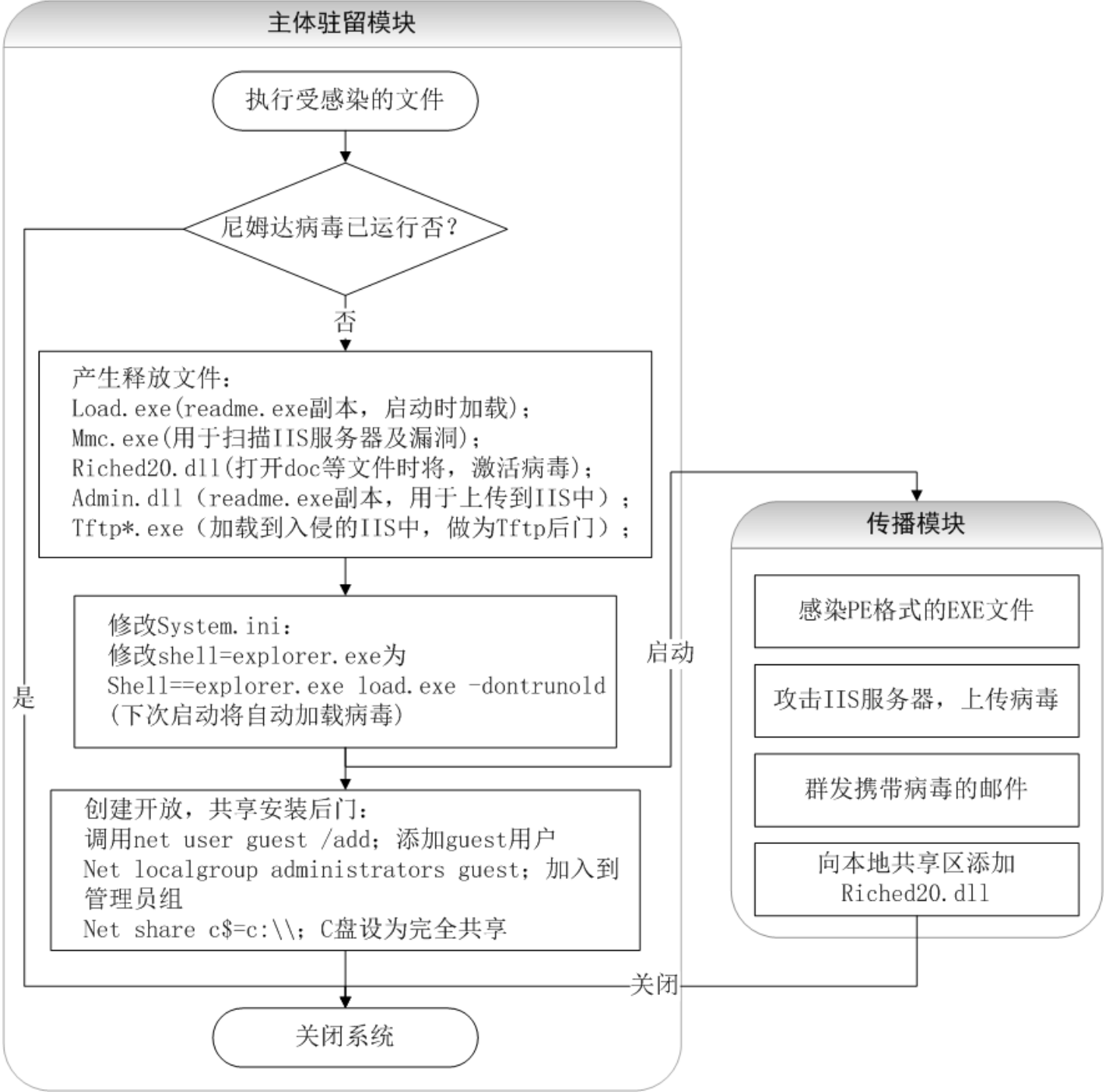
尼姆达蠕虫Worms.Nimda

- 2001年9月18日尼姆达病毒在全球蔓延，它能够通过多种传播渠道进行传播，传染性极强，同时破坏力也极大。
  - 尼姆达病毒是一个精心设计的蠕虫病毒，其结构复杂堪称近年来之最。
  - 尼姆达病毒激活后，使用其副本替换系统文件；将系统的各驱动器设为开放共享，降低系统安全性；创建Guest账号并将其加入到管理员组中，安装Guest用户后门。
  - 由于尼姆达病毒通过网络大量传播，产生大量异常的网络流量和大量的垃圾邮件，网络性能势必受到严重影响。

Nimda 传播途径


①攻击WEB服务器，用户通过网页感染
攻击代码
WEB服务器
染毒主页
④感染本地PE格式文件
本地文件
病毒文件
②构造带病毒邮件，群发传播病毒
尼姆达
病毒邮件
邮件服务器
病毒邮件
③像共享区复制病毒文件，传染访问此区的主机
病毒文件
本地网络共享区
病毒文件
网络主机

尼姆达病毒程序


主体驻留模块
执行受感染的文件
尼姆达病毒已运行否?
否
是
产生释放文件:
Load.exe(readme.exe副本，启动时加载);
Mmc.exe(用于扫描IIS服务器及漏洞);
Riched20.dll(打开doc等文件时将，激活病毒);
Admin.dll（readme.exe副本，用于上传到IIS中）;
Tftp*.exe（加载到入侵的IIS中，做为Tftp后门）;
修改System.ini:
修改shell=explorer.exe为
Shell==explorer.exe load.exe -dontrunold
(下次启动将自动加载病毒)
启动
创建开放，共享安装后门:
调用net user guest /add；添加guest用户
Net localgroup administrators guest；加入到管理员组
Net share c$=c:\\；C盘设为完全共享
关闭
关闭系统
传播模块
感染PE格式的EXE文件
攻击IIS服务器，上传病毒
群发携带病毒的邮件
向本地共享区添加Riched20.dll

防范及清除

- 感染的用户应重新安装系统，以便彻底清除其它潜在的后门。如不能立刻重装系统，可参考下列步骤来清除蠕虫或者防止被蠕虫攻击：
  ① 下载IE和IIS的补丁程序到受影响的主机上；
  ② 安装杀毒软件和微软的CodeRedII清除程序；
  ③ 备份重要数据；
  ④ 断开网络连接(例如拔掉网线)；
  ⑤ 执行杀毒工作，清除CodeRedII蠕虫留下的后门；
  ⑥ 安装IE和IIS的补丁；
  ⑦ 重启系统，再次运行杀毒软件以确保完全清除蠕虫。

6.2.4 木马

- 木马病毒，“木马计”，伪装潜伏的网络病毒。
  - 1986年的PC-Write木马是世界上第一个计算机木马
  - 木马是有隐藏性的、传播性的可被用来进行恶意行为的程序，因此，也被看作是一种计算机病毒。
  - 木马一般不会直接对电脑产生危害，以控制电脑为目的，当然电脑一旦被木马所控制，后果不堪设想。
- 木马的传播（种木马或植入木马）方式
  - 主要通过电子邮件附件、被挂载木马的网页以及捆绑了木马程序的应用软件。
  - 木马被下载安装后完成修改注册表、驻留内存、安装后门程序、设置开机加载等，甚至能够使杀毒程序、个人防火墙等防范软件失效。

木马病毒分类

（1）盗号类木马

（2）网页点击类木马

（3）下载类木马

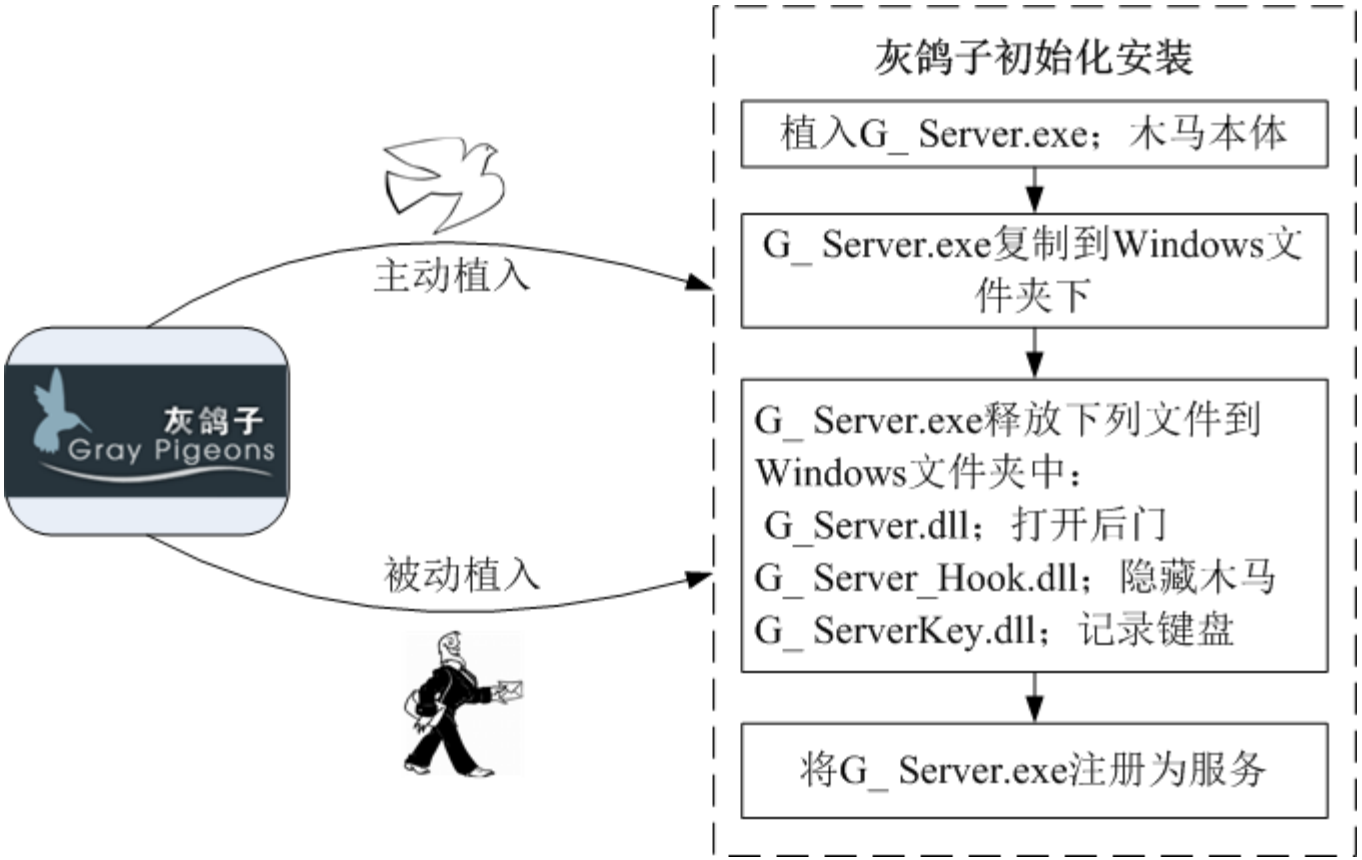
（4）代理类木马

木马病毒程序组成

- 控制端程序(客户端)
  - 是黑客用来控制远程计算机中的木马的程序；
- 木马程序（服务器端）
  - 是木马病毒的核心，是潜入被感染的计算机内部、获取其操作权限的程序；
- 木马配置程序
  - 通过修改木马名称、图标等来伪装隐藏木马程序，并配置端口号、回送地址等信息确定反馈信息的传输路径。

灰鸽子的植入方法

- 被动植入是指植入过程必须依赖受害用户的手工操作；
- 主动植入是将灰鸽子程序通过程序自动安装到目标系统。



灰鸽子的隐藏技术

- 隐藏文件
- 隐藏进程
- 隐藏通讯
  - 通讯端口复用技术是指将自己的通讯直接绑定到正常用户进程的端口，接收数据后，根据包格式判断是不是自己的，如果是它的，自己处理，否则通过127.0.0.1的地址交给真正的服务器应用进行处理。
  - 反弹端口技术是指木马程序启动后主动连接客户，为了隐蔽起见，控制端的被动端口一般设置为80端口。对内部网络到外部网络的访问请求，防火墙一般不进行过于严格的检查，加之其连接请求有可能伪造成对外部资源的正常访问，因此可以通过防火墙。

客户端程序

- 定制生成服务器端程序。
  - 首先利用客户端程序配置生成一个服务器端程序文件，服务器端文件的名字默认为G_ Server.exe，然后开始在网络中传播植入这个程序。
- 控制远程的服务器端。
  - 当木马植入成功后，系统启动时木马就会加载运行，然后反弹端口技术主动连接客户控制端。
- 客户控制端程序的功能：
  - 对远程计算机文件管理
  - 远程控制命令
  - 捕获屏幕，实时控制
  - 注册表模拟器

6.2.5 病毒防治

- 病毒防治技术略滞后于病毒技术
- 对于大多数计算机用户来说，防治病毒首先需要选择一个有效的防病毒产品，并及时进行产品升级。
- 计算机病毒防治技术主要包括:
  - 检测、清除、预防和免疫。
  - 检测和清除是根治病毒的有力手段，
  - 预防和免疫也是保证计算机系统安全的重要措施

检测

- 病毒检测方法主要包括：特征代码法、校验和法、行为监测法以及软件模拟法等。
- 特征代码法
  - 特征代码查毒就是检查文件中是否含有病毒数据库中的病毒特征代码。
- 校验和法
  - 对正常状态下的重要文件进行计算，取得其校验和，以后定期检查这些文件的校验和与原来保存的校验和是否一致。

- 行为监测法
  - 利用病毒的特有行为特征来监测病毒的方法，称为行为监测法。当一个可疑程序运行时，监视其行为，如果发现了病毒行为，立即报警。
- 软件模拟法
  - 软件模拟法是为了对付多态型病毒。软件模拟法是通过模拟病毒的执行环境，为其构造虚拟机，然后在虚拟机中执行病毒引擎解码程序，安全地将多态型病毒解开并还原其本来面目，再加以扫描。软件模拟法的优点是可识别未知病毒、病毒定位准确、误报率低；缺点是检测速度受到一定影响、消耗系统资源较高。

计算机中毒的常见症状

- 系统运行速度减慢；
- 系统经常无故发生死机
- 文件长度发生变化；
- 存储的容量异常减少；
- 丢失文件或文件损坏；
- 屏幕上出现异常显示；
- 系统的蜂鸣器出现异常声响；
- 磁盘卷标发生变化；
- 系统不识别硬盘；
- 对存储系统异常访问；
- 键盘输入异常；
- 文件的日期、时间、属性等发生变化；
- 文件无法正确读取、复制或打开；
- 命令执行出现错误；
- WINDOWS操作系统无故频繁出现错误；
- 系统异常重新启动；
- 一些外部设备工作异常；
- 出现异常的程序驻留内存

清除

- 清除病毒主要分为
  - 使用防病毒软件和手工清除病毒两种方法。
  - 防病毒软件由安全厂商精心研制，可以有效查杀绝大多数计算机病毒，多数用户应采用防病毒软件来清除病毒。
    - 防病毒软件对检测到的病毒一般采取三种处理方案，分别是清除、隔离和删除。
    - 清除是指在发现文件被感染病毒时，采取的清除病毒并保留文件的动作。
    - 隔离是指在发现病毒后，无法确认清除动作会带来什么后果，又不想直接删除文件，故采取监视病毒并阻止病毒运行的方法。
  - 某类病毒清除失败、删除失败、隔离失败，对个人用户来讲，格式化硬盘、重建系统可能就是最后的有效选择。

蠕虫、木马等病毒的清除

- 结束所有可疑进程
- 删除病毒文件并恢复注册表
- 内核级后门的清除
- 重启后扫描
  - 完成了上述三步，随后需要重新启动系统，并使用带有最新病毒库的防病毒软件对全盘进行扫描（这一步非常重要，做不好的话前功尽弃）

预防

- 安装防毒软件
  - 打开你的防毒软件的自动升级服务，定期扫描计算机
- 注意软盘、光盘以及U盘等存储媒介
  - 在使用软盘、光盘、U盘或活动硬盘前，病毒扫描
- 关注下载安全
  - 下载要从比较可靠的站点进行，下载后做病毒扫描。
- 关注电子邮件安全
  - 来历不明的邮件决不要打开，决不要轻易运行附件
- 使用基于客户端的防火墙
- 警惕欺骗性的病毒
- 备份

