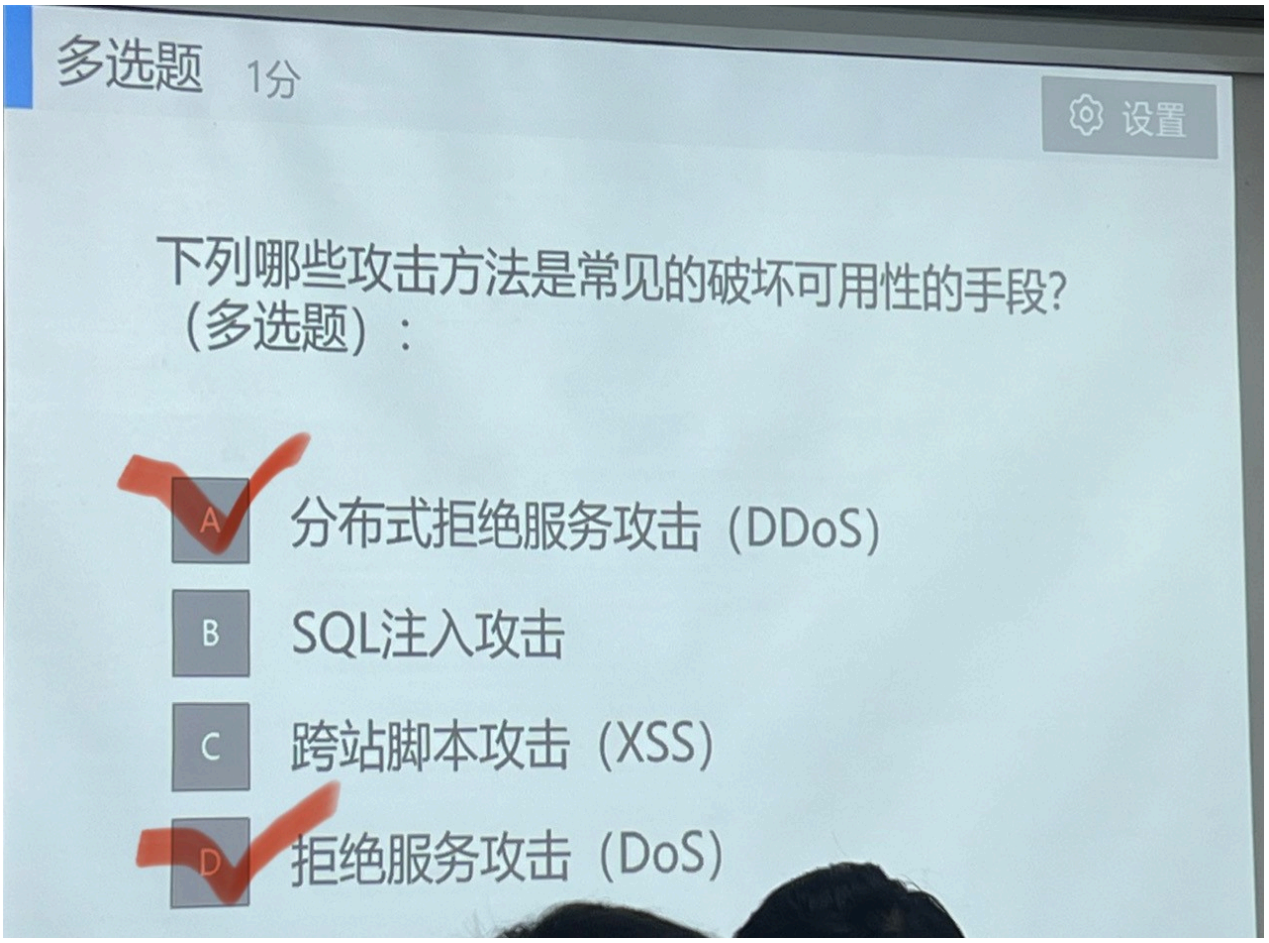
第四章 基本云安全

4.1 基本术语和概念

1. **风险**(risk)：指执行一个行为带来损失或危害的可能性。
    1. 风险一般由它的**威胁等级**和可能/已知的**漏洞数量**来衡量。
    2. 确定IT资源风险的标准：
        1. 威胁利用IT资源中漏洞的概率
        2. 如果IT资源被损害，预期会造成的**损失**。
2. **威胁**：指潜在的**安全性违反**，可能试图**破坏隐私**并/或**导致危害**，以此挑战防护。
    1. 手动或自动的威胁被设计用来利用已知的弱点，这些弱点称为**漏洞**(vulnerability)。
    2. 威胁实施的结果就是**攻击**(attack)。
3. **漏洞**(vulnerability)：是一种可能被利用的弱点，可能是因为安全控制保护不够，也可能是因为攻击击败了现有的安全控制。
    1. 造成IT资源漏洞的**原因**很多，包括：配置缺陷、安全策略弱点、用户错误、硬件或者固件缺陷、软件漏洞、安全架构薄弱等等。
4. 安全需求：
    1. 基本安全需求：保密性（Confidentiality），完整性（Integrity），可用性（Availability），这三个安全需求通常被简称为”CIA”。
    2. 延伸的安全需求：真实性（Authenticity），不可抵赖性（Non-Repudiation），可问责性（Accountability）。
5. **保密性**(confidentiality)
    1. 定义：指事物只有被授权才能访问的特性。
    2. 云计算语义下，主要是关于对**传输和存储**的数据进行访问限制的。
    3. 防御方法：数据加密、访问控制策略等
        1. 加密：智能家居中，若智能电表的用电数据没有良好加密，则不法分子可利用这些用电数据推断用户的习惯，从而猜测用户当前是否在家
        2. 访问控制：在云存储服务中，企业可能将员工分为不同的角色，每个角色有不同的数据访问权限。
    4. 例：
        1. 2017年3月，Spiral Toys玩具数据遭到泄露，泄露的敏感信息包括玩具的录音、220万账户的语音信息、MongoDB的数据等。
        2. 2017年8月，深圳某公司制造的17.5万个物联网安防摄像头被曝很容易就可被利用，只需使用默认凭证登陆就可访问摄像头的转播画面。
6. **完整性**(integrity)：指未被未授权方篡改的特性。一个比较重要的问题是**传送**到云服务的数据和云服务**接收**到的数据**完全一致**。
    1. **数据完整性**：信息在**存储或传输**的过程中保持未经授权不能篡改的特性。
    2. **系统完整性**：确保系统免于未经授权的操作，**预期功能不受损害**，也可理解为系统的可靠正确地实现功能。

