



探讨移动互联网安全风险及端到端的业务安全评估

岳 荣¹, 李 洪²

(1. 中国电信股份有限公司甘肃分公司 兰州 730010;

2. 中国电信集团公司网络运行维护事业部 北京 100032)

摘 要:介绍了移动互联网体系架构及其面临的安全风险,讨论了业务安全评价指标系统,主要指标包括机密性、完整性、可用性、可靠性、保险性和可行性。另外,提出了一种端到端的业务安全评估方法。

关键词:移动互联网;安全风险;端到端;机密性;完整性;可用性

doi: 10.3969/j.issn.1000-0801.2013.08.012

Study of Mobile Internet Security Risk and End-to-End Service Security Evaluation

Yue Rong¹, Li Hong²

(1. Gansu Branch of China Telecom Co., Ltd., Lanzhou 730010, China;

2. Network Operation & Maintenance Division, China Telecom Corporation, Beijing 100032, China)

Abstract: The mobile internet architecture and its security risks were introduced. Then the index system of evaluation was discussed, which mainly included confidentiality, integrity, availability, reliability, safety and performability. In the end, a method was proposed for evaluating end-to-end service security.

Key words: mobile internet, security risk, end-to-end, confidentiality, integrality, availability

1 引言

随着互联网的高速发展,尤其是移动互联网时代的来临,中国电信的网络规模和应用领域不断扩大,通过网络向用户提供的服务与应用越来越多,诸如网上营业厅、手机视频、手机支付、手机定位、电子邮箱、手机证券、上网浏览等。在各类增值业务蓬勃发展的同时,新的攻击技术和工具层出不穷,攻击具有的随机性、多样性、隐蔽性等特点,使得电信业务正面临前所未有的安全挑战。对业务运营者来说,如何对业务进行端到端的安全评估已经成为一个难题。本文将围绕移动互联网体系架构与端到端安全评估进行论述。

2 移动互联网架构概念

移动互联网是移动通信与互联网两大信息领域融合形成的,其体系架构涉及移动通信与互联网的内容应用、业务平台、终端、承载网络等各个方面。在云计算、智能终端等技术的推动下,这个架构仍在不断演变。如图1所示,移动互联网体系架构体现了端、管、云相结合的技术理念,其主要组成包括移动终端、智能管道、综合平台和内容与应用4个层面。

- 移动终端是指能够接入电信运营商的移动网络且向用户呈现相关业务的移动设备,主要由硬件、操作系统、中间件和终端应用组成。移动终端的形态是多样化的,主要有手机、数据卡、平板电脑、上网本、车载终端等。

