LVEE 2010

«ПРИМЕНЕНИЕ OPEN-SOURCE ИНСТРУМЕНТОВ ДЛЯ РАЗРАБОТКИ СИСТЕМЫ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ АНТИВИРУСНОГО ЯДРА.»

Ведущий разработчик и инженер-испытатель компании «ВирусБлокАда»
Романов Алексей Владимирович

Точка приложения

AB-ядро – программная библиотека, предназначенная для поиска вредоносных программ в объектах различных типов. Основные типы проверяемых объектов:

- Исполняемые файлы(PE, NE, ELF, EXE, COM)
- Документы в формате OLE, RTF, XML(.doc, .xls, .ppt)
- Архивы(RAR, ZIP, 7Z, ARJ, TAR, GZ, BZ2)
- Почтовые сообщения(MIME, plain text)
- Почтовые базы(DBX, MBX, TBB, PST)

Поддерживаемые платформы:

- Windows 98
- Windows NT 4.X, 5.X, 6.X
- Linux с ядрами 2.6.X и библиотекой glibc 2.3 и выше
- FreeBSD 5.X, 6.X, 7.X

Обоснование необходимости создания системы

- Антивирусное ядро(далее АВ-ядро) - крупный проект с широкими функциями
- АВ-ядро является динамично развивающимся проектом
- Качество ядра должно быть очень высоким, так как это основной компонент почти всех продуктов компании ВирусБлокАда
- Большое количество поддерживаемых программных платформ
- Недостаточное количество человеческих ресурсов для проведения ручных тестов
- Высокая стоимость ручного тестирования

Методика тестирования AB-ядра

- Функциональные тесты ядра
- Тестирование на стабильность
- Тестирование на утечки ресурсов ОС
- Тестирование на скорость работы
- Тестирование на ложные срабатывания
- Статический анализ исходного текста ядра

