Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 21 April 2022

D. von Hugo
Deutsche Telekom
B. Sarikaya

18 October 2021

Problem Statement for Internet of Things Sensing
draft-hsothers-iotsens-ps-00

Abstract

The document attempts to establish hardware based Internet of Things authentication as a future networking area beyond 5G going into 6G for standardization. The problem of hardware authentication is discussed and its relationship with Wireless Local Area network collaborative and/or multi-band sensing is established and then recent research efforts in the area are indicated.

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 21 April 2022.

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 human-independent operation of a multitude of devices and machines (things) has to be provided.

Therefore current authentication models like 802.1X [IEEE802.1X] which are based on human intervention do not fit well. Also this model does not scale well for the Internet of Things (IoT). What we need is hardware based admission model. Such a model will enable many new applications as we explain more in this document.

IEEE 802.11 [IEEE802.11] has a project on Wireless LAN (WLAN sensing) and 802.11bf task group (TG) in charge of this project [BFSFD]. Use cases for 802.11bf TG includes room sensing, i.e., presence detection, counting the number of people in the room, localization of active people, audio with user detection, gesture recognition at different ranges, device proximity detection, home appliance control. There are also health care related use cases like breathing/heart rate detection, surveillance of persons of interest, building a 3D picture of an environment, as, e.g., in-car sensing for driver sleepiness detection [BFUseCases].

Hardware based authentication that we address in this document builds on similar use cases. We can summarize the use cases we are currently considering here: Authenticating the device that is playing a melody, or a person has just touched; authenticating devices, i.e.

smart teapot with certain manifests, like blinking red and blue; authenticate the device when a camera is pointed at it; and the like [Henning]. 802.11bf sensing project provides proper framework for hardware based authentication because 802.11 or Wi-Fi devices are more and more diverse spanning from personal computers, smartphones, televisions, tablets, and all sorts of IoT devices or sensors.

TGbf is also working on Specification Framework Document with an outline of each of the functional blocks that will be a part of the final amendment like wireless LAN sensing procedure [BFSFD]. TGbf sensing is based on obtaining physical Channel State Information (CSI) measurements between a transmitter and receiver WLAN nodes, called stations (STA). Using these measurements, presence of obstacles between a transmitter and receiver can be detected and tracked. This way, using feature extraction and classification provided by means of artificial intelligence (AI), more higher level tasks like human activity recognition and object detection are available for authentication purposes, while hardware based authentication use cases can be achieved through computation of phase differences, etc.

TGbf Wi-Fi Sensing (SENS) is achieved by signaling between just an initiator and a responder. TGbf may also define more effective collaborative SENS (in short, CSENS) where multiple SENS-enabled devices can collaborate as a group in an orderly fashion to capture additional information about the surrounding environment [Rest21].

1.1. 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.

Sensing (SENS) is defined as the usage of received Wi-Fi signals from

a Station (STA) to detect features (i.e., range, velocity, angular, motion, presence or proximity, gesture, etc.) of intended targets (i.e., object, human, animal, etc.) in a given environment (i.e., house, office, room, vehicle, enterprise, etc.).

Collaborative sensing (CSENS) defines the operation in which multiple SENS enabled devices can collaborate as a group in an orderly fashion to capture additional information about the surrounding environment and allow for more precise detection, thus enabling a more reliable authentication.

Multi-band sensing is defined as sensing using both sub-7-GHz Channel State Information (CSI) measurements that provide indication of relatively large motions and that can propagate through obstacles (e.g., walls) and 60-GHz Received Signal Strength Indicator (RSSI) measurements at mmWave that provide highly-directional information through the usage of beamforming toward a given receiver, but have small range due to the presence of blockers (e.g., walls).

2. Hardware Based Authentication

Aim of this document is to lay ground for the need for new authentication models in the framework of devices (e.g., machines in IoT communication) within a (wireless or wireline-based) network. Currently employed authentication models (such as e.g., 802.1X certificate model) is based on a human being using the machine and providing credentials (e.g., user name/password or a permitted digital certificate) to the authenticator. Similarly, for user equipment (UE) to access a cellular network the device has to be equipped with a USIM and the user has to provide a secret key, i.e., PIN (Personal Identification Number). With the use case of massive IoT (mIoT) as foreseen, e.g., in 5G and with an increasing amount of devices within a household (smart home) and/or in the ownership of a customer (smart watch etc.) the need for an ease-of-use hardware-based admission model arises.

