作者：希赛教育软考学院　来源：希赛网　2014年05月21日

考点分析

第11章　安全性知识

安全性知识是软件设计师考试的一个必考点，每次考试的分数基本固定在3分左右。

信息安全有5个基本要素，分别为机密性、完整性、可用性、可控性和可审查性。机密性是指确保信息不暴露给未授权的实体或进程；完整性是指只有得到允许的人才能够修改数据，并能够判别数据是否已被篡改；可用性是指得到授权的实体在需要时可访问数据；可控性是指可以控制授权范围内的信息流向和行为方式；可审查性是指对出现的安全问题提供调查的依据和手段。

对于网络及网络交易而言，信息安全的基本需求是机密性、完整性和不可抵赖性。不可抵赖性是指数据发送、交易发送方无法否认曾经的事实。

11.1　考点分析

本节把历次考试中安全性知识的试题进行汇总，得出本章的考点，如表11-1所示。

表11-1 安全性知识试题知识点分布

考试时间	分数	考查知识点
10.11	3	抗抵赖性（1）、VPN（1）、防火墙（1）
11.05	3	防火墙（1）、密钥算法（2）
11.11	3	加密算法（2）、防火墙（1）
12.05	3	加密算法（2）、网络攻击（1）
12.11	3	安全技术（1）、冲击波（2）
13.05	3	网络攻击（1）、病毒（2）
13.11	3	数字证书（2）、VPN（1）
14.05	2	防火墙技术（1）、安全协议（1）

根据表11-1,我们可以得出安全性知识的考点主要有：

（1）密钥技术：主要考查各种加密算法。

（2）安全体系：包括防火墙、数字证书、病毒防范等。

（3）网络攻击：主要考查各种网络攻击的方法和特征。

（4）虚拟专用网（VPN）：主要考查VPN的基本概念和技术。

对这些知识点进行归类，然后按照重要程度进行排列，如表11-2所示。其中的五角星号（*）代表知识点的重要程度，星号越多，表示越重要。

表11-2 安全性知识各知识点重要程度

知识点	10.11	11.05	11.11	12.05	12.11	13.05	13.11	14.05	合计	比例	重要程度
密钥技术	1	2	2	2			2		9	39.13%	★★★★★
安全体系	1	1	1		3	2		2	10	43.48%	★★★★★
网络攻击				1		1			2	8.70%	★
VPN	1						1		2	8.70%	★

在本章的后续内容中，我们将对这些知识点进行逐个讲解。

密钥技术

11.2 密钥技术

本知识点重点在于了解加密体系的基本原理，掌握主要的对称加密、非对称加密、消息摘要等的主要算法和工作原理，了解Kerberos等与密钥管理相关的技术。

上一节　本书简介　下一节

数据加密技术

11.2.1 数据加密技术

数据加密就是对明文（未经加密的数据）按照某种加密算法（数据的变换算法）进行处理，从而形成难以理解的密文（经加密后的数据）。即使是密文被截获，截获方也无法或难以解码，从而防止泄露信息。

数据加密和数据解密是一对可逆的过程，数据加密是用加密算法E和加密密钥K1将明文P变换成密文C.数据解密是数据加密的逆过程，用解密算法D和解密密钥K2,将密文C转换在明文P.

1.数据传输加密

数据传输加密技术的目的是对传输中的数据流加密，以防止通信线路上的窃听、泄露、篡改和破坏。如果以加密实现的通信层次来区分，加密可以在通信的三个不同层次来实现，即链路加密（位于网络层以下的加密）、结点加密、端到端加密（传输前对文件加密，位于网络层以上的加密）。一般常用的是链路加密和端到端加密这两种方式。

链路加密侧重于在通信链路上而不考虑信源和信宿，是对保密信息通过各链路采用不同的加密密钥提供安全保护。链路加密是面向结点的，对于网络高层主体是透明的，它对高层的协议信息（地址、检错、帧头帧尾）都加密，因此数据在传输中是密文的，但在中央结点必须解密得到路由信息。

结点加密的加解密都在结点中进行，即每个结点里装有加解密保护装置，用于完成一个密钥向另一个密钥的转换。结点中虽然不会出现明文，但是需要在经过的每个结点上加装保护装置，这不仅不方便使用，而且会增加开支。

端到端加密则指信息由发送端自动加密，并进入TCP/IP数据包回封，然后作为不可阅读和不可识别的数据穿过互联网，当这些信息一旦到达目的地，将自动重组、解密，成为可读数据。端到端加密是面向网络高层主体的，它不对下层协议进行信息加密，协议信息以明文形式传输，用户数据在中央结点不需解密。

2.密钥体制

按照加密密钥K1和解密密钥K2的异同，有密钥体制以下两种：

（1）秘密密钥加密体制（K1=K2）：加密和解密采用相同的密钥，因而又称为对称密码体制。

因为其加密速度快，通常用来加密大批量的数据。典型的方法有DES、IDEA、MD5、RC-5等。

DES（数据加密标准）是国际标准化组织核准的一种加密算法，一般DES算法的密钥长度为56位。为了加速DES算法和RSA算法的执行过程，可以用硬件电路来实现加密和解密。针对DES密钥短的问题，科学家又研制了80位的密钥，以及在DES的基础上采用三重DES和双密钥加密的方法，即用两个56位的密钥K1、K2,发送方用K1加密，用K2解密，再使用K1加密。接收方则使用K1解密，使用K2加密，再使用K1解密，其效果相当于将密钥长度加倍。

IDEA（国际数据加密算法）算法是在DES算法的基础上发展起来的，类似于三重DES.发展IDEA也是因为感到DES具有密钥太短等缺点，IDEA的密钥为128位。

MD5（Message Digest ver5）是可产生一个128位的散列值的散列算法，可以用于生成数字摘要。采用单向HASH算法，将需要加密的明文进行摘要而产生的具有固定长度的单向散列值。其中，散列函数是将一个不同长度的报文转换成一个数字串（即报文摘要）的公式，该函数不需要密钥，公式决定了报文摘要的长度。报文摘要与非对称加密一起，提供数字签名的方法。目前，MD5算法已被破解。

