第 5 章 接入控制和访问控制

5.1 例 题 解 析

5.1.1 简答题解析

【例题 5.1】 简述接入控制设备的作用。

【解析】 接入控制设备的作用主要有以下两个：一是作为普通路由器实现接入网络与 Internet 的互连；二是完成对用户终端的接入控制过程，主要功能包括鉴别接入用户身份、动态分配 IP 地址、建立用于指明通往用户终端的传输路径的路由项。

【例题 5.2】 简述接入控制和身份鉴别之间的关系。

【解析】 接入控制是只允许主体 X 使用的终端接入网络的控制过程。身份鉴别是确定主体 X 身份的过程。通常在身份鉴别过程中建立主体 X 与某个标识信息之间的绑定关系，随后，通过判别是否携带与主体 X 绑定的标识信息判定是否是主体 X 使用的终端发送的信息。该标识信息可以是终端的 MAC 地址或 IP 地址，这种情况下，只有源 MAC 地址是与主体 A 绑定的 MAC 地址的 MAC 帧，或者源 IP 地址是与主体 A 绑定的 IP 地址的 IP 分组，才是主体 X 使用的终端发送的 MAC 帧或 IP 分组。

【例题 5.3】 简述鉴别者和鉴别服务器需要将 EAP 报文封装成 RADIUS 消息，而不是直接封装成 IP 分组的原因。

【解析】 RADIUS 的主要功能有以下两个：一是实现鉴别者与鉴别服务器之间的双向身份鉴别；二是实现敏感信息鉴别者与鉴别服务器之间的安全传输过程。IP 分组经过互连网传输的过程中，既无法对发送端和接收端的身份进行双向鉴别，也无法实现 IP 分组发送端和接收端之间的安全传输。因此，不能直接将 EAP 报文封装成 IP 分组，然后通过互连网实现 IP 分组鉴别者和鉴别服务器之间的传输过程。

【例题 5.4】 简述 Kerberos 用户和鉴别服务器之间基于共享密钥的身份鉴别过程和防中间人攻击机制。

【解析】 由于只有某个授权用户和鉴别服务器才能够知道该授权用户的口令，而共享密钥 K_C 是通过该授权用户的口令导出的，因此，只要双方能够导出相同的共享密钥 K_C，用户和鉴别服务器的身份就能得到证实。

如果黑客能够截获用户发送给鉴别服务器的身份鉴别请求，并将用户名由 ID_C 改为 ID_H，将封装身份鉴别请求的 IP 分组的源 IP 地址由 AD_C 改为 AD_H。鉴别服务器生成的票据中的用户名和终端地址也将改为 ID_H 和 AD_H。但由于黑客无法导出共享密钥 K_C，因

而无法获得鉴别服务器生成的用户与票据授权服务器之间的共享密钥 $K_{C,TGS}$，因此，无法生成用共享密钥 $K_{C,TGS}$ 加密 ID_H 后得到的鉴别信息，从而无法让票据授权服务器确认鉴别服务器已经完成对黑客的身份鉴别过程。

【例题 5.5】 简述资源访问控制原理及过程。

【解析】 配置授权用户身份标识信息；为每一个授权用户分配资源访问权限；一旦用户提出资源访问请求，首先鉴别该用户身份，鉴别用户身份的过程就是确定该用户提供的身份标识信息是否和配置的某个授权用户的身份标识信息相同的过程；确定用户提出的资源访问请求是否符合分配该用户的资源访问权限；在确定该用户为授权用户且具有资源访问请求中要求的资源访问权限后，完成资源访问过程。

5.1.2 设计题解析

【例题 5.6】 如果采用基于证书和私钥的身份鉴别机制，且鉴别身份时使用的私钥和数字签名时使用的私钥相同，会有什么后果？

【解析】 如果主体 A 鉴别身份时使用的私钥和数字签名时使用的私钥相同，主体 B 可以利用身份鉴别过程生成主体 A 对消息 P 的数字签名。如图 5.1 所示，主体 B 生成消息 P，并计算出消息 P 的报文摘要 MD(P)。然后主体 B 发起对主体 A 的身份鉴别过程，向主体 A 发送 MD(P)，主体 A 为了证明拥有私钥 SKA，生成并向主体 B 发送 D_{SKA}(MD(P))，其中 D 是 RSA 解密算法。主体 B 根据消息 P 和 D_{SKA}(MD(P))可以证明主体 A 向主体 B 发送了消息 P，且对消息 P 进行数字签名。

