密码学第一次作业-朱哲昊-21371276

朱哲昊

March 2023

1 当使用 POS 机刷银行卡进行支付时，用户通过提供个银行卡和个人身份识别码（PIN）来访问其账户，从而完成支付。请给出该支付系统相关机密性、完整性等所需的安全需求，并针对每个安全需求给出重要性程度。

1. 机密性：确保用户的银行卡号和个人身份识别码不会被未经授权的第三方获得或者泄露。重要性程度：非常高。机密性是保障用户账户安全的基本要求，一旦银行卡号和个人身份识别码被泄露，用户账户将面临巨大的安全风险。

2. 完整性：确保支付数据不被篡改或者损坏。重要性程度：非常高。支付数据的完整性是保障支付过程的基本要求，一旦支付数据被篡改或者损坏，支付过程将无法完成，且用户的账户可能会受到影响。

3. 可用性：确保支付系统始终可用，用户能够随时进行支付。重要性程度：高。可用性是保障用户体验的重要因素，一旦支付系统不可用，用户将无法进行支付，且可能会受到经济损失。

4. 身份验证：确保用户的身份得到验证，只有经过身份验证的用户才能进行支付。重要性程度：高。身份验证是保障支付系统安全的基本要求，只有经过身份验证的用户才能访问账户进行支付，可以有效地避免账户被未经授权的第三方使用。

总体来说，机密性和完整性是该支付系统的最重要的安全需求，需要采取严密的措施来保障用户银行卡号和个人身份识别码的安全性和支付数据的完整性。可用性和身份验证也是很重要的安全需求，需要保证支付系统的稳定性和用户身份的安全。

2 对于下面的资产，发生保密性、可用性和完整性损失时，分别为其产生的影响划分低、中和高等级，并陈述理由：合同签订机构的大单收购信息系统，包含敏感、预投标阶段的合同信息和例行的行政信息，分别评价这两份信息资产的影响情况及整个信息系统的影响情况。

1. 保密性保密性损失是指未经授权的人员获取了系统中包含的敏感信息。对于敏感、预投标阶段的合同信息，若未经授权的人员获得，将导致严重的商业竞争风险和信息泄露风险。因此，该资产的保密性损失属于高级别。

而对于例行的行政信息，虽然也存在泄露的风险，但相对合同信息来说影响更小，故保密性损失属于中级别。

2. 可用性可用性损失是指系统中的信息不能及时地被授权的用户所访问，导致工作受阻。对于敏感、预投标阶段的合同信息，如果由于攻击或其他原因而无法访问，将会对机构的商业活动造成重大影响，因此该资产的可用性损失属于高级别。

而对于例行的行政信息，尽管其重要性不如合同信息，但其不可用也将导致部分行政管理活动受阻，因此可用性损失仍然属于中级别。

3. 完整性完整性损失是指信息遭到未经授权的篡改、破坏或丢失。对于敏感、预投标阶段的合同信息，一旦被篡改或破坏，将导致商业交易的中断和公司的商誉受损，因此完整性损失属于高级别。

3 攻击分析

攻击手段	攻击者能力	破坏的安	应采用的安全机制
1)	被动攻击	未	加强安全漏洞扫描，实施多层次防御
2)	主动攻击	社交	弱口令检测，二次验证，防钓鱼培训，加密存储用户凭证
3)	主动攻击	滥用被盗账户	强化身份验证
4)	主动攻击	滥用被盗账户	限制高危操作权限
5)	主动攻击	智能合约攻击	强化代码审查

