IEEE 802
Privacy EC SG

IEEE 802 Privacy EC SG Proposed CSD

Date: 2015-07-15

Author(s):

Name	Affiliation	Address	Phone	Email
Juan Carlos Zuniga	InterDigital		+15149046300	j.c.zuniga@ieee.org

Abstract

This document contains the IEEE 802 Privacy Executive Committee SG proposed CSD.

1. IEEE 802 criteria for standards development (CSD)

The CSD documents an agreement between the WG and the Sponsor that provides a description of the project and the Sponsor's requirements more detailed than required in the PAR. The CSD consists of the project process requirements, 0, and the 5C requirements, 0.

1.1 Project process requirements

1.1.1 Managed objects

Describe the plan for developing a definition of managed objects. The plan shall specify one of the following:

a) The definitions will be part of this project.
b) The definitions will be part of a different project and provide the plan for that project or anticipated future project.
c) The definitions will not be developed and explain why such definitions are not needed.

This recommended practice document does not specify any managed objects.

1.1.2 Coexistence

A WG proposing a wireless project shall demonstrate coexistence through the preparation of a Coexistence Assurance (CA) document unless it is not applicable.

a) Will the WG create a CA document as part of the WG balloting process as described in Clause 13?
b) If not, explain why the CA document is not applicable.

A CA document is not applicable because this project does not specify wireless spectrum operations.

1.2 5C requirements

1.2.1 Broad Market Potential

Each proposed IEEE 802 LMSC standard shall have broad market potential. At a minimum, address the following areas:

a) Broad sets of applicability.

New Internet applications are being used across multiple networks and devices. These developments bring enormous economic and social value to individuals and to society as a whole. However, such value may not be fully achieved without successfully addressing the growing privacy threat.

b) Multiple vendors and numerous users.

Most Internet connections make use of technologies developed in IEEE 802 (e.g. IEEE 802.1, 802.3, 802.11, 802.15, etc.), and some companies have already started implementing privacy features on top of IEEE 802 standards. Providing privacy features is already seen as a business advantage, as users can continue to have confidence and trust in Internet technologies, applications and services. This recommendation will foster continued growth of deployment of IEEE 802 technologies for communication devices.

1.2.2 Compatibility

Each proposed IEEE 802 LMSC standard should be in conformance with IEEE Std 802, IEEE 802.1AC, and IEEE 802.1Q. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with IEEE 802.1 WG prior to submitting a PAR to the Sponsor.

a) Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q?

Yes

b) If the answer to a) is no, supply the response from the IEEE 802.1 WG.

The review and response is not required if the proposed standard is an amendment or revision to an existing standard for which it has been previously determined that compliance with the above IEEE 802 standards is not possible. In this case, the CSD statement shall state that this is the case.

1.2.3 Distinct Identity

Each proposed IEEE 802 LMSC standard shall provide evidence of a distinct identity. Identify standards and standards projects with similar scopes and for each one describe why the proposed project is substantially different.

There is currently no standard that defines a privacy threat model and associated recommended practice for IEEE 802 technologies.

1.2.4 Technical Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence that the project is technically feasible within the time frame of the project. At a minimum, address the following items to demonstrate technical feasibility:

a) Demonstrated system feasibility.

Privacy threat models have been developed in the industry by standards development organizations, such as the Internet Engineering Task Force (IETF). The recommended practice will define recommendations that can be followed by standards developers to improve privacy.

b) Proven similar technology via testing, modeling, simulation, etc.

The IEEE 802 LAN/MAN Standards Committee and the IETF have successfully carried out three experiments testing the feasibility of a proposed solution to address privacy risks associated with tracking globally-unique media access control (MAC) addresses in wireless networks based on IEEE 802.11™. Technical reports of these experiments have been published on the Privacy EC SG document area [Ref 1] [Ref 2].

1.2.5 Economic Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence of economic feasibility. Demonstrate, as far as can reasonably be estimated, the economic feasibility of the proposed project for its intended applications. Among the areas that may be addressed in the cost for performance analysis are the following:

a) Balanced costs (infrastructure versus attached stations).

The recommended practice will consider equally the possible cost implications on the stations and network infrastructure.

b) Known cost factors.

Recommended practices described in the specification will likely require changes in firmware and sowftware. The cost factors for these transitions are minimal and understood.

c) Consideration of installation costs.

Installation costs of mitigation methods is expected to be minimal or zero in most cases. For instance, experiements have been carried out at the group's meetings and the cost to develop and install the software tools used to implement some of the 802.11 privacy risk mitigation solutions is minimal compared to the cost of development of 802.11 chipsets.

d) Consideration of operational costs (e.g., energy consumption).

Freseen operational costs of mitigation methods is expected to be minimal or actual savings gain, like the case of personal data minimization on communications protocols, which reduces the number and size of probes and scans, which reduces energy consumption.

e) Other areas, as appropriate.

None.

References

1 "WiFi Privacy network experiment at IETF91", Carlos Bernardos, Fabio Giust, Antonio de la Oliva, Juan Carlos Zuniga; January 2015; https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0025-01-0000-wifi-privacy-network-experiment-at-ietf91.pptx

2 "WiFi Privacy network experiment at IEEE 802 Berlin Plenary and IETF92", Carlos Bernardos, Antonio de la Oliva, Juan Carlos Zuniga; July 2015; https://mentor.ieee.org/privecsg/dcn/15/privecsg-15-0028-00-0000-wifi-privacy-network-experiment-at-ieee-802-may-plenary-and-ietf91-meetings.pptx