Operational Security Capabilities for
IP Network Infrastructure (opsec)
Internet-Draft
Intended status: Informational
Expires: April 18, 2013

F. Gont
Huawei Technologies

October 15, 2012

Virtual Private Network (VPN) traffic leakages in dual-stack hosts/ networks
draft-gont-opsec-vpn-leakages-00

Abstract

The subtle way in which the IPv6 and IPv4 protocols co-exist in typical networks, together with the lack of proper IPv6 support in popular Virtual Private Network (VPN) products, may inadvertently result in VPN traffic leaks. That is, traffic meant to be transferred over a VPN connection may leak out of such connection and be transferred in the clear on the local network. This document discusses some scenarios in which such VPN leakages may occur, either as a side effect of enabling IPv6 on a local network, or as a result of a deliberate attack from a local attacker. Additionally, it discusses possible mitigations for the aforementioned issue.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

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 18, 2013.

Table of Contents

1. Introduction

It is a very common practice for employees working at remote locations to establish a VPN connection with their office or home office. This is typically done to gain access to some resources only available within the company's network, but also to secure the host's traffic against attackers that might be connected to the same remote location. In some scenarios, it is even assumed that employing a VPN connection makes the use of insecure protocols (e.g. that transfer sensitive information in the clear) acceptable, as the VPN provides security services (such as confidentiality) for all communications made over the VPN.

Many VPN products that are typically employed for the aforementioned VPN connections only support the IPv4 protocol: that is, they perform the necessary actions such that IPv4 traffic is sent over the VPN connection, but they do nothing to secure IPv6 traffic originated from (or being received at) the host employing the VPN client. However, the hosts themselves are typically dual-stacked: they support (and enable by default) both IPv4 and IPv6 (even if such IPv6 connectivity is simply "dormant" when they connect to IPv4-only networks). When the IPv6 connectivity of such hosts is enabled, they may end up employing an IPv6-unaware VPN client in a dual-stack network. This may have "unexpected" consequences, as explained below.

The subtle way in which the IPv4 and IPv6 protocols interact and co-exist in dual-stacked networks might, either inadvertently or as a result of a deliberate attack, result in VPN traffic leakages -- that is, traffic meant to be transferred over a VPN connection could leak out of the VPN connection and be transmitted in the clear on the local network, without employing the VPN services at all.

Section 2 provides some background about IPv6 and IPv4 co-existence, summarizing how IPv4 and IPv4 interact on a typical dual-stacked network. Section 3 describes the underlying problem that leads to the aforementioned VPN traffic leakages. Section 4 describes legitimate scenarios in which such traffic leakages might occur, while Section 5 describes how VPN traffic leakages can be triggered by deliberate attacks.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. IPv4 and IPv6 co-existence

The co-existence of the IPv4 and IPv6 protocols has a number of interesting and subtle aspects that may have "surprising" consequences. While IPv6 is not backwards-compatible with IPv4, the two protocols are "glued" together by the Domain Name System (DNS).

For example, consider a site (say, www.example.com) that has both IPv4 and IPv6 support. The corresponding domain name (www.example.com, in our case) will contain both A and AAAA DNS resource records (RRs). Each A record will contain one IPv4 address, while each AAAA record will contain one IPv6 address -- and there might be more than one instance of each of these record types. Thus, when a dual-stacked client application means to communicate with the aforementioned site, it can request both A and AAAA records, and use any of the available addresses. The preferred address family (IPv4 or IPv6) and the specific address that will be used (assuming more than one address of each family is available) varies from one protocol implementation to another, with many host implementations preferring IPv6 addresses over IPv4 addresses.

> [RFC6724] specifies an algorithm for selecting a destination address from a list of IPv6 and IPv4 addresses. [RFC6555] discusses the challenge of selecting the most appropriate destination address, along with a proposed implementation approach that mitigates connection-establishment delays.

This "co-existence" between IPv6 and IPv4 means that, when a dual-stacked client means to communicate with some other system, the availability of A and AAAA DNS resource records will typically affect which protocol is employed to communicate with that system.

3. Virtual Private Networks in IPv4/IPv6 dual-stack hosts/networks

Many Virtual Private Network (VPN) implementations do not support the IPv6 protocol -- or, what is worse, they completely ignore IPv6. This typically means that, when establishing a VPN connection, the VPN software takes care of the IPv4 connectivity by, e.g. inserting an IPv4 default route that causes all IPv4 traffic to be sent over the VPN connection (as opposed to sending the traffic in the clear, employing the local router). However, if IPv6 is not supported (or completely ignored), any packets destined to an IPv6 address will be sent in the clear using the local IPv6 router. That is, the VPN software will do nothing about the IPv6 traffic.

The underlying problem here is that while IPv4 and IPv6 are two different protocols incompatible with each other, the two protocols are glued together by the Domain Name System. Therefore, for dual-stacked systems, it is not possible to secure secure the communication with another system without securing both protocols (IPv6 and IPv4).

4. VPN traffic-leakages in legitimate scenarios

Consider a dual-stacked host that employs IPv4-only VPN software to establish a VPN connection with a VPN server, and that the host now attaches to a dual-stacked network (that provides both IPv6 and IPv4 connectivity). If some application on the client needs to communicate with a dual-stacked destination, the client will typically query both A and AAAA DNS resource records. Since the host will have both IPv4 and IPv6 connectivity, and the intended destination will have both A and AAAA DNS resource records, one of the possible outcomes is that the host will employ IPv6 to communicate with the aforementioned system. Since the VPN software does not support IPv6, the IPv6 traffic will not employ the VPN connection, and will be sent in the clear on the local network.

