IPSec

郑燕飞

主要内容

- IP安全
  - IP安全体系结构
  - 认证首部(AH)
  - 封装安全有效负载(ESP)

IPSec引言

- 1994年IAB(Internet Architecture Board)发表一份报告“ Internet体系结构中的安全性 ”(RFC1636)
  - 保护网络基础设施，防止非授权用户监控网络流量
  - 需要认证和加密机制增强用户-用户通信流量的安全性。

IP安全性概要

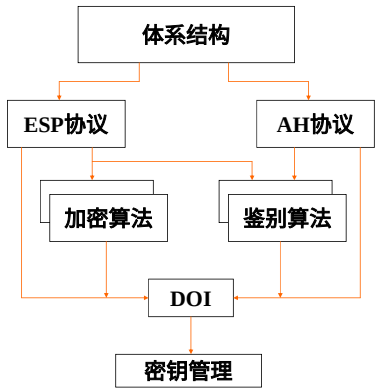
- IAB决定把认证和加密作为下一代IP的必备安全特性(IPv6)
- IPv4也可以实现这些安全特性。
- IP级安全问题涉及三个功能领域：认证、保密和密钥管理。

IPSec的应用

- IPSec提供对跨越LAN/WAN，Internet的通讯提供安全性
  - 分支办公机构通过Internet互连。(Secure VPN)
  - 通过Internet的远程访问。
  - 与合作伙伴建立extranet与intranet的互连。
  - 增强电子商务安全性。
- IPSec的主要特征是可以支持IP级所有流量的加密和/或认证。因此可以增强所有分布式应用的安全性。

IPSec的好处

- 在防火墙或路由器中实现时，可以对所有跨越周界的流量实施强安全性。而公司内部或工作组不必招致与安全相关处理的负担。
- 在防火墙中实现IPSec可以防止IP旁路。
- IPSec是在传输层(TCP,UDP)之下，因此对应用透明。不必改变用户或服务器系统上的软件。
- IPSec可以对最终用户透明。无须训练用户。
- 需要时IPSec可以提供个人安全性。这对非现场工作人员以及在一个组织内为一个敏感应用建立一个安全的虚拟子网是有用的。



- 体系结构：包括总体概念，安全需求，定义，以及定义IPSec技术的机制；
- ESP(Encapsulating Security Payload) ： 使用ESP进行包加密的报文包格式和一般性问题，以及，可选的认证
- AH (Authentication Header) ：使用ESP进行包加密的报文包格式和一般性问题；
- 加密算法：描述将各种不同加密算法用于ESP的文档
- 认证算法：描述将各种不同加密算法用于AH以及ESP认证选项的文档；
- 密钥管理：描述密钥管理模式；
- DOI： 其它相关文档，批准的加密和认证算法标识，以及运行参数等；

IPSec的主要目标

- 期望安全的用户能够使用基于密码学的安全机制
  - 应能同时适用与IPv4和IPv6, IPng.
  - 算法独立
  - 有利于实现不同安全策略
  - 对没有采用该机制的的用户不会有副面影响
- 对上述特征的支持在IPv6中是强制的，在IPv4中是可选的。都是采用在主IP报头后面接续扩展报头的方法实现的。

IPSec提供的服务

- IPSec在IP层提供安全服务，使得系统可以选择所需要的安全协议，确定该服务所用的算法，并提供安全服务所需任何加密密钥。
  - 访问控制
  - 连接完整性
  - 数据源认证
  - 拒绝重放数据包
  - 保密性（加密）
  - 有限信息流保密性

	AH	ESP(仅加密)	ESP(加密+认证)
访问控制	√	√	√
连接完整性	√		√
数据源认证	√		√
拒绝重放包	√	√	√
保密性		√	√
有限保密性		√	√

安全关联SA(Security Association)

- SA是IP认证和保密机制中最关键的概念。
- 一个关联就是发送与接收者之间的一个单向关系。
- 如果需要一个对等关系，即双向安全交换，则需要两个SA。
- 一个SA由一个Internet目的地址、一个安全变量SA索引SPI、安全协议标志符唯一标识。因此，任何IP包中，SA是由IPv4中的目的地址或IPv6目的地址和内部扩展头（AH或ESP）中的SPI所唯一标识的。

