1 引言

1.1 对网络安全需求

信息安全四个基本目标：

①**保密性**（confidentiality）：信息不泄漏给非授权的用户、实体或者过程的特性。 ②**完整性**(integrity)：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
③**可用性**(availability)：可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。 ④**合法使用**（LegitimateUse）：确保资源不被非授权的人或以非授权的方式使用。

网络安全发展态势：计算机病毒层出不穷、黑客攻势逐年攀升、系统存在安全漏洞、各国军方加紧信息战研究

网络安全需求：①敏感信息对安全的需求：根据多级安全模型，信息密级由低到高划分为秘密级、机密级、绝密级。敏感非机密信息也应进行加密保护。②网络应用对安全的需求：网络安全问题迅猛，存在着巨大的发展空间和潜力网络安全是互联网发展中需要解决的一个重要问题。

1.2 安全威胁与防护措施

安全威胁：故意（主动攻击、被动攻击）、偶然
基本威胁：①**信息泄漏**（窃听、流量分析、电磁/射频截获、人员疏忽、媒体废弃物）②**完整性破坏**（渗入、假冒、旁路控制、授权侵犯、物理侵入）
③**拒绝服务**（植入、特洛伊木马、陷门、服务欺骗）④**非法使用**（窃取）
主要可实现威胁：①**渗入威胁**（假冒、旁路控制、授权侵犯）
②**植入威胁**（特洛伊木马、陷门）
潜在威胁：窃听、Eavesdropping、流量分析、Traffic、analysis、操作人员不慎导致信息泄漏、媒体废弃物导致信息泄漏
概念：
信息窃取：未经授权利用可能的技术手段恶意主动获取信息系统中信息
信息泄漏：因误操作、软硬件缺陷或电磁泄漏等因素导致信息系统中的保密、敏感、个人隐私等信息暴露于未经授权者
信息篡改：未经授权将信息系统中的信息更换为攻击者所提供的信息
信息假冒：假冒他人信息系统收发信息
信息丢失：因误操作、人为或软硬件缺陷等因素导致信息系统中的信息丢失
拒绝服务攻击：利用信息系统缺陷或通过暴力攻击，大量消耗信息系统的CPU、内存、磁盘等资源，从而影响信息系统正常运行的攻击行为
安全防护措施：物理安全、人员、管理、媒体、辐射、生命周期控制

1.3 网络安全策略

安全策略：某个安全域内施加给所有与安全相关活动的一套规则。
安全域：属于某个组织机构的一系列处理进程和通信资源。
授权：是指主体（用户、终端、程序等）对客体（数据、程序等）的支配权利，它等于规定了谁可以对什么做些什么。
访问控制策略：①强制性访问策略 Mandatory（多等级策略）
②自主性访问策略 Discretionary（基于身份的策略、基于任务的策略）

1.4 攻击分类

两种安全攻击类型：①被动攻击（信息泄露、流量分析）
②主动攻击（伪装攻击、重放攻击、消息篡改、拒绝服务）
八种网络攻击形式：口令窃取、欺骗攻击、陷门和后门攻击、认证失效、协议缺陷、信息泄漏、指数攻击、拒绝服务攻击

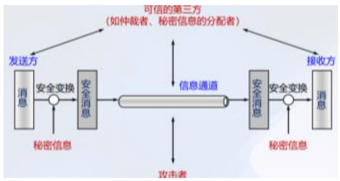
1.5 攻击形式

口令窃取：①**口令猜测攻击的三种基本方式**（利用已知或假定的口令尝试登录、根据窃取的口令文件进行猜测、窃听某次合法终端之间的会话并记录所使用的口令）②**抵御口令猜测攻击方式**（阻止选择低级口令、对口令文件严格保护）③**彻底解决口令机制的弊端**（使用基于令牌的机制，例如一次性口令方案 OTP-One-Time password）
缺陷和后门攻击：①**网络蠕虫传播**（方式之一是向守护程序发送新的代码，蠕虫向"读"缓冲区内注入大量的数据）②**缓冲器溢出（堆栈粉碎）攻击**（一种扰乱程序的攻击方法、通过改进设计或避免在堆栈上执行代码消除此缺陷）③**缺陷**（指程序中某些代码不能满足特定需求，采取相应的步骤来降低缺陷发生的可能性）
认证失效：①认证机制的失效易导致服务器被攻击者欺骗。②被破坏的主机不会进行安全加密，因此对源主机采用密码认证的方式无用。③通过修改认证方案消除其缺陷，完全可以挫败这种类型的攻击。
协议缺陷：①**协议本身的缺陷导致攻击的发生**（攻击者可以对 TCP 发起序列号攻击、DNS 和许多基于 RPC 的协议也遭到序列号攻击）②**安全壳（SSH）协议遭遭**（通过改进设计或避免在堆栈上执行代码消除此缺陷）③**802.11 无线数据通信标准中的 WEP 协议也存在缺陷**
信息泄漏：①协议丢失的信息易被攻击者利用，攻击者借助这些信息攻破系统（Finger 协议、口令窃取、欺骗攻击）②DNS 有丰富的数据来源，易被黑客利用
指数攻击：指数攻击能够使用程序快速复制并传播攻击
①蠕虫(Worms)程序自行传播 ②病毒(Virus)依附于其他程序进行传播
拒绝服务攻击：①**拒绝服务攻击**（过度使用服务，使软件、硬件过度运行，使网络连接超出其容量。造成关机或系统瘫痪，或者降低服务质量）②**分布式拒绝服务攻击**（使用很多 Internet 主机同时向某个目标发起攻击）

1.6 开放系统互联安全体系结构

X.800 安全服务：认证、访问控制、数据保密性、数据完整性、不可否认性
X.800 安全机制：加密、数字签名、访问控制、数据完整性、认证交换、路由控制、公正、流量填充

1.7 网络安全模型



2 计算机网络基础（非重点）

2.1 计算机网络的定义

简单定义：计算机网络是一些相互连接的、自治的计算机系统的集合。
通用定义：将处于不同位置并且具有独立功能的多个计算机系统通过通信线路和网络设备连接起来，以实现网络资源共享。

2.2 计算机网络体系结构

必须完成的工作：1.两台计算机间有一条传送数据的通路。2.发起通信的计算机必须将数据通信的通路进行激活。激活就是要发出一些信令，保证要传送的计算机数据能在这条通路上正确发送和接收的命令。3.告诉网络如何识别接收数据的计算机。4.发起通信的计算机要查明对方计算机是否已准备好接收数据。5.发起通信的计算机必须查明对方计算机的文件管理程序是否已做好文件接收和存储文件的准备工作。6.若两个计算机的文件格式不兼容，则至少其中一个计算机应完成格式转换。7.对出现的各种差错，应当有可靠的措施保证对方计算机最终能收到正确的文件。
网络分层的必要性：为了减少协议设计和调试过程的复杂性，计算机网络功能的实现都按照分层的方式来组织。通过"分层"，可以将庞大、复杂的问题转换为若干较小、简单和单一的局部问题，方便人们理解研究。
分层思想的提出：ARPANET 网，尽管连到网上的主机和终端型号及其性能不同，但由于共同遵守了计算机网络的协议，所以可以相互进行通信。
网络协议：明确规定了所交换的数据的格式以及有关的同步（含有时序）。这些为进行网络中的数据交换而建立的规则、标准或约定就是网络协议。
网络协议三要素：语法、语义、同步
OSI 七层参考模型（上层→下层）：应用层、表示层、会话层、运输层、网络层、数据链路层、物理层
TCP/IP 四层参考模型（上层→下层）：应用层（TELNET/FTP/SMTP 等）、运输层（TCP，UDP）、网际层 IP、网络接口层。
两个模型相似之处：都是基于独立的协议栈、每层的功能大体相同。
两个模型不同之处：服务、协议、接口。协议和模型的关系。面向连接服务和无连接服务。协议的具体实现。

3 Internet 协议的安全性

3.1 各层协议

①**网络接口层**：TCP/IP 模型的最底层 ②**网际层**：IP、ARP
③**传输层**：TCP、UDP ④**应用层**：HTTP、SMTP、POP3、FTP

