Общее описание проекта

Название проекта:	Верификация MSR IPv6
Тип проекта:	Промышленный проект
Исполнитель:	Пакулин Николай (ИСП РАН)
Заказчик:	Microsoft Research Cambridge
Дата начала проекта:	1 декабря 2000 г.
Дата окончания проекта:	30 ноября 2001 г.

Цели проекта

Проект преследовал несколько целей: (1) провести тестирование корректности реализации функций протокола IPv6 и надежности реализации IPv6 от Microsoft Research (MSR IPv6); (2) продемонстрировать применимость формальных методов к специфицированию и тестированию сложных программных интерфейсов, таких как реализация протокола IPv6; (3) продемонстрировать применимость указанного подхода к верификации внутренних подсистем Windows NT.

Входные данные проекта

Целевая система – реализация протокола IPv6 для Windows NT от Microsoft Research, MSR IPv6. Распространяется в исходных текстах. Более подробную информацию о MSR IPv6 можно получить с сайта Microsoft Research: http://research.microsoft.com/msripv6

Тестировали соответствие реализации ряда функций протокола IPv6 и служебных протоколов спецификациям протокола.

Оценка размера подсистем, подвергнутых тестированию – 9,000 строк на C (без пустых строк и комментариев).

Требования к тестируемой реализации извлекались из спецификаций протокола IPv6 и служебных протоколов (стандарты предметной области). Для прояснения неясностей мы также использовали: исходный код системы (часто), форумы/конференции, посвященные IPv6 (реже), и общение с разработчиками реализации (очень редко).

Требования извлекались из RFC. Всего использовались 10 RFC: RFC 2460, RFC 2461, RFC 2462, RFC 2463, RFC 2464, RFC 3513, RFC 2373, RFC 2292, RFC 2553, RFC 2675. Суммарный объём документов около 900 страниц, плоский текст. Выделено около 300 функциональных требований.

Используемый процесс

Метод: Использовался CTesK super-lite. Особенность данного проекта от прочих проектов с использованием UniTesK – наличие непроцедурных стимулов и отложенных реакций в целевой системе и спецификациях.

Разработка: Разработка велась на Windows 2000, для сборки использовали MS Visual Studio 6.0. Для тестирования был разработан инструмент для подачи непроцедурных стимулов, который получил название Remote Mediator.

Тестовый стенд и инструменты: Использовалась распределенная схема пространственного расположения компонентов тестового набора. Основная часть тестовой системы работала на той же машине, что и реализация, но часть компонентов располагалась на машинах, подключенных к локальной сети.

Был разработан инструмент для запуска удаленных компонентов тестового набора, получивший название TestManager.

Трудоемкость проекта:

длительность проекта: 1 год

затраченное число человеко-дней: порядка 3-х человеко-лет

Результаты проекта

Размер протестированного кода порядка 9,000 строк. Размеры компонентов тестового набора:

Название компонента	Размер, в строках
спецификации	8500
Тестовые сценарии	2500
медиаторы	6000

Общее число тестовых сценариев 15.

Всего было обнаружено четыре ошибки, из них две фатальные, которые приводят к перезагрузке операционной системы. Наиболее существенная ошибка позволяет строить удаленные DoS атаки: при получении определенной последовательности пакетов операционная система перегружается.

Проект достиг поставленных целей. Был разработан тестовый набор для тестирования соответствия реализации функций протокола IPv6 стандартам протокола. Разработанный тестовый набор покрывает большое число базовых функций протокола IPv6 и основных служебных протоколов. Тестовый набор был пропущен на целевой реализации и были обнаружены несоответствия и критические ошибки в реализации.

Кроме того, данный проект наглядно продемонстрировал, что UniTesK можно с успехом применять к тестированию реализаций протоколов и реактивных систем, а также к тестированию программных модулей, располагающихся в ядре операционной системы.