# Security – Drafts to RevCom

- P802E

# Motion

- Approve sending P802E/D2.0 to RevCom
- Approve CSD documentation in http://www.ieee802.org/1/files/public/docs2015/802e-csd-1715-v00.pdf
- P802E/D2.0 had 95% approval, 91% return rate at the end of the second recirculation SA ballot
  - No further comments or vote changes received on that recirculation
  - 4 Disapprove votes, 10 unresolved Must Be Satisfied Comments
- In the WG, Proposed: Mick Seaman, Second: Karen Randall
  - Sending draft (y/n/a): <y>, <n>, <a>
  - CSD (y/n/a): <y>, <n>, <a>
- In EC, mover: Glenn Parsons Second: Roger Marks
  - (y/n/a): <y>,<n>,<a>

# Supporting information P802E

## Project Information

| | |
|---|---|
| **PAR/Standard#:** | P802E |
| **Project Title:** | Recommended Practice for Privacy Considerations for IEEE 802 Technologies |
| **Project Type:** | New |
| **Ballot Stage:** | Comment Resolution - 2 |
| **Ballot Type:** | Individual |
| **Invitation Open Date:** | 15 Jul 2019 |
| **Invitation Close Date:** | 14 Aug 2019 |

## Standards Committee/Working Group

| | |
|---|---|
| **Standards Committee:** | IEEE Computer Society/LAN/MAN Standards Committee (C/LM) |
| **Standards Committee Chair:** | Paul Nikolich |
| **Standards Representative:** | James Gilb |
| **Working Group Type:** | Individual |
| **Working Group Chair:** | Glenn Parsons |
| **Program Manager:** | |

## Ballot Summary

**Open Date:** 29 May 2020 **Close Date:** 13 Jun 2020 **Status** Closed

**Ballot Group Members:** 92 **Ballot Stage:** Recirculation 2

Minimum should be 10

**Return Ballots:** (84) 91%

Minimum return rate is 75%

**Abstentions:** (3) 3%

Abstention must be below 30%

**Approval Rate:** 95%

Approval rate must be at least 75%

| Votes counted in approval rate | | Votes not counted in approval rate | |
|---|---|---|---|
| Approve | 77 | Disapprove Without MBS Comment(s) | 0 |
| Disapprove With MBS Comment(s) | 4 | Abstentions | 3 |
| Total | 81 | Total | 3 |

| | | | |
|---|---|---|---|
| Total Votes | 84 | Total Comments | 0 |

The vote tally for "Disapprove With MBS Comment(s)" = current Disapprove votes for which an MBS (Must Be Satisfied) comment existed in any round of balloting.

# Supporting information P802E

P802E D1.6 Recom. Practice for Privacy Consi. for IEEE 802 Initial Sponsor ballot comments

Cl 1 SC 1 P 1 L 1 # i-12

Byrd, William PRIVACOM VENTUR

*Comment Type* GR *Comment Status* R *MBS*

This does not appear to be a standard to me. It just looks like a Lawyer wrote a lot "don't sue me," junk. It just states the obvious and does nothing to explain how to implement anything.

It's just a complete waste of IEEE time, with zero value

*SuggestedRemedy*

Drop the entire standard.
Or, show specifically how and where privacy can be obtained on 802 networks. Not just "don't sue me, or blame me," nonsense

*Response* *Response Status* C

REJECT.
The proposed change in the comment does not contain sufficient detail for the Comment Resolution Group (CRG) to determine specific changes that would satisfy the comment. This Recommended Practice aims to help IEEE 802 protocol developers mitigate privacy threats. Discussion during its development revealed that the extent of the threat posed by information correlation and fingerprinting techniques was not generally understood (not obvious). The Recommended Practice helps inform developers and users on privacy requirements. Just as for security in general, there can be no expectation of absolute privacy (in the absence of a decision not to communicate at all) but merely a question of raising the effort expended by an adversary to the extent that violating privacy becomes an unprofitable/unattractive option.

Cl 1 SC 1.3 P 21 L 13 # i-13

Rannow, R K IEEE/SELF

*Comment Type* GR *Comment Status* R *MBS*

Uncomfortable with the introduction as, "a threat model" is not all encompassing.

One must use various models (HW, SW, architecture, etc.). Furthermore, there are vulnerabilities that might be considered, and this may require various considerations.

