



物联网智能终端设备识别方法

肖清旺^{1,2}, 王锦华^{1,2}, 朱易翔^{1,2}

(1. 移动互联网系统与应用安全国家工程实验室, 上海 201315;
2. 中国电信股份有限公司上海研究院, 上海 200122)

摘要: 物联网终端身份的正确识别是建立物联网安全连接的重要前提, 其中智能终端的身份识别问题尤为重要。介绍现有技术条件下, 物联网中智能终端的设备识别方法。从物联网安全的角度, 分析现有方案存在设备识别方式过于简单导致设备易被冒用的安全问题。为解决该问题, 将物联网领域内项目研究工作的成果和业界的经验相结合, 提出了物联网智能终端的多维度设备特征信息的识别方法。

关键词: 物联网; 智能终端; 设备识别

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017044

Intelligent terminal device identification method of internet of things

XIAO Qingwang^{1,2}, WANG Jinhua^{1,2}, ZHU Yixiang^{1,2}

1. Mobile Internet System and Application Security National Engineering Laboratory, Shanghai 201315, China
2. Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China

Abstract: The correct identification of the terminal of the internet of things is an important prerequisite to establish a secure connection of the internet of things. The identification of the intelligent terminal is particularly important. The device identification method of intelligent terminals in internet of things under the existing technology was investigated. From the perspective of the security of the internet of things, the security problem that the device identification method was too simple to be easily falsified of the existing scheme was analyzed. Combining the achievements of project research in the field of internet of things and the experience of the industry, the identification method of multidimensional device feature information of IoT intelligent terminals was proposed.

Key words: internet of things, intelligent terminal, device identification

1 引言

物联网的发展会接入各种设备, 这意味着物联网对现实世界会有更强的控制能力和数据采集能力。越来越强大的控制能力和数据采集能力, 使其对现实生活的影响程度与日俱增。所以在物联网飞速发展的同时, 物联网的安全问题是不容忽视的。目前业内对物联网安全的解决策略主

要有3点: 应用层由安全服务解决认证授权、数据保护等问题; 网络层在服务端和终端之间建立安全的连接; 感知层的终端有可靠安全的运行环境。终端身份的正确识别是物联网安全策略能成功执行的重要前提。

智能终端与普通的非智能终端相比, 功能强大且携带大量敏感数据, 如果发生设备盗用会对用户甚至社会造成严重的危害。智能终端的设备识别问题尤为重要。



2 智能终端识别方法及安全隐患

在现有的技术条件下,智能终端身份识别方法不是非常安全可靠。传统网络中,只有用户名口令、SIM卡等针对用户的识别方法,没有针对终端的身份标识方法。在物联网中,这一问题并没有被很好地解决。对业内众多优秀供应商的物联网解决方案进行调研,各供应商终端身份标识的方法大同小异。

2.1 现有技术方案

(1)移动终端识别方案

运营商提供给终端的用户标识信息和出厂时写入终端设备的识别信息计算生成身份识别ID,用于终端与网络服务端的认证。

(2)有线终端识别方案

运营商提供的入网密钥和出厂时写入终端设备的识别信息生成身份识别ID,用于终端与网络服务端的认证,身份标识由网络服务器对终端进行操作。

分析现有技术,出厂时写入设备的识别码(多为出厂编号或预置密钥),由于是出厂前置入且内容单一,并不能严谨地代表当前设备的合法接入身份。

2.2 现有方案存在的问题

从智能终端特征分析,现有方案存在由于设备标识内容过于简单而极易被盗用身份的问题。

终端具有硬件型号、操作系统种类及版本、常用App行业类别、用户上下线地域和时间域等特征,由于系统版本升级以及用户行为的不同,App特征信息、用户行为特征等信息是出厂前无法预知的,所以出厂前配置的识别特征码无法正确代表用户。智能终端身份识别信息应当包含用户行为、系统版本、App环境等信息,所以使用出厂前置码识别设备本身的方案是不严谨的。在终端被盗窃或者终端被非法入侵时,攻击者盗用合法用户的身份信息,由于身份标识的信息太少而且过于简单,所以在身份识别的环节,危害是难以防范的。