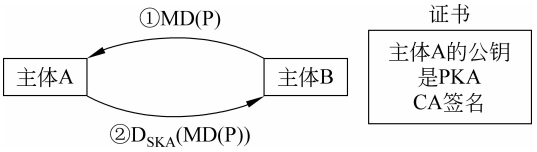
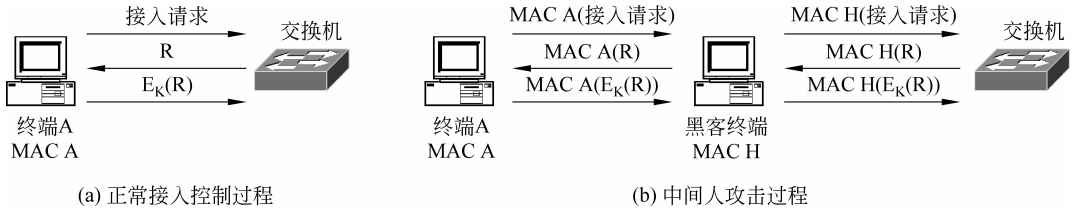


图 5.1 主体 B 利用身份鉴别过程获取主体 A 的数字签名

【例题 5.7】 假定基于共享密钥的接入控制过程如图 5.2(a)所示，终端 A 只要能够向交换机证明自己知道共享密钥 K，交换机则允许终端 A 接入，即允许转发以 MAC A 为源或目的 MAC 地址的 MAC 帧，但如图 5.2(a)所示的基于共享密钥的接入控制过程容易招致如图 5.2(b)所示的中间人攻击过程。如果黑客终端能够截获终端 A 与交换机之间传输的 MAC 帧，黑客终端可以将终端 A 发送的 MAC 帧篡改为黑客终端发送的 MAC 帧，并将交换机发送给它的随机数转发给终端 A。最终结果是导致交换机允许不知道共享密钥的黑客终端接入。修正如图 5.2(a)所示的基于共享密钥的接入控制过程，使黑客



(a) 正常接入控制过程　　(b) 中间人攻击过程

图 5.2 基于共享密钥的接入控制过程

终端无法通过如图 5.2(b)所示的中间人攻击过程接入交换机。

【解析】 改进后的基于共享密钥的接入控制过程如图 5.3 所示，终端 A 接收到交换机发送的随机数 R 后，将随机数 R 和自己的 MAC 地址 MAC A 串接在一起，用共享密钥 K 对串接结果进行加密，生成密文 $E_K(R \| MAC\ A)$，然后把密文发送给交换机。交换机用共享密钥解密密文后，得到 R ‖ MAC A，根据随机数 R，确定终端 A 具有共享密钥 K，允许转发以 MAC A 为源或目的 MAC 地址的 MAC 帧。

【例题 5.8】 假定用户 A 和用户 B 有着共享密钥 KAB，用户 A 和用户 B 通信时，确定双方身份的过程如图 5.4 所示。假定用户 C 能够截获用户 A 发送给用户 B 的鉴别消息，给出用户 C 让用户 A 误认为是用户 B 的过程，并给出如图 5.6 所示的确定双方身份过程的改进版。