免疫

- 计算机病毒免疫
  - 提高计算机系统对计算机病毒的抵抗力，从而达到防止病毒侵害的目的
  - 一是提高计算机系统的健壮性，二是给计算机注射“病毒疫苗”。
  - 提高系统健壮性的主要途径包括以下内容：
    - 及时升级操作系统，保证系统安装最新的补丁；
    - 安装防病毒软件，及时升级病毒定义文件和防病毒引擎；
    - 定期扫描系统和磁盘文件；
    - 打开个人防火墙；
    - 使用软盘或U盘写保护
    - 重要的数据信息写入只读光盘；

注射“病毒疫苗”

- 实施免疫的主要方法包括以下几个方面：
  - 感染标识免疫
    - 人为地为正常对象中加上病毒感染标识，使计算机病毒误以为已经感染从而达到免疫的目的。
  - 文件扩展名免疫
    - 将扩展名改为非COM、EXE、SYS、BAT等形式，
    - 将系统默认的可执行文件的后缀名改为非COM、EXE、SYS、BAT等形式。
  - 外部加密免疫
    - 外部加密免疫是指在文件的存取权限和存取路径上进行加密保护，以防止文件被非法阅读和修改。
  - 内部加密免疫
    - 对文件内容加密变换后进行存储，在使用时再进行解密。

6.3 网络入侵

- 1980年，James P Anderson首次提出了“入侵”的概念，
  - “入侵”是指在非授权的情况下，试图存取信息、处理信息或破坏系统，以使系统不可靠或不可用的故意行为。
  - 网络入侵一般是指具有熟练编写、调试和使用计算机程序的技巧的人，利用这些技巧来获得非法或未授权的网络或文件的访问，进入内部网的行为。
  - 对信息的非授权访问一般被称为破解cracking。

网络入侵

- 一般分：前期准备、实施入侵和后期处理。
  - 准备阶段需要完成的工作主要包括明确入侵目的、确定入侵对象以及选择入侵手段，
    - 入侵目的一般可分为控制主机、瘫痪主机和瘫痪网络；
    - 入侵对象一般分为主机和网络两类；
    - 根据目的和后果分为：拒绝服务攻击、口令攻击、嗅探攻击、欺骗攻击和利用型攻击。
  - 实施入侵阶段是真正的攻击阶段，主要包括扫描探测和攻击。
    - 扫描探测主要用来收集信息，为下一步攻击奠定基础；
    - 攻击：根据入侵目的、采用相应的入侵手段向入侵对象实施入侵。
  - 后期处理主要是指由于大多数入侵攻击行为都会留下痕迹，攻击者为了清除入侵痕迹而进行现场清理。

6.3.1 拒绝服务攻击

- 拒绝服务攻击DoS (Denial of Service)
  - DoS并不是某一种具体的攻击方式，而是攻击所表现出来的结果最终使得目标系统因遭受某种程度的破坏而不能继续提供正常的服务，甚至导致物理上的瘫痪或崩溃。
- 通常拒绝服务攻击可分为两种类型，
  - 第一类攻击是利用网络协议的缺陷，通过发送一些非法数据包致使主机系统瘫痪；
  - 第二类攻击是通过构造大量网络流量致使主机通讯或网络堵塞，使系统或网络不能响应正常的服务。

Ping of Death

- TCP/IP的规范，一个包的长度最大为65536字节。
- 利用多个IP包分片的叠加能做到构造长度大于65536的IP数据包。
- 攻击者通过修改IP分片中的偏移量和段长度，使系统在接收到全部分段后重组报文时总的长度超过了65535字节。
- 一些操作系统在对这类超大数据包的处理上存在缺陷，当安装这些操作系统的主机收到了长度大于65536字节的数据包时，会出现内存分配错误，从而导致TCP/IP堆栈崩溃，造成死机。

Tear drop

- IP数据包在网络传递时，数据包可能被分成多个更小的IP分片。
- 攻击者可以通过发送两个（或多个）IP分片数据包来实现Tear Drop攻击。
- 第一个IP分片包的偏移量为0，长度为N，第二个分片包的偏移量小于N，未超过第一个IP分片包的尾部，这就出现了偏移量重叠现象。
- 一些操作系统无法处理这些偏移量重叠的IP分片的重组，TCP/IP堆栈会出现内存分配错误，造成操作系统崩溃。

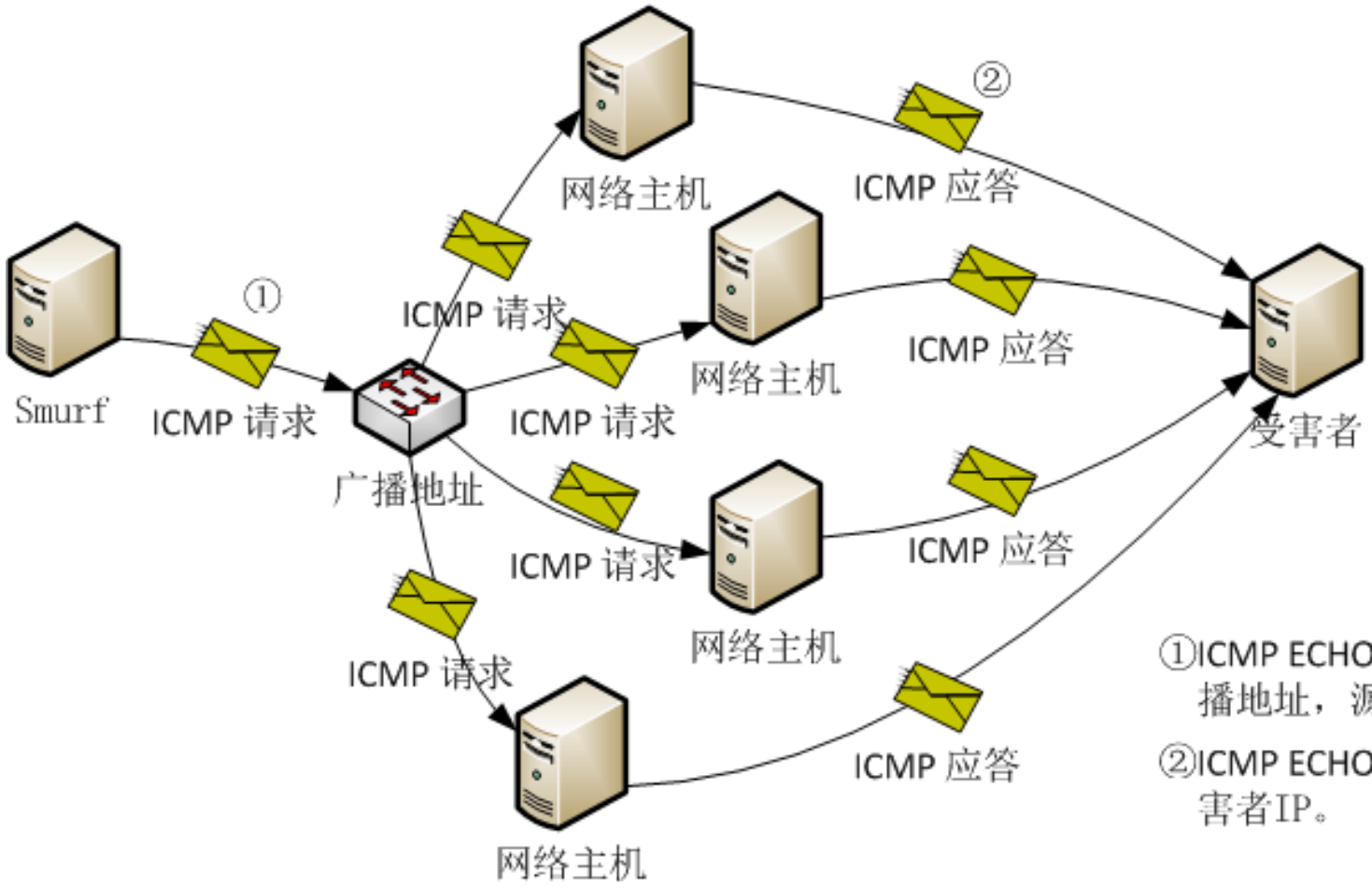
Syn Flood

- 攻击者伪造TCP的连接请求，向被攻击的设备正在监听的端口发送大量的SYN连接请求报文；
- 被攻击的设备按照正常的处理过程，回应这个请求报文，同时为它分配了相应的资源。
- 攻击者不需要建立TCP连接，因此服务器根本不会接收到第三个ACK报文，现有分配的资源只能等待超时释放。
- 如果攻击者能够在超时时间到达之前发出足够多的攻击报文，被攻击的系统所预留所有TCP缓存将被耗尽。

Smurf攻击

- Smurf攻击是以最初发动这种攻击的程序Smurf来命名的，这种攻击方法结合使用了IP地址欺骗和ICMP协议。
- 当一台网络主机通过广播地址将ICMP ECHO请求包发送给网络中的所有机器，网络主机接收到请求数据包后，会回应一个ICMP ECHO响应包，这样发送一个包会收到许多的响应包。
- Smurf构造并发送源地址为受害主机地址、目的地址为广播地址的ICMP ECHO请求包，收到请求包的网络主机会同时响应并发送大量的信息给受害主机，致使受害主机崩溃。
- 如果Smurf攻击将回复地址设置成受害网络的广播地址，则网络中会充斥大量的ICMP ECHO响应包，导致网络阻塞。

Smurf攻击过程示意图



①ICMP ECHO请求包：目的地址为广播地址，源地址为受害者IP；

②ICMP ECHO应答包：目的地址为受害者IP。

电子邮件炸弹

- 实施电子邮件炸弹攻击的特殊程序称为Email Bomber。
  - 邮箱容量是有限的，用户在短时间内收到成千上万封电子邮件，每个电子邮件的容量也比较大，那么经过一轮邮件炸弹轰炸后电子邮邮箱的容量可能被占满。
  - 另外一方面，这些电子邮件炸弹所携带的大容量信息不断在网络上来回传输，很容易堵塞网络；
  - 邮件服务器需要不停地处理大量的电子邮件，如果承受不了这样的疲劳工作，服务器随时有崩溃的可能。

DDoS

- DDoS攻击就是很多DoS攻击源一起攻击某台服务器或网络，迫使服务器停止提供服务或网络阻塞。
- DDoS攻击需要众多攻击源，而黑客获得攻击源的主要途径就是传播木马，网络计算机一旦中了木马，这台计算机就会被后台操作的人控制，也就成了所谓的“肉鸡”，即黑客的帮凶。
- 使用“肉鸡”进行DDoS攻击还可以在一定程度上保护攻击者，使其不易被发现。

对于DoS的防御

- 及时为系统升级，减少系统漏洞，很多DoS攻击对于新的操作系统已经失效，如Ping of Death攻击；
- 关掉主机或网络中的不必要的服务和端口，如对于非WEB主机关掉80端口；
- 局域网应该加强防火墙和入侵检测系统的应用和管理，过滤掉非法的网络数据包。

6.3.2 口令攻击

- 口令攻击过程一般包括以下几个步骤。
  - 步骤一、获取目标系统的用户帐号及其它有关信息；
    - 获取目标系统的用户帐号及其它有关信息一般可以利用一些网络服务来实现，如Finger、Whois、LDAP等信息服务。
  - 步骤二、根据用户信息猜测用户口令；
  - 步骤三、采用字典攻击方式探测口令；
    - 使用一些程序，自动地从电脑字典中取出一个单词，作为用户的口令输入给远端的主机，进入系统。
    - 如果口令错误，就按序取出下一个单词，进行下一个尝试。并一直循环下去，直到找到正确的口令或字典的单词试完为止。
    - 由于这个破译过程由计算机程序来自动完成，几个小时就可以把字典的所有单词都试一遍。
  - 步骤四、探测目标系统的漏洞，伺机取得口令文件，破解取得用户口令。

- 系统中可以用作口令的字符有95个，
  - 10个数字、33个标点符号、52个大小写字母。
  - 采用任意5个字母加上一个数字或符号则可能的排列数约为163亿，即$52^5 \times 43=16,348,773,000$。
- 这个数字对于每秒可以进行上百万次浮点运算的计算机并不是什么困难问题，也就是说一个6位的口令将不是安全的
- 一般建议使用10位以上并且是字母、数字加上标点符号的混合体。

防范口令攻击的方法

- 口令的长度不少于10个字符；
- 口令中要有一些非字母；
- 口令不在英语字典中；
- 不要将口令写下来；
- 不要将口令存于电脑文件中；
- 不要选择易猜测的信息做口令；
- 不要在不同系统上使用同一口令；
- 不要让其他人得到口令；
- 经常改变口令；
- 永远不要对自己的口令过于自信。

6.3.3 嗅探攻击

- 嗅探攻击也称为网络嗅探，是指利用计算机的网络接口截获目的地为其它计算机的数据包的一种手段。
- 网络嗅探的工具被称为嗅探器（sniffer），是一种常用的收集网络上传输的有用数据的方法，
- 嗅探攻击一般是指黑客利用嗅探器获取网络传输中的重要数据。网络嗅探也被形象地称为网络窃听。

共享网络环境

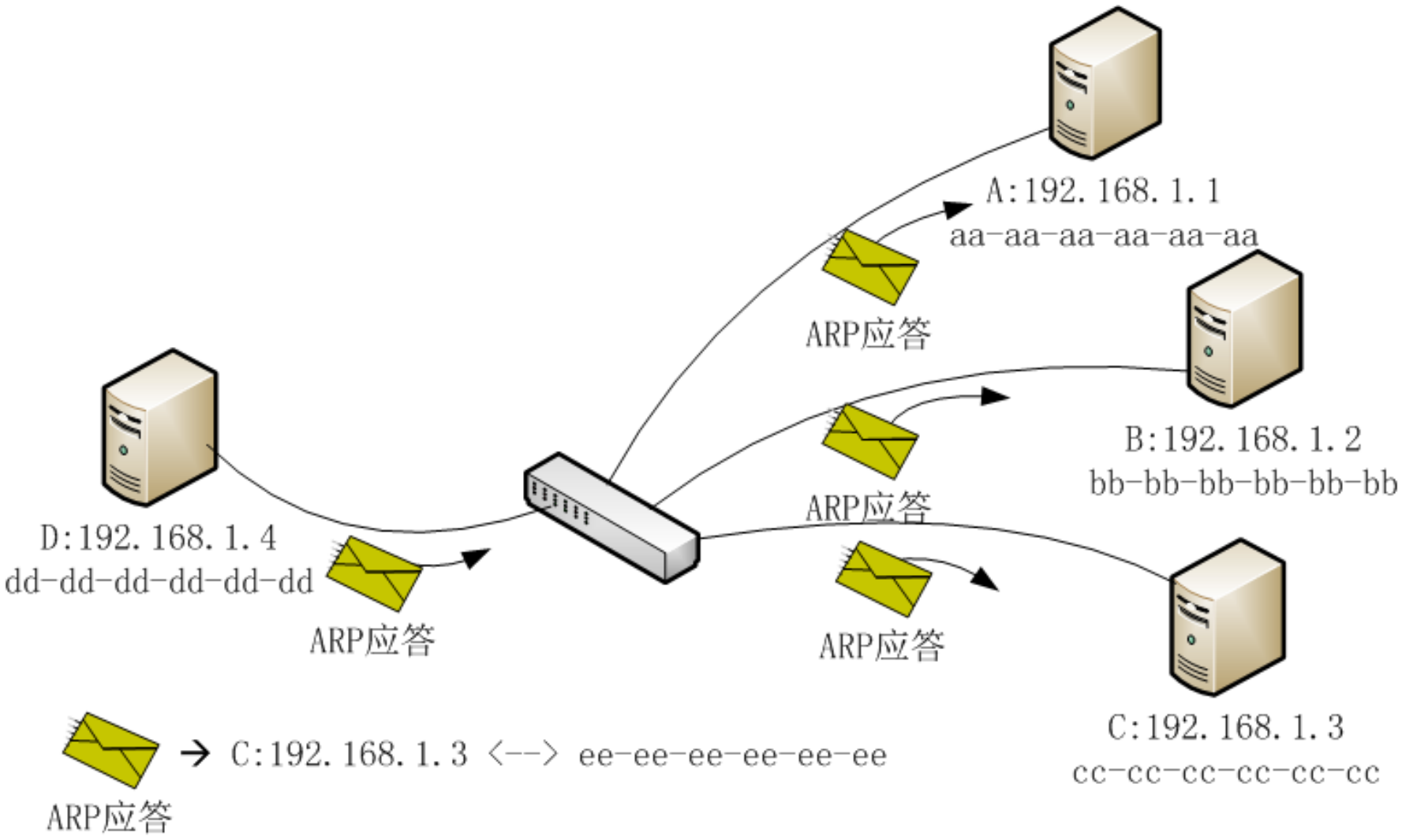
- 以太网卡共有四种工作方式：
  - 广播方式：网卡能够接收网络中的广播数据；
  - 组播方式：网卡能够接收组播数据；
  - 直接方式：只有目的网卡才能接收该数据；
  - 混杂模式：网卡能够接收一切通过它的数据。
- 如果攻击者获得其中一台主机的root权限，并将其网卡置于混杂模式，这就意味着不必打开配线盒来安装偷听设备，就可以在对共享环境下的其它计算机的通信进行窃听，在共享网络中网络通信没有任何安全性可言。

