应用程序和微服务架构中实施安全性

描述主要关于计算机系统中的安全性，特别是如何在单体应用程序和微服务架构中实施安全性。它详细说明了用户如何与这些系统交互、身份验证如何进行、会话管理、安全上下文如何在系统中传递、以及如何保护资源和资产免受未经授权的访问。

具体来说，描述了以下几个方面：

用户与系统的交互：用户如何通过加密通道（如 TLS）向系统发送请求，以及系统如何验证用户的身份。

身份验证和授权：介绍了使用密码或其他身份验证因素来验证用户身份的过程，以及通过 OAuth 等标准在 API 网关中执行身份验证的方法。

会话管理：在用户成功验证后，如何在系统中管理会话，以及如何在微服务架构中共享安全上下文。

令牌的使用：解释了如何在微服务之间传递身份验证和授权信息，通常通过 JWT（JSON Web Tokens）或 Paseto 等令牌。

访问控制和审计：如何限制用户对资源的访问，并通过不可修改的访问日志来跟踪用户活动，以便进行审计。

速率限制和配额管理：如何防止拒绝服务攻击并确保合法用户的可用性，通常通过定义和执行配额来实现。

安全目标和威胁评估：强调了在为应用程序设计安全性时需要

考虑的不同方面，包括要保护的资产、安全目标（如机密性、完整性和可用性），以及系统运行的环境和存在的具体威胁。

信任边界：提到了信任边界的概念，即程序的数据或执行改变其信任级别的边界，这是系统安全性的一个重要方面。

综上所述，上述描述主要关注计算机系统中安全性的实施和管理，特别是在单体应用程序和微服务架构中。它详细说明了身份验证、授权、会话管理、令牌使用、访问控制、审计、速率限制、安全目标和威胁评估等方面的内容。