Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 22, 2014

T. Hardie

October 19, 2013

A personal touchstone for discussions of pervasive passive monitoring
draft-hardie-perpass-touchstone-00

Abstract

This document contains the author's personal statement regarding pervasive monitoring and it suggests a touchstone for the Internet engineering community to consider in protocol and system design.

Status of This Memo

This Internet-Draft is submitted to IETF 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 April 22, 2014.

Table of Contents

1. Introduction 2
2. Motivation 2
3. What is to be done? 3
4. A personal touchstone 3
5. Security Considerations 3
6. IANA Considerations 4
7. Acknowledgments 4
8. References 4
Author's Address 4

1. Introduction

It has become public knowledge that multiple national governments have severally and together engaged in pervasive monitoring of Internet communications. By reducing expectations of privacy for Internet-based communication, this surveillance circumscribes the conditions under which users will feel it is safe or appropriate to use the network. This state surveillance thus amounts to an attack on the value of the Internet, as it reduces the network effect of each user's participation. This document argues that it is the responsibility of the Internet engineering community to restore that trust and proposes a touchstone or litmus test for protocols and systems intended for Internet scale.

2. Motivation

Surveillance gives rise to self-censorship. Because the Internet is one of a very few global communication technologies, the impact of pervasive surveillance on it is self-censorship on a scale that harms humanity as a whole. Individuals who would use the network to speak may remain mute. Both within and among nations, communities which would otherwise form or grow may be retarded in their emergence or completely silenced. The scope of human interconnection is being damaged by these actions, and it must be restored.

3. What is to be done?

The Internet must change to respond to pervasive monitoring. Where protocols have traditionally mandated the implementation of integrity protection and confidentiality but not mandated their use, the use of techniques to achieve these must become a baseline expectation. Mechanisms to detect forgery of credentials must be improved and deployed. We must consider more carefully and more consistently the effects of information leakage by DNS and other infrastructure. Review and re-review of the components and systems which enable confidentiality and integrity protection must become a norm.

4. A personal touchstone

Beyond these thoughts of the Internet infrastructure changes required to restore trust in the network, I believe Internet engineers need to have a focus on the users of their systems and protocols in order to see the impact of the tradeoffs they are making. An example for me is this:

"Can a gay kid in Uganda use this safely?"

If the answer to that is "yes", chances are it meets a reasonable set of confidentiality and integrity requirements. If the answer is "no", the default response for me will be to take it back to the forge for a bit more fire and shaping. In extraordinary circumstances, another response would be a very strong statement of the limits on when this tool could be used.

Obviously, there are many possible litmus tests which could be applied. I have chosen this one in part because Uganda has a challenging network environment where it would be tempting to optimize network capacity or locality in ways which risk privacy. I have chosen it in part because gay people are a target of state suspicion or action in multiple countries. Mostly, though, I have chosen it because gay kids who find no community kill themselves in shocking numbers. There can be for me no better call to action to restore the human communication that this monitoring costs.

As noted above, this is a personal touchstone, and it may not be appropriate for all readers, all circumstances, or the community as whole. I believe, however, that considering the impact of pervasive surveillance is difficult in part because its effects are diffused across the whole network. Focusing on a touchstone user or class of users can help focus consideration of the impact of protocol choices or system design decisions. I encourage readers making such choices to choose their own.

5. Security Considerations

This document asserts that mandatory to implement security is too weak a response to pervasive surveillance, and it proposes that confidentiality and integrity protection become the norm. It also suggests that the balance between confidentiality and other optimizations needs to be seriously reconsidered by the Internet community as a whole.

6. IANA Considerations

This document makes no requests of IANA

7. Acknowledgments

The author thanks those folks kind enough to review early versions of this document.

8. References

Author's Address

Ted Hardie

Email: Ted.ietf@gmail.com