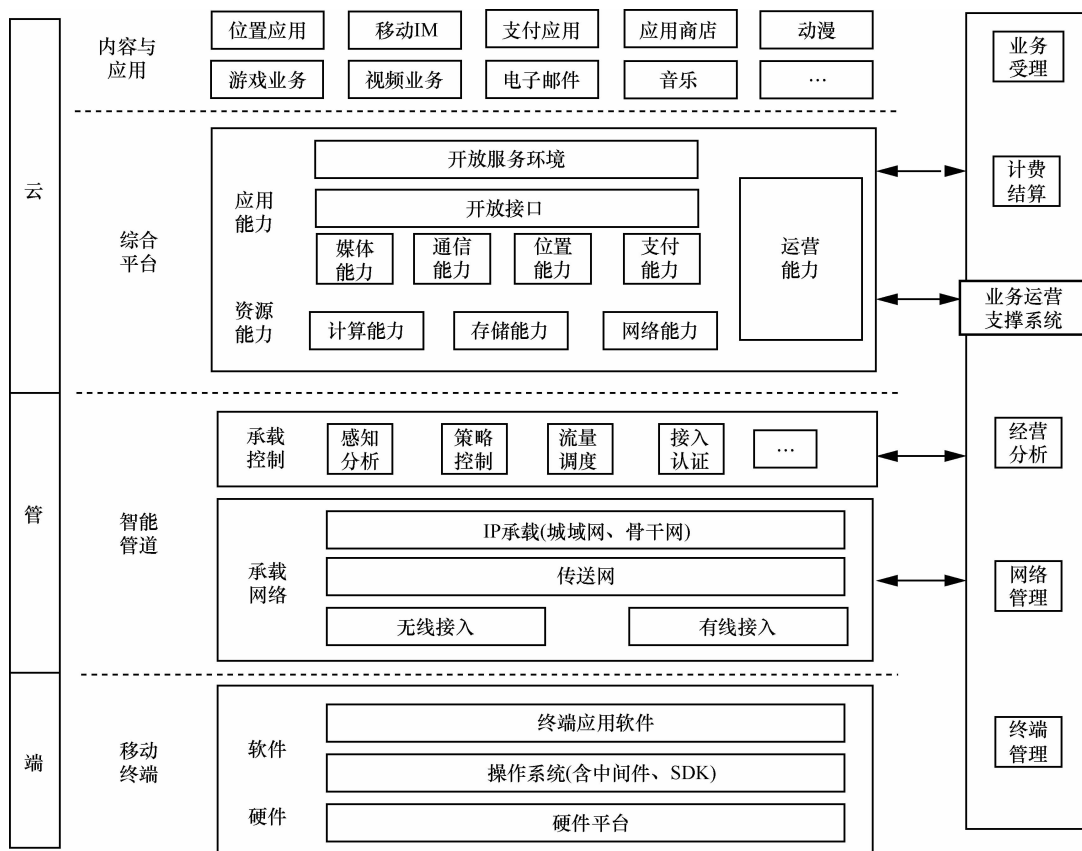


图 1 中国电信移动互联网架构

- 智能管道是中国电信提供的承载网络和承载控制，包括覆盖广且高速的网络、资源指配机制、接入灵活协同的能力、质量按需保障的服务。
- 综合平台是物理上分散、逻辑上一体的平台体系，通过对平台基础通信能力的整合集约以及云计算的引入等，将能力对外开放，向合作者提供互联网应用生成与运营的生态环境。
- 内容与应用是指依托中国电信网络、能力和规模等优势，通过广泛合作，提供给用户的各种移动互联网应用。

3 移动互联网面临的安全问题

为了全面认识移动互联网面临的安全问题，下面将从端、管、云 3 个不同领域进行说明，如图 2 所示。

3.1 终端面临的安全问题

传统的固定终端，如 PC、电话等，作为业务的入口与业务呈现的载体，其所面临的安全问题并不陌生，此处不再详述。在移动互联网领域，业务由平台和终端共同产生，终端与业务的捆绑关系越来越紧密，下面重点对移动终端

的安全问题进行说明。

(1) 移动终端硬件层面

移动终端硬件层面包括基带芯片和物理器件的安全，应在芯片设计阶段考虑具备抗物理攻击的功能，防止攻击者利用高科技手段(如探针、光学显微镜等方式)获取硬件信息。

(2) 操作系统层面

一是智能手机使用的是开放的操作系统和软件平台架构，如 Android、Windows Mobile、Symbian 等，开放的 API 和开发平台在为应用开发者带来便利的同时，也会被不法分子用来开发恶意软件。

