

中华人民共和国通信行业标准

YD/T 2694-2014

移动互联网联网应用安全防护要求

Security Protection Requirements for
Networked Application over Mobile Internet

2014-10-14 发布

2014-10-14 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	3
4 移动互联网应用安全防护概述	3
4.1 移动互联网应用安全防护范围	3
4.2 移动互联网应用安全风险分析	4
4.3 移动互联网应用安全防护内容	4
5 移动互联网应用安全防护要求	5
5.1 第 1 级要求	5
5.2 第 2 级要求	5
5.3 第 3 级要求	10
5.4 第 4 级要求	13
5.5 第 5 级要求	13
附录 A (规范性附录) 移动互联网应用风险分析	14

前 言

本标准是“电信网和互联网安全防护体系”系列标准之一。该系列标准预计结构及名称如下：

1. 《电信网和互联网安全防护管理指南》
2. 《电信网和互联网安全等级保护实施指南》
3. 《电信网和互联网安全风险评估实施指南》
4. 《电信网和互联网灾难备份及恢复实施指南》
5. 《固定通信网安全防护要求》
6. 《移动通信网安全防护要求》
7. 《互联网安全防护要求》
8. 《增值业务网—消息网安全防护要求》
9. 《增值业务网—智能网安全防护要求》
10. 《接入网安全防护要求》
11. 《传送网安全防护要求》
12. 《IP承载网安全防护要求》
13. 《信令网安全防护要求》
14. 《同步网安全防护要求》
15. 《支撑网安全防护要求》
16. 《非核心生产单元安全防护要求》
17. 《电信网和互联网物理环境安全等级保护要求》
18. 《电信网和互联网管理安全等级保护要求》
19. 《固定通信网安全防护检测要求》
20. 《移动通信网安全防护检测要求》
21. 《互联网安全防护检测要求》
22. 《增值业务网—消息网安全防护检测要求》
23. 《增值业务网—智能网安全防护检测要求》
24. 《接入网安全防护检测要求》
25. 《传送网安全防护检测要求》
26. 《IP承载网安全防护检测要求》
27. 《信令网安全防护检测要求》
28. 《同步网安全防护检测要求》
29. 《支撑网安全防护检测要求》
30. 《非核心生产单元安全防护检测要求》
31. 《电信网和互联网物理环境安全等级保护检测要求》
32. 《电信网和互联网管理安全等级保护检测要求》
33. 《域名系统安全防护要求》

34. 《域名系统安全防护检测要求》
35. 《网上营业厅安全防护要求》
36. 《网上营业厅安全防护检测要求》
37. 《WAP网关系统安全防护要求》
38. 《WAP网关系统安全防护检测要求》
39. 《电信网和互联网信息服务业务系统安全防护要求》
40. 《电信网和互联网信息服务业务系统安全防护检测要求》
41. 《增值业务网 即时消息业务系统安全防护要求》
42. 《增值业务网 即时消息业务系统安全防护检测要求》
43. 《域名注册系统安全防护要求》
44. 《域名注册系统安全防护检测要求》
45. 《移动互联网应用商店安全防护要求》
46. 《移动互联网应用商店安全防护检测要求》
47. 《互联网内容分发网络安全防护要求》
48. 《互联网内容分发网络安全防护检测要求》
49. 《互联网数据中心安全防护要求》
50. 《互联网数据中心安全防护检测要求》
51. 《移动互联网应用安全防护要求》(本标准)
52. 《移动互联网应用安全防护检测要求》
53. 《公众无线局域网安全防护要求》
54. 《公众无线局域网安全防护检测要求》
55. 《电信网和互联网安全防护基线配置要求及检测要求 网络设备》
56. 《电信网和互联网安全防护基线配置要求及检测要求 安全设备》
57. 《电信网和互联网安全防护基线配置要求及检测要求 操作系统》
58. 《电信网和互联网安全防护基线配置要求及检测要求 数据库》
59. 《电信网和互联网安全防护基线配置要求及检测要求 中间件》
60. 《电信网和互联网安全防护基线配置要求及检测要求 web应用系统》
61. 《电信和互联网用户个人信息保护通用技术要求和管埋要求》
62. 《电信和互联网用户个人信息保护检测要求》

本标准与YD/T 2695—2014《移动互联网应用安全防护检测要求》配套使用。

随着电信网和互联网的发展,将不断补充和完善电信网和互联网安全防护体系的相关标准。

本标准按照GB/T1.1-2009给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位:工业和信息化部电信研究院、中国电信集团公司、中国移动通信集团公司、深圳腾讯计算机系统有限公司、北京新浪互联信息服务有限公司。