3.2 网际层协议

IP 网际协议(Internet Protocol)：是 TCP/IP 协议族的核心，网际层最重要。
IP 协议安全问题：①监听窃取→加密 ②修改内容→完整性检测 ③IP 欺骗攻击→源地址鉴别 ④注入病态小数据报→防火墙 ⑤定向广播地址→配置路由器禁止发送定向广播数据报
ARP 地址解析协议(Address Resolution Protocol)：是根据 IP 地址获取物理地址的一个 TCP/IP 协议。以太网发送的是 48 位以太地址的数据包。IP 驱动程序必须将 32 位 IP 目标地址转换成 48 位的物理地址;
ARP 协议的安全问题：攻击者发动 ARP 欺骗攻击，可以完全控制主机 A 和 B 之间的流量，发动被动攻击（流量监测、获取涉密信息）或主动攻击（伪造数据）。**防范**：在交换机上配置 IEEE 802.1x 协议，攻击者连接交换机时需进行身份认证。建立静态 ARP 表，但破坏了动态 ARP 协议。
ICMP 控制报文协议(Internet Control Message Protocol)：是一个重要的错误处理和信息处理协议。是一种差错和控制报文协议，用于传输差错报文、控制报文。通知主机到达目的地的最佳路由，报告故障路由。
ICMP 重定向攻击：攻击者利用 ICMP 对消息进行重定向，使目标机器遭受连接劫持和拒绝服务等攻击。
ICMP 路由器发现攻击：ICMP 并不对应答方进行认证，使得它可能遭受严重的中间人攻击。
ICMP 防火墙穿越攻击：攻击者能够穿越某个防火墙的访问控制列表和规则集，进而确定该防火墙过滤的内容和具体的过滤方式。

3.3 传输层协议

TCP 传输控制协议(Transmission Control Protocol)：是一种面向连接的、可靠的传输层通信协议。
TCP 第一类 SYN Flood 攻击：攻击者不断向服务器的监听接口发送建立 TCP 连接的请求 SYN 数据包，使服务器一直处于半开放连接状态，无法接受其他正常的连接请求。属于拒绝服务(DoS)攻击。**防护措施**：在服务器前端部署网络安全设备(防火墙)进行数据包过滤。阻止第 3 次握手。
TCP 第二类的 TCP 会话劫持攻击：针对 TCP 协议不对数据包加密和认证的漏洞。TCP 协议确认数据包的真实性依据判断数据包中独有的 32 位序列号。如果攻击者能够预测目标主机的起始序号，就可以欺骗该目标主机。**防护措施**：在 TCP 连接建立时采用一个随机数最为初始序列号。
TCP 第三类连接后攻击：针对 TCP 的拥塞控制机制的特性，在 TCP 连接建立后的数据阶段攻击。拥塞控制功能防止过多数据注入网络。攻击者利用机制特性，周期性制造关键节点的拥塞，不断触发拥塞窗口的慢启动过程，以降低正常传输能力。**防护措施**：网管实时监测网络异常流量。
UDP 用户数据报协议(User Datagram Protocol)：是一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务。(无需连接传输高效、无拥塞控制的不可靠交付、数据报首部 8B、网络拥塞不会降低发送速率)
UDP Flood 攻击：DoS 攻击中的流量型攻击。攻击源发送大量的 UDP 小包到攻击目标，使其忙于处理和回应 UDP 报文，系统资源使用率高，导致该设备不能提供正常服务甚至全网瘫痪。**防护措施**：①当攻击包是大包，则根据攻击包大小设定包碎片重组大小（不小于 1500）②当攻击端口为业务端口，根据该业务 UDP 最大包长设置 UDP 最大包以过滤异常流量。③非业务端口，则设置 UDP 连接规则，要求先建立 TCP 连接。

3.4 应用层协议

HTTP 超文本传输协议(Hyper Text Transfer Protocol)：是一个客户端和服务器端请求和应答的标准，是互联网上应用最广泛的一种网络协议。
HTTP 协议的安全问题：HTTP 协议中数据是直接通过明文进行传输，不提供任何数据加密。①攻击者可获得明文传输数据。②HTTP 协议是一种无状态连接，唯一的完整性检验是报文头部的数据传输长度，而未对传输内容进行消息完整性检测。攻击者可篡改传输数据，发动中间人攻击。
防护措施：在 HTTP 协议和 TCP 协议之间增加安全层来增强安全性。安全层主要通过安全套接层(SSL)及其替代协议传输层安全协议(TLS)实现。
TELNET 远程登录协议(Teletype Network)：是 TCP/IP 协议族中的一员，是 Internet 远程登录服务的标准协议和主要方式。
TELNET 安全问题：Telnet 提供了简单终端到某台主机的访问。用户输入帐户和口令进行登录。Telnet 程序可能会泄露秘密信息，攻击者通过 Sniffer 记录相关信息。或采取主动攻击方式，如劫持 Telnet 会话并在认证完成后篡改命令。还可以使用 TCP 劫持工具劫持 Telnet 对话。
防护措施：对 Telnet 会话进行加密，如 Stel、SSLtelnet、Stelnet、SSH 等协议。SSH 已经成为远程登录的标准协议。
DNS 域名系统(Domain Name System)：是一个分布式数据库系统，用来实现域名与 IP 地址之间的映射。（端口 UDP 53）
DNS 欺骗攻击：攻击者假冒域名服务器的一种欺骗行为。**防范**：暴露的主机不要采用基于名称的认证。改为基于地址的认证虽然也很脆弱。
DNS 缓存中毒攻击：攻击者给 DNS 服务器注入非法网络域名地址。当非法地址写入服务器缓存，用户就会跳转到 DNS 指定的非法地址。**防范**：攻击者可以从主机名中找出信息，因此不要把秘密信息放在主机名中。
DNS 重定向攻击：将 DNS 名称查询重定向到恶意 DNS 服务器上，域名解析就会被劫持。**防范**：采用 DNSsec 新标准，但仍存在很多问题。
SMTP 简单邮件传输协议(Simple Mail Transfer Protocol)：是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。
SMTP 协议的安全问题：攻击者用 DoS 攻击阻止合法用户使用该邮件服务器。邮件的别名有时也会提供信息。"开放中继"允许在任何人之间进行邮件传递，非常危险。**防范**：使用 SMTP 认证并与加密 SMTP 会话结合。
FTP 文件传输协议(File Transfer Protocol)：是 Internet 文件传送的基础。
FTP 协议安全问题：①**使用 PORT 命令**（主动模式）：服务器主动对客户机进行连接，一旦该连接受到黑客攻击，防火墙无法作出正确处理。还会引起 FTP 反弹攻击，客户机在 PORT 命令中发送了自己的 IP 和端口号。②将 Java 程序伪装成 FTP 客户机发动攻击。③登录口令容易被探测或猜测。④FTPD 守护程序缺陷。
防范：使用 PASV（被动模式）命令，同时在配置防火墙时禁止所有进入的 TCP 连接。使用密文来传输用户名和口令。

4 单钥（私钥）密码体制、对称

4.1 密码体制的定义

明文：需秘密传送可读懂的消息。 **密文**：明文经密码变换后不可读消息。
加密：由明文到密文的数学变换。 **解密**：从密文恢复出明文的数学变换。
加密/解密算法：对明文进行加密/解密时采用的一组规则。
密钥：加密和解密时使用的一组秘密信息。
密码体制的语法定义：
明文消息空间 M：某字母表上的串集 密文消息空间 C：可能的密文消息集
加密密钥空间 K：可能的加密密钥集 解密密钥空间 K'：可能的解密密钥集
有效的密钥生成算法 ζ：$N \to K \subseteq K'$
加密算法 E：$M \subseteq K \to C$ 解密算法 D：$C \subseteq K' \to M$
∀整数 1^l，$\zeta(1^l)$输出长为 l 的密钥对$(k_e, k_d) \in K \times K'$
$\forall m \in M, c \in C$，有 $c=E_{ke}(m), m=D_{kd}(c)=D_{kd}(E_{ke}(m))$
密码体制的分类：①单钥加密体制（对称加密体制、私钥加密体制）
②双钥加密体制（非对称加密体制、公钥加密体制）
单钥体制的分类：①**流密码**(Stream Cipher)数据逐比特加密，数据流与密钥流逐比特进行异或运算②**分组密码**(Block Cipher)对数据分组进行处理。
双钥体制的分类：分组密码

4.2 古典密码

古典密码分类：①**置换密码**：明文字母不变，但顺序打乱。②**代换密码**：明文字母被替换，顺序不变。（单表代换、多表代换、弗纳姆密码）
置换密码—周期置换：密钥空间是列数的阶乘（密钥 hand，按列读取结果）
单表代换—凯撒密码（移位密码）：将字母按顺序推后 3 位（破解：每个字母使用的频率不相等）
多表代换—维吉尼亚密码：对字母表编号，把 A~Z 依次编为 0~25。明文字母与密钥字母的模 26 加得到密文字母。字母为密钥，密钥长度是 m，密钥空间大小为 26^m。（明文 data security，密钥 best）

