Chapter 1

概论

1 信息系统的脆弱性主要体现在以下几个方面：

1. 物理因素，物理设备的自然、人为破坏。
2. 网络因素，信息系统软件复杂度越来越高。
3. 系统因素，信息系统软件复杂度越来越高
4. 应用因素，不正确的操作和人为的蓄意破坏。
5. 管理因素，管理制度、法律不健全。

2 信息安全的目标： 对网络中的硬件、软件和系统中的数据进行保护，不受偶然或者恶意的因素影响而遭到破坏、更改、泄漏，使系统能稳定可靠正常地运行，使信息服务不中断。

3 信息安全关注的几点问题:

1. 密码理论与技术
2. 安全协议理论与技术
3. 安全体系结理论与技术
4. 信息对抗理论与技术
5. 网络安全与安全产品

4 互联网络的特点:

1. 无中心网，再生能力强
2. 可实现移动通信、多媒体通信等多种服务
3. 互联网一般分为外部网和内部网
4. 互联网的用户主体是个人

5 P2DR 模型

- Policy 安全策略
- Protection 防护
- Detection 检测
- Response 响应

6 PDRR 模型

- Protection 防护
- Detection 检测
- Response 响应
- Recovery 恢复

7 ISO 开方系统互联安全体系的五类安全服务

1. 鉴别服务
2. 访问控制服务
3. 数据机密性服务
4. 数据完整性服务
5. 抵抗性

Chapter 2

密码学概论

1 密码学分支

1. 密码编码学, 将明文转换为密文
2. 密码分析学，破译密文

2 密码元素

1. 明文
2. 密文
3. 加密
4. 解密
5. 密钥

三元素： 明文，密钥，密文
五元素: 明文空间、密文空间、密钥空间、加密算法、解密算法。

3 密码分析方法

1. 唯密文攻击: 密码分析者拥有一些消息的密文，这些消息都是用同样的加密算法来加密的
2. 已知明文攻击：密码分析者不仅拥有一些消息的密文，而且还拥有这些密文对应的明文
3. 选择明文攻击：分析者不仅拥有一些消息的密文和相应的明文，而且他们还可以进行有选择地加密明文。
4. 选择密文攻击：密码分析者能够选择不同的密文，而且能够得到与之对应的明文。

