

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: August 26, 2021

J. Arkko  
Ericsson  
S. Farrell  
Trinity College Dublin  
February 22, 2021

**RFC 7258 additions due to evolving Internet thread model  
draft-arkko-farrell-arch-model-t-7258-additions-02**

**Abstract**

Communications security has been at the center of many security improvements in the Internet. The goal has been to ensure that communications are protected against outside observers and attackers.

[RFC 7258](#) is the IETF guidance on taking into account pervasive monitoring threats in Internet technology development work. This memo suggests additions to [RFC 7258](#) to cater for the evolving threats. For instance, it may be necessary to also worry about information collected by a legitimate protocol participant being misused for pervasive monitoring purposes.

**Status of This Memo**

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 26, 2021.

**Copyright Notice**

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

|                             |  |                   |
|-----------------------------|--|-------------------|
| <a href="#">1.</a>          | Introduction . . . . .   | <a href="#">2</a> |
| <a href="#">2.</a>          | Potential Changes in <a href="#">BCP 188</a> /RFC 7258 . . . . . | <a href="#">2</a> |
| <a href="#">3.</a>          | Security Considerations . . . . .                                | <a href="#">3</a> |
| <a href="#">4.</a>          | IANA Considerations . . . . .                                    | <a href="#">3</a> |
| <a href="#">5.</a>          | References . . . . .   | <a href="#">3</a> |
| <a href="#">5.1.</a>        | Normative References . . . . .                                   | <a href="#">3</a> |
| <a href="#">5.2.</a>        | Informative References . . . . .                                 | <a href="#">3</a> |
| <a href="#">Appendix A.</a> | Acknowledgements . . . . .                                       | <a href="#">3</a> |
| Authors' Addresses          | . . . . .  | <a href="#">4</a> |

## [1.](#) Introduction

Communications security has been at the center of many security improvements in the Internet. The goal has been to ensure that communications are protected against outside observers and attackers. At the IETF, this approach has been formalized in [BCP 72](#) [[RFC3552](#)], which defined the Internet threat model in 2003. Additional guidance to take into account dangers posed by pervasive monitoring were covered in [BCP 188](#) [[RFC7258](#)].

However, threats in the Internet continue to evolve, as discussed in [[I-D.arkko-farrell-arch-model-t-redux](#)].

The rest of this document tentatively suggests a small (but our view, important) change to the BCP.

Comments are solicited on this document. The best place for discussion is on the model-t list.  
(<https://www.ietf.org/mailman/listinfo/model-t>)

## [2.](#) Potential Changes in [BCP 188](#)/RFC 7258

Additional guidelines may be necessary also in [BCP 188](#)/RFC 7258[RFC7258], which specifies how IETF work should take into account pervasive monitoring.

An initial, draft suggestion for starting point of those changes could be adding the following paragraph after the 2nd paragraph in [Section 2](#):



NEW:

PM attacks include those cases where information collected by a legitimate protocol participant is misused for PM purposes. The attacks also include those cases where a protocol or network architecture results in centralized data storage or control functions relating to many users, raising the risk of said misuse.

### **[3.](#) Security Considerations**

The entire memo covers the security considerations.

### **[4.](#) IANA Considerations**

There are no IANA considerations in this work.

### **[5.](#) References**

#### **[5.1.](#) Normative References**

- [RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", [BCP 72](#), [RFC 3552](#), DOI 10.17487/RFC3552, July 2003, <<https://www.rfc-editor.org/info/rfc3552>>.
- [RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", [BCP 188](#), [RFC 7258](#), DOI 10.17487/RFC7258, May 2014, <<https://www.rfc-editor.org/info/rfc7258>>.

#### **[5.2.](#) Informative References**

- [I-D.arkko-farrell-arch-model-t-redux] Arkko, J. and S. Farrell, "Internet Threat Model Evolution: Background and Principles", [draft-arkko-farrell-arch-model-t-redux-00](#) (work in progress), November 2020.

### **[Appendix A.](#) Acknowledgements**

The authors would like to thank the IAB:

Alissa Cooper, Wes Hardaker, Ted Hardie, Christian Huitema, Zhenbin Li, Erik Nordmark, Mark Nottingham, Melinda Shore, Jeff Tantsura, Martin Thomson, Brian Trammel, Mirja Kuhlewind, and Colin Perkins.

The authors would also like to thank the participants of the IETF SAAG meeting where this topic was discussed:



Harald Alvestrand, Roman Danyliw, Daniel Kahn Gilmore, Wes Hardaker, Bret Jordan, Ben Kaduk, Dominique Lazanski, Eliot Lear, Lawrence Lundblade, Kathleen Moriarty, Kirsty Paine, Eric Rescorla, Ali Rezaki, Mohit Sethi, Ben Schwartz, Dave Thaler, Paul Turner, David Waltemire, and Jeffrey Yaskin.

The authors would also like to thank the participants of the IAB 2019 DEDR workshop:

Tuomas Aura, Vittorio Bertola, Carsten Bormann, Stephane Bortzmeyer, Alissa Cooper, Hannu Flinck, Carl Gahnberg, Phillip Hallam-Baker, Ted Hardie, Paul Hoffman, Christian Huitema, Geoff Huston, Konstantinos Komaitis, Mirja Kuhlewind, Dirk Kutscher, Zhenbin Li, Julien Maisonneuve, John Mattson, Moritz Muller, Joerg Ott, Lucas Pardue, Jim Reid, Jan-Frederik Rieckers, Mohit Sethi, Melinda Shore, Jonne Soininen, Andrew Sullivan, and Brian Trammell.

The authors would also like to thank the participants of the November 2016 meeting at the IETF:

Carsten Bormann, Randy Bush, Tommy C, Roman Danyliw, Ted Hardie, Christian Huitema, Ben Kaduk, Dirk Kutscher, Dominique Lazanski, Eric Rescorla, Ali Rezaki, Mohit Sethi, Melinda Shore, Martin Thomson, and Robin Wilton

Finally, the authors would like to thank numerous other people for insightful comments and discussions in this space.

#### Authors' Addresses

Jari Arkko  
Ericsson  
Valitie 1B  
Kauniainen  
Finland

Email: [jari.arkko@piuha.net](mailto:jari.arkko@piuha.net)

Stephen Farrell  
Trinity College Dublin  
College Green  
Dublin  
Ireland

Email: [stephen.farrell@cs.tcd.ie](mailto:stephen.farrell@cs.tcd.ie)

