ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

移动互联网第三方应用服务器安全技术要求

Security requirements for third-party application servers in mobile Internet

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：中国信息通信研究院、中国电信广东研究院、北京邮电大学

本标准主要起草人：陈泓汲、潘娟、落红卫、金华敏、徐国爱

引　言

移动互联网第三方应用服务器是支撑移动互联网应用业务功能的各类后台服务器（不包括应用商店）的统称。随着移动互联网应用对在线服务的依赖程度逐渐加深，第三方应用服务器的重要程度也与日俱增，如果其中存在安全问题，轻则致使大量用户无法正常使用移动互联网应用提供的各类业务，重则可能导致用户个人信息遭到大规模泄露等安全风险。本标准的目的是对移动互联网第三方应用服务器提出明确的安全要求，其意义是通过规范第三方应用服务器来完善整个移动互联网的安全架构，确保用户权益不受损害，维护产业有序健康发展。

移动互联网第三方应用服务器安全技术要求

1 范围

本标准对移动互联网第三方应用服务器进行资产分类，规范第三方应用服务器的安全技术目标和安全体系架构，依据第三方应用服务器安全技术框架规范具体安全技术要求。

本标准适用于支持移动应用业务功能的各类后台服务器（不包括应用商店）的开发、运行、管理和维护。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
GB/T 20272-2006 信息安全技术 操作系统安全技术要求

3 术语、定义和缩略语

3.1 术语和定义

3.1.1

移动互联网第三方应用服务器 Third-party Mobile Application Servers
支撑移动互联网应用业务功能的各类后台服务器（不包括应用商店）。

3.2 缩略语

下列缩略语适用于本文件。

CPU	Central Processing Unit	中央处理单元
CVV	Card Verification Value	卡片验证码
HTTPS	Hypertext Transfer Protocol Secure	安全超文本传输协议
I/O	Input/output	输入/输出
IMEI	International Mobile Equipment Identity	国际移动设备识别码
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
IP	Internet Protocol	网际协议
MAC	Media Access Control	媒体访问控制
SNMP	Simple Network Management Protocol	简单网络管理协议
SQL	Structured Query Language	结构化查询语言

SSH	Secure Shell	安全外壳协议
TLS	Transport Layer Security	传输层安全
VPN	Virtual Private Network	虚拟专用网
WLAN	Wireless Local Area Network	无线局域网
XSS	Cross-site Scripting	跨站脚本攻击

4 资产分类

4.1 物理资产

移动互联网第三方应用服务器的物理资产主要指构成服务器实体的物理硬件设备，包括但不限于：

- 系统硬件：第三方应用服务器的系统硬件设备，如CPU、内存、硬盘等。

4.2 系统资产

移动互联网第三方应用服务器的系统资产主要指支撑服务器业务正常运行的基础软资源，包括但不限于：

- 操作系统：第三方应用服务器上运行的、用于实现对系统软硬件资源的管理、并且向上层应用提供系统调用接口的软件程序，如内核、驱动程序、软件库、系统工具等；
- 中间件：为在线应用支持软件提供数据存取、运行时环境和外部网络界面等服务的支撑性软件，通常使用成品软件直接搭建，并且与在线应用支持软件紧密集成，如数据库软件、Web服务器等。

4.3 业务资产

移动互联网第三方应用服务器的业务资产主要指用于提供服务器各项业务功能的软件资源，包括但不限于：

- 在线业务支持软件：为在线移动业务提供联网服务支撑、实现第三方应用服务器业务逻辑的软件系统，通常由第三方应用服务器的运营者根据业务功能的要求而自主开发。

4.4 数据资产

移动互联网第三方应用服务器的用户数据资产主要指服务器上存储的、由移动应用用户提供或与用户相关的数据资源，包括但不限于：

- 账户信息：与特定的用户账户相关联、仅限于该用户访问或适用于该用户的信息，如登录账户的用户名和口令、账户内的选项设置等；
- 通信信息：用户用于发起通信以及在通信过程中产生的信息，如通信录、通话记录、电子邮件、即时通信消息等；
- 位置信息：反映用户当前位置或活动轨迹的信息，如卫星定位信息、小区基站位置信息、WLAN接入点位置信息、IP归属地信息等；
- 支付信息：与用户的支付活动有关的信息，如借记卡和信用卡账号、信用卡CVV码、有效期等；
- 设备信息：可区分和识别终端设备的标识信息，如IMEI号、IMSI号、无线网卡MAC地址等。

