Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: April 24, 2014

A. Cooper
CDT
S. Farrell
Trinity College Dublin
S. Turner
IECA, Inc.

October 21, 2013

Privacy Requirements for IETF Protocols
draft-cooper-ietf-privacy-requirements-01.txt

Abstract

It is the consensus of the IETF that our protocols be designed to avoid privacy violations to the extent possible. This document establishes a number of protocol design choices as Best Current Practices for the purpose of avoiding such violations.

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 April 24, 2014.

Table of Contents

1. Introduction

The IETF has long-standing principles that support strong security in protocol design and a tradition of encouraging protocol designers to take these principles into account. [RFC1984] articulated the view that encryption is an important tool to protect the cofidentiality of communications, and that as such it should be encouraged and available to all. [RFC3365] requires that all protocols implement strong security. [RFC3552] provides guidance about how to consider security in protocol design and how to document security choices. In [RFC2804], the IETF established a policy of not considering wiretapping requirements in IETF standards-track protocols. [RFC6973] explains the many different aspects of privacy that can be affected by Internet protocol design and provides guidance to help designers consider privacy in their work.

This document extends the existing body of IETF principles concerning security by articulating Best Current Practices for avoiding privacy violations and establishing support for privacy as a principle of IETF protocol design. These principles, old and new, should be applied when designing new protocols, and where applicable, should be considered for updates of existing protocols.

It is also the consensus of the IETF that pervasive surveillance is an attack on privacy that should be defended against through protocol design.

Discussion of this draft is directed to the ietf-privacy@ietf.org list.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. These words take their normative meanings only when they are presented in ALL UPPERCASE.

"Opportunistic encryption" is defined as encryption without any pre-arrangement specific to the pair of systems involved (e.g., by using a Diffie-Hellman exchange). See [RFC4322].

Privacy-specific terminology is provided in [RFC6973]. Of particular relevance to this document is the term "personal data," defined as "any information relating to an individual who can be identified, directly or indirectly." Identifiers such as IP addresses that can remain consistent over time or that particular parties associate with directly identifiable information (such as a real name or street address) are therefore considered to be personal data.

3. Recommendations

There are inherent privacy risks with protocols that allow the communicating parties to store personal data, transport personal data, or are vulnerable to other parties observing the personal data in the exchanged communications. Most Internet communications involve such risks, which can allow entities to build large databases of information that by themselves or in conjunction with other databases can identify people and their actions in invasive ways.

Therefore, to the extent consistent with basic protocol operation and management, standards-track IETF protocols that involve transmission of personal data:

1. MUST minimize their use of such personal data, and

2. where personal data is sent, MUST have well-defined and interoperable ways to send such data encrypted for the intended recipient(s).

While existing principles call for strong security, it is important to note that strong security only in cases where the other party can be authenticated does not by itself solve all privacy problems. To guard against dangers of large-scale privacy attacks, some protection is needed also for other situations.

As a consequence, at minimum, opportunistic encryption MUST be well-defined for new IETF standards track protocols. This requirement can be waived only in exceptional circumstances where the protocol's utility would be eliminated or severely diminished if opportunistic

encryption were defined. Note that encryption provides one aspect of privacy protection, namely confidentiality. In most cases it will be better to (also) specify how to do one-sided (e.g., TLS server authentication as commonly used in the web) or mutually authenticated encryption. Where both opportunistic and one-sided or mutually authenticated encryption are specified, protocols MUST also protect against downgrade attacks so that scenarios where authentication is required cannot easily be manipulated into using opportunistic encryption which will often be subject to man-in-the-middle attacks.

Note that these encryption requirements are contingent on practicality - if some personal data really has to be sent in clear for a protocol to be able to operate, and even opportunistic encryption is not possible, then a standards-track protocol that does not define how to protect that data will be consistent with this BCP. The IETF will have to decide in such cases whether standardising that protocol benefits the Internet or not.