二是终端操作系统的非法刷新问题，移动终端应具备系统程序一致性检测功能，当发现未经授权的非法修改时，可在系统启动阶段检测出来，从而有效阻止非法刷机。

三是智能终端的外部接口类型越来越丰富，比如 Wi-Fi、USB、WLAN、蓝牙等，为病毒的传播提供了通道。

四是移动终端支持多用户带来的安全问题。不同于个人电脑，其操作系统允许每个用户可以有不同的运行环境，不同的用户以不同的用户名/密码登录系统，用户之间



业务 承载	端		管	云	
	移动终端	固定终端	智能管道	综合平台	内容应用
评价 指标	机密性 完整性 可用性		机密性 完整性 可用性	机密性 完整性 可用性	
安全 问题	· 基带芯片和物理安全; · 数据存储安全; · 移动终端实现强认证的难度大; · 移动终端支持多用户带来的安全问题; · 安全浏览环境; · 移动终端操作系统安全加固难度大; · 应用隔离问题; · 信息泄露; · 移动病毒、蠕虫、后门、间谍软件和恶意软件等; · 终端操作系统补丁与各业务应用平台间的兼容问题; · 移动终端对SSL的使用与支持问题; · 移动终端位置隐私与安全		· 攻击者在空口窃听信令或用户业务; · 攻击者通过在空口插入、修改、重放或删除信令数据/控制数据/用户业务数据等手段,拒绝合法用户业务或伪装成网元攻击网络 · 攻击者进行DoS攻击; · 针对机密性的攻击,如窃听、流量分析 · 针对完整性的攻击,如篡改、伪装、否认等; · 针对可用性的攻击,如拒绝服务攻击	· 硬件资源脆弱性; · 软件资源脆弱性; · 网络和通信协议脆弱性; · 数据库管理系统安全脆弱性; · 跨站脚本; · SQL注入; · CSRF攻击; · HTTP重定向; · 钓鱼攻击; · 会话伪造; · Web服务地址欺骗; · 缓冲区溢出攻击; · 参数篡改; · XML植入; · BPTEL状态偏移; · 工作流引擎劫持	

图2 移动互联网面临的安全问题

实现了较好的安全隔离。但是,对移动终端来说,以不同的身份登录移动终端实现困难,一旦终端发生短暂移交,可能就会带来个人隐私、账户信息等数据的泄露。

五是移动终端操作系统安全加固比较困难,如果不进行加固,会直接影响到用户对业务的使用体验。从技术上来说,终端操作系统的补丁升级不是挑战,然而,各类增值应用与终端操作系统补丁之间的兼容性测试与安全评估耗时较长,这与业务运营永远是矛盾的,由此带来的安全隐患无法预估。

六是移动终端本地存储的个人信息遭到非法访问的问题,如应用相关的密码文件、认证令牌以及电话簿、银行账户、信息内容等个人数据,如何对其进行保护,能否以一种安全的模式对敏感信息进行存储,是移动终端操作系统急需解决的一个问题。

七是移动终端对安全套接层(SSL)的支持问题,SSL是可靠和安全的运行环境所必备的。但是,许多老旧的移动终端并不支持SSL或支持(SSL)但会影响到用户较高期望的使用体验,这势必影响到端到端的安全服务提供。

(3) 应用软件层面

首先移动终端应能够对应用软件的一致性进行检测,防止安装应用软件时植入病毒。

第二是应用隔离问题。随着智能终端处理能力、存储空间提高,终端安装的软件越来越多,从涉及工作的各种企业应用、进行娱乐的游戏应用到连接朋友和家庭的社交应用,这些应用以及使用这些应用的人都需要访问大量的数据。如何对这些应用及应用所需的数据进行隔离也是一个安全难题。

第三,移动终端实现强认证的难度大。通常情况下,强认证是指包括了字符(至少其中之一是大写字母)、数字、特殊符号以及空格等组成的密码或密码短语。然而,要在移动终端上利用有限的键盘实现强认证是比较困难的,对用户来说也十分不方便。

第四,安全浏览环境受限引起的安全问题。利用3G网络上网浏览已经成为移动用户的最大乐趣之一,高速增长的用户访问请求次数与流量足可见证。但是对于移动终端来说,一个最基本的问题是缺乏足够的显示空间,恶意人员利用终端上URL显示不全甚至不显示、浏览内容中内嵌等问题,恶意行为更容易得逞。

此外,目前手机上推广的各种应用越来越多,部分新业务可能带来新的安全隐患。比如,利用移动定位技术获取到用户自身位置信息的同时,位置信息又是用户的个人隐私,因此在开展移动定位业务时,必须从技术和管理角

度考虑用户个人位置信息不被泄露。

3.2 管道面临的安全问题

针对无线接入网络,移动设备(ME)与接入网络(AN)之间的空中接口是容易遭受攻击的部分,其面临的攻击主要有:攻击者在空口窃听信令或用户业务;攻击者通过在空口插入、修改、重放或删除信令数据/控制数据/用户业务数据等手段,拒绝合法用户业务或伪装成网元攻击网络;攻击者通过物理方法阻止用户业务、控制数据、信令数据在无线接口上传输;攻击者进行 DoS 攻击。