RC-5也是对称密码，使用可变参数的分组迭代密码体制，它面向字结构，便于软件和硬件的快速实现，适用于不同字长的微处理器。RC-5加密效率高，适合于加密大量的数据。RC-5还引入了一种新的密码基本变换数据相依旋转（Data-Dependent Rotations）方法，即一个中间的字是另一个中间的低位所决定的循环移位结果，以提高密码强度，这也是RC-5的新颖之处。

（2）公开密钥加密体制（K1≠K2）：又称非对称密码体制，其加密和解密使用不同的密钥；其中一个密钥是公开的，另一个密钥保密的。典型的公开密钥是保密的。发送者利用不对称加密算法向接收者传送信息时，要用接收者的公钥加密。接收者收到信息后，用自己的私钥解密读出信息。由于加密速度较慢，所以往往用在少量数据的通信中。典型的公开密钥加密方法有RSA和ECC.

RSA（Rivest-Shamir-Adleman）算法密钥长度为512位，其保密性取决于数学上将一个大数分解为两个素数的问题的难度，根据已有的数学方法，其计算量极大，破解很难。但是加密/解密时要进行大指数模运算，因此加密/解密速度很慢，影响推广使用，它适合加密非常少量的数据，例如加密会话密钥，一般用在数字签名和密钥交换中。

ECC（Elliptic Curve Cryptography,椭圆曲线密码）也是非对称密码，加解密使用不同的密钥（公钥和私钥），它们对计算资源的消耗较大，适合加密非常少量的数据，例如加密会话密钥。它被美国国家安全局选为保护机密的美国政府资讯的下一代安全标准。这种密码体制的诱人之处在于在安全性相当的前提下，可使用较短的密钥。而且它是建立在一个不同于大整数分解及素域乘法群而广泛为人们所接受的离散对数问题的数学难题之上。

总而言之，对称密码加密的效率高，适合加密大量的数据；非对称密码速度很慢，适合加密非常少量的数据。

认证技术

11.2.2 认证技术

认证技术主要解决网络通信过程中通信双方的身份认可。认证的过程涉及加密和密钥交换。通常，加密可使用对称加密、非对称加密及两种加密方法混合的方法。认证方一般有账户名/口令认证、使用摘要算法认证、基于PKI的认证。

1.Hash函数和信息摘要

Hash函数又称为杂凑函数、散列函数，它提供了这样的一种计算过程：输入一个长度不固定的字符串，返回一串定长的字符串（又称为Hash值），单向Hash函数用于产生信息摘要。

信息摘要简要地描述了一份较长的信息或文件，它可以被看做是一份长文件的"数字指纹",信息摘要可以用于创建数字签名。对于特定的文件而言，信息摘要是唯一的。而且不同的文件必将产生不同的信息摘要。常见的信息摘要算法包括MD5（产生一个128位的输出，输入是以512位的分组进行处理的）和SHA（安全散列算法，也是按512位的分组进行处理，产生一个160位的输出），它们可以用来保护数据的完整性。

2.数字签名技术

数字签名是通过一个单向函数对要传送的报文进行处理，得到用以认证报文来源并核实报文是否发生变化的一个字母数字串。它与数据加密技术一起构建起了安全的商业加密体系：传统的数据加密是保护数据的最基本方法，它只能防止第三者获得真实的数据（即数据的机密性），而数字签名则可以解决否认、伪造、篡改和冒充的问题（即数据的完整性和不可抵赖性）。

数字签名可以使用对称加密技术实现，也可以使用非对称加密技术（公钥算法）实现。但如果使用对称加密技术实现，需要第三方认证，比较麻烦，因此现在通常使用的是公钥算法。

整个数字签名应用过程很简单：

（1）信息发送者使用一单向散列函数对信息生成信息摘要。

（2）信息发送者使用自己的私钥签名信息摘要。

（3）信息发送者把信息本身和已签名的信息摘要一起发送出去。

（4）信息接收者通过使用与信息发送者使用的同一个单向散列函数对接收的信息本身生成新的信息摘要，再使用信息发送者的公钥对信息摘要进行验证，以确认信息发送者的身份是否被修改过。

如果接收者收到的信息是P（用E代表公钥、D代表私钥），那么要保留的证据就应该是：E发送者（P），这也就证明了信息的确是"发送者"发出的。

上一节　本书简介　下一节

数字证书

11.2.3 数字证书

数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密和解密。每个用户将设定两个私钥（仅为本人所知的专用密钥，用来解密和签名）和公钥（由本人公开，用于加密和验证签名）两

个密钥，用以实现：

（1）发送文件：发送方使用接收方的公钥进行加密，接收方使用自己的私钥解密。

（2）接收方能够通过数字证书来确认发送方的身份，发送方无法抵赖。

（3）信息自数字签名后可以保证信息无法更改。

数字证书的格式一般使用X.509国际标准。X.509是广泛使用的证书格式之一，X.509用户公钥证书是由可信赖的证书权威机构（CA,证书授权中心）创建的，并且由CA或用户存放在X.500的目录中。任何一个用户只要得到CA中心的公钥，就可以得到该CA中心为该用户签署的公钥。因为证书是不可伪造的，因此对于存放证书的目录无须施加特别的保护。

因为用户数量多，因此会存在多个CA中心。但如果两个用户使用的是不同CA中心发放的证书，则无法直接使用证书；但如果两个证书发放机构之间已经安全地交换了公开密钥，则可以使用证书链来完成通信。

较通行的数字证书格式还有PGP.