5 安全框架

根据移动互联网第三方应用服务器的安全目标，并结合安全风险分析，可确定第三方应用服务器的安全框架，如图1所示。

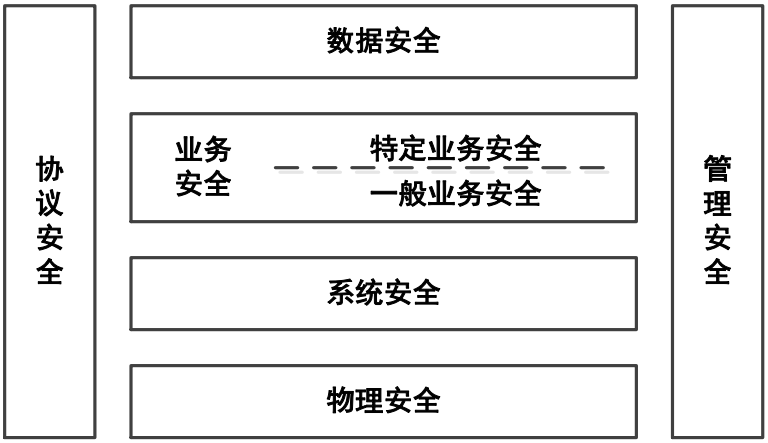

图1　安全框架

6　数据安全

6.1　数据本身安全

——移动互联网第三方应用服务器应对存储的用户数据进行完整性保护。应根据对用户数据完整性保护要求不同分为完整性检测和完整性检测恢复。

——移动互联网第三方应用服务器应对存储的用户数据进行保密性保护。应根据不同数据类型的不同保密性要求，进行不同程度的保密性保护，确保除具有访问权限的合法用户外，其余任何用户不能获得该数据。

——移动互联网第三方应用服务器已经删除数据不可恢复。移动互联网第三方应用服务器应采用专门的方法对已删除数据进行彻底清除。

6.2　数据防护安全

——移动互联网第三方应用服务器应支持数据访问鉴别，只有鉴别成功的用户或者系统可以访问相应数据。

——移动互联网第三方应用服务器应支持通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全。

——移动互联网第三方应用服务器应定期地或按某种条件实施数据备份，备份方式包括并不限于如下方式：人工数据备份、增量数据备份、局部数据备份和全系统备份。备份要求应符合 GB/T 20271-2006 《信息安全技术 信息系统通用安全技术要求》的“4.2.6 备份与故障恢复”的要求。

——移动互联网第三方应用服务器应依据不同备份方式支持相应恢复能力。

7　业务安全

7.1　业务安全构成

移动互联网第三方应用服务器业务安全要求包括两个部分：通用业务安全要求和特定业务安全要求。前者适用于所有业务类型的第三方应用服务器，而后者则对提供某些特定业务的第三方应用服务器提出附加要求。

7.2 一般业务安全要求

——移动互联网第三方应用服务器在处理用户登录请求时，若短时间内连续出现多次登录失败的情况，则应要求用户输入验证码，并且限制重试登录的速率。

——移动互联网第三方应用服务器在存储用户登录凭据时，不应直接存储口令原文，而应保存口令添加盐值后的散列值，其中散列算法应选用当前通用的、尚未发现存在安全缺陷的成熟算法，并且盐值的取值空间应足够大。

——移动互联网第三方应用服务器后台管理入口以及管理帐户密码不得明文保存在客户端代码中。

——移动互联网第三方应用服务器不得向客户端推送含恶意代码。

——移动互联网第三方应用服务器在处理移动应用客户端发来的数据时，应对数据的有效性进行验证，过滤其中可能导致安全问题的内容，以防范诸如 SQL 注入及 XSS 等形式的网络攻击。