This could inadvertently expose sensitive traffic that was assumed to be secured by the VPN software. In this particular scenario, the resulting VPN traffic leakage is a side-effect of employing IPv6-unaware software in a dual-stacked host/network.

5. VPN traffic-leakage attacks

A local attacker could deliberately trigger IPv6 connectivity on the victim host by sending forged ICMPv6 Router Advertisement messages. Such packets could be sent by employing standard software such as rtadvd [RTADVD], or by employing packet-crafting tools such as the [SI6-Toolkit] or THC-IPv6 [THC-IPv6]. Once IPv6 connectivity has been enabled, communications with dual-stacked systems could result in VPN traffic leakages, as previously mentioned.

While this attack may be useful enough (due to the increasing number of IPv6-enabled sites), it will only lead to traffic leakages when the destination system is dual-stacked. However, it is usually trivial for an attacker to trigger such VPN leakages for any destination systems: an attacker could simply advertise himself as the local recursive DNS server by sending forged Router Advertisement messages that include the corresponding RDNSS option, and then perform a DNS spoofing attack such that he can become a "Man in the Middle" and intercept the corresponding traffic. As with the previous attack scenario, packet-crafting tools such as [SI6-Toolkit] and [THC-IPv6] can readily perform this attack.

Some systems are known to prefer IPv6-based recursive DNS servers over IPv4-based ones, and hence the "malicious" recursive DNS servers would be preferred over the legitimate ones advertised by the VPN server.

6. Mitigations to VPN traffic-leakage vulnerabilities

There are a number of possible mitigations for the VPN traffic-leakage vulnerability discussed in this document.

If the VPN client is configured by administrative decision to redirect all traffic for IPv4 to the VPN, it should:

1. If IPv6 is not supported, disable IPv6 support in all network interfaces

   For IPv6-unaware VPN clients, the most simple mitigation (although not necessarily the most desirable one) would be to disable IPv6 support in all network interface cards when a VPN connection is meant to be employed. Thus, applications on the host running the VPN client software will have no other option than to employ IPv4, and hence they will simply not even try to send/process IPv6 traffic.

2. If IPv6 is supported, ensure that all IPv6 traffic is also sent via the VPN

If the VPN client is configured to only send a subset of IPv4 networks to the VPN tunnel (split-tunnel mode), and the VPN client does not support IPv6, it should disable IPv6 as well. If it supports IPv6, it is the administrators responsibility to ensure that the correct corresponding sets of IPv4 and IPv6 networks get routed into the VPN tunnel.

Additionally, VPN clients that support IPv6 should mitigate all ND-based attacks that may introduce new entries in the routing table, such attacks based on forged RA messages containing more specific routes, forged ICMPv6 Redirect messages, etc.

A network may prevent local attackers from successfully performing the aforementioned attacks against other local hosts by implementing First-Hop Security solutions such as Router Advertisement Guard (RA-Guard) [RFC6105] and DHCPv6-Shield [I-D.gont-opsec-dhcpv6-shield]. However, for obvious reasons, a host cannot and should not rely on this type of mitigations when connecting to an open network (cybercafe, etc.).

Besides, popular implementations of RA-Guard are known to be vulnerable to evasion attacks [I-D.ietf-v6ops-ra-guard-implementation].

7. IANA Considerations

This document has no actions for IANA.

8. Security Considerations

This document discusses how traffic meant to be transferred over a VPN connection can leak out of the VPN, and hence appear in the clear on the local network. This is the result of employing IPv6-unaware VPN client software on dual-stacked hosts.

Possible ways to mitigate this problem include fixing the VPN client software, or disabling IPv6 connectivity on all network interfaces when the previous option is not feasible.

9. Acknowledgements

The author would like to thank (in alphabetical order) Gert Doering and Tor Houghton, who providing comments on earlier versions of this document.

This documents has benefited from the input of Cameron Byrne, Gert Doering, Seth Hall, Tor Houghton, Alastair Johnson, Henrik Lund Kramshoj, and Jim Small, while discussing this topic on the ipv6hackers mailing-list [IPv6-Hackers]. It has also benefited from discussions with Andrew Yourtchenko on the opsec wg mailing-list [OPSEC-LIST].

10. References

10.1. Normative References

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

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, September 2012.

[RFC6555] Wing, D. and A. Yourtchenko, "Happy Eyeballs: Success with Dual-Stack Hosts", RFC 6555, April 2012.

10.2. Informative References

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, February 2011.

[I-D.ietf-v6ops-ra-guard-implementation] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", draft-ietf-v6ops-ra-guard-implementation-04 (work in progress), May 2012.

[I-D.gont-opsec-dhcpv6-shield] Gont, F., "DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers", draft-gont-opsec-dhcpv6-shield-00 (work in progress), May 2012.

[IPv6-Hackers] "IPv6 Hackers mailing-list", http://lists.si6networks.com/listinfo/ipv6hackers/.

[OPSEC-LIST] "OPSEC WG mailing-list", https://www.ietf.org/mailman/listinfo/opsec.

[SI6-Toolkit] "SI6 Networks' IPv6 toolkit",

<http://www.si6networks.com/tools/ipv6toolkit>.

[THC-IPv6] "The Hacker’s Choice IPv6 Attack Toolkit", <http://www.thc.org/thc-ipv6/>.

[RTADVD] "rtadvd(8) manual page", <http://www.freebsd.org/cgi/man.cgi?query=rtadvd&sektion=8>.

Author's Address

Fernando Gont
Huawei Technologies
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: http://www.si6networks.com