主要内容

- **网络安全**
  - 网络协议的脆弱性
  - Internet的安全协议
  - 匿名通信（选）
  - 无线网络安全概述（选）

注意：

- 在课程中心截止期前 每人提交大作业技术报告
- 期末考试时间
  - 19周： 1月15日（周五）时间： 19:00-21:00地点： 主M202

网络安全概述

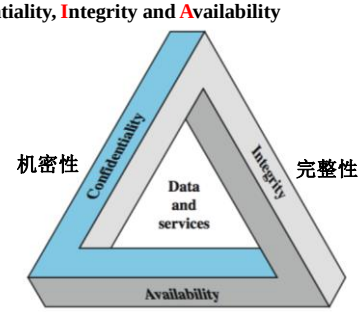
概念和协议

网络安全：CIA三元组

- **机密性Confidentiality**
  - 机密性是指保证信息不能被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用
    - 数据机密性
    - 隐私性
- **完整性Integrity**
  - 完整性是指维护信息的一致性，即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改。
    - 数据完整性
    - 系统完整性
- **可用性Availability**
  - 可用性是指保障信息资源随时可提供服务的能力特性，即授权用户根据需要可以随时访问所需信息

核心概念：CIA三元组

Confidentiality, Integrity and Availability

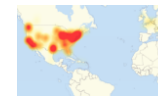


网络安全事件-1

- 2014年4月7日，OpenSSL宣布在OpenSSL 1.0.2-beta及1.0.1系列（2012年3月14日发布，除1.0.1g）的所有版本中，其所实现的TLS心跳扩展存在严重的内存处理错误.
  - 心脏出血漏洞（Heartbleed bug），CVE-2014-0160
  - 是OpenSSL中的一个漏洞,自2011年12月31日，漏洞就已经存在。会使攻击者可读取受攻击服务器的部分内存，可能会泄漏服务器的用户数据。
  - 黑客可以对使用https(存在此漏洞)的网站发起攻击，每次读取服务器内存中64K数据，不断的反复获取，内存中可能会含有用户http原始请求、用户cookie甚至明文帐号密码等。
  - 使用https的网站，包括微信、淘宝、网银、社交、门户等。

5

网络安全事件-2



- 2016年10月21日Dyn网络攻击
  - 拒绝服务攻击，目标是域名系统提供商Dyn公司。这些攻击造成服务器位于欧洲和北美的大型互联网平台和服务无法直接访问。
  - 由众多物联网设备（包括网络监控摄影机、家庭路由器和婴儿监视器）组成的一个僵尸网络发起，这些设备均已感染了Mirai恶意软件
  - 这场攻击估计有1.2Tbps的流量，是迄今为止规模最大的网络攻击
    - 第一波攻击：7:10 – 9:20 EDT
      第二波攻击：11:50 – 13:11 EDT
      第三波攻击：16:00 – 18:11 ED

6

网络安全事件-3

- 2017年5月，勒索病毒WannaCry（WannaCrypt、WanaCrypt0r 2.0、Wanna Decryptor）
  - 利用美国国家安全局NSA的“永恒之蓝”（EternalBlue）漏洞利用程序通过互联网对全球运行Microsoft Windows操作系统的计算机进行攻击的加密型勒索软件兼蠕虫病毒（Encrypting Ransomware Worm）。
  - “永恒之蓝”利用了某些版本的微软服务器消息块（SMB）协议中的数个漏洞，特别是允许远程电脑运行代码。
  - 使用AES-128和RSA算法恶意加密用户文件以勒索比特币，使用Tor进行通讯。
  - 全球超过100多个国家共有423804套系统受到了破坏，包括英国的国家医疗服务体系、法国的汽车制造商、韩国的连锁影院、俄罗斯的银行、西班牙的电信运营商

7

各种数据泄露事件

- 雅虎共超15亿用户信息遭窃
- 2.7亿Gmail、雅虎和Hotmail账号遭泄露
- “希拉里邮件门”事件
- 4.27亿MySpace数据泄漏
- 索尼影业公司被黑客攻击
- iCloud数据泄露
- eBay数据泄露事件
- ……
- Facebook数据泄露
- 圆通10亿快递信息泄露
- 喜达屋酒店客房预订数据库遭黑客入侵
- 瑞士数据管理公司 Veeam 泄露 4.45 亿条用户数据
- 问答网站 Quora户数据遭泄露1个亿
- AcFun受黑客攻击，近千万条用户数据外泄
- ……

8

新型网络攻击: APT

- APT高级持续性威胁(Advanced Persistent Threat)
  - 有组织、有特定目标、持续时间极长的新型攻击和威胁，或者称之为“针对特定目标的攻击”
  - 以窃取核心资料为目的，具备高度的隐蔽性，针对特定对象，长期、有计划性和组织性地窃取数据
  - 是以商业和政治为目的的一个网络犯罪类别
- 高级性主要体现在APT在发动攻击之前需要对攻击对象的业务流程和目标系统进行精确的收集。
- 主要特征：潜伏性，持续性，目标性，远控性

9

震网攻击

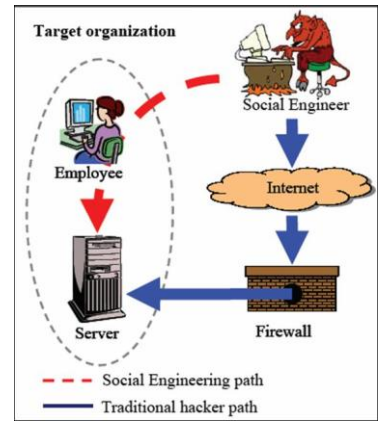
- 2010年伊朗布什尔核电站遭到Stuxnet蠕虫的攻击，导致离心机超速运转并损毁
- 核电站计算机系统实际上是与外界物理隔离的，理论上不会遭遇外界攻击。
- 超级工厂病毒的攻击者针对核电站相关工作人员的家用电脑、个人电脑等能够接触到互联网的计算机发起感染攻击，以此为第一道攻击跳板，进一步感染相关人员的U盘
- 病毒以U盘为桥梁进入“堡垒”内部，利用多种漏洞，包括当时的一个0day漏洞进行破坏。
- 有效控制攻击范围