攻击强度递增，唯密文是最弱的一种攻击，选择密文是最强的一种攻击，如果一个系统能够抵抗选择密文攻击，他一定能够抵抗其他攻击。

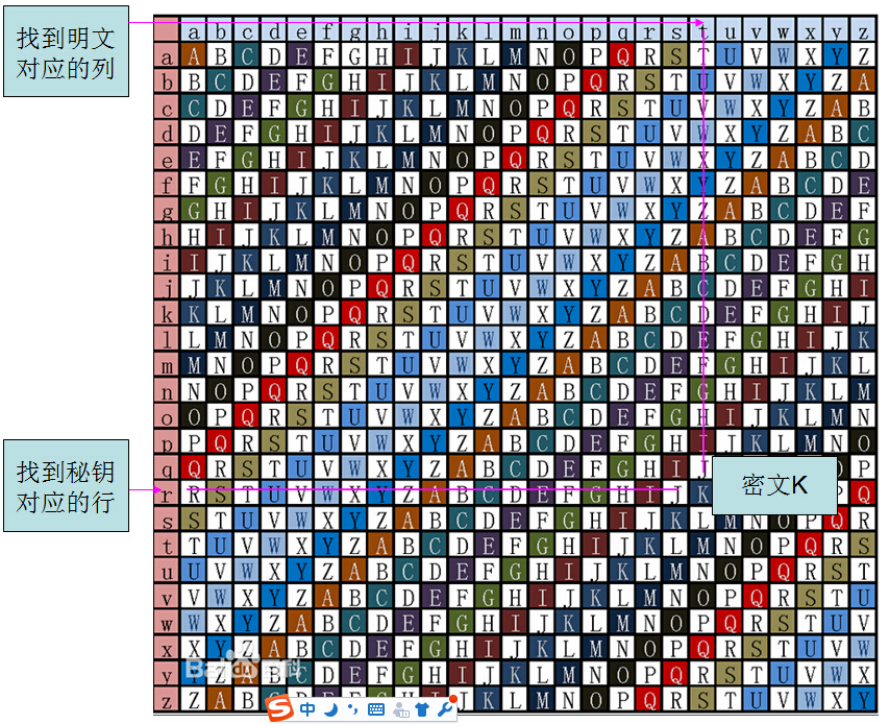
衡量密码攻击的复杂度有两个方面：

- 数据复杂度，为了实施攻击所需输入的数据量
- 处理复杂度, 处理这些数据所需的计算量

4 凯撒算法

$$C = E(p) = (p + k) mod 26 \tag{2.1}$$
$$p = D(C) = (C - k) mod 26 \tag{2.2}$$

5 维吉尼亚加密算法 生成维吉尼亚矩阵，和**与明文长度一样的密钥**，然后明文找列，密钥找行，生成密文。



6 现代加密算法分类

1. 对称加密算法，加解密都采用一样的密钥，加/解密速度快，但密钥分发问题严重
2. 非对称加密算法，加解密采用不同密钥，加/解密速度较慢，但无密钥分发问题

7 DES 是一种**块加密算法**，**对称加密算法**，每块 64bit。

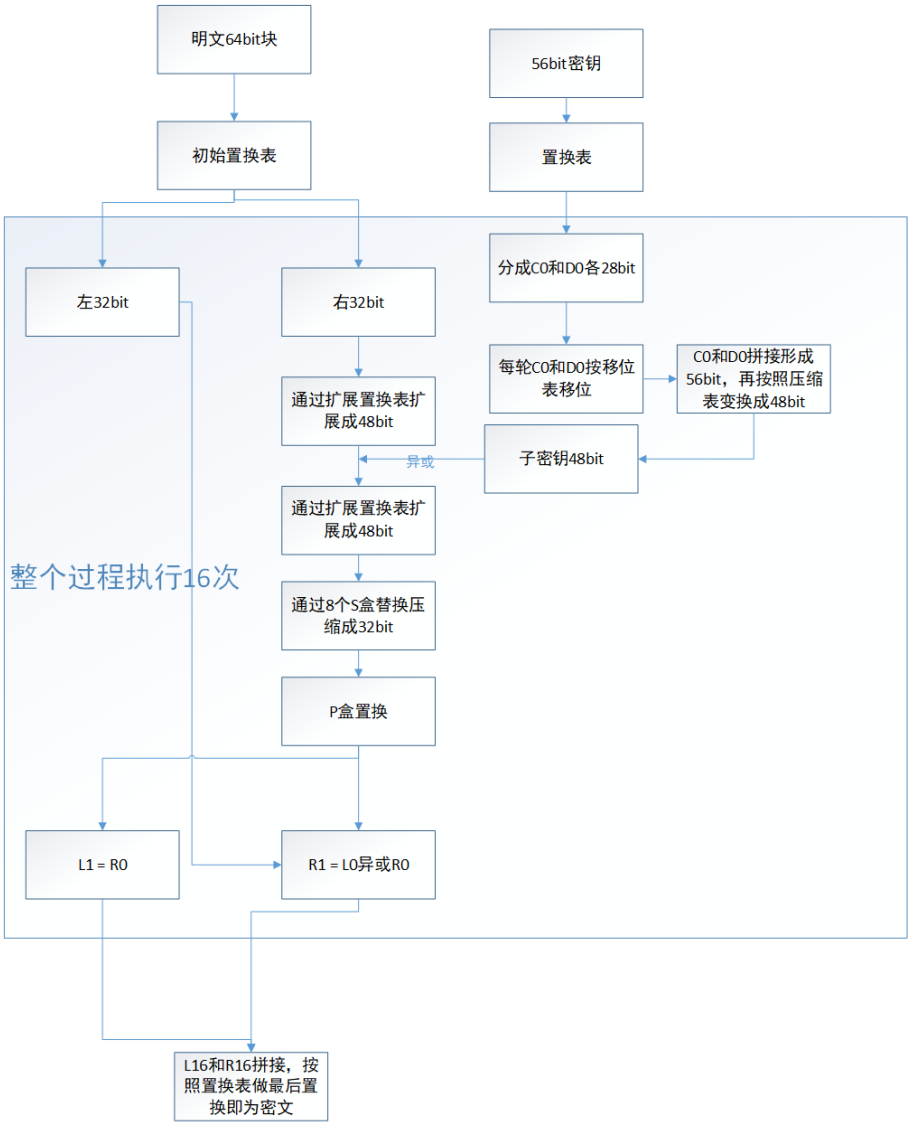


Figure 2.1:

8 其余几种对称加密算法

1. IDEA,64 位输入，128 位密钥，64 位输出
2. AES ，128bit 输入，密钥长度可变，为 128/192/256bit，相应的轮数 r 为 10/12/14
3. 2DES, 采用两个密钥（不相同），加密时，先使用 K_2 加密，再使用 K_1 加密，解密时先使用 K_1 解，在使用 K_2 解
4. 3DES. 重复三次。

9 RSA 算法 非对称加密算法，安全性基于分解大整数的困难性
公钥与密钥的产生

1. 随意选择两个大的质数 p 和 q，p 不等于 q，计算 N=pq。
2. 根据欧拉函数，求得 r = (p-1)(q-1)

3. 选择一个小于 r 的整数 e，求得 e 关于模 r 的模反元素，命名为 d。(模反元素存在，**当且仅当 e 与 r 互质**)

$$e \times d = 1 \ mod \ r \tag{2.3}$$

4. 将 p 和 q 的记录销毁。

(N,e) 为公钥，(N,d) 为私钥。**采用公钥加密，私钥解密**
一个实例

$$p = 3, q = 11, N = pq = 33 \tag{2.4}$$
$$r = (p-1)(q-1) = 2 * 10 = 20 \tag{2.5}$$
$$ed = r * n + 1 \tag{2.6}$$
$$e = 3, d = 7 \tag{2.7}$$
$$\tag{2.8}$$

所以公钥 (33,3), 私钥 (33,7)。要传输的消息 m = 24

$$\text{加密} \quad m^e mod N = 24^3 \% 33 = 30 \tag{2.9}$$
$$\text{解密} \quad c^d mod N = 30^d \% 33 = 24 \tag{2.10}$$

