Network Forensics of Covert Channels in IPv6

Lourdes Gino D and Prof. Raymond A. Hansen
Department of Computer and Information Technology
Purdue University

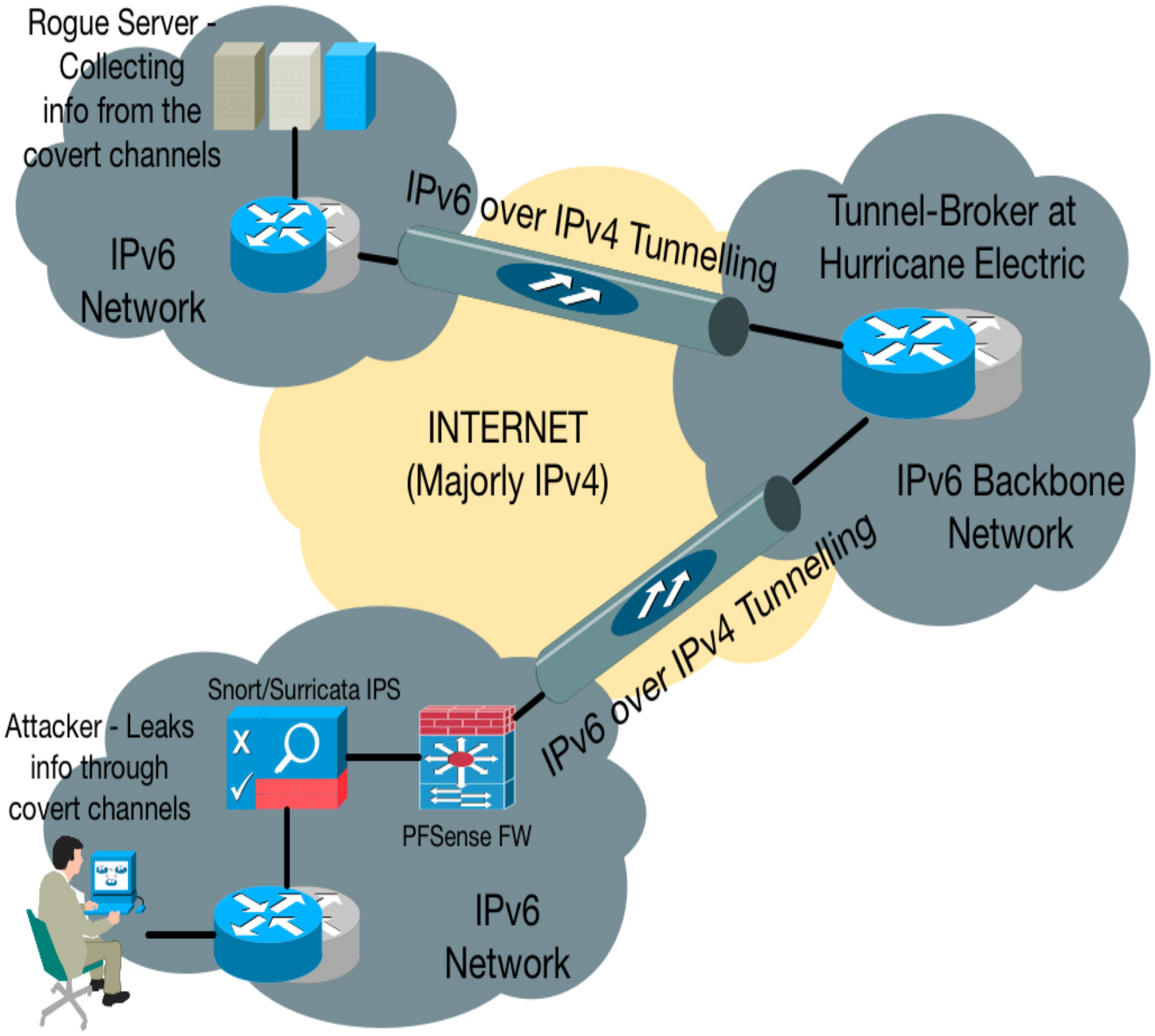
Abstract

“A covert channel is described as, any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy. Essentially, it is a method of communication that is not part of an actual computer system design, but can be used to transfer information to users or system processes that normally would not be allowed access to the information” (US DOD, 1985). Covert channels in IPv4 has been existing for a while and there has been various detection mechanisms. But the advent of IPv6 requires new research to identify covert channels and be able to perform forensics on such attacks. The current study aims at exploring the possibilities of performing forensics on such covert channels in IPv6.

Research Methodology:

Phase 1: In 2006, RP Murphy demonstrated a proof-of-concept of IPv6-based covert channeling tool called the v00d00N3t. Major changes to IPv6 has been done in the past 8 years. Hence Phase 1 involved verification of IPv6 covert channeling using the existing IPv6 and ICMPv6 standards. The above setup was implemented and the capability was **verified successfully**.

Phase 2: Even though migration of IPv4 to IPv6 has started widely, the capabilities of major IPS and Firewalls in detecting IPv6 based attacks are still a major concern. Hence Phase 2 deals with analyzing the capabilities of these devices, finding & recording the thresholds at which they detect these covert channels, analyzing the types of signatures required and recording the rate of false positives/negatives. **Currently in progress**.


Rogue Server - Collecting info from the covert channels
IPv6 Network
IPv6 over IPv4 Tunnelling
Tunnel-Broker at Hurricane Electric
INTERNET (Majorly IPv4)
IPv6 Backbone Network
IPv6 over IPv4 Tunnelling
Snort/Suricata IPS
Attacker - Leaks info through covert channels
PFSense FW
IPv6 Network

Phase 3: Involves the understanding of forensic-soundness of the data/logs/info captured. **Future work.**

Phase 4: Building a layered model for forensic analysis of such covert channels, with logs/packet captures/netflow data at the lower-layers and a more-defined intelligence model at the upper-layers. **Future work.**

Phase 5: Build an algorithm/signature to detect the covert channels with a better error rates. **Future Work.**

References:

1. U. S. Department Of Defense, 1985. Trusted Computer System Evaluation Criteria.
2. https://www.defcon.org/images/defcon-14/dc-14-presentations/DC-14-Murphy.pdf
3. “Covert Channels in IPv6” Norka B. Lucena, Grzegorz Lewandowski, Steve J. Chapin. Springer, 2006.