物联网智能联网设备口令保护技术研究

王 滨[1] 刘贤刚[2] 陈学明[1] 李 琳[2]

[1](杭州海康威视数字技术股份有限公司 杭州 310051)

[2](中国电子技术标准化研究院信息安全研究中心 北京 100007)

(wangbin2@hikvision.com)

Research on Password Protection Technology of Intelligent Connected Device About Internet of Things

Wang Bin[1], Liu Xiangang[2], Chen Xueming[1], and Li Lin[2]

[1](*Hangzhou Hikvision Digital Technology Co.,Ltd.*, *Hangzhou* 310051)

[2](*Information Security Research Center*, *China Institute of Electronic Technology Standardization*, *Beijing* 100007)

Abstract As a common method of identification for intelligent connected devices, password authentication involves many security threats during its use. Based on the analysis of the security risks during the password authentication, this paper puts forward the security technical requirements and security objectives from the aspects of the generation, management and use of the accounts and passwords of intelligent connected devices, to guide manufacturers connected to design and implement password protection functions securely, and also serve as the basis for the supervision and inspection of password's secure use of intelligent connected devices.

Key words Internet of things; intelligent connected device; password; account; identity authentication

摘 要 口令认证作为当前智能联网设备普遍采用的身份认证方式,在使用的过程中存在诸多安全威胁.在分析口令认证过程中面临的安全风险的基础上,从智能联网设备账号和口令在生成、管理和使用等方面提出了安全技术要求和安全目标,从而指导智能联网设备生产制造商安全设计和实现口令保护功能,同时也为智能联网设备口令安全使用的监督、检查提供依据.

关键词 物联网;智能联网设备;口令;账号;身份认证

中图法分类号 TP309

口令,又称密码(Password 或 Passcode).由于口令具有简单易用、低成本、易实现等特性,已经成为当前应用最为广泛的身份认证方法之一,是各种信息系统安全的第一道防线[1],甚至是最重要的一道防线.近年来,随着物联网的兴起,智能终端大量地布放于感知层,且绝大多数的智能终端都是使用口令作为唯一的访问控制的机制,所以一旦口令的安全机制出现问题,如使用弱口令、没有防暴力破解机制等,将会导致智能终端完全被攻击者控制,如果大量的智能终端被攻击者控制,

收稿日期:2019-08-16

基金项目:国家重点研发计划项目(2018YFB2100400)

将会引发严重的安全问题，如 2016 年 10 月发生的“美国断网”事件等.

近年来由于智能终端的口令引发的网络安全问题日益严重，Forrester 的一项调查表明：80％的 IoT 设备采用简单密码[2]，面对这种情况国内外已有的标准中会涉及少量的口令要求[3-6]，但没有对口令的安全进行系统详细的规范，所以国家信息安全标准委员会立项制定了一系列的物联网安全标准[7-8]，其中包括 2017 年启动了由杭州海康威视数字技术股份有限公司牵头的《信息安全技术 智能联网设备口令保护指南》标准的制定，解决智能联网设备的账号和口令在生成、管理和使用等方面的安全技术要求，指导智能联网设备生产制造商安全设计和实现口令保护功能，同时也为智能联网设备口令安全使用的监督、检查提供依据.

1 智能联网设备口令安全问题概述

近些年，伴随着“中国制造”“互联网＋”的开展以及智慧城市建设的深入，物联网得到国家政策的大力支持[9]，2015 年市场规模达到 7 500 亿元，同比增长 21％.中国物联网研究发展中心预计，到 2020 年我国物联网产业规模将达到 2 万亿，未来 5 年复合增速 22％.未来物联网产业规模孕育的产业链机会巨大.

随着物联网技术的快速发展，各种类型的智能联网设备不断涌现，并且得到了广泛应用.智能联网设备成为网络攻击的一个重点，特别是智能联网设备口令安全问题已经成为突出的网络安全威胁，近期物联网安全事件频发，其安全风险主要集中在以下几点：

1）物联网智能联网设备通常数量庞大，部署位置也较为分散，可能会出现断网、设备故障、状态异常等情况；

2）物联网智能联网设备大多存在弱口令、默认口令问题，一旦被黑客利用，后果极为严重；

3）物联网智能联网设备部署位置分散，会被恶意攻击利用，遭到替换设备并伪造身份，被利用作为攻击源，进而对整体网络造成安全威胁；

4）物联网设备存在大量无品牌产品，没有安全和隐私控制措施，极易泄露用户隐私.

针对物联网产业发展遇到的安全问题，制定物联网智能联网设备口令保护相关标准势在必行.

2 智能联网设备口令安全威胁分析

身份认证是安全的第一道防线，是安全技术的重要构成部分.由于成本、易用性等原因，智能联网设备普遍采用口令认证的方式.一般账号和口令是成对出现的.账号的作用是标识用户的身份，口令的作用是对用户的身份进行认证.