Kerberos

11.2.4 Kerberos

在分布式网络应用环境中，要保证其使用的安全性，就必须让工作站能够用可信、安全的方式向服务器证实其身份，否则就会出现许多安全问题。而解决这个问题的技术称之为身份认证。比较常见的身份认证技术包括：用户双方指定共享密钥（最不安全）、使用智能卡生成密钥、使用Kerberos服务、使用PKI服务（即通过从CA中心获取数字证书的方式）。

Kerberos并非为每一个服务器构造一个身份认证协议，而是提供一个中心认证服务器，提供用户到服务器以及服务器到用户的认证服务。Kerberos的核心是使用DES加密技术，实现最基本的认证服务。Kerberos采用了连续加密的机制来防止会话被劫持。

Kerberos认证过程可以分为3个阶段，6个步骤：

第一阶段：认证服务交换、客户端获取授权服务器访问许可票据。

（1）用户A输入自己的用户名，以明文的方式发给认证服务器。

（2）认证服务器返加一个会话密钥KS和一个票据KTGS（A,KS），这个会话密钥是一次性的（也可以使用智能卡生成），而这两个数据包则是使用用户A的密钥加密的，返回时将要求其输入密码，并解密数据。

第二阶段：票据许可服务交换，客户端获得应用服务访问许可票据。

（3）用户A将获得的票据、要访问的应用服务器名B,以及用会话密钥加密的时间标记（用来防止重发攻击）发送给授权服务器（TGS）。

（4）授权服务器（TGS）收到后，返回A和B通信的会话密钥，包括用A的密钥加密的，和B的密钥加密的会话密钥KAB.

第三阶段：客户端与应用服务器认证交换，客户端最终获得应用服务。

（5）用户A将从TGS收到的用B的密钥加密的会话密钥发给服务器B,并且附上用双方的会话密钥KAB加密的时间标记以防止重发攻击。

（6）服务器B进行应答，完成认证过程。

安全体系

11.3 安全体系

在安全的开放环境中，用户可以使用各种安全应用。安全应用由一些安全服务来实现；而安全服务又是由各种安全机制或安全技术实现的，同一安全机制有时也可以用于实现不同的安全服务。

OSI（Open System Interconnection）安全体系方案X.800将安全服务定义为通信开放系统协议层提供的服务，用来保证系统或数据传输有足够的安全性。X.800定义了5类可选的安全服务，分别是认证（Authentication）、保密（Encryption）、数据完整性（Integrity）、不可否认（Non-repudiation）和访问控制（Access Control）。

（1）认证，包括实体认证与数据源认证。

（2）数据保密性，包括连接机密性、无连接机密性、选择域机密性与业务流机密性。

（3）数据完整性，包括恢复连接完整性、无恢复连接完整性、选择域连接完整性、无连接完整性与选择域无连接完整性。

（4）抗抵赖性，包括有源端证据的抗抵赖性与有交付证据的抗抵赖性。

（5）访问控制。

安全机制主要有：

（1）加密机制，存在加密机制意味着存在密钥管理机制。

（2）数字签名机制。

（3）访问控制机制。

（4）数据完整性机制。

（5）认证机制。

（6）通信业务填充机制。

（7）路由控制机制。

（8）公证机制。

在网络安全的防护方面，主要的技术手段包括防火墙、入侵检测、病毒扫描、安全扫描、日志审计、网页防篡改、私自拨号检测、PKI技术和服务等。下面我们就主要的几个技术手段进行进一步说明。

防火墙

11.3.1 防火墙

防火墙是一种综合性的技术，涉及计算机网络技术、密码技术、安全技术、软件技术、安全协议、网络标准化组织的安全规范，以及安全操作系统等方面。防火墙的主要目标是控制出入一个网络的权限，并迫使所有连接都经过这样的检查。

1.包过滤防火墙

包过滤防火墙也称为访问控制表或屏蔽路由器。它根据定义好的过滤规则审查每个数据包并根据是否与规则匹配来决定是否能够通过。

包过滤防火墙的优点是处理速度快、费用低（许多路由软件已包含）、对用户透明。缺点是维护比较困难，只能阻止少部分IP欺骗，不支持有效的用户认证，日志功能有限，过滤规则增加会大大降低吞吐量，无法对信息提供全面控制。

包过滤防火墙的适用场合主要有非集中化管理的机构，没有强大的集中安全策略的机构，网络的主机较少，主要依赖于主机安全来防止入侵，没有使用DHCP.

2.双穴主机

双穴主机也称为双宿网关防火墙，它是由一台至少装有两块网卡的堡垒主机作为防火墙，位于内外网络之间，分别与内外网络相离，实现物理上的隔开。它有两种服务方式：一种是用户直接登录到双宿主机上；另一种是在双宿主机上运行代理服务器。

双宿网关防火墙的优点是安全性比屏蔽路由器高，缺点是入侵者一旦得到双穴主机的访问权，内部网络就会被入侵，因此需具有强大的身份认证系统，才可以阻挡来自外部的不可信网络的非法入侵。

3.屏蔽主机防火墙

屏蔽主机防火墙强迫所有外部主机与一个堡垒主机相连接，而不让它们直接与内部主机相连接。它是由包过滤路由器和堡垒主机组成的。

屏蔽主机防火墙的优点是因为它实现了网络层安全（包过滤）和应用层安全（代理），因此安全等级比屏蔽路由器要高。缺点是堡垒主机可能被绕过，堡垒主机与其他内部主机间没有任何保护网络安全的东西存在，一旦被攻破，内网就将暴露。

4.屏蔽子网防火墙

屏蔽子网防火墙用了两个屏蔽路由器和一个堡垒主机，也称为"单DMZ防火墙结构".

