Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 8 May 2023

D. von Hugo
Deutsche Telekom
B. Sarikaya

4 November 2022

The Need for New Authentication Methods for Internet of Things
draft-hsothers-iotsens-ps-03.txt

Abstract

In framework of future 6G the need for easy and secure connectivity between a great amount of small devices as sensors and household appliances will be essential. Such massive Internet of Things (mIoT) requires authentication methods which are reliable also in case of vulnerable wireless links and work for simple cheap (dumb) devices.

Aim of this document is to lay ground for the need for new authentication models and admission methods in the framework of devices (e.g., machines in IoT communication) within a (wireless or wireline-based) network.

Simple devices may only have a minimum amount of physical interfaces available. As an example for establishing an out-of-band channel for exchange of authentication material radio sensing technology may serve. This is currently under investigation for Wireless LAN and upcoming cellular radio at both IEEE and 3GPP.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 May 2023.

Table of Contents

1. Introduction

Future networking to make full use of 5G capabilities or even resembling an evolution to beyond 5G will have to exploit a much more heterogeneous environment in terms of network and device connectivity technologies and applications. In addition, ease of use for customers and an as far as possible human-independent (autonomous) operation of a multitude of devices and machines (things) should be enabled.

Basic pre-requisite for flawless operation of any communication service is secure and safe access to the network. Both the device and the network infrastructure have to authenticate each other during

the bootstrapping process, which starts when the device is switched into operational status. Depending on the specific access technology or family of technology variants multiple authentication methods have been developed and deployed. Regarding the aspect of ease of use and in view of the upcoming use case of massive Internet of Things (mIoT) with huge amounts of cheap und thus very simple devices many of the existing authentication methods will not be optimal here. E.g., authentication models like 802.1X [IEEE802.1X] are based on human intervention and do not scale well for mIoT. Same holds true similarly for 3GPP authentication, where user equipment (UE) has to be equipped with a USIM (Universal Subscriber Identity Module) to access a cellular network and the user has to provide a secret key, i.e., PIN (Personal Identification Number).

Also such approach requires exchange of information on the communication channel in advance of the authentication and identification and thus could result in security issues.

To overcome those issues and lower the risk higher levels of admission methods need a second (or out-of-band, OOB) channel to communicate with the device for authentication. Provision of at least two independent channels would allow for and be part of the Multi- or Two-Factor Authentication (MFA/TFA/2FA) required for security in high-risk scenarios.

Device Provisioning Protocol (DPP) developed by Wi-Fi Alliance makes use of an out-of band channel beside the Wi-Fi interface for bootstrapping and authentication [dpp]. Thus another (trusted) device such as a mobile phone can be employed to exchange essential data via, e.g., Bluetooth or Near-Field Communications (NFC). Also visible (QR code or blinking LED) or audible (melody, human speech) information can be used via a smart phone's built-in camera or microphone, assuming that advances in signal processing may make it possible to realize these and similar use cases. More examples are mentioned in [Henning].

However, this approach requires again human intervention and/or a second interface both at the 'dumb' device and at the point of attachment to the network (e.g., Wi-Fi access point). An alternative may be to use the single radio interface in terms of sensing the signal strength and temporal and geographical change of the signal pattern as has been investigated by IEEE and 3GPP:

IEEE802.11 has a project on Wireless LAN (WLAN sensing) and 802.11bf task group (TG) is in charge of this project [BFSFD]. 3GPP is studying for Rel. 19 the topic of Integrated Sensing and Communication [TR22.837]. More discussion on radio sensing can be found in Section 3.

2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. 3GPP and Wireless LAN Sensing

3GPP document [TR22.837] defines many use cases that vary from indoor using 3GPP signal measured by UE to outdoor using 3GPP signal measured at the Base Stations. Use cases include intruder detection in smart home, pedestrian or animal intrusion detection on a highway, rainfall monitoring, flooding in smart cities, Automated Guided Vehicles (AGVs) detection and tracking in smart factories. It is foreseen that operators will define sensing area whereby the Base Stations and UEs can be used in sensing the characteristics of an airborne object of interest generating and reporting sensing measurement data (e.g., related to an unmanned aerial vehicle (UAV) position, velocity) to a 5G sensing processing entity.

