信息安全作业 11

190110429-何为

1. IPSec 的两个主要协议有什么区别?

答:

（1） 协议提供的服务

ESP 协议对 IP 数据报文实施加密和可选认证双重服务，提供了数据保密性、有限的数据流保密性、数据源认证、无连接的完整性以及抗重放攻击等服务。

AH 协议对 IP 数据报文实施认证服务，提供数据源认证、无连接的完整性以及一个可选的抗重放服务。

（2） 保护范围

AH 协议和 ESP 协议都支持认证功能，但二者保护范围存在着一定的差异。AH 的作用域是整个 IP 数据包，包括 IP 头和承载数据。ESP 认证功能的作用域只是承载数据，不包括 IP 头。

（3） 认证的安全性

理论上讲，AH 所提供的认证的安全性高于 ESP 的认证服务。

2. IPSec 是如何防范重放攻击的?

答:

抵御重放攻击主要方法包括:

（1） 序列号:

（2） 时间戳（Timestamp）:

（3） 盘问/应答方式（Challenge/Response）:

而 IPSec 为了抵御重放攻击，在安全关联 SA 中定义了序号计数器和抗重放窗口。

序号计数器提供了设置 IPSec 包中序列号域的值，当新 SA 建立后，发送方将序号计数器的初值置为 0，每发送一个包，计数器的值加 1 并并置于序列号域中，直至 2^32-1。如需提供抗重放服务，则发送方不允许重复计数。当序列号达到 2^32 时，原 SA 必须终止，并产生新的 SA 继续工作。

抗重放窗口 W 实际上就是某个特定时间接收到的数据包序号是否合法的上、下界，同时窗口具有滑动功能。若序列号 sn 在窗口 W 内，则检查该序列号的相应位置是否被标记，如未标记，则接收此数据包，并做标记；如已标记，则为重放，丢弃此数据包。若序列号 sn 在窗口 W 左侧，则为重放，丢弃此数据包。若序列号 sn 在窗口 W 右侧，且数据包通过 MAC 验证，则窗口向右滑动。