IEEE P802E

Revisions to Clause 6 following comments in San Diego IEEE 802 Plenary meeting

Date: 2018-07-10

Author(s):

Name	Affiliation	Address		
Juan-Carlos Zúñiga	SIGFOX	juancarlos.zuniga@sigfox.com		
Amelia Andersdotter	ARTICLE 19	amelia@article19.org		
Dan Harkins	HPE	3333 Scott Boulevard Santa Clara, California, United States of America		

Abstract

Revisions to Clause 6 in line with comments presented by during San Diego IEEE 802 Plenary Session, and clarification of a definition in line with observations made during the San Diego IEEE 802.1 SEC TG meeting on Tuesday July 10th.

R0: Restructuring of Clause 6 in line with comments presented during SEC TG Tuesday AM session.

R1: added a proposed alternative definition of PCI, following discussion in the SEC TG Tuesday PM session.

R2: different wording in the last sentence of the preamble of Clause 6 following feedback.

R3: added a subclause in Clause 7 to describe discovery threats particular to radio-based technologies following comments made in SEC TG Tuesday AM session.

3. Definitions

Personal Correlated Information (PCI): data gathered about an individual or a group thereof, by observing activities or events associated with those individuals.

6. Rationale for Privacy in IEEE 802

IEEE 802 specifications focus on the physical and Medium Access Control layers. Privacy is not limited to these layers. Protecting privacy by providing recommendations solely for the first 2 layers of the OSI model is not be a fully efficient method. However, privacy protection is contingent on consistent efforts through-out value chains, and on privacy by design and default.

The rationale behind this Recommended Practise is to provide a framework within which privacy by design and by default can more easily be implemented in the context of IEEE 802 standards development and use. The 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;
(iii) specified/defined/created externally to IEEE 802 standards but whose use is part of the specified operation of an IEEE 802 standard.

The 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). The use of the word privacy in this Recommended Practise does not preclude a broader understanding of the word privacy, and in is intended to be interpreted reasonably within the context of the scope of the IEEE 802 project applying these recommendations.

6.1 Identifiers, observers and identifiable information

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

Amelia Andersdotter 7/11/18 4:45 AM
Comment [1]: Proposed alternative definition.

Amelia Andersdotter 7/11/18 1:34 AM
Deleted: **Overview and Scope**

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: As a consequence, p

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: might

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: and unique

Amelia Andersdotter 7/11/18 1:43 AM
Comment [2]: Moved from below.

Amelia Andersdotter 7/11/18 1:49 AM
Comment [3]: Shifted down to 6.1

Amelia Andersdotter 7/11/18 1:49 AM
Deleted: 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.

Amelia Andersdotter 7/11/18 1:49 AM
Deleted: However, device identification is not always necessary. By following the ... [1]

Amelia Andersdotter 7/11/18 1:43 AM
Comment [4]: Shifted up.

Amelia Andersdotter 7/11/18 1:43 AM
Deleted: In order to limit the risk of PI ... [2]

Amelia Andersdotter 7/11/18 1:35 AM
Comment [5]: Note removal of short-f ... [3]

Amelia Andersdotter 7/11/18 1:45 AM
Deleted: is

Amelia Andersdotter 7/11/18 1:45 AM
Deleted: r

Amelia Andersdotter 7/11/18 1:45 AM
Deleted: p

Amelia Andersdotter 7/11/18 1:46 AM
Comment [6]: We propose this sentenc ... [4]

Amelia Andersdotter 7/11/18 1:48 AM
Deleted: **Context**

Amelia Andersdotter 7/11/18 1:46 AM
Deleted: The term privacy is used in m ... [5]

Amelia Andersdotter 7/11/18 7:37 PM
Comment [7]: Removed and replaced b ... [7]

Amelia Andersdotter 7/11/18 1:46 AM
Deleted: specific to a domain (e.g. regu ... [6]

Amelia Andersdotter 7/11/18 1:46 AM
Deleted: their needs. IEEE groups dev ... [8]

Amelia Andersdotter 7/11/18 1:46 AM
Deleted: consequence, the present docu ... [9]

or contact information of an individual might be derived, including data which allows the identification of 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.

In 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: a device or flow might need to be clearly identified in order to receive the service and the 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.

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.

Amelia Andersdotter 7/11/18 1:41 AM
Comment [8]: This is reducing the example to only one sentence makes the text "flow better" to me. Also, I use the colon ":" to mean " introducing a second clause to explain the first", which is correct in this case.

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: 6.2 IEEE 802 and Privacy

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: 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.

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: 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.

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: 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.

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: 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 exp ... [10]

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: In particular, this document focuses on PII that is in one or more of the following categories:

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: (i) specified/defined/created and used within an IEEE 802 standard;

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: (ii) specified/defined/created and used within an IEEE 802 standard and used by other standards, protocols or specifications;

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: (iii) specified/defined/created externally to IEEE 802 standards but whose use is part of the specified operation of an IEEE 802 standa ... [11]

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: This recommended practice does not necessarily address the issue of PII that transit as simple data payload through IEEE 802

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: technologies (except for identifying the need to support security with confidentiality so that data is not

Amelia Andersdotter 7/11/18 1:37 AM
Deleted: **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 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.

7.9 Threats During Discovery

Amelia Andersdotter 7/11/18 1:34 AM
Deleted: .

The IEEE 802 family of standards share privacy threats due to their capacity to provide communication for frame-based data networks. In addition, radio-based technologies in the IEEE 802 family of standards have unique privacy threats due to their expansive discovery processes and the ability of an adversary to eavesdrop on those communications.

Network discovery by radio-based standards such as IEEE 802.11 result in gratuitous sending of probes which search for available and suitable networks to connect to. This exposes the DA/SA common fields threat vector (section 7.2) to anyone within range of the device's radio.

It is also possible for radio-based technologies to permit transactional forms of discovery of network services. These frame exchanges can expose PII that may aid correlation and fingerprinting depending on the form of the particular type of service being searched for.