——移动互联网第三方应用服务器应采取会话保护措施保障与应用软件之间的会话不可被窃听、篡改、伪造、重放等。

7.3 特定业务安全要求

7.3.1 支付业务

——移动互联网第三方应用服务器在提供支付业务时，应使用支付行业相关标准中规定的加密算法和密钥强度，确保支付信息在网络传输过程中的安全。

——移动互联网第三方应用服务器在处理支付交易时，除支付网关外，不应向任何其它服务器传输用户提交的支付信息。

——移动互联网第三方应用服务器在处理支付交易时，不应以任何持久性的方式存储用户提交的支付信息，包括但不限于数据库、数据文件、日志记录和调试记录。

——移动互联网第三方应用服务器在完成支付交易、不再需要使用用户提交的支付信息时，应使用“0”字节、“1”字节或随机字节对内存中保存相关信息的数据结构进行填充处理。

7.3.2 推送业务

——移动互联网第三方应用服务器在提供推送业务时，应采取适当的技术措施对其推送内容直接指向的网络链接的安全性进行审核，避免推送可将用户定向到恶意应用安装包下载地址、含有攻击代码的网站以及钓鱼网站的内容。

7.3.3 广告业务

——移动互联网第三方应用服务器在提供广告业务时，应采取适当的技术措施对其投放内容直接指向的网络链接的安全性进行审核，避免投放可将用户定向到恶意应用安装包下载地址、含有攻击代码的网站以及钓鱼网站的广告内容。

——移动互联网第三方应用服务器在提供广告业务时，在未向用户明确提示并获授权的情况下，不应借助移动应用客户端从用户设备中收集个人信息，包括但不限于通信信息、位置信息和设备信息。

——移动互联网第三方应用服务器在提供广告业务时，只有当其移动应用客户端在前台运行时，方

可向终端投放更新的广告内容。

7.3.4 即时通信业务

——移动互联网第三方应用服务器在提供即时通信业务时，应采取适当的加密措施，确保即时消息在网络传输过程中的安全。

——移动互联网第三方应用服务器在提供即时通信业务时，应采取适当的技术措施对文字消息中包含的网络链接的安全性进行审核。若发现其指向恶意应用安装包下载地址、含有攻击代码的网站以及钓鱼网站，则应提醒信息接收者潜在的安全风险。

——移动互联网第三方应用服务器在提供即时通信业务时，应采取适当的技术措施对用户传输的文件进行安全扫描。若发现文件中含有恶意代码，则应阻止文件的传输和接收。

8 系统安全

8.1 操作系统安全

——移动互联网第三方应用服务器应符合 GB/T 20272-2006 《信息安全技术 操作系统安全技术要求》的“4.1.1.1 身份鉴别”的要求。

——移动互联网第三方应用服务器应加强对操作系统用户账户的管理，禁用或删除所有对于业务应用正常运行所非必须的账户，并且为启用的账户设置适当的密码复杂性策略，防止使用空口令或弱口令。

——移动互联网第三方应用服务器上运行的操作系统应关闭所有对于业务应用正常运行所非必须的、外部可访问的端口、共享和服务。

——移动互联网第三方应用服务器应配置操作系统的访问控制策略，如文件系统权限、进程沙箱等，将中间件可访问的系统资源限制在最少够用的范围内，并且在不同的中间件进程之间实现隔离。

——移动互联网第三方应用服务器应通过升级操作系统版本或安装安全更新等方式及时修复操作系统中存在的安全漏洞。对于因软件版本依赖等特殊原因无法升级系统或安装更新的情况，应采取特定措施避免相关安全漏洞被恶意利用。

——移动互联网第三方应用服务器应部署安全防护软件或设备，包括但不限于防病毒软件、防火墙、入侵检测系统和入侵防御系统。恶意代码防护应符合 GB/T 20271-2006 《信息安全技术 信息系统通用安全技术要求》的“4.2.7 恶意代码防护”的要求。