明文	d	a	t	a	s	e	c	u	r	i	t	y
编码	3	0	19	0	18	4	2	20	17	8	19	24
密钥	b	e	s	t	b	e	s	t	b	e	s	t
编码	1	4	18	19	1	4	18	19	1	4	18	19
模26加	4	4	11	19	19	8	20	13	18	12	11	17
密文	e	e	l	t	t	i	u	n	s	m	l	r

代换密码—弗纳姆密码（一次一密密码）：将明文与密钥进行膜 2 加法运算。
一次一密是不可攻破的密码体制：从密文中得不到任何关于明文的信息，除非知道密钥。缺点是密钥很长，产生和传输费用高，密钥只能用一次。

4.3 流密码

特点：明文 $m=m_1,m_2,\ldots,m_k$ 伪随机序列 $k=k_1,k_2,\ldots,k_k$ 密文 $c_i=E_{ki}(m_i)$
解密过程与加密过程一致、序列密码安全性完全依赖于伪随机数强度
流密码的描述（有限状态自动机）：若密钥流是一个完全随机的非周期序列，则可用它实现一次一密体制。但实用中的流密码大多采用有限存储单元和确定性算法，可用有限状态自动机(Finite State Automation)来描述。

流密码分类—同步流密码：若σ_i与明文消息无关，则密钥流将独立于明文，称此类流密码为同步流密码（Synchronous Stream Cipher）。对于明文而言，这类加密变换是无记忆的，但它是时变的。**优点**：没有差错传播
缺点：对失步敏感，只有保持两端精确同步才能正常工作。
流密码分类—自同步流密码：若σ_i依赖于(k_i,σ_{i-1},m_i)，则密钥流与明文 $m=m_1,\cdots,m_{i-1}$有关，称这类流密码为自同步流密码(Self-Synchronous Stream Cipher) **缺点**：传输过程中一位出错，影响后 n 位密钥的正确性
优点：收端只要连续正确地收到 n 位密文，则在相同密钥作用下就会产生相同的密钥，因而它具有自同步能力

4.4 流密码算法 RC4

RC4 流密码：每次加密一个字节的明文。在加密过程中，密钥输入到一个伪随机数发生器，其产生一串随机的 8 位密钥流，通过与同一时刻一个字节的明文流进行异或产生密钥流。
特点：①RC4 是一个以分组长度 n=8 为参数的二元加法流密码体制。②内部状态由一个包含 N=2^n 个字节的 S 盒和两个 n=8 比特的指针 i 和 j 组成。③S 盒看作一个随机置换，算法包含密钥调度算法和密钥流生成算法，前者用可变长度的加密密钥产生密钥流生成器的初始状态，后者根据初始状态产生密钥流，使之与明文相异或产生密文。算法中所有的"+"运算都是模 N 的加法。

4.5 分组密码

分组密码定义：是将明文消息编码表示后的数字序列划分成长为 m 的组，各组分别在密钥控制下变换成等长的输出数字序列。
分组密码的设计要求：①分组长度足够大（≥128~256 比特）
②密钥量要足够大（≥128~192~256 比特）③算法足够复杂（包括子密钥产生算法）④加密、解密算法简单，易软硬件实现⑤数据无扩展（只在引入同态置换和随机化加密时有扩展）⑥差错传播尽可能得小
Shannon 的密码设计思想：①扩散：将每位明文及密钥数字的影响尽可能迅速地散布到较多个输出的密文数字中，以便隐蔽明文数字的统计特性。通过置换（比如重新排列字符）产生扩散。②混淆：使作用于明文的密钥和密文之间的关系复杂化，使明文和密文、密文和密钥之间的统计相关特性极小化，从而使统计分析攻击不能奏效。通常方法是代换。

4.6 数据加密标准 DES（Data Encryption Standard）

DES 是一种分组密码，其输入的明文长度为 64bit，密钥长度为 56bit，输出的密文长度为 64bit。
DES 过程：①64bit 明文数据 ②初始置换 IP（扩散） ③16 轮迭代变化（轮密钥在此作用，混淆） ④逆置换 ⑤64bit 密文数据
DES 特点：①加密和解密运算步骤相同。②加密和解密时使用的轮密钥次序为相反。③DES 采用 Feistel 网络结构，是一种对称结构，满足对合性。优点是加解密可用同一芯片。
DES 的 8 个 S 盒：混淆 (x1,x2,x3,x4)选择列，(x0,x5)选择行，输出 4 位
DES 的 P 盒：扩散 对 S1 至 S8 盒输出的 32bit 数据进行坐标置换

4.7 高级加密标准 AES（Advanced Encryption Standard）

避免了多重加密（例如 3DES）的使用。
AES 长度：密钥长度为 128/192/256bit，分组长度固定为 128bit。
Rijndael：是分组长度和密钥长度均可变的分组密码。128/192/256bit
AES 加密过程：明文→轮密钥加→1~9 轮变换（字节代换、行移位、列混淆、轮密钥加）→字节代换→行移位→轮密钥加→密文。每一轮（最后 1 轮除外）变换由 4 个不同的变换组成。

4.8 分组密码的工作模式

电码本模式 ECB：对连续排列的消息进行逐段加密，是确定性的加密模式
密码分组链接模式 CBC：分组密码算法，使得每个密码分组不仅依赖于所对应的原文分组，而且依赖于所有以前的数据分组。密文输出随机化。
密码反馈模式 CFB：将输出的密码分组反馈至移位寄存器作为输入，经加密后形成密钥流分组，再与输入明文分组相异或。
输出反馈模式 OFB：将输出分组反馈回去，经分组加密后输出一个密钥流分组，再将密钥流分组与明文分组相异或。
计数器模式 CTR：将计数器从初始值开始计数，得到的值反馈给算法。随计数增加，输出连续的密钥流分组，再将密钥流与明文分组相异或。

算法	分组长度	密钥长度	加密轮数	安全性
DES	64bits	56bits	16	密钥短且分组长度不适应64位总线
AES	128bits	8/192/256b	2010/12/14	安全
SM4	128bits	128bits	32	安全

单钥体制的不足：①密钥管理量的困难：两两分别用一个密钥时，n 个用户需要 C(n,2)=n(n-1)/2 个密钥，当用户量增大时，密钥空间急剧增大。
②密钥建立问题：对协商密钥的信道的安全性的要求比正常的传送消息的信道的安全性要高。③数字签名问题：传统加密算法无法实现抗抵赖。

5 双钥（公钥）密码体制、非对称

5.1 双钥密码体制的基本概念

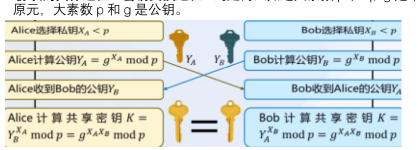
公钥密码体制：又称非对称密码体制或双钥密码体制，其加密和解密数据使用不同的密钥。用对方公钥加密。用自己私钥解密。
特点：①每个用户都公钥和私钥 ②解决了密钥的发布和管理问题
用途：①密钥分发（交换秘密信息、交换对称加密密钥）
②消息加密（直接加密、公钥加密私钥解密、密钥匹配）
③数字签名（发送方用自己私钥签名、接收方用对方公钥验证签名）

5.2 RSA

RSA 安全性：取决于模 n 分解的困难性（大整数分解）。
RSA 过程：①设 Bob 的公钥为(e, n)，私钥为 d，明文为 m
②Alice 用 Bob 的公钥做加密：c=m^e mod n，发给 Bob
③Bob 用 Bob 的私钥做解密：m=c^d mod n
RSA 特点：①双方从不认识，都可进行保密通信，只要 A 知道 B 的公钥。
②速度慢，它不适用于对图像、话音等进行实时数据加密。
③要求对公开密钥进行保护，防止攻击者对公钥的修改和替换。
RSA 局限性：加密速度很慢（DES 的 1‰），一般只用于密钥交换与认证。
RSA 应用：数据加密、数字签名、同时达到秘密通信与数字签名

5.3 D-H 公钥密码体制（Diffie-Hellman）

D-H 核心思想：交换公钥、计算共享密钥。基于求解离散对数难题。
D-H 安全问题：可抵抗被动攻击，但不能抵抗中间人攻击。两个主体每次可以选择新的秘密钥(私钥)，并计算及交换新的公钥。
D-H 协议的具体过程—密钥交换过程：约定两人知道大素数 p 和 q，g 是本原元，大素数 p 和 g 是公钥。



5.4 其它公钥密码

Rabin 密码体制（RSA 特例，安全）、Merkle-Hellman 背包密码体制（已攻破）、McEliece 体制（基于纠错码，已攻破）、LUC 密码体制（安全）、椭圆曲线密码体制 ECC（安全）、有限自动机体制（中国提出，已攻破）、概率加密体制（不能用于数字签名）