10 密钥管理

1. 密钥生成, 两方或多方提供共享的秘钥以便在以后的安全通信中进行加密解密、消息认证或身份认证。
2. 密钥传送, 由一方建立密钥，然后安全地传送给其他地方
   (a) 点对点模式需要共享密钥的双方直接通信，传递密钥，即采用人工分发的形势，也可以通过数字信封，用一个双方预先共享的密钥来加密新密钥，然后通过 Internet 传送；
   (b) 密钥服务器模式需要密钥服务器 (Key Server, KS) 的参与，分为两种情况：其一，密钥服务器生成密钥，然后通过安全信道分别传送给通信的各方；其二，密钥服务器只负责密钥的传递，不负责密钥的生成。密钥的生成由通信各方中的一方生成。
3. 密钥协商，双方或多方共同参与密钥形成过程中。通过 DH 密钥交换协议，通信双方能够在不安全的通信信道上传递公开信息，继而各自计算出共享密钥。

Chapter 3

数字签名与身份认证

1 计算机安全的四大原则 ，机密性、完整性、可认证性、不可抵赖性。

2 安全协议

1. 以密码学为基础
2. 也是通信协议

分类:

1. 密钥生成协议
2. 认证协议
3. 电子商务协议
4. 安全多方计算协议

3 数字签名 ，**基于非对称密码算法**，是一串数据，该数据仅能由有签名人生成，并且该数据能够表明签名人的身份。在**身份认证和不可否认性等方面**有重要意义；一般由两个部分组成

1. 签名算法，由签名方秘密保存
2. 验证算法，通常是公开的，便于他人验证签名的有效性

通常分为两类:

1. 直接数字签名
2. 基于仲裁的数字签名

4 数字签名算法 ，原则“私钥加密，公钥解密”

1. DSA

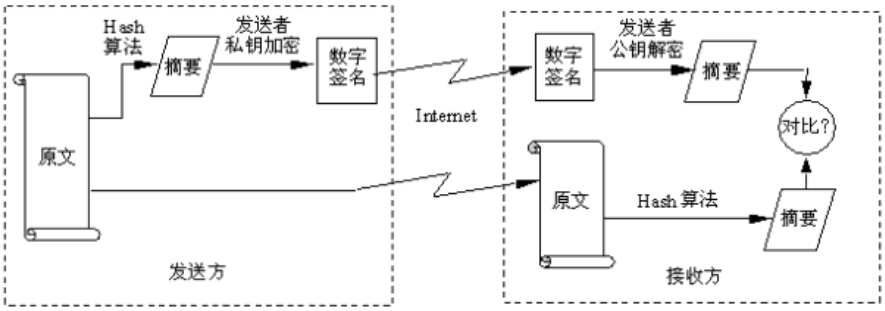


图1. 数字签名的原理图

(a) 使用 SHA 编码将发送文件加密产生 128bit 的数字摘要；

(b) 发送方用自己的专用密钥对摘要再加密，形成数字签名；

(c) 将原文和加密的摘要同时传给对方；

(d) 接受方用发送方的公共密钥对摘要解密，同时对收到的文件用 SHA 编码加密产生同一摘要；

(e) 将解密后的摘要和收到的文件在接受方重新加密产生的摘要相互对比，如果两者一致，则说明在传送过程中信息没有破坏和篡改。否则，则说明信息已经失去安全性和保密性。

2. RSA 签名方产生一对公钥 (N,e) 和私钥 (N,d) 之后，就可以对消息进行签名。

(a) 利用摘要算法计算消息的摘要 H(M)

(b) 用私有密钥 (n,d) 加密消息摘要得到 $s = H(M)^d mod n$

(c) 签名完成后，签名房将 (M,s) 发送给对方

(d) 接收方利用摘要算法计算消息的摘要 $H(M_1)$

(e) 再用公开密钥 (n,e) 解密消息摘要得到 $s1 = s^e mod n$，比对 $s1 = H(M_1)$，如果相同则通过，否则拒绝接受。

5 消息认证 值接收方对收到的消息进行检验，检验内容包括消息的源地址、目的地址，消息的内容是否收到篡改以及消息的有效生存时间等。消息认证可以时实时的也可以是非实时的。
消息认证离不开 HASH 函数。这里介绍几个概念:

1. 单向函数，已知 x 计算 $y = f(x)$ 很容易，但是已知 y 很难求出 $x = f^{-1}(x)$

2. 哈希函数，将**可变长度**的输入映射为**固定长度**，同时不同输入应该有不同输出。哈希函数不一定是单向函数，即是哈希又是单向的成为**单向哈希函数**

3. 单向陷门函数，特殊的单向函数，在不知道秘密陷门时，很难反向计算，但是知道了秘密陷门，很容易计算反向函数。

消息认证的方式有两种

1. 采用消息认证码，需要密钥参与

2. 采用 Hash 函数，不需要密钥参与。将任意长度消息 M 映射为一个较小固定长度值 H(M)。原消息中任何一个 bit 的改变都会使得 Hash 码发生巨大改变。因此可以利用 Hash 函数检测消息传播过程中**是否遭受篡改**（类似于 CRC）。配置**非对称加密算法（如 DSA,RSA）**可进行数字签名的功能。

6 消息认证算法

MD5 输入任意长，以 512 位为单位分成快，输出是 128 为的消息摘要。步骤

1. 填充字节，增加的长度在 1-512. 从而使填充后的消息长度为 $512n - 64$。64 用来记录消息长度。
2. 分块，每块长度 512
3. 初始化寄存器
4. 处理每一个分块，由压缩函数处理
5. 输出结果