本标准主要起草人:封莎、崔涛、许子先、魏薇、张彦超、杨丁宁、杨正军、王新峰、陈军、杨晓光、陈洋、龚雪、许章毅。

移动互联网应用安全防护要求

1 范围

本标准规定了移动互联网应用相关的业务系统分安全保护等级的安全防护要求，涉及到业务及应用安全、网络安全、设备及软件系统安全、物理安全和管理安全。

本标准适用于移动互联网应用相关业务系统。

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。

YD/T 1754-2008	《电信网和互联网物理环境安全防护要求》	
YD/T 1756-2008	《电信网和互联网管理安全防护要求》	
YD/T 1734-2009	《移动通信网安全防护要求》	
YD/T 2052-2009	《域名系统安全防护要求》	
YD/T 2587-2013	《移动互联网应用商店安全防护要求》	
YD/T 2439-2012	《移动互联网恶意程序描述格式》	
YD/T 2584-2013	《互联网数据中心安全防护要求》	
YD/T 2589-2013	《互联网内容分发网络安全防护要求》	
YD/T 2698-2014	《电信网和互联网安全防护基线配置要求及检测要求	网络设备》
YD/T 2699-2004	《电信网和互联网安全防护基线配置要求及检测要求	安全设备》
YD/T 2701-2014	《电信网和互联网安全防护基线配置要求及检测要求	操作系统》
YD/T 2670-2014	《电信网和互联网安全防护基线配置要求及检测要求	数据库》
YD/T 2702-2014	《电信网和互联网安全防护基线配置要求及检测要求	中间件》

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

移动互联网应用安全等级 Security Classification of Networked Application Over Mobile Internet

移动互联网应用重要程度的表征。重要程度从移动互联网应用受到破坏后，对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害来衡量。

3.1.2

移动互联网应用安全等级保护 Classified Security Protection of Networked Application Over Mobile Internet

对移动互联网应用分等级实施安全保护。

3.1.3

移动互联网应用安全风险 Security Risk of Networked Application Over Mobile Internet

人为或自然的威胁可能利用移动互联网应用存在的脆弱性导致安全事件的发生及造成的影响。

3.1.4

移动互联网应用资产 Asset of Networked Application Over Mobile Internet

移动互联网应用具有价值的资源，是安全防护体系保护的對象。移动互联网应用的资产可能以多种形式存在，无形的、有形的、硬件、软件，包括客户端软件、后台系统及操作维护终端硬件及相关软件、关键数据等各种类型的资源。

3.1.5

移动互联网应用威胁 Threat of Networked Application Over Mobile Internet

可能导致对移动互联网应用产生危害的不希望事故潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。

3.1.6

移动互联网应用脆弱性 Vulnerability of Networked Application Over Mobile Internet

移动互联网应用的资产中存在的弱点、缺陷与不足，不直接对移动互联网应用资产造成危害，但可能被移动互联网应用威胁所利用从而危害移动互联网应用资产的安全。

3.1.7

移动互联网应用灾难 Disaster of Networked Application Over Mobile Internet

由于各种原因，造成移动互联网应用故障或瘫痪，使移动互联网应用支持的业务功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.1.8

移动互联网应用灾难备份 Backup for Disaster Recovery of Networked Application Over Mobile Internet

为了移动互联网应用灾难恢复而对相关网络要素进行备份的过程。

3.1.9

移动互联网应用灾难恢复 Disaster Recovery of Networked Application Over Mobile Internet

为了将移动互联网应用从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

3.1.10

移动互联网应用安全评测 Security Testing of Networked Application Over Mobile Internet

对移动互联网应用的安全保护能力是否达到相应安全等级的安全防护要求进行衡量。

3.1.11

原生应用 Native Application

使用C、Java等编程语言编写的，运行于移动通信终端操作系统的应用软件。

3.1.12

Web应用 Web Application

使用HTML5等Web语言编写的，运行于移动通信终端浏览器等Web运行环境中的应用软件。

3.1.13

会话 Session

在客户端和服务端之间创建关联，从而起到交换数据包作用的机制。

3.2 缩略语

下列缩略语适用于本文件。

DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Service	拒绝服务
DNS	Domain Name System	域名系统
HTML	HyperText Mark-up Language	超文本标记语言
SSL	Secure Sockets Layer	安全套接层协议层
TLS	Transport Layer Security	传输层加密

4 移动互联网应用安全防护概述

4.1 移动互联网应用安全防护范围

移动互联网应用泛指以移动互联网智能终端为载体，通过应用软件客户端调用后台系统功能为用户提供各种类型移动服务的应用软件及后台系统。

按照实现形式，移动互联网应用可分为原生应用和 Web 应用。原生应用是指使用 C、Java 等编程语言编写的，运行于移动通信终端操作系统的应用软件。Web 应用是指使用 HTML5 等 Web 语言编写的，运行于移动通信终端浏览器等 Web 运行环境中的应用软件。

移动互联网应用包含移动互联网应用客户端和移动互联网应用后台系统。移动互联网应用安全防护是针对联网应用客户端、联网应用后台系统以及应用客户端和后台系统在联网交互中的联网行为和交互数据进行安全防护，其系统架构如图 1 所示。