算法＼功能	加密/解密	密钥交换	签名/验证
RSA	是	是	是
ElGamal	是	是	是
ECC	是	是	是
DSA	否	否	是
DH	否	是	否
SM2	是	是	是

6 消息认证和杂凑函数

6.1 消息的真实性与认证

认证：①保密性（confidentiality）采用加密机制：不希望他人知道消息
②真实性（authenticity）采用认证机制：消息内容的完整性、消息内容的真实性、消息来源的真实性、实体身份的真实性
认证方式：①对称认证：双方信任，防止第三方攻击
②非对称认证：双方不信任，防止对方攻击

6.2 杂凑（Hash）函数：不需要密钥

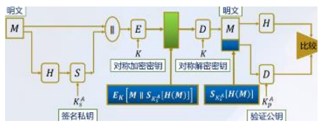
杂凑（Hash）函数：将任意串压缩成定长的比特串。常用有 MD5、SHA、采用分组密码算法构造的 hash 函数等。
单向杂凑函数（One-way Hash Function）满足：
①快速性：任给x，计算$y=H(x)$容易
②单向性：任给y，由$y=H(x)$计算x困难
③无碰撞：寻找$x1 \neq =x2$，满足$H(x1)=H(x2)$是困难的。
杂凑函数性质：①变量x是任意长度，而$H(x)$的结果是固定的长度$n$bits
②抗原象攻击：已知杂凑值y，找一个输入串x使$y=H(x)$在计算上不可行
③抗碰撞攻击：找两个输入$x1$和$x2(x1 \neq x2)$，使得$H(x1)=H(x2)$不可行
杂凑函数满足条件：①函数的输入可以是任意长度 ②函数的输出是固定长度 ③已知x求$H(x)$较为容易，可用硬件或软件实现 ④已知 h，求使得$H(x)=h$的x在计算上不可行（函数的单向性）称$H(x)$为单向杂凑函数 ⑤已知x找$y(y \neq x)$使得$H(y)=H(x)$在计算上是不可行 ⑥找出任意两个不同的输入x和y使得$H(y)=H(x)$在计算上是不可行的（⑤⑥是无碰撞）
Hash 码的分类：①校验和 CRC ②消息认证码 MAC 算法是使用密钥参与杂凑运算的算法 ③消息检测码 MDC 算法是无密钥参与杂凑运算的算法（单向 Hash 函数 OWHF、抗碰撞 Hash 函数 CRHF）④无碰撞性 Hash

6.3 消息认证码 MAC 与消息检测码 MDC

消息认证码（校验和）：$MAC = H(m||k)$，m 变长消息，k 双方共享密钥。
消息检测码（篡改检测码）：$MDC = H(m)$

6.4 杂凑函数的应用

保密性（仅双方有 K）、消息认证（签名私钥）、数字签名（$H(M)$）



6.5 常用杂凑函数

	MD4	MD5	SHA
Hash值	128bit	128bit	160bit
分组处理长	512bit	512bit	512bit
基本字长	32bit	32bit	32bit
步数	48(3*16)	64(4*16)	80(4*20)
消息长	≤2^64bit	不限	2^64bit
基本逻辑函数	3	4	3(第2,4轮相同)
常数个数	3	64	4
速度		约为MD4的1/7	约为MD4的3/4

杂凑函数在密码学中的应用：数字签名、公钥密码系统、随机数发生器

7 数字签名

7.1 数字签名的基本概念

概念：对数字消息进行签名，以防消息伪造或篡改，也可用于身份鉴别。
条件：①收方能够确认发方的签名，但不能伪造。②发方发出签名的消息后，不能再否认他所签发的消息。③收方对已收到的签名消息不能否认。④第三者可以确认收发双方之间的消息传送，但不能伪造。
特征：①可信：任何人都可以方便地验证签名的有效性。②不可伪造：除了合法的签名者之外，任何其他人伪造其签名是困难的。③不可复制：对一个消息的签名不能通过复制变为另一个消息的签名。④签名的消息是不可改变的：经签名的消息不能被篡改。一旦被篡改，则可以发现不一致性。⑤不可抵赖：发送消息方和接受消息方都不可抵赖。
作用：身份认证、防假冒、防抵赖、防信息篡改、法律效益
与公钥加密的区别：①**公钥加密**：A 采用 B 的公钥加密，A 将密文发送给 B。B 用自身私钥对收到的密文解密，恢复出明文。
②**数字签名**：A 用自己的私钥对消息m签名，A 将m和签名发送给 Bob。B 收到m和签名后，B 采用 A 的公钥验证签名的有效性。
③**区别**：一个签名的消息很可能在多年之后才验证其真实性、数字签名可能需要多次验证、数字签名的安全性和抗伪造性要求很高、数字签名要求签名速度比验证速度更快
与消息认证的区别：①**消息认证**：收方能够验证消息发送者身份、消息内容是否被篡改（对身份认证，保持数据完整性，无不可否认性）
②**数字签名**：身份认证，保持数据完整性，不可否认性
分类：①按照消息**是否被压缩**分类：对整体消息、压缩消息进行签名
②按照**是否直接签名**分类：直接数字签名、可仲裁的数字签名（发送方先对消息签名，再将签名和消息一起发送给仲裁者，仲裁者对其进行验证，签发一个证据证明它的真实性，最后消息、数字签名、签名真实性一起发给接受者）③按照消息 / 签名的对应关系分类：确定性、随机性
数字签名体制的构成：签名算法、验证算法
数字签名安全性约定：签名密钥（私钥）保密、验证密钥（公钥）公开
为什么对消息的 Hash 函数值签名而不是直接对消息签名？ 定长、省时间

7.2 RSA 签名体制

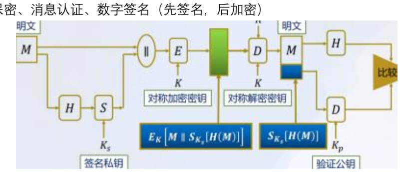
RSA 安全性：依赖于 n=p1×p2 分解的困难性

7.3 DSS 签名体制

DSS 数据签名标准：使用了 DSA 算法。（RSA 算法只用于双钥密码体制）
DSA 算法：是 DSS 签名标准中所采用的数字签名算法。
DSA 特点：DSA 只是一种算法，和 RSA 不同之处在于它不能用作加密和解密，也不能进行密钥交换，只用于签名，它比 RSA 要快很多。

7.5 应用方案

保密、消息认证、数字签名（先签名，后加密）



7.6 其它数字签名体制

双重签名 DS（Dual Signature）：消息发送方对发给不同接收方的两条信息分别进行哈希运算，得到各自摘要，然后将这两条摘要连接，再进行哈希运算，生成新的摘要，即双重数字摘要，最后用发送方的私人密钥对新的双重数字摘要加密，得到一个基于两条数字摘要基础上的数字签名。
双重签名优点：①能够证实商家收到的信息没有被篡改，还能证实银行收到的信息也没有被篡改，同时保证了商家与银行只能知晓客户发出的完整购物单据信息中应看的那一部分，对客户的其它隐私进行了保密。
②发信者对两个消息 M1 和 M2 只需要计算一个签名。
盲签名 BS（Blind Signature）：某人对数据签名，但不让他知道数据内容。
盲签名特点：①消息内容对签名者不可见。②签名被公开后，不能追踪签名。
群签名 GS(Group Signature)：①只有群中的成员才能代表该群体进行签名。②接收方用公钥验证群签名，但无法知道由群体中的哪个成员所签。③发生争议时，由群体中的成员或可信赖机构识别群签名的签名者。
数据时间戳 DTS（Digital Time-Stamp）：是由专门的机构提供电子文件发表时间的安全保护。时间戳是电子文件产生时间、内容完整性及不可否认性的有效电子凭证。防止重放攻击。
组成：①需加时间戳的文件的摘要 ②收到的时间 ③DTS 的数字签名
不可否认签名 US（Undeniable Signature）:要求在签名者合作下才能验证签名。以防止复制和散布签名者所签的文件。可以用于知识产权的保护。
防失败签名 FSS（Fail-Stop Signature）：强安全性的数字签名。当用户的签名受到攻击，甚至已分析出私钥，也难以伪造。同时用户也难以对自己的签名进行抵赖。是一次性签名方案，即给定密钥只能签署一个消息。
代理签名 PS(Proxy Signature)：代理签名就是某人授权其代理进行的签名，在委托签名时，签名密 钥不交给代理人。（不可区分性、不可伪造性、代理签名的差异、可证实性、可识别性、不可抵赖性）
指定证实人签名 DCS（Designated Confirmer Signature）：在一个机构中，指定一个人负责证实所有人的签名。任何成员的签名都具有不可否认性，但证实工作均由指定人完成。签名者必须限定由谁才能证实他的签名。证实人充当了仲裁角色，使用证实人的公钥验证所有人的签名。
一次性签名 OTS(One-Time Signature)：签名者至多对一个消息进行签名，否则签名就可能被伪造。在公钥签名体制中，一要求对每个签名消息都要采用一个新的公钥作为验证参数。**优点**是签名和验证速度非常快。