用处：

1. 防止被篡改
2. 防止直接看到明文
3. 防止抵赖（数字签名）

SHA 算法，输入上限 2^64，输出 160. 算法流程和 MD5 相同。但是在“处理每一个分块”时，压缩函数迭代次数更多。

HMAC 算法，SSL 中使用了 HMAC 算法。

7 身份认证的概念 目的是在不可信的网络上建立通信实体之间的信任关系。有

1. 口令认证
2. 智能卡认证
3. 基于生物特征的认证
4. 双因素认证
5. 基于源地址的认证
6. 基于 PAP 的认证
7. 基于 CHAP 的认证

8 身份认证协议

1. 双向身份认证协议
2. 单向身份认证协议
3. 零知识身份认证协议

9 身份认证协议实例

1. RADIUS, 远程身份验证拨入用户服务协议。用于**认证，计费，授权**
2. Kerberos。通信主体客户 A，服务器 B 以及认证服务器，票据服务器。

Chapter 4

PKI 技术

1 PKI 的概念及作用 PKI 是一个用**非对称密码算法**原理和技术来实现并**提供安全服务**的具有通用性的安全基础设施。能够为所有网络应用提供采用加密和数字签名等密码服务所需要的**密钥和证书管理**。

2 为什么需要 PKI？ 在网络、信息系统上，需要统一的、安全的认证技术

3 提供的服务

1. 认证:PKI 通过证书进行认证，这个证书是一个可信的第三方证明的，通过它，通信双方可以安全地进行互相认证，而不用担心对方是假冒的。
2. 数据保密: 通过加密证书，通信双方可以协商一个密钥，而这个密钥可以作为通信加密的密钥。
3. 完整性与不可否认: 通过数字签名和可信的第三方仲裁来保证完整性和不可否认。

4 证书内容 1、版本信息 2、序列号 3、签名算法 4、发行机构 5、有效期 6、拥有者 7、公开密钥 8、签名

5 PKI 的组成

- PKI 策略
- 软硬件系统
- 注册机构（RA）
- 认证中心（CA）**核心**
- 证书签发系统
- PKI 应用
- PKI 应用接口系统

6 PKI 互通的实现途径

1. 根 CA 之间的交叉认证。桥接
2. 全球性统一根 CA。代理

Chapter 5

防火墙

1 什么是防火墙 防火墙是一种协助确保信息安全的设施，**依照特定的规则**，允许或是禁止传输的数据通过。

2 防火墙放置位置 位于信任内部网络和不可信任的外界网络之间，如网关, 防火墙主机上的一些特定的应用程序。

3 防火墙的特性

1. 内部网络和外部网络之间的所有网络数据都必须经过防火墙
2. 只有符合安全策略的数据流才能通过防火墙
3. 防火墙自身应具有非常强的抗攻击免疫力

4 防火墙的功能

1. 防火墙是网络安全的屏障
2. 防火墙可以强化网络安全策略
3. 防火墙可以对网络存取和访问进行监控审计
4. 防火墙可以防范内部消息的外泄

5 防火墙网络层的性质指标

1. 吞吐量指标
2. 时延指标
3. 丢包率指标
4. 背靠背缓冲指标

6 防火墙常见的功能指标

1. 服务平台支持
2. LAN 口支持
3. 协议支持
4. VPN 支持
5. ...

7 防火墙核心技术

1. 包过滤技术, 在**网络层**截获网络数据包，根据防火墙的规则表，来检测攻击行为，在网络层提供较低级别的安全防护和控制
2. 应用网关技术, 又被成为代理技术，位于应用层上，所以主要采用协议代理服务。应用代理防火墙壁分组过滤防火墙提供更高层次的安全性，但这丧失对应用程序的透明性。
3. 状态检测技术，采用一种基于连接的状态监测机制，将属于同一连接的所有包作为一个整体的数据流看待，构成连接状态表，通过规则表与状态的共同配置，对表中的各个连接状态因素加以识别。**是一种动态的判定方法。（前两种为静态）**Steps:
   - 检查是否属于一个已建立的连接
   - 若已建立，则根据连接状态表的策略对数据包实施丢弃、拒绝或是转发。
   - 若未建立连接，会检查数据包是否与他配置的规则集匹配。

8 防火墙分类

1. 个人防火墙
2. 分布式防火墙
3. 分层式防火墙

9 防火墙的体系结构, 部署位置

基本概念:

1. 堡垒主机，一种被强化的可以防御攻击的计算机，作为进入内部网络的一个检查点。堡垒主机是网络中**最容易受到侵害**的主机。**包过滤路由器和应用代理服务器均可视为堡垒主机**。
2. 非军事区，也成为“隔离区”，他是为了解决安装防火墙后，外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。

体系结构分类:

1. 筛选路由器体系结构。
2. 单宿主堡垒主机，由包过滤路由器和堡垒主机构成。外部路由器配置把所有进来的数据发送到堡垒主机上，所有出去的数据包也经过堡垒主机（代理）。实现了网络层安全（包过滤）和应用层安全（代理服务）。缺点: 可通过重新配置路由器，使数据绕过堡垒主机。
3. 双宿主堡垒主机，与单宿主堡垒主机的区别在于，双宿主堡垒主机有两块网卡，一块连接内部网络，一块连接包过滤路由器，但是主机两个端口之间直接转发信息的功能被关闭。在应用层提供代理服务
4. 屏蔽子网体系结构：由两个包过滤路由器和一个堡垒主机构成，支持网络层和应用层的安全功能。在定义非军事区 (DMZ)，即屏蔽子网后。存在内部防火墙和外部防火墙。攻击者要通过外部防火墙，堡垒主机和内部防火墙三道防线，才能到达内部网络。