交换网络环境

- Arp协议
  - 当主机接收到ARP应答数据包的时候，就使用应答数据包内的数据对本地的ARP缓存进行更新或添加。

Internet	地址	物理地址
192.168.1.100	00-30-48-31-26-98	动态
192.168.1.101	00-00-00-00-01-89	动态
192.168.1.102	00-24-dc-b8-47-f0	动态
192.168.1.255	ff-ff-ff-ff-ff-ff	静态

Arp欺骗


A:192.168.1.1
aa-aa-aa-aa-aa-aa
ARP应答
B:192.168.1.2
bb-bb-bb-bb-bb-bb
ARP应答
D:192.168.1.4
dd-dd-dd-dd-dd-dd
ARP应答
ARP应答
C:192.168.1.3
cc-cc-cc-cc-cc-cc
→ C:192.168.1.3 <--> ee-ee-ee-ee-ee-ee
ARP应答

防范嗅探攻击

- 检测嗅探器
  - 检测混杂模式网卡来检查嗅探器的存在，AntiSniff。
- 安全的拓扑结构
  - 嗅探器只能在当前网络段上进行数据捕获。将网络分段工作进行得越细，嗅探器能够收集的信息就越少。
- 会话加密
  - 即使嗅探器嗅探到数据报文，也不能识别其内容。
- 地址绑定
  - 在客户端使用arp命令绑定网关的真实MAC地址；
  - 在交换机上做端口与MAC地址的静态绑定；
  - 在路由器上做IP地址与MAC地址的静态绑定；
  - 用静态的ARP信息代替动态的ARP信息。

6.3.4 欺骗类攻击

- 欺骗类攻击是指构造虚假的网络消息，发送给网络主机或网络设备，企图用假消息替代真实信息，实现对网络及主机正常工作的干扰破坏。
- 常见的假消息攻击有IP欺骗、ARP欺骗、DNS欺骗、伪造电子邮件等

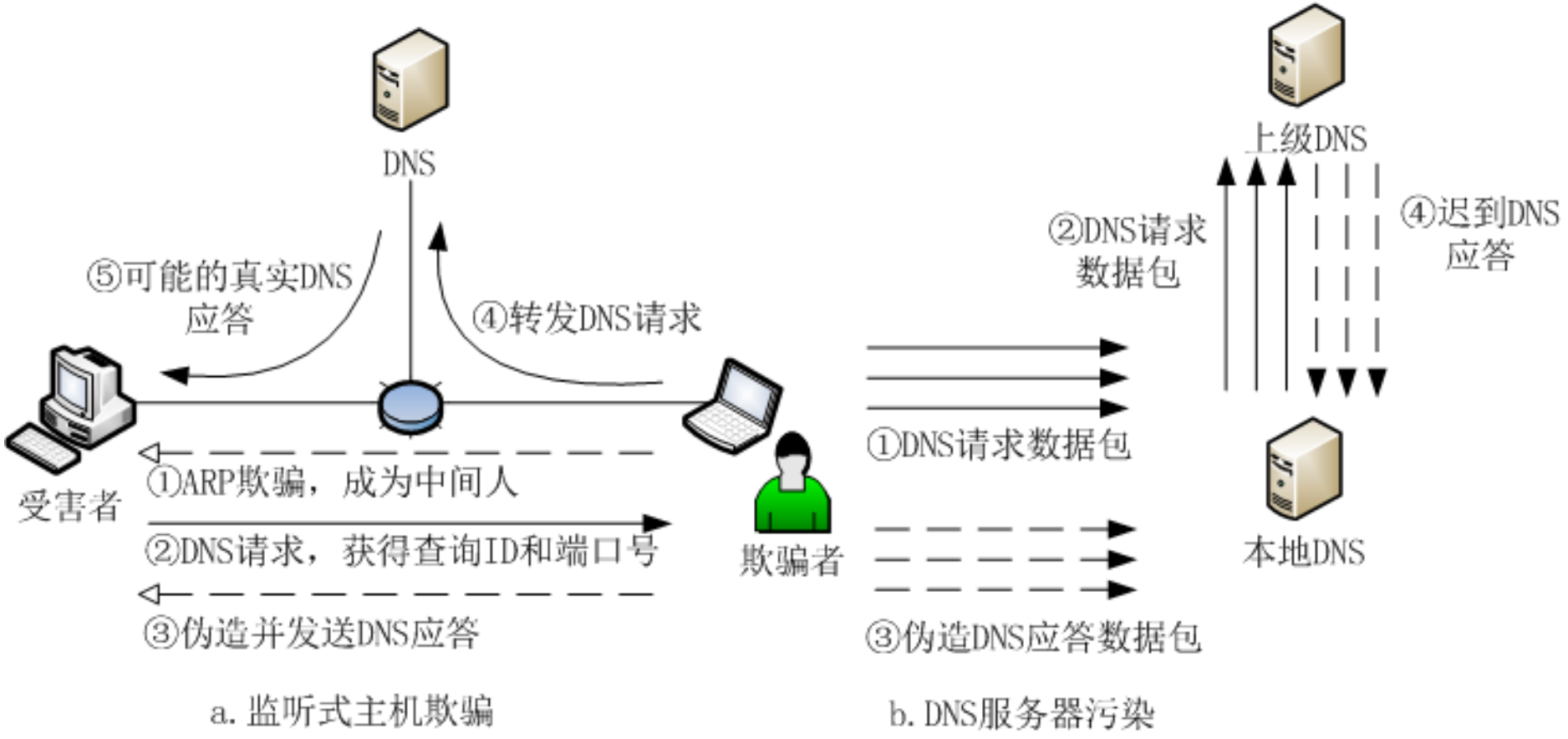
IP欺骗

- IP欺骗简单地说就是一台主机设备冒充另外一台主机的IP地址，与其它设备通信。
- IP欺骗主要是基于远程过程调用RPC的命令，比如rlogin、rcp、rsh等，
- 这些命令仅仅根据信源IP地址进行用户身份确认，以便允许或拒绝用户RPC。
- IP欺骗的目的主要是获取远程主机的信任及访问特权。

IP欺骗攻击主要步骤

- 第一步 选定目标主机并发现被该主机信任的其它主机；
- 第二步 使得被信任的主机丧失工作能力；
- 第三步 使用被目标主机信任的主机的IP地址，伪造建立TCP连接的SYN请求报文，试图以此数据报文建立与目标主机的TCP连接；
- 第四步 序列号取样和猜测。
- 第五步 使用被目标主机信任的主机的IP地址和计算出的TCP序列号，构造TCP连接的ACK报文，发送给目标主机，建立起与目标主机基于地址验证的应用连接。
  - 如果成功，攻击者可以使用一种简单的命令放置一个系统后门，以进行非授权操作。

DNS欺骗


DNS
⑤可能的真实DNS
应答
④转发DNS请求
受害者
①ARP欺骗，成为中间人
②DNS请求，获得查询ID和端口号
③伪造并发送DNS应答
欺骗者
a. 监听式主机欺骗
上级DNS
②DNS请求
数据包
④迟到DNS
应答
①DNS请求数据包
本地DNS
③伪造DNS应答数据包
b. DNS服务器污染

伪造电子邮件

- 由于SMTP并不对邮件的发送者的身份进行鉴定，攻击者可以冒充别的邮件地址伪造电子邮件。
- 攻击者伪造电子邮件的目的主要包括：
  - 攻击者想隐藏自己的身份，匿名传播虚假信息，如造谣中伤某人；
  - 攻击者想假冒别人的身份，提升可信度，如冒充领导发布通知；
  - 伪造用户可能关注的发件人的邮件，引诱收件人接收并阅读，如传播病毒、木马等。

对于欺骗类攻击的防范方法

- 抛弃基于地址的信任策略，不允许使用r类远程调用命令。
- 配置防火墙，拒绝网络外部与本网内具有相同IP地址的连接请求；过滤掉入站的DNS更新。
- 地址绑定，在网关上绑定IP地址和MAC地址；在客户端使用arp命令绑定网关的真实MAC地址命令。
- 使用PGP等安全工具并安装电子邮件证书。

6.3.5 利用型攻击

- 利用型攻击是通过非法技术手段，试图获得某网络计算机的控制权或使用权，达到利用该机从事非法行为的一类攻击行为的总称。
- 利用型攻击常用的技术手段主要包括：
  - 口令猜测、木马病毒、僵尸病毒以及缓冲区溢出等。

僵尸病毒

- 僵尸病毒（Bot）是通过特定协议的信道连接僵尸网络服务器的客户端程序，
  - 被安装了僵尸程序的机器称为僵尸主机，
  - 僵尸网络（BotNet）是由这些受控的僵尸主机依据特定协议所组成的网络。
- 僵尸病毒的程序结构与木马程序基本一致，
  - 木马程序是被控制端连接的服务器端程序。
  - 僵尸程序是向控制服务器发起连接的客户端程序。
- 僵尸病毒的传播和木马相似
  - 途径包括电子邮件、含有病毒的WEB网页、捆绑了僵尸程序的应用软件以及利用系统漏洞攻击加载等。
- 黑客经常利用其发起大规模的网络攻击，
  - 如分布式拒绝服务攻击（DDoS）、海量垃圾邮件等，

缓冲区溢出

- 缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量，溢出的数据覆盖了合法数据。
- 缓冲区溢出是一种非常普遍、非常危险的程序漏洞，在各种操作系统、应用软件中广泛存在。
- 缓冲区溢出攻击，可以导致程序运行失败、系统宕机、重新启动等后果；更为严重的是可以利用它执行非授权指令，甚至可以取得系统特权并控制主机，进行各种非法操作。

缓冲区的理论基础

- 缓冲区溢出的产生存在着必然性，现代计算机程序的运行机制、C语言的开放性及编译问题是其产生的理论基础。
  - 程序在4GB或更大逻辑地址空间内运行时，一般会被装载到相对固定的地址空间，使得攻击者可以估算用于攻击的代码的逻辑地址；
  - 程序调用时，可执行代码和数据共同存储在一个地址空间（堆栈）内，攻击者可以精心编制输入的数据，通过运行时缓冲区溢出，得到运行权；
  - CPU call调用时的返回地址和C语言函数使用的局部变量均在堆栈中保存，而且C语言不进行数据边界检察，当数据被覆盖时也不能被发现。

例子

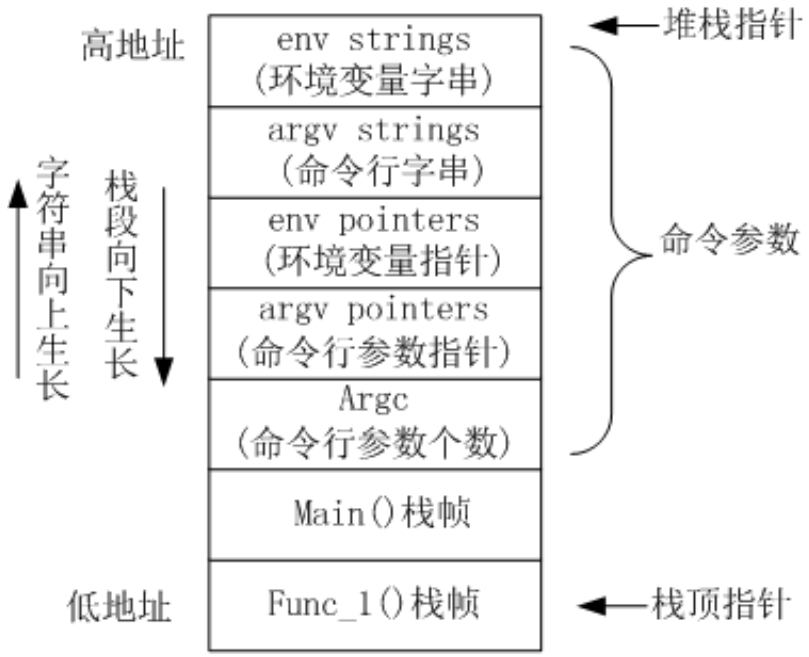
```
#include <stdio.h>
#include <string.h>
void Sayhello(char* name)
{
char tmpName [8];
strcpy(tmpName, name);
printf("Hello %s\n", tmpName);
}
```

- int main(int argc, char** argv)
- {
- Sayhello(argv[1]);
- return 0;
- }

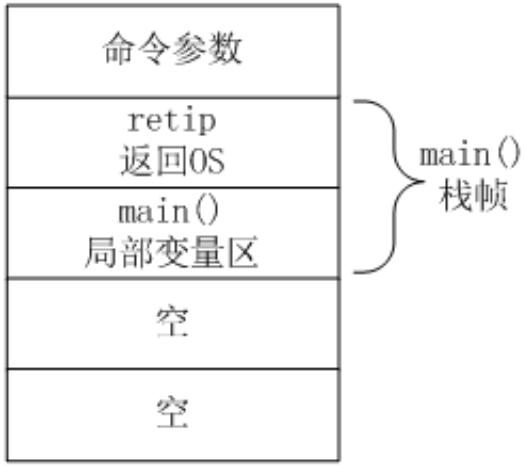
下面内容是在Linux环境下example.c程序的执行情况：

```
$ ./ example computer
Hello computer
$ ./ example computersssssssss
Hello computersssssssss
Segmentation fault (core dumped)
```

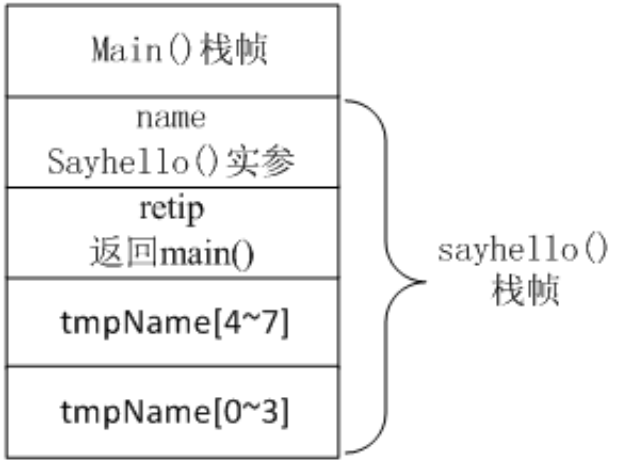
分析



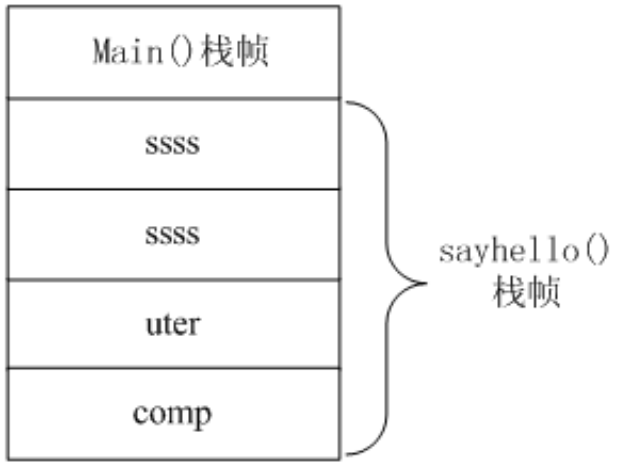
a. 程序执行时栈段分配



b. sayhello()调用之前



c. sayhello()正常调用



d. sayhello()产生溢出

6.4 诱骗类威胁

- 诱骗类威胁是指攻击者利用社会工程学的思想，利用人的弱点（如人的本能反应、好奇心、信任、贪便宜等）通过网络散布虚假信息，诱使受害者上当受骗，而达到攻击者目的的一种网络攻击行为。
- 准确地说，社会工程学不是一门科学，而是一门艺术和窍门，它利用人的弱点，以顺从你的意愿、满足你的欲望的方式，让你受骗上当。

