

目录

第 6 章 信息安全 1

6.1 内容提要1

6.2 加密技术与认证技术2

6.3 网络安全协议10

6.4 网络威胁12

6.5 安全控制技术19

6.6 系统安全分级23

第 6 章 信息安全



软件设计师考试
信息安全

www.educity.cn — 帮助客户成功，创造社会价值

6.1 内容提要



 课程内容提要

信息安全

1、加密技术和认证技术

2、分层网络安全协议

3、网络威胁

4、安全控制技术

5、系统安全分级

对称加密技术

非对称加密技术

加密技术应用

数字签名

信息摘要

数字证书

网络攻击

计算机病毒与木马

防火墙技术

入侵检测与防御

其他安全措施

www.educity.cn — 帮助客户成功，创造社会价值



考情分析

(希赛)

考试分值分布													平均
加密技术与认证技术	对称加密与非对称加密		1		1			1	1				0.4
	信息摘要与数字签名	1			2	2			1				0.6
	数字证书		2	2					1				0.5
网络安全协议			1	1		1	2	1			1		0.7
网络威胁	网络攻击		1			1	1					1	0.4
	计算机病毒与木马			1	1								0.2
安全控制技术	防火墙技术			1			1					1	0.3
	其他网络安全控制技术	1					1				1		0.3
系统安全分级									1				0.1
其它		1				1							0.2
信息安全 (合计)		3	5	5	4	5	5	3	3	2	2		3.7

www.educity.cn — 帮助客户成功, 创造社会价值

6.2 加密技术与认证技术



知识点分析

(希赛)

加密技术与认证技术

- 考点1: 对称加密与非对称加密技术
- 考点2: 数字签名与信息摘要应用
- 考点3: 数字证书应用

www.educity.cn — 帮助客户成功, 创造社会价值



知识点分析

(希赛)

加密技术与认证技术

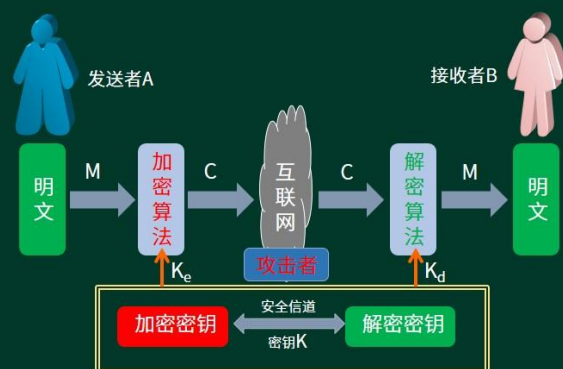
- 考点1: 对称加密与非对称加密技术

www.educity.cn — 帮助客户成功, 创造社会价值



对称加密技术

(希赛)



对称加密: $K_e = K_d$;

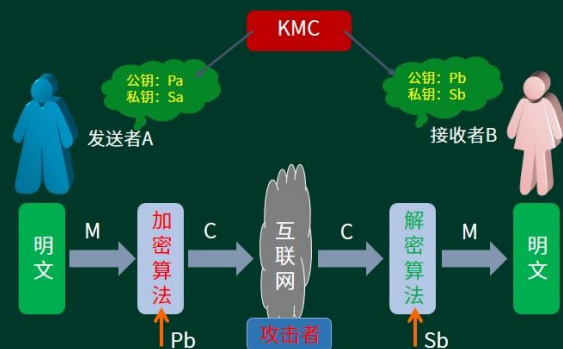
特点: 1、加密强度不高, 但效率高; 2、密钥分发困难。

常见对称密钥 (共享密钥) 加密算法: DES、3DES(三重DES)、RC-5、IDEA算法。

www.educity.cn — 帮助客户成功, 创造社会价值



非对称加密技术



非对称加密: $K_e \neq K_d$; 密钥必须成对使用 (公钥加密, 相应的私钥解密)。
特点: 加密速度慢, 但强度高。
常见非对称密钥 (公开密钥) 加密算法: RSA、ECC