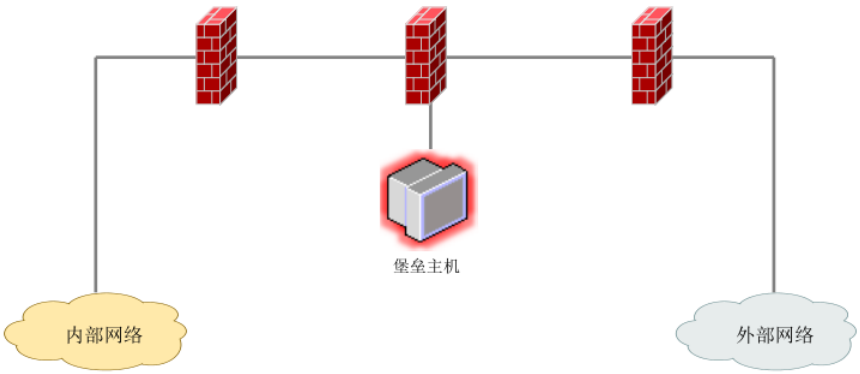


Figure 5.1:

10 常见产品

1. Firewall
2. PIX
3. AXENT Raptor
4. NetScreen
5. 天融信网络卫士
6. 东软 NetEye 4032 防火墙

Chapter 6

入侵检测

1 什么是入侵检测 指“通过对行为、安全日志、审计数据或其他网络上可以获取的信息进行分析，对系统的闯入或闯出的企图进行检测”的安全技术。

2 入侵检测系统分类

1. 按入侵检测的数据来源分类
   (a) HIDS, 以主机数据作为分析对象，通过分析主机内部活动痕迹，如系统日志、系统调用、系统关键文件完整性等，判断主机上是否有入侵行为发生。
   (b) NIDS, 以一种或者多种网络数据作为分析对象，用一定的分析方法，判断在主机或网络中是否有入侵行为发生。
   (c) HIDS，混合 IDS。
2. 按使用的入侵检测分析方法分类
   (a) 误用检测，用恰当的方法分析、提取并表示隐藏在具体入侵行为中的内在代表性特征，形成相应的**入侵模式库**，并以此为依据实现对目标流量的有效检测和行为发现。**缺点：**不能检测模式库中没有现存模式的未知入侵。需要及时更新入侵模式库。
   (b) 异常检测，对正常状态下的系统行为建立模型，然后将所有观测到的和目标对象相关的活动与建立的系统正常行为模型进行比较，将与系统正常行为模型不相符的活动判定为可以或入侵行为。**缺点：**误警率较高。尚未商用
   (c) 混合检测，综合上述两种方法，以模式为主，异常为辅。
3. 按系统体系结构分类
   (a) 集中式 IDS，由一个入侵检测服务器和分布于不同主机的多个审计程序组成，主要适用于小型网络中的入侵程序
   (b) 分布式 IDS，针对比较复杂的网络，各组件分布在网络中不同的计算机或设备上，其分布性主要体现在**数据收集**和**数据分析**上。
4. 在线 IDS（实时性高，占用资源）；离线 IDS（实时性不高，节约资源）
5. 主动响应（发现并阻断攻击）；被动响应 (警告和记录)
6. 连续 IDS，周期 IDS。

3 入侵检测系统体系结构

1. 集中式体系结构
   - 优点：全面掌握采集到的数据，从而对入侵检测分析更加精确
   - 缺点：可扩展性差；改变配置和加入新功能困难；存在单点失效的问题
2. 分布式体系结构
   - 优点：较好的完成数据的采集和检测内外部的入侵行为。
   - 缺点：现有的网络普遍采用的是层次化的结构，**纯分布式的入侵检测要求所有的代理处于同一层次上**，如何代理所处的层次过低，则无法检测针对网络上层的入侵行为，反之则不无法检测下层。
3. 分层式体系结构，树状结构
   - 底层，收集所有的基本信息，然后对信息进行简单的处理。**处理速度快，数据量大**
   - 中间层，连接上下层，起到代理的作用。减轻了中央控制台的负载压力，体改了系统的可伸缩性
   - 中央控制台，负责在整体上对各级带进行协调和管理

4 入侵检测技术

1. 基于行为的检测方法
   (a) 概率统计方法
   (b) 人工神经网络
   (c) 人工免疫系统
2. 基于知识的入侵检测技术
   (a) 专家系统
   (b) 模型退你
   (c) 状态转换分析

Chapter 7

虚拟专用网

1 什么是 VPN VPN 是一种依靠互联网服务提供商和其他网络服务提供商**在公共网络中建立专用的数据通信网络的技术**

- 它是虚拟的网，即没有固定的物理连接，网络只有用户需要时才建立
- 他是利用公共网络设施构成的专用

2 VPN 的关键技术 ，通过各种技术满足通信安全，实现**身份认证**、**数据保密性**、**数据完整性**

1. 隧道技术，将一种协议封装在另一种协议中传输，从而实现协议对公共网络的透明性
2. 加密技术，隐藏传输信息的真实内容
3. 密钥管理技术，确保在公网数据网上安全地传递密钥而不被窃取。
   (a) 手工配置，小网，更新不快
   (b) 密钥交换歇息动态分发，适合复杂网，快速更新。需要 PKI。-
4. 用户认证技术
   (a) 仲裁认证
   (b) 共享认证

