IP Navigator security audit

Michael C. Richardson
Sandelman Software Works Inc.
mcr@sandelman.ottawa.on.ca

March 8, 1997

1 Executive Summary

This document describes a proposal from Sandelman Software Works to Ascend Communications to do a security audit of Ascend's IP Navigator ATM switch. This document outlines the project's scope, provides a proposed list of deliverables and a cost estimate. Three phases are described: project definition, tool/test case development, and product testing.

2 Background

Prior to the IP Navigator feature being added to Ascend carrier class and WAN switches, there was no interaction between the data flowing through the switch, and its management functions. The ATM switch, being unaware of the Internet Protocol (IP) datagrams that were passing through it, could not provide efficient routing of the data. The introduction of IP to the ATM switch provides many benefits, but exposes the switch to the possibility of attacks from the users of the network.

Many defenses against attacks have been implemented, but only a limited confidence may be put in the defenses until they have been tested and audited by a third party. This project is about doing that audit.

Quality of service is a high profile feature of the switch. It is critical that quality of service guarantees are not broken during an attack by a malicious party. It is important to test the performance of the defenses as well as their effectiveness.

3 Project definition (phase I)

This phase is a short phase that is used to properly define and scope the other two phases. Phase II and phase III are optional: should Ascend Communications be unsatisfied with the results, phase II and III would be cancelled at no penalty.

3.0.1 Deliverables

- detailed project plan
- labour cost estimate
- hardware needed

3.0.2 Receivables

- access to architectural personel at Ascend
- access to testing personel at Ascend
- description and inventory of testing facilities

3.0.3 Costs

The project definition phase will take four days at a rate of $1000 (US) per day.

4 Security tool/test case development (Phase II)

This section will list the test cases that will be created. As the details of this section depends on a better understanding of the internal components in the IP Navigator, this section is currently short. This section will be refined during phase I of this project.

A white box testing methodology will be used.

In general, three layers of testing will be done: IP layer, TCP or UDP layer and application (FTP, TFTP, Telnet, SNMP, HTTP, etc as applicable).

4.1 IP layer testing

- IP source address (ingress) filtering: to verify the ability source address spoofing if appropriate
- source routed packets: can this be disabled, if so, does it work.
- directed broadcasts: can this be disabled, if so, does it work.
- fragment tests: ping of death, landmine, fragment expiry

4.2 Transport layer testing

- TCP: SYN scanning
- TCP: SYN spoofing defenses
- TCP: teardrop-type attacks
- UDP: payload trojans: do stats/bandwidth guarantees account for entire packet?
- UDP: port scan
- UDP: chargen spamming
- ICMP: ICMP redirects: can they be disabled, does it work.

4.3 Application layer

- BGP and other routing protocols: can bogus routes be introduced? Can unauthenticated machines cause route flapping with ICMP host unreachables?
- Telnet: are there any buffer overflows in the admin interface?
- SNMP: default public strings? What can be read? What SETs are possible? Are there buffer overflows problems?

- TFTP for boot images: how to force new firmware? Buffer overflows.
- Other admin interfaces: HTTP, etc. — overflows, access to inappropriate data.
- RSVP: does the authentication work correctly?

4.4 Deliverables

- report on each test
- description of test initiator hosts
- source code for all test cases

4.5 Receivables

- 2 Ascend IP Navigators, with ATM fiber loopback. Machines need to have ethernet ports rather than V.35/HDLC interfaces.
- documentation and setup instructions for IP Navigators
- access to IP Navigator support personnel

4.6 Costs

All work in this phase will occur on the premises of Sandelman Software Works, in Ottawa, Ontario.

Four days for setup and initial configuration of equipment.

One day for each test that is agreed to. (17 are listed above)

Five days to the final report.

Total is 27 days of effort @$800US/day, for a total cost of $21600US.

Should any defects in the IP Navigator be found, other testing will continue (if possible). Once a fix has been received, the test vector will be repeated as well as other tests in that category, at a cost of 0.5 days.

5 Automation of security tests (Phase III)

It is not useful for a defence against an attack to cause a switch to stop, or slow, its movement of data. Any slowdown provides avenues for denial of service attacks.

This phase of the project would involve automating a subset of the tests, and introducing the test vectors into the performance testing that Ascend already does on its products.

It is estimated that only IP and some transport layer tests will be appropriate for automated testing. The exact number will be decided during project definition (phase I).

It is estimated that five days will be required to translate the host (Unix based) tests to a form appropriate for the high speed/high load testing environment. Information about the testing environment received during phaseI may allow this conversion time to be reduced.

It is suggested that two, three day sessions with Ascend testing personel, at an Ascend location be planned. The first session will attempt to make all tests function within the Ascend testing environment, while the second session will a full testing session. An interval between the two sessions would allow both parties to fix any problems that are discovered during the first session.

5.1 Deliverables

Documented test vectors.

5.2 Receiveables

Access to testing lab, and testing personnel.

5.3 Costs

Five days in Ottawa, @$800US/day and six days in Boston at @$1000US/day, for a total of $10000.

6 Summary of costs

Phase I:	\$4000.
Phase II:	\$21600.
Phase III:	\$10000.
Total	\$35600