针对有线接入网、传送网及 IP 承载网,在机密性、完整性和可用性方面的攻击主要有以下几种。

(1) 针对机密性的攻击方法

- 嗅探或窃听,是一种监控网络中 Web 服务流量的行为,攻击者可在网络层监控传输的消息内容,从而获取敏感的纯文本数据和在 SOAP、WSDL 等消息中携带的安全配置信息。使用一个简单的数据分组嗅探器,攻击者可以很容易截获网络中传输的信息,利用获知的信息发起攻击。窃听行为的发生,对通信中数据机密性造成了极大的威胁。
- 流量分析是通过技术手段获得情报监测模块的传输通信,在交互中,消息流承载大量的信息。

(2) 针对完整性的攻击方法

- 篡改是指攻击者通过增加、删除、修改和重新安排等方法来改变原有的消息。
- 伪装是攻击者可能冒充合法用户来获取未经授权的特权。
- 重放攻击是将以前获取的正确信息再次传输。这些信息可以是整个路由数据分组或仅仅是附在虚假信息后的认证信息。后者可以被攻击者用来破坏设计不完善的安全方案,这也是假冒攻击的第 1 步。通过重放以前截获的数据分组,攻击者可以破坏不同路由域之间的同步。已经过时的路径可以按照新路径的方式出现,对中继节点的路由表进行破坏。

(3) 针对可用性的攻击方法

针对可用性的攻击方法主要以 DoS 攻击为主,目的是使计算机或网络无法提供正常的服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。带宽攻击是指以极大的通信量冲击网络,使得所有可用网络资源都被消耗殆尽,最后导致合法的用户请求无法通过。连通性攻击是指用大量的连接请求冲击计算机,使得所有可用的操

作系统资源都被消耗殆尽,最终计算机无法再处理合法用户的请求。

3.3 业务平台面临的安全问题

业务平台自身由于主体和客体的原因可能存在不同的脆弱性,为攻击者提供了入侵、骚扰或破坏系统的途径和方法。业务平台自身的脆弱性主要包括业务平台的硬件资源、通信资源、软件及信息资源等,因各种原因而可能导致系统受到破坏、更改、泄露和功能失效,使系统处于异常状态甚至瘫痪等。

随着 Web 技术的发展,业务平台与 Web 技术的关系越来越紧密,针对 Web 服务的攻击依赖于大量的系统脆弱性,主要攻击行为有强制浏览攻击、代码模板、字典攻击、缓冲区溢出攻击、参数篡改、XML 植入、SQL 注入、跨站脚本、BPEL 状态偏移、实例泛洪、间接泛洪、Web 服务地址欺骗、工作流引擎劫持等。除此之外,还将面临来自于网络服务和业务流程方面的安全威胁,其中,网络服务安全是体现 Web 服务安全需求的最重要标准,为 Web 服务提供了完整性、机密性与认证。业务流程描述为实现某一共同目标或特殊功能的多个网元或功能模块之间如何交互和协作的过程,其业务模型与业务规则的设计对安全运行至关重要。

4 端到端的业务安全评估过程

业务安全评估可按照以下步骤进行:确定评估指标、业务分析、业务平台分析、风险识别、风险分析和安全评估。

4.1 确定评估指标

对增值业务进行安全评估的前提和基础是要建立可量化和可操作的安全评价指标系统,要求指标能够客观、真实地反映业务的安全变化情况。

目前,安全性评价指标中关注度较高的基本属性主要有 6 个,包括可靠性(reliability)、可用性(availability)、保险性(safety)、可行性(performability)、机密性(confidentiality)和完整性(integrity)。

可靠性是衡量业务平台在一个特定时间内能够持续执行特定功能的指标,它侧重于分析业务平台正常运行的连续性。可靠性分析主要依赖于业务平台中软、硬件故障发生的频率和平台架构的选择。

业务平台最基本的功能是向用户提供服务,而用户所要求的服务是多层次、随机的,可用性是指业务平台可被授权用户访问并按需求使用的特性,是衡量业务提供连续



性的重要指标之一。

保险性定义为在一个周期时间内业务平台不对环境和用户造成灾难性后果的概率。它依赖于业务平台发生安全失效后所造成的影响,而与失效的具体起因无关。

可行性强化了网络系统在可能发生失效情况下的运行性能,提供了安全性与系统性能之间的一种综合定量评价标准。

机密性是指系统中受保护的信息不泄漏给未经授权的用户、实体、过程或供其利用的特性。在业务平台的各个层次上有不同的机密性及相应的防范措施。例如,在物理层,要保证系统实体不以电磁的方式向外泄露信息,在数据处理、传输层面,要保证数据在传输、存储过程中不被非法获取、解析,主要的防范措施是采用加密技术。