屏蔽子网防火墙的拓扑结构如图11-1所示。外部路由器用于防范通常的外部功能，并管理外部网到DMZ的访问；内部路由器（阻塞路由器）则保护内部网不受DMZ和Internet的侵害，执行大部分的过滤工作。

屏蔽子网防火墙的优点是在定义了"非军事区（DMZ）"网络后，它支持网络层和应用层安全功能，这也是最安全的防火墙系统。

DMZ网络通常较小，处于Internet和内部网络之间，一般情况下，将其配置成使用Internet和内部网络系统对其访问会受限制的系统，例如：堡垒主机、信息服务器、Modem组以及其他公用服务器。

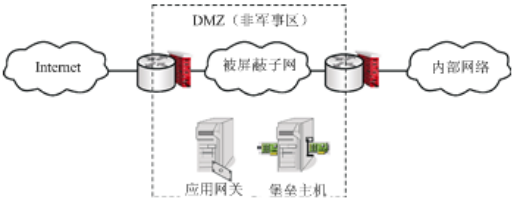

图11-1 屏蔽子网防火墙

5.其他结构防火墙

在实际应用中，经常在前四种基本结构的基础上进行组合。

（1）合并"非军事区"的外部路由器和堡垒主机结构（也是单DMZ结构）：由双穴堡垒主机执行原来外部路由器的功能，但会缺乏专用路由器的灵活性及性能，除了需注意保护堡垒主机外，与屏蔽子网防火墙结构相比没有明显弱点。如图11-2（a）所示。

（2）合并内部路由器和堡垒主机结构（也是单DMZ结构）：这种结构并不提倡，因为堡垒主机一旦被入侵，内部网络就没有安全保护。如图11-2（b）所示。

（3）合并DMZ的内部路由器和外部路由器结构：只有当拥有功能强大的路由器时，才考虑合并内、外路由器。这种结构与屏蔽主机结构一样，路由器容易受到损害。其结构如图11-2（c）所示。

（4）两个堡垒主机和两个非军事区结构：也就是使用双台双穴主机，设立两个非军事区，从而将网络分成：内网、外网、内DMZ、外DMZ四个部分。其结构如图11-3所示。通常将不是很机密的服务器放在内DMZ网络上，敏感的主机放在内部网络中。另外值得一提的是，在这种结构中，可以在外部DMZ放置一些公共信息服务主机（如FTP,WWW），而堡垒主机对这些主机不予信任，这类主机称为"牺牲主机".

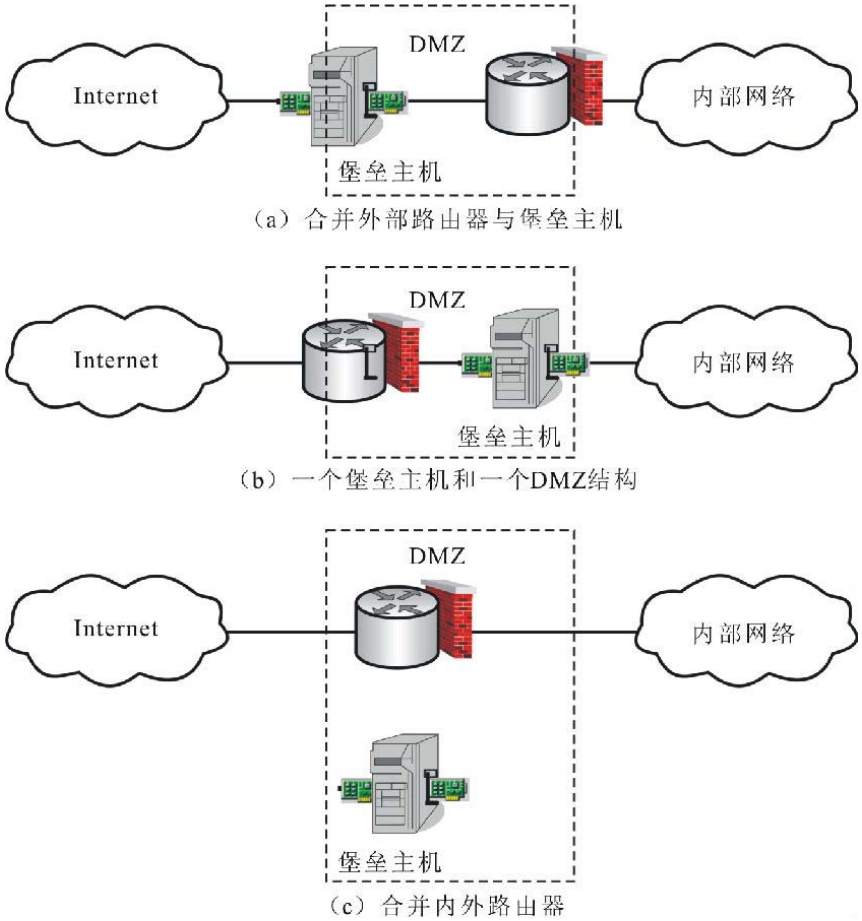

图11-2 单DMZ的三种变异

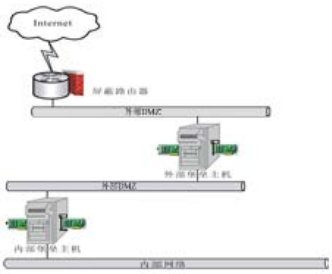

图11-3 双DMZ防火墙结构

由于防火墙主要用于限制保护的网络和互联网之间或与其他网络之间进行相互的信息存取、传递操作，它处于内部网络和外部网络之间，因此网络应用受到结构性限制，内部安全隐患仍然存在，效率较低，而故障率较高。这些问题导致了：

（1）不能防范外部的刻意的人为攻击。

（2）不能防范内部用户的攻击。

（3）不能防范内部用户因误操作而造成的口令失密受到的攻击。

（4）很难防止病毒或受病毒感染的文件的传输。

上一节　本书简介　下一节

入侵检测

11.3.2 入侵检测

入侵检测是指监视或在可能的情况下阻止入侵者试图控制自己的系统或网络资源的那种努力。它是用于检测任何损害或企图损害系统的机密性、完整性或可用性的行为的一种网络安全技术。它通过监视受保护系统的状态和活动，采用异常检测或误用检测的方式，发现非授权的或恶意的系统及网络行为，为防范入侵行为提供有效的手段。

入侵检测系统要解决的最基本的两个问题是如何充分并可靠地提取描述行为特征的数据，以及如何根据特征数据，高效并准确地判断行为的性质。由系统的构成来说，通常包括数据源（原始数据）、分析引擎（通过异常检测或误用检测进行分析）、响应（对分析结果采用必要和适当的措施）三个模块。

入侵检测系统所采用的技术可分为特征检测与异常检测两种。

（1）特征检测。假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。它可以将已有的入侵方法检查出来，但对新的入侵方法无能为力。其难点在于如何设计模式既能够表达"入侵"现象又不会将正常的活动包含进来。