口令认证是基于用户所知进行身份认证，通过用户设置和记忆的字符串来验证用户的身份.口令认证是最经济、最常用的身份认证方式，但是也被认为是最弱的一种身份认证方式，面临着诸多威胁.通过威胁建模分析识别出的口令认证过程的威胁如图 1 所示.

物联网概念从 1999 年被美国麻省理工学院(MIT)首次提出[10]后，一直受到业界的热捧，被人们视为继计算机、互联网之后信息技术产业发展的第 3 次革命，其泛在化的网络特性使得万物互联正在成为可能.由于整个物联网的发展受到了硬件成本、网络等多方面的制约，并未得到广泛的推广和使用，但是近年来随着相关" 瓶颈' 技术的解决，物联网技术得到的较大规模的普及和应用，智能家居、车联网、人工智能……这一切的背后正是物联网在加速落地、快速成熟，物联网时代的到来已经毋庸置疑.

从图 1 可以看出，口令认证过程的威胁可以分为 3 类：第 1 类是针对用户和口令输入界面的威胁，称之为用户端威胁；第 2 类是从网络上发起和针对网络传输的威胁，称之为网络威胁；第 3 类是针对设备上存储的口令文件的威胁，称之为设备端威胁.

用户端威胁主要包括：

1）肩窥.指的是某人越过其他人的肩膀观察其按键动作或偷看计算机屏幕上显示的数据.

2）社会工程.攻击者通过欺骗、诱导等社交手段来获取设备口令.

3）猜测.攻击者通过已经掌握的关于设备、用户的信息来猜测设备的口令.使用设备默认口令或个人信息衍生的口令都容易遭受猜测攻击.

网络威胁主要包括：

1）嗅探.一种被动网络攻击方式，通过侦听网

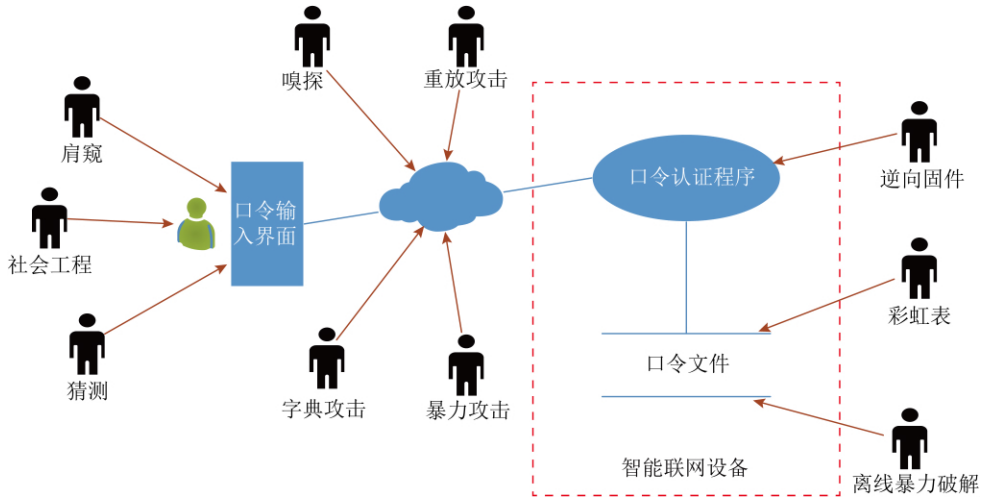

图 1　口令认证安全威胁分析图

络流量来捕获用户向设备中的认证程序正发送的口令.

2）重放攻击.攻击者复制认证过程的数据，并在其他时候重复使用这些数据来认证.

3）暴力攻击.使用工具，通过组合许多可能的字符、数字和符号来循环反复地尝试登录设备.

4）字典攻击.使用包含大量口令的字典文件与用户的口令进行比较，直至发现匹配的口令.

设备端威胁主要包括：

1）彩虹表.攻击者事先制作 1 张包含所有口令和对应哈希值的表，然后使用口令文件中的哈希值反查这张表获得口令.

2）离线暴力破解.攻击者模拟口令认证的过程，针对口令文件通过分析或者穷举来找到口令.

3）逆向固件.攻击者通过反编译设备固件中的口令认证部分来找出可绕过认证的漏洞或者硬编码口令.

我们需要从技术和管理 2 个方面入手，来增强智能联网设备口令认证的安全性.从技术层面，设备厂商应该在设计阶段就考虑口令安全保护问题，做到内建安全，使用户只能通过安全的方式使用设备；在管理层面，培养和增强用户的安全意识.厂商在技术上多做一点，对用户的安全意识要求就少一点，口令安全才能更好地贯彻和实现.

