INTERNET-DRAFT
Intended Status: Informational
Expires: June 8, 2014

S. Moonesamy

December 5, 2013

Traffic peeking
draft-moonesamy-traffic-peeking-01

Abstract

In June 2013, a news article revealed that the National Security Agency obtained direct access to the systems of several service providers from the United States through an undisclosed surveillance programme called PRISM. This document discusses about traffic peeking.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Table of Contents

1. Acknowledgements

The author would like to thank Iain Ross Learmonth for his comments.

2. Background

In June 2013, a news article [Guar1] revealed that the National Security Agency obtained direct access to the systems of several service providers from the United States through an undisclosed surveillance programme called PRISM [Guar2]. The surveillance programme intercepted traffic flowing through communication links used throughout the world. According to a news article published in October 2013, the National Security Agency had also been wiretapping traffic flowing between the datacenters used by Google and Yahoo [Wash1].

In 2007, Dan Shumow and Niels Ferguson discussed about the possibility of a backdoor in a Dual Elliptic Curve pseudorandom number generator [Rump] (see Appendix D for more information). In September, 2013, the National Institute of Standards and Technology reported that concern has been expressed about the Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG) algorithm published in one of its standards (SP 800-90/90A) [NIST].

3. Traffic peeking

RFC 1958 [RFC1958] states that "it is highly desirable that Internet carriers protect the privacy and authenticity of all traffic, but this is not a requirement of the architecture. "Tussle in Cyberspace: Defining Tomorrow's Internet" [Tussle] states that "peeking is irresistible". Given that most Internet traffic is not encrypted, there isn't any significant barrier to hamper an entity with the available resources to peek on the traffic of Internet carriers. As data storage is affordable the next step would be to go beyond traffic peeking and collect all the data. [Tussle] argued that "if there is information visible in the packet, there is no way to keep an intermediate node from looking at it. So the ultimate defense of the end to end mode is end to end encryption".

3.1. Encrypting traffic

Encrypting traffic "might just be the first step in an escalating tussle between the end user and the network provider, in which the response of the provider is to refuse to carry encrypted data" [Tussle]. It helps to shape the end user's expectations as the latter will be aware of the restrictions.

The end user relies on the organizations recommending the standards

as it is not possible for the average person to evaluate whether the encryption mechanism used will protect the traffic from wiretapping. It is to be noted that some encryption standards are incorporated by reference in standards used for the Internet.

4. Security Considerations

Entities exchanging traffic over the Internet should assume that any traffic which is not encrypted should be assumed to be compromised given that peeking is irresistible. There is a risk that encrypted traffic will not provide any protection if it is stored indefinitely as the ability to recover the traffic is preserved.

5. Conclusion

The security dilemma exists when "many of the means by which a country tries to increase its security decrease the security of others". It is up to designers and implementers of a protocol to see whether the encryption standard they use will provide a level of the security which they consider acceptable.

It is in the interest of a network provider or a provider of a service to collaborate with the relevant government. The end user will usually be at the losing end of the bargain in a tussle between the end user and government when Internet traffic wiretapping is a matter of national security.

6. IANA Considerations

[RFC Editor: please remove this section]

7. References

7.1. Informative References

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, June 1996.

[RFC0959] Postel, J. and J. Reynolds, "File Transfer Protocol", STD 9, RFC 959, October 1985.

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", RFC 1725, November 1994.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

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

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[RFC3924] Baker, F., Foster, B., and C. Sharp, "Cisco Architecture for Lawful Intercept in IP Networks", RFC 3924, October 2004.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008.

[Athens] Prevelakis V. and Spinellis D. "The Athens Affair. IEEE Spectrum 44", July 2007.

[ETSI1] European Telecommunications Standards Institute, Lawful Interception (LI); Requirements of Law Enforcement Agencies", TS 01 331 V1.3.1, October 2009.

[FBNZ] Facebook, Australia & New Zealand, "Comments on Telecommunications (Interception Capability and Security) Bill", July 2012, <http://www.parliament.nz/resource/0001672174>

[Guar1] <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

[Guar2] <http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>

[HUNZ] Huawei Technologies (New Zealand) Company Limited, "Submission from Huawei Technologies New Zealand Limited on the Telecommunications (Interception Capability and Security)", June 2013, <http://www.parliament.nz/resource/0001672362>

[MSNZ] Microsoft New Zealand Limited, "Comments on Telecommunications (Interception Capability and Security) Bill", June 2013, <http://www.parliament.nz/resource/0001678514>

[NIST] <http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf>

[Rump] <http://rump2007.cr.yp.to/15-shumow.pdf>

[Tussle] Clark D., Wroclawski J., Sollins K., Braden R., "Tussle in

cyberspace: Defining tomorrow's Internet", 2002.

