

Traffic peeking
draft-moonesamy-traffic-peeking-03

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 the practice of 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/lid-abstracts.html>

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

Copyright and License Notice

Copyright (c) 2014 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.	Acknowledgements	3
2.	Background	3
3.	Traffic peeking	3
3.1.	IETF Protocols without encryption	4
3.2.	Encrypting traffic	4
4.	Security Considerations	5
5.	Conclusion	5
6.	IANA Considerations	5
7.	References	5
7.1.	Informative References	6
Appendix A:	Electronic Surveillance	9
Appendix B:	Implementation of the Dual Elliptic Curve DRBG	10
	Author's Addresses	10

1. Acknowledgements

The author would like to thank Iain Ross Learmonth for his review and contributions to this document.

2. Background

In June 2013, a news article [[Guar1](#)] revealed that the (United States) 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](#)][Europa]. 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 through private networks between the datacenters used by Google and Yahoo [[Wash1](#)]. According to a news article [[Guar3](#)] millions of Yahoo webcam images were intercepted by GCHQ. Between 3% and 11% of the Yahoo webcam imagery harvested contained "undesirable nudity".

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 B](#) for more information). In September 2013, the (United States) 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](#)]. ISO/IEC JTC 1/SC 27 recommended [[JTC](#)] that users of the ISO/IEC 18031:2011 standard [[ISO8031](#)] take note of the concerns relating to the default application specific parameters that are provided in Annex D of that international standard. According to a news article [[Reuters](#)] published in December 2013 RSA received U.S. \$10 million in a deal that set the Dual Elliptic Curve Deterministic Random Bit Generation as the preferred, or default, method for number generation in the BSafe software [[RSA](#)].

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 even modest resources, let alone the resources of a nation's government, to peek on the traffic of Internet carriers. As data storage is becoming rapidly more affordable the next step would be to go beyond traffic peeking and archive 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. 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 list of specifications mentioned below lists a selection of IETF protocols vulnerable to traffic peeking but is definitely not an exhaustive list.

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](#)] is widely used to read email messages. [Section 11 of RFC 3501](#) [[RFC3501](#)] states that "protocol transactions, including electronic mail data, are sent in the clear over the network unless protection from snooping is negotiated". Details about negotiating encryption are provided; there isn't any recommendation about when encryption should be used. It could be argued that for accessing email, users have an expectation of the privacy of their messages and so encryption should be used unless it is technically or legally infeasible to do so. [RFC 3501](#) does not reflect this.

Similarly, the Post Office Protocol, Version 3 [[RFC1939](#)] is used to read email messages. [Section 13 of RFC 1939](#) [[RFC1939](#)] does not provide any guidance about encrypting the traffic generated by the protocol but does acknowledge that "use of the PASS command sends passwords in the clear over the network" and "use of the RETR and TOP commands sends mail in the clear over the network".

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".

3.2. 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](#)][[Torrent](#)]. In this case, protocols preferring encryption still have an advantage over those that don't as they can present the user with a warning that it will be necessary to fallback to an unencrypted communication. This allows the user to adjust their expectations of how private a communication will be.

The end user relies on the organizations recommending the standards and software vendors as it is not possible for the average person to evaluate whether the encryption mechanism used will protect the traffic from peeking [[Apple](#)][[Etisal](#)][[Mums](#)][[Ossl](#)]. It is to be noted that some encryption standards are incorporated by reference in standards used for the Internet [[IAB](#)]. There is a brief discussion about electronic surveillance in [Appendix A](#).

[4. Security Considerations](#)

Entities exchanging traffic over the Internet should assume that any traffic which is not encrypted can be intercepted 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 [[Netcraft](#)].

[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"[[Jervis](#)]. 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. Even where it is not possible to use encryption to prevent peeking, recommendations can still be provided to implementers to ensure that there is awareness of the security methods, or lack of, being used to protect the traffic generated by the protocol.

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 it is claimed that traffic peeking is a matter of national interest.