Ступени развития инструметов тестировани АВ-ядра

Ступени развития организации данных для тестирования АВ-ядра

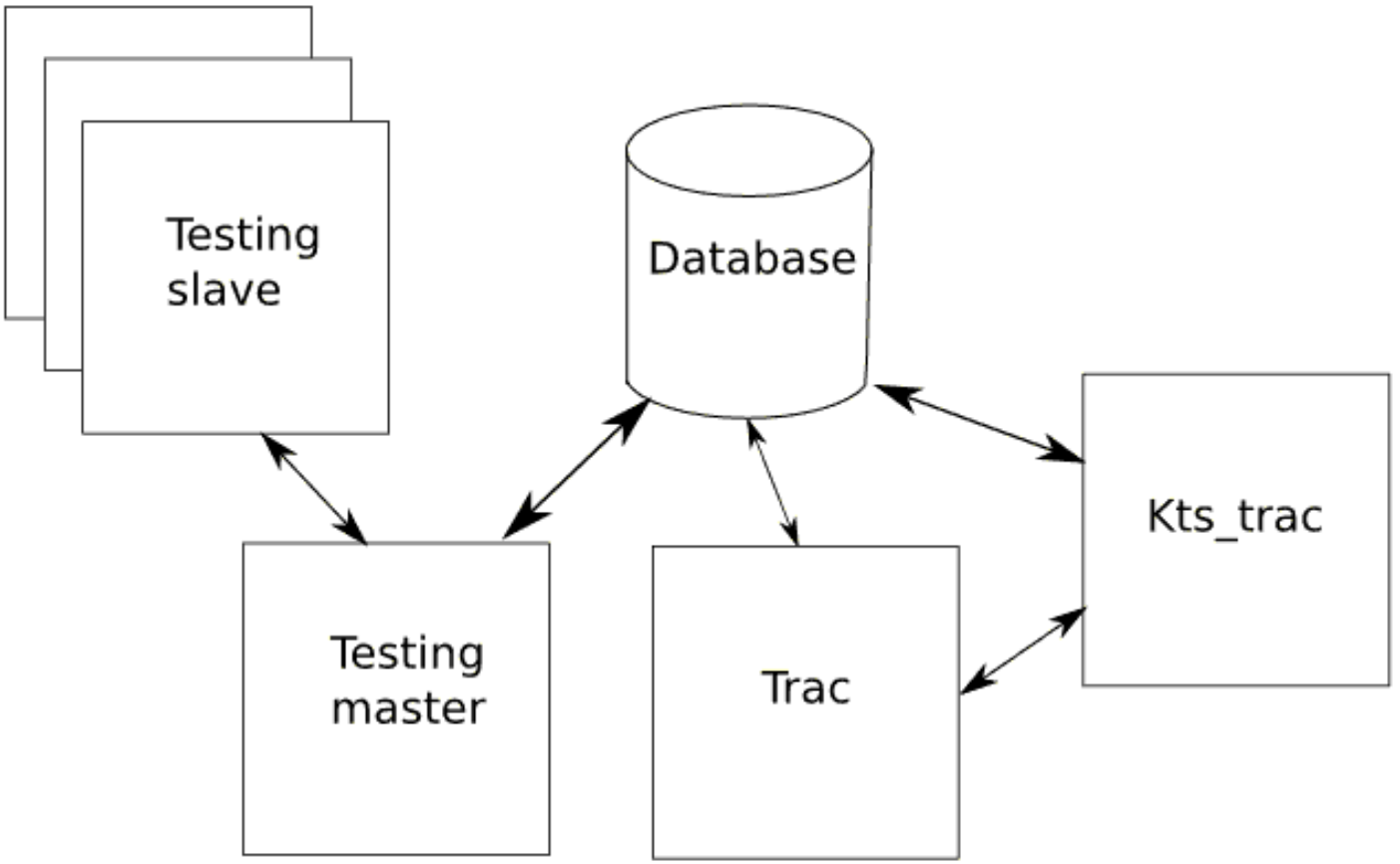
Требования к разрабатываемой системе

- Интеграция всех имеющихся тестов AB-ядра в систему
- Удобство представления результатов тестирования
- Доступность результатов тестирования
- Механизм уведомления о результатах тестов
- Прозрачность архитектуры и реализации
- Механизмы интроспекции
- ...

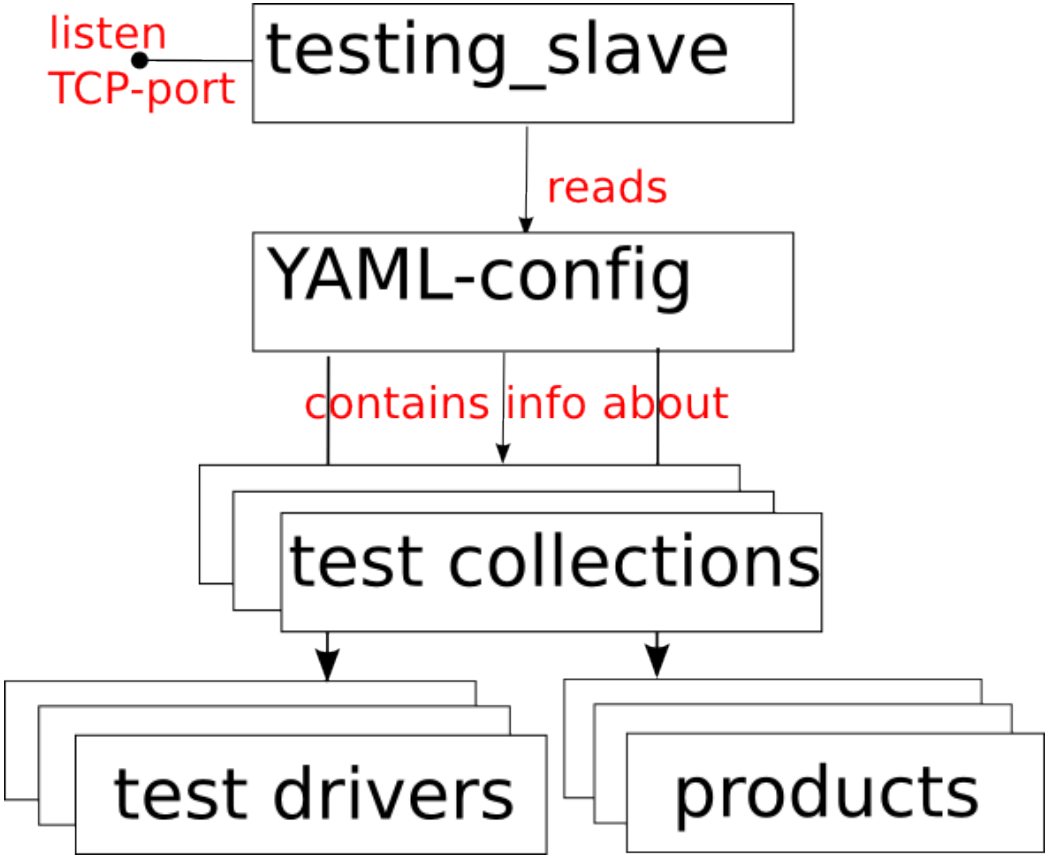
Выбор инструментов разработки

- Основной язык разработки - Python
- Инструмент поиска ошибок времени выполнения - Valgrind
- Фреймворк для создания асинхронных сетевых приложений - Twisted
- Инструмент для проектирования и разработки реляционной БД - SQLObject
- Библиотека для построения графиков - matplotlib