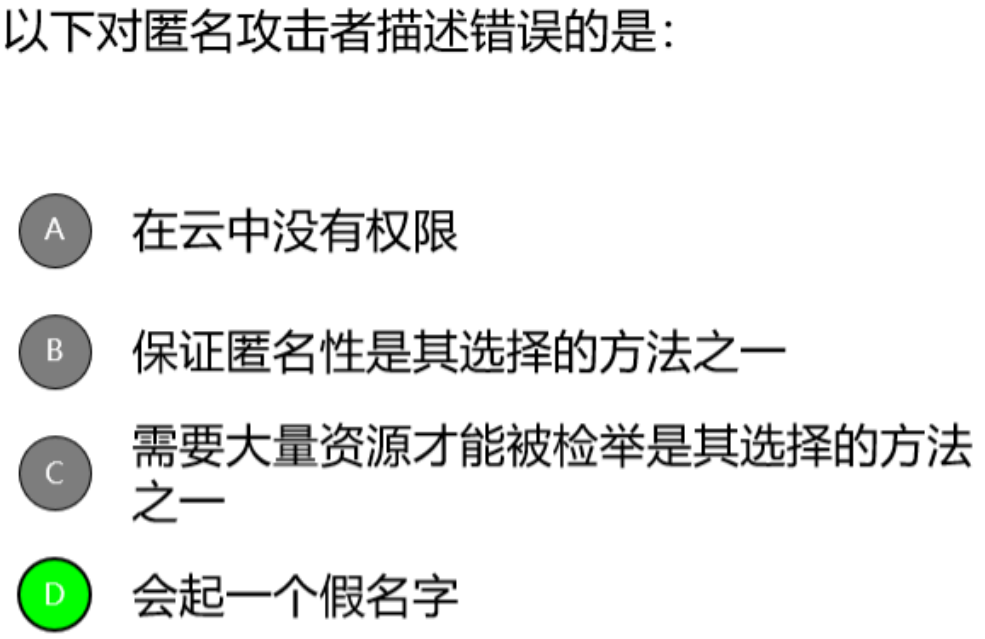
    4. 举例：智能安防系统的系统完整性是指它能在发生非法入侵等情况时及时报警，这是它的预期功能。若安防系统功能**出现问题，不会及时报警**，其后果可能是金钱损失，甚至威胁用户人身安全。
    5. 防御方法：Hash 函数，纠错码，消息认证码。
7. **可用性**(availability)：指特定时间段内可以访问和可以使用的特性。
    1. 云计算语义下，云服务的可用性，是**云提供者和云运营商**共同的责任。当基于云的解决方案**扩展到云服务用户**时，可用性也是**云用户**的责任。
    2. 在互联网中，破坏可用性的典型例子是攻击者通过分布式拒绝服务攻击（DDoS，Distributed Denial of Service），DDoS攻击是通过大量的垃圾请求阻塞服务器，使正常用户的请求得不到响应。
    3. 2017年5月， WannaCry勒索病毒感染了西班牙电信等公司，其利用 “永恒之蓝”（EternalBlue）漏洞加密系统数据，从而勒索用户。该事件是典型的传统互联网**数据可用性**被破坏的例子。在该事件中，用户计算机的所有数据都被加密，无法获取。
8. 真实性(authenticity)：指事务是由经过授权的源提供的特性 or 能够识别/实体认证及**确定数据来源**。
    1. 云计算语义下，
       1. 不可否认性：一方不能否认或质疑一次交互的真实性。
       2. 真实性提供了一种证明，证明这些交互是否是**唯一链接到一个经过授权的源**的，这意味着系统需要**验证用户或设备的身份**，该验证过程称为“**认证**”。
       3. 例如：在收到一个不可否认的文件后，如果不产生一条对此访问的记录，那么用户就不能访问该文件。
    2. 实现方法：认证、数字签名、公钥基础设施（PKI）
9. 可问责性(Accountability)：不能声称自己没有发送消息。
    1. 指对特定行为能唯一地跟踪到行为主体，是一项综合的安全需求。
    2. 系统的绝对安全是一个不可达到的目标，因此需要将破坏安全的行为追溯到责任方，以便于后续的责任追溯以及纠纷解除。
    3. 可以对破坏安全属性行为的威慑，帮助故障排除，入侵检测与防御，事后恢复等。
    4. 实现可问责性的关键组成部分：身份认证、日志记录和审计、访问控制、不可否认性

