**1.如何理解可信？**

可信是指值得信任，一个系统可信是指系统的运行（或输入输出关系）符合预期的结果，没有出现未预期的结果或故障。TCG（Trusted Computing Group）给出了可信的定义“如果一个实体的行为总是以预期的方式达到既定目标，那么它是可信的”。ISO/IEC 15408标准对可信的定义为：一个组件、操作或过程的可信是指在任意操作条件下是可预测的，并能很好地抵抗应用程序软件、病毒以及一定物理干扰所造成的破坏。“可信”强调行为的可预测性，能抵抗各种破坏，达到预期的目标。

**2.如何理解可信计算？可信计算在信息系统中的作用是什么？**

针对信息系统而言，“可信计算”的概念可以从以下几个方面来理解：

（1）用户的身份认证：使用者有合法的身份，可以使用该系统。

（2）平台软、硬件配置的正确性：使用者可以信任平台的运行环境，软、硬件配置没有问题。

（3）应用程序的完整性和合法性：在平台上运行的应用程序是可信的，是正版软件且未受破坏。

（4）平台之间的可验证性：在网络环境下运行的多个平台之间是可以相互信任的，即这些平台本身各自可信，且可以合法地相互访问，相互通信不存在安全问题。

**3.可信计算的基本功能是什么？**

**要点:（1）完整性度量、存储和报告；（2）平台证明；（3）受保护能力。**

**参考答案：**

一个可信平台能够达到可信的最基本原则是必须真实报告系统的状态，绝不暴露密钥和尽量不表露自己的身份。为此，可信计算必须有三个基本功能：完整性的度量存储和报告、平台证明、受保护能力。

完整性度量是一个过程，是在可信平台启动过程中，组件（固件或软件）加载和执行之前，其度量散列值被扩展到了 TPM 内部的平台配置寄存器中，通过计算该组件的散列值，并同期望值比较，就可以维护它们的完整性。

证明就是确认信息真实性的过程。通过这个过程，外部实体能够确认被保护区域、受保护能力和信任根，而本地调用不需要证明。通过证明，完成了远程实体对平台身份的认证。由于引入了 AIK 对 PCR 值和随机数 N 在 TPM 的控制下的签名，保证了平台配置信息的完整性和新鲜性，从而大大提高了通信的安全性。

受保护能力就是唯一被许可具有访问被保护区域的特权命令集，而被保护区域就是能够安全操作敏感数据的地方，如：内存、寄存器等。TPM 通过实现受保护能力和被保护区域，来保护和报告完整性度量值。

**4.可信计算的信任根有哪些？每个信任根的作用是什么？**

**要点：（1）RTM包括CRTM，作为平台可信度量起点;（2）可信存储根RTS是平台可信度量值的存储基点；（3）可信报告根时平台向访问者提供可信状态报告的起点。**

**参考答案：**

TCG 认为一个可信平台必须包含三个可信根：RTM，可信存储根（RTS）和可信报告根(RTR)。其中，RTM 存储在 TBB 中，而 RTS 和 RTR 存储在 TPM 中。对平台的可信性进行度量，对度量的可信值进行可信存储，当访问者询问时提供可信报告，这一机制简称为度量、存储和报告机制。这个机制是可信信息系统确保自身安全，并向外提供可信服务的一个重要机制。RTM 是平台进行可信度量的基点，RTS 是平台可信度量值的存储基点，RTR是平台向访问者提供平台可信状态报告的基点。

RTM是平台启动时首先执行的一段程序，它是由CRTM控制的计算引擎。在理想状态下，CRTM存储在TPM内部，但根据实现的需要，它可能需要加载到其他固件中， 如BIOS。