10

社会工程学（Social Engineering）

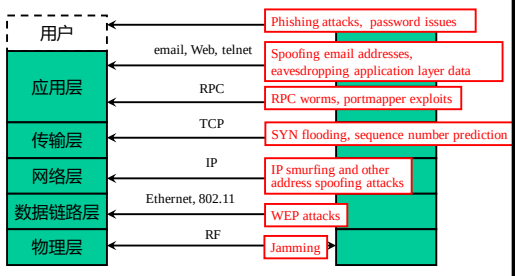
- 社会工程学是信息网络安全中的一个新的分支，其主要特点就是利用人的弱点来进行攻击
- 社会工程学
  - 是把对物的研究方法全盘运用到对人本身的研究上，并将其变成技术控制的工具。
  - 社会工程学是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的方法。
- 结合网络安全中的最新技术进行攻击，尤其结合浏览器等应用程序漏洞来进行钓鱼攻击等，危害巨大

11



12

网络体系结构 与 网络安全



13

网络协议的脆弱性

网络协议的脆弱性

- ARP欺骗
- IP欺骗
- TCP会话劫持

15

对局域网的攻击：LAN

- 例如：攻击者控制了局域网中的某台PC机
- 攻击者的行为
  - 安装数据包嗅探软件
  - 获取密码，甚至根密码
  - 接管相应的账号。
- 防御方法：阻止密码嗅探攻击
  - 使用挑战-应答密码生成器
  - Kerberos
  - ssh协议(保证LAN上不会有明文密码传送)

16

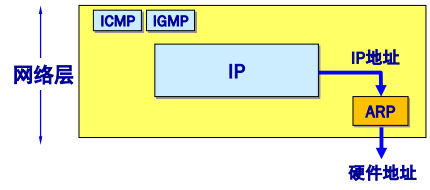
对局域网的攻击：WLAN

- 欺骗访问点(非法AP，Rogue Access Point)
  - 公共区域中的WiFi热点，例如机场，但该访问点已被恶意部署。
  - 如果用户使用该接入点，黑客就可以嗅探用户输入的明文密码，或将用户导向到恶意站点。
  - 此外，欺骗访问点也可能是雇员为了自己方便而违反公司安全策略要求安装的设备
  - 也可以是错误配置(以至于不能对网络流量进行加密)的正式节点。

17

地址解析协议 ARP 的作用

- 已经知道了一个机器（主机或路由器）的IP地址，如何找出其相应的硬件地址？
- 地址解析协议 ARP 就是用来解决这样的问题的



ARP 协议的作用

ARP 作用：从网络层使用的 IP 地址，解析出在数据链路层使用的硬件地址。

18

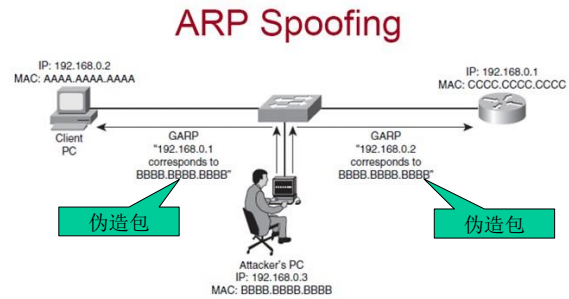
ARP欺骗攻击

- ARP攻击主要存在于局域网网络中
- 攻击方法：通过伪造IP地址和MAC地址实现ARP欺骗
  - 能够在网络中产生大量的ARP通信量使网络阻塞，
  - 持续不断的发出伪造的ARP响应包就能更改目标主机ARP缓存中的IP-MAC条目，造成网络中断或中间人攻击
- 局域网中若有一台计算机感染ARP木马，则感染该ARP木马的系统将会试图通过“ARP欺骗”手段截获所在网络内其它计算机的通信信息，并因此造成网内其它计算机的通信故障。

19

ARP欺骗攻击

- ARP欺骗攻击（ARP毒化，ARP缓存中毒）
- Gratuitous ARP（GARP）：主机使用自己的IP地址作为目标地址发送ARP请求

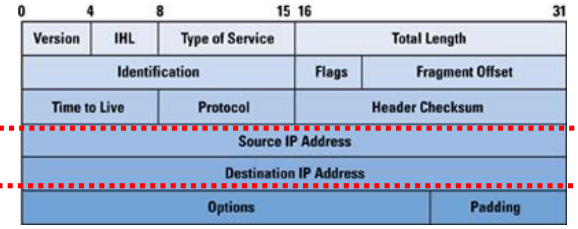


IP欺骗

- IP spoofing (IP 欺骗)
  - 用伪造的源IP地址来发送 IP 数据包，例如，采用可信源的 IP 地址来尝试绕过防火墙
  - 这将使防火墙误以为来自入侵者的数据包是来自可信源端的
  - IP 欺骗也可以仅用于隐藏攻击的真实来源
- 能否收到响应包？
  - 由于入侵者伪装成他人出现，因此，如果发送响应，该响应将发往入侵者所伪造的地址，而非其真实地址。
- 结合其他中间人攻击
  - TCP劫持
  - 拒绝服务攻击