12. **总结**：
    1. 保密性、完整性、可用性、真实性、不可抵赖性、可问责性是与衡量**安全性**相关联的特性。
    2. 威胁、漏洞、风险是与衡量和评估**不安全性或安全性缺乏**相关联的。
    3. 安全控制、机制、策略是与建立支持改进安全性的**对策和保护措施**相关联的。

13. 

4.2 威胁作用者

1. **威胁作用者**(threat agent)：是引发威胁的实体，因为它能够**实施攻击**。
    1. 分类
        1. 内部 / 外部
        2. 人 / 软件程序
    2. **匿名攻击者**(anonymous attacker)：是云中**没有权限、不被信任**的云服务用户。
        1. 它通常是一个**外部软件程序**，通过公网发动网络攻击。
        2. 当匿名攻击者对安全策略和防护所知有限时，会抑制他们形成有效攻击的能力。
        3. 匿名攻击者往往诉诸**绕过用户账号**或**窃取用户证书**的手段，同时使用能确保**匿名性或需要大量资源才能被检举**的方法。



4.

3. **恶意服务实施者**(malicious service agent)：能**截取并转发**云内的网络流量。
    1. 它通常是带有**被损害的**或**恶意逻辑**的服务代理（或伪装成服务代理的程序）。
    2. 也可能是能够**远程截取并破坏消息内容**的外部程序。
4. **授信的攻击者**(trusted attacker)：又称**恶意租户**(malicious tenant)，与同一云环境中的云用户共享IT资源，试图利用合法的证书来把云提供者、以及与他们共享IT资源的云租户作为攻击目标。
    1. 通过**滥用合法证书、挪用敏感和保密信息**，在云的信任边界**内部**发动攻击。
    2. 恶意租户能够使用基于云的IT资源做很多非法之用，包括非法入侵认证薄弱的进程、破解加密、往电子邮件账号发送垃圾邮件、发起拒绝服务等常见的攻击等。
5. **恶意的内部人员**(malicious insider)：是**人为**的威胁作用者，他们的行为代表**云提供者**，或者**与之有关**。
    1. 他们通常是现任或前任雇员，或是能够访问云提供者资源范围的第三方。
    2. 这种类型的威胁作用者会带来极大的破坏可能性，因为恶意的内部人员可能拥有访问云用户IT资源的管理特权。