www.educity.cn — 帮助客户成功, 创造社会价值



例题讲解

DES是 () 算法。

- A、公开密钥加密
- B、共享密钥加密
- C、数字签名
- D、认证

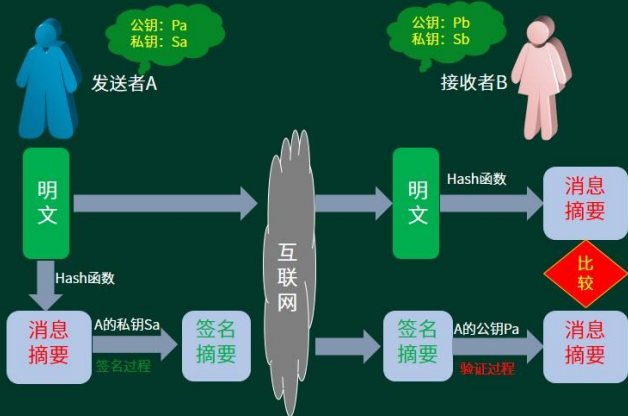
www.educity.cn — 帮助客户成功, 创造社会价值



加密技术与认证技术

➢ 考点2：数字签名与信息摘要应用

数字签名





消息摘要

数字摘要：由单向散列函数加密成固定长度的散列值。

消息摘要 希赛教育:IT在线教育 平台,让每个人随时随 地享受IT教育 产生信息摘要 %&^#@(*&@

常用的消息摘要算法有MD5, SHA等, 市场上广泛使用的MD5, SHA算法的散列值分别为128和160位, 由于SHA通常采用的密钥长度较长, 因此安全性高于MD5。

www.educity.cn — 帮助客户成功, 创造社会价值



例题讲解

可用于数字签名的算法是 ()。

- A、RSA B、IDEA C、RC4 D、MD5

www.educity.cn — 帮助客户成功, 创造社会价值



例题讲解

(希赛)

MD5是（ ）算法，对任意长度的输入计算得到的结果长度为（ ）位。

- A、路由选择 B、摘要 C、共享密钥 D、公开密钥
A、56 B、128 C、140 D、160

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解

(希赛)

在安全通信中，S将所发送的信息使用（ ）进行数字签名，T收到该消息后可利用（ ）验证该消息的真实性。

- A、S的公钥 B、S的私钥 C、T的公钥 D、T的私钥
A、S的公钥 B、S的私钥 C、T的公钥 D、T的私钥

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解

(希赛)

- () 不是数字签名的作用。
- A、接收者可验证消息来源的真实性
 - B、发送者无法否认发送过该消息
 - C、接收者无法伪造或篡改消息
 - D、可验证接收者合法性

www.educity.cn — 帮助客户成功，创造社会价值



知识点分析

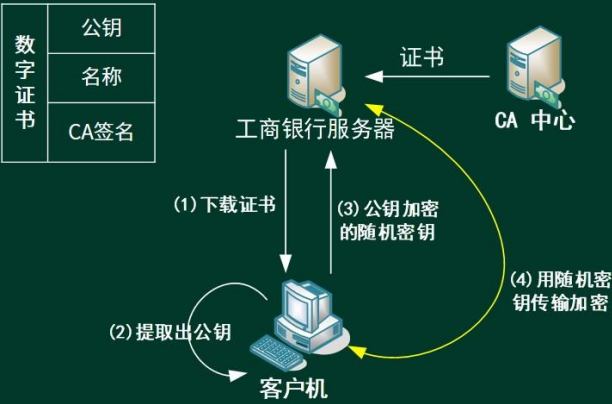
(希赛)

加密技术与认证技术

- 考点3：数字证书应用

www.educity.cn — 帮助客户成功，创造社会价值

PKI公钥体系



www.educity.cn — 帮助客户成功，创造社会价值

例题讲解

某电子商务网站向CA申请了数字证书，用户可以通过使用（ ）验证（ ）的真伪来确定该网站的合法性。

- A、CA的公钥
- B、CA的签名
- C、网站的公钥
- D、网站的私钥

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解

(希赛)