[USGov1] United States Government Printing Office, "47 U.S.C. 1008 - Payment of costs of telecommunications carriers to comply with capability requirements"

[Wash1] <http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html>

Appendix A: IETF Protocols without encryption

There are several widely deployed IETF protocols which generate plain text (unencrypted) traffic. The specifications of these protocols usually have a Security Considerations section to discuss the security issues. The specifications mentioned below is not an exhaustive list of IETF protocols which are vulnerable to traffic peeking.

The File Transfer Protocol (FTP) [RFC0959] is sometimes used for transferring files. The specification does not provide any guidance about encrypting the traffic generated by the protocol.

The Hypertext Transfer Protocol (HTTP) [RFC2616] is widely used to access the web. The protocol is sometimes used to provide web access to email. Section 15 of RFC 2616 [RFC2616] does not provide any guidance about encrypting the traffic generated by the protocol.

The Internet Message Access Protocol, Version 4rev1 [RFC3501] can be used by the end user to read email messages. Section 11 of RFC 3501 [RFC3501] states that "sent in the clear over the network unless protection from snooping is negotiated". There is some information about encrypting the traffic generated by the protocol.

The Post Office Protocol, Version 3 [RFC1939] can be used by the end user to read email messages. Section 13 of RFC 1939[RFC1939] does not provide any guidance about encrypting the traffic generated by the protocol.

The Simple Mail Transfer Protocol [RFC5321] is used for sending email messages. Section 7 of RFC 5321[RFC5321] states that "SMTP mail is inherently insecure". It is mentioned in the section that "real mail security lies only in end-to-end methods".

Appendix B: Wiretapping

The IETF decided not to consider requirements for wiretapping as part

of the process for creating and maintaining IETF standards [RFC2804]. It was the belief of the IETF that "in the case of traffic that is today going across the Internet without being protected by the end systems (by encryption or other means), the use of existing network features, if deployed intelligently, provides extensive opportunities for wiretapping". It was noted that "the end systems take adequate measures to protect their communications".

A well-known wiretapping case is the Athens affair [Athens] which targeted the conversations of specific, highly placed government and military officials. The scope of the activity is to a large extent unknown.

Appendix C: Lawful Interception

It was the belief of the IETF that "mechanisms designed to facilitate or enable wiretapping, or methods of using other facilities for such purposes, should be openly described". RFC 3924 [RFC3924] describes the Cisco Architecture for Lawful Intercept in IP Networks.

The European Telecommunications Standards Institute, Technical Committee Lawful Interception (TC LI) [ETSI1], publishes standards about lawful interception. The standards specify the network or service protocols necessary to provide handover of lawfully intercepted data and traffic, as well as the physical or logical point at which the interception has to take place (the handover interface) both for packet data and circuit-switched communications.

In Europe, the Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01) enables its member states "to conduct the lawful interception of telecommunications", subject to national law and interpreted in accordance with applicable national policies. Most countries have a legal framework which "generally obliges all providers of public electronic communications networks and services to cooperate". This includes the obligation to install interception equipment, usually without compensation.

In the United States, the Communications Assistance for Law Enforcement Act requires telecommunications carriers (including broadband Internet access providers and providers of VoIP services) "to ensure that equipment, facilities, or services that allow a customer or subscriber to "originate, terminate, or direct communications," enable law enforcement officials to conduct electronic surveillance pursuant to court order or other lawful authorization". The legislation provides for the payment of costs of telecommunications carriers to comply with capability requirements [USGov1].

Article 3 of the Budapest Convention on Cybercrime about illegal interception requires the countries ratifying the treaty "to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally".

The New Zealand Parliament updated its legislation about Interception Capability and Security this year. Several entities provided comments about the legislation where it was proposed [FBNZ][HUNZ][MSNZ]. It is to be noted that the entities operate in several jurisdictions.

Appendix D: Implementation of the Dual Elliptic Curve DRBG

The Dual EC DRBG was implemented in OpenSSL, an open source general purpose cryptography library, in 2011 at the request of a paying customer. The implementer was "well aware at the time of the dubious reputation of the algorithm". It was mentioned that cryptography in the United States Federal government is heavily constrained by standards [NIST] and vendors selling products to that government don't have much of a choice.

Author's Addresses

S. Moonesamy
76, Ylang Ylang Avenue
Quatre Bornes
Mauritius

Email: sm+ietf@elandsys.com