IEEE 802.11 Wireless LAN sensing being developed by TGbf is based on obtaining physical Channel State Information (CSI) measurements between a transmitter and receiver WLAN nodes. Using these measurements, presence of obstacles between a transmitter and receiver can be detected and tracked. This way, using feature extraction and classification of artificial intelligence (AI), more higher level tasks like human activity recognition and object detection may become available for authentication purposes. In addition to already proposed use cases as room sensing, i.e., presence detection, gesture recognition, or building a 3D picture of an environment also the unambiguous identification of an IoT device or the owner of that device could be achieved.

Wireless sensing technologies such as New Radio (NR)-based sensing and WLAN sensing aim at acquiring information about a remote object while the corresponding perception data can be utilized for analysis to obtain meaningful information. Here use cases on combining sensor data with other (e.g., location) and transparent sensing as well as protection of sensing information may be adapted to provide information usable for IoT device authentication.

4. IoT Authentication Issues

4.1. General Considerations and Requirements

IoT applications may cover a broad range of domains from smart cities, industry, and homes to personal (e.g., wearable) devices, and can reach a huge number of entities. Since applications as e-health and connection to critical infrastructure may be included, the security requirements in terms of preventing unauthorized access are very high. Therefore very robust authentication mechanisms have to be applied. At the same time depending on the specific scenario a trade-off between resources as processing power and memory as driven by security protocol complexity has to be considered. Therefore it should be possible for the owner to flexibly choose and subsequently agree with the authentication system on the method to authenticate a device and the correspondingly required set of characteristic parameters. Consideration of the amount and type of resources as well as their location and availability will play a role: E.g., whether these resources are provided either within the local system components (e.g., the device itself and the point of attachment or access point) and/or within the network infrastructure (e.g., an edge cloud instance or a central data base).

The result of the detection process (e.g., radio wave analysis outcome as parameters as modulation scheme, number of carriers, and fingerprinting or QR code detection) has to be compared with the required (correct) reference parameter values which are safely and confidentially stored within the network.

On all levels of handling these data, i.e., storage, processing, and transport via a communication network, the integrity of the content has to be preserved. One should keep in mind, that any unintended authentication request should be prevented to minimize the risk of occasional attachment of malicious users to networks and subsequent exposure of sensitive user data.

[RFC8576] serves as a reference for additional details about IoT specific security considerations including the area of authentication and documents their security challenges, threat models, and possible mitigations.

4.2. Exemplary Protocols for IoT Authentication

OAuth [RFC6749] protocol extends traditional client-server authentication by providing a third party with a token. Since such token resembles a different set of credentials compared to those of the resource owner, the device needs not be allowed to use the resource owner’s credentials to access protected resources. In addition [RFC8628] specifies how to complete the authorization request of a device with a one-way channel via a secondary device,

such as a smartphone.

Task of a Public Key Infrastructure (PKI) with its various components (authorities) is to manage (including generation, distribution, operational usage, secure storage as well as revocation) certificates (e.g., of type X.509) to enable authentication and identification of IoT devices. The role of an IoT client to communicate with PKI system may be played by the local access point which usually has corresponding processing capabilities rather than the simple and cheap IoT devices.

In case of manufacturer-installed X.509 certificates the 'Bootstrapping Remote Secure Key Infrastructure' (BRSKI) protocol [RFC8995] provides means for authentication both devices and the network and specifies a Secure Key Infrastructure (SKI) for bootstrapping.

EAP (Extensible Authentication Protocol) [RFC3748] defines a flexible authentication framework for network access of a peer towards an authenticator or authentication server. Advantage of EAP for IoT is the support of multiple authentication mechanisms without need for pre-negotiation. Recently, Nimble out-of-band authentication for EAP or EAP-NOOB [RFC9140] was proposed to apply EAP to very simple IoT devices. Here, the need for pre-established (e.g., manufacturer provided certificate) relation with server or user or pre-provisioning of identifier or credentials could be avoided. For sake of security they need, however, a second interface for out-of-band communication. This OOB channel enables the device to send critical data needed, i.e., a secret nonce to EAP server. In addition, EAP ecosystem may be too complex for simple IoT devices and EAP-NOOB would require user assistance in message exchange for authenticating in-band key exchange. Therefore a more simple approach should be envisioned.