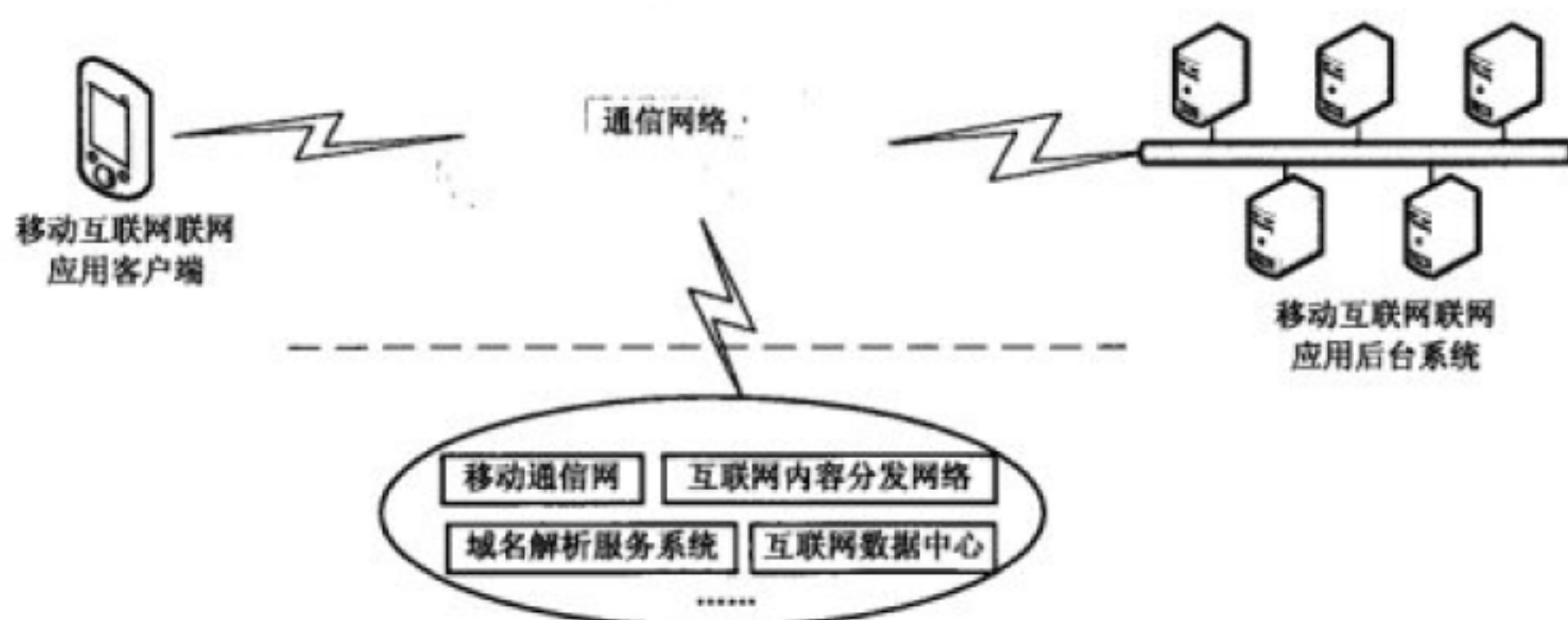


图 1 移动互联网应用系统架构

本标准主要针对移动互联网应用系统提出安全防护要求，与移动互联网应用系统相关的其他业务平台安全防护要求不属于本标准规定范畴，如移动互联网应用商店见 YD/T 2587-2013《移动互联网应用商店安全防护要求》，移动通信网见 YD/T 1734-2009《移动通信网安全防护要求》，域名解析服务系统见 YD/T 2052-2009《域名系统安全防护技术要求》，与互联网相关的互联网数据中心见 YD/T 2584-2013《互联网数据中心安全防护要求》，互联网内容分发网络见 YD/T 2589-2013《互联网内容分发网络安全防护要求》。

4.2 移动互联网应用安全风险分析

移动互联网应用的重要资产至少应包括：

- ◆ 移动互联网应用客户端软件；
- ◆ 移动互联网应用后台系统及操作维护终端硬件及相关软件；
- ◆ 移动互联网应用关键数据，如用户身份信息、认证信息、交易信息、位置信息、联系人信息、聊天记录信息等；

移动互联网应用其他资产可见附录 A 表 A.1 对资产的分类及举例。

移动互联网应用的脆弱性可以从技术脆弱性和管理脆弱性两个方面考虑。脆弱性识别对象应以资产为核心。移动互联网应用的脆弱性分析应包括但不限于附录 A 表 A.2 所列范围。

移动互联网应用的威胁根据来源可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。移动互联网应用的威胁分析应包括但不限于附录 A 表 A.3 所列范围。

移动互联网应用可能存在的安全脆弱性被利用后会产生很大的安全风险，主要包含以下几个方面：

1) 移动互联网应用客户端软件

移动互联网应用客户端可能面临的安全风险主要包括：一是客户端信息泄露，如用户信息、系统配置信息、访问路径、位置信息等被窃取或上传至后台系统；二是恶意应用未经用户同意私自发送短信、拦截短信、拨打电话、下载软件等，造成用户信息泄露、资费损失、手机电量消耗等，或客户端软件被恶意卸载。

2) 移动互联网应用后台系统及操作维护终端硬件及相关软件

移动互联网应用后台系统及操作维护终端硬件及相关软件可能面临的安全风险主要包括：一是遭受 DDOS 攻击，导致服务器运行故障或宕机；二是系统被入侵，导致大量用户信息泄露，系统瘫痪等。

3) 移动互联网应用客户端与后台系统之间的数据交互

移动互联网应用客户端与后台系统之间的数据交互可能面临的安全风险主要包括：一是应用升级或联网交互时感染包含病毒、木马、恶意链接等恶意代码；二是未经用户同意上传用户通信录、聊天记录、位置信息等用户信息。