（2）异常检测。假设入侵者活动异常于正常主体的活动。根据这一理念建立主体正常活动的"活动简档",将当前主体的活动状况与"活动简档"相比较，当违反其统计规律时，认为该活动可能是"入侵"行为。异常检测的难题在于如何建立"活动简档"以及如何设计统计算法，从而不把正常的操作作为"入侵"或忽略真正的"入侵"行为。

入侵检测系统常用的检测方法有特征检测、统计检测与专家系统。据公安部计算机信息系统安

全产品质量监督检验中心的报告，国内送检的入侵检测产品中95%是属于使用入侵模板进行模式匹配的特征检测产品，其他5%是采用概率统计的方法统计检测产品与基于日志的专家知识库检测产品的。

（1）特征检测。对已知的攻击或入侵的方式作出确定性的描述，形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时，即报警。原理上与专家系统相仿。其检测方法上与计算机病毒的检测方式类似。目前基于对包特征描述的模式匹配应用较为广泛。 该方法预报检测的准确率较高，但对于无经验知识的入侵与攻击行为无能为力。

（2）统计检测。统计模型常用异常检测，在统计模型中常用的测量参数包括：审计事件的数量、间隔时间、资源消耗情况等。常用的入侵检测5种统计模型为操作模型、方差、多元模型、马尔柯夫过程模型和时间序列分析。统计方法的最大优点是它可以"学习"用户的使用习惯，从而具有较高检出率与可用性。但是它的"学习"能力也给入侵者以机会通过逐步"训练"使入侵事件符合正常操作的统计规律，从而透过入侵检测系统。

（3）专家系统。用专家系统对入侵进行检测，经常针对有特征的入侵行为。所谓的规则，即知识，不同的系统与设置具有不同的规则，且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性，知识库的完备性又取决于审计记录的完备性与实时性。入侵的特征抽取与表达，是入侵检测专家系统的关键。运用专家系统防范有特征入侵行为的有效性完全取决于专家系统知识库的完备性。

病毒和木马扫描

11.3.3 病毒和木马扫描

病毒是指一段可执行的程序代码，通过对其他程序进行修改来感染这些程序，使其含有该病毒的一个复制，并且可以在特定的条件下进行破坏。因此在其整个生命周期中包括潜伏、繁殖（也就是复制、感染阶段）、触发和执行4个阶段。

对于病毒的防护而言，最彻底的方法是不允许其进入系统，但这是很困难的，因此大多数情况下，采用"检测-标识-清除"的策略来应对。在病毒防护的发展史上，共经历了以下几个阶段。

（1）简单扫描程序：需要病毒的签名来识别病毒。

（2）启发式扫描程序：不依赖专门的签名，而使用启发式规则来搜索可能被病毒感染的程序。还包括诸如完整性检查等手段。

（3）行为陷阱：即用一些存储器驻留程序，通过病毒的动作来识别病毒。

（4）全方位保护：联合以上反病毒技术组织的软件包，包括扫描和行为陷阱。

特洛伊木马（Trojans）是指一个正常的文件被修改成包含非法程序的文件。特洛伊木马通常包含具有管理权限的指令，它们可以隐藏自己的行踪（没有普通的窗口等提示信息），而在后台运行，并将重要的账号、密码等信息发回给黑客，以便进一步攻击系统。

木马程序一般由两部分组成，分别是Server（服务）端程序和Client（客户）端程序。其中

Server 端程序安装在被控制计算机上，Client端程序安装在控制计算机上，Server端程序和Client端程序建立起连接就可以实现对远程计算机的控制了。

首先，服务器端程序获得本地计算机的最高操作权限，当本地计算机连入网络后，客户端程序可以与服务器端程序直接建立起连接，并可以向服务器端程序发送各种基本的操作请求，并由服务器端程序完成这些请求，也就实现了对本地计算机的控制。

因为木马发挥作用必须要求服务器端程序和客户端程序同时存在，所以必须要求本地机器感染服务器端程序，服务器端程序是可执行程序，可以直接传播，也可以隐含在其他的可执行程序中传播，但木马本身不具备繁殖性和自动感染的功能。

反病毒技术的最新发展方向是类属解密和数字免疫系统。与入侵检测技术一样，现在的反病毒技术只能够对已有病毒、已有病毒的部分变种有良好的防护作用，而对于新型病毒还没有有效的解决方式，需要升级特征库。另外，它只是对病毒、黑客程序、间谍软件这些恶意代码有防护作用，其他网络安全问题不属于其关注的领域。

上一节　本书简介　下一节

安全扫描

11.3.4 安全扫描

安全扫描是指对计算机系统及网络端口进行安全性检查，它通常需要借助一个被称为"扫描器"的软件。扫描器并不是一个直接攻击网络漏洞的程序，它仅仅能够帮助管理员发现目标机的某些内在弱点，一个好的扫描器能够对得到的数据进行分析，帮助管理员查找目标主机的漏洞。它能够自动查找主机或网络，找到运行的服务及其相关属性，并发现这些服务潜在的漏洞。

因此从上面的描述中，我们可以发现安全扫描技术是一个帮助管理员找到网络隐患的工具，并不能直接解决安全问题，而且对未被业界发现的隐患也无法完全找到。

上一节　本书简介　下一节

日志审计系统

11.3.5 日志审计系统

日志文件是包含关于系统消息的文件，这些消息通常来自于操作系统内核、运行的服务，以及在系统上运行的应用程序。日志文件包括系统日志、安全日志、应用日志等。现在的Windows和UNIX（包括Linux）系统都提供了较完善的日志系统。

日志审计系统则通过一些特定的、预先定义的规则来发现日志中潜在的问题，它可以用来事后

亡羊补牢，也可以用来对网络安全攻击进行取证。显然它是一种被动式、事后的防护或事中跟踪的手段，很难在事前发挥作用。

　作者：希赛教育软考学院　来源：希赛网　2014年05月21日

公共密钥基础设施

11.3.6 公共密钥基础设施

公共密钥基础设施（Public Key Infrastructure,PKI）是CA安全认证体系的基础，是一种网络安全技术和安全规范，为安全认证体系进行密钥管理提供了一个平台。它能够为所有网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理。PKI由认证中心、证书库、密钥备份及恢复系统、证书作废处理系统和客户端证书处理系统这5大系统组成。

