

# Active Networks Intrusion Detection and Response (AN-IDR)

Intrusion detection and response with greater adaptability, mobility, power, and effectiveness

## Overview

The Network Associates Laboratories Active Networks Intrusion Detection and Response (AN-IDR) project seeks to develop intrusion detection and response (IDR) mechanisms having greater adaptability, mobility, power, and effectiveness by exploiting the technology produced by the Defense Advanced Research Projects Agency (DARPA) Active Networks program. Active network technology provides a highly flexible infrastructure that allows network users to reprogram and customize routers, firewalls, switches, and other components to provide new network services on the fly. AN-IDR is part of the DARPA Active Networks program, serving as a challenge problem to derive requirements and determine to what extent Active Networks technology meets those requirements.

This project has developed evolving active-network-based prototypes providing intrusion detection, tracing, response, and defense that are self-deploying, i.e., autonomous and migrating; and adaptive to location, and topology.

## Research Approach

The effectiveness of conventional IDR mechanisms is limited for several reasons. These mechanisms cannot detect all attacks because new attacks are continuously being created. They cannot be deployed everywhere and kept fully enabled because of performance costs. It is difficult to keep them properly configured at all times because the network and threat environment continually evolves. Furthermore, the evolution of attacks toward coordinated actions against networks of hosts over long periods of time may require detection and response services that can themselves migrate through the network in reaction to evidence of such an attack.

The AN-IDR project team consists of Network Associates Laboratories and Boeing Phantom Works. Both organizations have several years of joint experience developing the Intruder Detection and Isolation Protocol (IDIP) and associated software under DARPA funding. IDIP provides cooperation among intrusion detection systems, firewalls, routers, network management components, and hosts so that intrusions that cross multiple network boundaries can be automatically traced and blocked as close to their sources as possible. The AN-IDR project has built new IDR functions that run on active network technology, using IDIP as a source for IDR concepts and functionality.

The project team defined IDR usage scenarios and has used Active Network Technology to deploy new and adaptive IDR functions.

From these IDR scenarios, twenty-seven specific functional requirements for active network infrastructure components were derived. The team built prototypes to demonstrate how Active Networks enhance IDR and to test the underlying Active Networks Execution Environments (EE).

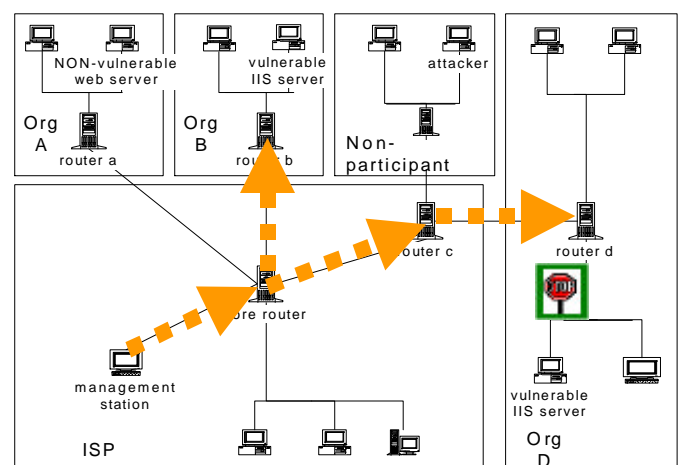
## Mobile DDoS Defense Prototype

Our initial prototype illustrates the potential value active network technology can provide in the intrusion detection and response problem domain. This prototype demonstrates the capability to automatically detect and respond quickly and effectively to distributed denial-of-service (DDoS) attacks launched by a hacker using the Stacheldraht toolkit.

This prototype uses the Secure ANTS (SANTS) EE, which provides the ability to securely execute mobile code. Mobile code and its parameters are protected with cryptography, ensuring confidentiality, that only trusted individuals can execute software, and additional security features. SANTS is implemented in Java and requires that mobile programs be written in Java.

