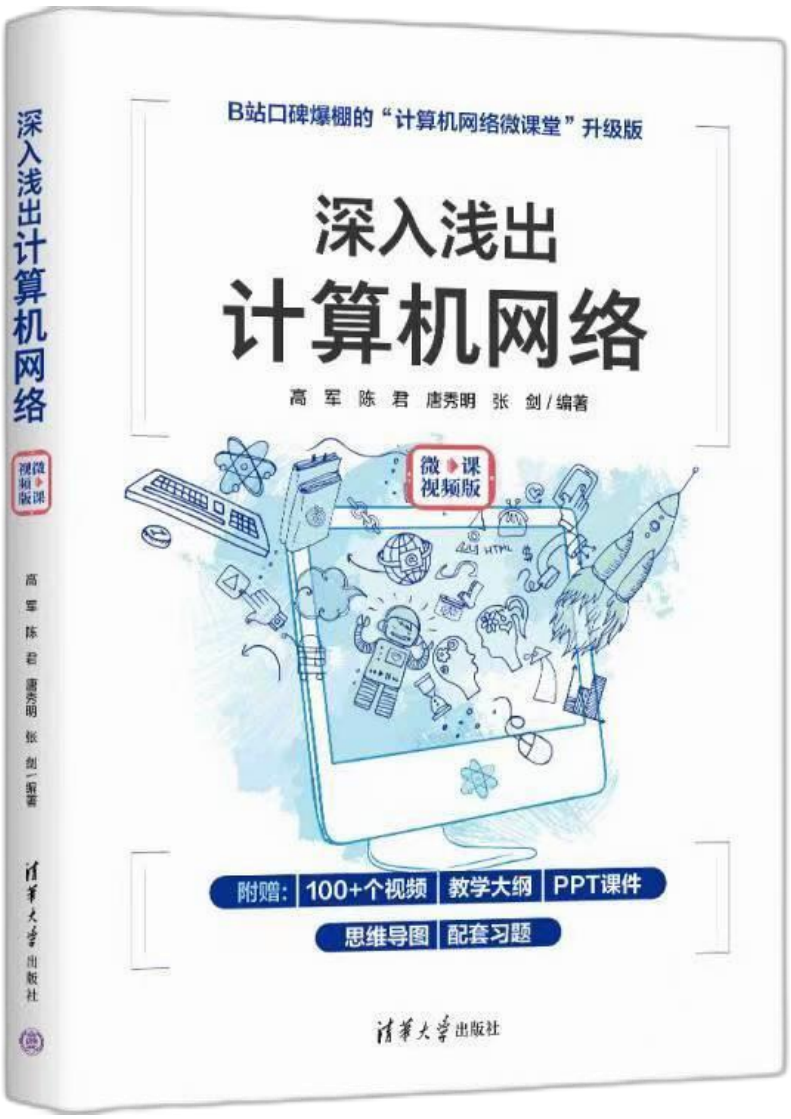

深入浅出计算机网络
微课视频版
高 军 陈 君 唐秀明 张 剑 编著
清华大学出版社
B站口碑爆棚的“计算机网络微课堂”升级版
深入浅出
计算机网络
高 军 陈 君 唐秀明 张 剑/编著
微课视频版
附赠：100+个视频 教学大纲 PPT课件
思维导图 配套习题
清华大学出版社

第 7 章 网络安全 习题答案及解析

7-1 以下网络攻击中，属于被动攻击的是（　）。

A. 攻击者通过监听截获网络中传输的信息

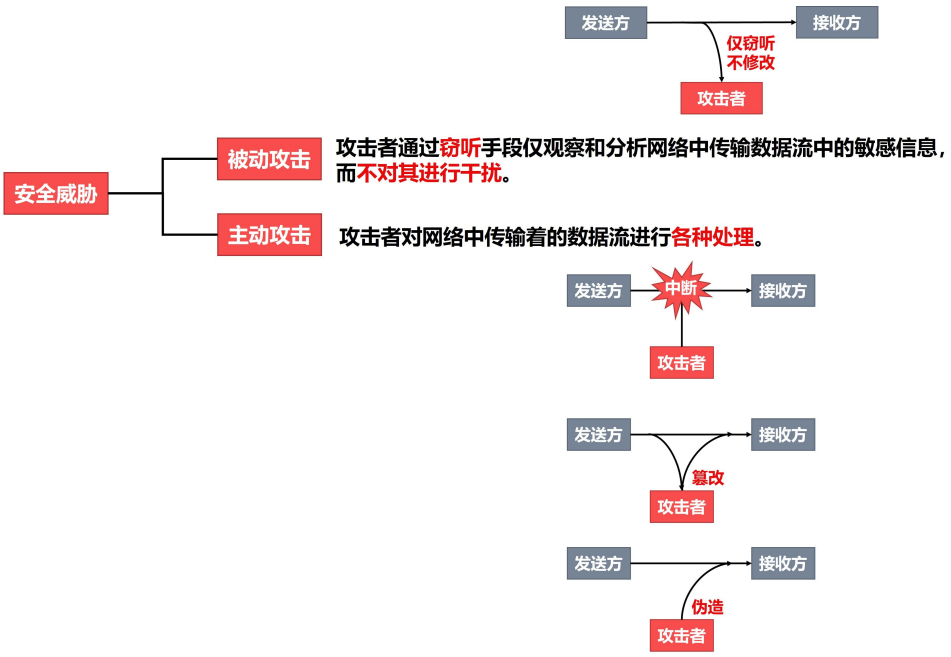
B. 攻击者故意中断他人的网络通信

C. 攻击者故意篡改网络中传送的 PDU

D. 攻击者伪造 PDU 在网络中传送

【答案】A

【解析】



7-2 以下有关密码学的基本概念中，错误的是（　）。

A. 加密和解密可以使用同一个密钥作为参数

B. 加密和解密的过程可以公开

C. 增加密钥长度可以增加破解密文的难度

D. 用于加密的密钥必须公开

【答案】D

【解析】

对于对称密钥密码体制，加密密钥与解密密钥是相同的，并且必须保密，不能公开。

7-3 以下有关对称密钥密码体制的基本概念中，正确的是（　）。

A. 加密密钥与解密密钥相同

B. 加密密钥可以公开

C. 解密密钥可以公开

D. DES 是对称密钥密码体制的典型代表，它被认为是非常安全的

【答案】A

【解析】

对于对称密钥密码体制，加密密钥与解密密钥是相同的，并且必须保密，不能公开。

现在对于 56 比特的 DES 密钥的搜索已成常态，56 比特 DES 已不再被认为是安全的。

7-4　以下有关公钥密码体制的基本概念中，错误的是（　）。

A. 加密密钥是公开的

B. 解密密钥需要保密

C. 加密密钥与解密密钥相同

D. RSA 算法是目前最著名的公钥密码算法

【答案】C

【解析】

■ **公钥密码体制使用不同的加密密钥和解密密钥，其概念是由Stanford大学的研究人员Diffie和Hellman于1976年提出的。**

☐ **加密密钥是向公众公开的，称为公钥（Public Key，PK）。**

☐ **解密密钥是需要保密的，称为私钥或密钥（Secret Key，SK）。**

请同学们注意：
尽管SK由PK决定，但却不能根据PK计算出SK。

☐ **加密算法E和解密算法D都是公开的。**

■ **公钥密码体制的加密/解密过程的一般表示式：** $D_{SK}(E_{PK}(X)) = X$　（X为明文）

■ **加密和解密运算可以对调：** $E_{PK}(D_{SK}(X)) = X$

■ **PK只能用来加密，而不能用来解密：** $D_{PK}(E_{PK}(X)) \neq X$

■ **公钥密码体制提出不久，研究人员就找到了三种公钥密码算法。1976年由美国三位科学家Rivest、Shamir和Adleman提出，并在1978年正式发表的RSA（Rivest、Shamir and Adleman）算法，就是目前最著名的公钥密码算法，它是基于数论中大数分解问题的算法。**

7-5　以下有关报文摘要和密码散列函数的相关描述中，错误的是（　）。

A. 只对长度固定且比整个报文长度短得多的报文摘要进行加密要比对整个报文进行加密简单得多

B. 密码散列函数是一种单向函数，可把密码散列函数运算看作是没有密钥的加密运算

C. MD5 输出 128 比特的摘要，根据给定的 MD5 报文摘要，想要找出一个与原报文具有相同报文摘要的另一个报文，其难度在计算上几乎是不可能的

D. SHA-1 输出 160 比特的报文摘要，其计算要比 MD5 慢一些

【答案】C

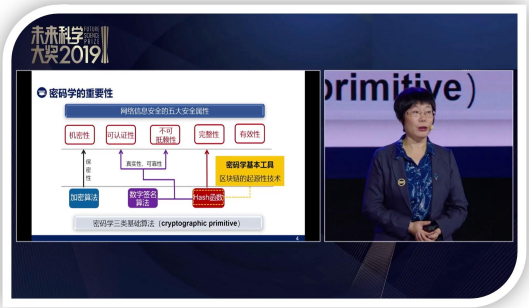
【解析】

■ **最有名的报文摘要算法（或称密码散列函数或散列算法）有MD5（Message Digest，MD-5）和安全散列算法1（Secure Hash Algorithm，SHA-1）。**

■ **MD5是Rivest于1991年提出并获得了广泛应用的报文摘要算法[RFC 1321]。**

☐ **MD5输出128比特的摘要。**

☐ **MD5希望达到的设计目标：根据给定的MD5报文摘要，想要找出一个与原报文具有相同报文摘要的另一个报文，其难度在计算上几乎是不可能的。**



2004年，我国学者王小云发表了轰动世界的密码学论文，证明了可以用系统的方法找出一对报文，这对报文具有相同的MD5报文摘要，而这仅需要15分钟至不到1小时的时间。这使得“密码散列函数的逆变换是不可能的”这一传统观念受到了颠覆性的动摇。