用户A和B要进行安全通信，通过程需确认双方身份和消息不可否认。
A和B通信时可使用（ ）来对用户的身份进行认证；使用（ ）确保消息不可否认。

- | | | | |
|--------|--------|--------|--------|
| A、数字证书 | B、消息加密 | C、用户私钥 | D、数字签名 |
| A、数字证书 | B、消息加密 | C、用户私钥 | D、数字签名 |

www.educity.cn — 帮助客户成功，创造社会价值

6.3 网络安全协议



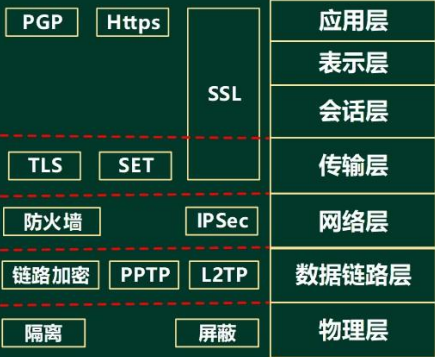
知识点分析

(希赛)

网络安全协议

www.educity.cn — 帮助客户成功，创造社会价值

网络安全 – 各个网络层次的安全保障



www.educity.cn — 帮助客户成功，创造社会价值

例题讲解

与HTTP相比，HTTPS协议对传输的内容进行加密，更加安全。
HTTPS基于（ ）安全协议，其默认端口是（ ）。

- | | | | |
|--------|-------|-------|--------|
| A RSA | B DES | C SSL | D SSH |
| A 1023 | B 443 | C 80 | D 8080 |

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解




下述协议中与安全电子邮箱服务无关的是（ ）。


- A、SSL
- B、HTTPS
- C、MIME
- D、PGP

www.educity.cn — 帮助客户成功，创造社会价值

6.4 网络威胁



知识点分析



网络安全威胁

- 考点1：主动攻击与被动攻击
- 考点2：计算机病毒与木马

www.educity.cn — 帮助客户成功，创造社会价值



知识点分析

(希赛)

网络安全威胁

➤ 考点1：主动攻击与被动攻击

www.educity.cn — 帮助客户成功，创造社会价值



信息安全基本要素

(希赛)

信息安全包括5个基本要素



机密性：确保信息不暴露给未授权的实体或进程。



完整性：只有得到允许的人才能修改数据，并且能够判断出数据是否已被篡改。



可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。



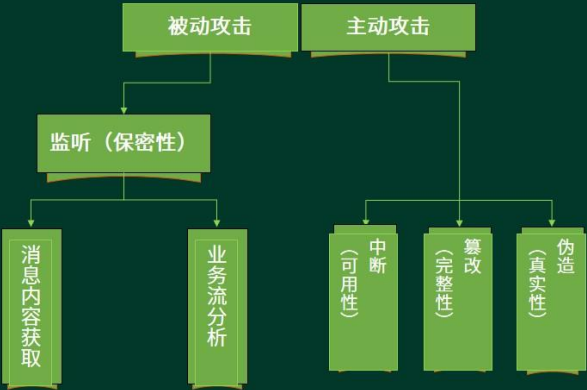
可控性：可以控制授权范围内的信息流向及行为方式。



可审查性：对出现的信息安全问题提供调查的依据和手段。

www.educity.cn — 帮助客户成功，创造社会价值

网络安全 – 主动攻击与被动攻击



www.educity.cn — 帮助客户成功，创造社会价值

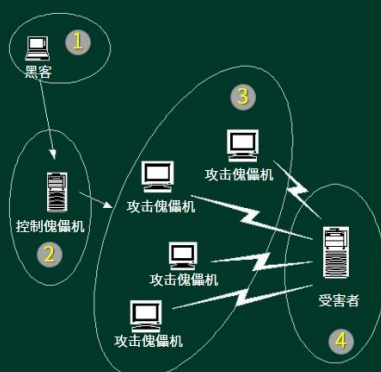
安全威胁

攻击类型	攻击名称	描述
被动攻击	窃听 (网络监听)	用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。
	业务流分析	通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从而发现有价值的信息和规律。
	非法登录	有些资料将这种方式归为被动攻击方式。
主动攻击	假冒身份	通过欺骗通信系统 (或用户) 达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。黑客大多是采用假冒进行攻击。
	抵赖	这是一种来自用户的攻击，比如：否认自己曾经发布过的某条消息、伪造一份对方来信等。
	旁路控制	攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。
	重放攻击	所截获的某次合法的通信数据拷贝，出于非法的目的而被重新发送。
	拒绝服务 (DOS)	对信息或其它资源的合法访问被无条件地阻止。

