 DOI: https://doi.org/10.12349/iser.v3i1.572

Fingerprint Authentication Method Based on IoT Device

Zhiyuan Yu

Beijing Broadthinking Technology Limited, Beijing, 100047, China

Abstract

The complexity of the network environment and information technology makes the security of the Internet of Things more prominent. In order to improve and optimize the authentication problem of IoT devices from the source and enhance the security of IoT devices, a method based on the fingerprint context authentication of IoT devices is proposed. In the process of system design, the context authentication process was clarified, and a fingerprint situational authentication system for IoT devices including contextual information collection, contextual information storage, and context authentication was constructed. At the same time, the Telnet/SSH environment, cloud environment, Mirai attack environment, and scenario authentication environment are set up, and the user control scenario experiment, DTU terminal device scene experiment, and scenario authentication experiment are carried out on the system.

Keywords

Internet of Things; cybersecurity; device fingerprint; contextual authentication

基于物联网设备指纹认证方法

於志渊

北京博思汇众科技有限公司，中国·北京 100047

摘　要

网络环境及信息技术的复杂性使物联网安全问题愈加突出。为从源头上改进和优化物联网设备认证问题，提升物联网设备安全，提出了一种基于物联网设备指纹情境认证的方法。在系统设计过程中，先明确了情境认证流程，构建了包括情境信息收集、情境信息存储、情境认证的物联网设备指纹情境认证系统。同时，设置了Telnet/SSH环境、云环境、Mirai攻击环境、情境认证环境，对系统进行用户控制场景实验、DTU终端设备场景实验、情境认证实验。

关键词

物联网；网络安全；设备指纹；情境认证

1 引言

现阶段，物联网（IoT）的应用愈加深入和广泛，已经成为推动社会经济快速发展的“重要生产力”[1]。在信息技术快速发展的支持下，物联网的运行环境愈加复杂，使物联网设备安全问题成为当前信息技术人员及社会公众高度重视的问题[2]。现阶段，已经形成并应用了基于瞬态特征、调制信号、内部传感器的设备安全保护方法，但仍存在易受环境干扰等问题，难以有效应对愈加复杂的网络环境带来的安全风险。对此，提出一种物联网设备指纹情境认证方法，并对提出的方法进行实验验证，以期有效提升物联网设备使用安全性，切实保障物联网用户的信息数据安全。

【作者简介】於志渊（1977–），男，中国上海人，硕士，从事智能卡、安全芯片、安全通信、物联网解决方案、边缘计算、云计算、虚拟化等研究。

2 物联网设备指纹情境认证方法的提出

基于信息技术的快速发展，物联网在愈加复杂的网络环境中的应用愈加深入，使其安全性面临严峻挑战[3]。结合既有研究成果分析发现，物联网安全研究侧重设备、协议与平台。

其中，物联网设备安全问题比例最高，其原因在于物联网设备默认密码、无保护调试接口等成为易受攻击的对象。由于设备指纹是一种唯一识别设备及其特征的标识符，且现有设备指纹认证技术，包括瞬态特征、调制信号、内部传感器等，易受环境干扰，难以在愈加复杂的网络环境中保障物联网安全。据此，提出一种物联网设备指纹情境认证方法，即通过在设备端对设备进行指纹信息数据处理，挖掘出设备各种隐性特征，并对其身份进行唯一标识确认的方法。以有效提升物联网设备安全，保障 IoT 设备双向认证安全，切实保护网络安全。

3 物联网设备指纹情境认证系统设计

3.1 情境认证流程

为保证物联网设备指纹情境认证系统有效应用，明确情境认证的方法为：对用户所应用的控制程序或设备，进行设备身份与通信间的流量关联分析，找出涉及的情境因素：设备指纹的吻合性、用户名及密码的正确性、协议的变化情况、登录频率异常、登录时间异常、IP 异常等。并通过决策树分类算法，对情境因素进行分类分析，最终实现物联网设备安全控制。物联网设备指纹情境认证流程框架如图 1 所示。

3.2 情境认证系统框架

基于情境认证流程分析，确定情境认证系统的整体框架，该系统主要包括情境信息收集、情境信息存储、情境认证。

情境信息收集主要是通过数据包抓取，对情境信息数据进行解析和汇总的过程。在此过程中，通过 TShark 命令，对数据包信息进行捕获；通过 filter_eapol 函数编写应用，保证信息捕获后可以在设备上建立连接。

情境信息存储主要是对设备的身份特征进行存储，当系统接收到身份认证挑战时，对数据信息进行认证及动态更新、存储的过程。在此过程中，建立 fingerprint 表与 telephone 表，对情境因素信息进行收集和存储。同时，将 telephone 表应用于 DTU 手机号数据信息存储，并应用于身份认证挑战的信息认证方面。若设备信息交互过程中，存在用户名和密码，则在情境因素中录入用户名和密码，若其他设备不存在该信息，则选用并输入其他情境指纹信息。

