网络安全协议及分析
应用安全

密码与网络安全系　刘虹

2025年春季学期

课程体系

第一章 概述

第二章 链路层扩展L2TP

第三章 IP层安全IPSec

第四章 传输层安全SSL和TLS

第五章 会话安全SSH

第六章 代理安全Socks

第七章 网管安全SNMPv3

第八章 认证协议Kerberos

第九章 应用安全

本章学习目标

- 熟悉DNS安全DNSsec
- 熟悉Web安全SHTTP

提纲

一、DNS安全DNSsec

二、Web安全SHTTP

DNS安全

- DNS安全DNSsec
  - 不改变DNS的框架和报文格式，而是以新的资源记录（Resource Record，RR)的形式进行了安全扩展。
- DNS面临的安全威胁：DNS欺骗
  - 数据窃听和篡改
  - ID猜测和请求预测
  - 名字连锁攻击
  - 信任服务器背叛
  - 否认域名的存在
  - 通配符

DNS安全

- DNSsec思想
  - 从实际看，DNS面临的主要安全风险就是DNS欺骗，即恶意攻击者通过发送伪造的DNS应答报文将被攻击者导向恶意网站。
  - DNS欺骗可通过两种途径实现：
    - 一是伪装成DNS服务器
    - 二是篡改DNS应答消息
  - DNSsec利用数字签名技术提供对DNS消息的认证功能，包括
    - 数据源发认证和完整性校验
    - 提供与公钥分发有关的机制

提纲

一、DNS安全DNSsec

二、Web安全SHTTP

二 Web安全

- **HTTPS=HTTP+SSL（TLS）**
- **SHTTP：并未改变HTTP协议框架，利用HTTP报文的首部，扩展了新的选项，提供三种安全保护：**
  - **加密：基于加密的消息机密性保护**
  - **基于MAC的认证：基于MAC的完整性保护和数据源发认证**
  - **签名：基于数字签名的认证和不可否认性保护**

二 Web安全

- SHTTP支持以下密钥交换方式：
  - 带内（inband）：会话密钥直接放在HTTP报文的首部
  - 带外（outband）：接收方可以通过关键字匹配数据库或配置文件以获取事先配置的密钥。
  - D-H交换方式：传递密钥素材
  - 基于RSA公钥加密的密钥传输方式

二 Web安全

- SHTTP应用
  - SHTTP能够提供客户端和服务器不可否认性，但HTTPS不具备这项功能；
  - SHTTP是应用层协议，防火墙可以对相关行为进行检测，但防火墙无法看到除端口外SHTTP报文的任何信息；
  - SHTTP比HTTPS更为灵活，比如可以选择任意安全服务的组合；
  - HTTPS需依托证书，但SHTTP没有此限制。

办公地点：理科大楼B1209

联系方式：17621203829

邮箱：liuhongler@foxmail.com