3 解决策略

针对现有终端设备识别方法过于简单导致的安全问题,提出新的终端识别方式,以解决终端身份易被盗用的问题。

使用新的设备标识方式,不再使用出厂置入终端设备的设备编号作为标记设备的设备ID。而是对设备进行特征分析,使用多维度的复合信息生成设备识别ID,用于终

端设备的识别。多维度的信息终端设备识别策略流程如图1所示。

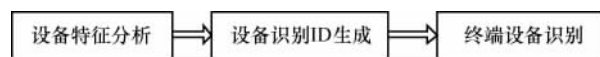


图1 多维度的信息终端设备识别流程

综合获取的信息包括操作系统种类、操作系统实时版本、涉及敏感数据的App特征、用户行为特征等,将混合信息生成智能终端的设备识别特征。如果有异常,更新设备识别信息,确保接入终端身份标识的合法性和有效性。多维度复合的终端标识信息,可以解决由于标识信息过于简单带来的合法终端易被盗用的问题。

3.1 智能终端研究范围

本文研究的对象是智能终端,包括所有具有独立操作系统的嵌入式设备。设备特征分析如下:

- 硬件包括包芯片、PCB、外围接口等;
- 驱动包括各种设备驱动、外围驱动等;
- 操作系统包括 Windows 系列、Linux 系列、Mac 系列以及其他实时或分时的嵌入式操作系统等;
- App 的行业特征及运行环境需求特征;
- 用户及终端设备在运行期间的业务习惯、空间域、时间域等。

3.2 设备特征分析

使用多维度的复合信息标识终端设备,首先要做的是对设备进行特征分析。设备特征包括构成终端设备的芯片型号、PCB 型号版本号、外围接口类型、驱动版本、操作系统种类、操作系统版本、App 特征、终端行为特征及用户行为特征等。终端特征分析维度见表1。

3.3 设备识别ID生成

分析设备特征后,需要将设备特征转化为设备的国际标识码(international equipment identity, IEID)。对于移动终端,转化为国际移动设备身份码(international mobile equipment identity, IMEI)。具体方法是:使用通过终端设备特征分析得到的多维度信息数据,通过计算,生成可以代表设备现有状态的唯一标识ID。

生成设备识别ID前,先生成设备特征分析数据表。终端在设备特征分析数据表中查询生成数据特征码。设备特征分析数据表的生成方式由各物联网平台自定义。现提供假想终端部分特征数据的参考表,各类特征(如芯片特征、PCB 特征、驱动特征等)采用统计注册的方式,具体见表2。其中,App 特征、用户特征及终端工作特征需要使用深度

表 1 智能终端特征分析项

终端特征	信息标识策略	标识信息
硬件特征	芯片特征	芯片型号、物理参数等
	PCB 特征	板材等
	终端外围接口特征	外围接口种类特征、外围接口占用特征
驱动特征	驱动功能	各驱动使能的功能特征
	驱动版本	各驱动版本特征、版本编号等
操作系统特征	操作系统发布类型	系统类型、系统版本
	操作系统版本号	系统更新版本号
	操作系统最近更新时间	更新时间列表
	操作系统后台插件	插件功能、占用资源等信息
	文件系统特征	文件系统类型、存储特征
	资源消耗特征	操作系统对 CPU、内存、硬盘等资源的消耗情况
敏感 App 特征	行业特征	根据 App 的种类特征,分析终端行业用途
	运行环境特征	各 App 占用的资源特征
	App 后台插件特征	App 使用的插件特征
用户行为特征	用户空间域	对可远程登录终端的用户,用户的登录地点分析
	用户时间域	用户使用终端的使用时间分析
	用户业务习惯	用户常用业务的特征分析
	用户登录习惯	用户常用登录习惯的特征分析
终端行为特征	终端空间域	终端入网地点的特征
	终端时间域	终端执行业务时间段的特征
	终端业务习惯	终端业务类型的特征
	终端接入习惯	终端接入方式的特征分析

学习的方式进行分析。

表 2 所示的仅是部分多维度信息,在实际生产中,可以采用更加丰富的信息作为数据分析表。对分析到的数据进行处理,如散列处理、加密处理、压缩处理等,最终生成可以严谨代表终端的设备标识码(IEID 或 IMEI),如图 2 所示。

3.4 终端设备识别

设备识别方式本质是生成更有效的 IEID(或 IMEI)。

平台识别终端时,根据设备的识别码,反向分析设备的特征,以确保设备的正确性。在进行验证、授权、业务交互等动作前,对终端设备进行实时识别,即将解析 IMEI(或 IEID)生成的设备注册数据与实时获取的设备数据进行比对,数据匹配才可进行其他业务。具体如图 3 所示。

经过第 3.1 节的分析和第 3.2 节的计算,最终生成了可以唯一代表终端设备本身的设备标识码。将设备标识码与运营商提供的用户识别码结合,作为终端的最终入网设备识别码。智能终端入网识别方法示意如图 4 所示。