2. 总结
    1. 匿名攻击者是不被信任的威胁作用者，通常试图从云边界的**外部**进行攻击
    2. 恶意服务作用者截取网络通信，试图恶意地**使用或篡改**数据。
    3. 授信的攻击者是经过授权的**云服务用户**，具有合法的证书，他们会使用这些证书来访问基于云的IT资源或攻击其他资源。
    4. 恶意的内部人员是试图**滥用**对云资源范围的**访问特权**的人。

以下对威胁作用者描述不正确的是：

A 匿名攻击者是不被信任的威胁作用者

B 恶意服务作用者一般提供恶意服务

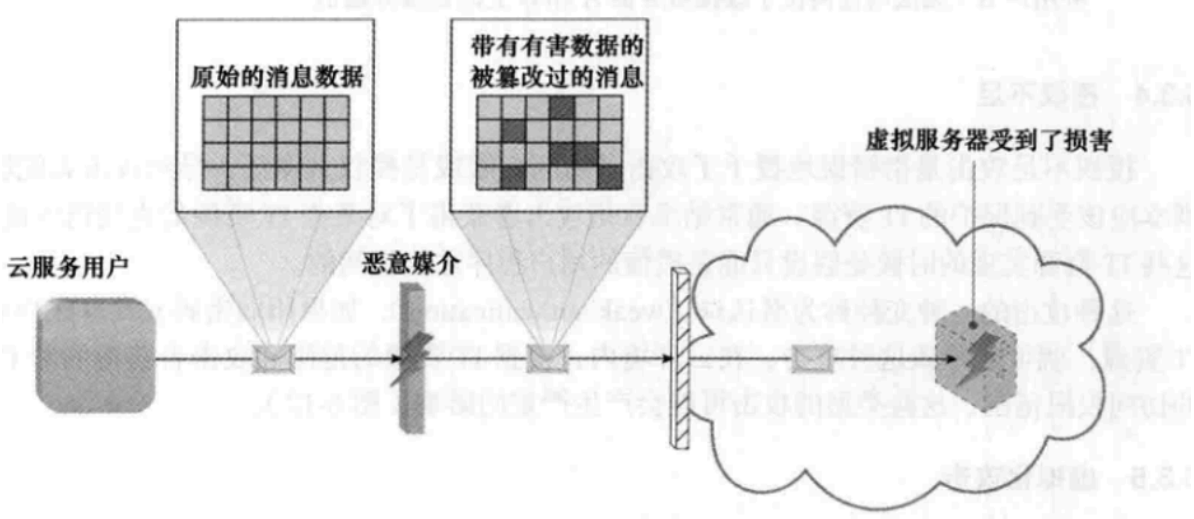
C 授信的攻击者是经过授权的云服务用户

D 恶意的内部人员具有访问IT资源的特权

3.