9 数字证书与公钥基础设施 PKI

9.1 公钥基础设施 PKI 的基本概念(Public Key Infrastructure)

起因：公钥安全分发问题。建立大家都信任的第三方，并参与公钥的分发。
PKI 概念：是一种用公钥密码理论和技术实施和提供安全服务的、具有普适性的安全基础设施。

PKI 目的：解决网上身份认证、电子信息的完整性和不可抵赖性等安全问题，为网络应用提供可靠安全服务

PKI 任务：在电子商务和电子政务中，为网络用户提供可信的数字身份认证。

PKI 组成：证书机构 CA、注册机构 RA、证书发布库、密钥备份与恢复、证书撤销、PKI 应用接口

1 证书机构 CA：证书生成、证书颁发、证书撤销、证书更新、证书归档、CA 自我审查、日志审计、密钥恢复

功能：①负责发放和管理数字证书。②提供网络身份认证，负责证书签发及证书的管理。（跟踪证书状态、在证书需要撤销时发布证书撤销通知）③维护证书档案和证书相关的审计。

2 注册机构 RA：是数字证书注册审批机构，是认证中心的延伸。RA 按照政策与管理规范对用户的资格进行审查。（接受与验证最终用户的注册信息，为最终用户生成密钥、接收与授权证书撤销请求）

3 证书发布库：用于集中存放 CA 颁发证书和证书撤销列表 CRL。支持分布式存放提高查询效率，LDAP 协议是创建高效的大规模 PKI 认证的关键。

4 密钥备份与恢复：①备份：仅备份和恢复 CA 的公钥/私钥对，而不备份用户的签名密钥。②恢复：若用户声明公钥/私钥对是用于数据加密的，则 CA 即可对该用户的私钥进行备份。用户丢失后可通过可恢复。

5 证书撤销：①周期性发布机制（证书撤销列表 CRL）

②在线证书查询机制（在线证书状态协议 OCSP）

PKI 的应用：认证服务、数据完整性、、数据保密性、、不可否认、、公正服务

RA 与 CA 的关系：注册机构 RA 主要帮助证书机构 CA 与最终用户交互，注册机构 RA 不能签发证书，证书只能由证书机构 CA 签发。

9.2 数字证书

数字证书概念：将用户身份 ID 与其所持有的公钥PK绑定，再由认证中心 CA 对该用户身份及对应公钥的组合$\{ID||PK\}$进行数字签名得到S，然后将$\{签名S||身份ID||公钥PK\}$加以存储，即数字证书。

数字证书结构：证书序号、签名算法标识符、签名者、有效期（之前/之后）、主体名、主体公钥信息、签名者唯一标识符、主体唯一标识符、扩展信息、认证机构数字签名

数字证书生成步骤：密钥生成、用户注册、验证信息、证书生成

1 密钥生成：由用户自己/注册机构 PKI 的 RA 生成公钥/私钥对

2 注册：用户将公钥和证明材料发送给注册机构

3 验证信息：①RA 验证用户材料，明确是否接受用户注册

②检验用户私钥的拥有证明 POP(Proof Of Possession)

4 证书生成：①RA 将用户申请数据信息传递给证书机构 CA。②证书机构验证后生成数字证书。③证书机构将证书发给用户。④在 CA 维护的证书目录中保留一份证书记录。(RA 将数字证书采用用户公钥加密后，发送给用户。用户需要用与公钥匹配的私钥解密方可取得对证书。)

数字证书的签名与验证

1 CA 签发证书：前几个字段→消息摘要算法→消息摘要→（证明机构的私钥）数字签名算法→数字签名（"CA 签名"字段没有参与消息摘要运算）

2 数字证书验证：消息摘要算法→取出 CA 签名→签名验证算法→比较摘要

数字证书的层级结构：根 CA、二级 CA、三级 CA

数字证书撤销检查：脱机撤销状态检查（证书撤销列表 CRL）、联机撤销状态检查（联机证书验证协议 OCSP、简单证书验证协议 SCVP）

脱机检查：证书过期、证书简明机构链、序列号是否在 CRL

联机检查：OCSP 请求、查询 X.500 目录、查询响应、回复证书有效性

9.3 PKI 体系结构：PKIX 模型

PKIX 提供的公钥基础设施服务：注册、初始化、认证、密钥对回复、密钥生成、密钥更新、交叉证书、撤销

PKIX 体系结构 X.509 v3：操作协议（定义基础协议，向 PKI 用户发布证书、CRL 和其他管理与状态信息的传输机制）、管理协议（支持不同的 PKI 实体交换信息）、策略大纲（定义了生成证书策略之类的文档，确定对于特定领域选择证书类型时要考虑的重点）、时间标注与数字证书服务（构建权限管理基础设施 PMI 的基础，这些结构支持访问控制等应用）

9.5 授权管理设施：PMI（核心思想：以资源管理为核心）

区别：PKI 证明用户是谁，PMI 证明这个用户有什么权限。PMI 建立在 PKI 提供的可信身份认证服务的基础上，以属性证书的形式实现授权的管理。

PNI 的定义：是属性证书、属性权威、属性证书根架等部件的集合体，用来实现属性证书的产生、管理、存储、分发和撤销等功能。

PMI 的实现机制：①基于 Kerberos 的机制：便于软硬件实现且比非对称密码算法更快、存在不便于密钥管理和单点失败的问题，适用于大量的实时事务处理环境中的授权管理 **②基于策略服务器概念的机制**：高度集中便于单点管理、容易形成通信瓶颈、适用于地理位置集中的实体环境 **③基于属性证书的机制**：具有失败拒绝的优点，性能不高，适用于不可否认的授权管理

	PKI	PMI
证书	PKC公钥证书	AC属性证书
颁发者	证书机构	属性机构
接收者	证书主体	证书持有者
绑定	主体的名字绑定到公钥	证书持有者绑定到一个或者多个特权属性
撤销	证书撤销列表CRL	属性证书撤销列表ACRL
根	根CA或信任锚	权威源SOA
子机构	子CA	AA
验证者	可信方	特权验证者

12 防火墙

12.1 防火墙概述

防火墙概念：防火墙是由软件和硬件组成的系统，它处于安全的网络和不安全的网络之间，根据由系统管理员设置的访问控制规则，对数据流进行过滤。对于内部攻击以及绕过防火墙的连接却无能为力。

防火墙对数据流的处理方式：①允许满足规则的数据流通过。②拒绝不满足规则的数据流通过，并向发送者回复消息，提示发送者该数据流已被拒绝。③将数据流丢弃，不做进行任何处理，且不回复。

防火墙满足的要求：①所有进出网络的数据流都必须经过防火墙。②只允许经过授权的数据流通过防火墙。③防火墙自身对入侵是免疫的。

防火墙不能防范的攻击：内部攻击、不通过它的连接、病毒、所有的威胁

防火墙的功能：数据包状态检测过滤、管理进出网络的访问行为、封堵某些禁止的业务、记录进出网络的信息和活动、对网络攻击进行检测和报警

防火墙的发展：①第一代：包过滤 ②电路级网关 ③应用及网关 ④动态包过滤 ⑤第五代：1998 年内核代理结构

12.2 防火墙的类型和结构（分类）

按软硬件：软件防火墙、硬件防火墙、芯片级防火墙

按应用部署：单一主机防火墙、路由器集成式防火墙、分布式防火墙

按防火墙结构：单一主机防火墙、路由器集成式防火墙、分布式防火墙

按防火墙性能：百兆级防火墙、千兆级防火墙

按防火墙技术：①包过滤型：第一代静态包过滤、第二代动态包过滤

②应用代理型：第一代应用网关型代理防火、第二代自适应代理防火墙

OSI 模型与防火墙类型的关系：

数据包规则的应用策略：

①默认接受：除明确指定禁止的数据包，其他都允许通过。"黑名单"。

②默认拒绝：除明确指定通过的数据包，其他都禁止通过。"白名单"。

12.3 静态包过滤防火墙（网络层）

包过滤防火墙：①也称访问控制列表，根据已定义的过滤规则来审查每个数据包，确定该数据包是否与过滤规则匹配，从而决定数据包是否能通过。②与规则相匹配的包根据路由信息继续转发，否则将之丢弃。③包过滤防火墙会对每一个通过防火墙的数据包的包头长度、选项、数据段和标志等信息进行结构化检查，以防止错误的数据包通过防火墙。