The automated response is implemented as mobile code that installs itself on the router nearest the attack's target, a streaming video server, and migrates to upstream routers along all attack paths between the target and packet flooding sources. The mobile code invokes a conventional rate limiter algorithm that allows suspicious traffic, containing a mix of legitimate and bogus flood packets, through routers at a controlled rate; it discards excessive packets that would otherwise overwhelm the streaming video

## AN-IDR Management Station Deploying Mobile Code Scanners to Edge Routers



# Active Networks Intrusion Detection and Response (AN-IDR)

Intrusion detection and response with greater adaptability, mobility, power, and effectiveness

server's network. The result is that the server is able to resume providing usable video service for the legitimate packets that pass through the rate limiter. The effectiveness of the rate limiter program increases successively as it migrates closer to the flooding sources.

## Mobile Intrusion Blocking Prototype

Subsequent prototypes illustrate the potential value of active network technology for preventing different types of intrusion attacks. By preventing intrusions in the first place, system owners could be spared from having their sensitive data exposed or destroyed and having their systems rendered inoperative or used to attack others. The Internet on the whole could benefit by having fewer compromised systems that could be used as launching points for penetration or denial-of-service attacks.

A proactive Internet Service Provider (ISP) or Managed Service Provider (MSP) could provide non-intrusive defense for customers by deploying intrusion blockers on the routers connected to customer networks. The first mobile intrusion blocker implementation uses SANTS. We assume the ISP or MSP has service agreements with its customers allowing vulnerability scanning and intrusion blocking to run on routers that reside on customer premises. When a new vulnerability is discovered or an outbreak occurs, an ISP or MSP administrator performs a vulnerability scan to determine which systems are vulnerable.

The scanner is a mobile program that moves to routers on the edge of the network. At the edge, the scanner determines which customer systems are

vulnerable and sends the results back to the administrator. By running at the edge of the network, it can run more efficiently, by leveraging the aggregate computing power of multiple edge nodes.

The administrator then sends an intrusion blocker directly to the routers connected to vulnerable customer systems. The blocker looks for traffic that matches the attack signature directed at the vulnerable systems—by executing the blocker only on routers where it is necessary and only to prevent specific threats to known vulnerable systems, the overall performance impact is reduced. When an attack is attempted, the blocker drops the offending traffic and no longer allows communication on that connection. This focus allows the blocker to be lightweight, while still allowing valid traffic. Versions of the blocker have been implemented to defend against the widely publicized and ongoing Code Red, a Domain Name System (DNS) hijacking attack, and the Ramen Linux worm.

The second intrusion blocker implementation uses the Active Signal Protocol (ASP) Execution Environment, a Java-based EE, also part of the Active Networks program. ASP was chosen because it offers more control over low-level network functions. The new blocker implementation uses adaptive migration—a technique to migrate the blocker based on dynamic network conditions—and also operates on the high-end Intel IXP 1200 network processor. The IXP represents next-generation high-speed network processing systems that could be used for programmable routers.

The second blocker adaptively migrates, based on resource constraints. It can

determine when the router where it is executing is under greater network or processing load. Under greater loads, it might not be able to monitor for potentially malicious traffic and still forward unmonitored traffic. When the blocker identifies a potential overload condition, it attempts to migrate to more powerful neighboring routers, such as an IXP 1200. Another example of adaptive migration would allow protection of a network whose router's security policy does not allow the blocker. When a blocker fails to migrate to such a router, it could run on neighboring routers instead.

The AN-IDR project is concluding by measuring the performance of the Mobile Intrusion Blocker on the ASP platform. This performance testing is intended to determine if the ASP EE is a viable platform and whether the intrusion blocker can perform sufficiently for real world deployment.

AN-IDR has used existing Active Networks technology to develop adaptive security software. The team has developed prototypes that defend against real attacks, such as the Stacheldraht DDoS attack and the Code Red worm. AN-IDR technology allows the development of innovative defenses of unforeseen attacks, to address the threats coming over the horizon.

## Additional Information

For additional information contact Dan Sterne (dan\_sterne@nai.com) at (301) 527-9500 or visit our Web page at: [www.networkassociates.com/labs](http://www.networkassociates.com/labs).