对于带 SIM 卡的移动终端,由于终端本身可以拥有运营商用户识别码,所以可以直接使用 IMSI 与 IMEI 结合标识的方式。

对于不带 SIM 卡的移动终端,此类设备不通过蜂窝移动网络,而是通过其他方式接入网关之后再接入应用平台。所以需要采用终端本身的 IMEI 与网关设备的 ISID 相结合的方式。此类设备接入时,要求网关或者 NS 一定要有运营商提供的 ISID。

对于有线终端,使用 ISID 与 IEID 结合标识的方式。有线设备具有相对固定的特点,可以由所在地的运营商提供 ISID,结合 IEID 入网。

3.5 应用场景示例

应用场景以移动智能终端为例,通过 IMEI 与 IMSI 结合的方式标识。业务主要过程如图 5 所示。

(1)设备入网注册,将设备特征分析数据表通过散列、加密、压缩等方式计算生成 IMEI,与 IMSI 信息结队标识合法的接入设备,将信息存入物联网应用服务平台。

(2)当智能终端向应用服务平台发起接入申请时,服务平台根据合法的 IMSI 信息,查询对应的 IMEI 信息。IMEI 经反向计算生成终端在平台注册的设备特征表。

(3)将平台分析出的设备特征表与设备中实时获取的设备特征表进行比对,分析结果。



表 2 自定义智能终端特征数据(表格 Demo)

终端特征	特征项	标识信息示例	特征编码内容示例
硬件特征	芯片特征(以 ARM7AT91 系统其中一款部分参数为例)	芯片型号	AT91F40162
		供应商	ATMEL
		电压-电源(VCC/VDD)	2.7~3.6 V
		主频	40 MHz
		RAM	8 KB×8
	PCB 特征	板材	CEM-3
		规格	L29.2 mm×W19.1 mm×T1.2 mm
	外围接口	USB 接口	2.0×2 3.0×1 No.1 online No.2 offline
		UART 接口	232×1 485×1 No.1online
		百兆网口	*1 VMnet0 backup
驱动特征	驱动功能	终端已经安装驱动种类	*1 VMnet1
	驱动版本	D*2 Mouse Pen No.1 online	
		外接鼠标驱动	version 2017.1.5.15.04
		外接绘图手写板驱动	version 2017.1.5.15.05
系统特征	操作系统(仅示例部分操作系统)	系统类型	Android 4.4 Huawei
			WinCE
			Linux Telecom
			Linux Ubuntu
			Linux Fedora
		系统版本(仅以 Ubuntu 系统示例)	Ubuntu 14
			Ubuntu 16
			version 2017.1.5.15.06
	系统版本号	系统更新版本号	version 2017.1.5.15.06
	系统更新时间	更新时间列表	version 2017.1.6.15.05
			version 2017.1.7.15.05
			version 2017.1.8.15.05
	系统后台插件	安全插件	1 MB
		协议分析插件	1 MB
	文件系统特征	文件系统类型	NTFS、FAT32、EXT、JSF
		硬盘消耗记录	10 GB
		CPU 消耗记录	1.8 GHz×4 70%
		内存消耗记录	8 GB 70%
App 特征	行业特征	金融、医疗、交通等	金融
	运行环境特征	App Demo 占用	1 MB
	后台插件特征	安全插件	输入保护;1 MB
用户特征	用户空间域	说明城市、所在建筑等信息	上海市浦东新区电信大厦
	用户时间域	用户习惯使用的时间	17:30
	用户业务习惯	数据分析、打印功能	数据分析
	用户登录习惯	指纹	指纹
工作特征	终端空间域	GPS 坐标、经度、纬度等	经度 100 m、纬度 100 m、海拔 100 m
	终端时间域	09:00-17:00	14:00
	终端业务习惯	金融、医疗、交通	金融
	终端接入习惯	SSH 登录、Telnet、4G	SSH 登录
出厂编号			编号示例略