4.3 移动互联网应用安全防护内容

移动互联网应用的主要功能是为移动互联网用户提供各种类型的业务，因此保障业务的安全稳定运行和用户信息的安全可靠至关重要。保障移动互联网应用的基础设施安全、管理安全等也是安全防护的主要内容。移动互联网应用的安全防护内容具体包括：

1) 业务及应用安全

业务及应用安全包括向用户提供的相关业务及应用在实现技术、逻辑、管理和控制等方面的安全要求，主要包括业务逻辑安全、原生应用及后台系统安全、Web 应用及后台系统安全、数据安全、能力开放接口安全等。其中，业务逻辑安全从业务逻辑层面提出身份鉴别、访问控制、安全审计等方面的安全防护要求；原生应用及后台系统安全针对原生应用提出安全防护要求；Web 应用及后台系统安全针对 Web 应用提出安全防护要求；数据安全包含用户信息安全和灾难备份相关安全防护要求；能力开放接口安全针对后台系统能力开放平台提出安全防护要求。

2) 网络安全

网络安全主要包括移动互联网应用系统内部网络结构安全、入侵防范和安全审计方面的安全防护要求。其中，网络结构安全针对网络拓扑结构、子网划分等方面提出安全防护要求；入侵防范针对如何防止网络入侵提出安全防护要求；安全审计针对相关设备审计记录提出安全防护要求。

3) 设备及软件系统安全

设备及软件系统安全主要包括网络及安全设备、操作系统、数据库、中间件在身份鉴别、访问控制、安全审计、入侵防范和资源控制等方面的安全防护要求。

4) 物理安全

物理安全主要包括系统所处的物理环境在机房位置、电力供应、防火、防水、防静电、温湿度控制等方面的安全防护要求。

5) 管理安全

管理安全主要包括管理制度、人员和技术支持能力、运行维护管理能力、灾难恢复预案等方面的安全防护要求。

5 移动互联网应用安全防护要求

5.1 第1级要求

5.1.1 业务及应用安全

5.1.1.1 业务逻辑安全

a) 对提供登录功能的业务系统，应对登录用户进行身份标识和鉴别。

b) 对提供登录功能的业务系统，应提供并启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

c) 对提供登录功能的业务系统，应提供并启用用户身份标识唯一检查功能，保证系统中不存在重复用户身份标识。

d) 应由经过授权的主体配置访问控制策略，并严格限制默认用户的访问权限。

e) 应采用加密方式存储业务用户的密码信息。

5.1.2 网络安全

不作要求。

5.1.3 设备及软件系统安全

不作要求。

5.1.4 物理安全

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第1级的相关要求。

5.1.5 管理安全

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第1级的相关要求。

5.2 第2级要求

5.2.1 业务及应用安全

5.2.1.1 业务逻辑安全

除满足第1级的要求之外，还应满足：

5.2.1.1.1 身份鉴别

- a) 应提供专门的登录控制模块对登录用户进行身份标识和鉴别。
- b) 应提供并启用用户鉴别信息复杂度检查功能，保证身份鉴别信息不易被冒用。

5.2.1.1.2 访问控制

- a) 应严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。
- b) 应严格设置登录策略，按安全策略要求具备防范账户暴力破解攻击措施的能力（如，限定用户连续错误输入密码次数，超过设定阈值，对用户进行锁定，并设定锁定时间，在锁定时间内被锁定的用户需通过注册时的标志信息进行密码重新设定或者凭有效证件进行设定）。
- c) 当进行业务权限更改时（如密码重置、密码找回等），应设置相关策略，防止暴力破解攻击。
- d) 业务订购、变更、退订流程应根据实际业务需求，应采用“认证码”或“二次短信认证”等方式加强安全性，应限定同一用户每日业务订购次数。

5.2.1.1.3 安全审计

- a) 审计范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件（如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作）。
- b) 应保护审计记录，保证无法删除、修改或覆盖等。
- c) 业务相关审计记录应包括事件日期、时间、发起者信息、类型、描述和结果等。
- d) 应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能。

5.2.1.1.4 其他

- a) 当用户和业务系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话。
- b) 应能对含有恶意代码链接的信息建立发现和处理机制，防止类似信息的扩散。
- c) 软件运行时，未经用户同意，不得擅自为用户自动开启其他服务功能（如定位等）。

5.2.1.2 原生应用及后台系统安全

5.2.1.2.1 输入验证

应对输入数据做严格验证，默认所有输入都可能包含恶意信息。

5.2.1.2.2 身份认证

- a) 应确保身份认证模块不能被非法绕过。
- b) 软件的用户身份鉴别模块应对用户身份鉴别信息进行保护，防止泄露。

5.2.1.2.3 会话管理

应采取会话保护措施保障软件与后台服务器之间的会话不可被窃听、篡改、伪造、重放等。

5.2.1.2.4 数据存储

应确保软件配置信息、用户认证信息等敏感数据采用加密方式存储。

5.2.1.2.5 日志记录

- a) 后台日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件（如普通用户异常登录、发布恶意代码、异常修改账号信息等行为，以及管理员在业务功能及账号控制方面的关键操作）。