[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.
- [Apple] Apple Inc., "About the security content of iOS 7.0.6", February 2014, <<http://support.apple.com/kb/HT6147>>
- [Dual] Checkoway S., Fredrikson M., Niederhagen R., Green M., Lange T., Bernstein D. J., Maskiewicz J. and Shacham H., "On the Practical Exploitability of Dual EC in TLS Implementations". 5 , and Hovav Shacham
- [Etisalat] "Etisalat's BlackBerry patch designed for surveillance", July 2009, <<http://www.itp.net/561962-etisalats-blackberry-patch-designed-for-surveillance>>
- [ETSI] European Telecommunications Standards Institute, "Lawful Interception (LI); Requirements of Law Enforcement Agencies", TS 01 331 V1.3.1, October 2009.
- [Europa] European Commission, "PRISM scandal: The data protection rights of EU citizens are non-negotiable", June 2013,

<http://europa.eu/rapid/press-release_SPEECH-13-536_en.htm>

- [Fbnz] Facebook, Australia & New Zealand, "Comments on Telecommunications (Interception Capability and Security) Bill", July 2012,
<<http://www.parliament.nz/resource/0001672174>>
- [Guar1] The Guardian, "NSA Prism program taps in to user data of Apple, Google and others", June 2013,
<<http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>>
- [Guar2] The Guardian, "NSA Prism program slides", November 2013,
<<http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document>>
- [Guar3] The Guardian, "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ", February 2014,
<<http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo>>
- [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>>
- [IAB] IAB, "NIST Cryptographic Standards and Development Process", April 2014, <<http://www.iab.org/wp-content/IAB-uploads/2014/04/IAB-NIST7977-20140407.pdf>>
- [ISO8031] ISO, "ISO/IEC 18031:2011 Information technology -- Security techniques -- Random bit generation", November 2011
- [Java] RSA, The Security Division of EMC, "RSA BSAFE Share for JavaTM Platform", January 2013,
<<https://community.emc.com/docs/DOC-4741>>
- [Jervis] Jervis R., "Cooperation Under the Security Dilemma", World Politics, Vol. 30, No. 2, January 1978
- [JTC] ISO, "A Cautionary Note on the Use of ISO/IEC 18031:2011",
<<http://isotc.iso.org/livelink/livelink/open/16315553>>
- [Mcaf] McAfee, "Patches resolve RSA BSafe Dual Elliptic Curve DRBG algorithm vulnerability - Security Bulletins ID: SB10067", March 2014,

- <<https://kc.mcafee.com/corporate/index?page=content&id=SB10067>>
- [Msnz] Microsoft New Zealand Limited, "Comments on Telecommunications (Interception Capability and Security) Bill", June 2013, <<http://www.parliament.nz/resource/0001678514>>
- [Mums] Mumsnet, "Mumsnet and Heartbleed as it happened", April 2014, <<http://www.mumsnet.com/features/mumsnet-and-heartbleed-as-it-happened>>
- [Netcraft] Netcraft, "SSL: Intercepted today, decrypted tomorrow", September 2013, <<http://news.netcraft.com/archives/2013/06/25/ssl-intercepted-today-decrypted-tomorrow.html>>
- [NIST] National Institute of Standards and Technology, "NIST opens draft Special Publication 800-90A, Recommendation for Random Number Generation using Deterministic Random Bit Generators, for review and comment", September 2013, <http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf>
- [Ossl] OpenSSL Project, "OpenSSL Security Advisory - TLS heartbeat read overrun", April 2014, <https://www.openssl.org/news/secadv_20140407.txt>
- [Reuters] Reuters, "Secret contract tied NSA and security industry pioneer", December 2013, <<http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220>>
- [RSA] RSA, The Security Division of EMC, "RSA response to media claims regarding NSA relationship", December 2013, <<https://blogs.rsa.com/news-media/rsa-response/>>
- [Rump] Shumow D., Ferguson N., "On the possibility of a Back Door in the NIST SP800-90 Dual Ec Prng", August 2007, <<http://rump2007.cr.yp.to/15-shumow.pdf>>
- [Torrent] TorrentFreak, "https://torrentfreak.com/uk-internet-filter-blocks-vpns-australia-to-follow-soon-130905/", September 2013, <<https://torrentfreak.com/uk-internet-filter-blocks-vpns-australia-to-follow-soon-130905/>>
- [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] The Washington Post, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say", October 2013,
<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: Electronic Surveillance

Electronic surveillance is sometimes referred to as "wiretapping". A well-known electronic surveillance case is the Athens affair [[Athens](#)] which targeted the conversations of specific, highly placed government and military officials. The scope of that activity is to a large extent unknown. The following is a brief discussion of the topic in IETF RFCs, standards and legislation.

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".

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) [[ETSI](#)], 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 last 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 B: 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. RSA BSafe Dual Elliptic Curve DRBG implementation was used in McAfee Software [[Mcaf](#)] and Share for Java [[Java](#)]. "Depending on the design choices in the implementations, an attacker can recover TLS session keys within seconds on a single CPU or may require a cluster of more than 100,000 CPUs for the same task if a different library is used" [[Dual](#)].

Author's Addresses

S. Moonesamy

76, Ylang Ylang Avenue
Quatre Bornes
Mauritius

Email: sm+ietf@elandsys.com