IEEE P802.18
Radio Regulatory Technical Advisory Group (RR-TAG)

Proposed Comment to FCC NPRM: Cybersecurity Labeling for Internet of Things				
Date: 2023-09-28				
Author(s):				
Name	Company	Address	Phone	Email
Hassan Yaghoobi	Intel Corp.			hassan.yaghoobi@intel.com
Carol Ansley	Cox			carol@ansley.com
David Goodall	Morse Micro			dave@morsemicro.com
Mike Montemurro	Huawei			montemurro.michael@gmail.com

This document drafts a proposed comment to FCC NPRM: Cybersecurity Labeling for Internet of Things.

Electronic filing [September 28, 2023]

Erika Olson
Acting Chief Cybersecurity and Communications Reliability Division
Public Safety and Homeland Security Bureau
Federal Communications Commission
Washington, DC

Re: Comment to NPRM: Cybersecurity Labeling for Internet of Things

Dear Acting Chief Olson,

IEEE 802 LAN/MAN Standards Committee ("IEEE 802 LMSC") thanks the Federal Communications Commission (FCC) for issuing the consultation on the Notice of Proposed Rulemaking ("NPRM"): Cybersecurity Labeling for Internet of Things and for the opportunity to provide comments.

IEEE 802 LAN/MAN Standards Committee (IEEE 802 LMSC) is a leading consensus-based open standards development committee for networking standards that are used by industry globally. It produces standards for networking devices, including wired and wireless local area networks ("LANs" and "WLANs"), wireless specialty networks ("WSNs"), wireless metropolitan area networks ("Wireless MANs"), and wireless regional area networks ("WRANs"). Technologies produced by implementers of our standards are a critical element for all networked applications today.

IEEE 802 LMSC is a committee of the IEEE Standards Association and of Technical Activities, two of the Major Organizational Units of the IEEE. IEEE has about 400,000 members in over 160 countries and its core purpose is to foster technological innovation and excellence for the benefit of humanity. IEEE is also a major accredited standards development organization whose standards are recognized world-wide. In submitting this document, IEEE 802 LMSC acknowledges and respects that other components of IEEE Organizational Units may have perspectives that differ from, or compete with, those of IEEE 802 LMSC. Therefore, this submission should not be construed as representing the views of IEEE as a whole[1].

IEEE 802 LMSC applauds the Commission's NPRM that proposes a cybersecurity labeling program for Internet of Things (IoT). IEEE 802 LMSC recognizes the Commission's goal of improving consumer confidence and understanding of the security of their connected devices and supports proposed voluntary cybersecurity labeling program for such devices.

Please find below the IEEE 802 LMSC's comments, which provides the Commission with the latest information on IEEE 802's standards projects related to IoT devices operating in unlicensed bands, our support on selected comments about industry-led cybersecurity standards, scope of cybersecurity labeling, testing, and conformity.

IEEE 802 standards for Internet of Things devices

[1] This document solely represents the views of IEEE 802 LMSC and does not necessarily represent a position of either the IEEE or the IEEE Standards Association.

IEEE 802 wireless technologies such as IEEE 802.11 and IEEE 802.15 have been instrumental in enabling a rich diversity of IoT devices. This diversity includes, but is not restricted to, smart meters, smart lighting, smart plugs, switches and controls, sensor devices, locks, home appliances, and video cameras. In addition, many IoT devices combine sensors with cameras to support applications such as smart doorbells, and security cameras with motion detection or smoke detection, etc.

Of particulate note is the IEEE Std 802.11ah-2016 standard[2] and the IEEE Std 802.15.4-2020 standard[3]. The former, known as Wi-Fi HaLow in the marketplace, was developed with long range, low power sensor and IoT networks and applications such as agriculture[4] in mind. The latter was developed to support applications such as smart metering, known as Wi-SUN in the marketplace, and includes features such as location discovery and device ranging. Some other examples of the IoT devices which implement IEEE 802.15.4 technologies are TV remote controls, lighting, window and door locks, heating and air conditioning systems, alarm systems, and remote medical monitoring.

Standardized security mechanisms for IEEE 802.11 based IoT devices

The same robust security mechanisms defined in IEEE Std 802.11-2020 standard[5] that are found in consumer smartphone and PC products are available to IEEE 802.11 based IoT devices.

IEEE Std 802.11-2020 standard provides a security framework for wireless communications that includes access control through the IEEE Std 802.1X-2020 standard[6], robust authentication, data confidentiality, and key management. The IEEE 802.1X-2020 protocols are defined to establish a secure link for communications between the IoT device and the network. For home networks, the IEEE Std 802.11-2020 standard offers password-based authentication that is resistant to dictionary attacks. For managed networks, IoT devices can be authenticated using Authentication, Authorization, and Accounting (AAA) infrastructure.