PKI可以实现CA和证书的管理，密钥的备份与恢复，证书、密钥对的自动更换，交叉认证，加密密钥和签名密钥的分隔，支持对数字签名的不可抵赖性，密钥历史的管理等功能。PKI技术的应用可以在认证、机密性、完整性和抗抵赖性方面发挥重要的作用。

PKI技术主要借助数字签名技术实现以上方面的功能，数字签名是维护网络信息安全的一种重要方法和手段，在身份认证、数据完整性、抗抵赖性方面都有重要应用，特别是在大型网络安全通信中的密钥分配、认证和电子商务、电子政务系统中有重要作用。而且，它通过密码技术对电子文档进行电子形式的签名，是实现认证的重要工具。数字签名是只有信息发送方才能够进行的签名，是任何他人无法伪造的一段数字串，这段特殊的数字串同时也是对相应的文件和信息真实性的一个证明。

采用数字签名能够确认以下两点：一是信息是由签名者发送的；二是信息自签发到接收为止，没做任何修改。数字签名的特点是它代表了文件的特征。如果文件发生变化，数字签名的值也会发生变化，不同的文件会得到不同的数字签名。数字签名是通过Hash函数与公开密钥算法来实现的，其原理是：

（1）发送者首先将原文用Hash函数生成128位的数字摘要。

（2）发送者用自己的私钥对摘要进行加密形成数字签名，并且把加密后的数字签名附加在要发送的原文后面。

（3）发送者将原文和数字签名同时传送给对方。

（4）接收者把接收到的信息用Hash函数生成新的摘要，同时用发送者的公开密钥对信息摘要进行解密。

（5）将解密后的摘要与新的摘要对比，两者一致则说明传送过程中信息没有被破坏或篡改。

如果第三方冒充发送方发送了一个文件，由于接收方在对数字签名进行解密时使用的是发送方的公开密钥，因此只要第三方不知道发送方的私用密钥，解密后的数字摘要与计算机计算的新摘要必然是不同的。这就提供了一个安全的确认发送方身份的方法。

数字签名有两种：一种是对整体信息的签名，它是指经过密码变换的被签名信息整体；另一种是对压缩信息的签名，它是附加在被签名信息后或某一特定位置上的一段签名图样。若按照明文和

密文的对应关系划分，每一种又可以分为两个子类：一类是确定性数字签名，即明文与密文一一对应，它对一个特定信息的签名不变化，如RSA签名；另一类是随机化或概率化数字签名，它对同一信息的签名是随机变化的，取决于签名算法中的随机参数的取值。一个明文可能有多个合法数字签名。

一个签名体制一般包含两个组成部分：签名算法和验证算法。签名算法（也称签名密钥）是秘密的，只有签名人掌握。而验证算法是公开的，便于他人进行验证。

另外，如果要基于PKI实现数据的保密性，可以用对方的公钥对"原文+数字签名"所构成的信息包进行加密，这样就可以保证对方只能使用自己的私钥进行解密，从而达到保密性要求。

数字信封是PKI的一个实际应用，是用加密技术来保证只有规定的特定收信人才能阅读通信的内容的。数字信封中采用了对称密码体制和公钥密码体制。信息发送者首先利用随机产生的对称密码加密信息，再利用接收方的公钥加密对称密码，被公钥加密后的对称密码被称之为数字信封。在传递信息时，信息接收方若要解密信息，必须先用自己的私钥解密数字信封，得到对称密码，才能利用对称密码解密所得到的信息。这样就保证了数据传输的真实性和完整性。数字信封主要包括数字信封打包和数字信封拆解，数字信封打包是使用对方的公钥将加密密钥进行加密的过程，只有对方的私钥才能将加密后的数据（通信密钥）还原；数字信封拆解是使用私钥将加密过的数据解密的过程。

网络攻击

11.4 网络攻击

常见的网络安全威胁包括：窃听（即非授权访问、信息泄露、资源盗取等）、假冒（假扮另一个实体，如网站假冒、IP欺骗等）、重放、流量分析、破坏完整性、拒绝服务、资源的非法授权使用、陷门和特洛伊木马、病毒、诽谤等。

网络攻击的类型

11.4.1 网络攻击的类型

OSI安全体系方案X.800将安全性攻击分为两类，即被动攻击和主动攻击。

1.被动攻击

被动攻击是对信息的保密性进行攻击，即通过窃听网络上传输的信息并加以分析从而获得有价

值的情报，但它并不修改信息的内容。它的目标是获得正在传送的信息，其特点是偷听或监视信息的传递。被动攻击只对信息进行监听，不对其进行修改。被动攻击包括信息内容泄露和业务流分析两大类，具体有：

（1）窃听。信息在通信过程中因被监视窃听而泄露。

（2）电磁/射频截获。信息从电子或机电设备所发出的无线电磁波中被提取出来。

（3）业务流分析。通过观察通信业务流模式，使非授权实体（人或系统）获得信息等。

2.主动攻击

主动攻击是攻击信息来源的真实性、信息传输的完整性和系统服务的可用性的体现，有意对信息进行修改、插入和删除。主动攻击包括篡改数据流或伪造数据流，这种攻击试图改变系统资源或影响系统运行。它主要包括：