优点：对网络性能影响较小、成本较低

缺点：安全性较低、缺少状态感知能力、容易遭受 IP 欺骗攻击、创建访问控制规则比较困难

12.4 动态包过滤防火墙（传输层）

动态包过滤防火墙：①具有状态感知能力②典型的动态包过滤防火墙工作在网络层③先进的动态包过滤防火墙工作在传输层

比较：对外出数据包进行身份记录，便于下次让有相同连接的数据包通过。

工作原理：动态包过滤防火 墙需要对已建 接和规则表进行 动态维护，因此 是动态的和有状 态的。典型的动态包过滤防火墙能够感觉到新建连接与已建连接之间的差别。

优点：①采用 SMP 技术时，对网络性能的影响非常小。②动态包过滤防火墙的安全性优于静态包过滤防火墙。③"状态感知"能力使其性能得到了显著提高。④如果不考虑操作系统成本，成本很低。

缺点：①仅工作于网络层，仅检查 IP 头和 TCP 头。②没过滤数据包的净荷部分，仍具有较低的安全性。③容易遭受 IP 欺骗攻击。④难于创建规则，管理员必须要考虑规则的先后次序。⑤如果连接在建立时没有遵循三步握手协议，就会引入的风险。

其它防火墙

应用代理型防火墙：工作在应用层，特点是完全阻隔网络通信流，通过对每种应用服务编制专门的代理程序实现监视和控制应用层通信流的作用。

应用网关型防火墙：通过一种代理技术参与到一个 TCP 连接的全过程。数据包经处理后，像是源于防火墙外部网卡，达到隐藏内部网络的作用。

自适应代理型防火墙：在毫不损失安全性的基础上上将代理型防火墙的性能提高 10 倍以上。基本要素：自适应代理服务器+动态包过滤器

12.5 网络地址转换 NAT

NAT 的优点：隐藏内部网络的拓扑结构，提升网络安全性。

静态 NAT：在进行网络地址转换时，内部与外部的 IP 地址是一一对应关系。

实现：设置外部端口、设置内部端口、在内部本地与外部合法地址之间建立静态地址转换。

动态 NAT：可用的 IP 地址限定在一个范围内。

实现：设置外部端口、设置内部端口、定义合法 IP 地址池、定义内部网络中允许访问 Internet 的访问列表、实现网络地址转换。

PAT 端口地址转换：不仅网络地址发生改变，协议端口也会发生改变。

SNAT 源网络地址转换：当内部用户使用专用地址访问 Internet 时，必须将 IP 头部 的数据源地址转换成合法的 Internet 地址。

DNAT 目标网络地址转换：必须将数据包中的目的地址转换成服务器的专用地址，使合法的 IP 地址与内部网络中服务器的专用地址相对应。

NAT 的分类：静态网络地址转换、动态网络地址转换、端口地址转换

总结：NAT 技术能透明地对所有内部地址作转换，使外部网络无法了解内部网络的内部结构，同时允许内部网络使用自己偏的 IP 地址和专用网络，防火墙能详尽记录每一个主机的通信，确保每个分组送往正确的地址。

13 入侵检测技术 IDS (Instrusion Detection System) **非重点

13.1 入侵检测概述

入侵：非法取得系统控制权、利用系统漏洞收集信息、破坏信息系统

入侵检测：①检测对系统的非授权访问②监控系统运行状态，保证系统资源的保密性、完整性、可用性③识别针对计算机系统网络系统或广义信息系统的非法攻击

入侵检测系统的通用模型：

IDS 的主要功能：①网络流量的跟踪与分析功能②已知攻击特征的识别功能③异常行为的分析、统计与响应功能④特征库的在线和离线升级功能⑤数据文件的完整性检查功能 ⑥自定义的响应功能⑦系统漏洞的预报警功能 ⑧IDS 探测器集中管理功能

IDS 的任务/三个基本结构：

信息收集：系统和网络的日志文件、目录和文件中的异常改变、程序执行中的异常行为、物理形式的入侵信息（收集用户行为）

信息分析：模式匹配（只能检测已知风险）、统计分析、完整性分析（①操作模型 ②方差 ③多元模型 ④马尔可夫过程模型 ⑤时间序列）

安全响应：主动响应、被动响应（响应方式：记录日志、实时显示、E-mail 报警、声音报警、SNMP 报警、实时 TCP 阻断、防火墙联动）

13.2 入侵检测原理及主要方法

异常检测：又称为基于行为的入侵检测技术，用来识别主机和网络中的异常行为。该技术假设攻击与正常合法的活动有明显的差异。

检测方法：统计异常检测方法、特征选择异常检测方法、基于贝叶斯推理…、基于贝叶斯网络异常检测方法、基于模式预测异常检测方法。

误用检测：又称为基于知识的入侵检测技术。该技术假设所有 入侵行为和手段（及其变形）都能表达为一种模式或特征。

检测方法：基于条件的概率误用检测方法、基于专家系统误用检测方法、基于状态迁移分析…、基于键盘监控…、基于模型误用检测方法

入侵检测技术：①基于概率统计的检测（最常用技术，对历史行为建立模型）②神经网络③专家系统④模型推理⑤免疫⑥入侵检测的新技术

13.3 IDS 的结构与分类

按数据来源分类：①基于网络的 IDS（NIDS）：截获数据包，提取特征 并与知识库中已知的攻击签名相比较②基于主机的 IDS（HIDS）：通过对日志和审计记录 的监控和③分布式 IDS (DIDS)：同时分析来自主机系统审计日志和网络数据流

按检测策略分类：①滥用检测：将收集到的信息与数据库比较 ②异常检测：测量属性的平均值与系统行为比较 ③完整性分析：关注是否被更改

13.4 基于网络的 NIDS

NIDS 概念：根据网络流量、网络数据包和协议来分析入侵检测。利用运行在随机模式下的网络适配器来监视并分析通过网络的所有通信业务。

检测内容：包头信息+有效数据部分（两者之和为数据包）

NIDS 常用技术：①模式、表达式或字节匹配。 ②频率或穿越阈值。 ③低级事件的相关性。 ④统计学意义上的非常规现象检测。

NIDS 优点：①拥有成本低。②攻击者转移证据困难。③实时检测和响应。④能够检测未成功的攻击企图。 ⑤操作系统独立。

13.5 基于主机的 HIDS

HIDS 概念：①根据主机系统的系统日至和审计记录进行入侵检测。

②检测针对主机的攻击，通常被部署在关键服务器上，被认为是保护关键服务器的最后一道防线。

检测内容：系统调用、端口调用、应用日志、系统日志、安全审记

HIDS 常用技术：①文件和注册表保护技术。 ②网路安全防护技术。

③IIS 保护技术。④文件完整性分析技术。

HIDS 优点：①捕获应用层入侵。 ②监视特定的系统活动。 ③非常适应与加密和交换环境。 ④近实时的检测和应答。 ⑤不需要额外的硬件。

NIDS 和 HIDS 的共同缺点：①系统的弱点和漏洞分散在网络的各个主机上，这些弱点有可能被入 侵者一起利用。②入侵检测不再是单一的行为，表现出协作入侵的特点，如分布式拒绝服务攻击（DDos）。③入侵检测依靠的数据分散化，收集原始数据变得困难，如交换网络使得监听网络数据包收到限制。④网络传输速度加快，网络的流量大，集中处理原始数据的方式往往造成检测瓶颈，从而导致漏检。

14 VPN 虚拟专网 Virtual Private Network

14.1 VPN 概述

VPN 背景：在端到端的数据通路上随处都有可能发生数据的泄漏，包括接入段链路、ISP 接入设备上、因特网上、安全网关上、企业内部网上

VPN 概念：是指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专网。

VPN 分类：网关-网关 VPN、远程访问 VPN

VPN 特点：费用低、安全保障、服务质量保证、可扩充性和灵活、可管理

VPN 关键技术：隧道技术、加解密技术、密钥管理、身份认证、访问控制

14.2 隧道协议与 VPN

隧道技术：隧道是建立在公共网络上的一条加密的数据通道。利用公共网络已有的数据通信方式，在隧道的一端将数据进行封装，然后通过已建立的虚拟通道（隧道）进行传输。在隧道的另一端进行解封装操作，将得到的原始数据交给对端设备。在进行数据封装时，根据在 OSI 参考模型中位置的不同，可以分为第二层隧道技术和第三层隧道技术两种类型。

