Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

IEEE P802E

Privacy Considerations: Threat mitigation strategies

Date: 2018-03-08

Juan Carlos Zuniga 3/8/18 11:49 AM
Deleted: 2

Juan Carlos Zuniga 3/8/18 11:50 AM
Deleted: 28

Author(s):

Name	**Affiliation**	**Address**		
Juan-Carlos Zúñiga	Sigfox	juancarlos.zuniga@sigfox.com		
Amelia Andersdotter	ARTICLE 19	amelia@article19.org		
Mathieu Cunche	Univ. Lyon, INSA Lyon, Inria, CITI	mathieu.cunche@inria.fr		

Abstract

Revisions to Sections 3, 6 and 8 of Privacy Recommendations draft v. 0.07 amending recommendations, definitions and descriptive texts. The recommendations section takes cues from chiefly the Internet Engineering Task Force, while staying true to the peculiarities and mandate of the 802 LMSC. They also encompass the fullness of 802 activities, having been written to accommodate enough flexibility that it is suitable for both the wired and wireless specifications being developed in various working groups, while providing a strong framework for standard developers in either community to assess their privacy impact.

Juan Carlos Zuniga 3/7/18 10:04 AM

Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM

Deleted: 2

3. Definitions

For the purpose of this Recommended Practice, the following definitions apply:

3.1 Attack: the process of acting on one or several mediums or devices to obtain (in the context of this document) personally identifiable information.

3.2 Active adversary: An adversary who emits frames as part of the attack in order to cause a target to emit PII.

3.3 Adversary: A threat agent who is taking steps to fingerprint one or more targets. In the context of the threat analysis examined by the Recommended Practice, the adversary is assumed to have the capability to observe, manipulate or inject frames from anywhere on the medium, on the full communications path, on the administrative network, etc.

3.4 Correlation: the combination of several elements that provide identification or information about a person or a device.

3.5 Eavesdropping: the process of observing one or several mediums or devices in order to obtain personally
identifiable information.

3.6 Fingerprinting: the process of uniquely identifying (with a sufficiently high probability) a device or a person.

3.7 Identifier: The name, address, label, or distinguishing index, of a structure, service, medium or entity included in the specification.

3.8 Information element: a field or set of fields defined in an IEEE 802 standard which is used to convey protocol information and it is self-contained.

3.9 Passive adversary. An adversary who observes frames but does not emit frames as part of the attack.

3.10 Pattern: a combination of elements that form an identifiable repeating sequence.

3.11 Persistent identifier: An identifier that is reused at some point after the time where it was first used by reference to the same structure, service, medium or entity.

3.12 Personally Identifiable Information (PII): Any data that directly or indirectly identifies an individual or from which identity or contact information of an individual can be derived, including data which allows the identification of an individual based on correlations or patterns recognition or analysis.

3.13 Personal Correlated Information (PCI): Data gathered about a person by observing devices associated with that person.

3.14 Personal device: a device used by a single individual or a small group of individuals, such that identification of the device also allows identification of its user or group of users.

3.15 Respondent: The network device to which a target is intending to communicate.

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Amelia Andersdotter 2/14/18 1:35 AM
Deleted: actively…acting on one or se ... [1]

Amelia Andersdotter 2/14/18 1:36 AM
Deleted: Attacker.

Juan Carlos Zuniga 3/8/18 9:03 AM
Deleted: their

Amelia Andersdotter 2/26/18 7:06 PM
Deleted: An adversary is assumed to have the capabilities of the Most Powerful Attacker Model [KMM].

Juan Carlos Zuniga 2/22/18 9:22 AM
Deleted: and …anipulate or inject Targ ... [2]

Juan Carlos Zuniga 3/7/18 6:15 PM
Deleted: 8

Amelia Andersdotter 2/14/18 1:36 AM
Deleted: Attacker.…An adversary who ... [3]

Juan Carlos Zuniga 3/7/18 6:15 PM
Deleted: 9

Juan Carlos Zuniga 3/7/18 6:15 PM
Deleted: 10

Juan Carlos Zuniga 3/7/18 6:15 PM
Deleted: 11

Amelia Andersdotter 2/13/18 7:09 PM
Deleted: NOTE —Includes otherwise non-personal information when associated or combined with personal information. PII may not directly include personal informatic ... [4]

Juan Carlos Zuniga 3/7/18 6:15 PM
Deleted: 12

Amelia Andersdotter 2/26/18 6:55 PM
Deleted: .… Data gathered about a pers ... [5]

Juan Carlos Zuniga 3/7/18 6:15 PM
Deleted: 13

Amelia Andersdotter 2/26/18 7:06 PM
Deleted: Personal devices can be terminal equipment devices, but can also provide infrastructure services to one or

Juan Carlos Zuniga 2/22/18 9:35 AM
Deleted: a small group of

Amelia Andersdotter 2/26/18 7:06 PM
Deleted: multiple terminal equipment devices.