8.2 中间件安全

——移动互联网第三方应用服务器应加强对中间件用户账户的管理，禁用或删除所有对于业务应用正常运行所非必须的账户，并且为启用的账户设置适当的密码复杂性策略，防止使用空口令或弱口令。

——移动互联网第三方应用服务器上运行的中间件应关闭所有对于业务应用正常运行所非必须的、外部可访问的端口和服务。

——移动互联网第三方应用服务器应配置中间件的访问控制策略，将在线应用支持软件可访问的系统资源限制在最少够用的范围内，并且在不同的在线应用支持软件（如果存在多个）之间实现隔离。

——移动互联网第三方应用服务器应通过升级软件版本或安装安全更新等方式及时修复中间件中存在的安全漏洞。对于因软件版本依赖等特殊原因无法升级系统或安装更新的情况，应采取适

当措施避免相关安全漏洞被恶意利用。

——移动互联网第三方应用服务器应删除中间件软件默认安装的、对于业务应用正常运行所非必须的组件和数据，包括但不限于工具软件、用户文档、测试文件和示例数据。

——移动互联网第三方应用服务器应修改中间件的默认配置，从中间件向网络返回的信息（如banner 信息和错误信息）中移除有关中间件软件版本、配置选项和运行状态的内容。

9 物理安全

9.1 设备安全

——移动互联网第三方应用服务器至少应具备一条独立于主电源的备用电源，以便在主电源发生故障时维持服务器的正常运行。推荐使用不间断电源作为备用电源。

——移动互联网第三方应用服务器应提供可靠的运行支持，并通过容错和故障恢复等措施，支持信息系统实现不间断运行。

——移动互联网第三方应用服务器宜采用冗余备份的方式确保服务器设备的可靠性。常见的服务器冗余备份方式有双机热备份等；常见的存储设备冗余备份的方式有磁盘冗余阵列等。

10 协议安全

10.1 标准协议安全

——移动互联网第三方应用服务器宜使用业界标准的网络安全协议（如 TLS）与移动应用客户端进行通信，以实现客户端对服务器的身份认证和通信数据的加密传输。

——移动互联网第三方应用服务器使用标准协议与移动应用客户端进行通信时，宜使用相应协议最新的修订版本，并且禁用存在已知安全缺陷的协议版本。

10.2 私有协议安全

——移动互联网第三方应用服务器使用私有协议与移动应用客户端进行通信时，宜支持客户端对本服务器的身份进行认证。

——移动互联网第三方应用服务器使用私有协议与移动应用客户端进行通信时，宜使用加密方式保护本服务器与客户端之间传输的、用于实现用户身份认证的数据，推荐在用户会话的整个过程中采用加密方式传输数据。

11 管理安全

11.1 安全运维

——移动互联网第三方应用服务器应配备足够强的访问控制机制对服务器的管理端口进行保护。建议将服务器配置为仅允许通过控制台进行管理，或仅允许通过内网进行管理。对于提供互联网管理端口的服务器，建议使用安全的网络管理协议，如 SSH、HTPPS 或 SNMPv2/v3 等协议进行远程管理。

——安全审计移动互联网第三方应用服务器的运营者应定期对服务器进行安全漏洞扫描和渗透测试，对于在检测中发现的安全问题应及时修复。

——移动互联网第三方应用服务器未明确提示用户或未经用户许可,任何情况下不得恶意控制用户移动智能终端。

——移动互联网第三方应用服务器应对网络资源的使用进行限制，如设置网络带宽、服务器主机资源的最大使用限度。

——移动互联网第三方服务器不得存放、处理、推送涉黄、涉政、违法或没有版权的文本、图片、视频、音频等信息。

11.2 安全审计

——安全审计移动互联网第三方应用服务器的运营者应定期对服务器进行安全漏洞扫描和渗透测试，对于在检测中发现的安全问题应及时修复。

——移动互联网第三方应用服务器应为系统运行状况留存日志,必要时可使用专用的日志服务器保存日志信息，以防止服务器遭受攻击后日志被篡改。服务器的运营者应定期对日志进行安全审计，及时发现并调查日志中的异常事件。

