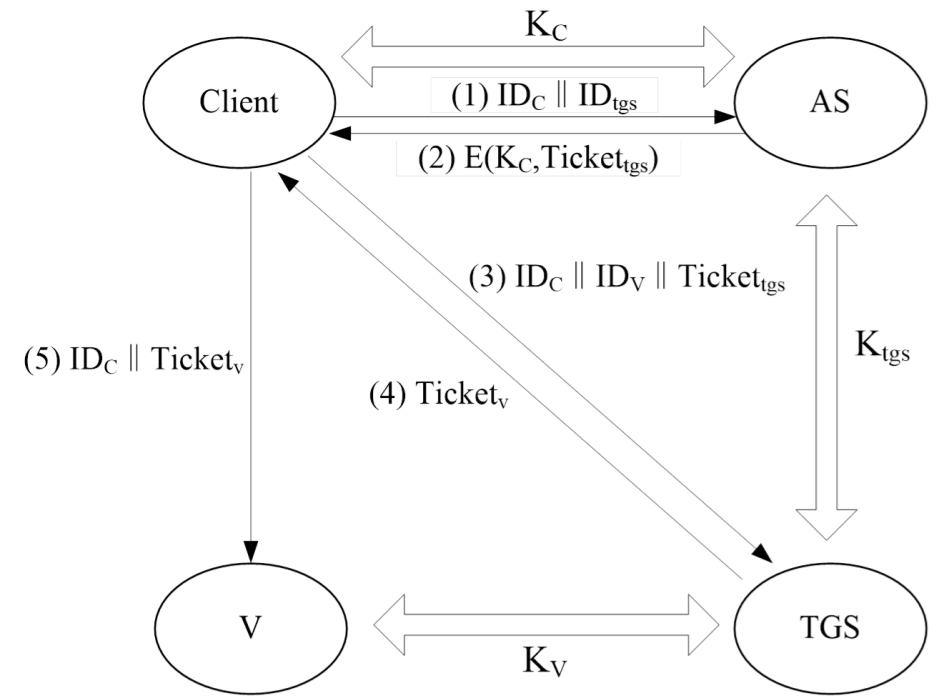
**44．在一个更安全的Kerberos鉴别对话中，除了客户C之外，系统中还有哪些主体（对象）？几者之间是如何共享哪些密钥的？试用一个简单的图形说明Kerberos系统中的这几个主体之间的关系（如如何共享密钥的）。再用带序号的箭头说明Kerberos的五步鉴别过程是如何实现的（只需要说明实现顺序，而不需要写出具体发送的消息内容）。**

****

**45．在一个更安全的Kerberos对话中，鉴别服务器AS是如何认证用户C的，使得既间接使用用户的口令进行认证，又不需要在网上直接传输用户的明文口令或口令散列？**

答：AS发回一张加密过的票据，加密密钥是由用户的口令导出的。当响应抵达客户端时，客户端提示用户输入口今，由此产生密钥，并试图对收到的报文解密。若口令正确，票据就能正确恢复。

因为只有合法的用户才能恢复该票据，这样，我们使用口令获得Kerberos的信任而无需传递明文口令。

**46．有哪三种主要的访问控制策略？TCSEC中的C级操作系统要求至少具有何种访问控制策略？B级以上操作系统要求具有何种访问控制策略？**

答：三种不同的访问控制策略：自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC）。

TCSEC中的C级操作系统要求至少具有自主访问控制DAC。

B级以上操作系统要求具有强制访问控制（MAC）。

**47．什么是MAC？它有阻止特洛伊木马的能力吗？MAC是通过“梯度安全标签”实现信息的单向还是双向流通来达到上述目的的？**

答：MAC是系统强制主体服从访问控制政策。它能阻止特洛伊木马。

是通过“梯度安全标签”实现信息的单向流通来达到上述的目的。

**48．MAC中有两个主要的访问控制模型：实现数据机密性的是哪个安全模型？它必须采用哪种读写规则？从而保证信息流只能以何种方向流动？实现数据完整性的是哪个安全模型？它必须采用哪种读写规则？MAC有哪些缺点？**

**机密性：Bell-Lapadula模型。下读/上写规则。信息流只能从低级别流向高级别。**

**完整性：Biba模型。上读/下写规则。**

**MAC缺点是实现工作量太大，管理不便，不够灵活，且过于偏重保密性。（1分）**

**49．在PKI技术中，如何使用CA确认某个人的真正公钥？（说明什么是数字证书以及如何通过颁发和验证数字证书以确认某个人真正公钥的整个过程）PKI中CA颁发的数字证书必须遵循什么标准？**

“数字证书”，它包含用户身份的部分信息及用户所持有的公开密钥。数字证书是一个经证书认证中心(CA)数字签名的包含公开密钥拥有者信息以及公开密钥的文件。

例如用户B要想和用户A使用公开密钥机制进行加密通信，首先他们必须到CA处申请了证书，在相互通信之前，必须到证书库获得对方的证书。这些证书都是由某个CA的私钥签名的，签名的内容包括这是谁的证书的标识和他的真正公钥。而该CA的公钥是众所周知的，A和B实现也有CA的公钥（假冒CA的公钥非常难）。B（A）用CA的公钥就能解密对方的数字证书，得到对方真正的公钥，就能在下面的通信中给真正的对方发送机密的数据。