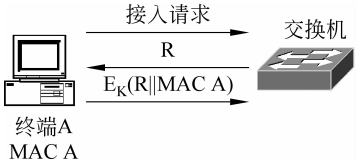


图 5.3　改进后的基于共享密钥的接入控制过程

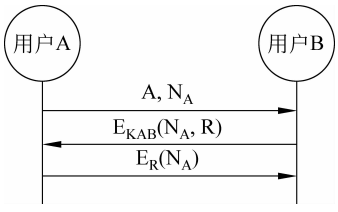


图 5.4　相互确认通信另一方身份的过程

【解析】 当用户 C 截获到用户 A 发送给用户 B 的鉴别消息(A, N_A)时，冒充用户 B 向用户 A 发送鉴别消息(B, N_A)，如图 5.5 所示。当用户 A 接收到鉴别消息(B, N_A)时，用用户 A 和用户 B 之间的共享密钥 KAB 加密 N_A 和用户 A 随机生成的会话密钥 R，然后将密文 $E_{KAB}(N_A, R)$发送给用户 B。用户 C 截获密文 $E_{KAB}(N_A, R)$后，将密文 $E_{KAB}(N_A, R)$发送给用户 A，用户 A 误认为密文 $E_{KAB}(N_A, R)$是用户 B 针对鉴别消息(A, N_A)发送的响应消息，确认用户 C 是用户 B。

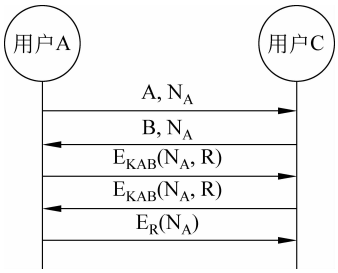


图 5.5　用户 C 冒充用户 B 的过程

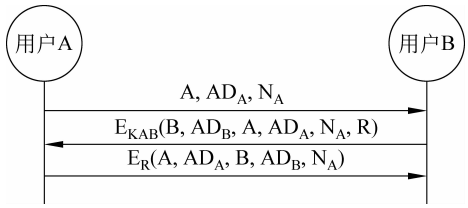


图 5.6　改进后的相互确认对方身份的过程

假定用户 A 终端的 IP 地址是 AD_A，用户 B 终端的 IP 地址是 AD_B，改进后的相互确认对方身份的过程如图 5.6 所示，用户 A 发送给用户 B 的鉴别消息中包含用户 A 的 IP 地址 AD_A，用户 B 发送的针对鉴别消息(A, AD_A, N_A)的响应消息是：用用户 A 和用户 B 之间的共享密钥 KAB 对用户 B 的标识符 B、用户 B 终端的 IP 地址 AD_B、用户 A 的标识符 A、用户 A 终端的 IP 地址 AD_A、随机数 N_A 和用户 B 随机生成的会话密钥 R 加密后生

成的密文 $E_{KAB}(B,AD_B,A,AD_A,N_A,R)$。用户 A 接收到密文 $E_{KAB}(B,AD_B,A,AD_A,N_A,R)$后，如果用用户 A 和用户 B 之间的共享密钥 KAB 解密后得到用户 A 的标识符 A、用户 A 终端的 IP 地址 AD_A 和随机数 N_A，且解密后得到的用户 B 终端的 IP 地址 AD_B 与封装密文的 IP 分组的源 IP 地址相同，用户 B 的身份得到证实。然后，用解密后得到的会话密钥 R 对用户 A 的标识符 A、用户 A 终端的 IP 地址 AD_A、用户 B 的标识符 B、用户 B 终端的 IP 地址 AD_B 和随机数 N_A 加密，生成密文 $E_R(B,AD_B,A,AD_A,N_A)$，将密文 $E_R(B,AD_B,A,AD_A,N_A)$发送给用户 B。用户 B 接收到密文 $E_R(B,AD_B,A,AD_A,N_A)$后，如果用会话密钥 R 解密后得到用户 B 的标识符 B、用户 B 终端的 IP 地址 AD_B 和随机数 N_A，且解密后得到的用户 A 终端的 IP 地址 AD_A 与封装密文的 IP 分组的源 IP 地址相同，用户 A 的身份得到证实。

【例题 5.9】 假定用户 B 鉴别用户 A 身份的过程如图 5.7 所示，其中 PKA 是用户 A 的公钥，A 和 B 是用户 A 和用户 B 的标识符，N_B 是用户 B 选择的随机数。请回答以下问题。