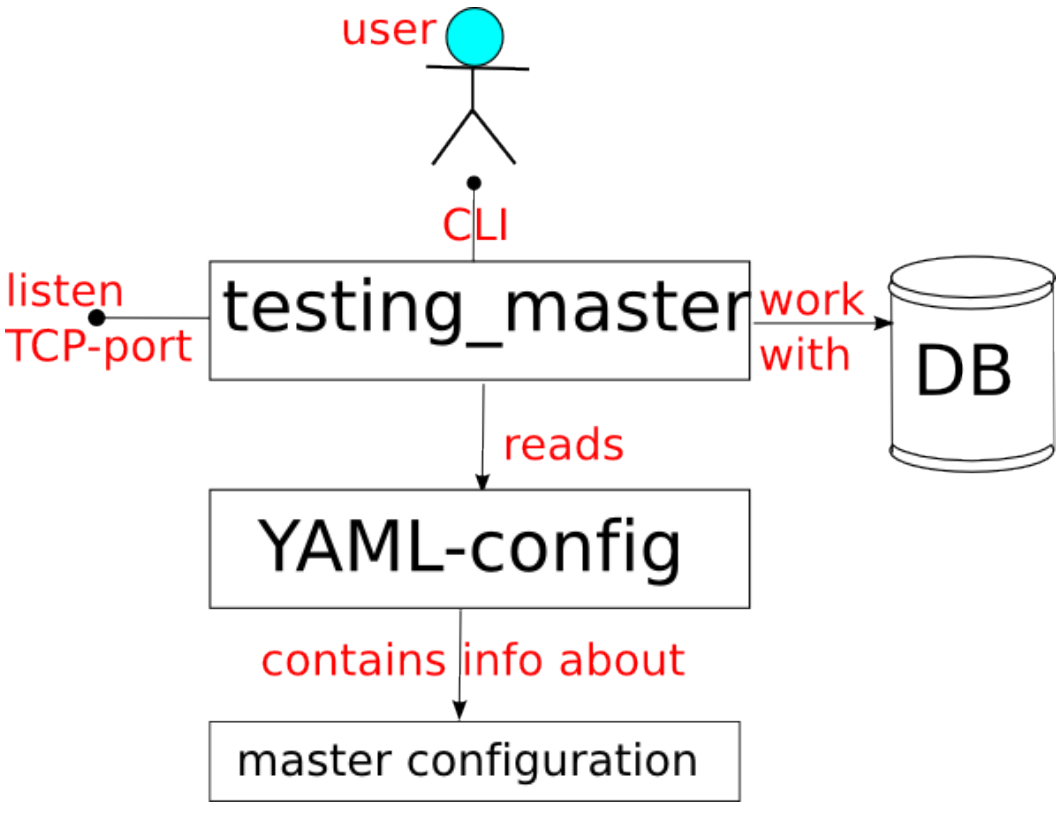
Общая архитектура системы



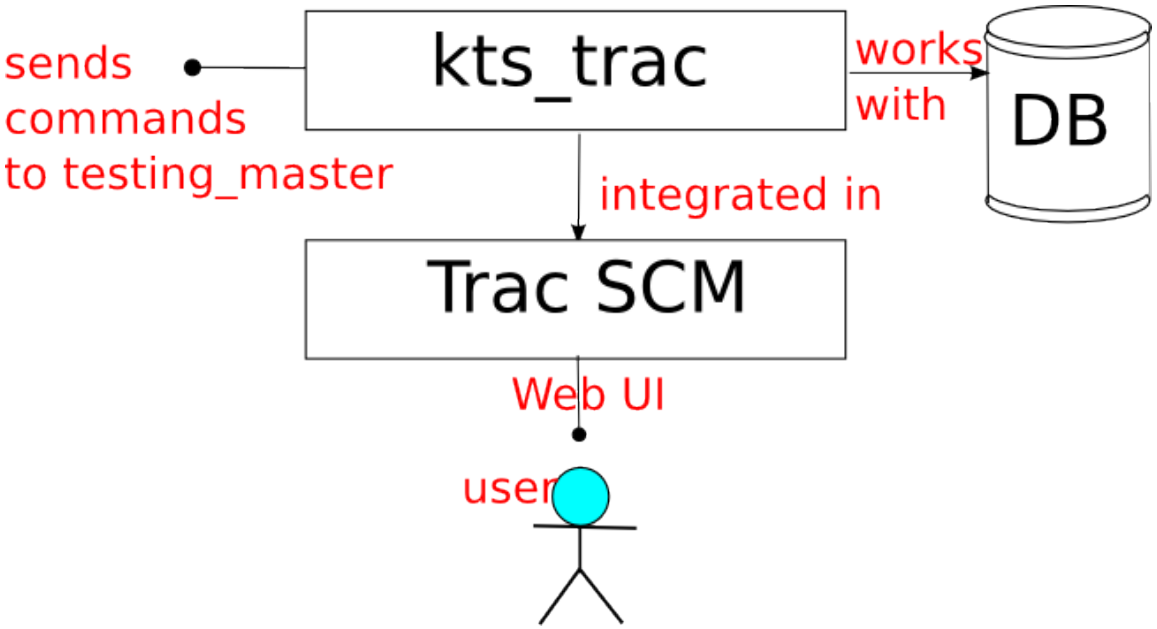
Пример тестового стенда



Testing_master крупным планом



kts_trac крупным планом



Протокол взаимодействия testing_master и testing_slave – VMSP.T

- VMSP.T является оригинальным протоколом прикладного уровня, работающим поверх стека TCP/IP
- VMSP.T является командно-ориентированным протоколом
- VMSP.T является текстовым протоколом
- При обмене сообщениями программы используют язык разметки YAML
- Основными командами демона testing_master являются: COLLECTIONS, DRIVERS, PRODUCTS, RELOAD
- Основными командами демона testing_slave являются: SLAVES, RESULTS, TESTS
- Разработанный протокол поддерживает механизм интроспекции

Компонент визуализации результатов тестов – kts_trac

kernel_testing_suite

Wiki | Timeline | Roadmap | Browse Source | New Ticket

☐	Slave ID	Slave name	Slave host	Slave port	Slave status
☐	1	eniac-2-slave	eniac-2	16008	NOT_CONNECTED
☐	2	w2008q-kts-slave	w2008q-kts	16008	WORKING
☐	3	mark-72-server-slave	mark-72-server	16008	WORKING
☐	4	w2003-kts-slave	w2003-kts	16008	SLEEPING
☐	5	cross-tt-i5-slave	cross-tt-i5	16008	NOT_CONNECTED
☐	6	cross-tt-i5-xp-slave	192.168.234.195	16008	SLEEPING