（1）截获/修改。某一通信数据在传输过程中被改变、插入和替代。

（2）重放。把所截获的某次合法通信数据进行复制，出于非法目的重新发送。

（3）伪装。某个实体假装成另一个实体，并获取该实体的权限。

（4）非法使用。某一资源被某个非授权实体或以某一非授权方式使用。

（5）服务拒绝。攻击者通过对系统进行非法和根本无法成功的访问尝试而产生过量的负荷，使合法用户的访问被无条件地被阻止。

（6）特洛伊木马。含有一个觉察不出或无害程序段的软件，当它被运行时，能损害系统的安全。

（7）陷门。在某个系统或其部件中设置"机关",使在提供特定的输入数据时发生违反安全策略的操作等。

上一节　本书简介　下一节

常见的网络攻击

11.4.2 常见的网络攻击

常见的网络攻击有对加密算法的攻击、网络监听、拒绝服务攻击、远程攻击、系统攻击等。

1.对加密算法的攻击

对加密算法的攻击主要集中于破译某段密文或分析加密密钥。通常破译者可对密码进行惟密文攻击、已知明文攻击、选择密文攻击和选择明文攻击及穷举攻击，对特定算法还有特定攻击方法，如对DES这类迭代分组密码可选择差分密码分析法、能量攻击法，对公钥算法RSA可采用公用模攻击、低加密指数攻击、定时攻击等方法。

2.网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理信道上传输的所有信息，而不管信息的发送方和接收方是谁。所以进行通信的信息必须进行加密，否则只要使用一些网络监听工具就可以截获包括口令和账号在内的信息资料。大部分的传输介质如Ethernet、FDDI、Token-ring、模拟电话线、无线接入网上都可实施网络监听，其中尤以Ethernet

与无线接入网最为容易，因为这两者都是典型的广播型网络。

3.拒绝服务攻击

一般来说，拒绝服务攻击（DoS）有些是用来消耗带宽的，有些是消耗网络设备的CPU和内存的。例如对UDP的攻击，原理就是使用大量的伪造的报文攻击网络端口，造成服务器的资源耗尽，使系统停止响应甚至崩溃。也可以使用大量的IP地址向网络发出大量真实的连接，来抢占带宽，造成网络服务的终止。

拒绝服务一般分两种：一是试图破坏资源，使目标无人可以使用此资源。如破坏或摧毁信息：删除文件、格式化磁盘、切断电源等。二是过载一些系统服务或者消耗一些资源，通过这样的方式可以造成其它用户不能使用这个服务。这两种情况大半是因用户错误或程序错误造成的，并非针对性的攻击。针对网络的拒绝服务攻击主要包括服务过载攻击、消息流攻击、Paste式攻击、SYN Flooding攻击、邮件炸弹攻击。

分布式拒绝服务（DDoS）攻击通过探测扫描大量主机，从而找到可以入侵的目标主机，通过一些远程溢出漏洞攻击程序，入侵有安全漏洞的目标主机并获取系统的控制权，在被入侵的主机上安装并运行DDoS分布式的攻击守护进程，然后利用多台已被攻击者控制的机器对另一台单机进行扫描和攻击，在大小悬殊的带宽之比下被攻击的主机很快失去反应能力。整个过程都是自动化的，攻击者可以在几秒钟内入侵一台主机并安装攻击工具，这样，在一个小时之内就可以入侵数千台主机。

4.远程攻击

远程攻击指在目标主机上没有账户的攻击者获得该机器的当地访问权限，从机器中过滤出数据、修改数据等的攻击方式。远程攻击的一般过程如下：

（1）收集被攻击方的有关信息，分析被攻击方可能存在的漏洞。

（2）建立模拟环境，进行模拟攻击，测试对方可能的反应。

（3）利用适当的工具进行扫描。

（4）实施攻击。

IP Spooting是一种典型的远程攻击，它通过向主机发送IP包来实现攻击，主要目的是掩盖攻击者的真实身份，使攻击者看起来像正常的用户或者嫁祸于其他用户。IP Spooting攻击利用了RPC服务器仅仅依赖于信源IP地址进行安全校验的特性，攻击最困难的地方在于预测A的ISN.

5.系统攻击

系统攻击指一台机器上的本地用户获取UNIX高级用户权限或Windows NT管理员权限的攻击方法。缓冲区溢出是典型系统攻击。它通过向程序的缓冲区写超出其长度的内容，造成缓冲区溢出，从而破坏程序的堆栈，使程序转去执行其它的指令，如果这些指令是放在有Root权限的内存里，那么，一旦这些指令得到了运行，入侵者就以Root的权限控制了系统。造成缓冲区溢出的原因大多是程序没有仔细检查用户输入的参数。缓冲区溢出攻击占所有系统攻击的80%以上。

入侵者要达到目的通常要完成两个任务：一是在程序的地址空间里安排适当的代码；二是通过适当地初始化寄存器和存储器，让程序跳转到安排好的地址空间执行。可以根据这两个任务对缓冲区溢出攻击进行分类：

（1）在程序的地址空间里安排适当的代码的方法。

（2）将控制程序转移到攻击代码的方法。

（3）植入综合代码和流程控制技术。

通常可以采用下列方法防止缓冲区溢出：

（1）正确地编写代码。

（2）设定非执行的缓冲区。

（3）检查数组边界，使之不溢出。

（4）检查程序指针的完整性。

另外，对于网络安全而言，大都是针对网络安全漏洞，进行网络攻击。其中安全漏洞包括物理安全隐患、软件安全漏洞、搭配的安全漏洞；网络攻击可分为被动攻击、主动攻击、物理临近攻击、内部人员攻击、分发攻击等。

上一节　本书简介　下一节

虚拟专用网

11.5 虚拟专用网

虚拟专用网（Virtual Private Network,VPN）提供了一种通过公用网络安全地对企业内部专用网络进行远程访问的连接方式。与普通网络连接一样，VPN也由客户机、传输介质和服务器三部分组成，不同的是VPN连接使用隧道作为传输通道，这个隧道是建立在公共网络或专用网络基础之上的，如Internet或Intranet.