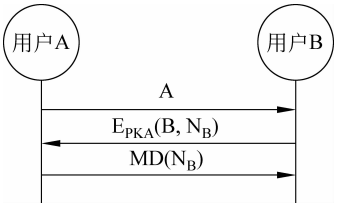


图 5.7 用户 B 鉴别用户 A 身份的过程

（1）身份鉴别和加密的区别。

（2）简述 N_B 的选择原则和作用。

（3）简述用户 A 回送 $MD(N_B)$的理由。

（4）图 5.7 所示的用户 B 鉴别用户 A 身份的过程存在哪些缺陷，请给出解决思路。

【解析】

（1）身份鉴别是验证主体的真实身份与其所声称的身份是否符合的过程，主体可以是用户、进程和主机等。验证主体 X 的身份需要做到以下两点：一是接收到只能由主体 X 生成的信息；二是确认接收到的信息是主体 X 发送的。加密是保证只允许授权访问的主体能够访问到某个信息的过程。当授权访问某个信息的主体大于 2 时，主体无法通过访问到该信息证明自己的身份。

（2）N_B 是随机数，具有以下两个特征：一是不会重复出现；二是无法预测。保证每一次身份鉴别时，用户 B 发送给用户 A 的 N_B 是不同的，且用户 A 无法预测下一次身份鉴别时用户 B 发送的 N_B，以此避免重放攻击。

（3）报文摘要算法具有单向性和抗碰撞性，因此，用户 A 回送 $MD(N_B)$，既可以让用户 B 确认用户 A 获得 N_B，又保证其他主体无法截获 N_B。

（4）虽然 $MD(N_B)$只能由用户 A 生成，但用户 B 接收到的 $MD(N_B)$可能是其他主体发送的。假如用户 C 能够截获用户 A 发送的 $MD(N_B)$，并将截获的 $MD(N_B)$转发给用户 B，使用户 B 将用户 C 误认为用户 A。

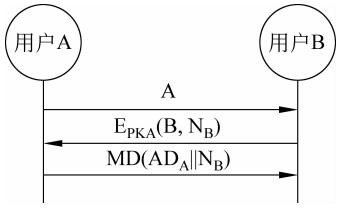


图 5.8 改进后的用户 B 鉴别用户 A 身份的过程

改进后的用户 B 鉴别用户 A 身份的过程如图 5.8 所示，用户 A 回送给用户 B 的是 $MD(AD_A \| N_B)$，其中 AD_A 是用户 A 使用的终端的 IP 地址。当用户 B 接收到封装 $MD(AD_A \| N_B)$的 IP 分组时，先将该 IP 分组的源 IP 地址和随机数 N_B 串接，并对串接结果计算报文摘要，

然后将用户 B 计算出的报文摘要与用户 A 发送的 MD($AD_A \| N_B$)进行比较，如果相等，则表明该 IP 分组确实是用户 A 所发的。

5.2　选择题分析

(1) 关于网络环境下的身份鉴别过程，以下哪一项描述是正确的？(　　)

A. 主体提供类似身份证的物理证件

B. 主体提供指纹

C. 主体提供视网膜

D. 主体提供能够证明其身份，且可以通过网络传输的主体身份标识信息

答案：D

【分析】 在网络环境下，主体和鉴别者相距甚远，无法确定经过网络传输的身份证、指纹、视网膜等扫描件与主体之间的绑定关系。

(2) 以下哪一项不是网络环境下的主体身份标识信息？(　　)

A. 密钥　　B. 用户名和口令　　C. 证书和私钥　　D. 身份证号码

答案：D

【分析】 主体身份标识信息是指可以证明主体身份的信息，鉴别者不能根据示证者能够提供 X 的身份证号码就确定示证者是 X。

(3) 对于密钥是主体身份标识信息的情况，以下哪一项描述是正确的？(　　)

A. 只有主体知道密钥

B. 只有示证者和鉴别者知道密钥

C. 主体通过向鉴别者发送密钥证明自己知道密钥

D. 只有鉴别者知道密钥

答案：B

【分析】 由于密钥只有示证者和鉴别者知道，且示证者能够向鉴别者证明自己知道密钥，示证者的身份可以因此得到证明。

(4) 对于用户名和口令是主体身份标识信息的情况，以下哪一项描述是正确的？(　　)

