|  |
| --- |
| XX银行手机银行登录安全设计咨询方案 |
|  |
|  |

目录

[1 简介 3](#_Toc11350768)

[1.1 文档目的 3](#_Toc11350769)

[1.2 文档范围 3](#_Toc11350770)

[1.3 目标对象 3](#_Toc11350771)

[2 手机银行登录场景业务流程 3](#_Toc11350772)

[3 手机银行登录场景威胁建模 4](#_Toc11350773)

[3.1 安全假设 6](#_Toc11350774)

[3.2 威胁分析 6](#_Toc11350775)

1. 分发控制

|  |  |  |
| --- | --- | --- |
| **读者** | **文档权限** | **说明** |
| 项目组成员 | 只读 |  |
| 项目经理 | 可修改 |  |

1. 文件版本信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **变更描述** | **日期** | **作者** | **批准** |
| V0.1 | 创建文档 |  |  |  |
|  |  |  |  |  |

1. 文件版本信息说明

文件版本信息记录本文件提交时的当前有效的版本控制信息，当前版本文件有效期将在新版本文档生效时自动结束。文件版本小于1.0 时，表示该版本文件为草案，仅可作为参照资料之目的。

1. 文档签字确认

安全负责人：

项目经理：

# 简介

## 文档目的

本文档针对XX银行手机银行的登录场景在架构设计阶段可能存在的安全风险及威胁，给出登录的架构安全设计咨询方案。

## 文档范围

本文档只涉及XX银行手机银行的登录场景。

## 目标对象

本文档主要的目标对象有：系统的架构设计人员、开发人员、测试人员、安全人员、以及相关的管理人员等。

# 手机银行登录场景业务流程

手机银行登录功能提供对访问手机银行的用户的身份验证，登录功能的安全能力对系统非常重要。经过调研了解，登录场景的数据流转情况如下。



详细的业务数据流程描述如下：

1. 用户打开手机银行APP，并在登录页面中输入用户的手机号和密码；
2. 手机银行APP获取手机的verifycode，并和用户输入的手机号、密码一起提交给手机银行服务器端；
3. 手机银行服务端通过手机号查询数据库的用户信息表，查询其对应的custid；
4. 手机银行服务端将custid和用户输的密码发送到安保系统进行认证；
5. 安保系统返回身份认证结果给手机银行服务端；
6. 手机银行服务端查询数据库的设备表，查询是否有APP提交的verifycode记录；若没有则提示要进行短信验证码校验；
7. 手机银行服务端生成登录会话，返回登录结果给APP；
8. 手机银行APP展示相应页面。

# 手机银行登录场景威胁建模

威胁建模是基于值得保护的具有有价值资产之系统与组织。这些资产具有明确的弱点，而内部或外部的威胁能使之曝露出来并造成资产的损失。威胁模型分析亦能用来寻找合适的对抗方式，以降低可能的威胁。

STRIDE模型是比较常用的威胁建模方法，它将威胁分为六大类，包括如下：

* 欺骗身份（Spoofing identity），欺骗意味着模拟其他用户访问系统。非法访问并使用其他用户的身份验证信息（例如用户名和密码）就属于身份欺骗。
* 篡改数据（Tampering with data），数据篡改包括对数据的恶意修改。包括未经授权更改永久数据（例如数据库中保存的数据）以及更改通过开放网络（例如 Internet）在两台计算机之间传输的数据。
* 否认（Repudiation），否认威胁是指用户在实施了某项操作后拒绝承认此操作是自己完成的。例如，用户在缺乏跟踪被禁止的操作的能力的系统中执行非法操作。
* 信息泄露（Information disclosure），信息泄漏威胁包括将信息泄漏给不应访问这些信息的个人。例如，用户能够读取未曾授予访问权限的文件，或者入侵者能够读取在两台计算机之间传输的数据。
* 拒绝服务（Denial of service），拒绝服务 (DoS) 攻击会造成有效用户的服务丢失。例如，使 Web 服务器暂时不可用或无法使用。必须避免受到特定类型的 DoS 威胁，以提高系统的可用性和可靠性。
* 权限提升（Elevation of privilege），在这种威胁中，无特权的用户获得特权，因此可以通过访问来威胁或破坏整个系统。权限提升威胁包括攻击者有效地穿过所有系统防御体系，已成为受信任系统本身的一部分。

本文档将对整个登录数据流分析为基础，分析数据流及其关联的资产信息是否容易受到任何S、T、R、I、D和E类威胁的攻击，以此构建手机银行登录流程的威胁模型。

## 安全假设

假设手机银行登录场景都满足其声称的描述。

## 威胁分析

对手机银行的登录场景进行威胁分析，并针对分析到的威胁确定对应的安全控制措施，结果如下：

|  |  |  |
| --- | --- | --- |
| 威胁 | 服务端威胁描述 | 客户端威胁描述 |
| S欺骗身份 | S1使用其他用户的手机号和密码进行登录 |  |
| S2暴力猜测其他用户的登录手机号和密码并登录 |  |
| S3冒充安保系统 |  |
| T篡改数据 |  | T1篡改APP程序中登录访问的地址 |
| T2篡改APP端发送到服务端的登录数据 |  |
| T3篡改安保系统发送到手机银行的数据 |  |
| R否认 | R1用户否认是其本人登录的手机银行 |  |
| R2安保系统否认手机银行与其进行交互 |  |
| I信息泄露 |  | I1反编译APP程序获得其中的登录相关信息 |
|  | I2恶意程序通过记录键盘操作获得登录手机号和密码信息 |
|  | I3恶意程序通过截屏获得登录手机号和密码信息 |
|  | I4恶意程序获得APP程序中的其它敏感信息 |
| I5APP程序传输登录信息到服务端过程中信息泄露 |  |
| I6手机银行数据库中的登录相关信息泄露 |  |
| I7服务器端与安保系统传输的登录密码等信息泄露 |  |
| I8登录失败提示信息泄露具体错误信息 |  |
| I9系统程序异常或错误泄露系统内部信息 |  |
| D拒绝服务 | D1大量的并发登录请求导致登录拒绝服务 |  |
| D2多次尝试登录导致账号被锁定 |  |
| D3畸形的数据查询导致系统拒绝服务 |  |
| E权限提升 | E1绕过登录认证控制直接访问手机银行业务 |  |