Analyzing Network-Aware Active Wardens in IPv6

Grzegorz Lewandowski, Norka B. Lucena, and Steve J. Chapin

Systems Assurance Institute
Syracuse University
Syracuse, NY 13244, USA
grlewand@syr.edu, {norka,chapin}@ecs.syr.edu

Abstract. A crucial security practice is the elimination of network covert channels. 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. The described covert channels are particularly harmful not only because of their potential to facilitate deployment of other attacks but also because of the increasing adoption of the protocol without a parallel deployment of corrective technology. We present a pioneer implementation of *network-aware* active wardens that eliminates the covert channels exploiting the *Routing Header* and the `hop limit` field as well as the well-known *Short TTL* Attack. Network-aware active wardens take advantage of network-topology information to detect and defeat covert protocol behavior. We show, by analyzing their performance over a controlled network environment, that the wardens eliminate a significant percentage of the covert channels and exploits with minimal impact over the end-to-end communications (approximately 3% increase in the packet roundtrip time).

Keywords: covert channels, evasion attacks, active wardens, stateless, stateful, network-aware, traffic analysis, traffic normalizers, active mappers.

1 Introduction

Although as of today publicly-accessible Internet addresses are primarily IPv4, the adoption of the Internet Protocol version 6 (IPv6)[1] is becoming imminent. For example, news from the IPv6 Task Force [1] report significant progress in both deployment and policy regarding networks using IPv6 technology in various continents [2,3]. IPv6 summits and other events present applications and services that will drive commercial implementations of IPv6 [4,5,6,7]. The U.S. government established that all federal agencies must deploy IPv6 by June 2008 [8], without disregarding the challenge of the Department of Defense (DoD) of monitoring operational IPv6 networks for unauthorized IPv6 traffic [9]. That global embracement of IPv6 calls for closer examination of its security risks, especially of those which are not so obvious nor possibly overcome by IPv4 security technologies.

Lucena, et al. [10] presents a comprehensive examination of covert channels in IPv6. It analyses 22 different network storage channels at the IP level, classifying them by

[1] IPv6 is also referred as the Next Generation Internet Protocol or IPng.

J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 58–77, 2007.

type of header. 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. A *stateless* active warden normalizes IPv6 traffic according to a protocol specification, without remembering anything about the packet that have already passed by. A *stateful* active warden records and recalls previous packet behaviors to discover a conceivably larger spectrum of hidden channels. A *network-aware* active warden is a stateful active warden with knowledge of network topology. The description of those active wardens is only conceptual. Until now, there has not been discussion of how one can implement network-aware wardens.

The IPv6 covert channels appear to be subtle types of aggression, when comparing to well-known buffer overflow attacks, for example. However, they are as harmful, especially under the presence of sophisticated adversaries[2]. It is feasible for an attacker to secretly transmit information into or out of a compromised machine residing on a secure network through the use of covert channels. For example, hacker Alice, after installing a key stroke logger and obtaining users' credentials, retrieves stolen information employing a covert channel. Alternatively, after installing a backdoor program, cracker Bob sends commands via a covert channel. Understanding that the use of IPv6 covert channels might be particularly damaging when an attacker utilizes them with the purpose of maintaining long-term control over a compromised machine, we present and evaluate an implementation of *network-aware* active wardens.

In this study, we consider two of the channels described in [10] and a well-known aggression in IPv4 [11,12,13,14]: the Routing Header covert channel, the Hop Limit channel, and the Short TTL Attack, respectively. The first two covert channels exemplify secret communication mechanisms of high and low bandwidth, respectively. The last one defines a relevant crossover point between the two versions of the IP protocol. The *Routing Header covert channel* takes advantage of the IPv6 source routing functionality to transfer data in a way that violates system security policies. The *Hop Limit channel* achieves a similar goal by manipulating the `hop limit` field of the IPv6 header. The *Short TTL* Attack allows an attacker to mask malicious communications or another attack from a Network Intrusion Detection System (NIDS). For a more detailed description of these attacks, please see Appendix A.

To prove that network-aware active wardens constitute an appropriate countermeasure against the selected IPv6 covert channels, we measure their effectiveness within a controlled network environment, by estimating a percentage of extermination per case and by measuring the increase over the roundtrip time of end-to-end traffic flows. We aim to defeat the selected channels, while causing roundtrip times increments no higher than 5%.

The remainder of this document is organized as follows. Section 2 compiles previous work on network covert channels in both IPv4 and IPv6, summarizing existing countermeasures. Section 3 specifies the design and implementation of the network-aware active wardens, presents results of performance tests set up on a controlled network, and discusses the implication of the obtained outcomes. Finally, Section 4 draws conclusions and suggests future directions of research related with the topic.

[2] The more secure nature of IPv6 in relation to IPv4 demands even more knowledgeable foes.