- SA由三个参数唯一确定：
  - Security Parameters Index(SPI)：安全变量索引。分配给这个SA的一个位串并且只有本地有效。SPI在AH和ESP报头中出现，以使得接收系统选择SA并在其下处理一个收到的报文。
  - IP目的地址：目前，只允许单点传送地址；这是该SA的目标终点的地址，它可以是一个最终用户系统或一个网络系统如防火墙或路由器。
  - 安全协议标识符：表明是AH还是ESP的SA

SA的参数

- 序数计数器：一个32位值用于生成AH或ESP头中的序数字段；
- 计数器溢出位：一个标志位表明该序数计数器是否溢出，如果是，将生成一个审计事件，并禁止本SA的进一步的包传送。
- 防回放窗口：用于确定一个入站的AH或ESP包是否是一个回放
- AH信息：认证算法、密钥、密钥生存期、以及与AH一起使用的其它参数
- ESP信息：加密和认证算法、密钥、初始值、密钥生存期、以及ESP一起使用的其它参数
- SA的生存期：一个时间间隔或字节记数，到时后一个SA必须用一个新的SA替换或终止，以及一个这些活动发生的指示。
- IPSec协议模式：隧道、运输、统配符。
- 通路MTU：任何遵从的最大传送单位和老化变量

SA选择符

- IP信息流与SA关联的手段是通过安全策略数据库SPD(Security Policy Database)
- 每一个SPD入口通过一组IP和更高层协议域值，称为选择符来定义。
- 以下的选择符确定SPD入口：
  - 目的IP地址：可以是单地址或多地址
  - 源地址：单地址或多地址
  - UserID: 操作系统中的用户标识。
  - 数据敏感级别：
  - 传输层协议：
  - IPSec协议（AH, ESP, AH/ESP)
  - 源/目的端口
  - 服务类型(TOS)

Authentication Header（AH）

- Next Header(8bits)
- Payload Length(8bits)
- Reserved (16bits)
- Security Parameters Index(32bits)
- Sequence Number
- Authentication Data(variable):一个变长字段，包含ICV(Integrity Check Value) 或MAC

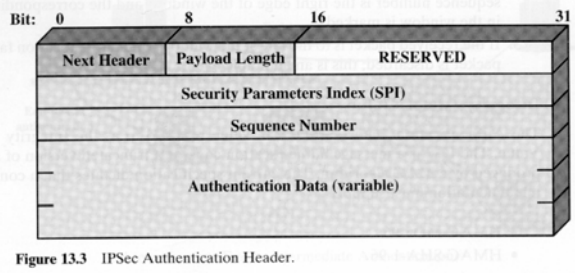


Figure 13.3 IPSec Authentication Header.

IPSec认证头

窗口与回放攻击检测

- 如果收到的包落在窗口中并且是新的，其MAC被检查。如果该包已被认证，则对应的窗口项做标记。
- 如果接收包已到窗口右边并且是新的，其MAC被检查。如果该包一被认证，窗口向前运动，让该包的顺序号成为窗口的右端，对应的项做标记。
- 如果接收的包在窗口的左边，或认证失败，该包被丢弃，并做审计事件记录。

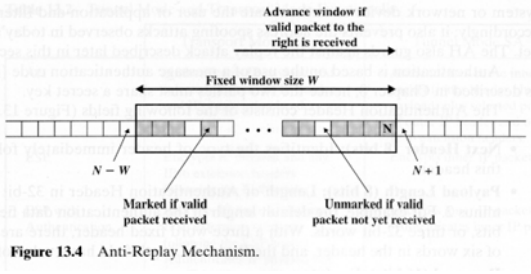
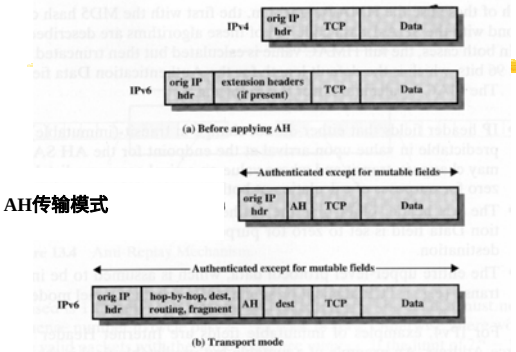


Figure 13.4 Anti-Replay Mechanism.

