IEEE 802  
Privacy EC SG

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Internet Privacy Recommendations - A Survey | | | | |
| Date: 2015-10-21 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | Email |
| Juan Carlos Zuniga | InterDigital |  |  | j.c.zuniga@ieee.org |
| Piers O’Hanlon | Oxford Internet Institute |  |  | pohanlon@gmail.com |

Abstract

This document captures some (Internet) privacy recommendations that have been developed in the industry recently. These references can be useful to assess and define privacy recommendations for IEEE 802 protocol developers.

### RFC 6973: Privacy Considerations for Internet Protocols

RFC 6973 [1] provides a comprehensive view of the different considerations that need to be taken into account when designing Internet protocols.

The document takes a broad approach at assessing and mitigating privacy risks. However, the document was written prior to several revelations made in 2013 and therefore it misses some now well-known threats, such as pervasive monitoring.

Some threats described in RFC 6973 that could apply to IEEE 802 technologies are:

* Surveillance, stored data compromise, intrusion (DoS), and potentially misattribution.

Some considerations provided in RFC 6973 that are relevant to IEEE 802 technologies include:

* Data minimization, anonymity, pseudonymity, and confidentiality.

Similarly, considerations about identification (or use of identifiers) and correlation (between identifiers) can be applicable to IEEE 802 protocols.

### RFC 7624: Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement

RFC 7624 [2] describes a threat model post-2013 revelations, with an emphasis on pervasive surveillance.

Particularly relevant to IEEE 802 protocols is the description about the tracking of link-layer identifiers. Nonetheless, other relevant privacy threats can be applicable to IEEE 802 technologies, such as the use of protocol headers, and potential correlation of identifiers and addresses.

Proposed mitigations include an analysis of the cost and risk of each attack. This technique helps identifying the most effective remedies for each type of attack.

### W3C Security and Privacy Questionnaire

The W3C has written an informal questionnaire to help understand security and privacy implications of (new) features in a technical specification [3].

Some of these questions can be relevant for IEEE 802 protocol developers when defining, amending or correcting IEEE 802 specifications. For instance:

* Does this specification deal with personally-identifiable information?
* Does this specification deal with high-value data?
* Does this specification expose persistent, cross-origin state (to the web/Internet)?
* Does this specification expose any other data to an origin that it doesn’t currently have access to?
* Does this specification allow an origin access to a user’s location?
* Does this specification allow an origin access to sensors on a user’s device?
* Does this specification allow an origin access to other devices?
* Does this specification expose (temporary) identifiers (to the web/Internet)?
* Does this specification persist data to a user’s local device?
* Does this specification have a "Security Considerations" and "Privacy Considerations" section?

Asking some of these questions could allow changing the way a protocol feature is defined, or even assessing the value of adding the feature altogether.

## References

1. RFC 6973; Privacy Considerations for Internet Protocols; July 2013; <https://tools.ietf.org/html/rfc6973>
2. RFC 7624; “Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement”; August 2015; <https://tools.ietf.org/html/rfc7624>
3. W3C Security and Privacy Questionnaire; April 2015; <https://w3ctag.github.io/security-questionnaire/>