b) 应禁止在后台以及客户端日志中记录用户密码等敏感信息,如果确实需要记录敏感信息,则应进行模糊化处理。

c) 应防止日志欺骗,如果在生成后台日志时需要引入来自非受信源的数据,则需要进行严格校验,防止日志欺骗攻击。

d) 应确保后台日志数据的安全存储并严格限制日志数据的访问权限,可对后台日志记录进行签名来实现防篡改。

5.2.1.2.6 其他

a) 应用软件不应含有移动互联网恶意程序。移动互联网恶意程序的判定依据见YD/T 2439-2012的相关要求。

b) 应确保软件内存管理不存在逻辑缺陷,如未释放资源、敏感信息驻留内存等。

c) 应确保软件不非法操作与自身功能不相关的文件(如图片、通信录、其他应用软件等)。

d) 客户端软件应进行代码变量隐藏。

5.2.1.3 Web 应用及后台系统安全

5.2.1.3.1 输入验证

a) 应对输入数据(如文件路径、URL地址等)做安全验证,默认所有输入都可能包含恶意信息,并尽量使用白名单验证方法。

b) 应在服务器端进行输入验证,避免客户端输入验证被绕过。

c) 关键参数应直接从服务器端提取,避免从客户端输入,防止关键参数被篡改。

5.2.1.3.2 身份认证

a) 应禁止明文传输用户密码,可采用SSL/TLS加密隧道确保用户密码的传输安全。

b) 应禁止在数据库或文件系统中明文存储用户密码,可采用单向散列值在数据库中存储用户密码,降低存储的用户密码被字典攻击的风险。

c) 应禁止在COOKIE中保存明文用户密码。

d) 应采取措施防止暴力破解、恶意注册、恶意占用资源等行为。

e) 应对关键业务操作进行二次鉴权,例如修改用户认证鉴权信息(如密码、密码取回问题及答案、绑定手机号码等),避免用户身份被冒用。

f) 应避免认证错误提示泄露信息,在认证失败时,应向用户提供通用的错误提示信息(如不应区分是账号错误还是密码错误),避免这些错误提示信息被攻击者利用。

g) 应支持密码策略设置,从业务系统层面支持强制的密码策略,包括密码长度、复杂度、更换周期等,特别是业务系统的管理员密码。

h) 应支持账号锁定功能,系统应限制连续登录失败次数,在客户端多次尝试失败后,服务器端需要对用户账号进行短时锁定,且锁定策略支持配置解锁时长。

i) 应确保用户不能访问到未授权的功能和数据,未经授权的用户试图访问受限资源时,系统应予以拒绝或提示用户进行身份鉴权。

5.2.1.3.3 会话管理

a) 应确保会话的安全创建。在用户认证成功后,应为用户创建新的会话并释放原有会话;创建的会话标识应满足随机性和长度要求,避免被攻击者猜测;会话与IP地址可绑定,降低会话被盗用的风险。

b) 应确保会话数据的存储安全。用户登录成功后所生成的会话数据应存储在服务器端,并确保会话数据不能被非法访问;当更新会话数据时,要对数据进行严格的输入验证,避免会话数据被非法篡改。

c) 应确保会话数据的传输安全,防止泄露会话标识。

d) 应确保会话的安全终止。当用户登录成功并成功创建会话后,应在Web应用系统的各个页面提供用户登出功能,登出时应及时删除服务器端的会话数据;当处于登录状态的用户直接关闭浏览器时,需要提示用户执行安全登出或者自动为用户完成登出过程,从而安全的终止本次会话。

e) 应设置合理的会话超时阈值,在合理范围内尽可能减小会话超时阈值,可以降低会话被劫持和重复攻击的风险,超过会话超时阈值后立刻销毁会话,消除会话的信息。

f) 应限制会话并发连接数,限制同一用户的会话并发连接数,避免恶意用户创建多个并发的会话来消耗系统资源,影响业务的可用性。

g) 在涉及到关键业务操作的Web页面,应为当前Web页面生成一次性随机令牌,作为主会话标识的补充。在执行关键业务前,应确保用户提交的一次性随机令牌与服务器端保存的一次性随机令牌匹配,以避免跨站请求伪造等攻击。

5.2.1.3.4 数据存储

a) 对于不同类别的数据,比如日志记录和业务数据,应采取相应的隔离措施和安全保护措施。

b) 禁止在客户端本地存储用户敏感数据,如用户密码、身份信息等。

c) 应避免在代码中硬编码密码(即在代码中直接嵌入密码,会导致密码修改困难,甚至密码的泄露),可从配置文件载入密码。

d) 在配置文件中禁止明文存储数据库连接密码、FTP服务密码、主机密码、外部系统接口认证密码等。

5.2.1.3.5 数据传输

应确保通信信道的安全,在客户端与Web服务器之间使用并正确配置 SSL/TLS,应使用SSL 3.0/ TLS 1.0以上版本,对称加密密钥长度不少于128位,非对称加密密钥长度不少于1024位,单向散列值位数不小于128位。