PKI中CA颁发的数字证书必须遵循X.509 V3标准

**50．目前有哪四种常用的信任模型？在这些信任模型中哪些通过建立信任树进行认证？哪些通过建信任网进行认证？**

过建立信任网进行认证？信任树和信任网的最根本区别是什么？

1. 认证机构的严格层次结构模型 （信任树）

2. 分布式信任结构模型 （信任树）

3. Web模型 （信任树）

4. 以用户为中心的信任模型 （信任网）

**51．在使用PKI时，用户在CA处生成自己的公钥时有哪两种具体的方式？有什么主要区别？**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 产生方法 | 分发方法 | 优点 | 缺点 | 对应证书类型 | 适用  场合 |
| 用户自己生成 | 将自己公钥以安全方式传送给CA | CA也不知道用户私钥 | 密钥对安全强度可能不高 | 由浏览器产生的普通证书和测试证书 | 不适合比较重要的网络交易 |
| CA 替用户生成 | 将用户私钥以安全方式传送给用户 | 密钥对安全强度比较高 | CA必须销毁自己保存的用户私钥 | 商家证书和服务器证书 | 重要的应用场合 |

**52．为什么在实际使用PKI技术时，每个用户需要生成两个公钥/私钥对？这两对密钥各有什么功能？举例说明在管理这些密钥（如其中的两个私钥）有什么主要区别？**

因为公钥有两大用途：验证数字签名和加密信息所以相应的要求有两个密钥对。

签名密钥对用于数字签名/验证，加密密钥对用于加密/解密。

·签名密钥对的私钥不允许做备分和存档，丢失后重新生成，验证公钥匙需存档

·加密密钥对的私钥需要备份和存档，加密公钥无需备份，丢失后重新生成

**54．AH协议为IP数据包提供哪几种安全服务？简单说明它们分别是如何实现的？**

·无连接的数据完整性验证，通过哈希函数（如MD5）产生的校验来保证

·数据源身份认证，通过在计算验证码时加入一个共享密钥来实现

·防重放攻击，AH报头中的序列号可以防止重放攻击

**55．ESP协议为IP数据包提供哪几种安全服务？简单说明它们分别是如何实现的？**

ESP为IP数据包提供AH已有的3种服务外还提供数据包加密和数据流加密。

**56．IKE协议的作用是什么？它与AH和ESP协议有什么关系？**

IKE负责密钥管理，定义了通信实体间进行身份认证、协商加密算法以及生成共享的会话密钥的方法。IKE将密钥协商的结果保留在安全联盟(SA)中，供AH和ESP以后通信时使用。

1、在PGP中，发送方执行签名、加密、压缩操作的顺序是什么？为什么要按这样的顺序进行？

答：对未压缩的邮件正文进行散列计算后，再对散列值进行签名。然后将邮件正文和签名拼接后进行压缩后加密。

在压缩之前进行签名的主要原因有两点：一是对没压缩的消息进行签名，可便于对签名的验证，如果在压缩后再签名，则需要保存压缩后的消息或在验证时重新压缩消息，增加了处理的工作量；二是由于压缩算法ZIP在不同的实现中会在运算速度和压缩率之间寻求平衡，因而可能会产生不同的压缩结果（当然，直接解压结果是相同的），因此压缩后再进行签名就可能导致无法实现鉴别（接收方在验证签名时可能会因压缩的原因而出现验证失败）。

PGP对加密前的明文（含签名）进行压缩，而不是在加密后再压缩的主要原因也有两点：一方面因为先压缩再加密方案缩短了报文大小，从而减少了网络传输时间和存储空间；另一方面经过压缩实际上是经过了一次变换，变换后减少了明文中上下文的关系，比原始消息的冗余信息更少，再加密的安全性更高，而如果先加密，再压缩，效果会差一些。

2、在密钥信任方面，X.509和PGP有什么不同？

答：PGP主要采用以用户为中心的信任模型，也就是信任网模型（Web of Trust）。该模型中，没有一个统一的认证中心来管理用户公钥，每个人都可以作为一个CA对某个用户的公钥签名，以此来说明这个公钥是否有效（可信）。而X.509是基于一个统一的认证中心（CA）来建立密钥的信任关系。