☐	7	cross-tt-i5-w7-slave	cross-tt-i5-w7	16008	NOT_CONNECTED
☐	8	cross-tt-i5-debian-slave	192.168.234.195	16008	SLEEPING
☐	9	cross-tt-i5-suse-slave	cross-tt-i5-suse	16008	NOT_CONNECTED
☐	10	cross-tt-i5-freebsd-slave	cross-tt-i5-freebsd	16008	NOT_CONNECTED

Update

trac Powered by Trac 0.11.2

Общая таблица с результатами тестов в kts_trac

Filters

Collection contains functional -

Test is smart_kts_base -

Add filter +

Max items per page 20 Page # 1 of 34

Update

☐	ID	Status	Test	Product	Slave	Collection	Driver	Started	Spent
☐	2197	unknown	smart_kts_base	console_release	w2008q-kts-slave	kernel_functional	test_all	2010-06-13 09:24:56	0:15:47
☐	2196	unknown	smart_kts_base	console_prebeta	w2008q-kts-slave	kernel_functional	test_all	2010-06-13 08:45:00	0:16:19
☐	2194	unknown	smart_kts_base	console_alfa	w2008q-kts-slave	kernel_functional	test_all	2010-06-13 08:04:49	0:16:52
☐	2193	unknown	smart_kts_base	console_alfa	w2003-kts-slave	kernel_functional	test_all	2010-06-13 07:03:52	1:06:14

Тестирование AB-ядра на функциональные регрессии

Param	Value
ID	2196
Status	unknown
Test	smart_kts_base
Product list	console_prebeta
Slave	w2008q-kts-slave
Collection	kernel_functional
Driver	test_all
Start time	2010-06-13 08:45:00
End time	2010-06-13 09:01:19
Time spent	0:16:19