4.3 云安全威胁

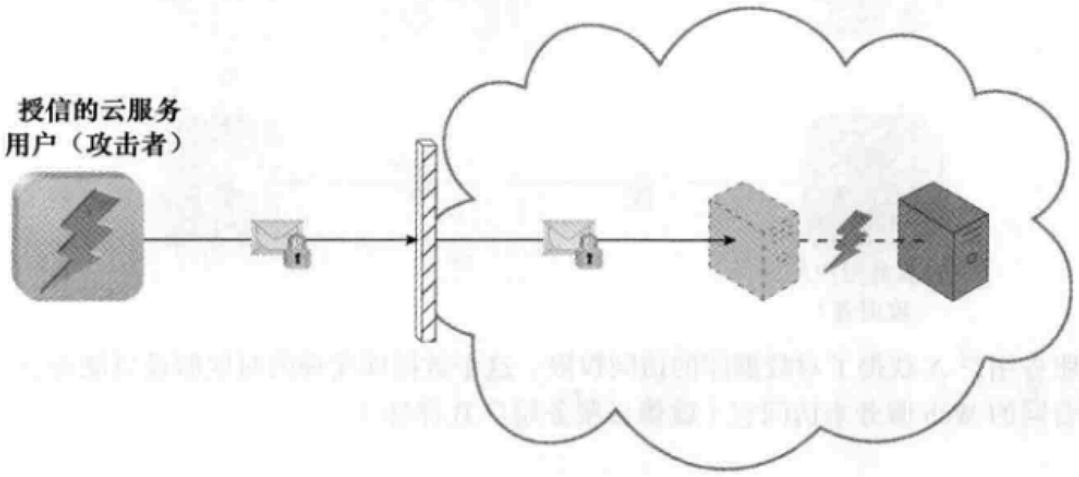
1. **流量窃听**(traffic eavesdropping)：指当数据在传输到云中或在云内部传输时（通常是从云用户到云提供者），被**恶意的服务作用者被动地截获**，用于非法的信息收集，破坏**保密性**。
    1. 由于这种攻击被动的性质，其更容易长时间进行而不被发现。
    2. 美国的“上游”计划：企图通过监听海底光缆截取流经海底光缆及通信基础设施的信息，以便量子计算机出现之后，进行开发。
2. **恶意媒介**(malicious intermediate)：是指消息被**恶意服务作用者**截获并篡改，因此可能会破坏消息的**保密性**和**完整性**。
    1. 它还有可能在把消息转发到目的地之前插入有害数据。



恶意的服务作用者截获并修改云服务用户发往位于虚拟服务器上的云服务（图中未显示）的消息。因为有害数据被打包进了消息，虚拟服务器受到了损害

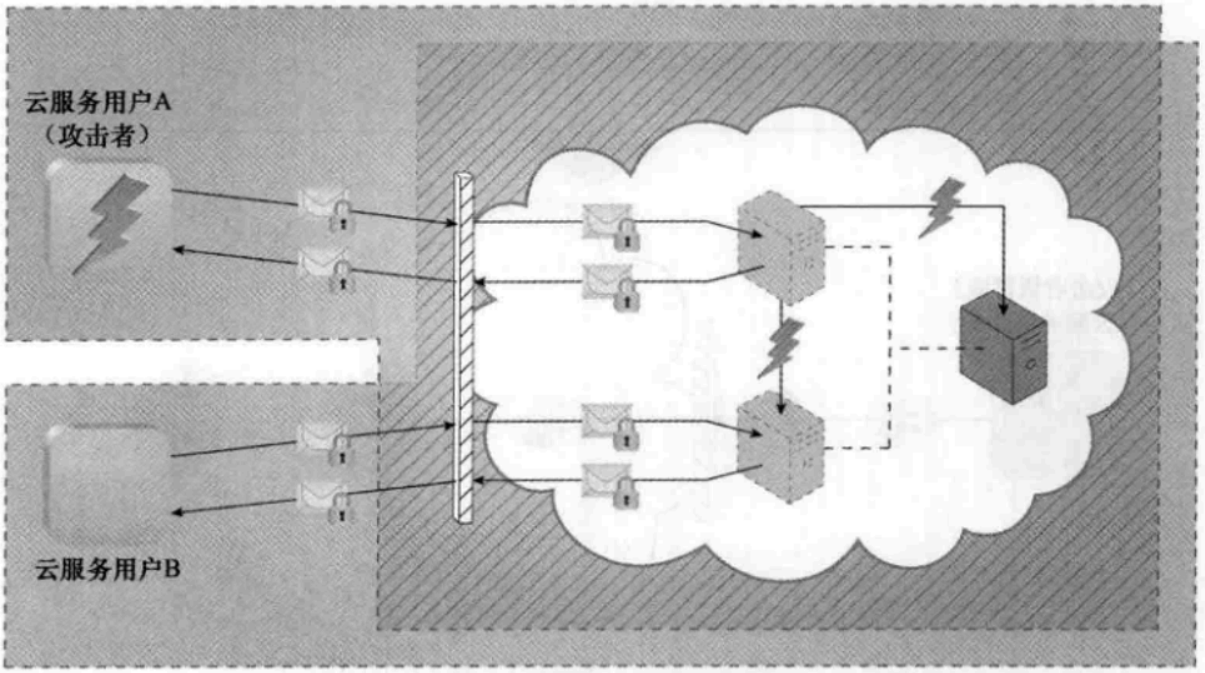
    2.
3. 拒绝服务(DoS)：攻击的目标是使IT资源过载至无法正确运行。

