Network Working Group
Internet-Draft
Intended status: BCP
Expires: May 24, 2014

S. Farrell
Trinity College Dublin
H. Tschofenig

November 20, 2013

Pervasive Monitoring is an Attack
draft-farrell-perpass-attack-00.txt

Abstract

The IETF has consensus that pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

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 http://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 May 24, 2014.

Copyright Notice

Copyright (c) 2013 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 (http://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.

1. It's an Attack

[[Note: This draft is written as if IETF consensus has been established for the text.]]

The technical plenary of IETF 88 [IETF88Plenary] discussed pervasive monitoring and participants had strong agreement that this was an attack and one that should be mitigated where possible via the design of protocols that make pervasive monitoring significantly more expensive or infeasible. Such pervasive surveillance requires the monitoring party to take actions that are indistinguishable from an attack on Internet communications. This Best Current Practice (BCP) documents that consensus.

For the purposes of this BCP "pervasive monitoring" means very widespread privacy-invasive gathering of protocol artefacts including application content, protocol meta-data (such as headers) or keys used to secure protocols. Other forms of traffic analysis, for example, timing or measuring packet sizes can also be used for pervasive monitoring. A fuller problem statement with more examples and description can be found in [ProblemStatement].

Note that the term "attack" is used here in a techincal sense that differs somewhat from the natural English usage. In particular, the term, when used technically, implies nothing about the motivation of the bad-actor mounting the attack, who is still called a bad-actor no matter what one really thinks about their motivation. We also use the term in the singluar here, even though pervasive monitoring in reality may require a multi-faceted set of co-ordinated attacks.

The motivation behind pervasive monitoring is not particularly relevant for this document, but can range from non-targeted nation-state surveillance, to legal but privacy-unfriendly purposes by commercial enterprises, to illegal purposes by criminals. The same techniques can be used in each case, regardless of motivation, and we cannot defend against the most nefarious actors while allowing monitoring by other actors no matter how benevolent some might consider those. As technology continues to advance rapidly techniques that have been shown to work but were once only accessible to nation-state actors become accessible to non-nation-state actors, so mitigating this threat is not only relevant when considering nation-state bad actors.

2. And we'll work to Mitigate the Attack

The IETF also have consensus to, where possible, work to mitigate the technical parts of the pervasive monitoring attack, in just the same

way as we do with any other protocol vulnerability.

There are various ways in which IETF protocols can be designed in order to mitigate pervasive monitoring, but those will change over time as mitigation and attack techniques develop and so are not described here. This BCP simply records the consensus to design protocols so as to mitigate the attack, where possible.

Note that more limited-scope monitoring to assist with network management or that is required in order to operate the network or an application are not considered pervasive monitoring. There is though a clear potential for network management mechanisms to be abused as part of pervasive monitoring, so this tension needs careful consideration in protocol design: making networks unmanageable in order to mitigate pervasive monitoring would not be an acceptable outcome, but equally, ignoring pervasive monitoring in designing network management mechanisms would go against the consensus documented in this BCP. An appropriate balance will likely emerge over time as real instances of this tension are considered.

It is also important to note that the term "mitigation" is also a technical term that does not necessarily imply an ability to completely prevent or thwart an attack. In this case, designing IETF protocols to mitigate pervasive monitoring will almost certainly not completely prevent such from happening, but can increase the cost significantly or force what was covert monitoring to be more overt, or more likely to be detected (possibly later) via other means. And even where the IETF has done this work well and that has been fully deployed, there will still be some privacy-relevant information that will inevitably be disclosed by protocols.

Finally, we note that the IETF is not equipped to tackle the non-technical aspects of mitigating pervasive surveillance. We hope that others will step forward to tackle those.

3. Process Note

In the past, architectural statements of this sort, e.g., [RFC1984] and [RFC2804] have been published as joint products of the IESG and IAB. However, since those documents were published, the IETF and IAB have separated their publication "streams" as described in [RFC4844] and [RFC5741]. This document was initiated by both the IESG and IAB, but it is being published as an IETF-stream consensus document, having garnered the consensus of the IETF as approved by the IESG.

4. Security Considerations

This BCP is all about privacy. More information about the relationship between security and privacy threats can be found in [RFC6973]. Section 5.1.1 of [RFC6973] specifically addresses surveillance as a combined security-privacy threat.

5. IANA Considerations

There are none. We hope the RFC editor deletes this section before publication.

6. Acknowledgements

We would like to thank the participants of the IETF 88 technical plenary for their feedback. Additionally, we would like to thank all those who contributed to their suggestions on how to improve Internet security on various IETF mailing lists, such as the ietf@ietf.org and the perpass@ietf.org lists.

Thanks in particular to the following for useful comments: Jari Arkko, Marc Blanchet, Benoit Claise, Spencer Dawkins, Russ Housley, Joel Jaeggli, Eliot Lear, Barry Leiba, Ted Lemon, Erik Nordmark, Pete Resnick,

7. Informative References

[IETF88Plenary]
IETF, "IETF 88 Plenary Meeting Materials", URL: https://datatracker.ietf.org/meeting/88/materials.html, Nov 2013.

[ProblemStatement]
Richard Barnes, "Pervasive Monitoring: Problem Statement", URL: To-Be-Published, Nov 2013.

[RFC1984] IAB, IESG, Carpenter, B., and F. Baker, "IAB and IESG Statement on Cryptographic Technology and the Internet", RFC 1984, August 1996.

[RFC2804] IAB and IESG, "IETF Policy on Wiretapping", RFC 2804, May 2000.

[RFC4844] Daigle, L. and Internet Architecture Board, "The RFC Series and RFC Editor", RFC 4844, July 2007.

[RFC5741] Daigle, L., Kolkman, O., and IAB, "RFC Streams, Headers, and Boilerplates", RFC 5741, December 2009.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

Authors' Addresses

Stephen Farrell
Trinity College Dublin
Dublin, 2
Ireland

Phone: +353-1-896-2354
Email: stephen.farrell@cs.tcd.ie

Hannes Tschofenig
Brussels,
Belgium

Phone:
Email: hannes.tschofenig@gmx.net