ICV/MAC计算

- ICV计算应支持: HMAC-MD5-96、HMAC-SHA-1-96, 仅用96位。
- MAC计算所有变化的字段填0后参与运算

AH传输模式



AH隧道模式

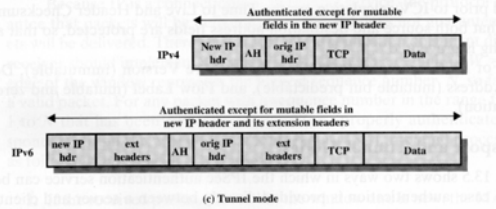


Figure 13.6 Scope of AH Authentication.

封装安全负载ESP

- 格式
- 算法
  - 3DES、RC5、IDEA、3IDEA、CAST、Blowfish

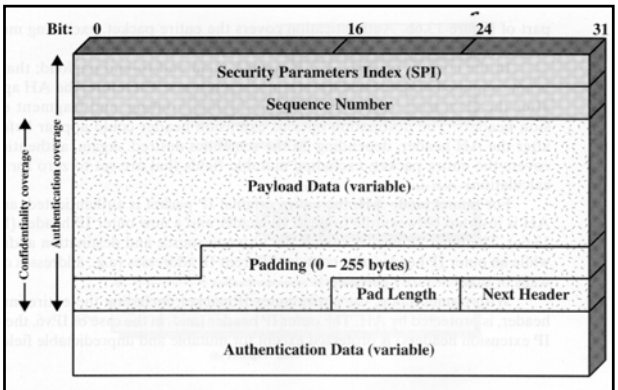
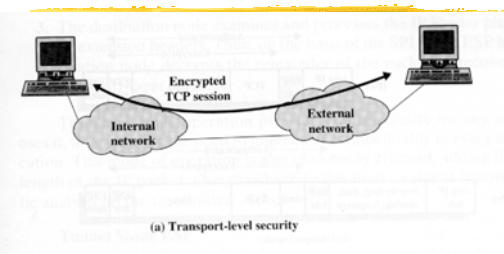


Figure 13.7 IPSec ESP Format.

ESP传输与隧道模式

- 下图显示使用IPSec ESP服务的两种方式：
  - 传输级的安全性
  - 隧道方式

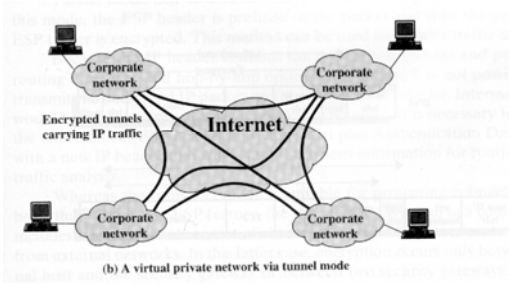
加密的TCP会话



(a) Transport-level security

两个主机之间的加密

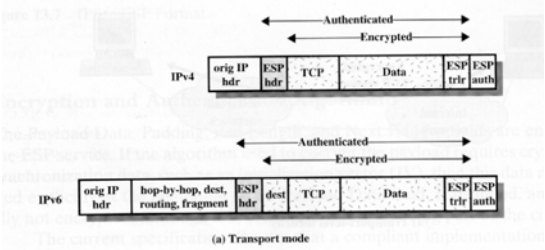
基于隧道方式的VPN



(b) A virtual private network via tunnel mode

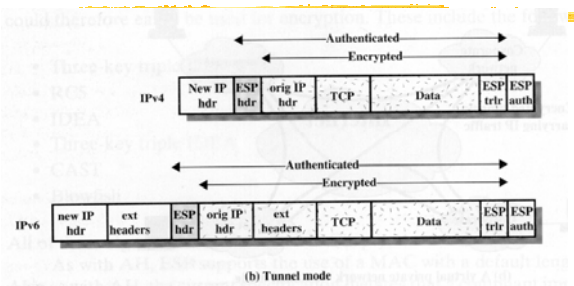
加密隧道运送IP信息流

ESP的传输模式



(a) Transport mode

ESP的隧道模式



(b) Tunnel mode

SA的组合

- 安全关联可以用两种方式组合
  - 传输邻接
  - 循环隧道
- 安全关联的基本组合

密钥管理

- 手工
- 自动
  - 模块密钥管理协议MKMP(IBM)
  - 简单Internet密钥管理协议SKIP(SUN)
  - Internet安全关联密钥管理协议ISAKMP(NSA)
  - OAKLEY密钥判定协议（Hilarie Orman)

END!