4 安全等级评价

1) 在控制器和设备之间必须建立双向验证机制

安全模式	保密性	完整性	可用性	真实性	可溯源性
安全需求	1	1	1	1	0
安全等级	高	低	低	高	0

这个项目必须确保用户身份真实性和账户信息保密性。建立双向验证机制有助于防止未授权的设备访问云资源

2) 确保云租户账户信息、鉴别信息、系统信息等不被泄露

安全模式	保密性	完整性	可用性	真实性	可溯源性
安全需求	1	1	1	1	1
安全等级	高	高	低	高	低

保障云租户账户信息、鉴别信息、系统信息不被泄露和管理权限的控制，是保护用户数据隐私和保密性的基本要求

3) 只有在管理设备授权下，云服务商或第三方才具有用户数据的管理权限

安全模式	保密性	完整性	可用性	真实性	可溯源性
安全需求	1	1	1	1	1
安全等级	高	高	低	低	低

保障云租户账户信息、鉴别信息、系统信息不被泄露和管理权限的控制，是保护用户数据隐私和保密性的基本要求

4) 屏蔽资源故障，当某台设备崩溃后，不会影响到整个系统和其他虚拟机

安全模式	保密性	完整性	可用性	真实性	可溯源性
安全需求	1	1	1	1	1
安全等级	低	低	高	低	高

只有可溯源才能保证设备的独立运转，要高可用性才可以使得系统的好用

5) 提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改

安全模式	保密性	完整性	可用性	真实性	可溯源性
安全需求	1	1	1	1	1
安全等级	高	高	低	低	低

提供虚拟机镜像，有助于确保虚拟机镜像敏感资源不被篡改和非法访问，从而保护数据完整性和保密性。对保密性和完整性的要求评级为高

5 请查阅资料，结合一个近年的网络安全事件，指出这起事件中相关系统的 3 条安全需求及对应的安全目标与安全等级，并简要阐述理由。

2017 年的 Equifax 数据泄露事件。这次事件导致了约 1.43 亿人的个人身份信息泄露，包括社会安全号码、出生日期、地址等重要信息。在这个事件中，相关系统需要满足以下三个安全需求：

保密性需求：保护个人身份信息不被未经授权的人访问和披露。安全目标：确保系统只有授权用户才能访问个人身份信息。

安全等级：机密性等级

理由：个人身份信息是敏感数据，一旦被未经授权的人访问和披露，将会对个人造成严重的损害。因此，保证个人身份信息的保密性至关重要，需要对系统进行机密性保护。

完整性需求：防止个人身份信息被恶意篡改或损坏。安全目标：确保个人身份信息在传输和存储过程中不被篡改或损坏。

安全等级：完整性等级

理由：如果攻击者能够篡改或损坏个人身份信息，将会对用户造成不可挽回的损失。因此，保障个人身份信息的完整性也是至关重要的。

可用性需求：确保系统能够及时、可靠地响应用户请求。安全目标：确保系统的可用性，防止拒绝服务攻击。

安全等级：可用性等级

理由：在处理大量用户请求时，系统容易受到拒绝服务攻击的影响。如果系统无法及时响应用户请求，将会导致用户无法使用服务。因此，保证系统的可用性也是重要的安全需求。2017 年的 Equifax 数据泄露事件。这次事件导致了约 1.43 亿人的个人身份信息泄露，包括社会安全号码、出生日期、地址等重要信息。在这个事件中，相关系统需要满足以下三个安全需求：

保密性需求：保护个人身份信息不被未经授权的人访问和披露。安全目标：确保系统只有授权用户才能访问个人身份信息。

安全等级：机密性等级

理由：个人身份信息是敏感数据，一旦被未经授权的人访问和披露，将会对个人造成严重的损害。因此，保证个人身份信息的保密性至关重要，需要对系统进行机密性保护。

完整性需求：防止个人身份信息被恶意篡改或损坏。安全目标：确保个人身份信息在传输和存储过程中不被篡改或损坏。

安全等级：完整性等级

理由：如果攻击者能够篡改或损坏个人身份信息，将会对用户造成不可挽回的损失。因此，保障个人身份信息的完整性也是至关重要的。

可用性需求：确保系统能够及时、可靠地响应用户请求。安全目标：确保系统的可用性，防止拒绝服务攻击。

安全等级：可用性等级

理由：在处理大量用户请求时，系统容易受到拒绝服务攻击的影响。如果系统无法及时响应用户请求，将会导致用户无法使用服务。因此，保证系统的可用性也是重要的安全需求。