**Router Packet Tampering**

**Description 1**

Through combinations of social engineering and ineffective passwords, attackers have gained control over thousands of Internet routers. Once a router has been compromised in such a fashion, **an attacker may interpose on the traffic stream and manipulate it maliciously to attack others by selectively dropping, modifying, or rerouting packets, and consequently cause router packet tampering.**

Router Packet Tampering is the problem that a compromised router is maliciously manipulating its stream of packets. In particular, people are concerned with a simple yet effective attack in which **a router selectively drops packets destined for some victim**. Unfortunately, it is quite challenging to attribute a missing packet to a malicious action because normal network congestion can produce the same effect. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities.

Previous detection protocols have tried to address router packet tampering problem with a user-defined threshold: too many dropped packets imply malicious intent. However, this heuristic is fundamentally unsound; setting this threshold is, at best, an art and will certainly create unnecessary false positives or mask highly focused attacks. Engineers have designed, developed, and implemented a compromised router detection protocol that dynamically infers, based on measured traffic rates and buffer sizes, the number of congestive packet losses that will occur. Once the ambiguity from congestion is removed, subsequent packet losses can be attributed to malicious actions. Engineers have tested effective protocol and have studied its effectiveness in differentiating attacks from legitimate network behavior. [1] [2]

[1] Mizrak, Alper T., Stefan Savage, and Keith Marzullo. "Detecting malicious packet losses." *IEEE Transactions on Parallel and distributed systems* 20.2 (2009): 191-206.

[2] X. Ao, Report on DIMACS Workshop on Large-Scale Internet Attacks, http://dimacs.rutgers.edu/Workshops/Attacks/internet-attack- 9-03.pdf, Sept. 2003.

[3] R. Thomas, ISP Security BOF, NANOG 28, http://www.nanog. org/mtg-0306/pdf/thomas.pdf, June 2003