情境认证主要是基于情境因素提取，完成身份认证、认证管理及身份认证挑战的过程。为提升情境认证模块的系统性和应用实效，在此模块中添加了身份认证、认证管理、身份认证挑战的小模块。身份认证方面，应用决策树算法输出指纹信息提取结果；应用 telephone 对 DTU 设备的情境数据匹配情况进行分析。

4 实验与结果分析

4.1 实验设备与工具

为有效验证系统的可行性，选择应用 TShark 网络协议分析工具、PyShark 数据包分析法、Raspberry Pi 电脑板、Weka 数据挖掘软件、IOS 手机、安卓手机、摄像头。实验设备应用了移动 SIM 卡、USR-GPRS232-730（DTU）。

4.2 实验环境

Telnet/SSH 环境：本实验在搭建的路由环境下进行，应用 Raspberry Pi 电脑板，部署了 Telnet/SSH 实验环境。

云环境：网络为无线网络，应用 Wireshark 对数据包情况进行记录，并分析指纹特征点。

Mirai 攻击环境：本实验中设置了 Mirai 攻击，流程为：

① IoT 设备感染 Mirai 病毒；② IoT 设备与 DNS 服务器进行交互，得到 CNC 服务器的 IP 地址；③ IoT 设备与 CNC 服务器进行周期交互，在此过程中，完成 IoT 设备扫描弱密码设备；④将扫描信息汇报给 Loader 服务器，应用该服务器对设备进行攻击。

情境认证环境：实验过程中，打开主机中的设置软件，选择波特率等参数，并打开串口。随后给 DTU 设备通电，指示灯亮起后，发送“Hello”。

4.3 实验过程

4.3.1 用户控制场景实验

Telnet 实验：

在连接不同的 IoT 设备时，收集到的指纹信息，具体如表 1 所示。

根据表 1 信息分析，总结出设备指纹特征与结论：

第一，根据相同控制端使用的不同控制程序，选择用户名、密码等收发方式时，信息收发方式存在不同；

第二，根据不同控制端使用的相同控制程序，激活选项与终端类型相同，若攻击者利用此便利远程登录，极有可能欺骗用户行为。由于本实验研究考虑的是攻击者不了解用户的控制端、控制程序等信息情况，所以笨实验将这种情况排除。

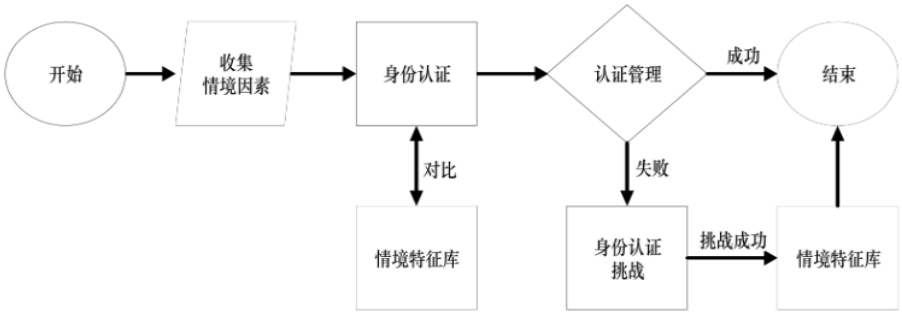

图 1 物联网设备指纹情境认证流程

表 1 连接不同 IoT 设备时不同设备指纹信息表现

软件		IOS 手机 1	IOS 手机 2	安卓手机 1	安卓手机 2	电脑
iTerminal	选项	18	18	—	—	—
	终端类型	VT100	VT100	—	—	—
	用户名 / 密码收发方式	询问式	询问式	—	—	—
Termius	选项	18/27	18/27	—	—	—
	终端类型	Xterm-256 color	Xterm-256 color	—	—	—
	用户名 / 密码收发方式	主动式	主动式	—	—	—
Connectbot	选项	—	—	18	18	—
	终端类型	—	—	Xterm—256 color	Xterm—256 color	—
	用户名 / 密码收发方式	—	—	询问式	询问式	—
命令行	选项	—	—	—	—	18/If/27
	终端类型	—	—	—	—	ANSI

SSH 实验：

通过 SSH 实验，得到设备指纹特征与结论：

第一，对于不同手机的不同控制程序，SSH 的版本信息有所不同。

第二，手机与 IoT 设备进行信息交换的顺序，与电脑与 IoT 设备进行信息交换的顺序不同。其中，手机端方面，手机可以先发送 SHH 信息符号串；电脑端方面，IoT 设备先发送 SHH 信息符号串。