6.4.1 网络钓鱼

- Phishing是英单词Fishing（钓鱼）和Phone（电话，因为黑客起初以电话作案）的综合体，所以被称为网络钓鱼。
- Phishing是指攻击者通过伪造以假乱真的网站和发送诱惑受害者按攻击者意图执行某些操作的电子邮件等方法，使得受害者“自愿”交出重要信息（例如银行账户和密码）的手段。

电子邮件诱骗

- 电子邮件服务是合法的Internet经典服务，攻击者进行电子邮件诱骗，一般需要经过以下几个步骤。

  第一步 选定目标用户群。

  第二步 构造欺骗性电子邮件。

  第三步 搭建欺骗性网站。

  第四步 群发邮件，等待上当的受害者。

假冒网站

- 建立假冒网站，骗取用户帐号、密码实施盗窃，这是对用户造成经济损失最大的恶劣手段。
- 为了迷惑用户，攻击者有意把网站域名注册成与真实机构的域名很相似，
  - 网址为“http: //www. 1cbc. com. cn”，而真正银行网站是“http: //www. icbc. com. cn”，

虚假的电子商务

- 攻击者建立电子商务网站，或是在比较知名、大型电子商务网站上发布虚假的商品销售信息。
- 网上交易多是异地交易，通常需要汇款。
  - 不法分子一般要求消费者先付部分款，再以各种理由诱骗消费者付余款或者其他各种名目的款项，得到钱款或被识破时，犯罪分子就销声匿迹。

6.4.2 对于诱骗类威胁的防范

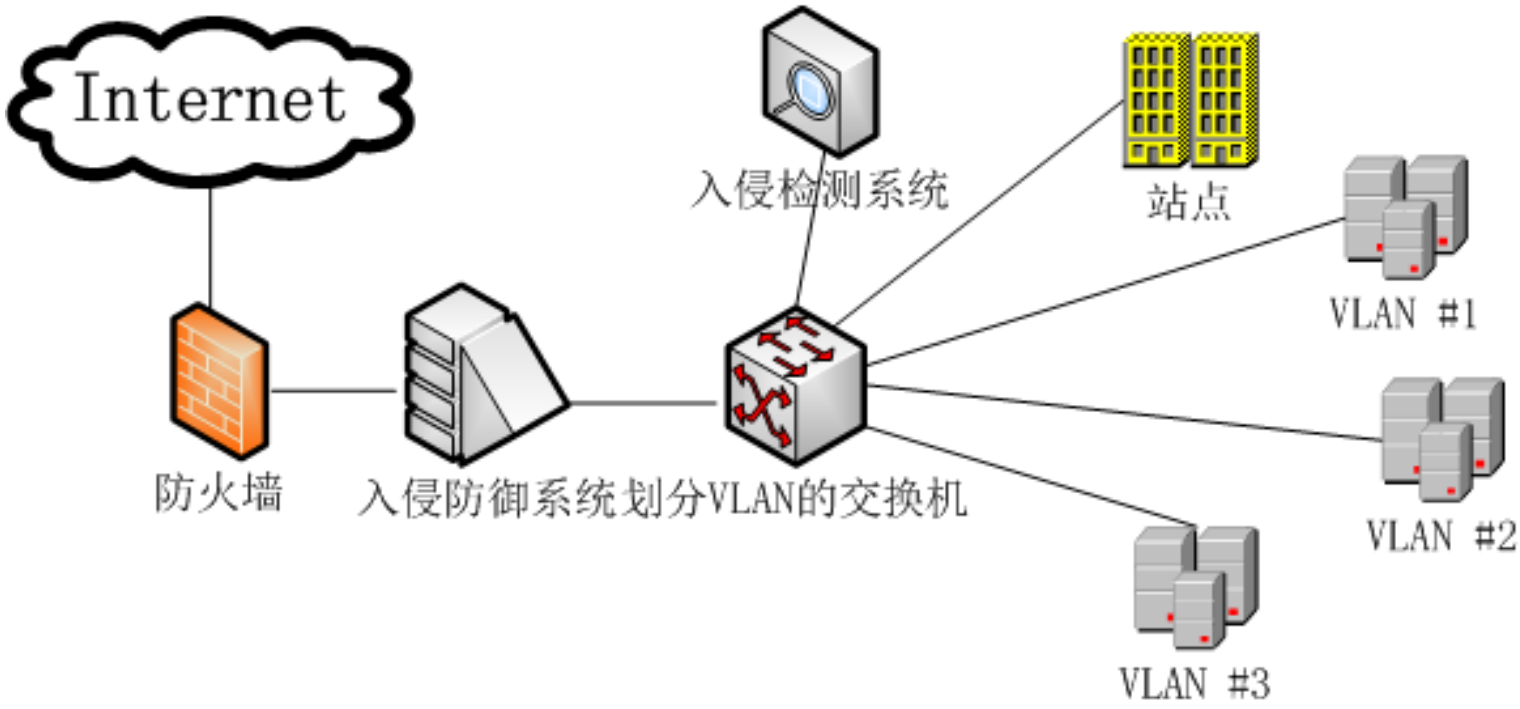
- 诱骗类威胁不属于传统信息安全的范畴，传统信息安全办法解决不了非传统信息安全的威胁。
  - 一般认为，解决非传统信息安全威胁需要运用社会工程学来反制。
  - 防范诱骗类威胁的首要方法是加强安全防范意识，多问“为什么”，减少“天上掉馅饼”的心理，那么绝大多数此类诱骗行为都不能得逞。
- 另外，用户还应该注意以下几点：
  - 确认对方身份
  - 慎重对待个人信息
  - 谨防电子邮件泄密
  - 注意网站的URL地址

第7章 网络防御

翟健宏

7.1 概述

- 网络防御是一个综合性的安全工程，不是几个网络安全产品能够完成的任务。
  - 防御需要解决多层面的问题，除了安全技术之外，安全管理也十分重要，实际上提高用户群的安全防范意识、加强安全管理所能起到效果远远高于应用几个网络安全产品。



7.2 防火墙

- 防火墙指的是一个由软件和硬件设备组合而成、在内部网络和外部网络之间构造的安全保护屏障，从而保护内部网络免受外部非法用户的侵入。
- 简单地说，防火墙是位于两个或多个网络之间，执行访问控制策略的一个或一组系统，是一类防范措施的总称。

7.2.1 防火墙概述

- 防火墙设计目标是有效地控制内外网之间的网络数据流量，做到御敌于外。
- 防火墙的结构和部署考虑:
  ① 内网和外网之间的所有网络数据流必须经过防火墙；
    - 阻塞点可以理解为连通两个或多个网络的唯一路径上的点，当这个点被删除后，各网络之间不在连通。
  ② 只有符合安全政策的数据流才能通过防火墙。
    - 要求防火墙具有审计和管理的功能，具有可扩展性和健壮性。

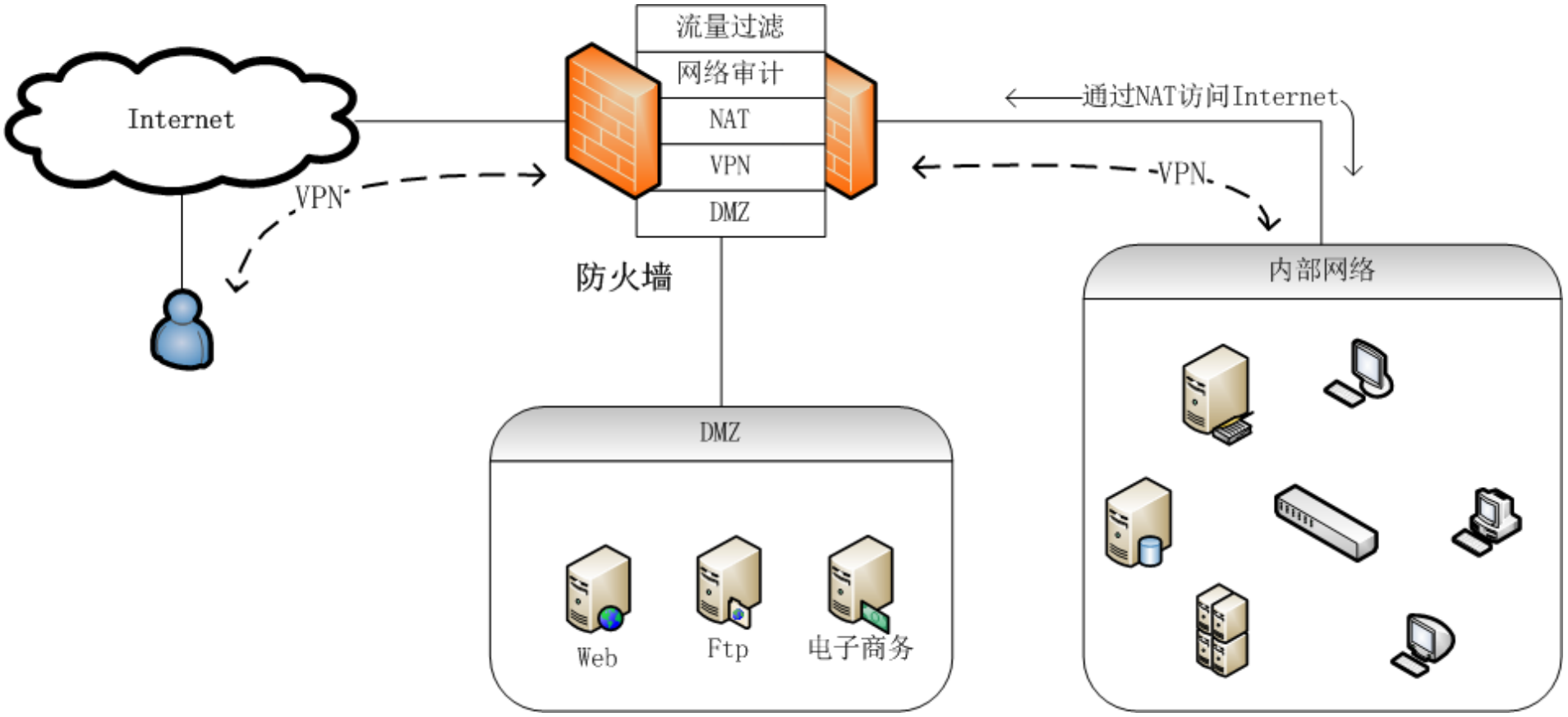
分类

- 从应用对象上，分为企业防火墙和个人防火墙
  - 企业防火墙的主要作用是保护整个企业网络免受外部网络的攻击；
  - 个人防火墙则是保护个人计算机系统的安全。
- 从存在形式上，可以分为硬件防火墙和软件防火墙
  - 硬件防火墙采用特殊的硬件设备，有较高性能，可做为独立的设备部署，企业防火墙多数是硬件防火墙；
  - 软件防火墙是一套安装在某台计算机系统上来执行防护任务的安全软件，个人防火墙都是软件防火墙。

防火墙主要作用

- 网络流量过滤
  - 通过在防火墙上进行安全规则配置，可以对流经防火墙的网络流量进行过滤。
- 网络监控审计
  - 防火墙记录访问并生成网络访问日志，提供网络使用情况的统计数据。
- 支持NAT部署
  - NAT（Network Address Translation）是网络地址翻译的缩写，是用来缓解地址空间短缺的主要技术之一
- 支持DMZ
  - DMZ是英文“Demilitarized Zone”的缩写,它是设立在非安全系统与安全系统之间的缓冲区。
- 支持VPN
  - 通过VPN，企业可以将分布在各地的局域网有机地连成一个整体。

典型企业防火墙应用

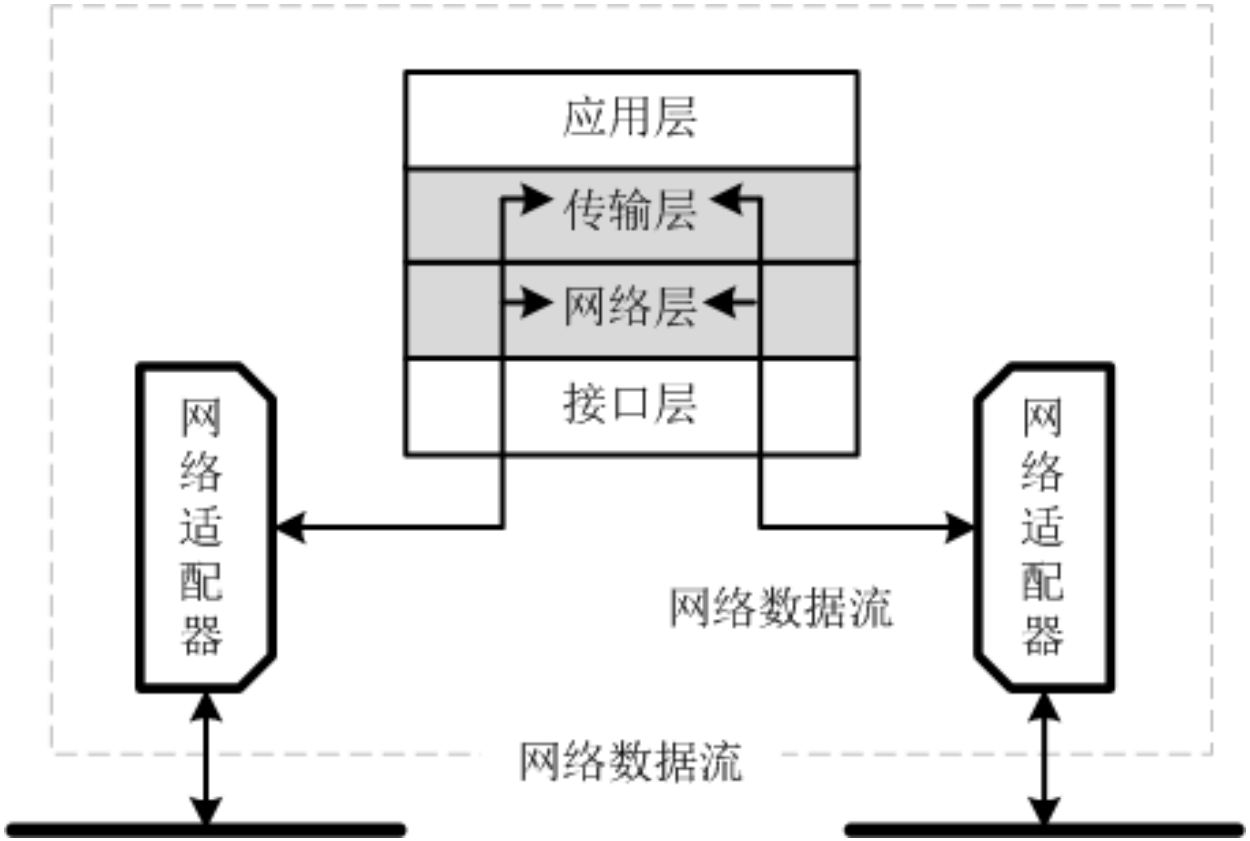

流量过滤
网络审计
NAT
VPN
DMZ
防火墙
Internet
VPN
通过NAT访问Internet
VPN
内部网络
DMZ
Web
Ftp
电子商务

局限性

- 防火墙无法检测不经过防火墙的流量，如通过内部提供拨号服务接入公网的流量；
- 防火墙不能防范来自内部人员恶意的攻击；
- 防火墙不能阻止被病毒感染的和有害的程序或文件的传递，如木马；
- 防火墙不能防止数据驱动式攻击，如一些缓冲区溢出攻击。