Many IETF protocols allow for some data items to be optionally or conditionally sent. If personal data can be sent, then the conditions above apply.

Specifications that do not meet the criteria above MUST include (or reference) an explanation of why they do not conform to this BCP.

4. Examples and Explanation

This section has some examples and explanatory material. [[More, including references, will be added as discussion evolves.]]

DHCP is an example of a protocol where it seems quite hard to provide useful confidentiality. Should a new DHCP option be defined that carries personal data, then the IETF would have to decide if the benefit of that outweighs the potential privacy cost.

For some protocols, layering on top of a security protocol like TLS, SSH or IPsec can be a useful way to provide confidentiality. However, just because it could be possible to do that does not mean that that is sufficient to claim conformance with this BCP. For example, claiming that Diameter conformed to this BCP becuase one could in principle run Diameter over IPsec would not be credible, as it seems that such deployments are rare to non-existent. In the same way that being being realistic is important when we consider a claim that sending personal data is unavoidable, it is just as important when claiming that layering on top of a security protocol can meet the requirements of this BCP.

For some protocols, minimizing the use of personal data involves limiting the lifetime of identifiers. In cases where an identifier refers to an individual (or a proxy for an individual, such as a host device or software instance), the longer that identifier persists and the more contexts in which it is used, the more it can facilitate correlation and tracking of information related to the individual and his or her activities. Creating identifiers that have limited lifetimes by default reduces the possibility that multiple protocol interactions or communications can be correlated back to the same individual. [RFC4941] provides an example in the case of stateless autoconfiguration of IPv6 interface identifiers.

Since the goal here is to have a BCP that covers all IETF standards track protocols we clearly cannot address all aspects of privacy, for example user participation, since that would only be relevant for a small proportion of IETF protocols.

One could consider mininimising the personal data sent by IETF protocols as a form being conservative in what you send, one of the longest standing principles in IETF protocol design. There doesn't seem to be an equivalent here for being liberal in what you accept.

5. Security Considerations

This document articulates a set of Best Current Practices for privacy that extend the IETF's existing security principles. At times, privacy and security may appear to be in tension. For example, adherence to the recommendation in this BCP to minimize the use of personal data will likely yield less use of persistent identifiers associated with individual users. Reducing the use of persistent identifiers can help attackers shield their identities and activities just as it can for legitimate users. However, even relatively unsophisticated attackers already have at their disposal a variety of tools for cloaking their identities. Recommending the minimization of personal data use at the protocol level can benefit the vast majority of legitimate users who depend on IETF protocols without materially improving attackers' existing tools for guarding their identities.

Similarly, malware and other attack traffic can generally already be transmitted using object encryption or protocol encryption if attackers so choose. Recommending that IETF protocols define mechanisms for opportunistic encryption can increase the availability of confidentiality protection to legitimate users without significantly changing the set of tools that attackers already use to shield their traffic from being identified and their attacks from being thwarted.

6. IANA Considerations

This document does not require actions by IANA.

7. Acknowledgements

Thanks to the following for useful comments. These folks may or may not agree with the content.

Jari Arkko, Bernard Aboba, Scott Brim, Benoit Claise, Nick Doty, Spencer Dawkins, Eliot Lear, Ted Lemon, SM, Avri Doria, Brian Trammell, Robin Wilton,

8. Informative References

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, August 2002.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[RFC4322] Richardson, M. and D. Redelmeier, "Opportunistic Encryption using the Internet Key Exchange (IKE)", RFC 4322, December 2005.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[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

Alissa Cooper
CDT
1634 Eye St. NW, Suite 1100
Washington, DC 20006
US

Phone: +1-202-637-9800
Email: acooper@cdt.org
URI: http://www.cdt.org/

Stephen Farrell
Trinity College Dublin
Dublin 2
Ireland

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

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

Phone: +1.703.628.3180
Email: turners@ieca.com