3 隧道协议 ，根据协议所处的网络层次，可分为第二层隧道协议和第三层隧道协议。

1. 第二层隧道协议，工作在数据链路层，吧龚总网络协议先封装到点对点协议中 (PPP)，然后进行隧道协议的封装，在通过数据链路层进行传输。
   (a) PPTP，点对点隧道协议。
   (b) L2FP，第二层转发协议
   (c) L2TP，第二层隧道协议
   (d) MPLS，多协议标记交换
2. 第三层隧道协议，工作在网络层
   (a) GRE, 通用路由协议封装，主要规定如何用一种网络层协议去封装另一种网络层协议，不提供**加密功能**，常与 IPSec 一起使用，由 IPSec 提供加密。
   (b) IPSec，IP 安全协议。可以对所有 IP 级的通信进行加密和认证。
3. 高层隧道协议

(a) 安全套阶层 SSL。位于 TCP/IP 与各种应用层协议之间，广泛地用于 Web 浏览器与服务器之间的身份认证和加密数据传输

i. SSL 记录协议。它建立在可靠的传输协议（如 TCP）之上，为高层提供**数据封装**、**压缩**、**加密**等基本功能的支持

ii. SLL 握手协议。建立在 SSL 记录协议之上，用在实际的数据传输开始前，通信双方进行身份认证、协商加密算法、交换加密密钥等。

4 IPSec VPN IPSec VPN 是 IPSec 的一种应用方式，其主要的应用场景可分为三种：

1. Site-to-Site（站点到站点或者网关到网关）。如一个机构的按个分之爱机构分布在互联网的 3 个不同地方，各使用一个网关相互简历 VPN 隧道，在机构内部网络之间的数据通过这些网关简历的 IPSec 隧道实现安全互联。
2. End-to-End（端到端或主机到主机）：两个主机之间的通信由两台主机之间的 IPSec 绘画保护，而不是网关。
3. End-to-Site(端到站点或主机到网关)：两台主机之间的通信由网关和异地户籍之间的 IPSec 进行保护

5 IPSec 的设计目标

1. 可认证 IP 报文的来源
2. 可保证 IP 报文的完整性
3. 可保护 IP 报文的私密性
4. 可防止认证报文被重放。

6 IPSec 的体系结构 textbf 包括：

1. AH，验证头。为 IP 数据包提供无连接完整性与数据源认证，并提供保护以避免重播情况。**信息源的认证**、**信息的完整性防御**、**报文重发**
2. ESP，封装安全载荷。加密需要保护的数据并且在 IPSec ESP 的数据部分进行数据的完整性校验，一次来保证机密性和完整性。**信息源的认证**、**信息的完整性**、**数据的私密性**、**防御报文重发**
3. IKE，密钥管理协议, 协商 AH 和 ESP 所使用的密码算法。
   (a) SA（安全联盟）, 描述通信对等体间对某些要素的约定，**单向的**，实现双向通信，至少需要两个方向的数据流进行安全保护。**建立方式:** 手工配置或者采用 IKE 自动协商方式。
   (b) 和 (ISAKMP) 密钥管理协议。
4. 用于验证和加密的一些算法

IPSec 工作时，首先两端的网络设备必须就 SA 达成一致。

7 IPsec 驱动程工作流程

1. 主机 A 向主机 B 发送一消息
2. 主机 A 上 IPsec 驱动程序检查 IP 筛选器，查看数据包是否需要加密以及需要受到何种保护
3. 驱动程序通知 IKE 开始安全协商
4. 主机 B 上的 IKE 收到请求安全协商的通知
5. 两台主机建立第一阶段 SA 对，各自共享主密钥
6. 协商建立第二阶段 SA 对 xxxx

P154

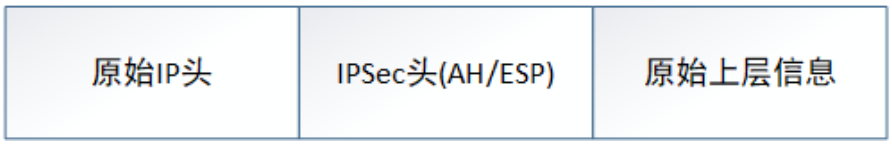


Figure 7.2:

8 IPSec 的工作模式

1. 隧道模式：封装了整个 IP 数据包，经过 IPSec 处理之后，在封装了一个外网 IP 头，主要用于 Site-to-Site

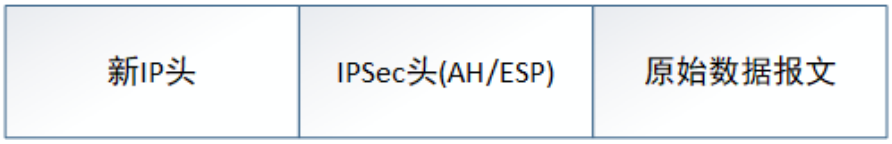


Figure 7.1:

2. 传输模式：仅仅封装 IP 数据包中上层协议信息，经过 IPSec 处理前后 IP 头部保持不变。主要用于 End-to-End 的应用场景。

9 AH 和 ESP

1. AH 提供身份验证、完整性和防止重发，包含整个数据包的签名

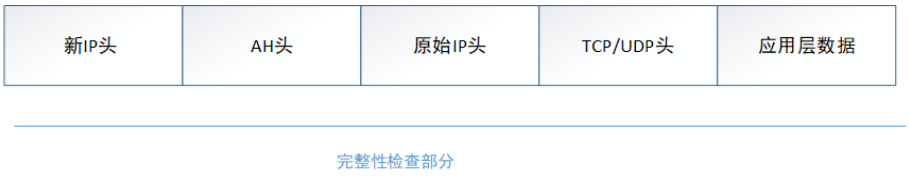


Figure 7.3:

2. ESP 除了 AH 的全部功能，还包括加密。通常不签署整个数据包，即通常只保护数据，而不保护 IP 头。ESP 使用 DES 或者 3DES 加算法为数据包提供保密性。

Figure 7.4:

功能比较图：P155

10 如何给一个信息系统定级

信息系统定级需要考虑的两个重点：

1. 受侵害客体

- 国家安全
- 社会秩序
- 个人安全

2. 受侵害的程度
    - 一般影响
    - 严重影响
    - 特别严重影响

信息系统定级需要考虑的两个方面

1. 信息安全：信息泄露、信息篡改
2. 服务安全

11 等级保护的等级划分准则 分为五级、级别越高危害程度越大。

Chapter 8

网络安全技术

1 安全漏洞 ，在硬件、软件、协议的具体实现或系统安全策略上存在缺陷，从而使攻击者能够在未收钱的情况下访问或破坏系统。
分为三级安全漏洞

1. A 级漏洞，允许恶意入侵者访问斌可能会破坏整个目标系统的漏洞，是威胁最大的一种漏洞。如允许远程用户未经授权访问
2. B 级漏洞, 允许本地用户提供访问权限，并可能允许其获得系统控制的漏洞
3. C 级漏洞, 允许用户中断，降低或阻碍系统操作的漏洞，如拒绝服务漏洞。

2 网络攻击的一般流程

- 信息的收集
- 系统安全缺陷探测
- 实施攻击
- 巩固安全成果

3 网络攻击分类

- 主动攻击，攻击者访问他所需信息必须要实施其主管上的故意行为。如拒绝服务攻击
- 被动攻击，主要收集信息而不是进行访问。如攻击嗅探。

4 网络探测 探测是攻击者在攻击开始前必须的情报搜集工作，同行包括

1. 踩点，攻击者手机攻击目标相关信息的方法和步骤，了解攻击目标的基本情况
2. 扫描，攻击者获取活动主机、来访服务、操作系统、安全漏洞等关键信息的重要技术
   (a) TCP 连接扫描
   (b) TCP SYN 扫描
   (c) TCP FIN 扫描
   (d) TCP ACK 扫描
   (e) TCP 窗口扫描
   (f) TCP RPC 扫描
   (g) UDP 扫描
   (h) ICMP 扫描
3. 网络查点，从目标系统中抽取有效账号或到处资源名的技术，通过主动目标系统建立连接来获取信息，因此这种探测方式在本质上要比网络彩电和网络扫描更具有入侵效果。

5 常见扫描工具 Nmap,PortScan 等。

6 网络欺骗 常见的网路欺骗包括 **IP 源地址欺骗、DNS 欺骗和源路由选择欺骗**

1. IP 源地址欺骗，伪造某台主机的 IP 地址的技术。通过 IP 地址的伪造使得某台主机能够伪装成另外一台主机，而这台主机往往具有某种特权或者被另外的主机所信任。
2. DNS 欺骗，将域名和 IP 地址映射篡改，用户访问的将不是原来的 IP。
3. 源路由选择欺骗，源路由是指在数据吧收不中列些除了所要经过的路由。某些路由器对源路由的反映是使用其指定的路由，并使用其反向路由来传送应答。要实现源路由选择欺骗，必须满足：1.IP 地址欺骗。2. 路由器支持源路由。

7 拒绝服务攻击 ，攻击这设法使目的主机停止提供服务，耗尽目标主机的通信、存储或计算资源的方式来迫使目标主机暂停服务。

1. DOS
   (a) SYN 泛洪
   (b) UDP 泛洪, 带宽攻击。
   (c) Ping 泛洪
   (d) 泪滴攻击
   (e) Land 攻击，源地址和目的地址都是服务器地址，建立空连接
   (f) Smurf 攻击，反弹攻击。伪造目的地址为目标主机地址。
2. DDos, 攻击主机操作大量傀儡主机同时向目标主机进行进攻的方式。

8 Dos 防范方法

1. 关闭不必要的服务
2. 限制同时打开的 SYN 半连接数目
3. 缩短 SYN 半连接的超时等待时间
4. 及时更新系统补丁

9 缓冲区溢出攻击

10 SQL 注入攻击 ，攻击者提交一段数据库查询代码，根据程序返回的结果，获得某些想得知的数据，这就是所谓的 SQL 注入攻击

原理 通过构建特殊的输入，将这些输入作为参数传入 Web 应用程序，通过执行 SQL 语句而执行入侵者想要的操作。

步骤
1. 寻找 SQL 注入点
2. 获取和验证 SQL 注入点
3. 获取信息
4. 实施直接控制
5. 实施间接控制

防范只有依赖于编程过程中严格设计和仔细检查。

11 计算机病毒 ，一种认为制造的，在计算机运行中对计算机信息或系统起到破坏作用的程序。包含以下**特性**。

1. 寄生性。依附于某种类型的文件上
2. 可执行性。
3. 传染性。
4. 潜伏性
5. 可触发
6. 破坏性
7. 不可预见性
8. 针对性
9. 衍生性

12 木马攻击 ，一种常用语网络攻击的特殊**软件**。一个完整的木马包含两个部分：**服务端和客户端**。攻击者可利用客户端对安装了服务端的主机进行远程控制。通常在目标主机运行木马程序的服务端后，会秘密打开一个特定的端口，用于接收攻击者发出的指令或向指定的目的地发送数据.

