General Project Description

Project title:	MSR IPv6 verification
Project kind:	Industrial project
Contractor:	Nickolay Pakoulin (ISP RAS)
Customer:	Microsoft Research Cambridge
Project start date:	December 1, 2000 г.
Project end date:	November 30, 2001 г.

Goals of the project

The goals of the project were: (1) to test conformance and robustness MSR IPv6 implementation; (2) to demonstrate applicability of formal methods to specification and verification of complex API such as an IPv6 implementation; (3) to demonstrate feasibility of the approach to verification of Windows NT internals.

Project Input

The implementation under test is MSR IPv6 -- an implementation of IPv6 for Windows NT developed by Microsoft Research. MSR IPv6 is distributed in sources. For more details about MSR IPv6 please visit the MSR web site, http://research.microsoft.com/msripv6

We tested how implementation of certain features of IPv6 in MSR IPv6 conforms to protocol specifications.

Size of the tested subsystem is about 9,000 lines (without comments and empty lines).

Requirements were elicited from IPv6 and service protocols specifications (domain standards). Domain standards are presented in the form of IETF Requests for Comments – RFC. We elicited requirements from 10 RFCs: RFC 2460, RFC 2461, RFC 2462, RFC 2463, RFC 2464, RFC 3513, RFC 2373, RFC 2292, RFC 2553, RFC 2675. Total size is about 900 pages, plain text. About 300 functional requirements were elicited.

Process Used

Method: CTesK super-lite toolkit. The project features that distinguish it from other UniTesK applications are presence of non-procedural stimuli in IUT interface and deferred reactions[1].

Development: Development was done on Windows 2000 using CTesK super-lite and Microsoft Visual Studio 6.0.

Test harness and tools: A specialized tool named Remote Mediator was developed for applying non-procedural stimuli (i.e. IPv6 packets) to the IUT. Most components of the test harness operate on the IPv6 node where IUT runs. Still some components operate on other nodes attached to the same link with IUT. We developed a tool to launch/ stop/ control remote components of the test harness. The tool was named Test Manager.

Project Effort:

Project duration: 1 year

Effort estimate: about 3 men-years

1Deferred reaction is a reaction that is demonstrated after a time delay since a stimulus was applied

Project Results

Tested subsystems size is about 9,000 lines. Test suite component sizes:

Test Suite Component	Size, in lines of code
Specification	8500
Test Scenarios	2500
Mediators	6000

Total number of test scenarios: 15.

Testing revealed 4 defects, and 2 are very severe ones. Most significant defect makes remote DoS attacks possible: upon receiving a certain sequence of IPv6 packets the Windows 2000 kernel crashes.

The project has achieved its goals. A test suite for IPv6 conformance testing was developed. The test suite covers basic features of IPv6 and main service protocols. The test suite was run on the IUT and revealed both inconsistencies with domain standards and critical programming errors.

The project demonstrated that UniTesK is well suited for conformance testing of telecommunication protocols and reactive systems. The project also showed that UniTesK is feasible for testing software modules residing in the kernel of an operating system.