Focusing on corresponding procedures starting with detection (sensing) of a new device and subsequent mutual authenticating of the device by and to the network a set of potential technologies are identified and described to allow for analysis in terms of criteria

as reliable operation (working), scalability, ease of use and convenience, security, and many more. Sensing is critical to Hardware Based Authentication because sensing (together with intelligent interpretation using possibly neural network models) will allow the detection of the device playing a melody, blinking red and blue, being pointed at, or somebody just touched and the like. Furthermore, the method should be applicable to future generations of network and of users, upcoming new applications and devices, assuming that todays established standard procedures do not fulfill the requirements sufficiently.

Hardware based authentication should leverage collaborative and multi-band sensing technologies to enable sensing with much higher precision and capacity using the state-of-art equipment. Also equally important is the use of all artificial intelligence and neural networks research results developed by the academia.

3. State of the Academic Approaches to IoT Authentication

A detailed review on current topics in IoT Security, Device Authentication and Access Control was provided in [Inayat]. The following list of literature on sensor data and WiFi sensing for securing and authenticating a user and a device shows the wide range of approaches and interest in this topic [Rest21].

[Ma], [Wang], [Zhu], [Wang2], and [Qian] provide a holistic overview on the evolution of Wi-Fi technology and on investigations in opportunistic applications of Wi-Fi signals for gesture and motion detection.

[Henning2] is investigating geospatial access control for IoT. There are attribute, role and identity based, time based and geospatial access control techniques. Real-world IoT access control policies will be a combination of all three, leading to powerful access control techniques to use in practice such as in university campus. Such access control or authorization techniques will likely be used in conjunction with Hardware Based Authentication.

Other notable literature includes [Al-Qaness] on the so-called

device-free CSI-based Wi-Fi sensing mechanism, [Pahlavan] using Wi-Fi signals for gesture and motion detection as well as for authentication and security, [Lui] distinguishing between Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) conditions in case of obstacles appearing between the transmitter and the receiver [Guo] studying HuAc (Human Activity Recognition) as a combination of WiFi-based and Kinect-based activity recognition system, [FURQAN] analyzing the wireless sensing and radio environment awareness mechanisms, highlighting their vulnerabilities such as dependency of sensing modes on external signals, and provides solutions for mitigating them, e.g., the different threats to REM (radio environment mapping) and its consequences in a vehicular communication scenario.

[Ma2] has studied reliable SENS algorithm for human and animal identification. The aim is to make it resilient to spoofing and adverse channel conditions, i.e., presence of noise and interference from other technologies.

[Restuccia] investigates data driven algorithms, neural networks, especially convolutional neural network (CNN) or digital signal processing (DSP) block to classify complex sensing phenomena. Also [Liao] and [Liao2] proposed to enhance security of industrial wireless sensor networks (IWSNs) by neural network based algorithms for sensor nodes' authentication and implementations in IWSNs have shown that an improved convolution preprocessing neural network

(CNN)-based algorithm requires few computing resources and has extremely low latency, thus enabling a lightweight multi-node PHY-layer authentication.

Further research on these and similar issues can be found in [Tian], [Bai], and [Axente].

4. IoT Authentication Protocols

Since IoT applications cover a broad range of domains from smart cities, industry, and homes to personal (e.g., wearable) devices, including security and privacy sensitive areas as e-health, and can reach a huge number of entities the security requirements in terms of preventing unauthorized access to data 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 and security protocol complexity has to be considered. Also a plethora of attack scenarios has to be in focus as well as scalability of the considered implicit and explicit hardware- and software-based authentication procedures. [RFC8576] serves as a reference for details about IoT specific security considerations including the area of authentication and documents their specific security challenges, threat models, and possible mitigations.

A more recent work surveys secure bootstrapping and onboarding protocols [I-D.irtf-t2trg-secure-bootstrapping-00] developed by IETF as well as other standards developing organizations such as IEEE, FIDO alliance, Open Connectivity Foundation (OCF), Open Mobile Alliance (OMA).