第三，上述特征可以对设备的指纹信息进行有效验证，有效避免非法用户的软件登录行为。

云实验：

通过云实验，得到设备指纹特征与结论：

第一，不同型号的摄像头、手机控制程序，与云服务器的数据交换时涉及的指纹特征信息不同；

第二，在接收到服务器信息后，手机控制程序与云端进行数据交互。

Mirai 实验：

Mirai 实验是考虑 IoT 设备感染 Mirai 病毒后，可以通过设备与服务器间的交互进行流量捕捉。若信息发送方 Bot 设备感染 Mirai 病毒，则其先与 DNS 进行交互，获得 CNC 的 IP 地址。因此，为保证本研究设计的物联网设备指纹情境认证系统有效应用，对感染后的 Bot 设备指纹进行提取设备指纹特征为 \x00\x00\x00\x01，这些数据表示 Bot 设备上线、短时间的数据包连接失败，有效反映出 IoT 设备的 Mirai 病毒感染情况。

4.3.2 DTU 终端设备场景实验

在进行 DTU 终端设备场景实验前，应明确设备指纹提取方式。在用户与 IoT 设备交互过程中，手机端或电脑端会有指纹特征信息，这些特征信息可以成为身份认证的关键信息。当 DTU 终端设备接收到数据，特有的设备指纹信息可以成为身份认证的有力证据，进而有效降低非法用户、非法 DUT 设备访问此设备。常见的流量特征信息提取方式为报文总数、上行报文数、下行报文数、最大报文净荷长度等。针对本实验的实验环境和实验过程，得到网络透传模式、UDC 模式，并用这两种模式进行实验。

基于网络透传模式的实验：

结合实际情况，确定了终端设备与服务器之间的信息交互过程，在此模式下，DTU 成为终端设备与服务器进行信息交互的数据打包转发站。在试验中，通过模块发送注册包信息到服务器中，并让每个数据包的最前端，结合注册包数据。通过实验，提取到 DTU 设备指纹信息：SIM 卡手机号、DTU 设备信息码、200ms 的成帧机制。同时，本实验

通过模块发送心跳机制到网络中发现，当网络连接异常时，模块可以自动检测到无法发送的心跳包数据信息，当发送失败 3 次后，系统会将其确定为异常，并重新尝试连接服务器。由于 DTU 的打包时间为固定模式，所以当打包时间超过 200ms 时，将随即打包数据。

UDC 模式实验：

在此模式下，可以提取到设备指纹特征信息，包括登录、心跳、数据上报信息。通过这些指纹信息收集，可以精准判断出设备是否在线、设备上线时间、设备数据交互情况等，进而对 DTU 设备指纹认证起到关键作用。

4.4 实验结果分析

关于 IoT 设备的双向认证，本研究设计的情境认证方式可以在用户控制端，实现 Telnet/SSH、用户控制端的双向信息认证；在设备端，实现了基于 DTU 设备的设备认证，有效完成了用户控制端、设备的双向信息数据认证，有效提升了设备的使用安全性。同时，通过设备指纹的实验数据分析，结合情境认证训练情况，将指纹认证信息数据存入系统数据库中，实现了设备实际运行数据的验证。综合实验结果数据分析可知，本研究设计的基于物联网设备指纹的情境认证方式对数据的认证护理的精准性为 96%，剩余 4% 数据信息可以通过身份认证挑战完成信息判断。

5 结语

综上所述，信息技术的快速发展，推动了物联网的广泛应用，并使物联网的运行环境愈加复杂，导致物联网设备的安全问题愈加突出。为保证物联网设备运行安全，提出了一种物联网设备指纹情境认证系统，通过指纹情境要素提取和信息判断，完成对 IoT 设备的信息双向认证。为验证系统应用的可行性，以用户控制场景、DTU 终端设备场景为前提，对系统进行 Telnet、SSH、Mirai 病毒实验验证。最终通过决策树，对情境因素进行分类和判断，精准率为 96%，剩余 4% 数据信息可以通过身份认证挑战完成信息判断。但由于实验数据相对较少，各种情境的关联性不强，所以需要在日后研究工作中对其进行补充和完善。

参考文献

[1] 张艳红,杨明剑,马宁,等.基于活体指纹识别与物联网的智能安防系统研究[J].技术与市场,2022,29(1):170-171.

[2] 林俊强,唐艳凤,郑焕坡,等.基于物联网云平台的智能门禁系统设计[J].物联网技术,2022,12(1):95-98.

[3] 李琪阳,董雷.基于朴素贝叶斯的物联网设备指纹算法[J].电子设计工程,2021,29(21):155-158.