Juan Carlos Zuniga 3/7/18 6:15 PM
Deleted: 14

Amelia Andersdotter 2/26/18 6:55 PM
Deleted: .… The network device to wh ... [6]

3.16 Shared service device: a device used by a group of individuals large enough that identification of the device does not easily allow identification of its user or group of user.

3.17 Target: The person (or frames from a machine associated with a person) from which the adversary wishes to obtain PII.

3.18 Temporary identifier: An identifier which is temporary in nature, in that it is exposed, transmitted ided.

3.1819 Threat.: A potential for violation of privacy, the unauthorized disclosure of PII.

3.1920 Threat Action.: The unauthorized disclosure of PII.

3.2021 Threat Agent: An entity that performs a threat action.

3.22 Tracking: The process of observing identifiers or information elements of personal devices repeatedly to perform fingerprinting.

or existing during a time period shorter than that over which the service is prov

3.23 Universal Address: A globally unique MAC address (see Clause 8.2 of [IEEE802]).

6. Overview and Scope

6.1 Context

The term privacy is used in many contexts, and is defined in multiple ways. These definitions might be specific to a domain (e.g. regulatory, social anthropology, etc.) or span across several domains. As a result, many organizations have defined privacy in a way specific to their needs. IEEE groups develop communication protocols that are applicable to multiple system architectures. This flexible applicability comes with the possibility of architecture-specific definition and contexts for privacy. As a consequence, the present document is not an attempt to provide a final or authoritative definition of privacy for IEEE 802, and recognizes that different definitions might be adopted by different IEEE 802 groups. However, this document adopts a definition of privacy that might be used by IEEE 802 groups when developing a specification, and by implementers of IEEE 802 specifications.

In the context of this document, privacy is concerned with the information that relates to a natural person. In particular, it concerns any data that directly or indirectly identifies an individual or from which identity or contact information of an individual might be derived, including data which allows the identification of

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Juan Carlos Zuniga 3/7/18 6:15 PM
Deleted: 15

Amelia Andersdotter 2/13/18 3:59 PM
Deleted: Strong PII: any IEEE 802 ele ... [7]

Juan Carlos Zuniga 3/7/18 6:15 PM
Deleted: 16

Amelia Andersdotter 2/26/18 6:56 PM
Deleted: .

cunche 2/15/18 5:26 PM
Deleted: containing PII which an ... [8]

Juan Carlos Zuniga 3/7/18 6:16 PM
Deleted: 17

Juan Carlos Zuniga 3/7/18 6:16 PM
Deleted: 18

Amelia Andersdotter 3/8/18 10:53 PM
Deleted: 19Threat. A potential for viol ... [9]

Juan Carlos Zuniga 3/7/18 6:16 PM
Deleted: 19

Amelia Andersdotter 3/8/18 10:53 PM
Deleted: 20Threat Action. The unauth ... [10]

Juan Carlos Zuniga 3/7/18 6:16 PM
Deleted: 20

Amelia Andersdotter 3/8/18 10:53 PM
Deleted: 21Threat Agent. An entity th ... [11]

Amelia Andersdotter 3/8/18 10:53 PM
Deleted: 3.22 Tracking: The process ... [12]

Juan Carlos Zuniga 3/7/18 6:16 PM
Deleted: 21

Amelia Andersdotter 2/26/18 6:56 PM
Deleted: .

Amelia Andersdotter 2/14/18 1:46 AM
Deleted: Weak PII: any element or co ... [13]

Amelia Andersdotter 2/26/18 7:07 PM
Deleted: can be…s defined in multipl ... [14]

Amelia Andersdotter 2/26/18 7:08 PM
Deleted: can be

Amelia Andersdotter 2/26/18 7:13 PM
Deleted: may…ight be adopted by dif ... [15]

Amelia Andersdotter 2/14/18 1:49 AM
Deleted: 6.2 Privacy Concept and Per ... [16]

Juan Carlos Zuniga 3/8/18 9:06 AM
Formatted ... [17]

Amelia Andersdotter 2/14/18 1:47 AM
Deleted: with the notion of person, and

Juan Carlos Zuniga 3/8/18 9:07 AM
Deleted:

Amelia Andersdotter 2/14/18 1:49 AM
Deleted: may be used to uniquely ide ... [18]

an individual based on correlations or patterns recognition or analysis (see definitions 3.11). This might include information that might be used to identify where a person is or has been, or to associate certain traffic with the person or to identify what the person is doing.

In all cases, there is an intrusion on a person's activity that correlates information collected through the usage of an 802 protocol and that person.

The collection of PII does not necessarily constitute a violation of privacy. Where PII is provided voluntarily and freely by a person who has been given a reasonable opportunity to understand the implications of their choices, or when the PII disclosure is necessary to provide the service requested by the user, collection of PII might imply big advantages for both the person and their service provider. A common example could be the registration to a private network based on a user 's MAC address (e.g. in the IEEE 802.11 network of a hotel), or a heart rate sensor and its associated traffic that is voluntarily associated to the person wearing the sensor. Many other cases associate the voluntary association of a device and its associated traffic to a consenting person.