第二层隧道技术：是在数据链路层使用隧道协议对数据进行封装，然后再把封装后的数据作为数据链路层的原始数据，并通过数据链路层的协议进行传输（协议：PPTP、L2F、L2TP）。

第三层隧道技术：是在网络层进行数据封装，利用网络层的隧道协议将数据进行封装，封装后的数据再通过网络层的协议进行传输(GRE、IPSec)

加密技术：通过公共网络传输的重要数据必须经过加密处理，以确保网络上其他未授权的实体无法读取该信息。常用的信息加密体制主要包括对称加密体制、非对称加密体制，实际应用时一般是将两种密体制混合使用，利用非对称加密技术进行密钥的协商和交换，而采用对称加密技术进行用户数据的加密。

14.3 VPN 的应用类型

远程接入 VPN (Access VPN)：也称移动 VPN，为移动用户提供一种访问单位内部网络资源的方式，主要应用于单位内部人员在外（非内部网络）访问单位内部网络资源的情况下，提供远程接入单位内部网络的服务。

优点：①简化网络配置②通过本地接入来代替长途接入，节省通信费用。③便于扩展，同时接入的用户不受线路限制。

内联网 VPN (Intranet VPN)：它将位于不同地址位置的两个内部网络（LAN1 和 LAN2）通过公共网络连接起来，形成一个逻辑上的局域网。位于不同物理网络中的用户在通信时，内联网就像在同一局域网中一样。

外联网 VPN（Extranet VPN）：在内联网 VPN 中位于 LAN1 和 LAN2 中的主机是平等的，可以实现彼此之间的通信。但在外联网 VPN 中，位于不同内部网络（LAN1、LAN2、LAN3）的主机在功能上是不平等的。在这种联系过程中，企业需要根据不同的用户身份（如供应商、销售商等）进行授权访问，建立相应的身份认证机制和访问控制机制。

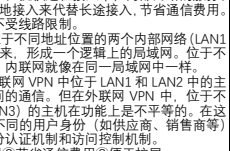
优点：①节省 WAN 带宽的费用②节省通信费用③便于扩展

VPN 的分类：①按应用范围（Access VPN 远程接入 VPN 远程办公室安全访问企业网络、Intranet VPN 组建跨地区的企业内部互联网络、Extranet VPN 企业与客户、合作伙伴之间建立互联网络。）

②按 VPN 网络结构（基于 VPN 的远程访问、…网络互联、点对点通信）

VPN 的应用范围：①已通过专线连接实现广域网的企业，增加业务带宽提高，经济可靠升级。②企业用户和分支机构分布范围广、距离远，部署展企业网实现远程访问和局域网互联（跨国、跨地区企业）。③分支机构、远程用户、合伙多的企业，需扩展企业网。④关键业务多且对通信线路保密和可用性要求高的。

14.4 IPSec VPN（网络层协议）



IPSec 概念

IPSec 协议概述：是 IPv6 的组成部分，也是 IPv4 的可选扩展协议。最主要的应用是构造 VPN，作为第三层隧道协议实现了 VPN 通信，是一种端到端的确保 IP 层通信安全的机制。不是单独的协议，是一组协议。

IPSec 服务：①数据加密：IPSec 的数据加密服务由 ESP(Encapsulating Security Payload，封装安全载荷）提供，算法采用 CBC（Cipher Block Chaining，加密块链接）方式，即使信息在传输过程中被窃听，非法用户也无法得知信息的真实内容。

②数据源地址验证、数据完整性检查：IPSec 使用 HMAC（Hash-Base Message Authentication Code）进行数据验证。HMAC 是使用单向散列函数对包中源 IP 地址、数据内容等在传输过程中不变的字段计算出来的，具有唯一性。数据如果在传输过程中发生改动，在接收端就无法通过验证。

③防止重放攻击：IPSec 使用 AH 为每个 SA 建立序列号，而接收端采用滑动窗口技术，丢弃所有的重复的包，因此可以防止重放攻击。

IPSec 包括：AH（Authentication Header，认证报头）、**ESP**（Encapsulating Security Payload，封装安全载荷）、**IKE**（Internet Key Management，密钥交换协议）、**SA**（Security Association，安全关联）、**DOI**（Domain of Interpretation，解释域），认证和加密算法。

IPSec 工作原理：类似于包过滤防火墙。网关通过查询 SPD 决定对接收到的 IP 数据包进行转发、丢弃或 IPSec 处理。网关可以对 IP 数据包只进行加密或认证，也可以对数据包同时实施加密和认证

SA 安全关联：①由一个（安全参数索引 SPI，源/目的 IP，安全协议号 AH/ESP）三元组唯一标识②决定了对报文的处理协定（协议 AH/ESP、算法 DES/3DES/AES、密钥）③SA 是单向的，具有生存周期④手工建立或协商生成，存入 SAD

IPsec 对等体：IPsec 的两个端点。要在两个对等体（安全网关）之间实现数据的安全传输，就要在两者之间建立 SA。SA 是 IPsec 的基础。

SPI 安全参数索引：32 比特的数值，每个 IPSec 报文中都携带，唯一标识 SA。

SPI 组成：序列号计数器、序列号溢出、防重放窗口、AH 认证密钥、ESP 认证密钥、ESP 加密算法、操作模式、PMTU 路径最大传输单元、SA 生存期

SAD 安全关联数据库(Security Association Database)维护 IPSec 中的所有 SA

SP 安全策略：目的 IP、源 IP、传输层协议、系统名、用户 ID、上层端口、标志（采取的动作 Discard/Bypass IPSec/Apply IPSec）、SA 指针（包括指向 SA 的指针、IPSec 协议、密码算法、生成 ICV）的算法）

SPD 安全策略数据库(Security Policy Database)：保存安全策略，在处理进入和外出包 时，需查阅 SPD，以判断为这个包提供哪些安全服务，具体策略包括丢弃、直接转发或应用安全服务处理等。

安全隧道：是点对点的安全"连接"。通过在安全隧道的两端，本端和对端，配置对应的安全关联，实现在本端对 IP 报文加密，在对端解密。可跨越多台路由器和多个网络，只有安全隧道的两端共享了秘密，对于隧道中间的路由器和网络，所有的加密报文和普通报文一样被透明地转发

AH 认证报头协议：为 IP 数据报的 IP 头和上层协议数据提供完整性检查（哈希函数校验）、数据源认证（加入共享密钥），并防止重放攻击（AH 报头序列号）。不提供数据加密服务。

ESP 封装安全载荷：提供数据加密，既可加密 IP 数据报内容（TCP、UDP、ICMP、IGMP），也可加密整个 IP 数据报。除提供 AH 协议功能外，还可对 IP 报文加密（数据包、数据流）。

AH 与 ESP 比较：AH 比 ESP 少了一个整体包的加密功能。而二者各自提供的认证其根本区别在于它们的覆盖范围。AH 关注 IP 包头的完整性，认证，而没有数据部分的加密。ESP 主要是完整性，认证，和数据部分的加密。但是 ESP 不能针对 ip 包头，只针对数据部分。

传输模式应用于主机之间端对端通信，该模式要求主机支持 IPSec。

隧道模式应用于网关模式，即在主机的网关（防火墙，路由器）上加载 IPSec，这个网关就同时升级为 **SG**（Security Gateway，安全网关）。

安全网关 SG：指具有 IPsec 功能的网关设备（安全加密路由器）。安全网关之间可以利用 IPsec 对数据进行安全保护，保证数据不被偷窥或篡改。

IPSec 的模式与加密传输流程（传输模式 Transport、隧道模式 Tunnel）

传输模式特点：封装模式相对简单且传输效率较高、IP 包头未被保护、适用于两台主机之间的数据保护

隧道模式特点：IP 包头被保护、适用于网关之间建立安全 VPN 隧道

IPSec 加密传输流程：IPsec 首先根据访问列表对照的结果，将对应的 SA 的信息与包头放到 IPsec 队列中排队逐一处理。之后根据该数据包指定的 SA 配置：①检查此 SA 的模式，隧道模式则将原 IP 包整个当作数据交给加密部分；传输模式则将 IP 包头提出来只送数据段到加密部分。②加密部分处理数据方式一致。③加密完成后为新的数据打上一个新的 IP 包头，隧道模式时将 SA 配置中设置的隧道的入口与出口 IP 地址作为新的源与目的地址。传输模式时把原来的 IP 包头直接放在数据前。