Lastly, the Open Authorization (OAuth) [RFC6749] protocol in the area of authorization is a standard for access delegation. It extends traditional client-server authentication by providing a third party client with a token instead of allowing it to use the resource owner's credentials to access protected resources while such token resembles a different set of credentials than those of the resource owner.

5. Hardware IoT Authentication Problem

Most of the state-of-art hardware identification techniques to authenticate the user use finger prints a.k.a. touch id and facial identification and they use detection by hardware i.e. touch, accelerometer, and gyro sensors or cameras. They are based on creating a signature, or the user's already stored password [Wang3].

On the other hand to authenticate a device based on a set of characteristic parameters which should be flexibly chosen by the owner and subsequently made known to the authentication system will require a certain level of processing and storage capacity either within the local system components (e.g., the device itself and the wireless point of attachment or access point) and/or within the network (e.g., an edge cloud instance or a central data base). The result of the detection process (e.g., radio wave analysis outcome in

terms of parameters as modulation scheme, number of carriers, and fingerprinting) has to be compared with the required (correct) parameter values which are safely stored within the network components. 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 to networks and subsequent exposure to attack to sensitive user data.

5.1. Architectural and Procedural Issues for Future IP-based IoT-Authentication

Here we will discuss possible solutions on IP level and identify benefits and potential gaps towards the requirements of next generation IoT systems. On IP or network layer for IPv6 IPsec protocol suite is mandatory and provides end-to-end security for authentication procedures, ensuring confidentiality and integrity of the transmitted data. Authentication for IoT may rely on a protocol as 6LowPAN (Low-power Wireless Personal Area Network) which is defined for optimizing the efficient routing of IPv6 packets for resource constrained machine- type communication applications.

When compared to a fully certificate-based authentication, however, a hardware-based AAA mechanism relying e.g., on WiFi sensing gesture detection does not require the user to know any key, identifier, or password for the device to be authenticated. A pre-defined type of access to the device (e.g., physical, photographic or video representation, unique description in terms of parameters, etc.) shall be sufficient for authentication.

[RFC8995] on 'Bootstrapping Remote Secure Key Infrastructure' (BRSKI) deals with authentication of devices, including sending authorizations to the device as to what network they should join, and how to authenticate that network by specifying automated bootstrapping of an Autonomic Control Plane (ACP). Secure Key Infrastructure (SKI) bootstrapping using manufacturer-installed X.509 certificates combined with a manufacturer's authorizing service, both online and offline, is called the Bootstrapping Remote Secure Key Infrastructure (BRSKI) protocol. Bootstrapping a new device can

occur when using a routable address and a cloud service, only link-

local connectivity, or limited/disconnected networks and includes support for deployment models with less stringent security requirements. When the cryptographic identity of the new SKI is successfully deployed to the device, completion of bootstrapping is achieved. A locally issued certificate can be deployed to the device via the established secure connection as well.

6. IANA Considerations

TBD.

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

TBD.

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

[Al-Qaness] Al-Qaness, M.A.A., Abd Elaziz, M., Kim, S., Ewees, A.A., Abbasi, A.A., Alhaj, Y.A., and A. Hawbani, "Channel State Information (CSI) from Pure Communication to Sense and Track Human Motion: A Survey", Sensors 2019, 19(15), 3329 , July 2019.

[Axente] Axente, M.-S., Dobre, C., Ciobanu, R.-I., and R. Purnichescu-Purtan, "Gait Recognition as an Authentication Method for Mobile Devices", Sensors 2020, 20, 4110 , July 2020.

[Bai] Bai, L., Zhu, L., Liu, J., Choi, J., and W. Zhang, "Physical Layer Authentication in Wireless Communication Networks: A Survey", Journal of Communications and Information Networks Vol.5, No.3, September 2020.

[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.

[BFUseCases] IEEE, "Institute of Electrical and Electronics Engineers, IEEE P802.11 - TASK GROUP BF (WLAN SENSING) 11-20/1712r2 "WiFi Sensing Use Cases"", January 2021.

[FURQAN] Furqan, H.M., Solaija, M.S.J., Tuerkmen, H., and H. Arslan, "Wireless Communication, Sensing, and REM: A Security Perspective", IEEE Open Journal of the Communications Society Vol. 2 , January 2021.