6.2 IEEE 802 and Privacy

IEEE 802 specifications focus on the physical and Medium Access Control layers. Privacy is not limited to these layers. As a consequence, protecting privacy by providing recommendations solely for the first 2 layers of the OSI model might not be a fully efficient and unique method.

In the context of IEEE 802 protocols, device identification or correlation is often necessary and sometimes needs to be explicitly stated. A typical case is where a device or a flow needs to receive a particular service. The device or flow then needs to be clearly identified in order to receive the service. This identifier might be local, or might be propagated with the flow along the communication path.

However, device identification is not always necessary. By following the recommendations of this document, an operator would limit the exposure of PII through IEEE 802 protocols.

In order to limit the risk of PII exposure, this Recommended Practice document provides recommendations aimed at protecting privacy in IEEE 802 protocols and their implementations, and does not address the reasons why privacy would be exposed or protected, or exceptions to this protection. This document describes potential PII and privacy elements, and provides recommendations on how protocols might protect these elements.

In particular, this document focuses on PII that is in one or more of the following categories:
(i) specified/defined/created and used within an IEEE 802 standard;
(ii) specified/defined/created and used within an IEEE 802 standard and used by other standards, protocols or specifications;

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Amelia Andersdotter 2/14/18 1:53 AM
Deleted: and

Amelia Andersdotter 2/14/18 1:52 AM
Deleted: Privacy is therefore concerned with the notion of personally identifiable information (PII). Personally Identifiable Information includes any data that identifies an individual or from which identity or contact information of an individual can be derived. The natural person to whom the PII relates is called the PII principal. PII does not address the identification of a system or a device directly, but addresses the identification of an individual owning or using this device.

Juan Carlos Zuniga 2/22/18 9:49 AM
Deleted: a

Amelia Andersdotter 2/26/18 7:10 PM
Deleted: Wi-Fi

Amelia Andersdotter 2/26/18 7:10 PM
Deleted: of

Amelia Andersdotter 2/14/18 1:53 AM
Deleted: 6.3 Privacy and Fair Use

Amelia Andersdotter 2/14/18 1:53 AM
Deleted: The collection of PII does not necessarily constitute a violation of privacy. There are multiple cases where PII is provided voluntarily and freely by an individual. A common example could be a heart rate sensor and its associated traffic that is voluntarily associated to the individual wearing the sensor. Many other cases associate the volunt ... [19]

Amelia Andersdotter 2/14/18 1:57 AM
Deleted: 4

Amelia Andersdotter 2/14/18 2:09 AM
Deleted: **IEEE 802 technologies allow transmission of information bet** ... [20]

Juan Carlos Zuniga 3/8/18 9:08 AM
Deleted: n

Amelia Andersdotter 2/15/18 4:12 PM
Deleted: Observation of the use of an IEEE 802 device may allow an active attack ... [21]

Amelia Andersdotter 2/15/18 4:12 PM
Deleted: This identification may in turn be correlated to the identification of an in ... [22]

Amelia Andersdotter 2/14/18 2:13 AM
Deleted: is violation

Amelia Andersdotter 2/26/18 6:56 PM
Deleted:

Amelia Andersdotter 2/26/18 7:02 PM
Deleted: sh

Amelia Andersdotter 2/26/18 7:14 PM
Deleted: may

(iii) specified/defined/created externally to IEEE 802 standards but whose use is part of the specified operation of an IEEE 802 standard [short form (i) IEEE802 internal, (ii) exported, (iii) imported].

This recommended practice does not necessarily address the issue of PII that transit as simple data payload through IEEE 802
technologies (except for identifying the need to support security with confidentiality so that data is not exposed, or traffic analysis might not be inferred).

6.3 Correlation, Patterns and Fingerprinting

Correlation, in the context of this document, represents the possibility to identify a physical individual through association with one or several observed IEEE 802 elements. The association might be direct (one IEEE 802 element associated directly to one physical individual) or indirect (several IEEE 802 elements observed and analyzed together to produce an association to a physical individual). Such correlation does not need to be completely deterministic. A reasonably high statistical chance of such analyzed correlation to be associated to a physical individual is enough to consider that PII might be exposed.

In addition to the identification of a physical individual, IEEE 802 protocol elements might be leveraged to infer personal attributes of this individual. For instance, IEEE 802.11 SSIDs might reveal employer's name, home location and other visited locations; likewise, MAC address and vendor name might reveal the model of the device which might be used to infer information on the user's wealth.

A strong correlation between one or more IEEE 802 elements and an individual device is called device fingerprinting. This correlation might be strong enough for the device to be later recognized by the mere observation of one or a few of the initial correlated elements. This identification might be used locally, and might be part of the general requirements of communication. This identification might also be used across locations, where fingerprinting established in one location is used to recognize the same device at another location.