3　智能联网设备口令安全要求

智能联网设备口令安全从账号安全、口令安全和用户安全使用 3 个方面提出安全要求.前 2 个方面主要是针对设备的设计实现方面的要求，后 1 个方面是对用户提出的要求.

3.1　设备基本要求

在设备中所有账号/口令都应该是可见和可管理的，设备制造商不应在设备中保留隐藏账号作为维护后门.

在设备中，集成的第三方软件特别是数据库软件中，有可能包含默认账号，如果设备没有使用该默认账号，应删除不使用的默认账号，以减小攻击面.

为了便于支持最小特权原则，设备要支持账号的权限分级机制，比如分为管理员和普通用户.只有管理员才能管理其他账号.设备的日常使用非管理员账号，降低账号口令被破解造成的损失.

因为口令是需要用户记忆的字符，人们可能会忘记口令.设备应提供通过物理按键或者其他的安全方式将设备恢复到出厂状态的功能.

设备中所有账号和口令的所有操作都应记录日志.为了保证日志内容的完整有效，日志内容至少包括用户 ID、IP 地址、操作时间、操作内容、操作结果等信息.设备应具有生成日志的能力，由于智能联网设备的存储能力受限，日志可以存储在设备上，也可以远程存储在日志服务器.

3.2　用户端安全要求

在新建和修改账号时，设备应保证账号不能与已有账号重复，以做到 1 个账号可以唯一标识 1

个用户，以便于事后追溯.设备还应对账号进行命名规则检查，对特殊字符如等号、单引号、& 等进行过滤，以预防 SQL 注入攻击，并且便于账号的输入和显示.

用户设置口令时，设备应对口令的复杂度进行检查，使用户不能设置过于简单的口令，防止对于口令的猜测攻击和暴力破解.综合安全性和易用性的要求，参考业界的最佳实践，对于智能联网设备口令复杂度的要求如下：对于随机生成的口令，长度应该不小于 6 个字符，对于人为设置的口令长度应该不小于 8 个字符，口令中要包含大小写字母、数字、特殊符号中的 2 种或 2 种以上.在用户设置口令时，设备应当对口令的复杂度进行检查，不允许用户设置不满足口令复杂度要求的口令.口令的复杂度应该在满足安全基线的情况下可配置，以满足高安全应用场景的需求.设备支持的口令的最大长度不小于 64 个字符.

用户设置口令时，设备应该显示口令的安全等级，以引导用户设置复杂度高的口令.通常口令的安全等级分为弱、中、强 3 个等级，口令的安全等级根据口令的长度、包含的字符种类等因素来确定.

为了防止肩窥，用户输入口令时要掩码显示，比如显示为********；设备应禁止口令输入框的复制功能，防止恶意程序通过复制获取口令明文；为了减少口令暴露的风险，即使用户认证通过后，也不能通过用户界面或者 API 来读取口令明文.

用户修改口令时，要求用户输入旧口令，并且 2 次输入新口令进行确认，在旧口令验证通过后才将口令更改为新口令.口令修改过程应以原子操作的形式实现.

为了降低默认口令的风险，有 2 种应对措施：第 1 种是采用激活机制，设备出厂时没有口令，用户初次使用设备时为设备设置符合复杂度要求的口令；第 2 种是在设备出厂时，为每一个设备生成随机的初始口令，每个设备的初始口令不同.由于设备的初始口令通常以标签的形式贴在设备上，而且厂商知道设备初始口令，设备需要提示用户修改初始口令.

3.3 网络安全要求

为了防止攻击者通过嗅探网络上的数据获得设备口令，在口令认证过程中不应传输口令的明文，应该传输口令计算的哈希值，并且采用挑战应答的方式，例如采用摘要认证的模式；为了增加安全性，口令认证的通道应采用安全通道，如 TLS，https 等.

基于挑战应答的口令认证过程如图 2 所示：

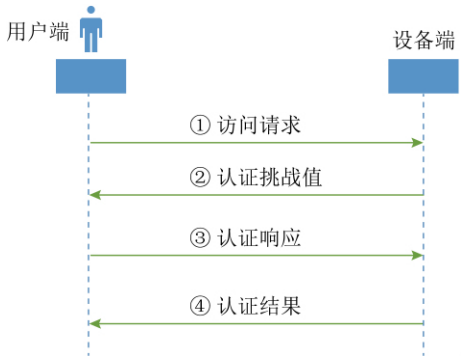

图 2 口令认证过程

设备先给用户端发送 1 个随机数挑战值，用户端使用口令和随机数挑战值计算出响应数据，在设备端对相应响应数据进行验证.由于每次口令认证过程中，随机挑战值是不同的，可以防止用户重放响应数据来通过认证.