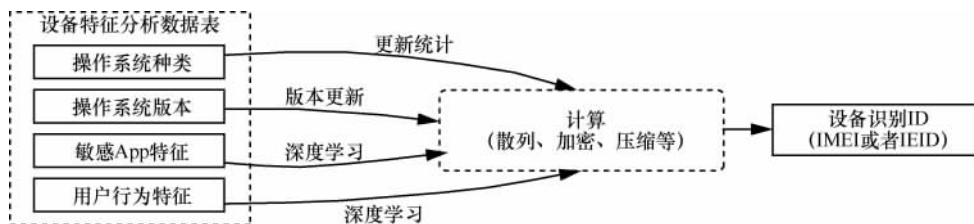


图2 设备特征生成设备 IEID 或 IMEI 示意

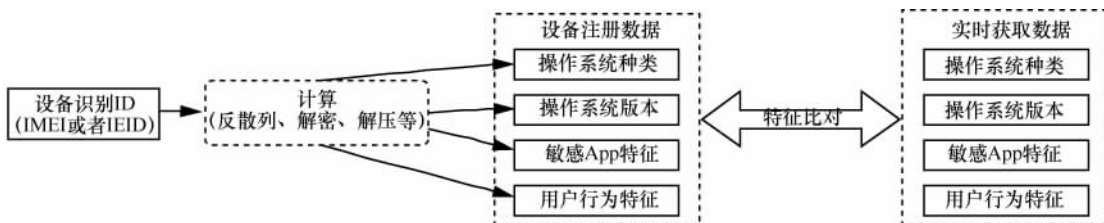


图3 IMEI(IEID)身份识别方法示意

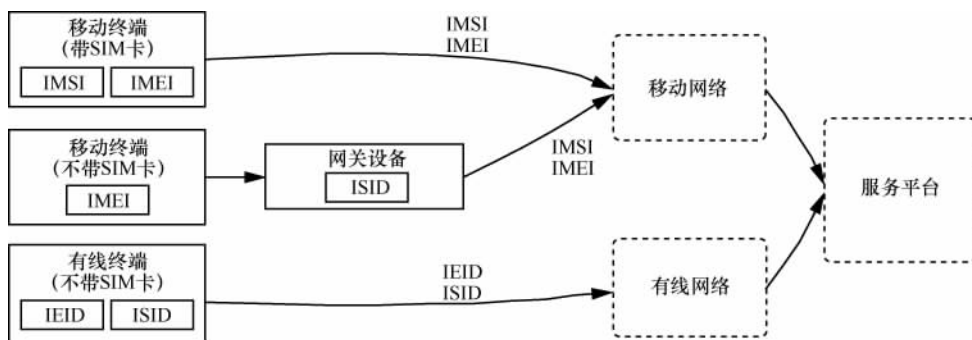


图4 智能终端入网识别方法示意

(4) 比对通过,则认为设备已经成功识别,然后进行后续的验证、授权及业务交互工作。

到此,终端设备识别方法研究完成。

4 运营商如何引领变革

在物联网时代,电信运营商需要做的是拒绝不合法的设备接入,为合法接入的设备提供安全服务,并推动物联网设备入网协议的标准化。具体可以做以下3件事。

(1) 接入许可

只允许同时满足 IMSI 合法和 IMEI 合法的终端设备接入网络。

(2) 提供安全服务

利用电信运营商大数据的优势,将反电子欺诈平台投入实际运营中并持续改进,不断优化升级反欺诈的能力,为公众提供安全可信的通信服务。

(3) 推动标准

利用电信运营商的甲方角色,推动更安全的设备识别

平台的发展。通过业务引导,逐渐地让更为安全的识别认证方式成为标准。

5 结束语

要保证物联网的安全,需要做好终端识别、终端身份验证、终端可用资源授权等一系列的工作,终端正确识别是一系列安全策略能有效执行的首要条件。现有的设备识别方式过于简单,存在严重的安全隐患。

现提出了使用多维度综合信息作为终端识别信息的策略,可以解决终端识别信息简单带来的终端冒用的隐患。相比传统的出厂置入设备识别码的方式,多维度的信息包含了众多终端的实时特性,比如系统版本号、系统更新时间、系统资源占用情况、终端使用特征和用户特征等信息。信息经过散列、加密、压缩等处理得到的识别码,可以在身份识别时反推出注册设备的特征,与设备的实时状态比对即可分析出当前设备是否真正可以合法接入,从而有效防止因设备盗窃、系统重置等攻击手段带来的危害。