——移动互联网第三方应用服务器至少应留存三种类型的日志信息：

- 操作日志：操作日志用于记录服务器管理员对服务器进行管理维护时执行的相关操作，其中至少应包括时间、登录方式、发起登录的地址和操作类型四个字段；
- 系统日志：系统日志用于记录服务器操作系统及中间件运行过程中所发生的事件，其中至少应包括产生日志的程序模块名称、严重性、时间、主机名/IP、进程名称、进程 ID 和正文七个字段；
- 应用日志：应用日志用于记录在线应用支持软件运行过程中所发生的事件，其中至少应包括时间、在线应用支持软件名称、严重性和正文四个字段。

附 录 A
（资料性附录）
安全风险分析

A.1 风险概述

移动互联网第三方应用服务器主要面临的安全风险包括：系统风险、用户风险和管理风险。

A.2 系统风险

移动互联网第三方应用服务器的系统风险是指系统软硬件无法提供正常服务而引发的安全风险，具体包括：

- 自身安全：在服务器托管的机房管理不善的情况下，服务器硬件容易遭受物理损坏或篡改；另外，由于第三方应用服务器通常可通过互联网连接，因此也容易遭受来自外部网络的攻击，导致系统破坏；
- 应用瘫痪：当用户数量较大、在线应用支持软件和服务器软件难以处理大量并发连接时，会发生无法正常提供应用支撑的情况，产生拒绝服务的风险。

A.3 用户风险

移动互联网第三方应用服务器的用户风险是指由于服务器的安全性遭破坏而给移动应用的用户所带来的连带风险，具体包括：

- 用户依赖：在服务器遭受攻击而瘫痪的情况下，大量用户将无法正常使用移动互联网应用提供的各类业务，从而带来用户依赖的风险。此类风险的大小与具体业务类型紧密相关，通常来说，即时通信和移动金融类业务往往具有较高的用户依赖风险；
- 隐私窃取：在提供移动互联网业务的过程中，第三方应用服务器可以获得用户账户数据、位置数据、金融数据、环境数据、传感数据等隐私信息。对于攻击者来说，通过服务器来获取大量用户的隐私信息是一种更加快捷和方便的途径，这就使服务器面临严重的隐私窃取风险；
- 资费消耗：用户往往通过移动蜂窝网络来访问移动互联网服务，而服务提供商也常使用短信通道收取增值服务费用。在这种情况下，第三方应用服务器就有可能通过流量消耗或恶意扣费而导致用户资费损失；
- 远程控制：移动终端通过使用移动互联网服务而与第三方应用服务器之间建立了紧密的绑定关系，这就使服务器有可能通过网络向移动终端发送恶意指令，导致终端操作系统和应用软件被远程控制。

A.4 管理风险

移动互联网第三方应用服务器的管理风险是指由于移动互联网业务的多样性和灵活性而给安全管理带来的风险，具体包括：

- 私有协议：出于保障通信安全、提高数据传输效率等因素的考虑，第三方应用服务器与移动应用通信时往往采用内部协议，并使用私有加密和压缩算法，难以进行识别和监管；

- 管理复杂：不同于位置固定的PC终端，移动互联网终端可随时随地接入网络与第三方应用服务器建立通信，不易管理；
- 溯源困难：移动终端总处于移动状态，位置信息和地址信息频繁改变，不利于确定位置。

参 考 文 献

GB/T 18336.1-2008 信息技术 安全技术 信息技术安全性评估准则 第1部分 简介和一般模型
GB/T 18336.2-2008 信息技术 安全技术 信息技术安全性评估准则 第2部分 安全功能要求
GB/T 18336.3-2008 信息技术 安全技术 信息技术安全性评估准则 第3部分 安全保证要求
GB/T 20270-2006 信息安全技术 网络基础安全技术要求
GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求
GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南
GB/T 25058-2010 信息安全技术 信息系统安全等级保护实施指南
GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求
GB/T 28448-2012 国家信息系统安全等级保护测评准则
GB/T 28452-2012 信息安全技术 应用软件系统通用安全技术要求