This document does not determine strict correlation statistical threshold, and considers that PII might be exposed as soon as a correlation might enable an association to a physical individual. The risk of correlation is context dependent. For this reason, it is up to each working or task group to assess and document on a case by case basis, to what extent correlation could be considered feasible for any particular adversary.

6.4 Personal devices and shared service devices

A personal device is primarily used by a single individual, or a small group of individuals (for example members of a single household). As such, any IEEE 802 element that uniquely identifies this device also identifies the associated individual or small group of individuals. This personal device might be a terminal equipment (for example a computer), or might provide infrastructure service to one or a small group of terminal equipment devices (for example a networking device connecting a single household to the Internet).

By contrast, a shared service device is used by a number of individuals large enough that 802 elements might identify the device without clearly identifying any individual using the services provided by that

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Juan Carlos Zuniga 3/8/18 9:09 AM
Deleted:

Amelia Andersdotter 2/26/18 7:36 PM
Deleted: can

Amelia Andersdotter 2/15/18 4:16 PM
Deleted: 5

Amelia Andersdotter 2/15/18 4:17 PM
Deleted: and

Amelia Andersdotter 2/26/18 7:14 PM
Deleted: may

Amelia Andersdotter 2/26/18 7:14 PM
Deleted: may

Amelia Andersdotter 2/26/18 7:37 PM
Deleted: can

Amelia Andersdotter 2/26/18 7:37 PM
Deleted: can

Amelia Andersdotter 2/26/18 7:37 PM
Deleted: can

Amelia Andersdotter 2/26/18 7:37 PM
Deleted: can

Amelia Andersdotter 2/26/18 7:15 PM
Deleted: may

Amelia Andersdotter 2/26/18 7:15 PM
Deleted: may

Amelia Andersdotter 2/26/18 6:56 PM
Deleted: However, this document uses the notion of strong PII, when PII can directly be derived using a correlation between one or several IEEE 802 elements, and weak PII, when no PII can easily be derived from a correlation between one or several IEEE 802 elements. In the case of weak PII, correlation may still be possible between one or several IEEE 802 elements and PII, but a high processing cost is needed for this correlation to bear a high probability.

Amelia Andersdotter 2/15/18 4:16 PM
Deleted: 6.6 Fingerprinting

Amelia Andersdotter 2/15/18 4:16 PM
Deleted: A strong correlation between one or more IEEE 802 elements and an individual device is called device fingerprinting. ... [23]

Amelia Andersdotter 2/15/18 4:17 PM
Deleted: 7

Amelia Andersdotter 2/26/18 7:16 PM
Deleted: may

Amelia Andersdotter 2/26/18 7:16 PM
Deleted: may

Amelia Andersdotter 2/26/18 7:16 PM
Deleted: may

device. An example of such shared service device includes a router, or a switch, in a medium to large network where multiple users exchange traffic.

8. Recommendations

The recommendations set forth here apply to standard developers, standard implementers and network designers. They are comprised of sets of questions tailored to the specific roles of each group to be used as support while evaluating privacy threats arising from any particular feature under development or system deployment. Accompanying the template questionnaires is an explanatory section with constructive examples.

8.1 Template questionnaires

8.1.1 Standard developers

This section provides guidance to standard developers in the form of a questionnaire, indicating a methodology for properly documenting, and if appropriate avoid introducing, features that might expose PII or facilitate correlation, eavesdropping, pattern recognition or fingerprinting by adversaries. The template questionnaire for standard implementers is meant to provide an overview for developers over their own processers.

8.1.1.1 Identifiers.

What is the minimum set of identifiers that are required by the service to operate?

What is the minimum set of identifiers that are required to manage the service?

Where are these identifiers foreseen to be stored, and for how long?

In which way might respondents or adversaries can use identifiers to perform correlation or fingerprinting?

Are there any information elements containing predictable sequence numbers that can be used as identifiers?

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Amelia Andersdotter 2/15/18 4:14 PM
Deleted: 6.8 MAC address as a PII

Amelia Andersdotter 2/15/18 4:14 PM
Deleted: MAC addresses are commonly used throughout IEEE 802 family of standards. When uniquely and statically associated to a physical device, MAC addresses can be used to identify the device. If another association can be made between the MAC address, or the device, and a physical individual, then a MAC address may be used as PII. Decoupling the strict device-to-MAC address unique association, for example by using random MAC addresses, may help protect PII, but only when such association is also correlated to a physical individual.