VPN可以实现不同网络的组件和资源之间的相互连接，利用Internet或其他公共互联网络的基础设施为用户创建隧道，并提供与专用网络一样的安全和功能保障。VPN允许远程通信方、销售人员或企业分支机构使用Internet等公共互联网络的路由基础设施以安全的方式与位于企业局域网端的企业服务器建立连接。VPN对用户端透明，用户好像使用一条专用线路在客户计算机和企业服务器之间建立点对点连接，进行数据的传输。

VPN技术同样支持企业通过Internet等公共互联网络与分支机构或其他公司建立连接，进行安全的通信。这种跨越Internet建立的VPN连接在逻辑上等同于两地之间使用广域网建立的连接。

上一节　本书简介　下一节

VPN的基本要求

11.5.1 VPN的基本要求

一般来说，企业在选用一种远程网络互联方案时都希望能够对访问企业资源和信息的要求加以控制，所选用的方案应当既能够实现授权用户与企业局域网资源的自由连接，不同分支机构之间的资源共享，又能够确保企业数据在公共互联网络或企业内部网络上传输时安全性不受破坏。因此，最低限度，一个成功的VPN方案应当能够满足以下所有方面的要求。

（1）用户验证。VPN方案必须能够验证用户身份并严格控制只有授权用户才能访问VPN.另外，方案还必须能够提供审计和计费功能，显示何人在何时访问了何种信息。

（2）地址管理。VPN方案必须能够为用户分配专用网络上的地址并确保地址的安全性。

（3）数据加密。对通过公共互联网络传递的数据必须经过加密，确保网络的其他未授权的用户

VPN的基本要求

（5）多协议支持。VPN方案必须支持公共互联网络上普遍使用的基本协议，包括IP,IPX等。

上一节　本书简介　下一节

隧道技术

11.5.2 隧道技术

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据（或负载）可以是不同协议的数据帧或包。隧道协议将这些其他协议的数据包重新封装在新的包头中发送。新的包头提供了路由信息，从而使封装的负载数据能够通过互联网络传递。

被封装的数据包在隧道的两个端点之间通过公共互联网络进行路由。被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。一旦到达网络终点，数据将被解包并转发到最终目的地。隧道技术是指包括数据封装、传输和解包在内的全过程。

隧道所使用的传输网络可以是任何类型的公共互联网络，下面主要以Internet为例进行说明。此外，在企业网络同样可以创建隧道。在经过一段时间的发展和完善之后，目前较为成熟的隧道技术主要有以下两种。

（1）IP网络上的SNA隧道技术。当系统网络结构（System Network Architecture,SNA）的数据流通过企业IP网络传送时，SNA数据帧将被封装在UDP和IP协议包头中。

（2）IP网络上的Novell NetWare IPX隧道技术。当一个IPX数据包被发送到NetWare服务器或IPX路由器时，服务器或路由器用UDP和IP包头封装IPX数据包后通过IP网络发送。另一端的IP-TO-IPX路由器在去除UDP和IP包头之后，把数据包转发到IPX目的地。

为创建隧道，隧道的客户机和服务器双方必须使用相同的隧道协议。

隧道技术可以分别以第2层或第3层隧道协议为基础。第2层隧道协议对应OSI模型中的数据链路层，使用帧作为数据交换单位。PPTP,L2TP和L2F（第2层转发）都属于第2层隧道协议，都是将数据封装在PPP帧中通过互联网发送。第3层隧道协议对应OSI模型中的网络层，使用包作为数据交换单位。IPoverIP及IPSec隧道模式都属于第3层隧道协议，都是将IP包封装在附加的IP包头中通过IP网络传送。

IPSec是第3层的协议标准，支持IP网络上数据的安全传输。除了对IP数据流的加密机制进行了规定之外，IPSec还制定了IPoverIP隧道模式的数据包格式，一般被称做IPSec隧道模式。一个IPSec隧道由一个隧道客户和隧道服务器组成，两端都配置使用IPSec隧道技术，采用协商加密机制。

为实现在专用或公共IP网络上的安全传输，IPSec隧道模式使用安全的方式封装和加密整个IP

包，然后对加密的负载再次封装在明文IP包头内通过网络发送到隧道服务器端。隧道服务器对接收到的数据包进行处理，在去除明文IP包头，对内容进行解密之后，获得最初的负载IP包。负载IP包在经过正常处理之后被路由到位于目标网络的目的地。

隧道可以分为自愿隧道和强制隧道两种类型。

1.自愿隧道

客户端计算机可以通过发送VPN请求配置和创建一条自愿隧道（Voluntary Tunnel）。此时，用户端计算机作为隧道客户方成为隧道的一个端点。目前，自愿隧道是最普遍使用的隧道类型。

当一台工作站或路由器使用隧道客户软件创建到目标隧道服务器的虚拟连接时建立自愿隧道。为实现这一目的，客户端计算机必须安装适当的隧道协议。自愿隧道需要有一条IP连接（通过局域网或拨号线路）。使用拨号方式时，客户端必须在建立隧道之前创建与公共互联网络的拨号连接。一个最典型的例子是Internet拨号用户必须在创建Internet隧道之前拨通本地ISP取得与Internet的连接。

对企业内部网络来说，客户机已经具有同企业网络的连接，由企业网络为封装负载数据提供到目标隧道服务器的路由。

2.强制隧道

由支持VPN的拨号接入服务器配置和创建一条强制隧道（Compulsory Tunnel）。此时，用户端的计算机不作为隧道端点，而是由位于客户计算机和隧道服务器之间的远程接入服务器作为隧道客户端，成为隧道的一个端点。

目前，一些商家提供能够代替拨号客户创建隧道的拨号接入服务器。这些能够为客户端计算机提供隧道的计算机或网络设备包括支持PPTP协议的前端处理器（FEP），支持L2TP协议的L2TP接入集线器（LAC）或支持IPSEC的安全IP网关。

上一节　本书简介　下一节

作者：希赛教育软考学院　来源：希赛网　2014年05月21日

考点分析

第12章　标准化知识

在标准化知识方面，软件设计师考试一般考1分左右，主要考查标准化法的相关规定。

12.1　考点分析

本节把历次考试中标准化知识方面的试题进行汇总，得出本章的考点，如表12-1所示。

表12-1 标准化试题知识点分布

考试时间	分数	考查知识点
10.11	2	GB 8567-88（1）、构件标准（1）
11.05	1	行业标准（1）
11.11	1	标准的周期（1）
12.05	1	标准的分类（1）
12.11	1	标准化法（1）
13.05	1	标准的代号（1）
13.11	0	
14.05	0	