21

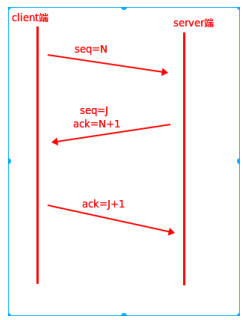
IP分组首部格式



22

TCP会话劫持

- TCP会话劫持（TCP Session Hijack）
  - TCP连接建立过程：三次握手
    - 序号Seq
    - 应答Ack
  - 为了生成一个伪造TCP数据包，攻击者需要获得特定TCP连接的当前识别信息
- 同一网段攻击
  - 数据包嗅探
  - 注入可能的序列号和命令
- 跨网段攻击
  - TCP序列预测：用数学方法猜测TCP连接的初始数值
  - 利用信任关系进行服务器攻击（rlogin，rsh，rcmd）



23

TCP报文段首部

24

分布式拒绝服务攻击
DDoS

（选）

DoS和DDoS概念

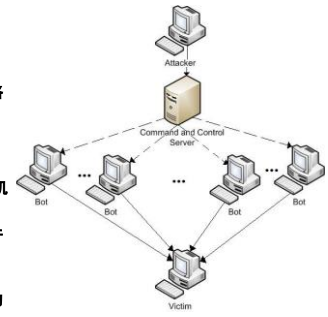
- Denial of Service (DoS) 拒绝服务攻击
  - 攻击者利用大量的数据包“淹没”目标主机，耗尽可用资源乃至系统崩溃，而无法对合法用户提供服务
- Distributed Denial of Service (DDoS)分布式拒绝服务攻击
  - 攻击者利用因特网上成百上千的“Zombie”（僵尸）主机，对攻击目标发动威力巨大的拒绝服务攻击
  - 攻击者的身份很难确认
- DDOS 最早可追溯到1996年最初，在中国2002年开始频繁出现，2003年已经初具规模

“拒绝服务”（DoS）的攻击方式


- 用户传送众多要求确认的信息到服务器，使服务器里充斥着这种无用的信息
- 所有的信息都有需回复的虚假地址，以至于当服务器试图回传时，却无法找到用户
- 服务器暂时等候，有时超过一分钟，然后再切断连接
- 黑客再度传送新一批需要确认的信息，这个过程周而复始，最终导致服务器处于瘫痪状态

分布式拒绝服务攻击（DDOS）

- 分布式拒绝服务攻击（distributed denial of service）
  - 1999年10月出现攻击
  - 1999-2000年前后，僵尸网络
    - 单一性配置，大量存在漏洞的计算机
- 僵尸网络（Bot Network）
  - 由存在不同类型漏洞的受控机器组成
  - 价值链：定向攻击，垃圾邮件，DDOS攻击
  - Fast Flux是当前的僵尸网络、恶意软件和仿冒方案最常用的通信平台

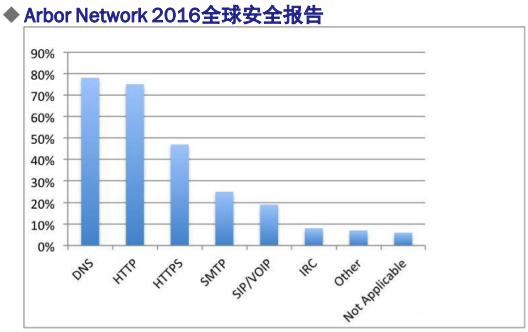


僵尸网络

- 僵尸网络通过掌握着的巨型僵尸网络可以在任何时候对任何目标发动DDoS攻击。
- 僵尸的感染对象
  - 服务器、PC、智能手机，摄像头、路由器、家居安防系统、智能电视、智能穿戴设备等
- Mirai僵尸由于源码的开放可能正在迅速的扩散
  - 2016年10月21日，美国知名网络域名服务提供商Dyn遭受到强力的DDoS攻击，攻击流量的来源之一是感染了Mirai僵尸的设备
  - IOT设备的密码固化在固件中，无法杜绝二次感染，并且隐藏在这种嵌入式设备中是极难判定其是否受到恶意感染。

易受到DDOS攻击的应用层协议

- Arbor Network 2016全球安全报告



DDoS攻击分类

	停止服务	消耗资源
本地	• 杀死进程（init，inet进程） • 重新配置系统 • 使进程崩溃	• 填充进程表 • 填充整个文件系统 • 填充整个网络
远程	• 恶意数据包攻击（Land，Teardrop等）	• 数据包泛滥（SYN Flood，Smurf，DDoS等）

Internet网络安全协议

（选）

Internet网络安全协议

- 应用层
  - E-mail: PGP, using a web-of-trust
  - Web: HTTP-S, using a certificate hierarchy
- 传输层
  - TLS/SSL(Transport Layer Security/ Secure Socket Layer)
- 网络层
  - IPSec
- 网络基础设施
  - DNS-Sec，BGP-Sec

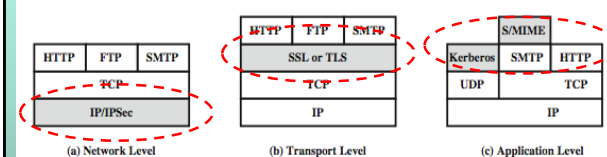
33

Web 安全需求

- WWW的广泛应用
  - 客户/服务器应用
  - 双向通信；门户和信息出口；软件复杂性；用户的多样性
- Web的安全威胁
  - 完整性 integrity: 木马，消息篡改等
  - 保密性 confidentiality：窃听
  - 拒绝服务 denial of service：DDOS, DOS攻击
  - 认证 authentication：假冒合法用户
- 需要增加安全机制
  - Web服务器
  - 浏览器
  - 浏览器和服务器之间的网络通信

34

网络安全协议



35

SSL/TLS协议历史

- 1994年Netscape开发了SSL(Secure Socket Layer)协议，Web安全机制，提供鉴别与保密服务，SSL 1.0，不成熟，未发布
- 版本和历史
  - 1995年，SSL 2.0，基本上解决了Web通讯的安全问题
    - Microsoft公司发布了PCT(Private Communication Technology)，并在IE中支持
  - 1996年发布SSL3.0，增加了一些算法，修改了一些缺陷
  - 1999年，IETF(www.ietf.org)将SSL作了标准化，即RFC2246,并将其称为TLS(Transport Layer Security)，TLS 1.0 也被称为SSL 3.1
  - 2006年和2008年，TLS 1.1 RFC 4346，TLS1.2
  - 2011年，TLS1.2修订版
- 目前，主流浏览器都已经实现了TLS 1.2的支持。
  - TLS 1.0通常被标示为SSL 3.1，TLS 1.1为SSL 3.2，TLS 1.2为SSL 3.3。