3、PGP为什么要对加密后的报文进行Base64编码？并分析编码对传输性能的影响。

答：加密后的报文使用Base64编码将报文转换成ASCII字符串，主要考虑到很多文件系统只允许使用ASCII字符组成的报文，所以需要对密文进行Base64编码。在实际应用中，使用Base64编码转换后将导致消息大小增加33%（每3个字节的二进制数据映射成4个ASCIII字符）。由于加密前对消息进行了压缩，因此实际的性能下降幅度要小很多。

4、PGP是如何交换会话密码的？这种交换密钥方式与前面学过哪种协议类似？

答：

PGP系统中发送方产生会话密钥，并用接收方的公钥加密会话密钥，与密文拼接后一起发送给接收方；接收方用自己的私钥解密加密的会话密钥，获得会话密钥。与前面学到的SSL/TLS所采用的方法一样。

1、网络防火墙有哪几种常见体系结构？安全性最高的是哪种？

答：主要有三种：双宿/多宿主机模式、屏蔽主机模式、屏蔽子网模式，其中屏蔽子网模式的安全性最高。

2、从采用的技术来分，网络防火墙主要有哪几种类型？

答：包过滤防火墙、状态检测防火墙、应用网关防火墙、代理服务器、下一代防火墙。

3、随着云计算的广泛应用，企业网络的边界越来越模糊，对传统网络防火墙有什么影响？

答：网络防火墙是一种被动的安全防护技术，它假设在内部网络和外部网络之间存在明确边界，防火墙部署在网络边界位置进行防护，适合于保护相对独立、与外部网络互联途径有限的网络。随着企业越来越多地使用云上的计算资源和存储资源，传统企业网络的边界越来越模糊，其网络一部分结点和资源在企业内网，一部分结点和资源在外网的云上，给传统网络防火墙的部署和安全控制带来了很多困难，从而难以发挥有效的边界防护作用。

第14章作业参考解答

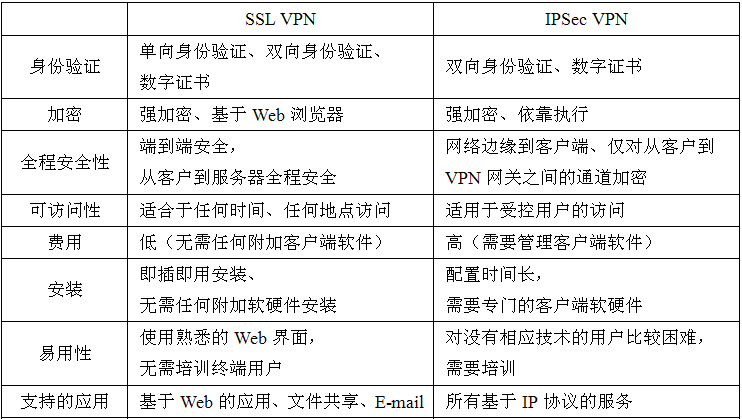
3. 什么是VPN的隧道（封装技术）？

答：VPN的隧道是指VPN节点间或VPN节点与用户节点间构建的传输数据的虚拟连接，一般通过隧道协议（如SSL/TLS、IPSec、GRE、SSH等）来构建。在传输用户数据包之前，首先通过加密和鉴别以确保隧道两端之间的传输安全，然后将数据包进行封装，通过隧道在公网上进行安全传输，离开隧道后进行解封装。

6. SSL VPN和IPSec VPN主要有哪些不同（可从应用范围、功能和成本等方面作比较）？哪些情况下适合使用SSL VPN？SSL VPN如何 与IPSec VPN结合作用？

答：

SSL VPN与IPSec VPN的不同之处如下表所示：



下列场景比较适合使用SSL VPN：企业需要通过Web远程接入互联网；客户端与目标服务器之间有防火墙或需要进行网络地址转换，允许 HTTPS数据包通过，但不允许IKE或IPSec包通过；企业无法在远程计算机上安装软件以提供远程访问；需要细粒度访问控制能力的场合。

一般建议以IPSec VPN作为一般远程接入方案和点对点连接方案，辅以SSL VPN作为访问Web服务器的远程接入方案，这样既安全又节省成本。

第15章作业参考解答

1、有了防火墙，为什么还需要入侵检测？

答：

主要是因为网络防火墙技术有一些不足之处，包括：第一，入侵者可寻找防火墙背后可能敞开的后门；第二，不能阻止内部攻击；第三，通常不能提供实时的入侵检测能力；第四，不能主动跟踪入侵者；第五，不能对病毒进行有效防护。所以需要入侵检测系统作为防火墙的有效补充，共同构建网络安全保障体系，这种补充主要表现在以下几个方面：