A. 只有主体知道用户名和口令

B. 只有示证者和鉴别者知道用户名和口令

C. 主体通过向鉴别者发送 MD(口令)证明自己知道口令

D. 只有鉴别者知道用户名和口令

答案：B

【分析】 一是不同的用户有着不同的用户名，二是每一个用户名对应一个口令。由于某对用户名和口令只有示证者和鉴别者知道，且示证者能够向鉴别者证明自己知道该对用户名和口令，示证者的身份可以因此得到证明。主体既需要向鉴别者发送用户名和口令，也不能简单地用口令的报文摘要(MD(口令))隐藏口令。

(5) 对于证书和私钥是主体身份标识信息的情况，以下哪一项描述是错误的？(　　)

A. 证书证明私钥对应的公钥与主体之间的绑定关系

B. 公钥与私钥一一对应

C. 鉴别者可以通过公钥证明主体知道私钥

D. 只有示证者和鉴别者知道私钥

答案：D

【分析】 只有主体知道私钥，鉴别者一是通过证书获取私钥对应的公钥，证明私钥对应的公钥与主体之间的绑定关系，二是通过公钥证明主体知道私钥。

(6) 如果终端已经接入 Internet，以下哪一项描述是错误的？(　　)

A. 已经建立终端与接入控制设备之间的传输路径

B. 已经为终端分配 IP 地址

C. 接入控制设备已经创建将分配给终端的 IP 地址和终端与接入控制设备之间的传输路径绑定在一起的路由项

D. 终端发送的信息中包含注册用户标识信息

答案：D

【分析】 在身份鉴别过程中，使用终端的用户需要证明自己是注册用户。一旦完成身份鉴别过程，用分配给终端的 IP 地址和已经建立的该终端与接入控制设备之间的传输路径唯一标识该注册用户使用的终端发送的数据。

(7) 以下哪一项是实现接入控制的前提？(　　)

A. 建立允许接入的授权用户的身份标识信息列表

B. 互连接入网络和 Internet 的路由器具有接入控制功能

C. 鉴别协议能够实现用户身份鉴别

D. 以上全是

答案：D

【分析】 A 和 C 选项是实现身份鉴别必需的，B 选项是接入网络结构所要求的。

(8) 对于具有 802.1X 接入控制功能的设备，以下哪一项描述是最贴切的？(　　)

A. 必须是路由器　　B. 必须是交换机

C. 可以是交换机　　D. 没有交换和路由功能的设备

答案：C

【分析】 802.1X 是以太网端口接入控制协议，具有以太网端口的设备都可具有 802.1X 接入控制功能。

(9) 对于具有 PPP 接入控制功能的设备，以下哪一项描述是最贴切的？(　　)

A. 必须是路由器　　B. 必须是交换机

C. 可以是交换机　　D. 没有交换和路由功能的设备

答案：A

【分析】 具有 PPP 接入控制功能的设备同时需要具有实现接入网络和 Internet 互连的功能。

(10) 关于接入控制设备，以下哪一项描述是错误的？(　　)

A. 是互连接入网络和 Internet 的路由器

B. 具有鉴别接入用户身份的功能

C. 具有为接入终端分配 IP 地址的功能

D. 具有发起建立与接入终端之间的传输路径的功能

答案：D

【分析】 通常由接入终端发起建立接入终端与接入控制设备之间的传输路径。

(11) 以下哪一项是接入控制的核心任务？(　　)

A. 为终端动态分配 IP 地址

B. 建立接入终端与接入控制设备之间的传输路径

C. 动态创建指明通往接入终端的传输路径的路由项

D. 鉴别启动接入终端接入 Internet 过程的用户的身份

答案：D

【分析】 接入控制的目的是只允许注册用户接入 Internet。

(12) 关于 PPP，以下哪一项描述是最贴切的？(　　)

A. PPP 是控制接入控制过程的协议

B. PPP 是鉴别用户身份的协议

C. PPP 是为终端动态分配 IP 地址的协议

D. PPP 是动态建立用于指明通往接入终端的传输路径的路由项的协议

答案：A

【分析】 PPP 只是一种控制接入控制过程的协议。其他选项的功能是在接入控制过程中由其他协议协同完成的功能。

(13) 以下哪一项功能与 PPP 作为接入控制协议无关？(　　)