    1. 发起形式包括：
        1. 云服务上的负载由于**伪造的消息或重复的通信请求**不正常的增加。
        2. 网络流量过载，降低了响应性，性能下降。
        3. 发出多个云服务请求，每个请求都设计成消耗过量的内存和处理资源。
4. 授权不足：是指**错误的授予**了攻击者**访问权限**，或是授权太宽泛，导致攻击者能够访问**本应该受到保护的IT资源**。
    1. 这种攻击的一种变种称为**弱认证**(weak authentication)，如果用弱密码或共享账户来保护IT资源，就可能导致这种攻击。
5. **虚拟化攻击**(Virtualization attack)：利用虚拟化平台的漏洞来危害虚拟化平台的保密性、完整性和可用性。例如：**虚拟机逃逸攻击**



授权的云服务用户发动了一场虚拟化攻击，滥用了他对虚拟服务器的管理权限来获取底层硬件

6. **信任边界重叠**：如果云中的**物理IT资源**是由不同的云服务共享的，那么这些云服务用户的信任边界是重叠的。恶意的云服务用户可以把目标设定为**共享的IT资源**，意图损害其他共享同样信任边界的云服务用户或IT资源。

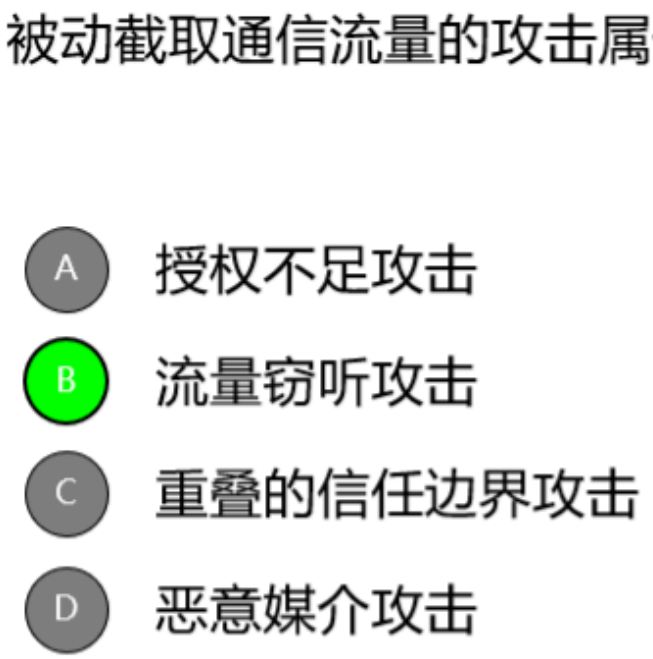


云服务用户 A 是被云授信的，因此获得了对虚拟服务器的访问权限，然后它再意图攻击底层的物理服务器以及云服务用户 B 使用的虚拟服务器

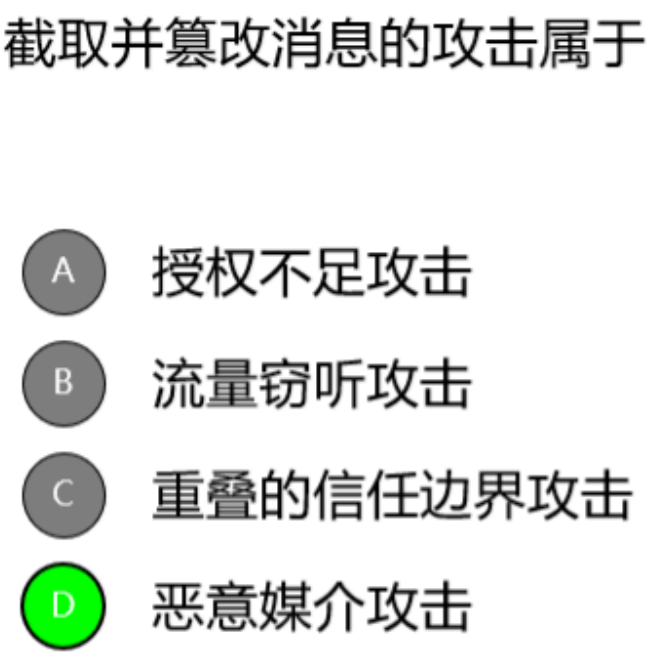
7. 总结

1. 流量窃听和恶意媒介攻击通常是由截取网络流量的**恶意服务作用者**实施的。
2. 拒绝服务攻击的发生是当目标IT资源由于请求过多而负载过重，这些请求意在使IT资源性能陷入瘫痪或不可用。
3. 授权不足攻击是指错误的授予了攻击者访问权限或是授权太宽泛，或是使用了弱密码。
4. 虚拟化攻击利用的是虚拟化环境的漏洞，获得了对底层物理硬件未被授权的访问。
5. 重叠的信任边界潜藏了一种威胁，攻击者可以利用多个云用户共享的、基于云的IT资源。

8. 练习

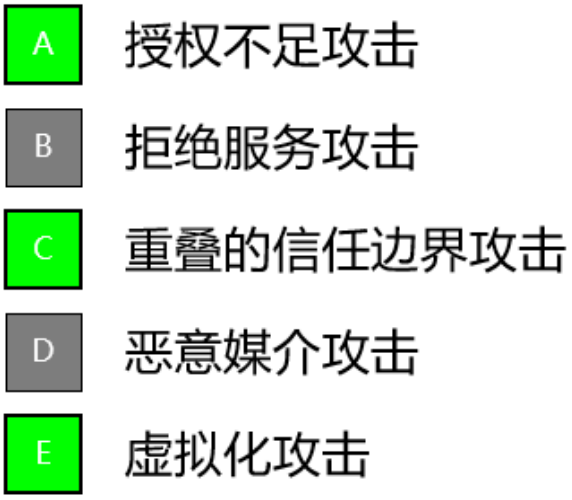


1.

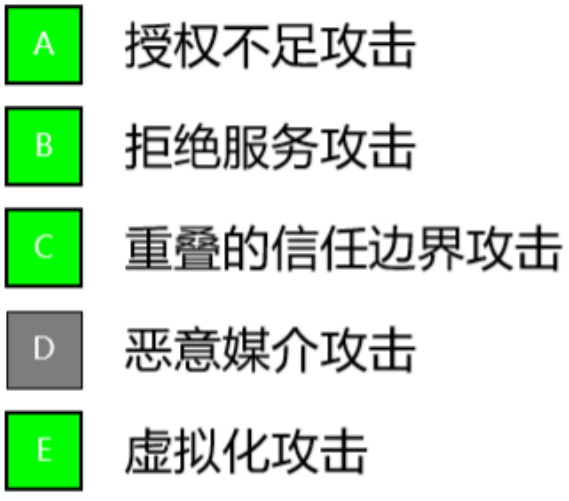


2.

3. 能获得不该访问的底层IT资源访问权的攻击包括：



4. 能导致不具有权限的底层IT资源异常（包括非法访问和运行异常）的攻击包括：



4.4 其他考量

1. 有缺陷的实现：
    1. 云服务部署不合规范的设计、实现或配置会有不利的后果，而不仅仅是运行时的异常和失效。
    2. 云提供者的软件或硬件有内在的安全缺陷或操作弱点，攻击者便会利用这些漏洞来损害**云提供者的IT资源**和由托管给云提供者的**云用户的IT资源**的完整性、保密性和可用性。
2. 安全策略不一致：

    1. 当云用户把IT资源放到公有云提供者那里时，就需要接受云提供者提供的信息安全方法，其与传统方法可能不完全相同，甚至不相似。
    2. 有些公有云中，其他第三方（如安全代理和证书授权方）可能会引入他们自己不同的安全策略和措施。
3. 合约：
    1. 云用户需要很小心的检查云提供者提出的合约和SLA，确保涉及资产安全的策略和其它相关保障令人满意。
    2. 需要有明确的语言指明云提供者承担的责任和 / 或云提供者可能要求的免赔等级。云提供者承担的责任越大，云用户的风险就越低。
    3. 需要指明云用户和云提供者资产之间的界限在哪里。

4. 总结：
    1. 云用户需要意识到，部署有缺陷的基于云的解决方案，可能会引入**安全风险**。
    2. 在选择云提供厂商时，理解云提供者如何定义和强加**所有权**，以及可能的**不兼容的云安全策略**，是形成评估标准的关键部分。
    3. 在云用户和云提供者签署的**法律协议**中，需要明确定义和相互理解对潜在的安全泄露的责任、免责和问责。
    4. 对于云用户来说，在理解具体针对某个特定云环境的安全相关的可能问题之后，对识别出的风险进行相应的**评估**是很重要的。