13 病毒与木马的区别 木马在本质上一种基于**客户/服务器模式**的远程管理工具，一般不具备自我传播能力，而是作为一种实施攻击的手段被病毒植入目标系统的主机中。

Chapter 9

操作系统安全

1 操作系统 充当着用户程序与计算机硬件之间的接口，负责提供用户与计算机系统的交互界面和环境，其目的是最大限度地、高效低、合理地使用计算机资源，同时对系统的所有资源进行管理。

2 操作系统的安全问题 物理分离、时间分离、逻辑分离、加密分离

3 操作系统的安全机制 内存保护机制、特征位、文件保护机制、用户鉴别机制、存取控制机制、恶意程序防御机制。

4 安全操作系统的设计方法 隔离设计、内核化设计、分层结构设计

5 向上读向下写

Chapter 10

计算机软件安全

1 什么是软件安全 软件安全是在软件生命周期中, 运用系统安全工程的技术原则保证软件采取正确的措施以增强系统安全, 确保那些使系统安全性降低的错误已被消除或已被控制在一个可接受的危险级别内

2 软件安全保护什么？ 软件的完整性、可用性、保密性、运行安全性。

3 软件安全

1. 软件自身安全
   (a) 软件自身完整性
   (b) 软件自身可信性
   (c) 隐蔽通道, 秘密的和未公开发表的进入软件模块的入口
2. 软件存储安全
   (a) 存储介质（磁盘）的可靠性
   (b) 文件系统的组织结构
3. 软件通信安全
   (a) 安全传输
   (b) 加密传输
   (c) 网络安全下载
   (d) 完整下载
4. 软件运行安全
   (a) 软件运行正确性
   (b) 运行日期和时间
   (c) 软件补丁

4 软件安全保护机制

1. 软件防复制（存储访问技术）
2. 软件防执行（运行控制技术）
3. 软件防暴露（加密解密技术）
4. 软件防篡改（完整可用技术）

5 软件安全性测试

安全性测试的目的 在测试软件系统中对程序的危险防止和危险处理进行的测试，以验证其是否有效

安全性测试方法 1. 功能验证

2. 漏洞扫描
3. 模拟攻击

Chapter 11

数据集数据库系统安全

1 什么是数据库 按照数据结构来组织、存储和管理数据的仓库。

2 数据备份 将数据已某种方式保留，当系统遭到破坏或者其他特定情况下重新加以利用。其核心是**恢复**

3 复制与备份的区别

- 数据复制关注的是当前数据，数据复制能够保证当前数据的一致，但对病毒攻击、人为误操作等数据损坏是无能为力的
- 数据备份关注的是历史数据，数据备份能够解决历史数据的恢复，当数据遭到病毒攻击、人为误操作时我可以通过数据备份恢复到前一个时间点的正常状态

4 构建备份系统的三要素

- 备份源点
- 存储设备
- 存储软件

5 热备份 阵列中某一磁盘发生故障时，热备磁盘便取代故障磁盘，并自动将故障磁盘的数据重构在热备磁盘上，热备不具有修复故障服务器的功能，而只是将故障隔离

6 数据备份的类型

1. 全备份：备份系统中的**所有数据**
   - 优点：恢复时间最短，最可靠，操作最方便
   - 缺点：备份的数量大，备份所需时间长
2. 增量备份：备份上一次 **备份**以后更新的所有数据
   - 优点：每次备份的数据少，占用空间少，备份时间短
   - 缺点：恢复时需要全备份及多份增量备份
3. 差量备份：备份上一次 **全备份**以后更新的所有数据
   - 优点：数据恢复时间短
   - 缺点：备份时间长，恢复时需要全备份及差量备份
4. 按需备份：根据临时需要有选择地进行备份

7 RAID 与 JBOD 是什么？

- RAID：(冗余独立磁盘阵列系统; 盘阵) 是一种磁盘集群技术
- JBOD:(只是一组盘, 磁盘组) 是在逻辑上把几个物理磁盘一个接一个的串联在一起，其目的纯粹是为了增加磁盘的容量，并**不提供数据安全保障**。

8 常见 RAID

RAID级别	RAID 0	RAID 1	RAID 3	RAID 5	RAID 10
容错性	无	有	有	有	有
冗余类型	无	镜像冗余	校验冗余	校验冗余	镜像冗余
可用空间	100%	50%*	(N-1)/N	(N-1)/N	50%*
读性能	高	低	高	高	普通
随机写性能	高	低	低	低	普通
连续写性能	高	低	低	低	普通
最少磁盘数	2个	2个	3个	3个	4个
应用场景	传输带宽需求大的应用	安全性要求较高的应用	大文件、连续数据的应用	读/写比率较高的应用	安全性要求高的应用

Figure 11.1:

9 存储网络的三种形态比较

	DAS（直连式存储）	NAS（网络连接式存储）	SAN（存储区域网络)
传输类型	SCSI、FC	IP	IP、FC、SAS
数据类型	数据块	文件	数据块
典型应用	任何(适用于小型机构的存储解决)	文件服务器	数据库应用

Figure 11.2:

10 数据库安全

定义 指保护数据库以防止非法用户访问数据库，造成数据泄露、更改或破坏

网络环境下 数据库的安全性与网络系统层、操作系统层、数据库管理系统层有关