1）入侵检测可以发现内部的攻击事件以及合法用户的越权访问行为，而位于网络边界的防火墙对于这些类型的攻击活动无能为力。

2）如果防火墙开放的网络服务存在安全漏洞，入侵检测系统可以在网络攻击发生时及时发现并进行告警。

3）在防火墙配置不完善的条件下，攻击者可能利用配置漏洞穿越防火墙，入侵检测系统能够发现此类攻击行为。

4）对于加密的网络通信，防火墙无法检测，但是监视主机活动的入侵检测系统能够发现入侵。

5）入侵检测系统能够有效发现入侵企图。如果防火墙允许外网访问某台主机，当攻击者利用扫描工具对主机实施扫描时，防火墙会直接放行，但是入侵检测系统能够识别此类网络异常并进行告警。

6）入侵检测系统可以提供丰富的审计信息，详细记录网络攻击过程，帮助管理员发现网络中的脆弱点。

2、与入侵检测相比，网络欺骗防御技术有什么优势？

答：与传统入侵检测相比，网络欺骗防御检测入侵的主动性更强，采用欺骗技术来迷惑、引诱攻击者进行攻击，同时对攻击者的行为进行严密的监视和控制，因而更能准确地检测一些未知攻击、高水平攻击，并了解攻击的细节，部分解决了传统入侵检测系统的误报和漏报问题，同时还具有防御攻击的能力。

3、比较分析特征检测与异常检测方法的优缺点。

答：特征检测方法的基本思路是事先提取出描述各类攻击活动的特征信息，利用攻击特征对指定的数据内容进行监视，一旦发现攻击特征在监视的数据中出现，即判定系统内发生了相应的攻击活动。

异常检测方法首先总结出正常活动的特征，建立相应的行为模式。在入侵检测的过程中，以正常的行为模式为基础进行判定，将当前活动与代表正常的行为模式进行比较，如果当前活动与正常行为模式匹配，则认为活动正常；而如果两者存在显著偏差，则判定出现了攻击。

特征检测方法只能检测已知攻击，误报率低，无法检测未知攻击，而异常检测方法可以检测未知攻击，但误报率高。

第17章作业参考解答

1、简要分析计算机病毒、木马、蠕虫的区别。

答：

|  |  |  |  |
| --- | --- | --- | --- |
| 比较项目 | 病毒 | 蠕虫 | 木马 |
| 存在形式 | 代码片段 | 独立个体 | 独立个体 |
| 复制机制 | 插入宿主程序 | 自身的复制 | 自身的复制 |
| 传染机制 | 宿主的运行 | 系统存在的网络安全漏洞 | 主动或被动植入目标计算机 |
| 攻击目标 | 本地文件 | 网络上的计算机 | 本地文件和系统、网络上的计算机 |
| 计算机使用者角色 | 病毒传播的关键环节 | 无关（通过程序自身） | 木马传播的关键环节 |
| 防治措施 | 从宿主文件中清除 | 为系统打补丁（Patch） | 停止并删除木马服务程序 |

2、为了提高隐蔽性，木马有哪些隐藏技术？

答：主要有存储隐藏、进程隐藏和通信隐藏。

木马在存储时的隐藏技术主要有：

1）已知文件类型的扩展名。

2）利用文件的“隐藏”属性进行隐藏。

3）木马可以利用系统中的一些特定文件夹（如回收站、控制面板等）实现自身的隐藏。

木马的进程隐藏技术主要有：

1）进程列表欺骗（在任务栏中隐藏或在任务管理器中隐藏）。

2）不使用进程，包括：Rundll32 xxx.dll方式；特洛伊DLL；动态嵌入技术，包括：窗口Hook；挂接API；远程线程注入。

木马的通信隐藏技术主要有：

1）使用ICMP协议进行通信。

2）端口复用。

3、比较分析木马静态检测和动态检测技术的优缺点。

答：静态特征码检测技术的主要优点是简单、检测速度快、准确率高，不足之处在于：不能检测未知恶意软件，对于恶意代码变体的容忍度也很低，稍微变形便无法识别；用户需要不断地升级（离线或在线）杀毒软件特征库，同时随着特征库越来越大，检测的效率会越来越低。

动态检测技术能够检测未知恶意代码、恶意代码的变种，但也存在着不足，如产生的误报率较高，且不能识别出病毒的名称和类型等。因此，现在很多杀毒软件在检测到异常时，例如检测到应用修改Windows注册表、一个进程在进行线程插入等，会给用户弹出告警提示，由用户确定是否允许操作继续，而采用特征码检测技术时，杀毒软件一般在检测到匹配的恶意代码时会默认将其查杀或隔离。