4.3. Assessment of Existing Authentication Methods

In view of the above mentioned methods using out-of band channel for IoT authentication the advantage of a mechanism relying on radio sensing may have the advantage not to need explicit user interaction. Beside it does not require the user to know any key, identifier, or password for the IoT device to be authenticated. For other OOB technics the need for a pre-defined means of identifying the device (e.g., physical, acoustic, photographic or video representation, unique description in terms of parameters, etc.) may be the only prerequisite for authentication. In addition, in case of radio sensing no other interface at the IoT device would be required beyond the radio interface which can be used for both, communication and the OOB transmission of the identity and unique token.

5. The Need for New Authentication Models

We solicit future work on the out-of band channels for device provisioning and the gaps identified below.

5.1. Out-of Band Channel for Device Provisioning

The newly to be designed authentication model for IoT devices shall be applicable to OOB transmission of a certificate to the authenticating entity as via, e.g., above mentioned radio sensing. However, other means to exchange the essential information may also be chosen such as detection by touch, accelerometer, and gyro sensors or cameras. LED (Light Emitting Diode) using LED light indicator and/or emitter available on the device can support LED light based authentication, e.g., via a smartphone with a client for certification. Experiments on such an approach have been set up and tested during lighthouse project (see, e.g., [Lins18], [Oden18]).

Criteria for choice of the corresponding technology depend on the use case and cover are reliable operation (working), scalability, ease of use and convenience, security, and many more.

The created token or signature (fingerprint) shall serve in a similar way as a password [Wang3] to allow the detection and authentication of the device by comparison with pre-shared and stored information.

Bluetooth Mesh Network standard for Bluetooth low energy (BLE) wireless technology [simpleconn] defines Output OOB and Input OOB authentication methods between a device and the provisioner, e.g., an access point.

In case of Output OOB, the unprovisioned device picks a random number and outputs that number in a way which is explained next. For example, if the unprovisioned device is a light bulb, it could blink a given number of times. If the device has an LCD screen, it could show the random number as a multiple digit value. The user of the provisioner inputs the number observed to authenticate the unprovisioned device. After the random number has been input, the provisioner generates and checks a confirmation value. The check confirmation value operation is identical within the overall authentication step, regardless of the authentication method used.

In case of Input OOB, the provisioner generates a random number, displays it, and then prompts the user to input the random number into the unprovisioned device using an appropriate action. For instance, a light switch may allow the user to input the random number by pressing a button an appropriate number of times within a certain period. After finishing the authentication action, the

unprovisioned device sends a Provisioning Input Complete PDU to the provisioner to inform it that the random number has been input. The process continues with the check confirmation value operation like in the case of Output OOB [simpleconn].

For use of 3GPP and Wireless LAN sensing as an OOB channel in IoT authentication, most possibly output OOB channel needs to be investigated. Since input OOB requires user interaction the use of radio sensing as an input OOB channel should not be the approach to be chosen.

5.2. The Gaps

Main gap between existing methods and the new authentication model to be derived is the required user interaction. Another challenge may be naming and re-naming of the devices to enable re-using (e.g., home appliances after moving to a new flat) or replacement (e.g., of a broken light bulb by a new one). For this either use of geo-locational parameters or time stamps with respect to, e.g., time of production or first installation (deployment or start of operation) may be considered. The automatic exchange of the old identity with the new one during re-booting may demand for a standard geospatial naming.

Aim of this document is to stimulate discussion on future directions in work at IETF towards secure and confident authentication of IoT devices to the network, independent of the access technology and the features of the IoT device.

6. IANA Considerations

This document makes no request to IANA for allocation of new registries.