之后，又有许多学者开发了对MD5的实际攻击方法，这导致MD5最终被安全散列算法SHA-1所替代。

7-6　以下有关数字签名的相关描述中，错误的是（　）。

A. 采用公钥算法比采用对称密钥算法更容易实现数字签名

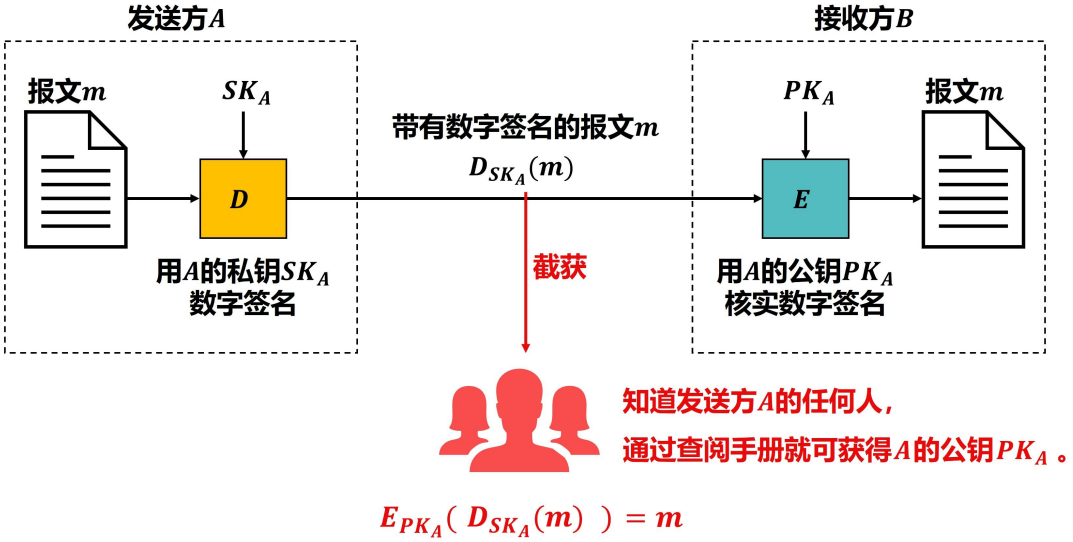
B. 使用数字签名的好处之一就是发送方事后不能抵赖对报文的数字签名

C. 对整个报文进行数字签名是一件非常耗时的事情，更有效的方法是仅对报文摘要进行数字签名

D. 对报文进行数字签名可以确保报文的保密性

【答案】D

【解析】



7-7　以下有关实体鉴别的相关描述中，错误的是（　）。

A. 实体鉴别就是通信双方的一方验证另一方身份的技术

B. 为了应对“重放攻击”，可以使用不重数（nonce）

C. 不能使用对称密钥密码体制来实现实体鉴别

D. 使用公钥密码体制实现实体鉴别时，仍有受到“中间人攻击”的可能

【答案】C

【解析】

实体鉴别的最简单方法就是使用用户名和口令。为了应对用户名和口令被攻击者截获的安全威胁，需要对用户名和口令进行加密。

7-8　以下有关密钥分发的相关描述中，错误的是（　）。

A. 对于对称密钥密码体制，目前常用的密钥分配方式是设立密钥分配中心 KDC

B. 密钥分配中心 KDC 分配给用户的主密钥应当定期更换以减少攻击者破译密钥的机会

C. 需要发布公钥的用户可以让认证中心 CA 为其公钥签发一个证书，证书中包含有公钥及其拥有者的身份标识信息（人名、公司名或 IP 地址等）。

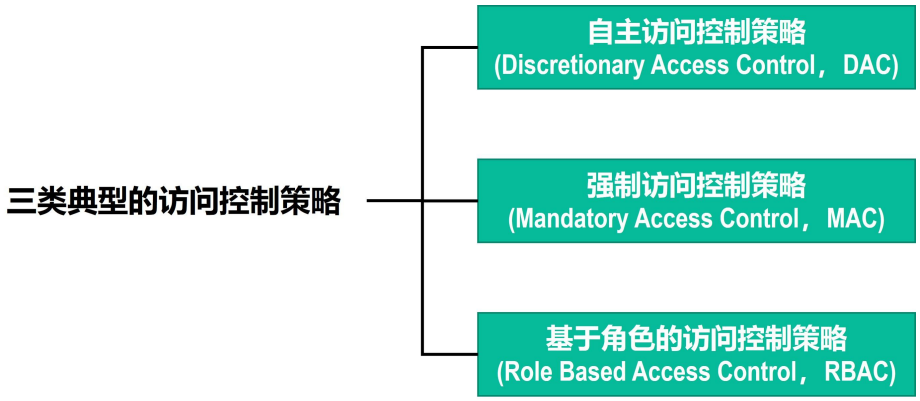
D. 只有网络安全管理员才能获取认证中心 CA 的公钥，并用这个公钥来验证某个证书的真伪。

【答案】D
【解析】
任何人都可从可信的地方（例如代表政府的报纸）获取 CA 自身的公钥，并用这个公钥来验证某个证书是否是该 CA 签发的真实证书。一旦证书被鉴别是真实的，则可以相信证书中的公钥确实属于证书中声称的用户。