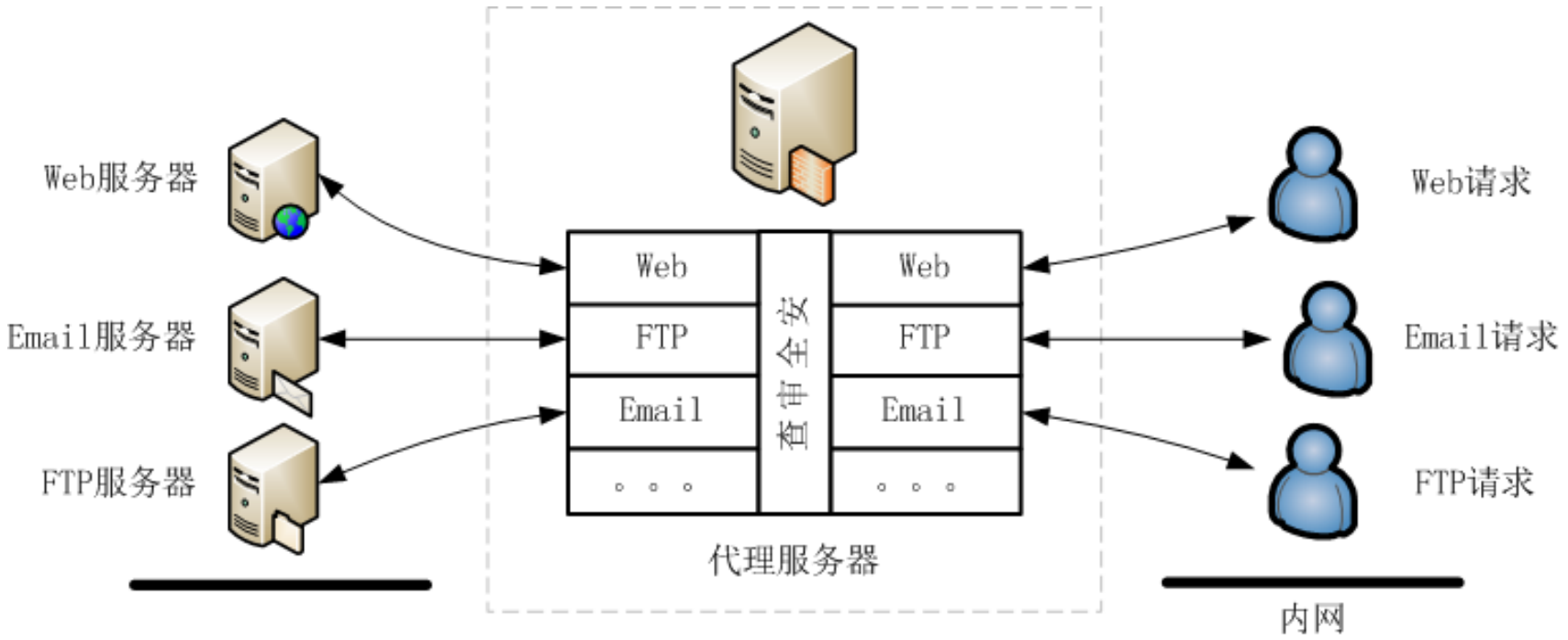
7.2.2 防火墙的主要技术

- 包过滤防火墙
  - 面向网络底层数据流进行审计和控管
  - 其安全策略主要根据数据包头的源地址、目的地址、端口号和协议类型等标志来制定，可见其主要工作在网络层和传输层。



代理防火墙

- 基于代理（Proxy）技术，使防火墙参与到每一个内外网络之间的连接过程
- 防火墙需要理解用户使用的协议，对内部节点向外部节点的请求进行还原审查后，转发给外部服务器；
- 外部节点发送来的数据也需要进行还原审查，然后封装转发给内部节点。



个人防火墙

- 目前普通用户最常使用的一种，常见如天网个人防火墙。
  - 个人防火墙是一种能够保护个人计算机系统安全的软件，
  - 直接在用户的计算机上运行，帮助普通用户对系统进行监控及管理，使个人计算机免受各种攻击。

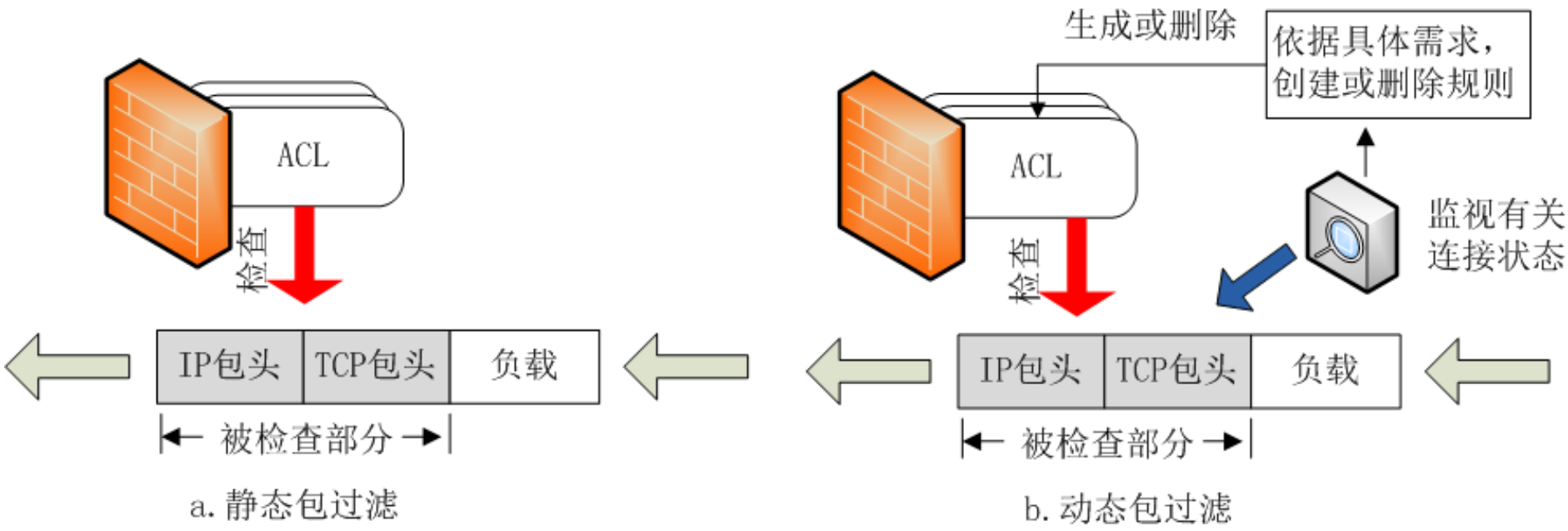
主要技术简介

- 访问控制列表ACL
  - Access Control List是允许和拒绝匹配规则的集合。
  - 规则告诉防火墙哪些数据包允许通过、哪些被拒绝。

顺序	方向	源地址	目的地址	协议	源端口	目的端口	是否通过
Rule 1	out	192.168.10.11	*.*.*.*	TCP	any	80	deny
Rule 2	out	*.*.*.*	202.106.85.36	TCP	any	80	accept

包过滤

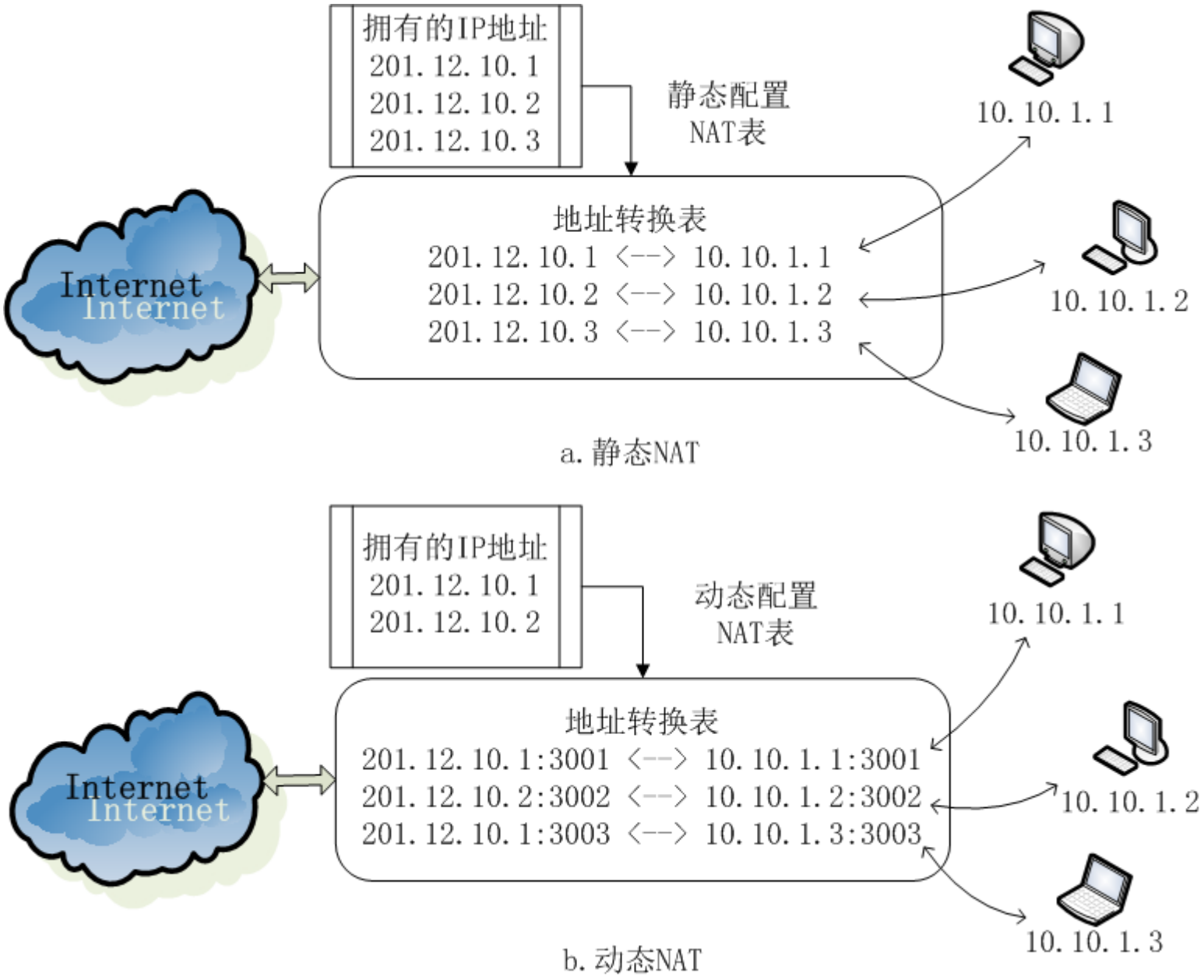
- 静态包过滤是指防火墙根据定义好的包过滤规则审查每个数据包，确定其是否与某一条包过滤规则匹配。
- 动态包过滤是指防火墙采用动态配置包过滤规则的方法。



代理网关

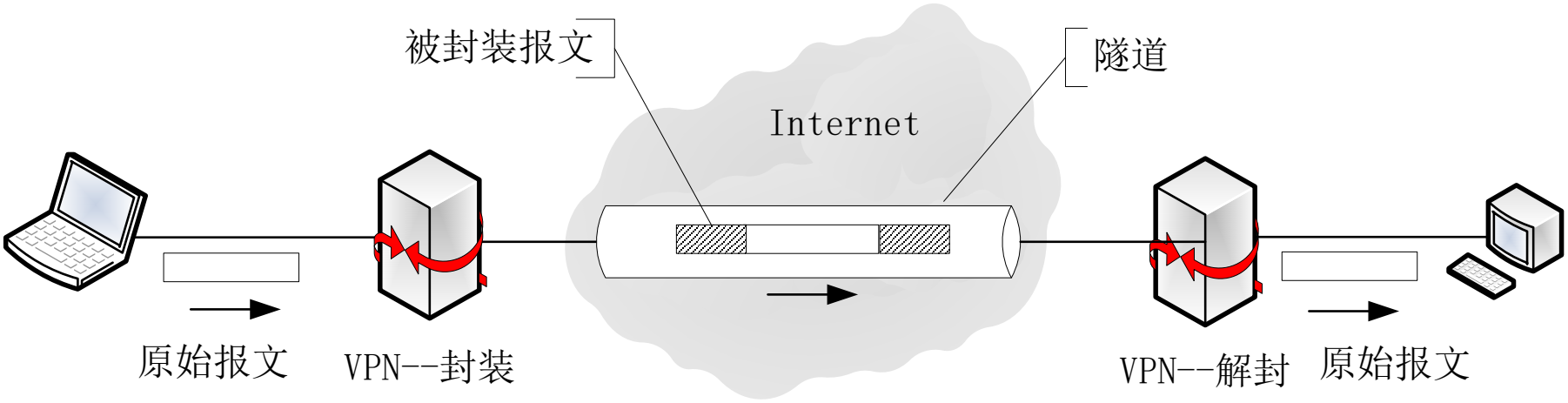
- 应用代理网关
  - 被认为是最安全的防火墙技术，应用代理网关防火墙彻底隔断内网与外网的直接通信，内网用户对外网的访问变成防火墙对外网的访问，外网返回的消息再由防火墙转发给内网用户
- 电路级网关（Circuit Gateway）
  - 工作原理与应用代理网关基本相同，代理的协议以传输层为主，在传输层上实施访问控制策略，是在内外网络之间建立一个虚拟电路，进行通信。

NAT（Network Address Translation）

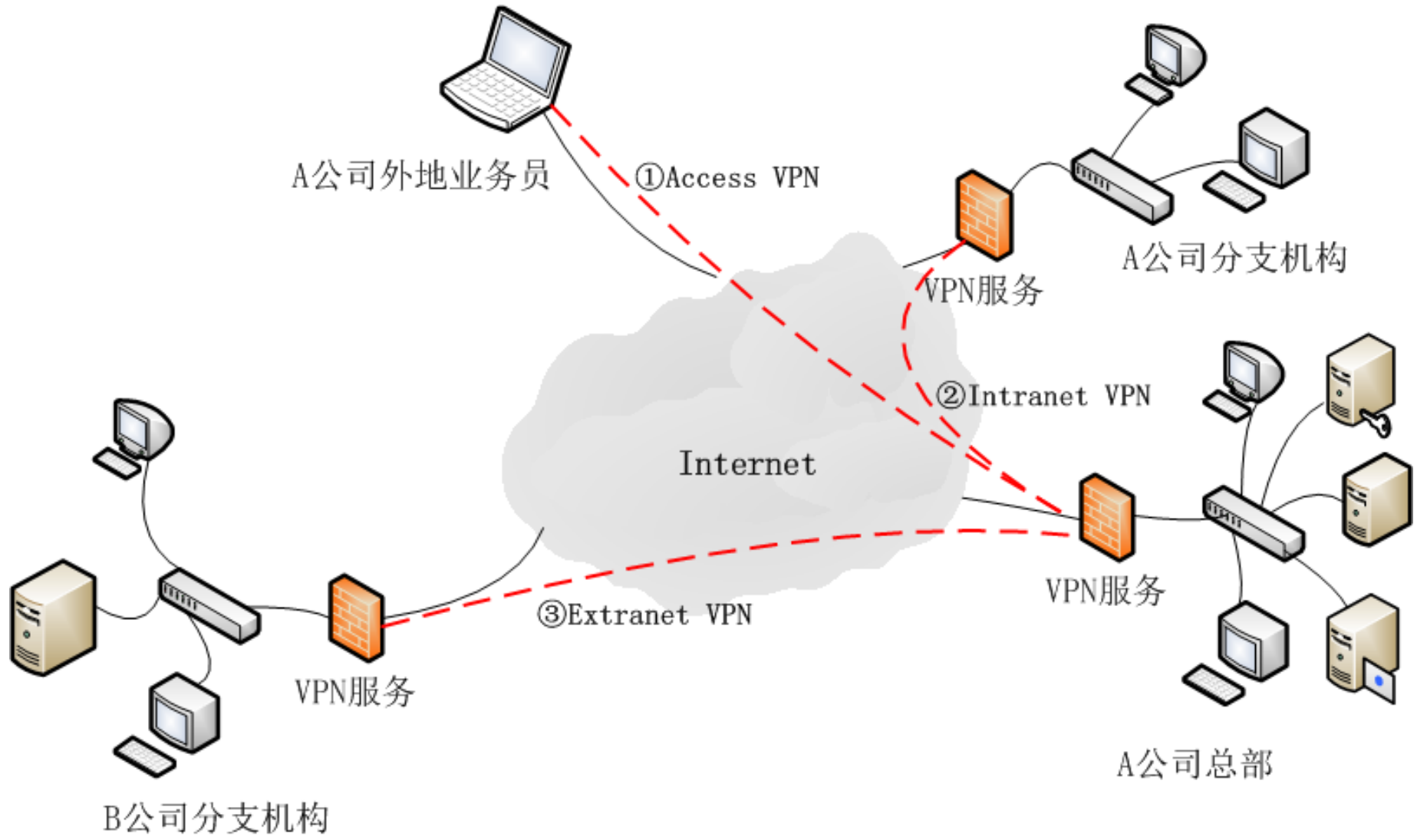


VPN（Virtual Private Network）

- VPN：虚拟的企业内部专线，也称虚拟私有网。
- VPN是通过一个公用网络（通常是Internet）建立一个临时的、安全的连接。
  - 可以理解为一条穿过公用网络的安全、稳定的隧道，两台分别处于不同网络的机器可以通过这条隧道进行连接访问，就像在一个内部局域网一样。