完整性是指系统中受保护的信息在存储或传输过程中保持不被未经授权的人修改、破坏和丢失的特性。影响信息完整性的主要因素包括设备故障、传输、处理或存储过程中产生的误码、网络攻击、计算机病毒等,其主要防范措施是校验与认证技术。

由上述 6 项指标的定义,不难看出安全评价的 3 个主要指标——机密性、完整性和可用性。机密性是最基本的要求之一,不仅针对信息的存储,也针对信息的传输。完整性要求信息变更过程中的变更操作只能由授权实体通过授权机制进行。可用性则要求业务平台提供的服务及信息对授权用户必须可用。

4.2 业务分析

开展业务分析是评估者对增值业务进行认识的过程,在深入调查分析评估对象的基础上,建立对应的业务模型,要求它能够清晰地反映出业务功能、业务流程、数据等信息,是安全评估的基础。这个阶段应识别评估业务相关的键信息资产,也就是决定业务安全性的键数据、服务和流程等。

4.3 业务平台分析

作为业务的重要承载者,对业务平台进行分析的目的是准确地掌握被评估业务的平台结构,包括网络拓扑结构、功能模块、接口关系、安全措施、系统边界以及相关的

内部和外部环境(网络环境、物理环境、相关基础设施和相关信息系统),建立业务平台模型。

4.4 风险识别

风险识别阶段主要对业务平台进行安全检测与核查,识别平台面临的威胁和脆弱性,这是对业务安全状况的数据采集过程。这个阶段要能整理并输出评估业务面临的主要风险。

4.5 风险分析

风险分析阶段是对风险识别阶段已经确定的威胁和脆弱性等风险进行分析,可利用的模型有攻击树、攻击图等。

4.6 安全评估

评估阶段是基于前面已建立的模型,分析主要风险对端到端业务安全指标的影响程度。

首先,要对机密性、完整性和可用性在端到端的业务安全指标中的权重系数进行测算。根据工业和信息化部电信网络安全防护定级标准,定级参考要素主要有社会影响力、服务重要性和服务范围,目前业务平台普遍定级为 2 级(定级对象受到破坏后,会对其所有者的合法权益产生严重损害或者对社会秩序、经济建设和公共利益造成轻微损害,但不损害国家安全)或 1 级(定级对象受到破坏后,会对其所有者的合法权益造成轻微损害,但不损害国家安全、社会秩序、经济建设和公共利益),定级描述表明,影响最为严重的是所有者的合法权益,即企业的业务收入,而增值业务的业务收入与用户规模成正比。假设 α, β, γ 分别是机密性、完整性和可用性在端到端的业务安全指标中的权重系数。对于 α, β, γ 的取值,建议以服务范围为主要参考要素进行计算,经过风险识别阶段的工作后,假设业务面临的主要风险有 i 项, $i=1, 2, \dots, n$, 则每项风险造成的机密性、完整性和可用性受影响服务范围分别是 U_{Ci}, U_{Li} 和 U_{Ai} , 则:

$$\alpha = U_{Ci} / (U_{Ci} + U_{Li} + U_{Ai})$$

$$\beta = U_{Li} / (U_{Ci} + U_{Li} + U_{Ai})$$

$$\gamma = U_{Ai} / (U_{Ci} + U_{Li} + U_{Ai})$$

具体如表 1 所示。

如图 1 所示,增值业务的载体涉及端、管、云 3 个不同

表 1 风险造成的机密性、完整性和可用性受影响服务范围

安全风险 $i(i=1, 2, \dots, n)$	机密性受影响用户范围 U_{Ci}	完整性受影响用户范围 U_{Li}	可用性受影响用户范围 U_{Ai}
安全风险 1	U_{C1}	U_{L1}	U_{A1}
安全风险 2	U_{C2}	U_{L2}	U_{A2}
安全风险 3	U_{C3}	U_{L3}	U_{A3}
...	...	...	...
	$U_C = (U_{C1} + U_{C2} + \dots + U_{Cn})$	$U_L = (U_{L1} + U_{L2} + \dots + U_{Ln})$	$U_A = (U_{A1} + U_{A2} + \dots + U_{An})$

