Abstract

Recent public disclosure of allegedly pervasive surveillance of Internet traffic has led to calls for action by the IETF. This draft exists solely to collect together a number of possible actions that were mentioned in a vigorous discussion on the IETF mailing list.

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 March 23, 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.
Table of Contents

1. Introduction .................................................. 3
2. Suggestions Made .............................................. 4
3. Security Considerations ................................. 7
4. IANA Considerations ........................................ 8
5. Acknowledgements ........................................... 8
6. Informative References ................................. 8
Author’s Address ................................................... 9
1. Introduction

Recent public revelations about PRISM, the alleged pervasive collection and analysis of Internet traffic, including various forms of metadata, are perhaps not surprising to those who recall ECHELON and the background to [RFC1984] and [RFC2804]. However, public knowledge that such activities are not only possible but allegedly widespread has renewed concerns about Internet surveillance and privacy. It is further alleged that some encryption systems widely regarded as reasonably safe have been compromised (https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html).

A call for IETF action has been made at http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying. Bruce Schneier states that "we need open protocols, open implementations, open systems - these will be harder for the NSA to subvert" and suggests that the IETF "needs to dedicate its next meeting to this task. This is an emergency, and demands an emergency response."

It is in fact alleged that the surveillance and compromised encryption are not mainly the result of defective standards, but rather of manufacturers and carriers being suborned. Whether it’s a real emergency can be debated. Nevertheless, it seems reasonable to discuss what the IETF could do better, in its specifications, to improve the protection of privacy, confidentiality and integrity of Internet traffic. With that in mind, the only purpose of this draft is to record a number of actionable ideas that have been mentioned in recent contributions to the IETF list. "Actionable" means that, in the editor’s view, they suggest concrete actions that the IETF could take as part of its work in developing and improving Internet technical specifications. There is no intention to imply that these ideas are good, bad or indifferent, and certainly other ideas have been and will be proposed. Important suggestions may have been missed: these are simply the ones that caught the editor’s eye, and they do not represent the outcome of an organised discussion or any kind of consensus. The contributions are presented essentially unedited (but abbreviated or truncated) and without further comment. Where a contribution led to discussion, that can be found in the mailing list archive.

This draft might be revised once or twice before IETF 88, but there are no plans for it beyond then. The editor is aware that prisms normally refract light rather than reflect it, but in this case, we are seeing reflections from a PRISM.
2. Suggestions Made

- We certainly need to apply RFC 3552. (Brian Carpenter)
- This list (http://www.nytimes.com/interactive/2013/09/05/us/unlocking-private-communications.html) includes a lot of IETF work that probably use MAY instead of SHOULD for some key choices. (Lucy Lynch)
- S/MIME is almost what we need to secure email. What is missing is an effective key discovery scheme. We could add that and add Ben Laurie’s Certificate Transparency and have a pretty good start on a PRISM Proof email scheme. ...

So that means that we have to have a key distribution infrastructure such that when you register a key it becomes available to anyone who might need to send you a message. We would also wish to apply the Certificate Transparency approach to protect the Trusted Third Parties from being coerced, infiltrated or compromised. Packaging the implementation is not difficult, a set of proxies for IMAP and SUBMIT enhance and decrypt the messages. The client side complexity is separated from the proxy using Omnibroker. ...

We do have several areas where we could make significant advances however:

1) Technical improvements to TLS such as recommending sites turn on PFS by default and remove weak ciphers.

2) Stop sending authentication cookies in the clear whether or not they are sent inside an encrypted tunnel ([I-D.hallambaker-httpsession]).

3) Fix the missing 5% that stops people using secure email. We have PGP that has mindshare and S/MIME that has deployment and both are too much trouble for most IETF people to use, let alone the typical Internet user. We can and should fix that. (Phill Hallam-Baker)

Also see [I-D.hallambaker-prismproof-req].

- Encrypting everything on the wire raises the cost for untargeted mass surveillance significantly. And that is what it is all about. And best is of course if this can be end to end, though hiding metadata requires either something onion like or transport encryption by layers below said metadata. (Martin Milnert)
- I think we can do more. Some examples:

  * we’re having a discussion in http 2.0 work whether encryption should be mandatory
the perpass list has talked about understanding better where fingerprinting is an issue with IETF protocols

maybe it would be time to start having specs say that implementations must refuse older, weak algorithms

we could do more analysis and review to understand where the weak points and development opportunities are -- too early to say there are none (Jari Arkko)

I just recently produced a short writeup about the efforts related to this topic ongoing at the last IETF meeting on my blog: http://www.tschofenig.priv.at/wp/?p=993.  (Hannes Tschofenig)

One way to frustrate this sort of dragnet surveillance would be to reduce centralization in the Internet’s architecture.  Right now, the way the Internet works in practice for private individuals, all your traffic goes up one pipe to your ISP.  It’s trivial to tap, since the tapping can be centralized at the ISP end.  [If the] IETF focused on developing protocols (and reserving the necessary network numbers) to facilitate direct network peering between private individuals, it could make it much more expensive to mount large-scale traffic interception attacks.  (Adam Novak)

There is a whole bunch of stuff we can do to make transit traffic less observable.  In other words we can modify things so the only think you know about a packet is where it is going, not what it is or who it came from.  ...

Clearly, we have a lot of specification work ongoing in different areas that helps to mitigate various security vulnerabilities.  This ranges from recent work on XMPP end-to-end security (as in [I-D.miller-3923bis]) all the way to the recent RTCWEB discussions on using DTLS-SRTP as a key management protocol.  (Stewart Bryant)

We setup the perpass list <https://www.ietf.org/mailman/listinfo/perpass> as a venue for triaging specific proposals in this space.  A few weeks in, we have [I-D.trammell-perpass-ppa] that tries to describe a threat model that matches the recent revelations, and that could be a good reference when folks are developing protocols.

We have found volunteers to write a draft for a BCP on how to use perfect forward secrecy in TLS, more common use of which (we still think) would mitigate a bunch of the ways in which TLS traffic could be subverted, given various forms of collusion/coercion.  (Stephen Farrell)

If we took protection against MitM attacks seriously, we would be using ZRTP for RTCWEB instead of DTLS-SRTP.  See [I-D.johnston-rtcweb-zrtp].  (Alan Johnston)
I think we need to separate the concept of end-to-end encryption from authentication when it comes to UI transparency. We design UIs now where we get in the user’s face about doing encryption if we cannot authenticate the other side and we need to get over that. In email, we insist that you authenticate the recipient’s certificate before we allow you to install it and to start encrypting, and prefer to send things in the clear until that is done. That’s silly and is based on the assumption that encryption isn’t worth doing *until* we know it’s going to be done completely safely. We need to separate the trust and guarantees of safeness (which require *later* out-of-band verification) from the whole endeavor of getting encryption used in the first place. (Pete Resnick)

One thing that would be helpful is to encourage the use of Diffie-Hellman everywhere. ... Using TLS with DH to secure SMTP connections is valuable even if it is subject to MITM attacks, and even if the NSA/FBI can hand a National Security Letter to the cloud provider. (Ted Ts’o)

And I think that one of the more important things we can do is to rethink UIs to give casual users more information about what is going on and to enable them to take intelligent action on decisions that should be under their control. There are good reasons why the IETF has generally stayed out of the UI area but, for the security and privacy areas discussed in this thread, there may be no practical way to design protocols that solve real problems without starting from what information a UI needs to inform the user and what actions the user should be able to take and then working backwards. (John Klensin)

What we should probably be thinking about here is:

- Mitigating single points of failure (IOW, we _cannot_ rely on just the root key)
- Hybrid solutions (more trust sources means more work to compromise)
- Sanity checking (if a key changes unexpectedly, we should be able to notice)
- Multiple trust anchors (for stuff that really matters, we can’t rely on the root or on a third party CA)
- Trust anchor establishment for sensitive communications (e.g. with banks) (Ted Lemon)

We could be telling the public about the protocols that we designed 10, 15, and even 20 years ago. Some of which even have rather widespread implementation, but seem to have zero use. (S/MIME is in every copy of Outlook and Thunderbird, AFAIK)
What would the spam situation be like if 90% of emails were regularly signed back in 1999? Yes, and DKIM can sign message bodies now too. We should be telling people about it.

