Here is our submission to RAID '99 of a paper, *"Defending Against Network IDS Evasion"*. It looks like the most appropriate topic category is "Innovative Approaches". The likely speaker will be:

Vern Paxson
ACIRI / ICSI and Lawrence Berkeley National Laboratory
1947 Center Street
Suite 600
Berkeley, CA 94704-1198

510-642-4274 x302
510-643-7684 (FAX)

vern@aciri.org

Vern Paxson received his M.S. and Ph.D. degrees from the University of California, Berkeley. He is a Senior Scientist at the AT&T Center for Internet Research at the International Computer Science Institute, and also a Staff Scientist at the Lawrence Berkeley National Laboratory. His research focuses on network intrusion detection and Internet measurement. He is one of the Transport Area Directors for the IETF and co-chairs the IETF's working group on TCP implementation.

Mark Handley received his BSc and PhD from University College London. For his PhD he studied multicast-based multimedia conferencing systems, and was technical director of the European Union funded MICE and MERCI multimedia conferencing projects. After two years working for the University of Southern California's Information Sciences Institute, he joined the AT&T Center for Internet Research at ICSI as a Senior Scientist. Most of his work is in the areas of scalable multimedia conferencing systems, reliable multicast protocols, multicast routing and address allocation, and network simulation and visualisation. He is co-chair of the IETF Multiparty Multimedia Session Control working group and the IRTF Reliable Multicast Research Group.

Defending Against Network IDS Evasion

Vern Paxson & Mark Handley
ACIRI / ICSI
vern@aciri.org, mjh@aciri.org

When attempting to build sound network intrusion detection systems, a major problem is hardening the monitor against "evasion": attempts by attackers to mislead the monitor as to the actual state of the end-to-end dialog between the attacker and its victim [Ptacek and Newsham 98, Paxson 98]. Evasion techniques include sending traffic that is ambiguous from the monitor's observational vantage point (such as whether a given packet has sufficient TTL to reach the victim) and attempting to overwhelm the monitor by clogging it with more connection state records than it can sustain ("state holding" attacks).

One technique for preventing certain forms of evasion attacks is "bifurcating analysis", in which the monitor deals with ambiguous traffic streams by instantiating separate analysis threads for each possible interpretation of the ambiguous traffic. We discuss the applicability of this approach to different forms of evasion, with the key distinction being tractable analysis for cases where the number of analysis threads can be bounded, versus problematic analysis for cases where the attacker can cause the number of threads to grow arbitrarily large.

Another technique for resisting evasion is to introduce a "traffic normalizer": a network forwarding element (i.e., a "bump in the wire") that attempts to eliminate ambiguous network traffic and reduce the amount of connection state that the monitor must maintain. Unlike a firewall, the primary function of a normalizer is to aid the IDS monitor rather than to selectively filter traffic, but if desired the functionality could be combined with a firewall into a single element.

We discuss a number of architectural considerations associated with designing a traffic normalizer. These include the degree to which the normalizer preserves end-to-end semantics; performance implications of the transformations performed by the normalizer; communication between the normalizer and the monitor; using the normalizer to offload processing from the monitor; attacks on the normalizer; and tradeoffs between maintaining critical state in the normalizer, versus the normalizer being able to reconstruct such state dynamically. We illustrate the issues by analyzing how a normalizer could prevent evasion attacks such as ambiguous TCP stream contents, manipulation of TCP connection state, and flooding the monitor with bogus state.