的领域,由终端、接入网、传送网、IP 承载网、能力平台以及内容及应用平台等组成。假设在端、管、云 3 个不同的领域某业务的机密性、完整性和可用性指标如表 2 所示,业务面临的主要风险有 i 项($i=1,2,\cdots,n$)。

表 2 业务的机密性、完整性和可用性指标

安全评价指标	领域			
	端	管	云	全程
机密性	T_C	P_C	C_C	$W_C=T_C\cdot P_C\cdot C_C$
完整性	T_I	P_I	C_I	$W_I=T_I\cdot P_I\cdot C_I$
可用性	T_A	P_A	C_A	$W_A=T_A\cdot P_A\cdot C_A$

可以用以下计算式计算第 i 项风险发生后端到端的业务安全指标:

$$W_S=\alpha\cdot W_C+\beta\cdot W_I+\gamma\cdot W_A \tag{1}$$

其中, W_S 代表端到端的业务安全指标, W_C 、 W_I 、 W_A 分别表示机密性、完整性和可用性的全流程指标, α 、 β 、 γ 分别表示机密性、完整性和可用性的权重系数, $\alpha\geq 0$ 、 $\beta\geq 0$,

· 简讯 ·

2013 年 7 月通信业主要指标完成情况(一)

指标名称	单位	本年本月止累计到达	比上年同期累计(±%)	本月
电信营业收入	亿元	7 626.7	11.8	1 154.2
其中:电信主营业务收入	亿元	6 645.3	8.8	1 002.7
电信固定资产投资完成额	亿元	1 514.2	-10.3	217.7
固定本地电话通话时长合计	万分钟	17 916 321.4	-16.6	2 694 966.3
区间电话通话时长	万分钟	1 872 420.4	-20.8	280 139.0
区内电话及拨号上网通话时长	万分钟	16 043 901.1	-16.1	2 414 827.3
固定长途电话通话时长合计	万分钟	3 459 751.5	-17.1	527 806.3
国内长途电话通话时长	万分钟	3 377 422.5	-17.2	515 956.7
国际电话通话时长	万分钟	50 073.0	-15.3	7 022.5
港澳台电话通话时长	万分钟	32 255.9	-16.0	4 827.1
移动电话通话时长合计(含本地)	万分钟	167 240 635.8	5.6	24 370 761.6
移动电话国内长途通话时长	万分钟	38 392 180.8	5.9	5 608 328.9
移动电话国际电话通话时长	万分钟	73 325.3	6.1	11 855.4
移动电话港澳台电话通话时长	万分钟	56 434.3	-4.1	8 315.1
移动短信业务量	万条	53 906 102.3	2.8	7 701 384.5
移动互联网接入流量	万 GB	69 077.2	63.8	11 372.9

注:(1)收入增长率按可比口径计算。(2)固定长途电话通话时长和移动电话通话时长均包含相应的 IP 电话通话时长。(3)通话时长各项指标均为去话通话时长。

(来源:工业和信息化部运行监测协调局)

$\gamma\geq 0$,且 $\alpha+\beta+\gamma=1$ 。
根据式(1),计算出所有主要风险对应的业务安全指标分别是 W_{S1} 、 W_{S2} 、 $\cdots$ 、 W_{Sn} ,这项增值业务端到端的安全指标取最小值,即业务面临的风险造成的最严重后果。

5 结束语

通过对移动互联网体系架构及其面临的各种安全风险的理解与认识,本文从全业务流程出发,提出了针对电信业务端到端的安全评估思路。由于电信增值业务的结构复杂,端到端的安全评估涉及的专业网络、业务网元过多,如何综合运用多种思想与方法提出高效率的端到端的业务安全评估解决方案仍是未来研究的重点。

参考文献

1 林闯,王元卓,汪洋.基于随机博弈模型的网络安全分析与评价.北京:清华大学出版社,2011
2 诸葛建伟.网络攻防技术与实践.北京:电子工业出版社,2011
(收稿日期:2013-08-07)