7-9　以下不属于访问控制策略的是（　）。

A. 自主访问控制
B. 强制访问控制
C. 基于角色的访问控制
D. 随机访问控制

【答案】D
【解析】



7-10　以下属于物理层安全措施的是（　）。

A. SSL
B. TLS
C. 信道加密
D. IPsec

【答案】C
【解析】
物理层安全措施：信道加密
网际层安全措施：IPsec
运输层安全措施：SSL/TLS

7-11　以下属于数据链路层安全措施的是（　）。

A. 802.11i
B. PGP
C. SSL/TLS
D. IPsec

【答案】A
【解析】
数据链路层安全措施：802.11i
网际层安全措施：IPsec

运输层安全措施：SSL/TLS
应用层安全措施：例如应用于电子邮件的 PGP

7-12　以下有关 WEP 的描述中，错误的是（　）。

A. WEP 加密算法是 802.11 无线局域网的数据链路层可选的一种安全机制
B. WEP 具有密钥分发机制
C. WEP 采用的加密算法的强度较低，存在严重的安全隐患
D. WEP 加密算法既用于实体鉴别，也用于数据通信

【答案】B
【解析】

7-13　以下有关 IPsec 的描述中，正确的是（　）。

A. 在 IPsec 的隧道方式下，IPsec 只保护 IP 数据报的数据载荷，而不保护 IP 数据报的首部
B. 在 IPsec 的运输方式下，IPsec 保护包括 IP 数据报首部的整个 IP 数据报
C. 使用 ESP 或 AH 协议的 IP 数据报称为 IP 安全数据报或 IPsec 数据报
D. IPsec 是为因特网的网际层提供安全服务的一个独立的协议

【答案】C
【解析】
在 IPsec 的隧道方式下，IPsec 保护整个 IP 数据报。
在 IPsec 的运输方式下，IPsec 只保护 IP 数据报的数据载荷。
在 IPSec 协议族中有两个主要的协议：鉴别首部（Authentication Header，AH）协议和封装安全有效载荷（Encapsulation Security Payload，ESP）协议。

7-14　以下有关 SSL 的描述中，正确的是（　）。

A. SSL 属于数据链路层安全措施
B. SSL 只能用于端系统应用层中的 HTTP 和运输层中的 TCP 之间
C. SSL 提供三种安全服务：SSL 服务器鉴别，SSL 客户鉴别和加密的 SSL 会话
D. SSL 是在 TLS 基础上修改而来的

【答案】C
【解析】
SSL 属于运输层安全措施。
SSL/TLS 作用于 TCP/IP 体系结构的应用层与运输层之间，在应用层中使用 SSL/TLS 最多的协议是 HTTP。

1995 年，在 SSL 3.0 的基础上设计了 TLS 协议。

7-15　以下有关 PGP 的描述中，错误的是（　）。

A. PGP 是一个电子邮件安全软件包
B. PGP 使用对称密钥和公钥的组合进行加密为电子邮件提供保密性
C. PGP 通过报文摘要和数字签名技术为电子邮件提供完整性和不可否认性
D. PGP 是因特网的正式标准

【答案】D

【解析】

PGP（Pretty Good Privacy）是已被广泛应用的，为电子邮件提供加密、鉴别、电子签名和压缩等技术的电子邮件安全软件包，它是 Zimmermann 于 1995 年开发的。PGP 不是因特网的正式标准。

