

PROJECT PROFILE

Automatic Intrusion Tracing and Response

Rapid response to intrusions has become a major requirement in defending critical systems. Because an adversary can take actions at computer speeds, network security systems of the future will need the capability to react without human intervention. NAI Labs, Boeing Phantom Works, and U.C. Davis, under a series of DARPA contracts, have developed a technology that supports automatically tracing attempted intrusions across network boundaries and blocking or otherwise responding to them near their sources. This technology will enable networks of networks to cooperatively detect system attacks, exchange information about attack behavior, and respond to attacks by dynamically reconfiguring routers, firewalls, and hosts to heighten their defensive posture and provide additional protection against subsequent attacks.

The heart of this technology is a new protocol, the Intruder Detection and Isolation Protocol (IDIP), which enables cooperation among such components. The IDIP team has developed an IDIP-based library of software infrastructure elements that can be easily integrated with detection and response components, thereby facilitating experimentation with automated response strategies. Components that have been successfully integrated with IDIP include boundary controllers such as NAI's Gauntlet Internet Firewall, a Linux-based router, and SCC's Sidewinder Firewall; intrusion detection systems such as NAI's Cybercop Monitor, ISS' RealSecure, NetSquared's Network Radar, and SRI's Emerald; and host security mechanisms including custom extensions to operating system kernels ("security wrappers"). Both COTS products and research prototypes have been used for demonstrations and experiments. Working together in internetworked systems, IDIP-enabled components can locate, isolate, and block an intruder close to the point of attack and provide diagnostic information so that network administrators can further investigate the intrusion.

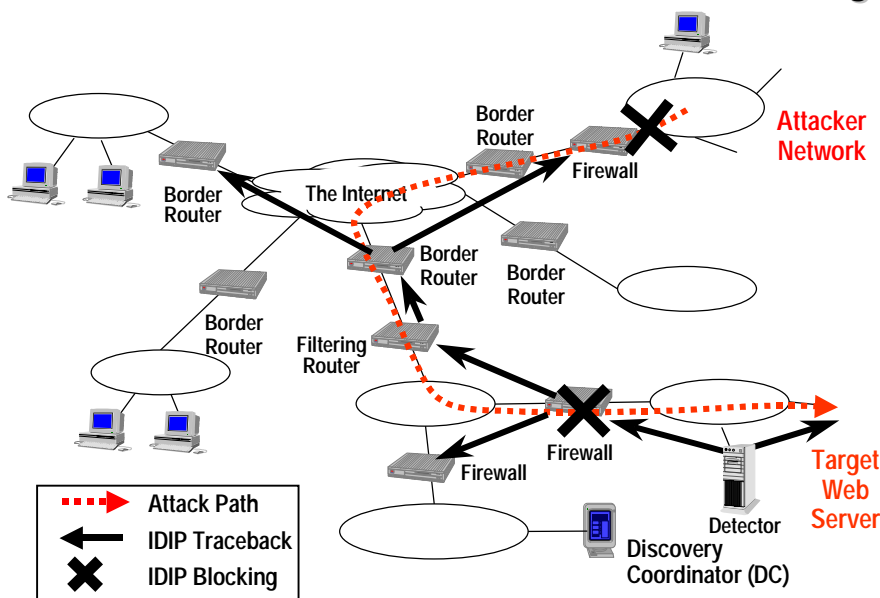
Research Focus

Disguised Attacks

Most internet attackers disguise their location by attacking their targets *indirectly* through other previously-compromised intermediary systems or by using spoofed source addresses. These techniques makes it virtually impossible for a victim organization operating alone to determine the true source of such attacks, stop them quickly, or deter them in the future. Addressing these problems will require a new level of cooperation among internet citizens, network equipment vendors, and internet service providers. IDIP technology, which encompasses an architecture, a secure network libraries, provides the technical means for these organizations to cooperate in *automatically* tracing and blocking attacks that cross network boundaries.

- Dan Sterne, Manager,
Adaptive Network
Defense Group

Automated Attack Traceback and Blocking



Efforts to enhance and further validate this technology are currently focusing on:

- expanding IDIP so that automated traceback and responses can span multiple administrative domains and support correlation of intrusion indications and warnings across domains;
- using mobile code techniques, developed by DARPA's *Active Networks Program*, to allow IDIP-enabled detectors and response components to migrate throughout a network, and
- evaluating the effectiveness of IDIP-enabled components in tracing and responding to distributed denial of service attacks.

For More Information

For more information about this research, contact Kelly Djahandari (kelly_djahandari@nai.com) or Dan Sterne (dan_sterne@nai.com) at 443-259-2300 or visit our Web page at: <http://www.pgp.com/research/nailabs/adaptive-networks.asp>.

1/5/01



Who's watching your network

For more information on NAI Labs, contact your authorized NAI Sales Representative, or visit <http://www.nailabs.com>.

CORPORATE Headquarters

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (800) 764-3337*
Fax (888) 203-9258

*Call for additional Worldwide Sales Offices