Eliminating Covert Channels in IPv6 with Network-Aware Active Wardens

Norka B. Lucena, Grzegorz Lewandowski, and Steve J. Chapin
Systems Assurance Institute
Department of Electrical Engineering and Computer Science
Syracuse University, Syracuse, NY 13244, USA
norka@ecs.syr.edu,grlewand@syr.edu,chapin@ecs.syr.edu

1. ABSTRACT

Although as of today publicly-accessible Internet addresses are primarily IPv4, the adoption of the Internet Protocol version 6 (IPv6) is imminent, as shown in Figure 1[1] [1]. For example, the U.S. government established that all federal agencies must deploy IPv6 by June 2008 and news from the IPv6 Task Force reports significant progress in the adoption of IPv6 technology in other continents, such as Asia and Europe. That global embracement of IPv6 calls for a closer examination of its security risks, especially of those which are not so obvious nor possibly to overcome by IPv4 security technologies.

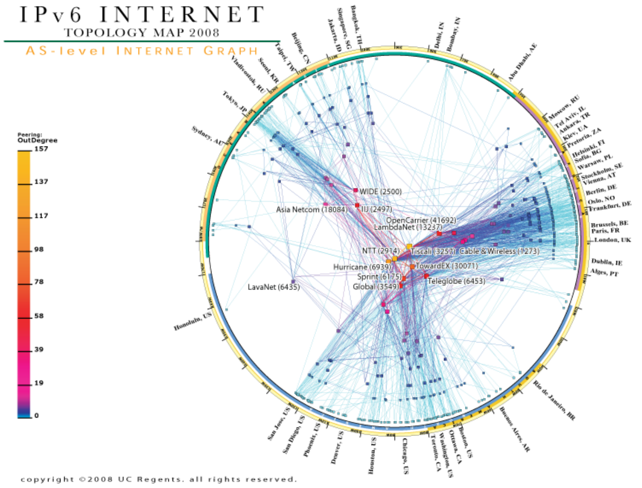

Figure 1: Snapshot of the IPv6 Topology at the Autonomous System Level as Observed in January 2008.

Network covert communication channels are one of those hidden security threats. A *covert* channel is a communication path that allows transferring information in a way that violates a system security policy. While covert channel-based attacks generally do not grant unauthorized access to a system, they can be used to maintain a stealthy, long-term control over an already-compromised host. Hence, covert channels offer the attacker an opportunity for greatly amplifying the damage inflicted on the victim system.

Recent research in IPv6 discovered that there exist, at least, 22 different covert channels, suggesting the use of advanced active wardens as an appropriate countermeasure [2]. The described covert channels are particularly harmful because of both: their potential to facilitate deployment of other attacks and the increasing adoption of the protocol without a parallel deployment of corrective technology. To defeat the identified channels, it defines three types of active wardens: *stateless*, *stateful*, and *network-aware*, which differ in complexity and ability to block some types of covert channels.

In particular, the *network-aware active* wardens are a sophisticated class of traffic normalizers that are able to record and recall previous packet behaviors and apply knowledge of the surrounding network topology to defeat the channels. In this study, we present a framework for the analysis of IPv6 covert channels that includes implementations of both the channels and the active-wardens [3], showing that indeed the latter are a viable mitigating tool against the former.

To prove that network-aware active wardens constitute an appropriate countermeasure against such threats, we evaluate their effectiveness within a controlled network environment, by estimating a percentage of elimination per case and by measuring the increase over the roundtrip time of end-to-end traffic flows. We demonstrate how to defeat all 22 of the reported channels, while causing roundtrip times increments no higher than 5%.

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]: Network Protocols—*Protocol Verification*

General Terms

Security

Keywords

Covert channels, IPv6, active wardens, passive wardens, traffic normalizers

2. REFERENCES

[1] CAIDA.org. Visualizing IPv6 AS-level Internet Topology 2008.

[2] Covert Channels in IPv6. In G. Danezis and D. Martin, editors, *PET 2005: Proceedings of the Privacy Enhancing Technologies*, volume 3856 of *Lecture Notes in Computer Science*, pages 147–166, Cavtat, Croatia, May 30-June 1, 2005. Springer.

[3] G. Lewandowski, N. B. Lucena, and S. J. Chapin. Analyzing Network-Aware Active Wardens in IPv6. In *IH 2006: Proceedings of the 8th Information Hiding worrkshop*, volume 4437 of *Lecture Notes in Computer Science*, pages 58–77, Old Town Alexandria, VA, USA, July 10-12, 2006. Springer.

[1] Permission to use, copy, modify and distribute any part of this "CAIDA IPv6 Internet Topology Map: AS-level Internet Graph" for educational, research and non-profit purposes, without fee, and without a written agreement is hereby granted, provided that the above copyright notice, and this paragraph appear in or near all copies.

SIGCOMM'08, August 17–22, 2008, Seattle, Washington, USA.
ACM 978-1-60558-175-0/08/08.