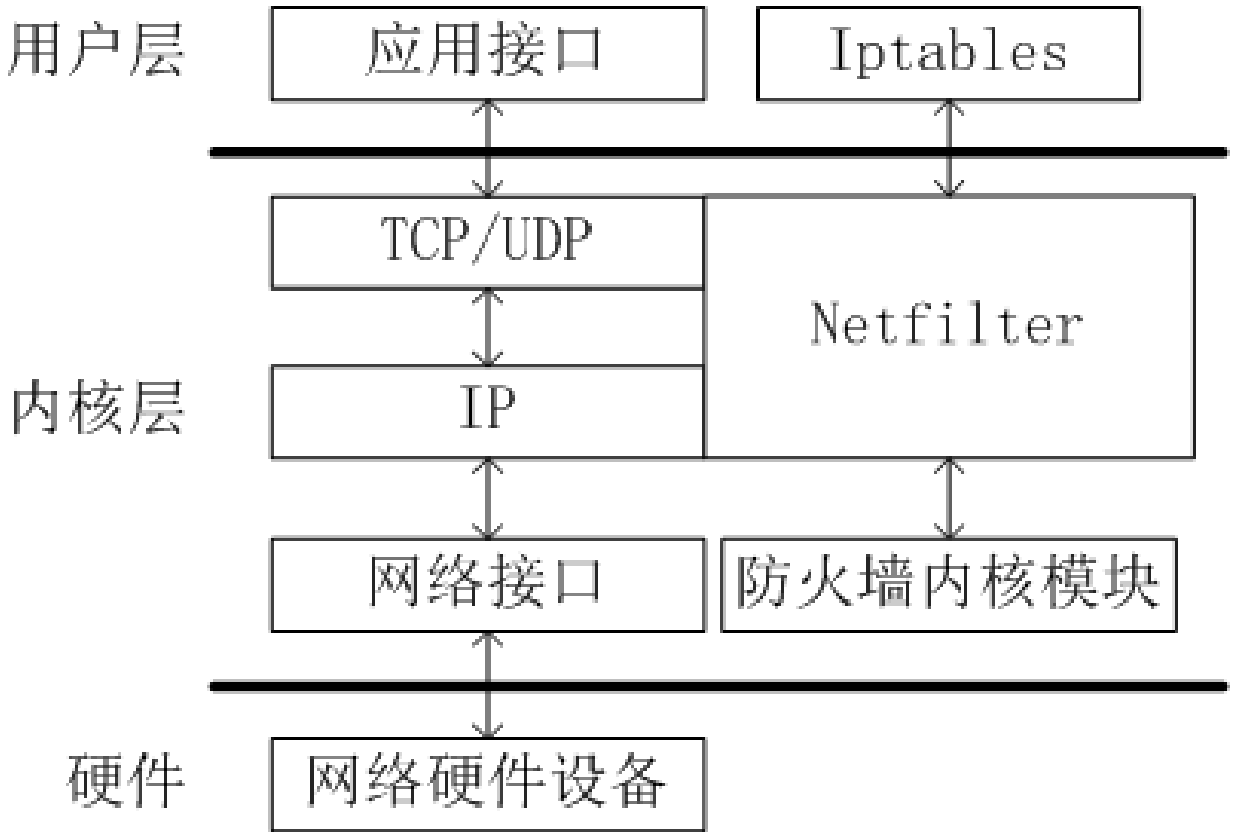


VPN典型应用


A公司外地业务员
①Access VPN
VPN服务
A公司分支机构
②Intranet VPN
Internet
③Extranet VPN
VPN服务
VPN服务
A公司总部
B公司分支机构

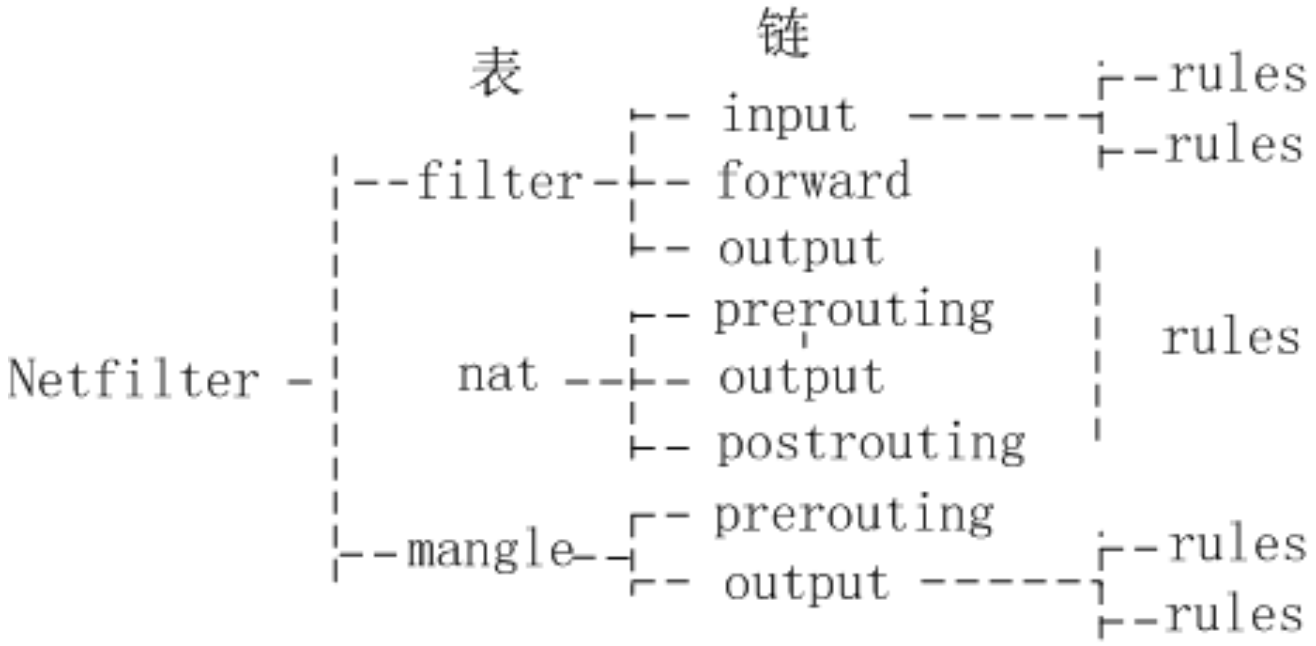
7.2.3 Netfilter/IPtables防火墙

- 2001年，Linux 2.4版内核，Netfilter/IPtables包过滤机制，被业内称为第三代Linux防火墙。

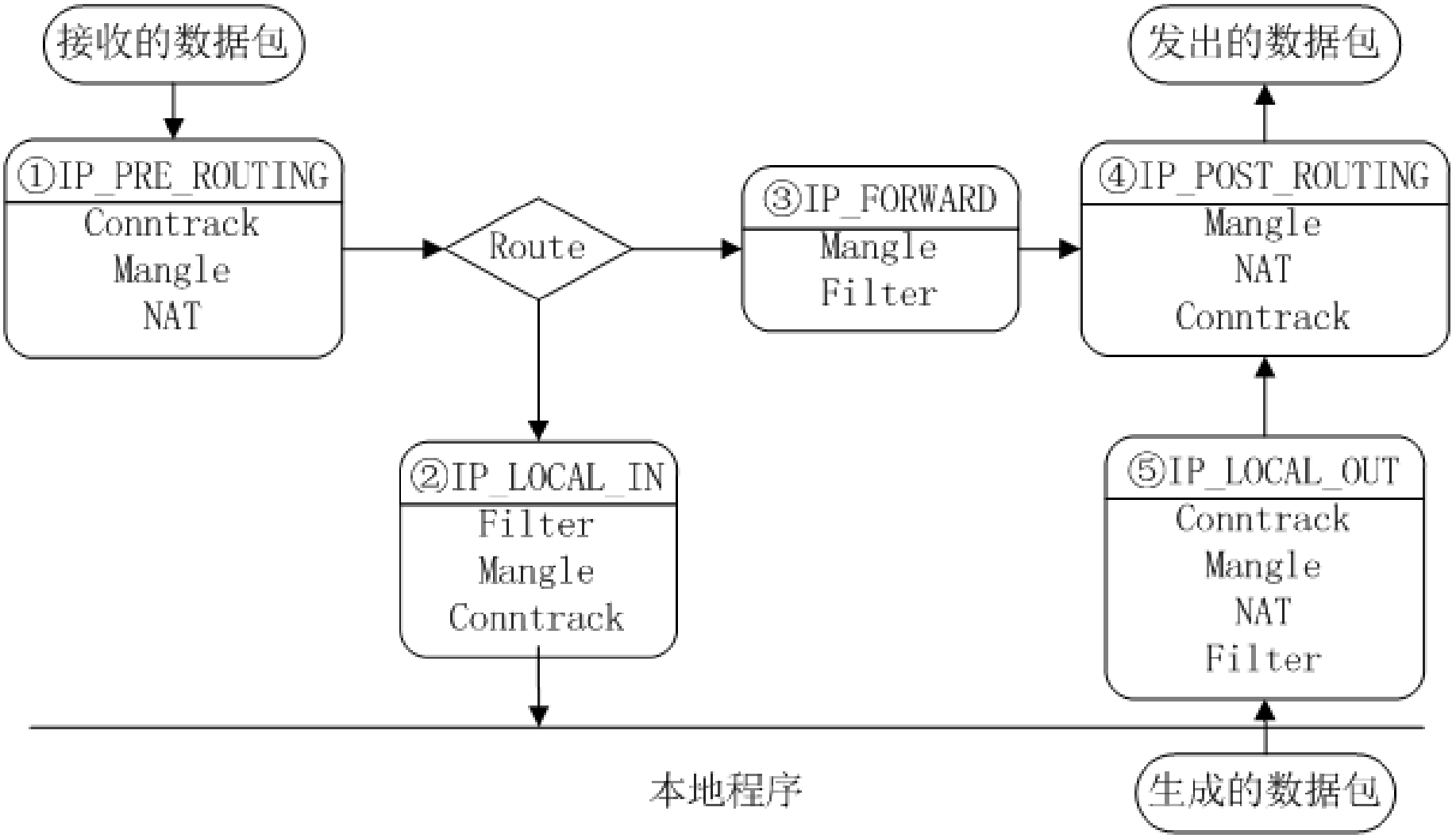


Netfilter通用架构

- 是嵌入在Linux内核IP协议栈中的一个通用架构。
  - 它提供了一系列的“表”（tables）
    - 每个表由若干“链”（chains）组成，
    - 每条链中可以有一条或数条规则（rule）。



Netfilter程序流程架构

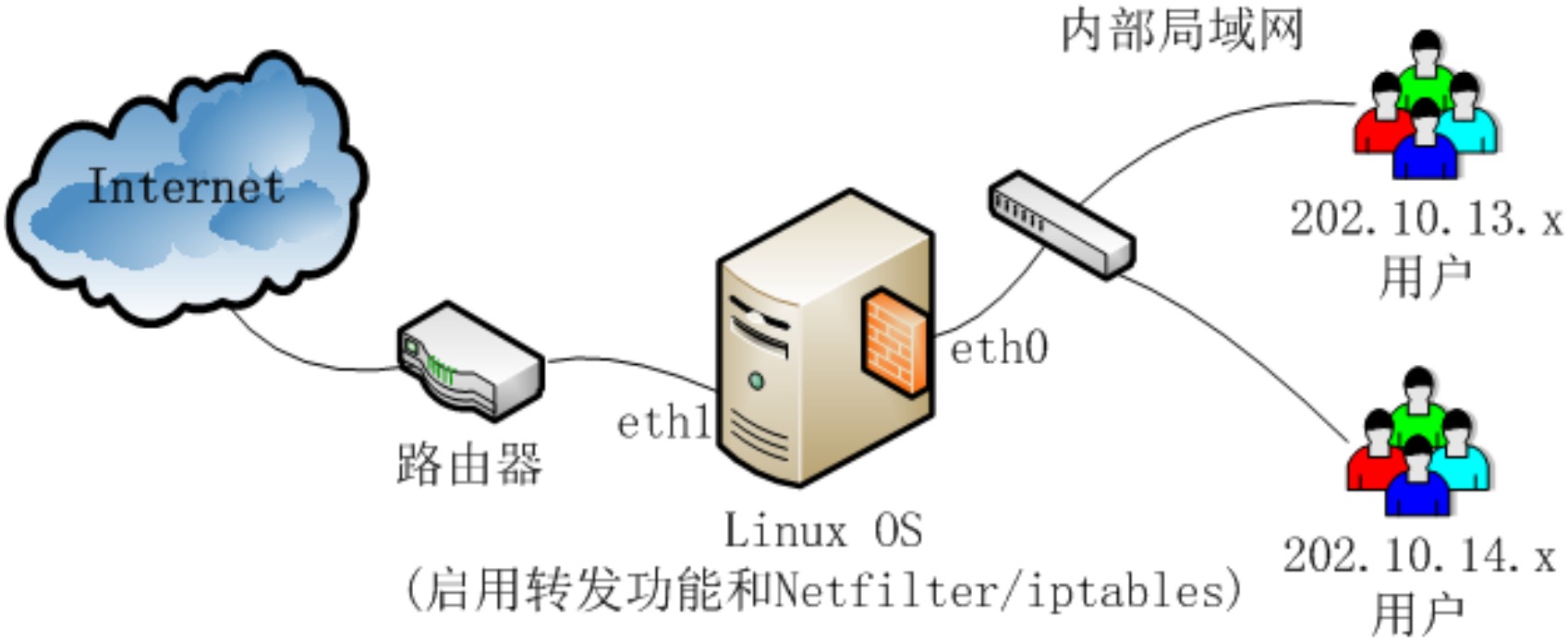


规则组成

- IPtables命令 = 工作表 + 使用链 + 规则操作 + 目标动作 + 匹配条件
  - 工作表：指定该命令针对的表，缺省表为filter；
  - 使用链：指定表下面的某个链，实际上就是确定哪个钩子点；
  - 规则操作：包括添加规则、插入规则、删除规则、替代规则、列出规则；
  - 目标动作：有两个，ACCEPT（继续传递数据包），DROP（丢弃数据包）；
  - 匹配条件：指过滤检查时，用于匹配数据包头信息的特征信息串，如地址、端口等。

Netfilter/Iptables 例子

- 目的：内网中只有202.10.13.0/24网段的用户可以访问外网，同时又只能使用TCP。
  - iptables -P FORWARD DROP
  - iptables -A FORWARD -p tcp -s 202.10.13.0/24 -j ACCEPT
  - iptables -A FORWARD -p tcp -d 202.10.13.0/24 -j ACCEPT