3636

SSL协议

- SSL (Secure socket Layer)安全套接层协议
  - 一种在客户端和服务器端之间建立安全通道的协议，主要是使用公开密钥体制和X.509数字证书技术保护信息传输的机密性和完整性
  - 它不能保证信息的不可抵赖性
  - 主要适用于点对点之间的信息传输，常用Web Server方式
- SSL包括：
  - 服务器认证
  - 客户认证（可选）
  - SSL链路上的数据完整性和SSL 链路上的数据保密性

37

SSL的作用

- 窃听风险（eavesdropping）
  - 第三方可以获知通信内容

所有信息都是加密传播，第三方无法窃听

- 篡改风险（tampering）
  - 第三方可以修改通信内容

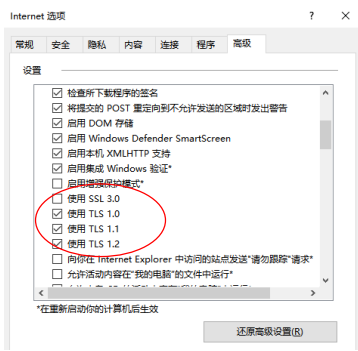
具有校验机制，一旦被篡改，通信双方会立刻发现

- 冒充风险（pretending）
  - 第三方可以冒充他人身份参与通信

配备身份证书，防止身份被冒充

38

例：SSL/TLS协议在浏览器中的设置



Internet Explorer 11

39

主要功能

- SSL服务器认证
  - 允许用户确认服务器身份
  - 支持SSL协议的客户机软件能使用公钥密码标准技术检查服务器证书、公用ID是否有效和是否由在客户信任的CA列表内的认证机构发放
- SSL客户机认证（可选）
  - 允许服务器确认用户身份
  - 使用应用于服务器认证同样的技术，支持SSL协议的服务器软件能检查客户证书、公用ID是否有效和是否由在服务器信任的认证机构列表内的CA发放

40

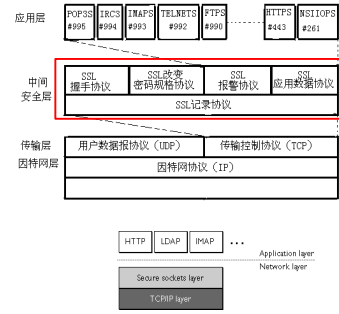
主要功能（续）

- **机密性**
  - 一个加密的SSL连接要求所有在客户机与服务器之间发送的信息由发送方软件加密和由接收方软件解密，这样提供了高度机密性
- **完整性**
  - 所有通过加密SSL连接发送的数据都被一种检测篡改的机制所保护，这种机制自动地决定传输中的数据是否已经被更改

41

SSL/TLS协议栈

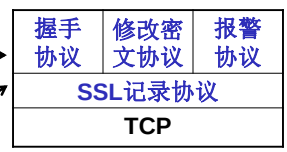
- **介于应用层和传输层之间**
  - TCP层之上
  - 为应用层提供安全性服务

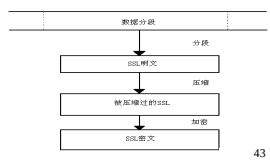


42

SSL协议的体系结构

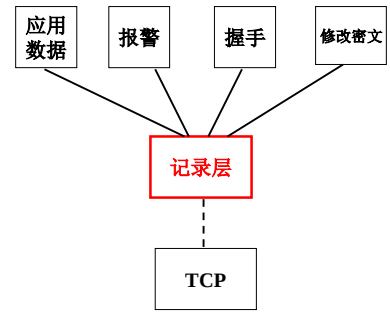
- **SSL协议工作过程**
  - 在应用层通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作
  - 在此之后,应用层协议所传送的数据都被加密
- **SSL是一个两层协议，包括：**
  - 底层：SSL记录协议
  - 高层：
    - SSL握手协议
    - SSL修改密文协议
    - SSL警告协议





43

各种消息协同工作



44

SSL记录协议

- 提供两种服务
  - 机密性：定义用于SSL数据加密的共享密钥
  - 消息完整性：定义用于产生MAC码的共享密钥
- SSL记录协议接收传输的应用报文
  - 将数据分片成可管理的块 $\leq 2^{14}-1=16383$个字节
  - 进行数据压缩(可选)
  - 应用消息认证码MAC
  - 接着利用IDEA、DES、3DES或其他加密算法进行数据加密,最后增加由内容类型、主要版本、次要版本和压缩长度组成的首部

45

TLS和SSL的细微差异

- 版本号
  - 记录 TLS 主版本号 3，副版本号1
- 消息认证码
  - TLS使用RFC2104中的 HMAC算法（异或）
- 伪随机函数PRF
  - a pseudo-random function expands secrets
  - based on HMAC using SHA-1 or MD5
- 增加报警码
- 密码构件的差异
- 证书类型：changes in certificate types & negotiations
- 密码计算与填充：changes in crypto computations & padding