IEEE Std 802.11-2020 standard provides two cryptographic encapsulation mechanism to ensure data confidentiality and data origin authenticity. Counter Mode (CTR) with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encapsulation provides Advanced Encryption Standard (AES) encryption with CTR for data confidentiality. Galois/Counter Mode Protocol (GCMP) provides AES encryption with GCM for integrity protection. Both mechanisms can be

[2] "IEEE Standard for Information technology—Telecommunications and information exchange between systems - Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation," in IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016), vol., no., pp.1-594, 5 May 2017, doi: 10.1109/IEEESTD.2017.7920364.

[3] "IEEE Standard for Low-Rate Wireless Networks," in IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015), vol., no., pp.1-800, 23 July 2020, doi: 10.1109/IEEESTD.2020.9144691.

[4] Wi-Fi Alliance: The future of farming: Testing the rural range of Wi-Fi CERTIFIED HaLow™. Available online [accessed: 28 September 2023]

[5] "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016) , vol., no., pp.1-4379, 26 Feb. 2021, doi: 10.1109/IEEESTD.2021.9363693.

[6] "IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control," in IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004), vol., no., pp.1-205, 5 Feb. 2010, doi: 10.1109/IEEESTD.2010.5409813.

established with either 128 or 256 bit key sizes. IEEE Std 802.11-2020 standard also provides data integrity and replay protection for broadcast/multicast management frames using AES in CMAC and GMAC modes with either 128 or 256 bit key sizes. All security protocols defined in the IEEE Std 802.11-2020 standard require fresh cryptographic keys and corresponding security associations. The standard provides procedures to establish fresh keys for both establishing a new communication link as well as refreshing keys on an existing link.

Industry-led Cybersecurity Standards

IEEE 802 LMSC supports the Commission's recognition of industry-led development, implementation, and testing of cybersecurity standards.

IEEE 802 LMSC believes that there is no need to convene a Commission-sponsored group to develop standards to avoid replicating the work already completed or those projects underway by industry-led standards bodies, in particular the NIST publications[7,8] that form the basis of the proposed voluntary requirement. Security protocols defined in the IEEE Std 802.11-2020 standard, using the IEEE Std 802.1X-2020 standard, are also certified as part of the Wi-Fi Alliance's Wi-Fi CERTIFIED WPA3 program[9].

IEEE 802 LMSC recommends the Commission to evaluate cybersecurity standards developed by approved or accredited industry organizations for adoption under the IoT Cybersecurity Labeling Program. Having said that, we recommend the Commission also consider ongoing industry work (e.g., IEEE 802.15 Working Group Task Group 4ac in IEEE 802 LMSC) in its evaluation.

Scope of Cybersecurity Labeling

IEEE 802 LMSC believes that the scope of the proposed cybersecurity labeling program should be carefully studied and limited to IoT consumer products. More specifically, IEEE 802 LMSC proposes to adopt NIST Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products[10] and exclude common general purpose computing equipment (e.g., personal computers, smartphones) as well as general internet and networking infrastructure (e.g., internet routers and switches).

In addition, to meet the goal of improving consumer confidence and understanding of the security of connected devices, IEEE 802 LMSC recommends to consider focusing on labeling IoT end products and exclude other components such as modules, gateways, backends, or applications.

Cybersecurity Testing and Conformity

IEEE 802 LMSC supports providing options for device manufacturers testing and self-assessment as well as FCC-approved, industry accredited labs (e.g., Wi-Fi Alliance authorized test labs[11]) or

[7] M. Fagan, *et al.*, "Profile of the IoT Core Baseline for Consumer IoT Products," NIST IR 8425, September 2022. Available online [accessed: 28 September 2023]

[8] M. Fagan, *et al*., "Foundational Cybersecurity Activities for IoT Device Manufacturers," NIST IR 8259, May 2020. Available online [accessed: 28 September 2023]. This paper defines "transducer" as an element of the definition of an IoT device.

[9] Wi-Fi Alliance: Security. Available online [accessed: 28 September 2023]

[10] Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products, Section 2.1 Scope of an IoT Product, February 2022. Available online [accessed: 28 September 2023]

[11] Wi-Fi Alliance: Certification, Authorized Test Labs. Available online [accessed: 28 September 2023]

by an FCC-approved CyberLAB. IEEE 802 LMSC believes that availability of these options for conformity is key in the efficiency of compliance programs and hence critical in successful adoption of such a voluntary program. Details of such options and the specific scope of such testing is a subject of further study.

Conclusion

IEEE 802 LMSC thanks the Commission for the opportunity to comment on this important NPRM on cybersecurity labeling program for IoT and supports initiating the voluntary labeling program. We respectfully request the Commission to consider our comments listed in this response.

Respectfully submitted

By: /ss/.
Paul Nikolich
IEEE 802 LAN/MAN Standards Committee Chairman
em: p.nikolich@ieee.org