A. 建立 PPP 链路时协商鉴别协议和网络控制协议

B. PPP 帧作为鉴别协议对应的协议数据单元的载体

C. PPP 帧作为 IP 控制协议对应的协议数据单元的载体

D. 实现 PPP 帧检错

答案：D

【分析】 D 选项的功能是链路层协议应该具备的功能，不是因为实现接入控制过程而增加的功能。

(14) 关于 PPP，以下哪一项描述是错误的？(　　)

A. 基于点对点信道的链路层协议

B. PSTN 作为接入网络时的接入控制协议

C. 通过 PPP over X 技术实现 PPP 帧经过多种不同类型的分组交换路径的传输过程

D. 通用的链路层协议

答案：D

【分析】 链路层协议与传输网络相关，没有适用于所有传输网络的通用链路层协议。

(15) 以下哪一项不是 PPP 链路建立过程完成的功能？(　　)

A. 两端协商与 PPP 帧传输过程相关的参数

B. 两端协商身份鉴别协议

C. 两端协商网络控制协议

D. 两端协商终端 IP 地址

答案：D

【分析】 D 选项是网络层协议配置过程完成的功能。

(16) 以下哪一种情况不是导致从身份鉴别阶段进入 PPP 链路终止阶段的原因？(　　)

A. 一端发起物理链路释放过程　　B. 物理链路上检测不到载波信号

C. 用户不是注册用户　　D. IP 地址池耗尽

答案：D

【分析】 身份鉴别阶段不分配 IP 地址。IP 地址池耗尽是导致从网络层协议配置阶段进入 PPP 链路终止阶段的原因。

(17) 以下哪一种情况不是导致从网络层协议配置阶段进入 PPP 链路终止阶段的原因？(　　)

A. 一端发起物理链路释放过程　　B. 物理链路上检测不到载波信号

C. 用户不是注册用户　　D. IP 地址池耗尽

答案：C

【分析】 用户不是注册用户，且已经进入网络层协议配置阶段，说明建立 PPP 链路时的协商结果是无须进行身份鉴别过程，因此，用户不是注册用户不会在网络层协议配置阶段成为进入 PPP 链路终止阶段的原因。

(18) 关于 EAP，以下哪一项描述是错误的？(　　)

A. EAP 报文可以封装多种鉴别协议 PDU

B. 多种传输网络对应的链路层帧可以封装 EAP 报文

C. 鉴别协议 PDU 封装成 EAP 报文、EAP 报文封装成传输网络对应的链路层帧

D. 不存在 EAP over LAN 和 EAP over PPP

答案：D

【分析】 当 EAP 报文封装成 LAN 对应的链路层帧时，称为 EAP over LAN。当 EAP 报文封装成点对点信道对应的 PPP 帧时，称为 EAP over PPP。

(19) 以下哪一种不是 EAP 定义的报文类型？(　　)

A. 请求报文　　B. 响应报文　　C. 成功报文　　D. 鉴别报文

答案：D

【分析】 EAP 共定义了 4 种类型的报文，它们分别是请求、响应、成功和失败报文，对应的编码分别是 1～4。

(20) 关于 EAP over PPP，以下哪一项描述是错误的？(　　)

A. 互连示证者和鉴别者是点对点信道

B. PPP 帧是适合点对点信道传输的链路层帧

C. 支持多种鉴别机制

D. 鉴别协议消息直接封装成 PPP 帧

答案：D

【分析】 鉴别协议消息封装成 EAP 报文，EAP 报文封装成 PPP 帧。

(21) 关于 EAPOL 和 802.1X，以下哪一项描述是错误的？(　　)

A. 802.1X 是一种实现 LAN 环境下身份鉴别和密钥管理的协议

B. EAPOL 实现 LAN 环境下 EAP 报文传输过程

C. 鉴别协议消息封装成 EAP 报文，EAP 报文封装成 LAN 对应的链路层帧

D. 802.1X 和 EAPOL 是同义词

答案：D

【分析】 802.1X 是一种实现 LAN 环境下身份鉴别和密钥管理的协议，EAPOL 只是定义 EAP 和 LAN 之间的绑定关系。802.1X 实现身份鉴别时，将鉴别协议消息封装成 EAP 报文。然后通过 EAPOL 实现 EAP 报文示证者和鉴别者之间的传输过程。