46

HTTPS

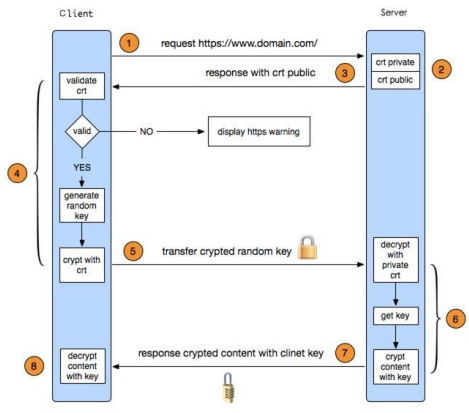
- HTTPS (HTTP over SSL)
  - https//：使用443端口
- HTTP与SSL/TLS相结合实现浏览器和WWW服务器之间的安全通信
  - RFC2818（HTTP over TLS）
- 加密以下信息
  - URL
  - document contents
  - form data
  - Cookies
  - HTTP headers

56

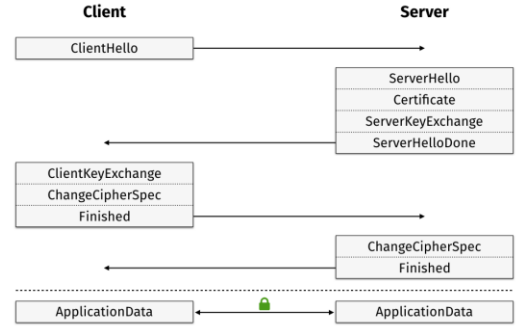
HTTPS的使用

- 建立连接
  - 客户端TLS握手(handshake)结束后， 发出第一个HTTP请求
    - TLS ClientHello
    - http request
- 关闭连接
  - HTTP记录中加入 “Connection: close”
  - TLS 关闭连接：使用TLS警告协议发送 close_notify alerts
  - 关闭TCP连接
  - HTTP客户端还必须连接异常关闭的情况
    - TCP close before alert exchange sent or completed

57



TSL握手协议



https:浏览器中的标志

- ◆网络攻击者
  - ❖控制路由器、DNS；注入、删除和修改分组
- ◆Web安全的目标
  - ❖认证：Provide user with identity of page origin
  - ❖保密：Indicate to user that page contents were not viewed or modified by a network attacker

针对https的攻击

1. HTTP 升级到 HTTPS
2. 针对证书的语义攻击
3. 无效证书
4. 混和内容
   - HTTP and HTTPS on the same page
5. 源污染（Origin contamination）
   - Weak HTTPS page contaminates stronger HTTPS page

IPSec

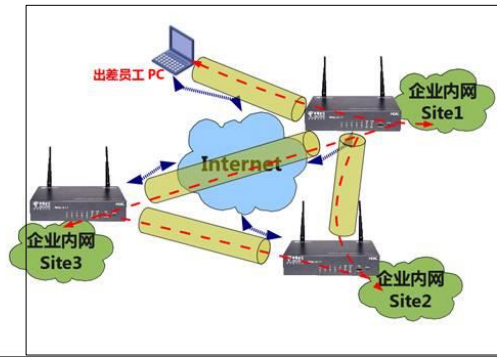
网络层的安全协议

IP 安全（IP Security）

- 1994年，互联网体系结构委员会（IAB）发表“互联网体系结构安全”报告（RFC1636）
  - 下一代IP的安全特性：认证和加密
  - IPv6实现
- IPSec规范：互联网安全标准
  - IPv4和IPv6中均可使用
- 用途
  - 通用的IP安全机制
  - 认证 authentication
  - 加密 confidentiality
  - 密钥管理 key management

65

IPSec VPN 应用需求



66

IPSec的服务

- 通用IP安全机制
  - LAN, WAN, Internet之间，包括以下功能：

数据机密性（Confidentiality）
- IPsec发送方在通过网络传输包前对包进行加密

数据完整性（Data Integrity）
- IPsec接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改

数据来源认证（Data Authentication）
- IPsec在接收端可以认证发送IPsec报文的发送端是否合法

防重放攻击（Anti-Replay）
- IPsec接收方可检测并拒绝接收过时或重复的报文

67

IPSec的优点

- 支持IKE（Internet Key Exchange，密钥交换）
  - 实现密钥的自动协商功能，减少了密钥协商的开销
  - 可以通过IKE建立和维护安全关联（SA）的服务，简化IPsec的使用和管理
- 应用透明性
  - 所有使用IP协议进行数据传输的应用系统和服务都可以使用IPsec，而不必对这些应用系统和服务本身做任何修改
  - 对端用户透明
- 可以对个人用户提供安全性

68

IPSec的优点(续)

- 数据的加密是以数据包(IP分组)为单位
  - 灵活性，可以有效防范网络攻击
  - 防止被旁路
- 提供安全路由体系结构
  - 路由器广播来源于授权的路由器
  - 相邻路由器广播来源于授权路由器
  - 重定向报文：来自发出初始包的路由器
  - 路由更新未被伪造

69

IPSec局限性

- 通信性能较低
- 需要为每一客户端安装客户端软件,可能带来了与其他系统软件之间兼容性问题的风险
- 安装和维护困难
- 不易解决网络地址转换(NAT)和“穿透”防火墙的问题。

70

IPSec的复杂性

- IPSec 运行在网络层，不能从用户空间直接访问。
  - 支持数据加密，数据完整性保护及身份认证
- 主要用于虚拟专用网VPN
- IPv6的基本要求之一
- 过度设计（Over-engineered）
  - 协议的复杂性；缺陷；互操作性
- IPsec协议不是一个单独的协议，它给出了应用于IP层上网络数据安全的一整套体系结构

71

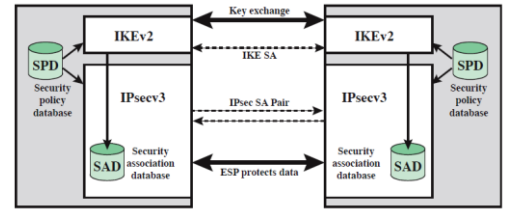
IP Sec体系结构

- **相关标准文档**
  - **体系结构**
    - RFC4301 *Security Architecture for Internet Protocol*
  - **认证报头** Authentication Header (AH)
    - RFC4302 *IP Authentication Header*
  - **封装安全负载** Encapsulating Security Payload (ESP)
    - RFC4303 *IP Encapsulating Security Payload (ESP)*
  - **密钥管理** Internet Key Exchange (IKE)
    - RFC4306 *Internet Key Exchange (IKEv2) Protocol*
  - **加密算法** Cryptographic algorithms