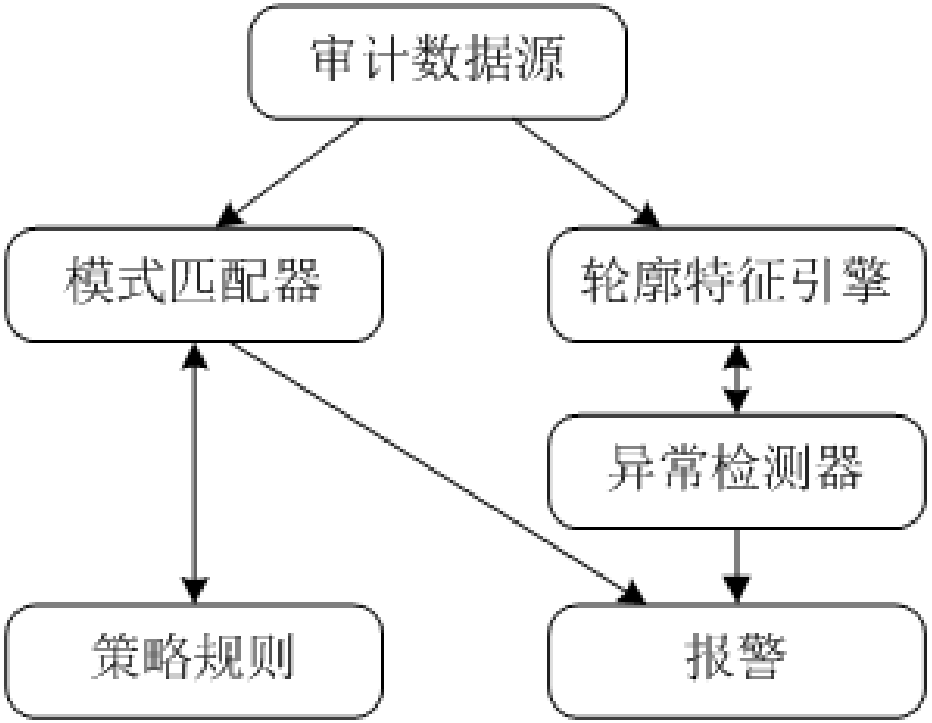


7.3 入侵检测系统

- IDS（Intrusion Detection System）
  - 一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全系统。
  - 一般认为防火墙属于静态防范措施，而入侵检测系统为动态防范措施，是对防火墙的有效补充。
  - 假如防火墙是一幢大楼的门禁，那么IDS就是这幢大楼里的监视系统。

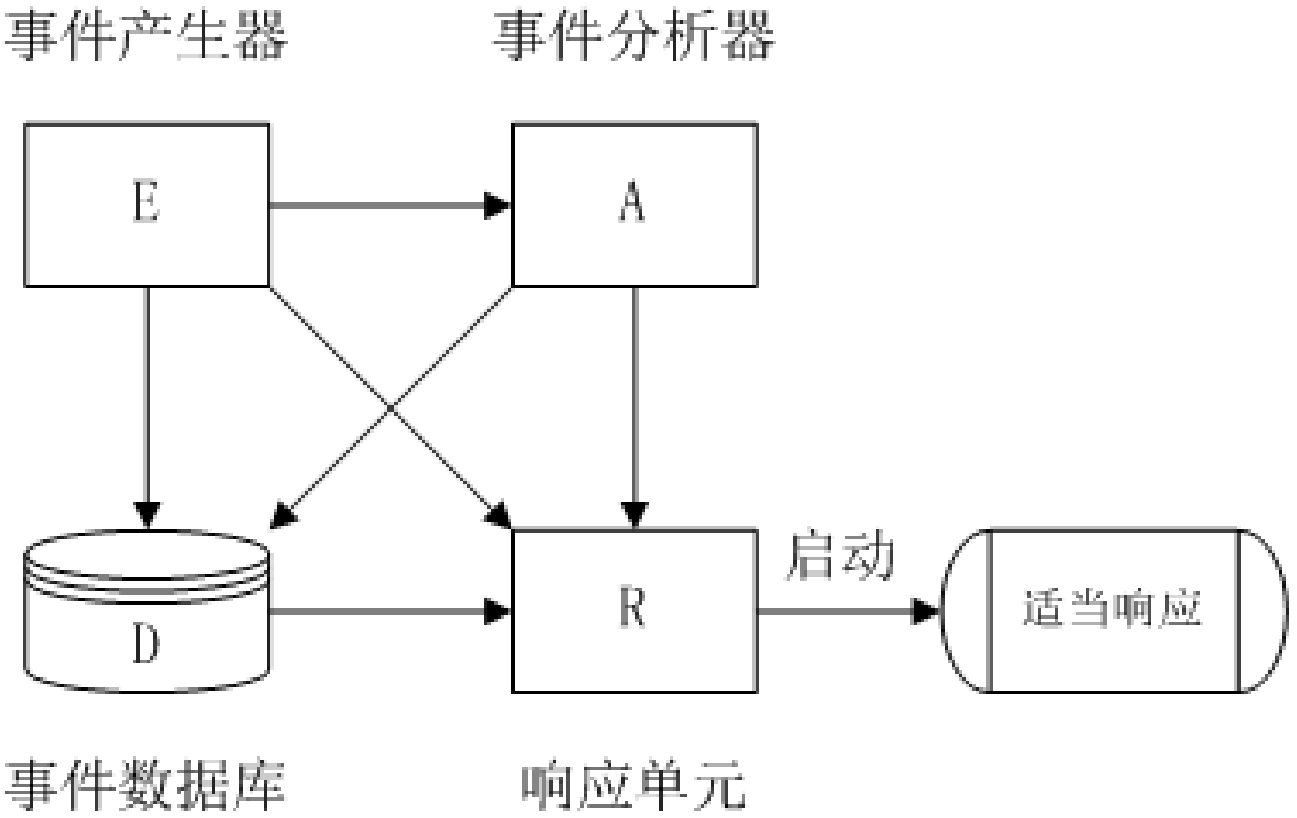
7.3.1 入侵检测概述

- 1980年，James P. Anderson，《Computer Security Threat Monitoring and Surveillance》此报告被公认是开山之作。
- 1984-1986年，Dorothy Denning和 Peter Neumann，实时入侵检测系统模型，IDES(Intrusion Detection Expert System)。



CIDF通用模型

- IDWG（Intrusion Detection Working Group，IETF下属的研究机构）和CIDF（Common Intrusion Detection Framework，一个美国国防部赞助的开放组织）



入侵检测几个重要概念

- 事件：
  - 当网络或主机遭到入侵或出现较重大变化时，称为发生安全事件，简称事件。
- 报警：
  - 当发生事件时，IDS通过某种方式及时通知管理员事件情况称为报警。
- 响应：
  - 当IDS报警后，网络管理员对事件及时作出处理称为响应。
- 误用：
  - 误用是指不正当使用计算机或网络，并构成对计算机安全或网络安全威胁的一类行为。
- 异常：
  - 对网络或主机的正常行为进行采样、分析，描述出正常的行为轮廓，建立行为模型，当网络或主机上出现偏离行为模型的事件时，称为异常。

- 入侵特征：
  - 也称为攻击签名（Attack Signature）或攻击模式（Attack Patterns），一般指对网络或主机的某种入侵攻击行为（误用行为）的事件过程进行分析提炼，形成可以分辨出该入侵攻击事件的特征关键字，这些特征关键字被称为入侵特征。
- 感应器：
  - 置在网络或主机中用于收集网络信息或用户行为信息的软硬件，称为感应器。感应器应该布置在可以及时取得全面数据的关键点上，其性能直接决定IDS检测的准确率。

入侵检测系统工作过程

- 信息收集：
  - 入侵检测的第一步是信息收集，收集内容包括系统和网络的数据及用户活动的状态和行为。信息收集工作一般由由放置在不同网段的感应器来收集网络中的数据信息（主要是数据包）和主机内感应器来收集该主机的信息。
- 信息分析：
  - 将收集到的有关系统和网络的数据及用户活动的状态和行为等信息送到检测引擎，检测引擎一般通过三种技术手段进行分析：模式匹配、统计分析和完整性分析。当检测到某种入侵特征时，会通知控制台出现了安全事件。
- 结果处理：
  - 当控制台接到发生安全事件的通知，将产生报警，也可依据预先定义的相应措施进行联动响应。如可以重新配置路由器或防火墙、终止进程、切断连接、改变文件属性等。

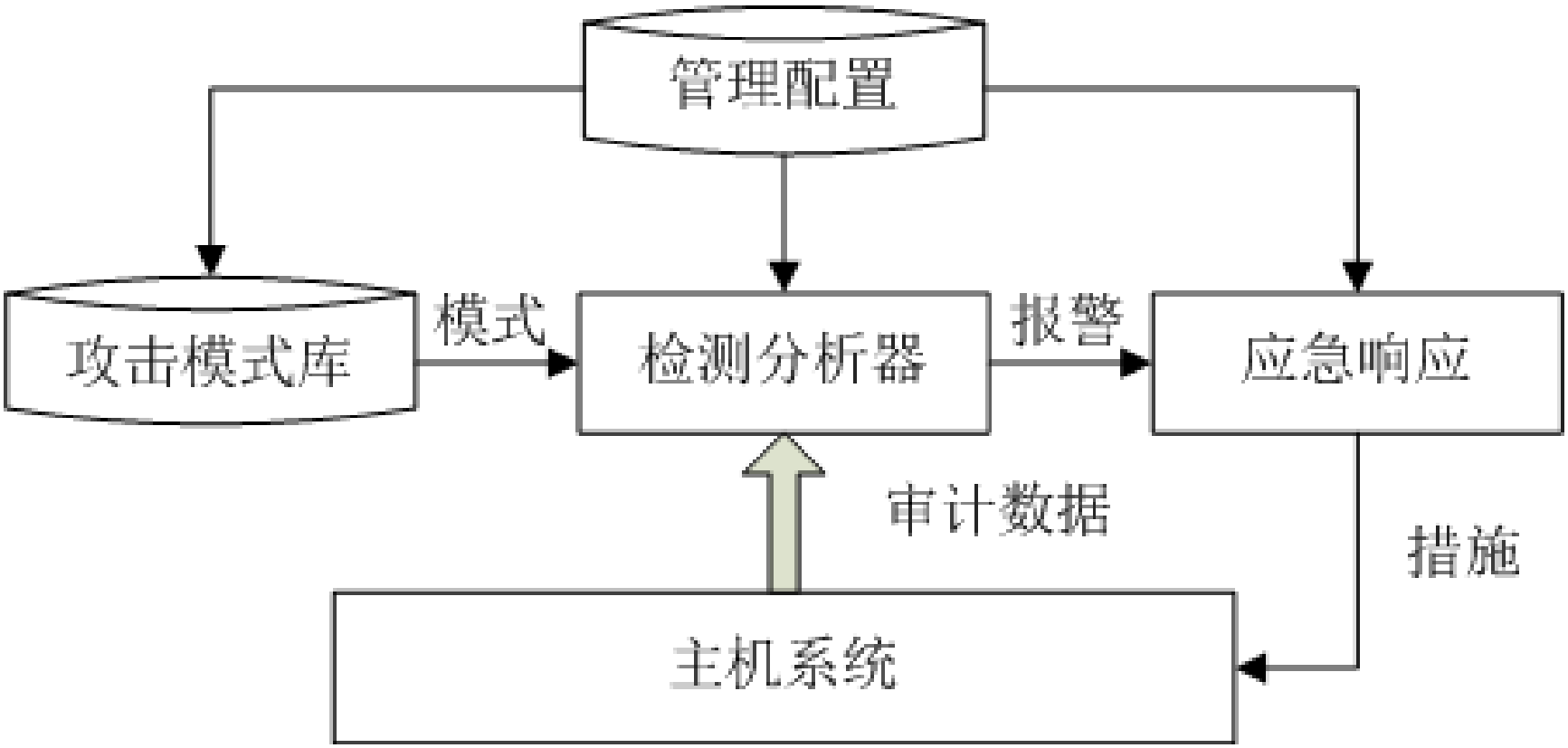
IDS主要功能

- 监测并分析用户、系统和网络的活动变化；
- 核查系统配置和漏洞；
- 评估系统关键资源和数据文件的完整性；
- 识别已知的攻击行为；
- 统计分析异常行为；
- 操作系统日志管理，并识别违反安全策略的用户活动。

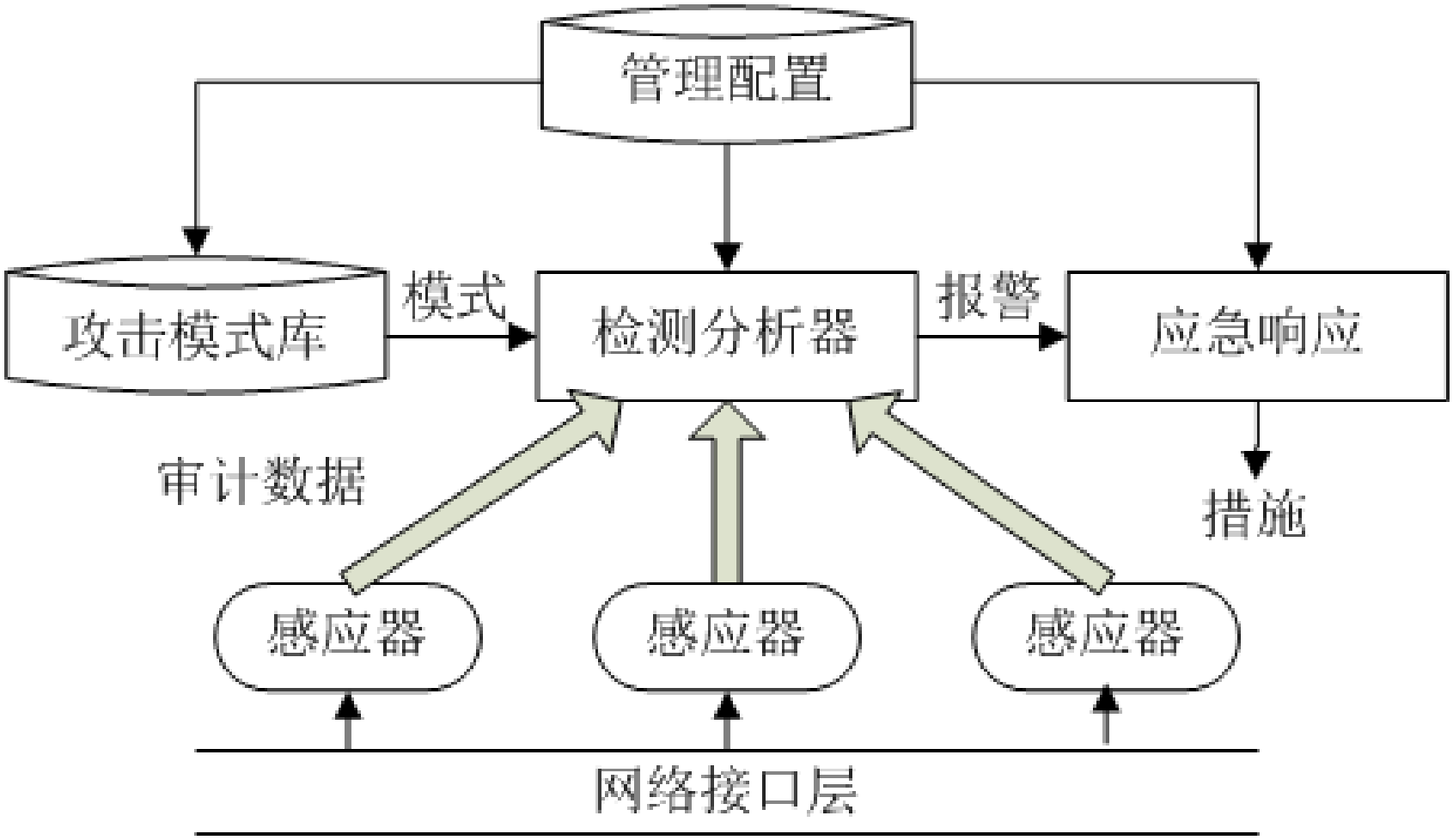
7.3.2 入侵检测系统分类

- 以数据源为分类标准
  - 主机型入侵检测系统HIDS（Host-based Intrusion Detection System ）和网络型入侵检测系统NIDS（Network-based Intrusion Detection System）。