Use this stuff ourselves!!!! (Michael Richardson)

- In other words, the IETF needs to assume that we don’t know what will work for end users and we need to therefore focus more on processing by end systems rather than end users. (Dave Crocker)
- In effect, DANE exchanges one trust model for another. I happen to believe that the damage risk is lower with DNSSEC + DANE than the traditional "any CA can issue a certificate for any domain name" setup.

Audit and open source seem to be good starting points. (Mans Nilsson)

- There was actually a proposal a couple of weeks back in the WG to encrypt all traffic on the inter-xTR stage [in the LISP protocol]. (Noel Chiappa)
- Review all key length recommendations and make them larger and strongly recommend not using any shorter than <foo>. While the reports are probably true that NSA can break common algorithms, making the key length longer will make it harder to do it in scale.

Move to real end to end security where key are shared via a different communication path. Perhaps like PGP.

Remove man in the middle attacks on common protocols like SSL/TLS. This is a giant problem, some people sell products that view this as a feature (including my employer). This is part of a general problem of middle boxes that change content, but can be fixed if we make sure they can’t alter the secure content.

Make everything run over secure paths. Even things like the DNS and ICMP. Perhaps if we can secure ICMP, it will mean that middle boxes will stop dropping things like PMTU discovery packets. (Bob Hinden, in private mail, included with permission).

- It is a shame that this opportunity was not taken to highlight the need for authentication. Having a totally secure channel with perfect encryption is of little value if the other end of the channel is a hostile power. (Tom Petch)

3. Security Considerations

See above. Also, an observation by Hannes Tschofenig seems relevant:

While we are able to fill gaps in security protocols fairly quickly
we don’t always seem to make the right choices because the interests of various participants are not necessarily aligned. In general, we seem to develop an insecure version and a secure version of a protocol. Unfortunately, the insecure version gets widely deployed and we have an incredible hard time to introduce the secure version.

In addition to the specification work we could think about how to reach out to the broader Internet ecosystem a bit better. Since we have lots of folks in the IETF I don’t think it is an impossible task but it might require a bit of coordination. Right now would be a good time to launch some of those initiatives since most people currently understand the need for security.

4. IANA Considerations

This document requests no action by IANA.

5. Acknowledgements

The ideas are credited above.

This document was produced using the xml2rfc tool [RFC2629].

6. Informative References

[I-D.hallambaker-httpsession]
Hallam-Baker, P., "HTTP Session Management",
draft-hallambaker-httpsession-01 (work in progress),
May 2013.

[I-D.hallambaker-prismproof-req]
Hallam-Baker, P., "PRISM-Proof Security Considerations",
draft-hallambaker-prismproof-req-00 (work in progress),
September 2013.

[I-D.johnston-rtcweb-zrtp]
Johnston, A., Zimmermann, P., Callas, J., Cross, T., and
J. Yoakum, "Using ZRTP to Secure WebRTC",
draft-johnston-rtcweb-zrtp-00 (work in progress),
August 2013.

[I-D.miller-3923bis]
Miller, M. and P. Saint-Andre, "End-to-End Object
Encryption for the Extensible Messaging and Presence
Protocol (XMPP)", draft-miller-3923bis-02 (work in


Author’s Address

Brian Carpenter (editor)
Department of Computer Science
University of Auckland
PB 92019
Auckland, 1142
New Zealand

Email: brian.e.carpenter@gmail.com