72

IPSec体系结构

- 密钥交换协议 Internet Key Exchange (IKE)
- IPSec
- 安全关联数据库 SAD(Security Association Database)
- 安全策略数据库 SPD(Security Policy database)



73

IPSec两个主要组成部分

- **Internet密钥交换协议**
  （IKE: Internet Key Exchange）
  - 双向交互认证
  - 生成会话密钥
- **封装安全负载和认证报头（ESP/AH）**
  - 封装安全负载ESP: Encapsulating Security Payload——IP分组加密和完整性保护
  - 认证报头AH: Authentication Header——完整性保护

75

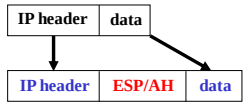
传输模式和隧道模式

- **传输模式（Transport Mode）**
  - 增加对IP包中负载的保护，如对TCP，UDP或ICMP包的保护
  - ESP 加密或认证IP数据负载
  - AH认证IP负载和IP报头部分字段
  - 可用于两个主机之间的通信（host to host）
- **隧道模式（Tunnel Mode）**
  - 加密整个IP分组
  - 增加新的IP报文头部
  - 路由器无法检查内部IP报文头部
  - 适用于VPNs, 网关-网关的安全

80

IPSec 传输模式

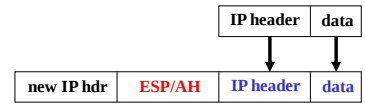
- IPSec 传输模式



- 用于*Host-to-host*通信
- 高效：仅增加少量额外头部信息
- 保持原始IP头部
  - 安全性
    - 被动攻击者可以发现通信双方的地址

IPSec 隧道模式

- IPSec隧道模式 Tunnel Mode



- 用于*firewall-to-firewall*的通信
  - 原始IP分组被封装在IPSec中
- 原始IP头部对攻击者不可见

AH协议

- IP协议号为51
- 提供数据源认证、数据完整性校验和防报文重放功能
- 它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。
- 工作原理
  - 在每一个数据包上添加一个身份验证报文头，此报文头插在标准IP包头后面，对数据提供完整性保护
  - 可选择的认证算法有MD5（Message Digest）、SHA-1（Secure Hash Algorithm）等。

ESP协议

- IP协议号为50
- 提供加密、数据源认证、数据完整性校验和防报文重放功能。
- 工作原理
  - 在每一个数据包的标准IP包头后面添加一个ESP报文头，并在数据包后面追加一个ESP尾。
  - 与AH协议不同的是，ESP将需要保护的用户数据进行加密后再封装到IP包中，以保证数据的机密性。
  - 常见的加密算法有DES、3DES、AES等。同时，作为可选项，用户可以选择MD5、SHA-1算法保证报文的完整性和真实性。
  - 空加密NULL encryption

匿名通信

（选）

匿名通信

- 研究如何隐藏通信实体的身份信息，使攻击者无法窃听和流量分析流量数据报头来得到用户的真实身份，或对用户通信进行跟踪。
- 匿名通信系统的研究目的是对网络用户的 IP 地址、通信关系等涉及用户隐私信息的保护，使其不被攻击者检测和发现。
- 保护类型
  - 匿名发送：保护发送者的身份标识
  - 匿名接收：保护接收者的身份标识
  - 匿名发送接收关系：很难找到特定消息的发送与接收者，无法推测通信双方

88

洋葱路由Onion Routing

[Reed, Syverson, Goldschlag 1997]

- 隐藏通信目标
  - 隐藏源和目的地址
- 加密
  - 用户从其他节点获取加密密钥
  - 路由器之间发送加密分组
- 路由
  - 洋葱路由器
  - 每个分组通过多跳路由

89

基本设计

- 覆盖网络 Overlay network
- 洋葱路由器 Onion routers route traffic
- 代理：Onion Proxy fetches directories and creates circuits on the network
- 使用TCP协议
- 固定分组大小：All data is sent in fixed size cells

CircID	CMD	Data

CircID	Relay	StreamID	Digest	Len	CMD	Data

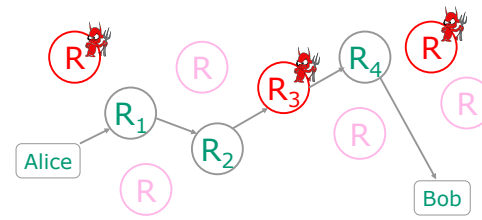
90

基本过程

- 发送：Sending an Onion-Routed Packet
- 加密：Encrypt the packet using the destination's key
- 封装：Wrap that with another packet to another router
  - Encrypted with that router's key
- 迭代：Iterate a bunch of times

91

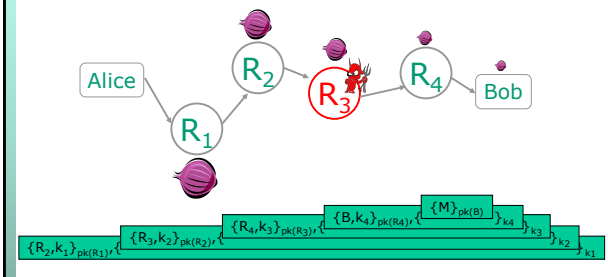
Onion Routing



- 发送方选择路由器序列
  - 可能包含恶意攻击者
  - 发送方控制路径长度

92

建立路由



- 每个链路的路由信息用路由器的公开密钥加密
- 每个路由器仅知道下一跳路由器的标识

93

特点

- 公钥密码体制加密的计算复杂性
- 高延迟
  - 适合email, 不适合匿名Web browsing
- 挑战：低延迟的匿名网络
  - 使用公钥加密体制建立“虚电路连接”，使用对称密钥加密两个节点之间的会话
  - 在数据传输过程中，在每个“虚电路连接”上使用对称密钥体制进行加解密
  - 即使一些节点被攻击，也可以保持匿名性