5.2.1.3.6 日志记录

a) 后台日志记录范围应覆盖到每个用户的关键操作、重要行为、业务资源使用情况等重要事件。如普通用户异常登录、发布恶意代码、异常修改账号信息等行为,以及管理员在业务功能及账号控制方面的关键操作。

b) 应禁止在后台日志中记录用户密码等敏感信息,如果确实需要记录敏感信息,则应进行模糊化处理。

c) 应防止日志欺骗,如果在生成后台日志时需要引入来自非受信源的数据,则需要进行严格校验,防止日志欺骗攻击。

d) 应禁止将后台日志保存到Web目录下,确保日志数据的安全存储并严格限制日志数据的访问权限,可对日志记录进行签名来实现防篡改。

5.2.1.3.7 其他

a) 应有技术手段检测和避免Web业务系统域名、访问链路的异常、访问延迟、解析错误等情况,并有应急处理能力。

b) 应避免存在常见的Web漏洞（如SQL注入、跨站脚本、跨站请求伪造等）。

c) 应能检测挂马、暗链等Web业务系统入侵事件，并有应急处理能力。

5.2.1.4 数据安全

a) 关键设备具备一定的灾难备份和恢复能力，重要部件应采用冗余的方式提供保护。

b) 应建立对业务及应用关键数据和重要信息进行备份和恢复的管理和控制机制。

c) 关键数据（如业务数据、应用配置数据、管理员操作维护记录、用户数据信息等）应有必要的灾难备份。

5.2.1.5 能力开放接口安全

a) 业务系统应有系统平台与外部平台接口之间的安全管控措施，接口协议操作应通过接口代码审计、黑、白名单等控制措施确保交互符合接口规范。

b) 应对能力开放接口调用有认证措施。

c) 应对关键接口的调用情况进行技术监控，如调用频率、调用来源等。

d) 应用能力开放接口生成的软件在供用户下载之前应通过安全检测。

e) 应制定能力开放接口管理机制和网络安全应急管理制度。

5.2.2 网络安全

5.2.2.1 结构安全

a) 应绘制与当前运行情况相符的系统拓扑结构图。

b) 应在满足高峰期流量需求的基础上，合理设计带宽。

c) 应按照统一的管理和控制原则划分不同的子网或网段，设备依照功能划分及其重要性等因素分区部署。

d) 网络节点、链路应有足够冗余，应能对主要网络设备进行状态监控。

e) 应能按照业务需求和安全需求，合理划分安全域。

5.2.2.2 入侵防范

应在系统边界处部署防火墙等安全防御设备或技术措施，有效抵御和防范各种攻击和入侵。

5.2.2.3 安全监测

a) 应对移动互联网应用后台系统边界流量进行DDoS攻击监测，发现攻击行为在60s之内提供告警，并进行相应处置。

b) 应定期（至少每半个月）对木马后门攻击、缓冲区溢出攻击和网络蠕虫攻击等进行检测，发现攻击行为在60s之内提供告警，并进行相应处置。

c) 应对系统中的重要设备运行状况进行监测，发现异常情况（如系统宕机等）在20s之内提供告警，并进行相应处置。

d) 应对系统中的网络流量信息进行监测，发现异常情况（如达到网络链路容量的三分之二及以上）在60s之内提供告警，并进行相应处置。

e) 应对系统中的各类监测数据进行日志记录，并且保留一定期限（至少180天）。

5.2.2.4 安全审计

a) 应具备对审计记录数据进行统计、查询、分析及生成审计报表的功能。

b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

- c) 应对审计记录进行保护, 避免受到未预期的删除、修改或覆盖等。

5.2.3 设备及软件系统安全

5.2.3.1 网络及安全设备

除满足YD/T 2698-2014《电信网和互联网安全防护基线配置要求及检测要求 网络设备》和YD/T 2699-2014《电信网和互联网安全防护基线配置要求及检测要求 安全设备》的要求之外, 还应满足:

- a) 应保证主要网络设备的业务处理能力具备冗余空间, 满足业务高峰期需要。
- b) 关键网络设备、重要线路、网络设备的重要部件应采用冗余的保护方式。

5.2.3.2 操作系统

除满足YD/T 2701-2014《电信网和互联网安全防护基线配置要求及检测要求 操作系统》的要求之外, 还应满足:

5.2.3.2.1 安全审计

- a) 审计范围应覆盖到主机/服务器上的每个操作系统用户。
- b) 审计内容应包括重要操作维护用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的相关事件。
- c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。
- d) 应保护审计记录, 避免其受到未预期的删除、修改或覆盖等, 保留一定期限(至少180天)。

5.2.3.2.2 灾难备份

a) 应建立对主机关键数据(如主机配置数据、管理员操作维护记录、用户信息等)和重要信息进行备份和恢复的管理和控制机制, 相关主机数据备份范围和时间间隔、数据恢复能力应满足行业管理、业务运营企业应急预案相关要求。

5.2.3.3 数据库

应满足YD/T 2700-2014《电信网和互联网安全防护基线配置要求及检测要求 数据库》的相关要求。

5.2.3.4 中间件

应满足YD/T 2702-2014《电信网和互联网安全防护基线配置要求及检测要求 中间件》的相关要求。

5.2.4 物理安全

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第2级的相关要求。

5.2.5 管理安全

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第2级的相关要求。

5.3 第3级要求

5.3.1 业务及应用安全

5.3.1.1 业务逻辑安全

除满足第2级的要求之外, 还应满足:

5.3.1.1.1 输身份鉴别

- a) 登录验证模块应能防止身份鉴别暴力攻击(如登录模块应采用随机验证码进行验证, 并且保证验证码不易被自动预测、识别)。
- b) 加强密码复杂度要求, 应不含有常用字符组合、数字组合、键盘顺序等可预测密码组合。
- c) 应采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

5.3.1.1.2 访问控制

- a) 业务系统管理后台不应暴露在公网，管理接口通信内容不应使用明文协议。
- b) 重要服务器应使用资源强制访问控制策略（如用户、进程、文件内核级保护等）。

5.3.1.1.3 其他

- a) 应定义业务水平阈值，能够对业务及应用服务水平进行检测，并具备当服务水平降低到预先规定的阈值时进行告警的功能。
- b) 应保证系统中使用的第三方软件、运维软件无已知后门、漏洞。
- c) 应提供有效的病毒和攻击检测过滤技术手段，能够对用户之间传送的文件进行必要的安全检查和过滤。

5.3.1.2 原生应用及后台系统安全

除满足第2级的要求之外，还应满足：

- a) 客户端软件上线前或升级后应进行代码审计，形成报告，并对审计发现的问题进行代码升级完善。
- b) 如使用开源第三方应用组件及代码，应对已公开漏洞（漏洞库可参考CVE、CNVD等）及时更新补丁。

5.3.1.3 Web 应用及后台系统安全

除满足第2级的要求之外，还应满足：

- a) Web程序上线前或升级后应进行代码审计，形成报告，并对审计发现的问题进行代码升级完善；
- b) 如使用开源第三方应用组件及代码，应对已公开漏洞（漏洞库可参考CVE、CNVD等）及时更新补丁。

5.3.1.4 数据安全

除满足第2级的要求之外，还应满足：

- a) 应建立对业务及应用全部数据、信息进行备份和恢复的管理和控制机制。
- b) 业务及应用应具备较好的灾难备份和业务恢复的能力，提供重要服务的业务及应用系统应进行系统级备份，以保证其业务连续性。
- c) 重要的业务及应用相关数据应进行异地备份。
- d) 应提供数据自动保护功能，当发生故障后应保证系统能够恢复到故障前的业务状态。

5.3.1.5 能力开放接口安全

同第2级要求。

5.3.2 网络安全

5.3.2.1 结构安全

除满足第2级的要求之外，还应满足：

- a) 应避免将重要设备部署在网络边界处且直接连接外部网络/系统，重要网段与其他网段之间采取可靠的技术隔离手段。
- b) 系统应具有过负荷保护功能，确保系统在过负荷时，重要业务能正常运行。
- c) 应具备必要的流量负荷分担设计。

5.3.2.2 安全监测

除满足第2级的要求之外，还应满足：

a) 应对重要服务器进行入侵行为监测,能够记录入侵的源IP、攻击的类型、攻击的目的地址、攻击的时间,发现严重入侵事件在60s之内提供告警,并进行相应处置。

b) 应对重要服务器进行性能监测,包括服务器的CPU、硬盘、内存、网络等资源的使用情况,发现异常情况(如达到资源容量的三分之二及以上)在60s之内提供告警,并进行相应处置。

c) 应对服务器、数据库等系统的服务水平设定告警阈值并进行监测,发现服务水平降低到阈值时在60s之内提供告警,并进行相应处置。

5.3.3 设备及软件系统安全

5.3.3.1 网络及安全设备

除满足第2级的要求之外,还应满足:

a) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素,划分不同的子网或网段,并按照方便管理和控制的原则为各子网、网段分配地址段。

b) 设备应按照对业务服务的重要次序来指定带宽分配优先级别,保证在网络发生拥堵时优先保护重要主机。

c) 应定期自检(漏洞扫描、弱口令扫描、基线配置信息等),对设备的端口、弱口令、安全漏洞、木马进行扫描。

d) 重要设备、线路应采用热备份的保护方式进行保护。

5.3.3.2 操作系统

5.3.3.2.1 身份鉴别

除满足第2级的要求之外,还应满足:

a) 应采用两种或两种以上组合的鉴别技术对相关设备的管理用户进行身份鉴别。

b) 重要主机应使用安全性较高的身份鉴别措施(如数字证书等)对用户进行身份鉴别。

5.3.3.2.2 安全审计

除满足第2级的要求之外,还应满足:

a) 应能根据记录数据进行分析,并生成审计报表。

b) 应保护审计进程,避免受到未预期的中断。

5.3.3.2.3 灾难备份

除满足第2级的要求之外,还应满足:

a) 系统应具备较好的灾难备份和业务恢复能力,提供重要服务的业务及应用系统应进行系统级备份,以保证业务的连续性。

b) 应提供数据自动保护功能,当发生故障后应保证系统能够恢复到故障前的业务状态,重要的数据应进行异地备份。

5.3.3.3 数据库

同第2级要求。

5.3.3.4 中间件

同第2级要求。

5.3.4 物理安全

应满足 YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第3.1级的相关要求。

5.3.5 管理安全

应满足 YD/T 1756-2008 《电信网和互联网管理安全等级保护要求》中第 3.1 级的相关要求。

5.4 第 4 级要求

同第 3 级要求。

5.5 第 5 级要求

待补充。

附录 A
(规范性附录)