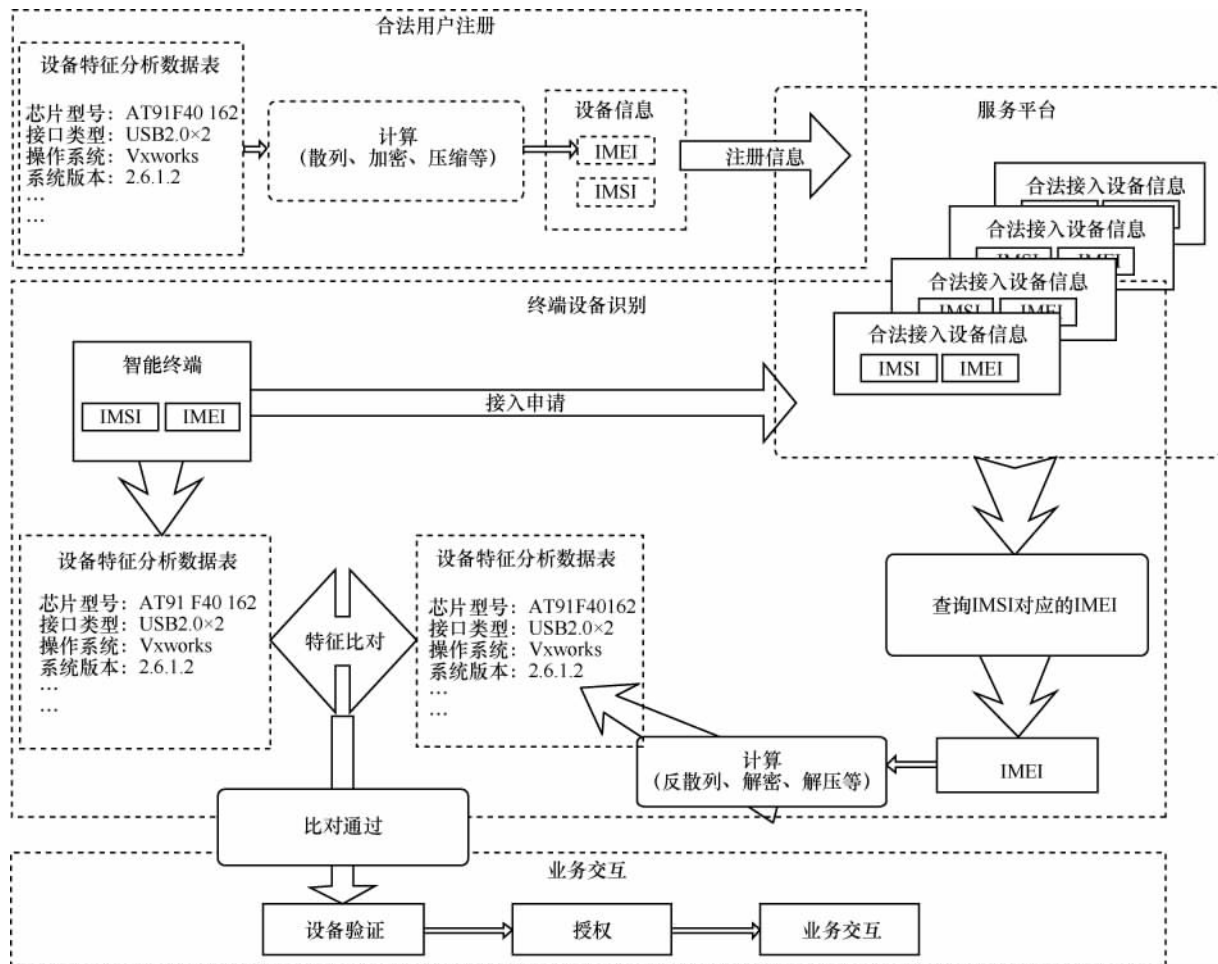


图5 业务主要过程

使用多维度的综合信息作为智能终端的识别信息,可以使物联网的安全性得到进一步的提高。电信运营商在这一过程中,可以通过接入许可管理、安全服务、业务引导等方式推动终端识别方式的发展,以争取在物联网时代,让运营商可以承担重要的生态链角色。

参考文献:

- [1] 吴新勇. 嵌入式操作系统安全保障技术研究[D]. 成都: 电子科技大学, 2003.
WU X Y. Embedded operating system security technology research [D]. Chengdu: University of Electronic Science and Technology, 2003.
- [2] 刘文懋. 物联网感知环境安全机制的关键技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2013.
LIU W M. Internet of things perception of environmental safety mechanism of key technology research [D]. Harbin: Harbin Institute of Technology, 2013.
- [3] 胡向东, 魏琴芳, 向敏, 等. 物联网安全 [M]. 北京: 科学出版社, 2012.

HU X D, WEI Q F, XIANG M, et al. Internet of things security [M]. Beijing: Science Press, 2012.

作者简介



肖清旺(1989-),男,移动互联网系统与应用安全国家工程实验室工程师,主要研究方向为物联网终端安全接入技术。

王锦华(1982-),男,移动互联网系统与应用安全国家工程实验室工程师,主要研究方向为云计算、大数据安全相关技术。

朱易翔(1979-),男,移动互联网系统与应用安全国家工程实验室副主任,负责移动互联网系统与应用安全国家工程实验室技术研发工作,主要研究方向为安全体系与架构、安全攻防与漏洞发掘、移动应用安全检测等。