Amelia Andersdotter 2/15/18 4:14 PM
Deleted: For example, such correlation may be possible between the MAC address of a personal device, and the owner of that device. In contrast, such correlation is unlikely between the MAC address of a router and any particular physical individual, except if the router is intended to only carry the traffic of that physical individual. As the numbe ... [24]

Amelia Andersdotter 2/15/18 4:13 PM
Deleted: 6.9 IEEE 802 and Privacy Protection

Amelia Andersdotter 2/15/18 4:13 PM
Deleted: IEEE 802 protocols focus on the physical and Medium Access Control ... [25]

Amelia Andersdotter 2/15/18 4:13 PM
Deleted: Even in the context of IEEE 802 protocols, device identification or corr ... [26]

Amelia Andersdotter 2/15/18 4:13 PM
Deleted: However, device identification is not always necessary. By following the ... [27]

Amelia Andersdotter 2/15/18 4:13 PM
Deleted: Some IEEE 802 protocols include provisions to limit the exposure of ide ... [28]

Amelia Andersdotter 2/13/18 3:59 PM
Deleted: in this document

Juan Carlos Zuniga 3/8/18 9:10 AM
Deleted: ,

Amelia Andersdotter 3/7/18 8:32 PM
Comment [1]: Moved from leading paragraph in section 8.1.2.

Juan Carlos Zuniga 3/6/18 11:19 AM
Deleted: they

Juan Carlos Zuniga 3/8/18 9:13 AM
Deleted: .

Juan Carlos Zuniga 2/13/18 5:52 PM
Deleted: r

Would exposure of PII such that it allows correlation or fingerprinting be continuous or might it be made temporary in duration?

Are the identifiers persistent, and could they be constructed so that they are not?

Could the goals of the feature be achieved with fewer identifiers or linkages between identifiers, or by making exposures of identifiers or linkers temporary rather than continuous, or by not exposing them?

If the questions cannot be answered specifically, a reason should be provided.

8.1.1.2 Observers.

Are persistent or temporary identifiers exchanged between respondents and personal devices prior to the establishment of state between respondent and personal device?

Are any persistent or temporary identifiers stored, and if so, can they be exposed to a potential adversary?

Is the respondent device the final recipient of any particular identifier used to carry the feature, or does the respondent device need to expose the identifier(s) to other nodes?

Is there a limit to the required dissemination of PIIs?

What protection mechanisms are foreseen to block adversaries from having direct or indirect access to the identifiers while in transmission from personal device to respondent and vice-versa?

Can an observer become an active adversary and obtain more PIIs?

8.1.1.3 Parameters selection.

In which way does the selection of parameters related to the feature (or a set of features) contributes to the correlation of identifiers, for instance by creating a set of parameters so unique that a node is effectively exposed through fingerprinting?

Is existence of persistent or temporary identifiers, as well as their foreseen trajectories between nodes, subject to configuration by the personal device (the target), by the respondent device, or both?

Which set of parameters would be most conducive to mitigate correlation, continuity or existence of identifiers?

Which set of parameters would be most conducive to mitigate transmission of identifiers to other nodes in the network?

Is this set of parameters the minimum needed to advance to the next step in the communications protocol, or are some parameters not needed at this stage?

If the feature needs to be configured through mechanisms not established in the standard specifying the feature, what mechanisms for configurability are envisaged?

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Juan Carlos Zuniga 2/13/18 5:57 PM
Deleted: e

Juan Carlos Zuniga 3/8/18 11:25 AM
Deleted: leakage

Juan Carlos Zuniga 3/7/18 6:25 PM
Deleted: Configurability

Juan Carlos Zuniga 3/7/18 6:26 PM
Deleted: configurability

Juan Carlos Zuniga 3/7/18 6:27 PM
Deleted: of

Juan Carlos Zuniga 3/8/18 11:26 AM
Deleted: configuration

Juan Carlos Zuniga 3/8/18 11:27 AM
Deleted: the user of

Juan Carlos Zuniga 3/8/18 11:27 AM
Deleted: deployer of the

Juan Carlos Zuniga 3/8/18 11:29 AM
Deleted: configuration

Juan Carlos Zuniga 3/8/18 11:30 AM
Deleted: of the feature by the respondent or personal device

Juan Carlos Zuniga 3/8/18 11:30 AM
Deleted: configuration of the feature by respondent or personal devices

8.1.1.4 Privacy clause

Reflections and answers to the questions listed above should be documented in a privacy clause in the standard, making it easier for standards implementers and network designers to assess the impact of their work on privacy and security features.

8.1.2 Standards implementers

To assist standards implementers in their work to interpret a standards specification with respect to its privacy impcats, the following questions may be answered in the clause proposed by section 8.1.1.4:

If a feature requires configuration, is there an indication to implementers of the configuration of a device at which the amount of identifiers (or correlated information elements) is minimised, regardless of whether the identifiers are transient or durable, capable of being correlated or uniquely tied to a personal device, or otherwise? Is there a similar indication for parameter selections, the order of their transmission and the order of their inclusion in a frame? Is it possible to provide an indication as to how different options as per the previous two configurations could contribute to tracking or correlation?

If answers to these questions cannot be detailed in the specification, then the specification should instead provide details about why it is not applicable to provide such indications.

8.1.3 Network designers

To assist network designers in their work to interpret a standards specification with respect to its privacy impacts, the following questions may be answered in the clause proposed by section 8.1.1.4:

…

If answers to these questions cannot be detailed in the specification, then the specification should instead detail why it has not been deemed possible to provide such indications.