Param	Value
EXPECTED_FAIL_TESTS	Test nameTest run log 04_archives/00_7z/006_various_type_detect 20_mime/08_regression_tests/002_eicar_binary 24_various_features/04_embedded_pe/008_embedded_suspected_detect 24_various_features/08_collect_tests/001_collect_suspected 24_various_features/08_collect_tests/002_collect_infected
OS info	Windows/w2008q-kts/Vista/6.0.6001//
PROBLEM_TESTS	Test nameTest run log 04_archives/99_all/001_mail_bomb_test 04_archives/99_all/005_al_test_0 04_archives/99_all/006_al_test_36 04_archives/99_all/007_al_test_100000 08_pe/03_various_malwares/014_virus.sality 16_digital_signature/004_reduce_detect_catalog_trusted_keys 16_digital_signature/021_adware_by_signature 18_containers/02_ms_office_actions/001_excel_2003_fd 18_containers/02_ms_office_actions/006_powerpoint_2003_fd
ERROR_COUNT	0

Тестирование AB-ядра на регрессии производительности

Test data

Param	Value
Test logs URL	ftp://logdb@192.168.234.72/log_storage/cross-tt-i5-debian-slave/time_test_base/time_test_yr/20100611_09-13-58 --> go

COMMON_TIME_INFO

	Vba32 Linux 3.12.12.5 / 2010.06.10 08:02 (Vba32.L) / release		Vba32 Linux 3.12.13 prebeta / 2010.06.11 03:42 (Vba32.L) / prebeta	
1	max_mem_size	117096	max_mem_size	117576
	real_time	1703.536569	real_time	1899.591123
	system_time	40.878554	system_time	44.942808
	input_ops	7719104	input_ops	9483504
	user_time	1620.533277	user_time	1788.539776
2	max_mem_size	117096	max_mem_size	117572
	real_time	1698.696327	real_time	1858.948864
	system_time	41.514594	system_time	39.69048
	input_ops	6896184	input_ops	5992560
	user_time	1616.505025	user_time	1782.83142
3	max_mem_size	117096	max_mem_size	117580
	real_time	1696.271862	real_time	1858.502684
	system_time	40.562535	system_time	38.89043
	input_ops	5809480	input_ops	5945680
	user_time	1620.601281	user_time	1783.627469

OS info	Linux/cross-tt-i5-debian/2.6.32-3-686/#1 SMP Thu Feb 25 06:14:20 UTC 2010/i686/
Run time	2:59:40.284405

AVERAGE_VALUES

Param	Vba32 Linux 3.12.12.5 / 2010.06.10 08:02 (Vba32.L) / release	Vba32 Linux 3.12.13 prebeta / 2010.06.11 03:42 (Vba32.L) / prebeta
max_mem_size	117096.0	117576.0
real_time	1699.501586	1872.347557
system_time	40.9852276667	41.1745726667
input_ops	6808256.0	7140581.0
user_time	1619.21319433	1784.999555

ERROR_COUNT	0
ERROR_LIST	
Driver version	0.1.0/R:795/L:795

Тестирование AB-ядра на стабильность

Param	Value
ID	2074
Status	unknown
Test	file_fuzz_test
Product list	console_alfa
Slave	w2008q-kts-slave
Collection	VirQ_1_all
Driver	fuzz_test
Start time	2010-06-07 20:04:44
End time	2010-06-08 05:25:42
Time spent	9:20:58
Test data	Param / Value HANGUP_COUNT: 0 ERROR_LIST: OS info: Windows/w2008q-kts/Vista/6.0.6001// Run time: 9:20:55.851000 ERROR_COUNT: 0 CRASH_COUNT: 35 PROCESSED_FILE_COUNT: 4000 SELECTED_FILE_COUNT: 4000 Driver version: 0.4.0/R:793/L:788 View all test data

Подводя итоги

- Разработанная система автоматизации тестирования сокращает время выхода продукта
- Разработанная система позволяет сократить до минимума время между внесением ошибки в код и её обнаружением
- Разработанная система позволяет в автоматическом режиме отыскивать уязвимости в АВ-ядре
- Использование проектов с открытыми исходными текстами позволяет значительно сократить затраты на автоматизацию процесса тестирования АВ-ядра
- ...

Спасибо за внимание!

Дзякую за увагу!
Благодарю за внимание!
Thank you for the attention!