移动互联网应用风险分析

本附录指导移动互联网应用风险分析过程中的资产、脆弱性、威胁分析。

移动互联网应用的资产至少应包括：设备软硬件，重要数据，文档，人员等，如表 A.1 所示。

表A.1 资产列表

类别	主要资产
设备及链路	各类业务及应用涉及的操作维护终端、服务器和数据库，各类业务及应用相关辅助设备（如安全过滤、入侵检测和防护设备），系统内部网络设备（如，系统内部组网路由器、交换机等设备）、系统内部链路
软件	相关业务或应用软件、数据库软件、业务控制和运维管理软件等
数据和信息	保证业务正常提供的数据和信息（如业务数据、系统配置数据、管理员操作维护记录、用户信息等）
业务及应用	系统提供的相关业务和应用
文档和资料	纸质以及保存在存储介质中的各种文件资料（如设计文档、技术要求、管理规定、工作计划、技术报告、用户手册等）
人员	相关管理、维护、开发、数据备份人员等
环境和设施	业务系统和设备所处的物理环境，机房、电力、防火、防水、防静电、温湿度控制等相关设施

表 A.2 列举出移动互联网应用的主要的脆弱性识别内容。

表 A.2 脆弱性分析表

类别	对象	主要脆弱性
技术脆弱性	业务及应用	相关服务器未进行合理备份，重要数据未及时进行备份； 相关业务/应用协议存在漏洞，相关服务器的应用代码存在漏洞、后门；相关服务器存在过多不必要的开放端口； 相关服务器配置不合理，访问控制策略设置不合理； 相关服务器的日志功能没有启用或不够详细； 系统规划、设备部署、链路部署、资源配置、业务保护和恢复能力、安全技术措施和策略等方面的缺陷
	设备	相关设备存在硬件隐患或质量问题； 相关设备的操作系统存在安全隐患； 相关密码设置不合理、复杂度不够、或没有经常更新； 设备重要部件未进行合理备份； 相关设备超过使用年限或核心部件老化； 相关设备发生故障后未及时告警
	物理环境	机房场地选择不合理； 防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范； 通信线路、相关服务器、主机等设备的保护不符合规范
管理脆弱性		安全管理机构方面：岗位设置不合理（如人员配置过少、职责不清）、授权和审批程序简化、沟通和合作未执行、审核和检查未执行等； 安全管理制度方面：管理制度不完善、制度评审和修订不及时等； 人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续、人员未进行安全培训、对于第三方人员未进行限制访问等； 建设管理方面：安全方案不完善、软件开发不符合程序、工程实施未进行安全验收或验收不严格等； 运维管理方面：物理环境管理措施简单、存储介质使用不受限、设备没有定期维护、厂商支持力度不够、关键性能指标没有定期监控、无恶意代码防范措施、无数据备份和恢复策略、访问控制不严格、操作管理不规范等，应急保障措施不到位，灾难恢复预案不完善

移动互联网应用安全威胁可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种。表 A.3 列举出移动互联网应用主要面临的威胁。

表 A.3 威胁来源列表

类别		主要威胁
技术威胁		相关主机和服务器的、及系统网络设备使用时间过长或质量问题等导致硬件故障； 系统链路发生故障； 相关设备的操作系统软件、应用软件运行故障； 相关设备数据丢失或系统运行中断； 存储介质老化或质量问题等导致不可用
环境威胁	物理环境	断电、静电、灰尘、潮湿、温湿度异常、电磁干扰等； 意外事故或通信线路方面的故障
	自然灾害	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷击
人为威胁	恶意人员	不满的或有预谋的内部人员滥用权限进行恶意破坏； 攻击者利用非法手段进入机房内部盗窃、破坏等，攻击者非法物理访问相关设备、存储介质等； 攻击者利用网络协议、操作系统、应用系统漏洞，越权访问相关设备的文件、数据或其他资源； 攻击者利用各种工具获取相关设备身份鉴别数据，并对鉴别数据进行分析和解剖，获得鉴别信息，未授权访问应用系统，或非法使用相关文件和数据； 攻击者利用应用系统扩散病毒、蠕虫、木马、垃圾电子邮件，利用相关攻击工具恶意消耗应用系统资源，导致系统能力下降或瘫痪、无法正常提供应用服务； 攻击者截获数据，进行篡改、插入，并重发，造成数据的完整性、真实性丧失
	非恶意人员	内部人员由于缺乏责任心或者无作为而应该执行而没有执行相应的操作、或无意地执行了错误或危险的操作导致安全事件； 内部人员没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致故障或攻击； 安全管理制度不完善、落实不到位造成安全管理不规范或者管理混乱导致安全事件

中华人民共和国
通信行业标准
移动互联网应用安全防护要求
YD/T 2694-2014

*

人民邮电出版社出版发行
北京市丰台区成寿寺路1号邮电出版大厦
邮政编码: 100164
北京康利胶印厂印刷
版权所有 不得翻印

*

开本: 880×1230 1/16 2015年9月第1版
印张: 1.5 2015年9月北京第1次印刷
字数: 37千字

15115·480

定价: 15元

本书如有印装质量问题, 请与本社联系 电话: (010)81055492