8.2 Specific recommendations and rules of thumb

It is recommended that each standard contain a privacy and security clause, describing to consumers of the standards what privacy and security features are envisaged in the standard (see section 8.1.1.4). Additionally it is recommended that:

- A service does not require that a device provides a unique identifier at different stages of the communication process, in so far as possible and feasible.

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Juan Carlos Zuniga 3/7/18 6:28 PM
Deleted: and security

Juan Carlos Zuniga 3/7/18 6:28 PM
Deleted: and security

Juan Carlos Zuniga 3/7/18 6:29 PM
Deleted: Template questionnaire for standard implementers is based on the assumption that information has been provided by the standard developers in accordance with sections 8.1.1.1, 8.1.1.2, 8.1.1.3 and 8.1.1.4 as foreseen. If standard information in accordance with these sections, standard implementers should try to assess the feature with respect to issues raised therein, and consider in particular how to enable privacy enhancing default configurations.

Juan Carlos Zuniga 3/7/18 6:29 PM
Deleted: is configurable

Juan Carlos Zuniga 3/7/18 6:29 PM
Deleted: might the default

Juan Carlos Zuniga 3/7/18 6:30 PM
Deleted: be made such that

Juan Carlos Zuniga 3/7/18 6:32 PM
Deleted: If this is not deemed to be the case, why not?

Juan Carlos Zuniga 3/7/18 6:32 PM
Deleted: Is it possible to introduce configurability in such a way that the existence, durability or transmission of identifiers is not an all-or-nothing situation, meaning that various configuration options could be made accessible to network designer, each of which introduces only minimally few further identifiers? If not,a detailed justification should be provided a documentation providing a detailed justification for consumers of the implemented device should be provided

Juan Carlos Zuniga 3/7/18 6:35 PM
Deleted: Template questionnaire for network designers is based on the assumption that information has been provided by the ... [29]

Juan Carlos Zuniga 3/7/18 6:35 PM
Deleted: What possibilities exist to plan the network in such a way that exposure ... [30]

Amelia Andersdotter 2/13/18 5:22 PM
Deleted: A first determination can be done to evaluate if transmission of target fram ... [31]

Amelia Andersdotter 2/13/18 5:22 PM
Deleted: If such exposure is possible, a next consideration may be to evaluate the s ... [32]

Juan Carlos Zuniga 3/6/18 12:25 PM
Deleted: this clause adheres to the following principles

- A service requiring identifiers should limit identifier storage strictly to the devices making use of those identifiers in providing that service (see sections 7.3- 7.4, 7.6-7.8 and 8.3.4 for examples, and sections 8.1.1.1-8.1.1.2 for questions).
- A service should permit temporary and non-persistent identifiers in so far as possible, especially for the use of short-lived services such as network probes.When switching to a new non-persistent identifier, variable fields such as sequence numbers should be reset to their default value or to a non-deterministic value (see sections 7.3-7.4, 7.6-7.8, 8.3.1-8.3.3 and 8.3.7 for examples, and sections 8.1.1.1 and 8.1.1.3 for questions).
- A service which requires periodic communications or transmissions of deterministic values or identifiers should be allowed for such values or identifiers to be sent with non-deterministic intervals (see sections 7.6 and 8.3.2 for examples, and sections 8.1.1.1 for questions).
- A service, if possible, should obfuscate any identifiers it requires with respect to other services or nodes, to decouple the association of a device identifier to a PII (see sections 7.3-7.6, 7.8, 8.3.3, 8.3.5 and 8.3.7 for examples, section 8.1.1.1 for questions).
- Similarly, a service should, if possible, allow the creation of temporary identifiers (see sections 7.3-7.9, 8.3.3, 8.3.5 and 8.3.7 for examples, section 8.1.1.1 for questions).
- A service should use identifiers specific to the service exchange, to facilitate obfuscation of personal devices (see sections 7.3-7.8, 8.3.3 and 8.3.5 for examples, section 8.1.1.1 for questions).
- A standard and any amendment thereof should contain a section describing the existence, persistence and storage of identifiers, possibly containing a description of configurability of such existence, persistence and storage as well (see section 8.1.1.4, 8.1.2-8.1.3).
- A service which assumes parameter selection, configuration or settings that impact the privacy of a target (or their personal device(s)) should, in so far as possible, allow for such selection, configuration or setting to be done by the target (see section 8.3.6 for example, sections 8.1.1.3-8.1.1.4, 8.1.2-8.1.3 for questions).
- The default parameters configuration should be the one that provides the highest level of privacy protections, while still allowing for the minimum acceptable level of service operation (see section 8.3.6 for example, sections 8.1.1.3-8.1.1.4, 8.1.2-8.1.3 for questions).

8.3 Threat mitigation examples

IEEE 802 standards commonly address communication mechanisms between devices assuming specific roles. In this text, these roles are described with the words target, personal device, respondent, and shared service device.