94

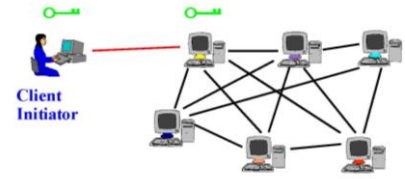
Tor

- 第二代洋葱路由网络
  - 最初该项目由 US Naval Research Laboratory赞助。2004年的后期，Tor成为Electronic Frontier Foundation（EFF）的一个项目。2005年后期，EFF不再赞助Tor项目，但他们继续维持Tor的官方网站。
  - http://tor.eff.org
  - 适用于低延迟的Internet匿名通信 (如 Web 浏览)
  - Running since October 2003
- 规模
  - 节点数：Hundreds of nodes on all continents
  - 用户数：Over 2,500,000 users
- 易用的客户端
  - Freely available, can use it for anonymous browsing

95

Tor Circuit Setup (1)

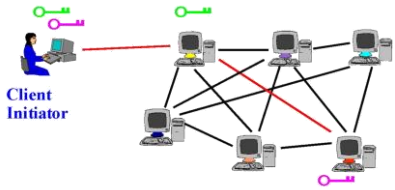
- Client proxy establishes a symmetric session key and circuit with Onion Router #1



96

Tor Circuit Setup (2)

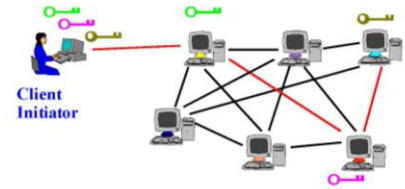
- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #2
  - Tunnel through Onion Router #1



97

Tor Circuit Setup (3)

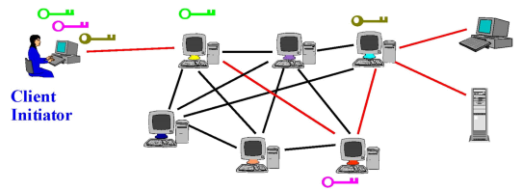
- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #3
  - Tunnel through Onion Routers #1 and #2



98

Using a Tor Circuit

- Client applications connect and communicate over the established Tor circuit
  - Datagrams are decrypted and re-encrypted at each link



99

Tor 的管理问题

- 多个应用可以共享一条“电路 circuit”
  - Multiple TCP streams over one anonymous connection
- Tor 路由器不需要根用户权限
  - Encourages people to set up their own routers
  - More participants = better anonymity for everyone
- 目录服务器
  - Maintain lists of active onion routers, their locations, current public keys, etc.
  - Control how new routers join the network
    - “Sybil attack”: attacker creates a large number of routers
  - Directory servers’ keys ship with Tor code

100

Tor网络中隐藏位置的服务器

- 目标
  - deploy a server on the Internet that anyone can connect to without knowing where it is or who runs it
- 任何地点可访问：
  - Accessible from anywhere
- 防止审查：
  - Resistant to censorship
- 防止DoS攻击
  - Can survive a full-blown DoS attack
- 防止物理攻击
  - Can’t find the physical server!

101

Tor网络危机

- 2014年卡巴斯基实验室发布了有关Tor安全性的最新研究结果
  - Tor网络中存在的近900个隐秘服务
  - Tor木马：在Tor网络中建立恶意软件的基础架构
  - Tor网络中的很多资源是专为恶意软件设计使用的，如C&C服务器、后台管理面板等

102

无线网络安全概述

无线网络的安全事件

- 公共免费Wi-Fi安全隐患
  - 利用伪造的Wi-Fi热点，不法分子可以在几分钟之内获得上网用户的设备运行数据、网络账户、密码、照片等私密信息，甚至可以窃取用户网银资产
- 非法AP：未经企业许可而私自接入企业网络中的无线路由器Rogue AP
- 家用无线路由器的安全问题
  - 一些路由器厂家为了日后调试和检测更方便，会在产品上保留超级管理权限。黑客可以利用这些后门直接控制路由器，进一步发起DNS劫持、窃取信息、网络钓鱼等攻击
  - 通过HTTP和SSH默认端口远程访问，恶意软件的变种被注入路由器
  - 密码破解
    - 无线路由器的接入密码和后台密码
    - . . .

104

无线网络的特点

- 信道
  - 共享，易受到监听和干扰
- 移动性
  - 移动性带来的安全隐患
- 资源
  - 移动设备中操作系统复杂，存储空间和资源有限
- 可访问性
  - 一些无线设备无人值守，易受到物理攻击

105

无线网络组成

- 无线客户端
  - 一般为手机、具有Wi-Fi功能的电脑、无线传感器、蓝牙设备等
- 无线接入点
  - 提供网络或服务的连接，一般为手机基站、Wi-Fi热点、接入有线局域网和广域网的无线接入点
- 传输介质
  - 用于数据传输的无线电波

106

无线网络的安全威胁

- 密码破解
  - 破解WEP和WPA的工具已经高度集成化，破解无线网络密码的技术门槛越来越低。
- 信息泄露
  - 通过“无线嗅探”、“无线监听”、“无线会话劫持”等方式，可以轻松的窃取到其他无线用户的用户名、密码等隐私信息。
- 无线钓鱼
  - 攻击者用相同的SSID搭建一个无线网络，诱使用户进行连接，从而监控用户流量