www.educity.cn — 帮助客户成功，创造社会价值



网络安全 – DoS（拒绝服务）与DDoS



分布式拒绝服务攻击体系结构

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解

下列攻击行为中，属于典型被动攻击的是（ ）。

- A、拒绝服务攻击
- B、会话拦截
- C、系统干涉
- D、修改数据命令

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解

(希赛)

攻击者通过发送一个目的主机已经接收过的报文来达到攻击目的，这种攻击方式属于（ ）攻击。

- A、重放
- B、拒绝服务
- C、数据截获
- D、数据流分析

www.educity.cn — 帮助客户成功，创造社会价值



知识点分析

(希赛)

网络安全威胁

- 考点2：计算机病毒与木马

www.educity.cn — 帮助客户成功，创造社会价值



计算机病毒与木马

病毒：编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

计算机病毒具有**隐蔽性**、**传染性**、**潜伏性**、**触发性**和**破坏性**等特点。

木马：计算机木马是一种后门程序，常被黑客用作控制远程计算机的工具。



计算机病毒与木马

类型	感染目标
引导型病毒	引导盘
文件型病毒	exe文件
宏病毒	doc、xls等office文件
网络型病毒	电子邮件
混合型	



计算机病毒与木马

- 系统病毒（前缀：Win32、PE、W32，如：KCOM——Win32.KCOM）
- 蠕虫病毒（如：恶鹰——Worm.BBeagle）
- 木马病毒、黑客病毒（如：QQ消息尾巴木马——Trojan.QQ3344）
- 脚本病毒（如：红色代码——Script.Redlof）
- 宏病毒（如：美丽莎——Macro.Melissa）
- 后门病毒（如：灰鸽子——Backdoor.Win32.Huigezi）
- 病毒种植程序病毒（冰河播种者——Dropper.BingHe2.2C）
- 破坏性程序病毒（杀手命令——Harm.Command.Killer）
- 玩笑病毒（如：女鬼——Jioke.Grl ghost）
- 捆绑机病毒（如：捆绑QQ——Binder.QQPass.QQBin）

www.educity.cn — 帮助客户成功，创造社会价值




例题讲解


计算机病毒的特征不包括（ ）。

- A、传染性 B、触发性 C、隐蔽性 D、自毁性

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解




震网（Stuxnet）病毒是一种破坏工业基础设施的恶意代码，利用系统漏洞攻击工业控制系统，是一种危害性极大的（ ）。


A、引导区病毒 B、宏病毒 C、木马病毒 D、蠕虫病毒

www.educity.cn — 帮助客户成功，创造社会价值

6.5 安全控制技术



知识点分析



安全控制策略

- 考点1：防火墙技术
- 考点2：其他安全控制策略

www.educity.cn — 帮助客户成功，创造社会价值



知识点分析

(希赛)

安全控制策略

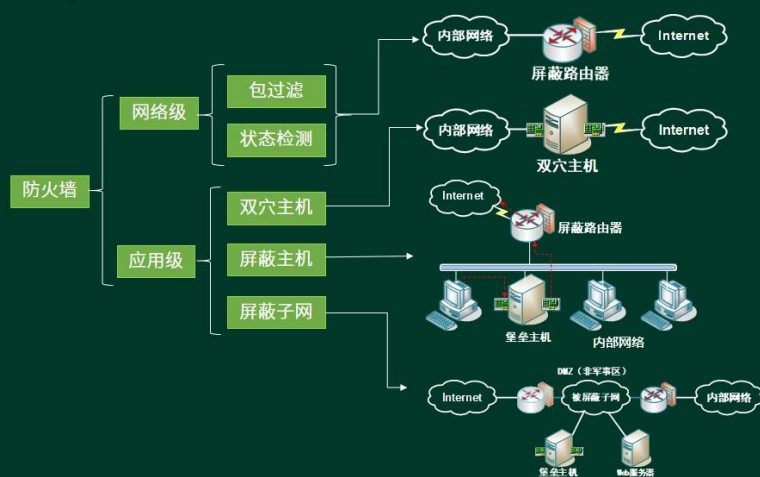
➤ 考点1: 防火墙技术

www.educity.cn — 帮助客户成功, 创造社会价值



网络安全 - 防火墙

(希赛)



www.educity.cn — 帮助客户成功, 创造社会价值



例题讲解

(希赛)