Transmissions from personal devices might be used to associate the device itself to a target Some examples of where the questionnaires and recommendations set out in sections 8.1 and 8.2 are applied follow:

8.3.1 Private discovery

If a form of discovery is operated by the personal device prior to the start of a session (identified and marked by a formal frame exchange), the personal device should be allowed to operate this discovery using a different identifier than that used for the actual session, unless the discovery is part of the session establishment and mandates an identity between the discoverer and the client device initiating the session. When such an identifier is necessary, protocol designers might consider including a privacy section in the standard that indicates the extent of the exposure.

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Juan Carlos Zuniga 3/7/18 6:38 PM
Deleted: random

Juan Carlos Zuniga 3/7/18 6:38 PM
Deleted: random periodicity

Juan Carlos Zuniga 3/7/18 6:43 PM
Deleted: A

Juan Carlos Zuniga 3/7/18 6:43 PM
Deleted: service provide as its

Juan Carlos Zuniga 3/7/18 6:46 PM
Deleted: **Personal device PII exposure**

Amelia Andersdotter 2/13/18 6:33 PM
Deleted: be intended to be shared service devices by function.ay devices, and minfrastructure be labeled ayther devices mSome o be intended to be personal devices by their function. ay be labeled as end-points, and maydevices mof these Some

Amelia Andersdotter 2/13/18 5:29 PM
Deleted: may

Amelia Andersdotter 2/14/18 1:40 AM
Deleted: the

Amelia Andersdotter 2/14/18 1:40 AM
Deleted: PII principal using the device. include the following elements:maySuch mitigation be easily uniquely identified through its Layer 1 and Layer 2 transmissions characteristics.may by reducing the likelihood that any individual personal device , the extent of this possible correlationto protocol designers concerned with privacy to limitAs a consequence, it is recommended

Juan Carlos Zuniga 3/7/18 9:08 AM
Deleted: I would not mandate that a personal device provides a unique identifier at different stages of the

Juan Carlos Zuniga 3/7/18 9:08 AM
Deleted: communication process. For example, iprotocolA f

Amelia Andersdotter 2/13/18 5:29 PM
Deleted: may

Amelia Andersdotter 2/13/18 5:32 PM
Deleted: d

8.3.2 Keepalives and probes

A protocol should not mandate that a personal device sends messages identical in nature (such as keepalives or probes), at regular or predictable intervals, especially if these messages contain a unique identifier, or identifiers that when sequentially considered amount to a unique identifier (i.e. tracking), for the personal device. When such messages are required, transmission at non-deterministic intervals might be considered.

8.3.3 Partial obfuscation

Some messages might not need emitter or receiver identifiers beyond the single message exchange (e.g. IEEE 802.11 Probe Request and Probe Response Exchange). In that case, partial or complete obfuscation of one or both sides real identity might be permitted. When information about a service is queried, it might be possible to provide identification of the side offering the service. Some other messages (e.g. keepalive) might require persistent identifiers. In that case, identification might only be needed for the duration of the period during which a specific service or session is maintained.

8.3.4 Identifier storage

When a service is not needed anymore, deletion of identifiers should be possible.
Identifiers might not need to be
stored, even during the period of validity of the service provided. Consideration should be made about the location of identifier storage when implementing the specification.

8.3.5 Correlation

A protocol should not mandate that a personal device sends messages exposing a list of characteristics that might be used to identify or track the personal device, if the list is not explicitly designed for this purpose.

For example, when a list of common optional features need to be agreed upon between the respondent device and the personal device, the respondent device can initiate the listing of supported features, and the personal device can be allowed to choose from that list. The personal device would not be mandated to expose which optional features it supports beyond those made accessible to it by the respondent device, as this exposure might allow distinguishing between personal devices connecting to the same respondent device.

Likewise, it should be considered that meta-data generated from the usage of the protocol should not allow generating undesired identifiers.

8.3.6 Opt-in and opt-out

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Juan Carlos Zuniga 3/7/18 6:49 PM
Deleted: should

Juan Carlos Zuniga 3/7/18 6:48 PM
Deleted: randomness of periodicity

Amelia Andersdotter 2/13/18 5:33 PM
Deleted: be allowedmay

Juan Carlos Zuniga 3/7/18 6:50 PM
Deleted: When randomness of periodicity is not possible, the personal device be allowed to obfuscate its unique identifiersty, for example by using changing a locally administered address from one period to the next.