RTS由TPM芯片中的PCR和存储根密钥（Storage Root Key，SRK）组成。TCG定义的多种密钥是按照树形结构进行组织和管理的，处于上级的父密钥的公钥对处于下级的子密钥进行加密保护，同时配合密钥访问控制机制，确保密钥体系的安全。存储密钥SK用于对其他密钥进行存储保护，它也是RSA密钥对。这些密钥是分级的，下级的密钥受到上级的存储密钥的加密保护，从而构成一个密钥树。处于密钥树根部的密钥是最高级存储密钥，即存储根密钥SRK，它是2048位的RSA密钥对，主要用于对由TPM使用，但存储在 TPM之外（如硬盘）的密钥进行保护。同时，它作为父密钥对其子密钥进行加密保护。

RTR由TPM芯片中的PCR和背书密钥（Endorsement Key，EK）组成。EK仅用于以下两种操作：一是创建TPM的拥有者；二是创建AIK及其授权数据。EK是唯一的，不作他用。一个EK唯一对应一个TPM，一个TPM唯一对应一个平台，因此，一个平台只有唯一一个EK，它是平台的身份标识。AIK是EK的替代物，也是2048位的RSA密钥。AIK仅用于对TPM内部标识平台可信状态的数据和信息（如PCR值、时间戳、计算 器值等数据）进行签名和验证签名，不用于数据加密。注：AIK不能签名其他非TPM状 态的数据，这样做的目的是防止攻击者伪造PCR让AIK签名。在上面讲到的平台远程 证明中，使用AIK向访问者提供平台状态的可信报告，但由于AIK是由EK控制产生的， 所以本质上EK是报告根，而AIK是EK的替代物。

**5. 目前，可信平台的起点是 BIOS。它是否与 TPM 的目的有冲突，是否存在安全问题？分析说明。**

**要点：有冲突，CRTM首先需要度量BIOS，把CRTM放在BIOS里面不符合TPM的目的。安全问题：（1）BIOS安全级别低于TPM芯片，易受恶意代码攻击；（2）BIOS对信息系统或TPM控制权过大，引发安全问题。**

**参考答案：**

TCG给出的信任链是CRTM→BIOS→OSLoader→OS→Applicatons，系统加电后需要由可信代码CRTM去度量BIOS代码的完整性。TPM的设计是基于可信的CRTM开始的信任链进行完整性度量，以此为起点保证整个平台的可信，因此最符合这一设计的方法是把CRTM嵌入TPM芯片内。如果起点在BIOS代码中，会导致BIOS自身代码的完整性没有经过度量，不符合TPM的目的。

存在的安全问题是，BIOS不具备TPM模块的安全级别，其中的代码有经受恶意代码攻击的风险。同时BIOS还需要完成硬件设备和配置信息的自检，具备对信息系统极大的控制权，以此作为可信平台的起点也构成安全问题。

**6.为什么要用 AIK 替代 EK？分析说明。**

**要点：（1）EK与系统绑定，不能迁移；（2）平台(或用户)可以针对不同应用或不同时间使用不同的AIK证书来表征平台身份可信性，利用AIK也可以实现与EK相比更大的新鲜度，保护用户隐私。**

**参考答案：**

EK密钥由TPM芯片生产厂商生成，是TPM芯片的唯一标识，在理想状态下，TPM内部保存着可信第三方颁发的EK证书用以证明EK的合法性。EK是重要的私有信息，用EK加密或签名数据，攻击者可能会从被加密的数据中获取EK的相关信息而攻击TPM。平台身份密钥AIK由此产生。利用AIK密钥可以进行签名与加密等操作。AIK密钥由平台所有者产生，保存在TPM、内部或外部。平台身份证书由可信第三方签发，用以证明AIK密钥的合法性。AIK可以看作是EK的“别名”，EK只有一对，但EK可以对应多对AIK，之后，平台(或用户)可以针对不同应用或不同时间使用不同的AIK证书来表征平台身份可信性，利用AIK也可以实现与EK相比更大的新鲜度。

**7.SRK 是什么？其主要用途是什么？是否可以迁移？**

**要点：（1）存储密钥根。管理用户数据，作为密钥树的根节点，保护子密钥。（2）不能，一个是部分子密钥不能迁移导致SRK不能迁移，另一个是SRK需要对持久存储区进行加密保护。**

SRK即存储根密钥，是存储密钥的一个特例。整个系统拥有一个最高权限的存储密钥，这个最高级密钥也就是存储根密钥。它很特殊，在每个用户创建的时候生成，管理这个用户的所有数据，也就是存储可信根。和背书密钥一样，一个TPM仅存在唯一一个。所有其它的密钥都在存储根密钥的保护之下。