7. Security Considerations

This document raises no new security concerns but tries to identify how to increase security in future IoT by discussing the issues of robust but easy to apply authentication mechanisms.

8. Acknowledgements

Discussions with Jan Janak, Henning Schulzrinne, and Michael Richardson as well as a review by Janfred Rieckers and Jari Arkko helped us improve the draft.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[BFSFD] IEEE, "Institute of Electrical and Electronics Engineers, IEEE P802.11 - TASK GROUP BF (WLAN SENSING) 11-21/0504r2 "Specification Framework for TGbf"", July 2021.

[dpp] Wi-Fi Alliance, "Wi-Fi Device Provisioning Protocol (DPP)", Wi-Fi Alliance Specification version 1.1, 2018, <https://www.wi-fi.org/download.php?file=/sites/default/files/private/Device_Provisioning_Protocol_Specification_v1.1_1.pdf>.

[Henning] Schulzrinne, H., "Do We Still Need Wi-Fi in the Era of 5G (and 6G)?", February 2021.

[I-D.irtf-t2trg-secure-bootstrapping-02] Sethi, M., Sarikaya, B., and D. Garcia-Carrillo, "Terminology and processes for initial security setup of IoT devices", Work in Progress, Internet-Draft, draft-irtf-t2trg-secure-bootstrapping-02, 25 April 2022, <https://www.ietf.org/archive/id/draft-irtf-t2trg-secure-bootstrapping-02.txt>.

[IEEE802.1X] IEEE, "Institute of Electrical and Electronics Engineers, "802.1X - Port Based Network Access Control"", January 2020.

[Lins18] Linssen, A., "Secure Authentication of Remote IoT Devices Using Visible Light Communication: Transmitter Design and Implementation", Columbia University , 2018, <https://www.cs.columbia.edu/~hgs/papers/Lins18_Secure.pdf>.

[Oden18] Odental, H., "Secure Authentication of Remote IoT Devices Using Visible Light Communication: Receiver Design and Implementation", Columbia University , 2018, <https://www.cs.columbia.edu/~hgs/papers/Oden18_Secure.pdf>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004, <https://www.rfc-editor.org/info/rfc3748>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

[RFC8576] Garcia-Morchon, O., Kumar, S., and M. Sethi, "Internet of Things (IoT) Security: State of the Art and Challenges", RFC 8576, DOI 10.17487/RFC8576, April 2019, <https://www.rfc-editor.org/info/rfc8576>.

[RFC8628] Denniss, W., Bradley, J., Jones, M., and H. Tschofenig, "OAuth 2.0 Device Authorization Grant", RFC 8628, DOI 10.17487/RFC8628, August 2019, <https://www.rfc-editor.org/info/rfc8628>.

[RFC8994] Eckert, T., Ed., Behringer, M., Ed., and S. Bjarnason, "An Autonomic Control Plane (ACP)", RFC 8994, DOI 10.17487/RFC8994, May 2021, <https://www.rfc-editor.org/info/rfc8994>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

[RFC9140] Aura, T., Sethi, M., and A. Peltonen, "Nimble Out-of-Band Authentication for EAP (EAP-NOOB)", RFC 9140, DOI 10.17487/RFC9140, December 2021, <https://www.rfc-editor.org/info/rfc9140>.

[simpleconn] Bluetooth Special Interest Group, "Mesh Profile", Version 1.0.1, 2019, <https://www.bluetooth.com/specifications/specs/mesh-profile-1-0-1/>.

[TR22.837] 3GPP Draft Technical Report Release 19, "3GPP, "Study on Integrated Sensing and Communication"", 2022.

[Wang3] Wang, H., Lymberopoulos, D., and J. Liu, "Sensor-Based User Authentication", EWSN 2015, LNCS 8965, 168 , 2015.

Acknowledgements

Authors' Addresses

Dirk von Hugo
Deutsche Telekom
Deutsche-Telekom-Allee 9
64295 Darmstadt
Germany
Email: Dirk.von-Hugo@telekom.de

Behcet Sarikaya
Email: sarikaya@ieee.org