Amelia Andersdotter 2/13/18 5:29 PM
Deleted: may…ight not need emitter ... [33]

Juan Carlos Zuniga 3/7/18 9:41 AM
Deleted: t o

Amelia Andersdotter 2/26/18 7:28 PM
Deleted: only…provide identificatio ... [34]

Amelia Andersdotter 2/13/18 5:46 PM
Deleted: the … service is not needed ... [35]

Amelia Andersdotter 2/13/18 5:46 PM
Deleted: consideration can be made about the persistence of the identifier ... [36]

Amelia Andersdotter 2/13/18 5:46 PM
Deleted: also…be made about the lo ... [37]

Juan Carlos Zuniga 2/13/18 6:18 PM
Deleted: would …hould not mandate ... [38]

Amelia Andersdotter 2/13/18 5:30 PM
Deleted: may

Amelia Andersdotter 2/13/18 5:58 PM
Deleted: infrastructure…device and t ... [39]

Amelia Andersdotter 2/13/18 6:48 PM
Deleted: PII utilization recommendations

Amelia Andersdotter 2/13/18 6:48 PM
Deleted: be associated to a personal device. may be limited whenever possible, especially if the identifier mayIt is recommended to protocol designers to consider the impact of unique identifier collection. Such collection

Amelia Andersdotter 2/13/18 6:48 PM
Deleted: be carefully weighted and limited, so as to avoid that mayWhen such collection is performed, its purpose It is also recommended that protocol designers consider if anonymization of the identifier is possible, to decouple the association of a device identifier to a PII. be made around the retention time of the collected identifier, to include provisions to delete information about collected identifiers as soon as the retention of these identifiers is not necessary anymore. mayunique identifiers be stored beyond the scope of the orig ... [40]

When multiple methods are allowed to achieve a given purpose, the parameter setting which allows the highest level of privacy under the intended functionality of the feature, should always be suggested to be used as the default. It should be indicated how individuals can be allowed to opt-in for methods that would allow a lower level of privacy in exchange for some service. After having opted-in, it is individuals should be allowed to opt back out to the method offering better privacy, if they so desire.

8.3.7 Implicit identifiers

It has been demonstrated that the order in which optional protocol information elements are sent, and the choice of them, might be used as temporary or persistent identifier (see e.g. IEEE privecsg-16-0003-00-0000). Effectively, the specific set of information elements and the order in which they are transmitted becomes an identifiable stream of information that can be used to pin down individual devices.

Mitigation strategies include reviewing over-all configurability options and liberties in the order of transmission and the usage of optional information elements in the communications protocol. Likewise, mandating a specific order of transmission, limiting the number of specific options (e.g. by creating configuration profiles), and suggesting a default configuration, would make communications properties more similar between different nodes and would avoid identifying nodes individually.

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

Juan Carlos Zuniga 2/13/18 6:19 PM
Deleted: maymight be

Juan Carlos Zuniga 3/7/18 6:51 PM
Deleted: it is recommended that the method allowing

Juan Carlos Zuniga 3/7/18 6:52 PM
Deleted: the

Juan Carlos Zuniga 2/13/18 6:19 PM
Deleted: s

Juan Carlos Zuniga 3/7/18 6:53 PM
Deleted: Users

Juan Carlos Zuniga 3/7/18 6:54 PM
Deleted: recommended that users

Juan Carlos Zuniga 3/8/18 11:37 AM
Deleted: Order of transmission

Juan Carlos Zuniga 3/8/18 11:37 AM
Deleted: the order of transmission and

Juan Carlos Zuniga 3/8/18 11:34 AM
Deleted: 8.3.8 Configurability

When transmission relies on specific modulations, scrambling operations, or optional protocol parameters in general, it is foreseen that specific settings or configurations in a network causes frames to be so easily distinguishable from a "typical frame" that that a device could be fingerprinted. In these cases, the algorithm should be chosen not only to serve its security purpose, but also in such a way that it is defined clearly enough to be implemented similarly (with the same chance of producing the similar and indistinguishable result) among various types of intended client devices.

Amelia Andersdotter 2/14/18 1:42 AM
Deleted: care is recommended

Amelia Andersdotter 2/14/18 1:43 AM
Deleted: to ensure that

Amelia Andersdotter 2/14/18 1:43 AM
Deleted: can

Amelia Andersdotter 2/14/18 1:43 AM
Deleted: would

Amelia Andersdotter 2/26/18 7:04 PM
Deleted: be

Juan Carlos Zuniga 3/7/18 10:04 AM
Deleted: 01

Amelia Andersdotter 3/8/18 10:56 PM
Deleted: 2

References:

J.C. Zúñiga, M. Vanhoef, C. Matte, M. Cunche, *Privacy Issues in 802.11 Networks*, IEEE 11-16-1492-00-0wngg, 8 November 2016.

M. Vanhoef, C. Matte, M. Cunche, L.S. Cardoso, F. Piessens, *Tracking 802.11 stations without relying on the link layer identifier*, IEEE privecsg-16-0003-00-0000, 14 April 2016.

J.C. Zúñiga, *802E Privacy Mitigations*, IEEE privecsg-16-0002-00-0000, 23 March 2016.

M. Riegel, *Privacy Engineered Access Network*, IEEE privecsg-15-0014-00-0000, 12 March 2015.

P. Barber, *Overview of Privacy in 802.16*, IEEE privecsg-14-0012-00-0000, 8 October 2014.

IETF RFC 6973, *Privacy Considerations for Internet Protocols*, July 2013.
https://tools.ietf.org/html/rfc6973