主机型入侵检测系统

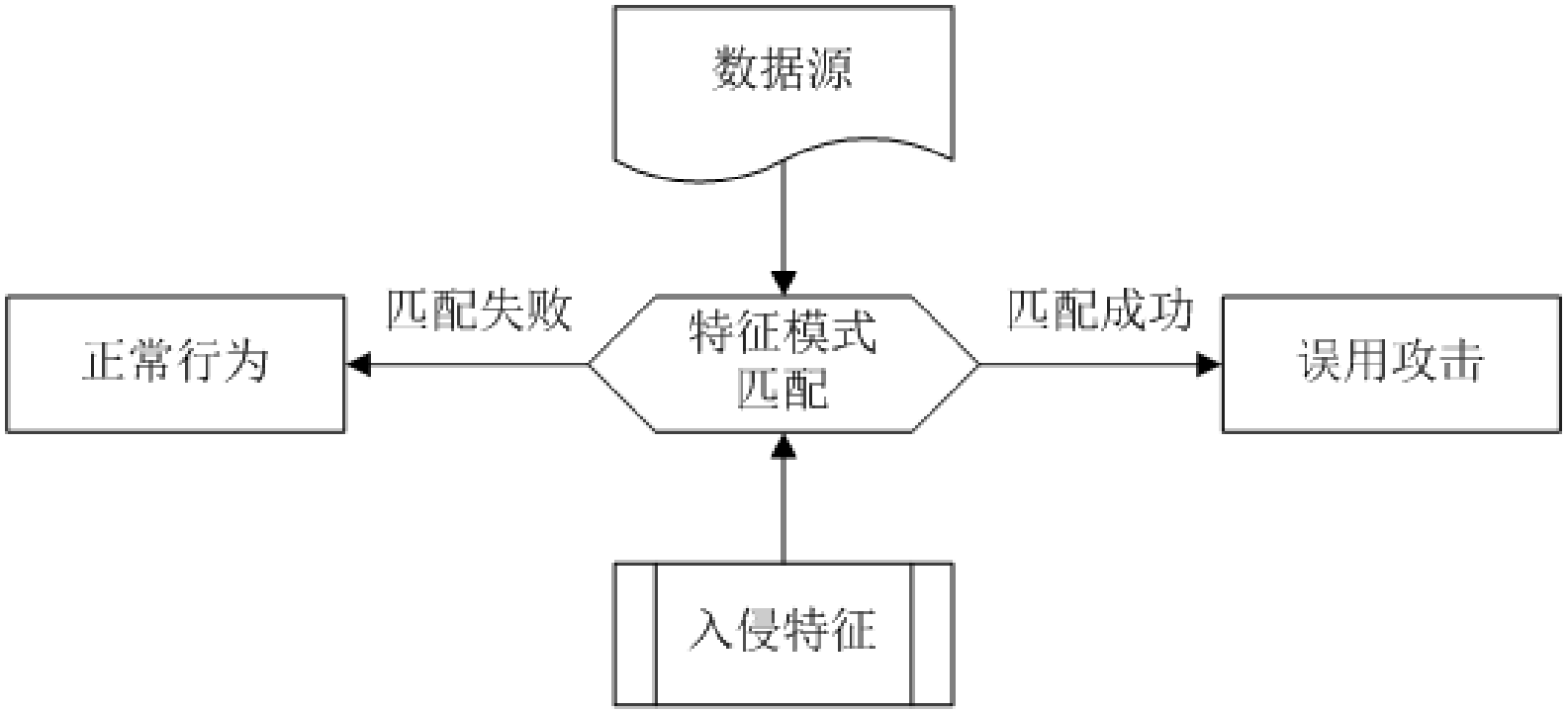


网络型入侵检测系统



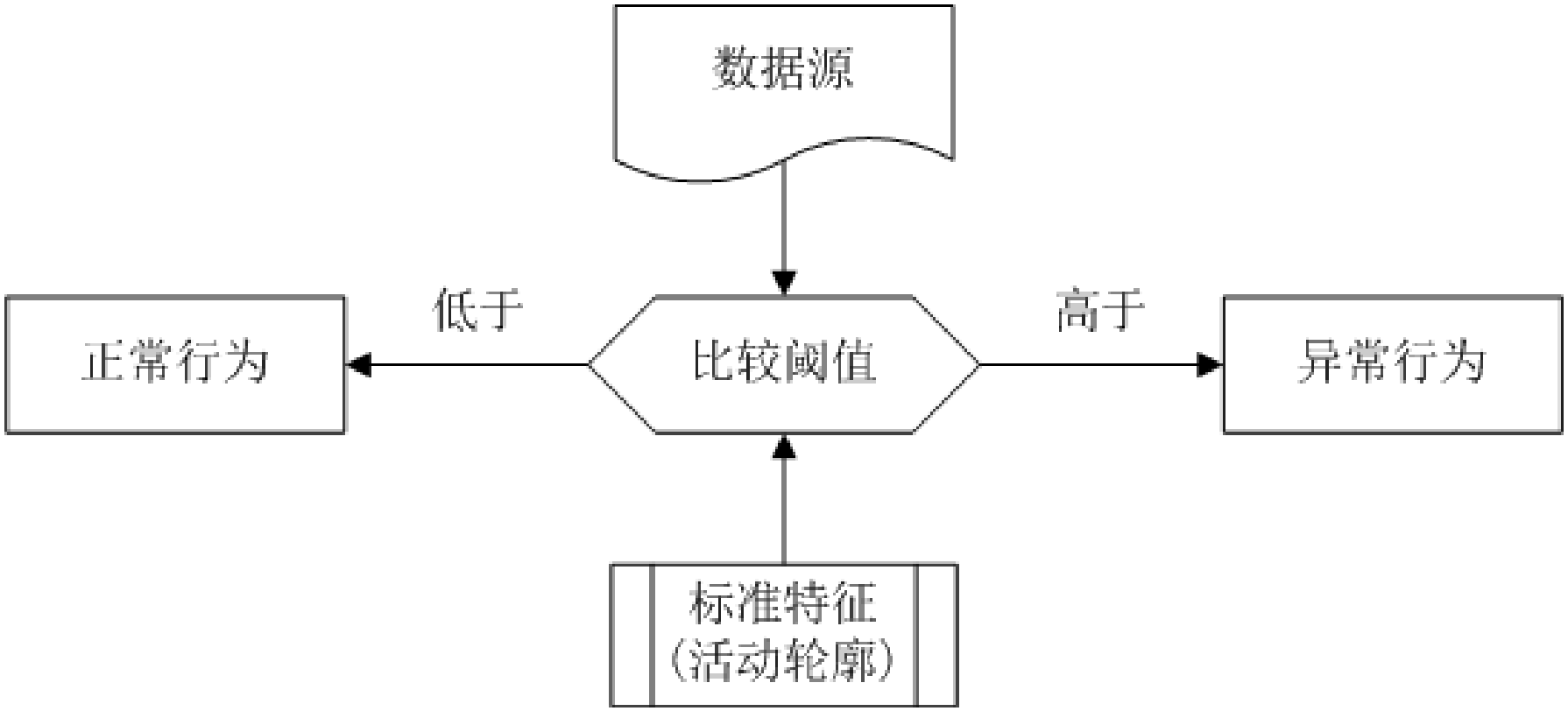
以检测技术为分类标准

- 基于误用检测（Misuse Detection）的IDS



误用检测模型

基于异常检测（Anomaly Detection）的IDS



7.3.3 入侵检测技术

- 入侵检测技术研究具有综合性、多领域性的特点，技术种类繁多，涉及到许多相关学科。
- 从误用检测、异常检测、诱骗和响应等四个方面分析一下入侵检测的主要技术方法。
- 误用检测技术
  - 专家系统
  - 特征分析
  - 模型推理
  - 状态转换分析
  - 完整性校验等

异常检测技术

- 异常检测是一种与系统相对无关、通用性较强的入侵检测技术。
- 异常检测的思想最早由Denning提出，即通过监视系统审计记录上系统使用的异常情况，可以检测出违反安全政策的事件。
- 通常异常检测都与一些数学分析方法相结合，但存在着误报率较高的问题。
- 异常检测主要针对用户行为数据、系统资源使用情况进行分析判断。
- 常见的异常检测方法主要包括统计分析、预测模型、系统调用监测以及基于人工智能的异常检测技术等。

入侵诱骗技术

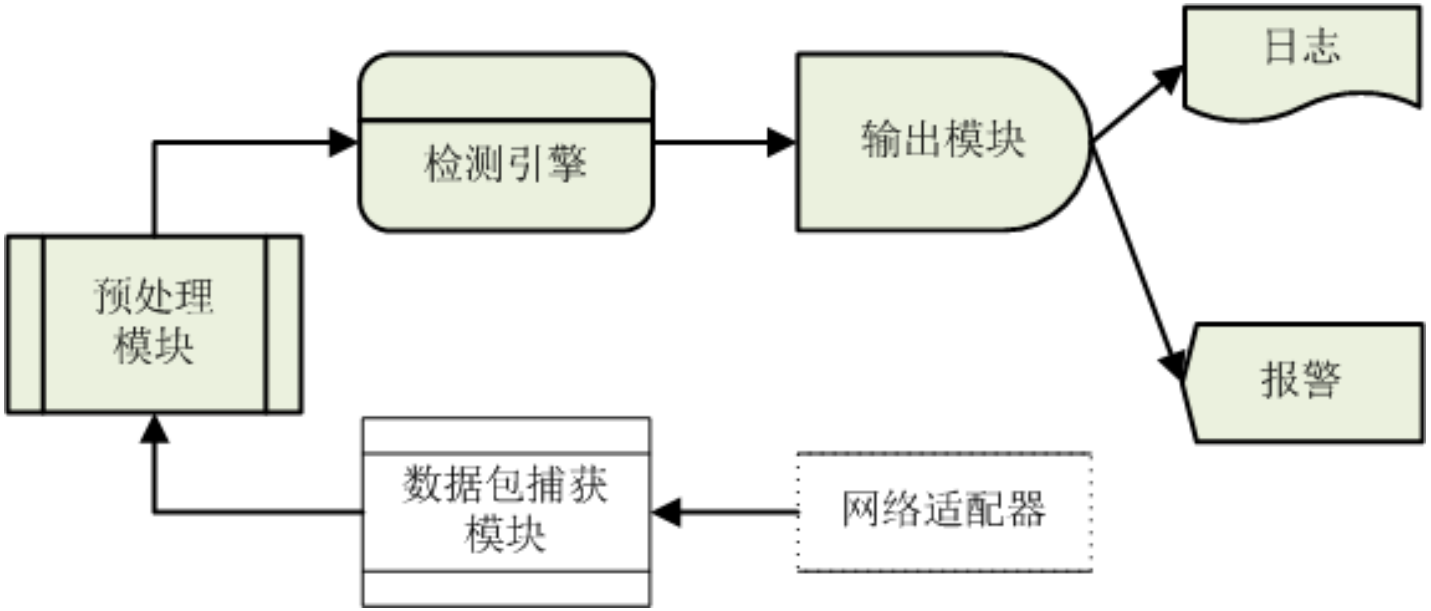
- 入侵诱骗是指用通过伪装成具有吸引力的网络主机来吸引攻击者，同时对攻击者的各种攻击行为进行分析，进而找到有效的应对方法。
- 具有通过吸引攻击者，从而保护重要的网络服务系统的目的。
- 常见的入侵诱骗技术主要有蜜罐（Honeypot）技术和蜜网（Honeynet）技术等。

响应技术

- 入侵检测系统的响应技术可以分为主动响应和被动响应。
  - 主动响应是系统自动阻断攻击过程或以其他方式影响攻击过程；
  - 被动响应是报告和记录发生的事件。

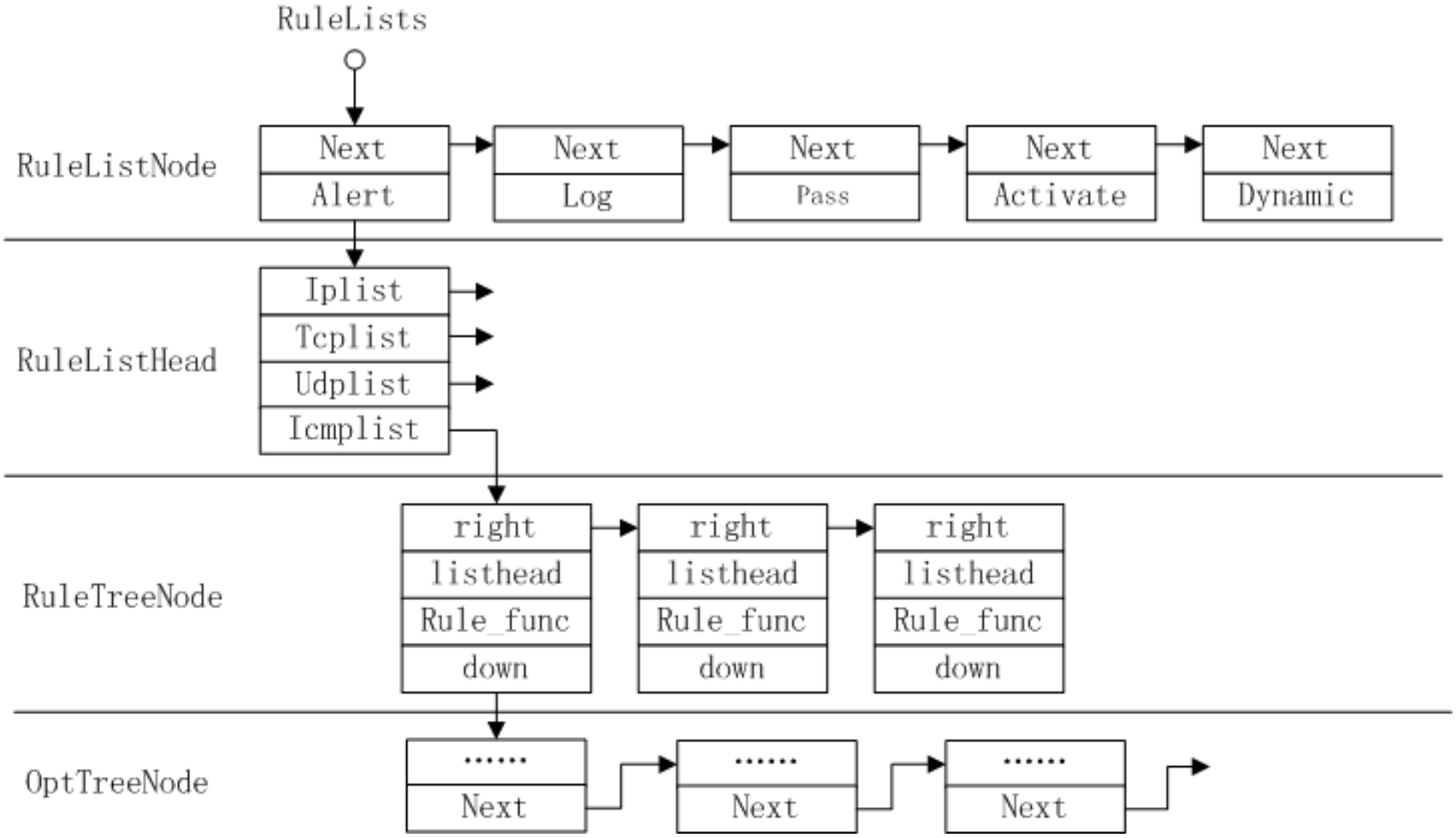
7.3.4 Snort系统

- Snort入侵检测系统是一个开放源代码的轻量级网络入侵检测系统。
- Snort遵循CIDF模型，使用误用检测的方法来识别发现违反系统和网络安全策略的网络行为。
- Snort系统包括数据包捕获模块、预处理模块、检测引擎和输出模块四部分组。



Snort规则库

- Snort将所有已知的入侵行为以规则的形式存放在规则库中，并以三维链表结构进行组织。



Snort规则例子

- Alert tcp any any->10.1.1.0/24 80(content:"/cgi-bin/phf"；msg:"PHF probe!"；)
- 在这个规则中，括号左面为规则头，括号中间的部分为规则选项，规则选项中冒号前的部分为选项关键字(Option Keyword)。
- 规则头由规则行为、协议字段、地址和端口信息3部分组成。Snort定义了五种可选的行为：
  - Alert：使用设定的警告方法生成警告信息，并记录这个数据报文；
  - Log：使用设定的记录方法来记录这个数据报文；
  - Pass：忽略这个数据报文；
  - Activate：进行alert，然后激活另一个dynamic规则。
  - Dynamic：等待被一个activate规则激活，被激活后就作为一条log规则执行。