以下关于防火墙功能特性的叙述中，不正确的是（ ）。

- A、控制进出网络的数据包和数据流向
- B、提供流量信息的日志和审计
- C、隐藏内部IP以及网络结构细节
- D、提供漏洞扫描功能

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解

(希赛)

()防火墙是内部网和外部网的隔离点，它可对应用层的通信数据流进行监控和过滤。

- A、包过滤
- B、应用级网关
- C、数据库
- D、Web

www.educity.cn — 帮助客户成功，创造社会价值



知识点分析

(希赛)

安全控制策略

➤ 考点2：其他安全控制策略

www.educity.cn — 帮助客户成功，创造社会价值



网络安全控制技术

(希赛)

	说明
防火墙技术	包过滤防火墙、应用代理网关防火墙、状态监测防火墙。防外不防内。
加密技术	对称与非对称加密技术。
用户识别技术	用户识别和验证。核心是识别访问者是否属于系统的合法用户，目的是防止非法用户进入系统。
访问控制技术	控制不同用户对信息资源的访问权限。
网络反病毒技术	杀毒软件等防病毒产品。
网络安全漏洞扫描技术	漏洞监测和安全风险评估技术，可预知主体受攻击的可能性和具体地指证将要发生的行为和产生的后果。网络漏洞扫描技术主要包括网络模拟攻击、漏洞监测、报告服务进程、提取对象信息以及测评风险、提供安全建议和改进等功能，帮助用户控制可能发生的安全事件，最大可能地消除安全隐患。
入侵检测技术	通过对系统中用户行为或系统行为的可疑程度进行评估，并根据评估结果来鉴别系统中行为的正常性，从而帮助系统管理员进行安全管理或对系统所受到的攻击采取相应的对策。 评估（专家系统）过程：攻击者行为与模式库可疑行为记录进行模式匹配，如果匹配成功则报警。

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解

(希赛)

()不属于入侵检测技术。

A. 专家系统

B. 模型检测

C. 简单匹配

D. 漏洞扫描



```
graph TD; A[(模式库)] --> C[模式匹配]; B[攻击者] --> C; C --> D[ ];
```

www.educity.cn — 帮助客户成功，创造社会价值

6.6 系统安全分级



知识点分析

(希赛)

安全防范体系分级

www.educity.cn — 帮助客户成功，创造社会价值



安全防范体系

安全防范体系的层次划分：

- (1) **物理环境的安全性**。包括通信线路、物理设备和机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件和传输介质）、软硬件设备的安全性（替换设备、拆卸设备、增加设备）、设备的备份、防灾害能力、防干扰能力、设备的运行环境（温度、湿度、烟尘）和不间断电源保障等。
- (2) **操作系统的安全性**。主要表现在三个方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制和系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。
- (3) **网络的安全性**。网络层的安全问题主要体现在计算机网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等。
- (4) **应用的安全性**。由提供服务所采用的应用软件和数据的安全性产生，包括Web服务、电子邮件系统和DNS等。此外，还包括病毒对系统的威胁。
- (5) **管理的安全性**。包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大地影响着整个计算机网络的安全，严格的安全管理制度、明确的部门安全职责划分与合理的人员角色配置，都可以在很大程度上降低其他层次的安全漏洞。

www.educity.cn — 帮助客户成功，创造社会价值



例题讲解

在网络设计和实施过程中要采取多种安全措施，其中（ ）是针对系统安全需求的措施。

- | | |
|-------------|--------|
| A、设备防雷击 | B、入侵检测 |
| C、漏洞发现与补丁管理 | D、流量控制 |

www.educity.cn — 帮助客户成功，创造社会价值



www.educity.cn — 帮助客户成功，创造社会价值