*SuggestedRemedy*

Recommend we also include TVA (threat and vulnerability analysis):

Threat and vulnerability models facilitate the framework and methodical identification of threats, risks or vulnerabilities associated with the identified threats, and possible mitigation or counter-measure solutions.

There are

*Response* *Response Status* C

REJECT.
The proposed change in the comment does not contain sufficient detail for the Comment Resolution Group (CRG) to determine specific changes that would satisfy the comment.

Cl 1 SC 1.4 P 22 L 7 # i-17

Rannow, R K IEEE/SELF

*Comment Type* GR *Comment Status* R *MBS*

Perhaps a missed opportunity, no meaningful boundaries described (where might privacy ownership lie) and developing a comprehensive model as part of a product spec.

*SuggestedRemedy*

Working on a more comprehensive proposal.

*Response* *Response Status* C

REJECT.
The proposed change in the comment does not contain sufficient detail for the Comment Resolution Group (CRG) to determine specific changes that would satisfy the comment.

The group did discuss this topic extensively in prior versions of the draft and concluded that the purpose of the recommended practice could not be to define privacy boundaries (as 1.5 makes clear), because such boundary definition could be argued against ad infinitum, and would vary as new standards are developed.

# Supporting information P802E

P802E D1.6 Recom. Practice for Privacy Consi. for IEEE 802 Initial Sponsor ballot comments

*Cl* 1 *SC* 1.4 *P* 22 *L* 15 # i-14

Rannow, R K IEEE/SELF

*Comment Type* GR *Comment Status* R *MBS*

Replace:

Helping to protect personal information against such less powerful adversaries remains an important goal.

*SuggestedRemedy*

With:

Helping to protect personal information against unauthorized access and less powerful adversaries remains an important goal.

*Response* *Response Status* C

REJECT.
The paragraph aims at specifying that this recommended practice aims at providing a framework to protect against adversaries that can use IEEE 802 technologies to perform fingerprinting and obtain PII, directly or indirectly. Unauthorized access seems to be break the balance of the sentence without adding more clarity to the meaning as unauthorized access would be what these adversaries perform.

---

*Cl* 1 *SC* 1.5 *P* 22 *L* 25 # i-18

Zalewski, Janusz Florida Gulf Coast Uni

*Comment Type* GR *Comment Status* R *MBS*

I cannot imagine how a guideline on "privacy" does not have it defined.

*SuggestedRemedy*

Any definition would be better than none.

*Response* *Response Status* C

REJECT.
The proposed change in the comment does not contain sufficient detail for the Comment Resolution Group (CRG) to determine specific changes that would satisfy the comment.

The existing text of clause 1.5 already discusses the various shades of meanings of privacy, and the IEEE Standards Dictionary Online (referenced by clause 3. Definitions for the definition of terms not defined in that clause) also provides a definition: "The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively."

The recommendations in this Recommended Practice do not depend on the selection of a particular definition of privacy, and would not be enhanced by introducing an additional definition.

---

*Cl* 1 *SC* 1.5 *P* 22 *L* 27 # i-15

Rannow, R K IEEE/SELF

*Comment Type* GR *Comment Status* R *MBS*

Not sure how privacy in "social anthropology" or the study of people conveys helpful insight on a definition.

*SuggestedRemedy*

Change, "social anthropology" to "societal norms" to perhaps align with IEEE EAD endeavors.

*Response* *Response Status* C

REJECT.
The meaning of this text is that the term privacy can have different definitions depending on the domain, regulatory is given as an example, social anthropology is given as another example of a domain where specific definitions can be found. The text refers here to a definition of a term in a field, not to the general notion that 'privacy' may have different definition depending on groups of people (which is what social anthropology would study, along with the associated definition of terms).

---

*Cl* 3 *SC* 3 *P* 23 *L* 20 # i-16

Rannow, R K IEEE/SELF

*Comment Type* GR *Comment Status* R *MBS*

vulnerability definition

*SuggestedRemedy*

Vulnerability:

The characteristics and circumstances of a community, system, device or asset that makes it susceptible to compromise or damaging effects of the vulnerability.

There are many aspects of vulnerability, and may include social, personal, physical, economic, and environmental.

*Response* *Response Status* C

REJECT.
The term vulnerability is not used in the Recommended Practice.