由于SRK作为父密钥对子密钥进行加密保护，并配合密钥访问控制机制保证密钥体系安全，而在密钥树上的部分密钥是不可迁移的。此外，由于 TPM 的存储容量有限，因此一般在磁盘上还需要构建一个持久存储区，使用 SRK 进行加密保护，从而保证受保护的数据可以扩充。综合以上两点SRK不能迁移。

**8.详细分析 PCR 在 TPM 所起到的作用。**

（1）存储SRK，组成RTS，实现密钥管理的功能，作为平台可信度量值的存储基点。

（2）存储EK，组成RTR，作为平台向访问者提供平台可信状态报告的基点。

（3）保存平台自上电启动到应用程序加载所参与组件的所有度量信息（包括平台状态转换信息），只保存经过扩展后的度量结果。

（4）与日志相互关联，在攻击者修改日志中的度量内容、时序和异常事件时，两者通过对比来实现异常检测，增强系统安全性。

**9.信任链是如何完成信任度量的？**

信任链的度量过程为：①当系统加电以后，首先，CRTM 度量 BIOS 的完整性。一般地，这种度量就是将 BIOS 当前代码的散列值计算出来，并将计算结果与预期值进行比对。如果两者一致，说明 BIOS 没有被篡改，是可信的；否则，说明 BIOS 已经被攻击，不可信，此时所有的启动将停止。②如果 BIOS 可信，则可信的边界将从 CRTM 扩展到CRTM＋BIOS。于是执行 BIOS。③BIOS 度量 OSLoader，OSLoader 是操作系统的加载器，包括主引导记录、操作系统引导扇区等。 ④如果OSLoader 可信，则可信的边界扩展到 CRTM＋BIOS＋OSLoader，执行操作系统的加载程序。⑤OSLoader 在加载操作系统之前，首先度量操作系统的完整性。⑥如果操作系统可信，则可信边界扩展到 CRTM＋BIOS＋OSLoader＋OS，加载并执行操作系统。⑦操作系统启动后，由操作系统度量应用程序的完整性。⑧如果应用程序可信，则可信边界扩展到 CRTM＋BIOS＋OSLoader＋OS＋Applications，操作系统将加载并执行应用程序。上述过程看起来是一条环环相扣的链条，因此称为“信任链”。

**10.详细分析基于静态可信根度量的缺陷。动态可信度量能够解决这些缺陷吗？为什么。**

**要点：（1）静态可信根度量无法保证系统运行时安全；（2）可以抵御针对BIOS的攻击和BootLoader的漏洞，但是存在TPM重置攻击的风险；（3）DRTM没有解决软件可信的问题。**

**参考答案：**

信任度量是在平台启动时进行的一次性完整性验证，此时作为可信度量根的 BIOS 在平台的运行生命周期内执行一次，且度量的实体资源仅限于操作系统及其加载之前的软硬件，这种度量被称为静态度量，它没有度量运行过程中加载的软件，因此无法保证系统运行时的安全。

动态可信度基于CPU中的动态可信根，以指令执行的方式通知TPM进行信任度量。因此动态可信度量可以抵御引导装载程序（BootLoader）的漏洞，以及针对 BIOS 的攻击，但还存在 TPM 被重置的攻击。

有了 DRTM 之后，TPM 可以在任何时候执行度量，重新构建平台的信任链，而不需要重启整个平台。这种重新构建信任链的过程，既可以在平台启动时完成，也可以在平台启动后运行的任何时候完成，从而重新创建可信计算环境，但 DRTM 技术只是实现了信任链的多次度量，其度量的内容还是软件的数据完整性，并不是软件的可信性，因此，DRTM 技术同样没有解决软件可信的问题。