7-16　以下有关防火墙的描述中，错误的是（　）。

A. 实现防火墙技术的设备有分组过滤路由器和应用网关
B. 分组过滤路由器不能防止 IP 地址和端口号欺骗
C. 应用网关可以过滤应用层数据并进行高层用户的鉴别
D. 防火墙对恶意代码（病毒、木马等）具有很强的查杀能力

【答案】D

【解析】

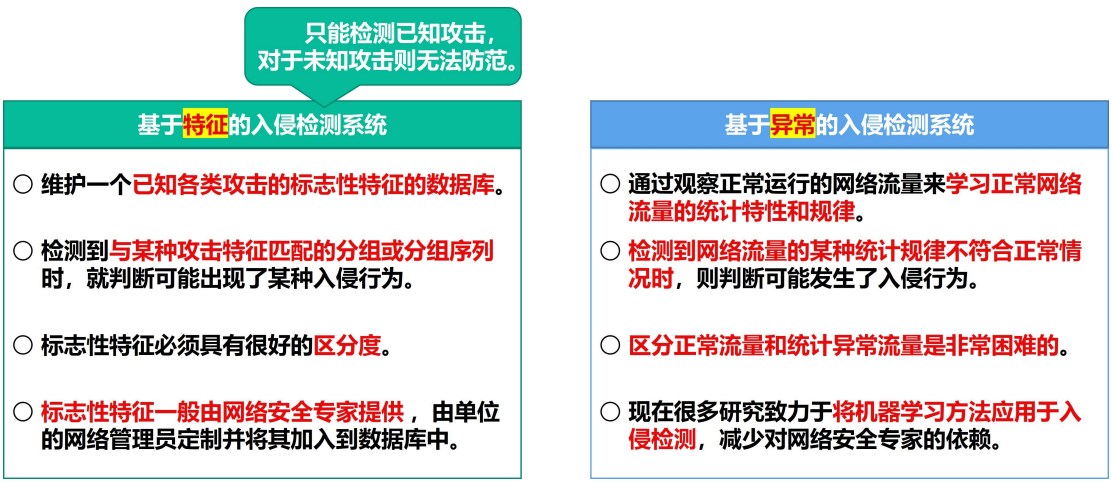
防火墙对恶意代码（病毒、木马等）的查杀能力非常有限，因此不能有效地防止恶意代码通过网络的传播。由于查杀恶意代码的计算开销非常大，若提高防火墙的查杀力度，则会降低防火墙的处理速度，进而降低用户的网络带宽。

7-17　以下有关 IDS 的描述中，错误的是（　）。

A. 防火墙并不能阻止所有的入侵行为，因此使用入侵检测系统 IDS 及时检测到入侵并尽快阻止入侵是非常有必要的
B. 入侵检测系统 IDS 一般分为基于特征的入侵检测和基于异常的入侵检测两种
C. 基于特征的入侵检测既可以检测已知攻击，也可以检测未知攻击
D. 基于异常的入侵检测通过观察正常运行的网络流量来学习正常网络流量的统计特性和规律。

【答案】C

【解析】



7-18　以下不属于网络扫描的是（　）。

A. 端口扫描
B. 主机发现
C. 病毒扫描
D. 漏洞扫描

【答案】C

【解析】

网络扫描主要有四种类型：主机发现、端口扫描、操作系统检测和漏洞扫描。

7-19　以下不属于网络监听的是（　）。

A. 分组嗅探器
B. 交换机毒化攻击
C. ARP 欺骗
D. Smurf 攻击

【答案】D

【解析】

常见的网络监听类型有：分组嗅探器、交换机毒化攻击和 ARP 欺骗。

Smurf 攻击属于拒绝服务攻击 DoS。

7-20　以下不属于 DoS 攻击的是（　）。

A. 交换机毒化攻击
B. “死亡之 ping”攻击
C. “TCP SYN 洪泛”攻击
D. 反射攻击

【答案】A

【解析】

交换机毒化攻击属于网络监听。

7-21　以下有关 DoS 攻击的描述中，错误的是（　）。

A. 常见的 DoS 攻击类型有：基于漏洞的 DoS 攻击、基于资源消耗的 DoS 攻击和分布式 DoS 攻击
B. 基于资源消耗的 DoS 攻击是 DoS 攻击中采用最多的一种攻击。攻击者通过向目标系统发送大量的分组，从而耗尽目标系统的资源，致使目标系统崩溃而无法向正常用户提供服务。
C. DDoS 攻击往往能产生巨大的流量来耗尽目标系统的网络带宽或导致目标系统资源耗尽而崩溃。
D. DoS 攻击是目前最容易实现和防范的攻击手段。

【答案】D

【解析】

DoS 攻击是目前最容易实现却又最难防范的攻击手段。