为了防止在线口令暴力破解，需要有账号锁定策略，阈值限制，达到一定次数就锁定账号或者操作 IP.

4 设备端安全要求

对于设备端的认证程序，所有的口令都应是可更改的，禁止口令硬编码.口令硬编码有很多安全问题：首先，硬编码口令通过对设备固件进行逆向分析很容易就可获得，其次，硬编码口令泄露后，没有办法通过修改口令来遏制攻击.

存储口令的文件，也需要进行安全保护.首先要限制对口令文件的访问和修改，可以通过使用操作系统的访问控制机制来实现.同时，口令文件中不能直接存储口令的明文.最好的办法是存储口令的哈希值.为了防止彩虹表攻击，应该在计算口令哈希值的过程中添加变量，引入随机值.为了增加离线暴力破解的难度，计算哈希值的过程可以采用多轮迭代.比如在没有进行多轮迭代的情况下，攻击者离线暴力破解口令需要 1 天，如果迭代 500 次，则攻击者暴力破解口令就需要 500 天.

5 用户口令安全使用要求

增强用户的安全意识是提高口令认证安全性的一个不容忽视的环节.本标准提出了用户在使用和管理账号/口令时应注意的基本事项.

用户开始使用设备时应该及时修改设备的初始口令,为设备设置一个满足口令复杂度要求的高安全级别的口令.

用户应为不同类型的设备设置不同的口令,防止一种设备的口令泄露,造成全盘的损失.

对于已知曾被泄露的口令,可能已经在黑客的口令字典里,用户应该避免使用.

用户在设置口令时,要避免常见的弱口令,比如有意义的单词,如 Password,重复或顺序的单词,如 abcd1234,QWER1234,以及上下文相关的字眼,如 admin12345.

用户应该妥善地保管设备的用户名、口令.比如不能把口令写在纸条上,贴在显示器上,或者放到键盘下面.

用户应该定期对口令进行修改.因为经常修改口令,可能会造成用户忘记口令,所以这一条放在用户安全要求中,没有做到设备的策略管理里.

6 小 结

口令认证是当前智能联网设备普遍采用的身份认证方式.口令认证虽然具有便于使用、成本低等优点,但也存在诸多威胁,成为黑客攻击智能联网设备的重要切入点.《智能联网设备口令保护指南》标准中提出的安全要求,能够有效地应对设备口令认证过程中的各种安全威胁,提高设备的安全性.

参 考 文 献

[1] Bonneau J, Herley C, Van Oorschot PC, et al. Passwords and the evolution of imperfect authentication [J]. Communications of the ACM, 2015, 58(7): 78-87

[2] Forrester. Security: The vital element of the Internet of things [R/OL]. Forrester, 2015 [2020-01-10]. http://www. bankinfosecurity. com/whitepapers/security-vital-element-internet-things-w-3833

[3] International Organization for Standardization. ISO/IEC 29180: 2012: Telecommunications and Information Exchange Between Systems-Security Framework for Ubiquitous Sensor Networks [S]. Geneva: International Organization for Standardization, 2012

[4] International Electrotechnical Commission. IEC TS 62443-1-1: 2009 Industrial communication Networks—Network and System Security—Part 1-1: Terminology, Concepts and Models [S]. Geneva: International Electrotechnical Commission, 2009

[5] International Telecommunication Union. ITU-T Y. 2060: Overview of the Internet of Things [S]. New York: International Telecommunication Union, 2016

[6] National Institute of Standards and Technology. NIST Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management [S]. Maryland: National Institute of Standards and Technology, 2017.

[7] 全国信息安全标准化技术委员会(tc260). GB/T 33474—2016 物联网 参考体系结构[S]. 北京: 中国标准出版社, 2016

[8] 全国信息安全标准化技术委员会(tc260). GB/T 33745—2017 物联网 术语[S]. 北京: 中国标准出版社, 2017

[9] 工业和信息化部电信研究院. 物联网白皮书(2017年)[R]. 北京: 工业和信息化部电信研究院, 2017

[10] Sarma S, Brock D, Ashton K. The networked world, MIT-AUTOID-WH-001 [R]. Boston: MIT, 1999

王 滨
博士后,研究员,杭州海康威视数字技术股份有限公司副总裁,中电海康集团首席专家.主要研究方向为物联网安全、密码学等.
wangbin2@hikvision.com

刘贤刚
博士,高级工程师,中国电子技术标准化研究院信息安全研究中心主任.主要研究方向为可信计算、数据安全和隐私保护.
Liuxg@cesi.cn

陈学明
硕士,高级工程师.主要研究方向为物联网安全、网络安全架构、可信计算.
chenxueming@hikvision.com

李 琳
博士,高级工程师,主要研究方向为工业信息安全,数据分析.
lilincesi@126.com