[Guo] Guo, L., Wang, L., Liu, J., Zhou, W., and B. Lu, "HuAc: Human Activity Recognition Using Crowdsourced WiFi Signals and Skeleton Data", Hindawi Wireless Communications and Mobile Computing, Volume 2018 , February 2021.

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

[Henning2] Jan Janak, Luoyao Hao and Henning Schulzrinne, ., "How do we program the Internet of Things at scale?", September 2021.

[I-D.irtf-t2trg-secure-bootstrapping-00] Sethi, M., Sarikaya, B., and D. Garcia-Carrillo, "Secure IoT Bootstrapping: A Survey", Work in Progress, Internet-Draft, draft-irtf-t2trg-secure-bootstrapping-00, 7 April 2021, <https://www.ietf.org/archive/id/draft-irtf-t2trg-secure-bootstrapping-00.txt>.

[IEEE802.11] IEEE, "IEEE Std. 802.11-2016", December 2016, <https://standards.ieee.org/findstds/standard/802.11-2016.html>.

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

2020.

[Inayat] Ali, I., Sabir, S., and Z. Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 8 , August 2016.

[Liao] Liao, R.-F., Wen, H., Wu, J., Pan, F., Xu, A., Jiang, Y., Xie, F., and M. Cao, "Deep-learning-based physical layer authentication for industrial wireless sensor networks", Sensors 2019, 19(11), 2440 , May 2019.

[Liao2] Liao, R.-F., Wen, H., Wen, H., Xie, F., Pan, F., Pan, F., and F. Xie, "Multiuser Physical Layer Authentication in Internet of Things With Data Augmentation", IEEE Internet of Things Journal, vol. 7, no. 3, pp. 2077-2088 , March 2020.

[Lui] Liu, J., Wang, L., Fang, J., Guo, L., Lu, B., and L. Shu, "Multi-Target Intense Human Motion Analysis and Detection Using Channel State Information", Sensors 2018, 18(10), 3379 , October 2018.

[Ma] Ma, Y., Arshad, et al, S., and , "Location-and Person-Independent Activity Recognition with WiFi, Deep Neural Networks, and Reinforcement Learning,", 2021.

[Ma2] Ma, Y. and G. Zhou, et al, "WiFi Sensing with Channel State Information: A Survey,", ACM Computing Surveys (CSUR), , vol. 52, no. 3, pp. 1-36, 2019.

[Pahlavan] Pahlavan, K. and P. Krishnamurthy, "Evolution and Impact of Wi Fi Technology and Applications: A Historical Perspective", Springer Science+Business Media, LLC, part of Springer Nature 2020 , November 2020.

[Qian] Xian, K. and C. Wu, et al, "Widar: Decimeter-level Passive Tracking via Velocity Monitoring with Commodity WiFi,", Proc. of ACM MobiCom, , 2017.

[Rest21] Restuccia, F., "IEEE 802.11bf: Toward Ubiquitous Wi-Fi Sensing", arXiv preprint arXiv:2103.14918 7 pages, March 2021.

[Restuccia] Restuccia, F. and T. Melodia, "Deep Learning at the Physical Layer: System Challenges and Applications to 5G and Beyond,", IEEE Communications Magazine, , vol. 58, no. 10, pp. 58-64, 2020.

[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>.

[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>.

[Tian] Tian, Q., Lin, Y., Guo, X., Wang, J., AlFarraj, O., and A. Tolba, "An Identity Authentication Method of a MIoT Device Based on Radio Frequency (RF) Fingerprint Technology", Sensors 2020, 20(4), 1213 , February 2020.

[Wang] Wang, X. and C. Yang, et al, "TensorBeat: Tensor Decomposition for Monitoring Multiperson Breathing Beats with Commodity WiFi,", ACM Transactions on Intelligent Systems and Technology (TIST), , vol. 9, no. 1, pp. 1-27, 2017.

[Wang2] Wang, X. and C. Yang, et al, "PhaseBeat: Exploiting CSI Phase Data for Vital Sign Monitoring with Commodity WiFi Devices,", Proc. of IEEE ICDCS, , 2017.

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

[Zhu] Zhu, H. and F. Xiao, et al, "R-TTWD: Robust device-free through-the-wall detection of moving human with WiFi,", IEEE Journal on Selected Areas in Communications, , vol. 35, no. 5, pp. 1090-1103, 2017.

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