# Supporting information P802E

P802E D1.6 Recom. Practice for Privacy Consi. for IEEE 802 Initial Sponsor ballot comments

---

*Cl* 3 *SC* 3 *P* 24 *L* 1 # i-19

Zalewski, Janusz Florida Gulf Coast Uni

*Comment Type* GR *Comment Status* R *MBS*

I cannot imagine how a guideline on "privacy" does not have it defined.

*SuggestedRemedy*

Any definition would be better than none.

*Response* *Response Status* C

REJECT.
The proposed change in the comment does not contain sufficient detail for the Comment Resolution Group (CRG) to determine specific changes that would satisfy the comment.

The recommendations in this Recommended Practice do not depend on the selection of a particular definition of privacy (see clause 1.5 in the draft). The IEEE Standards Dictionary Online (referenced by clause 3. Definitions for the definition of terms not defined in that clause) provides this definition: "The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively."

---

*Cl* 8 *SC* 8.1 *P* 34 *L* 13 # i-28

Riegel, Maximilian Nokia

*Comment Type* TR *Comment Status* R *MBS*

In terms of PII exposure, short-lived services are not less vulnerable than longer lasting services. Once an identifier is visible, it's known. You may had in mind, that more frequent services like network probes have higher likelihood of observation when moving around.

*SuggestedRemedy*

Change sentence to 'Temporary identifiers should not be used or at least permitted whenever possible'.

*Response* *Response Status* C

REJECT.
The proposed remedy implies that permanent identifiers are preferred. The meaning of the recommendation is that temporary services may be better served if temporary identifiers are used, so as to avoid permanent association with a device.

# Supporting information P802E

P802E/D2.0 Recommended Practice for Privacy 1st Sponsor recirculation ballot comments

*Cl* 6 *SC* 6.3 *P* 22 *L* 32 # R1-3

Riegel, Maximilian Nokia

*Comment Type* TR *Comment Status* D *MBS*

... or (for a wireless device) characteristics of the radio implementation: it is not well expressed that the characteristics of the radio must allow for fingerprinting, ie. must contain some kind of information that is unique for that single device

*SuggestedRemedy*

Amend to the end of 'or can be persistent, e.g. using a permanently assigned MAC address or (for a wireless device) characteristics of the radio implementation' unique for a device.

*Proposed Response* *Response Status* W

REJECT.
It is not necessary that the radio implementation information be unique for that single device. It only need to be correlated with a device, and thus contribute to fingerprinting (as explained in lines 21 through 26 of the page referenced by this comment).

[FYI : The paper at
https://www.ccs-labs.org/bib/bloessl2015scrambler/bloessl2015scrambler.pdf
provides a detail analysis of the use of radio scrambler properties in an attack on location privacy scenario, as well as mentionning other radio properties that can be correlated for long enough to be useful to an adversary.]

*Cl* 7 *SC* 7.2 *P* 24 *L* 32 # R1-4

Riegel, Maximilian Nokia

*Comment Type* TR *Comment Status* D *MBS*

Header changed to 'MAC and Physical Layer Operations', however this change misses that IEEE 802 protocols also comprise functions above the MAC layer. As IEEE 802 protocol operations belong to Data Link layer and Physical Layer, it makes no sense to exclude IEEE 802 protocol functions above the MAC layer.

*SuggestedRemedy*

Change header to 'Data Link and Physical Layer Operations' and also change 'MAC' in line 33 to Data Link'

*Proposed Response* *Response Status* W

REJECT.
1. Subclause 7.2 is part of this Recommended Practice, and not a definition of its entire Scope. The title of the subclause reflects its contents. Other aspects of IEEE 802 operation (MAC Addresses, Network Discovery etc. are addressed by other subclauses.
2. The functions above the MAC Layer use protocol identifiers (EtherTypes, LLC Addresses). Renaming this particular subclause would be to advocate the replacement of these persistent identifiers with ephemeral values, and thus require a completely new approach to protocol identification. No such proposal has been made, and no such proposal is required as data above the MAC (including protocol identifiers) can be (and often is) cryptographically confidentiality protected and thus privacy protected between communicating 802 end stations (see IEEE Std 802.1X and related standards).

# Security – Internal WG motions

- Teleconferences, subject to 10 days notice

# MOTION

- Authorize the Security Task Group to hold teleconferences to progress P802.1AEdk and task group matters arising:
  - Dates/times to be announced subject to notice of at least 10 days to the 802.1 email exploder

- Proposed: Seaman Second: Randall
- For: Against: Abstain: