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

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。

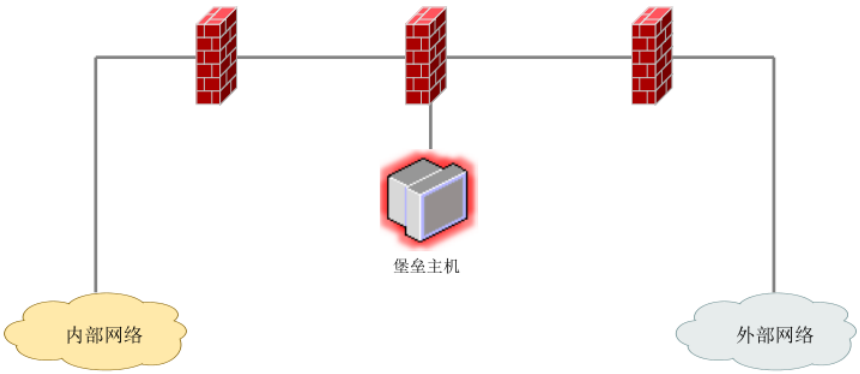

Figure 2.1:

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 3

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 4

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

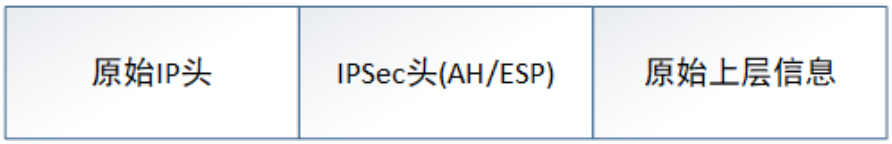

Figure 4.2:

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

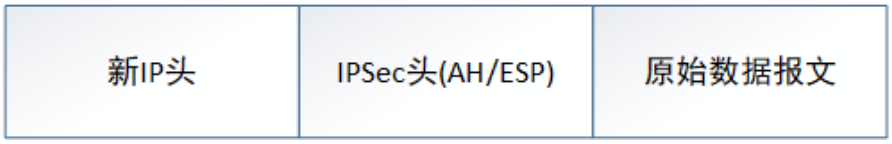

Figure 4.1:

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 Site-to-Site 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

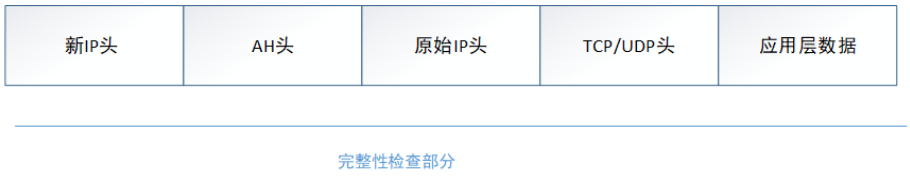

Figure 4.3:

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 4.4:

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。