(22) 以下哪一项不是 RADIUS 具有的功能？(　　)

A. 实现对 NAS 源端鉴别

B. 加密用户身份标识信息

C. 经过 IP 网络实现鉴别协议对应的 PDU 的传输过程

D. 建立 NAS 与鉴别服务器之间的数据传输通路

答案：D

【分析】 RADIUS 是应用层协议，建立 NAS 与鉴别服务器之间的数据传输通路不是应用层协议的功能。

(23) 以下哪一项不是鉴别服务器对应每一个 NAS 需要配置的信息？(　　)

A. 客户端名字　　B. 客户端 IP 地址

C. 共享密钥　　D. 对称密钥加密算法

答案：D

【分析】 在 RADIUS 加密用户身份标识信息过程中，只使用共享密钥和报文摘要算法。

(24) 关于 RADIUS 和统一鉴别，以下哪一项描述是错误的？(　　)

A. 鉴别者中不存储用户身份标识信息

B. 由鉴别服务器统一存储用户身份标识信息

C. 互连示证者和鉴别者是传输网络，互连鉴别者和鉴别服务器是互连网

D. RADIUS 消息直接封装成传输网络对应的链路层帧

答案：D

【分析】 由于鉴别者和鉴别服务器之间可以是互连网，互连网端到端传输的是 IP 分组，因此，RADIUS 消息需要封装成 IP 分组后，再封装成传输网络对应的链路层帧。

(25) 关于访问控制，以下哪一项描述是错误的？(　　)

A. 通过身份鉴别确定用户身份

B. 为每一个用户授权

C. 保证每一个用户只能访问授权访问的资源

D. 身份鉴别和授权控制只能由资源所在的主机完成

答案：D

【分析】 可以由独立的鉴别服务器完成身份鉴别，独立的授权服务器完成每一个用户授权，资源所在主机和鉴别服务器、授权服务器可以是不同的设备。

(26) 分布式网络环境下的 Kerberos 协议属于以下哪一项协议类型？(　　)

A. 认证协议　　B. 加密协议

C. 完整性检验协议　　D. 访问控制协议

答案：D

【分析】 Kerberos 协议用于实现分布式网络环境下的访问控制过程。

(27) 以下哪一项不是对 Kerberos 票据的正确描述？(　　)

A. 票据用于证明客户对某台服务器的访问权限

B. 客户无法解密票据

C. 票据中授权客户访问的服务器能够解密票据

D. 票据用于证明发送票据的客户的身份

答案：D

【分析】 票据不具有源端鉴别功能。客户端通过发送鉴别信息证实自己的身份。

(28) 关于 Kerberos 中鉴别服务器发送的票据，以下哪一项描述是错误的？(　　)

A. 票据由鉴别服务器与票据授权服务器之间的共享密钥加密

B. 通过票据证明某个用户的身份已经得到证实

C. 票据中含用户名和用户终端的 IP 地址

D. 票据只能使用一次

答案：D

【分析】 票据在有效期内一直有效，即在有效期内，用户只需完成一次身份鉴别过程。

(29) 关于 Kerberos 中票据授权服务器发送的票据，以下哪一项描述是错误的？(　　)

A. 票据由票据授权服务器与应用服务器之间的共享密钥加密

B. 通过票据证明某个用户的权限

C. 票据中含用户名和用户终端的 IP 地址

D. 票据只能使用一次

答案：D

【分析】 票据在有效期内一直有效，即针对同一台应用服务器，在有效期内只需完成一次权限鉴别过程。

(30) 关于 Kerberos 中的应用服务器，以下哪一项描述是错误的？(　　)

A. 存储用户需要访问的资源

B. 用于票据授权服务器之间的共享密钥证实用户访问权限

C. 可以实现与用户之间的安全传输

D. 定义每一个用户的权限

答案：D

【分析】 每一个用户的权限是在票据授权服务器中定义的。