107

无线网络的安全威胁

- 偶然连接
  - 用户被自动锁定在临近的无线接入点
- 恶意连接
  - 伪装成合法接入点
- Ad hoc网络
  - 分布式、无中心点的控制，存在安全隐患
- 非传统型网络
  - 蓝牙设备，条形码识别器，PDA，摄像头
  - 面临窃听和欺骗等安全威胁
- 身份盗窃（MAC欺诈）
  - 监听网络流量，盗用MAC
- 中间人攻击
- 拒绝服务攻击（DoS）
- 网络注入
  - 伪造配置命令，影响路由器和交换机，降低网络性能

108

无线安全措施

- 安全无线传输
  - 信息隐藏技术：取消广播服务；降低信号强度；定向天线；信号屏蔽
  - 无线传输加密
- 安全无线接入点
  - 认证
  - 基于端口的网络访问控制 IEEE802.1X
- 安全无线网络
  - 加密机制
  - 杀毒软件，防火墙等
  - 关闭标识符广播
  - 改变路由器的标识符
  - 改变预设密码
  - 只允许专用计算机访问无线网路
  - 及时升级固件和软件的漏洞

109

使用移动设备的网络

- 一个组织的网络必须适应如下情况：
  - 新设备不断增加
    - 多种终端设备
  - 基于云的应用
    - 应用可以运行在传统服务器上、云服务器、移动虚拟服务器等，各种基于云的应用和服务
  - 去边界化
    - 围绕设备、应用、用户和数据有众多网络边界
  - 外部业务需求
    - 多种接入方式和权限：访客、合作方、第三方承包方等，多种设备、多种位置接入网络

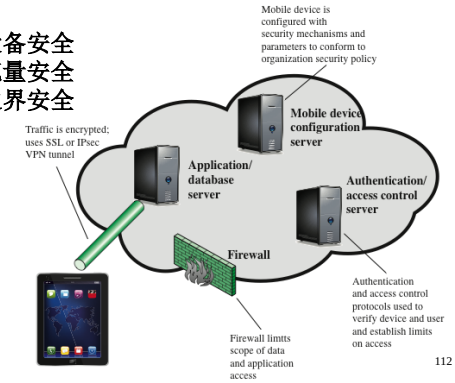
110

移动设备的安全威胁

- 缺乏物理安全控制
- 不可信移动设备的使用
- 不可信任网络的使用
- 未知来源的应用程序的使用
- 与其他系统的相互作用
  - 如云存储
- 不安全内容的使用
  - 如二维码扫描，导致移动设备访问恶意网站
- 位置服务的使用
  - 攻击者利用GPS定位功能确定位置

移动设备安全元素

- 设备安全
- 流量安全
- 边界安全



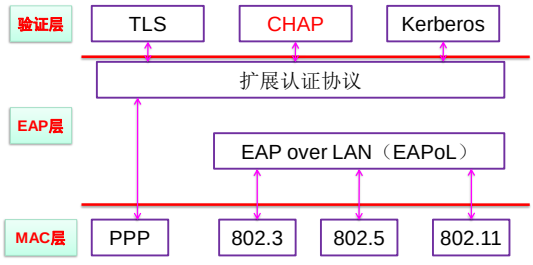
移动设备安全策略

- 设备安全
  - 企业允许携带自己的设备办公（BYOD），访问企业的资源
  - 采用安全控制规则对设备进行配置
- 流量安全
  - 加密
  - 安全传输：SSL或IPv6协议
  - 虚拟私有网络VPN
  - 二层认证机制：先认证设备；再认证使用设备的用户
- 边界安全
  - 防火墙可以拦截不合法的访问
  - 对入侵检测系统IDS和入侵防御IPS进行配置，对移动设备的数据流设置更严格的规则

IEEE 802.1x认证协议

- IEEE 802.1x于2001年6月由IEEE正式发布，是基于端口的访问控制方案，同时还有认证和计费功能
  - 最初是为有线网络设计，2004年修订，支持无线网络WLAN的接入
  - Port based network access control protocol
- 链路层协议，在一个端口被分配IP地址之前强制进行认证
  - 核心是扩展认证协议（Extensible Authentication Protocol，EAP）
  - RFC3748

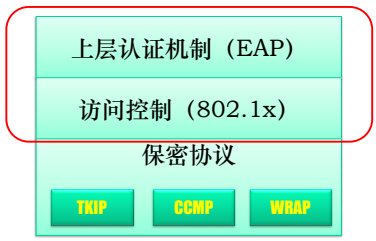
802.1x的协议栈



802.11 WLAN 安全性

- 无线通信的广播特性
  - 流量监测：任意在无线范围的站点均能传递信息和接收信息
- 最初的802.11 规范的安全特征
  - WEP(Wired Equivalent Privacy):有线等效保密（隐私）存在严重缺陷，易于被攻击
- 802.11i：解决WLAN的安全问题
  - Wi-Fi联盟发布无线网络保护接入WPA(Wi-Fi Alliance Wi-Fi Protected Access)：Wi-Fi网络安全存取
    - WEP到IEEE 802.11i的过渡方案
  - 最终形式：健壮安全网络(Robust Security Network，RSN)
- Wi-Fi 联盟基于WPA2的802.11i规范认证厂商设备
- WAPI（无线网鉴别和保密基础结构，我国）

IEEE 802.11i的协议结构



- TKIP： Temporal Key Integrity Protocol，暂时密钥完整性协议
- CCMP：计数器模式密码块链消息完整码协议
- WRAP： Wireless Robust Authenticated Protocol，无线增强认证协议

802.11的加密机制—WEP

- 早期无线加密机制，802.11b，1999年
- 有线等效保密WEP（Wired Equivalent Privacy）
  - 数据链路层安全协议，对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络。
  - 2003年，被 Wi-Fi Protected Access (WPA) 淘汰
  - 2004年， 发布IEEE 802.11i标准（又称为 WPA2）
- 特点：认证，加密；共享密钥
- WEP的破解
  - 利用加密体制缺陷，通过收集足够的数据包，使用分析密算法还原出密码。
  - 破解WPA密码使用的是常规的字典攻击法。