	传输模式SA	隧道模式SA
AH	对IP载荷和IP报头的选中部分、IPv6的扩展报头进行认证	对整个内部IP包（内部报头和IP载荷）和外部IP报头的选中部分、外部IPv6的扩展报头进行认证
ESP	对IP载荷和跟在ESP报头后面的任何IPv6扩展报头进行加密	加密整个内部IP包
带认证的ESP	对IP载荷和跟在ESP报头后面的任何IPv6扩展报头进行加密。认证IP载荷但不认证IP报头	加密整个内部IP包。认证内部IP包

因特网密钥交换协议 IKE

IKE 功能：协商通信参数和安全特性、认证通信对端、保护实体、建立安全关联、产生和交换和建立密钥、管理和删除 SA

IKE 混合协议的组成：①SKEME(决定了 IKE 主要使用 DH 来实现密钥交换）

②Oakley（决定了 IPSec 的框架设计，让 IPSec 能够支持更多的协议）

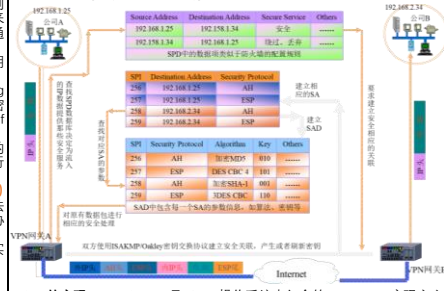
③ISAKMP（决定了 IKE 协商包的封装格式、交换过程和模式切换）

ISAKMP 因特网安全关联与密钥管理协议：①只能够为密钥交换来交换数据包，不能决定密钥交换实现的方式。②没有定义任何密钥交换协议的细节和加密算法、密钥生成技术或认证机制。与密钥交换独立，可被不同的密钥交换协议使用。③可用 UDP 或 TCP，常用 UDP。

VPN 通道的建立方式

建立方式	主机A	网关A	主机A-网关A	网关A-网关B	网关B-主机B	网关B	主机B
Host-Host	必须支持	任意	安全通道	安全通道	安全通道	任意	任意
Host-VPN	必须支持	任意	安全通道	安全通道	非安全通道	必须支持	必须支持
VPN-VPN	任意	必须支持	非安全通道	安全通道	非安全通道	必须支持	任意
RemoteUser-VPN	必须支持	用PSTN到ISP接入服务器/安全	安全通道	非安全通道	必须支持	任意

网关与网关之间的完整 VPN 工作原理图：



IPSec 的实现：Free SWAN 是 Linux 操作系统中包含的 IPsec VPN 实现方案

优点：①IPSec 与应用无关，IPSec VPN 的客户端支持所有 IP 层协议。

②IPSec 技术中，客户端至站点、站点对站点、客户端至客户端（client-连接所使用的技术是完全相同的。③IPSec VPN 网关一般整合了网络防火墙的功能。④IPSec 客户端程序可与个人防火墙等其他安全功能一起销售，因此，可保证配置、预防病毒，并能进行入侵检测。

缺点：①IPSec VPN 需要安装客户端软件，但并非所有客户端操作系统均支持 IPSec VPN 的客户端程序。②IPSec VPN 的连接性会受到网络地址转换 NAT 的影响，或受网关代理设备 proxy 的影响。③IPSec VPN 需要先完成客户端配置才能建立通信信道，且配置复杂。

15 身份认证

身份认证的必要性：防止身份欺诈、通信和数据系统的安全性、计算机的访问和使用、安全区的出入

身份证明系统的组成：示证者 P、验证者 V、攻击者 A、（第四方：可信者）

身份证明系统的要求：最大可能正确、识别合法示证者、通信有效性、最大可能防止攻击者伪装欺骗、计算有效性、无可传递性、可证明安全性、秘密参数、能安全存储、第三方实时参与、交互识别、第三方可信性

身份证明的基本分类：身份验证（是或否）、身份识别（是谁）

身份证明的基本途径：①个人特征（指纹、笔迹）②所知 ③所有

身份证明系统的服务质量评价指标：拒绝率(FRR)、漏报率(FAR)

15.1 身份证明（交互证明：零知识证明）

交互证明系统参与方：证明者 P、验证者 V

交互证明过程：每轮 V 向 P 发出一询问，P 向 V 做出一应答。所有轮执行完后，V 根据 P 是否在每一轮的应答，决定是否接受 P 的证明。

交互证明和数学证明的区别：数学证明的证明者可自己独立完成证明，交互证明是由 P 产生证明、V 验证证明，因此双方必须通过某种信道通信。

交互证明系统须满足以下要求：①正确性：若 P 知道某一秘密，V 将接受 P 的证明。②正确性：如果 P 能以一定的概率使 V 相信 P 的证明，则 P 知道相应的秘密。

15.2 口令认证系统

口令认证系统定义：根据已知事物验证份的方法，被广泛使用

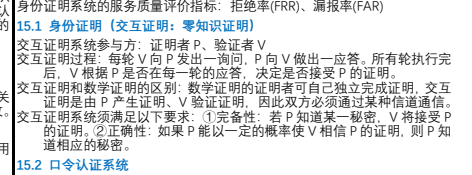
口令选择原则：易记、难以猜中或发现、能抵御蛮力破解攻击

口令认证系统系统分类：①非保密的联机系统：多个用户共用一个口令 ②安全性要求高的系统：每个用户配有专用口令

口令防止泄露的措施：①个人身份和口令用软件加密。②采用通行短语代替口令，通过密钥碾压技术生成较短的随机性密钥。

口令分发：邮寄方式、限定尝试输入口令的次数

询问法：



口令的控制措施：系统消息、系统口令的生成、双口令系统、封锁用户系统、最小长度、根口令的保护、限制试探次数、口令有效期

口令的控制措施：①反应法：被检口令与易猜中口令表逐个比较、检验费时、口令都有一定的可猜测性。②支持法：用户选择口令程序检验，若易于猜中须重新选择，可猜中性与安全性之间折中

15.3 个人特征的身份认证技术

个人生物特征的身份认证技术：可信度高、个人特征因人而异难以伪造、随身携带不易丢失、以用于刑事案件侦查

手书签字验证：①依据：每个人的签名动作和字迹具有明显的个性，手书签名可作为身份验证的可靠依据 ②发展：机器自动识别手书签字的研究

其它：指纹、语音、视网膜、虹膜、脸型

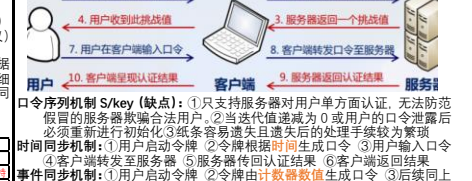
身份证明系统的设计：设备系统强度、用户可接受性、系统成本

15.4 一次性口令认证

攻击的主要方式：窃取口令文件和窃听网络连接，以获取用户 ID 和口令

攻击的主要技术：缓冲区溢出技术、木马技术、计算机病毒（宏病毒和网络蠕虫）、分布式拒绝服务攻击、Sniffer 报文截获等

挑战/响应机制：⑤输入挑战值到令⑥令牌由该挑战值生成口令



口令序列机制 S/key（缺点）：①只支持服务器对用户单方面认证，无法防范假冒的服务器欺骗合法用户。②当迭代值递减为 0 或用户的口令泄露后必须重新进行初始化③纸条容易遗失且遗失后的处理手续较为繁琐

时间同步机制：①用户启动令牌 ②令牌根据时间生成口令 ③用户输入口令 ④客户端转发至服务器 ⑤服务器传回认证结果 ⑥客户端返回结果

事件同步机制-1：用户启动令牌 ②令牌由计数器数值生成口令 ③后续同上

事件同步机制-重同步方法：设置窗口值

机制	通信量	复杂度	安全性	服务器计算量
挑战/响应	大	简单	差	大
S/key	大	简单	差	大
时间同步	小	复杂	好	小
事件同步	小	简单	好	中

Kerberos 认证系统

Kerberos 组成：AS 认证服务器、TGS 票据授权服务器。

15.5 基于证书的认证（更安全）

存在问题：滥用别人的证书 **解决办法：**双因子认证（证书+口令）

步骤：①生成、存储和发布数字证书 ②用户以用户名、数字证书发出登录请求 ③服务器随机生成挑战值 ④用户对随机挑战值签名 ⑤服务器验证签名并反馈认证结果

15.6 智能卡技术及其应用

认证工具：令牌、磁卡、智能卡(IC 卡)

磁卡与智能卡：①嵌有磁条的塑卡数据易于被转录。②智能卡将微处理器芯片嵌在塑卡上代替无源存储磁条，安全性有了很大提高

这玩意儿就离谱

NewBabyLasTer

2020 年 6 月 9 日