Разработка без опасности или сертификация безопасного

Сертификация

Внедрение РБПО

Разработка документации

Подготовка к СИ

СИ

СИ

Совершенствование практик разработки безопасного программного обеспечения

Как изменилась команда лаборатории при работе в парадигме РБПО

- Команда статического анализа (5 человек)
- Команда фаззинг тестирования (2 человека)
- Команда архитектурного анализа (2 человека)

Как изменилась команда лаборатории при работе в парадигме РБПО

Размечено работок 1600

Более 40 принятых исправлений

https://github.com/python/cpython/issues/106831
https://github.com/HdrHistogram/HdrHistogram_c/issues/118
https://github.com/nodejs/node/issues/50896
https://github.com/php/php-src/issues/12791
https://github.com/php/php-src/issues/12962
https://listengine.tuxfamily.org/chrony.tuxfamily.org/chrony-dev/2023/10/msg00000.html
https://listengine.tuxfamily.org/chrony.tuxfamily.org/chrony-dev/2023/10/msg00001.html
https://github.com/OpenPrinting/libcupsfilters/issues/42
https://github.com/OpenPrinting/cups-filters/issues/552
https://github.com/OpenPrinting/cups-filters/issues/551
https://github.com/OpenPrinting/cups-browsed/issues/22

Центр исследования безопасности системного программного обеспечения

Входящие

Отправленные

Черновики

a.kuznetcov@fobos-nt.ru

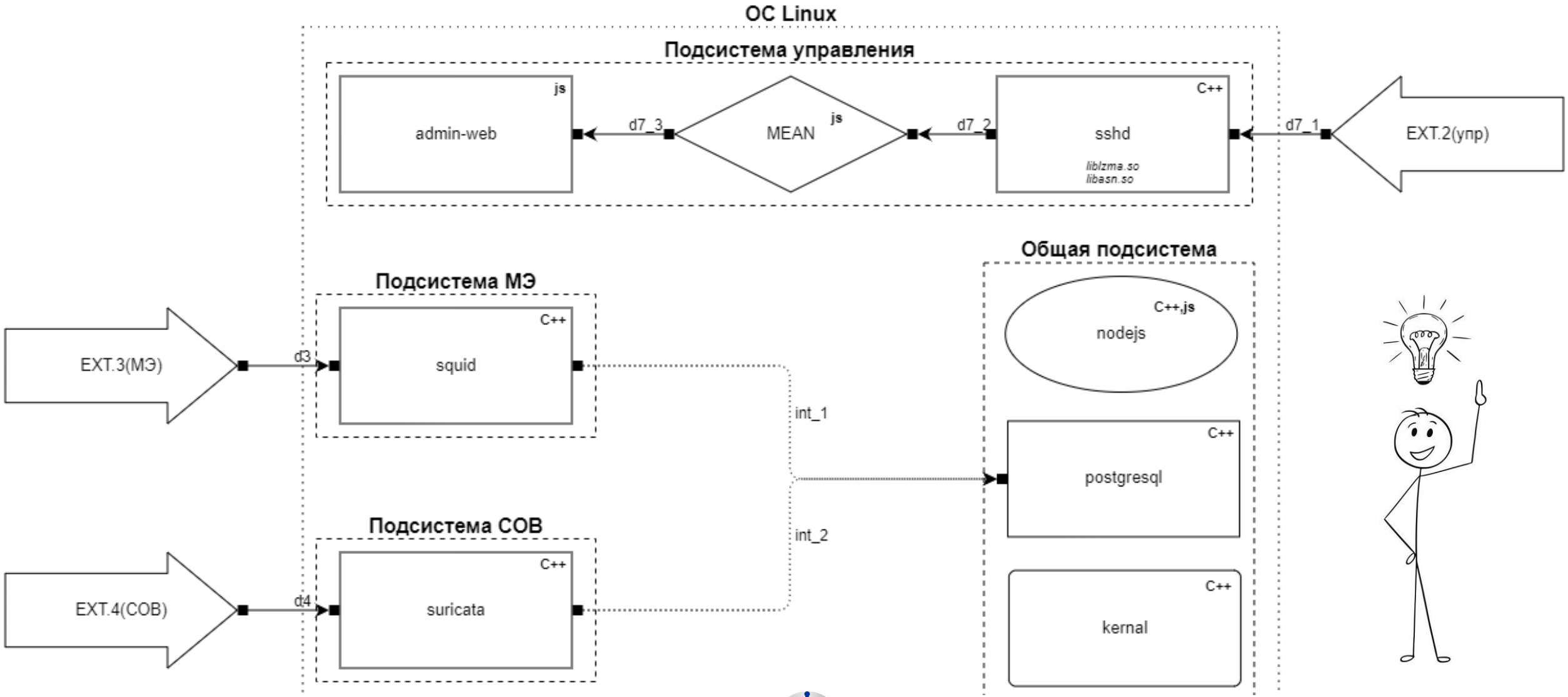
Входящие 25

Все Непрочитанные

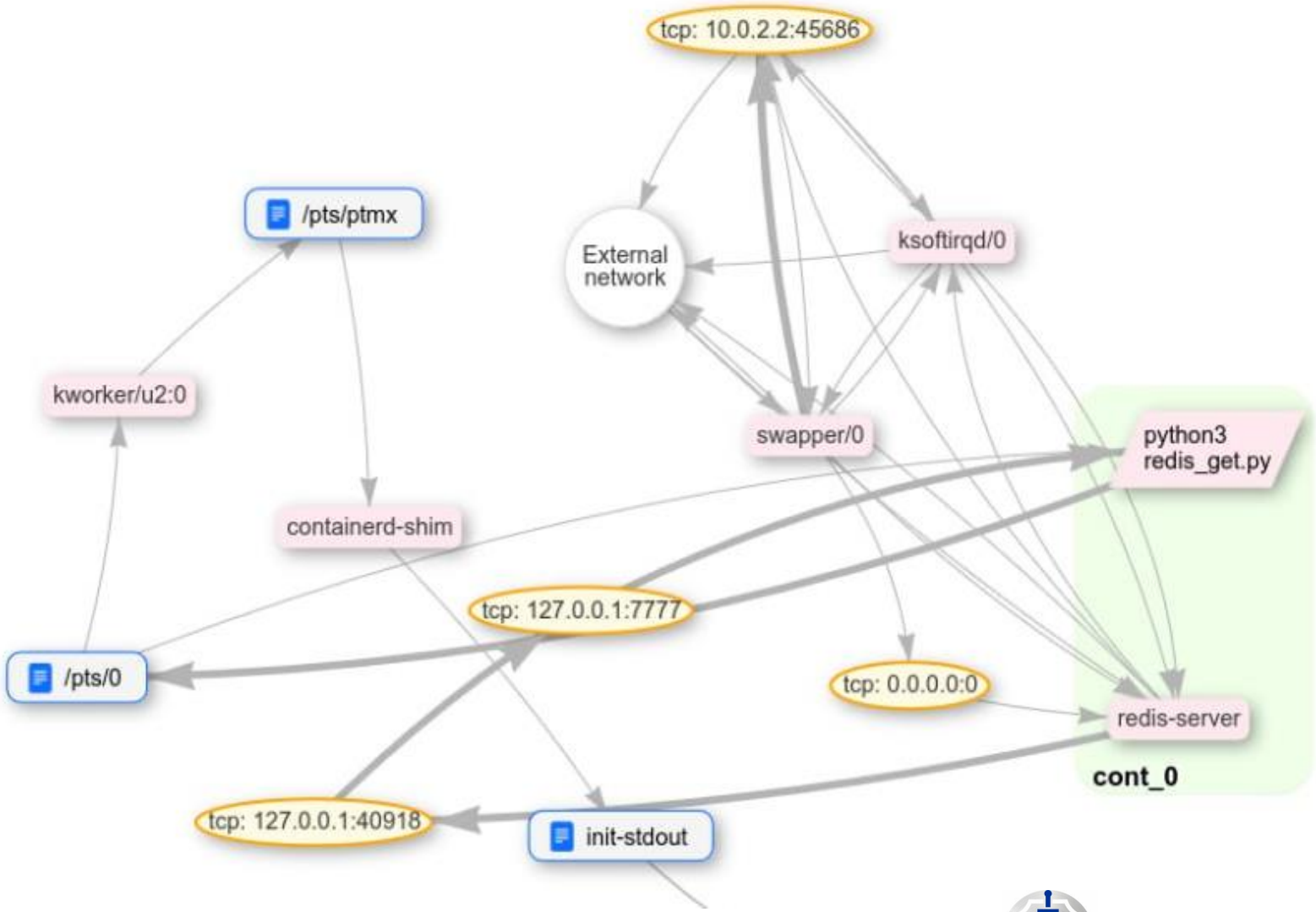
ОТ	ТЕМА
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] REDUNDANT_COMPARISON.ALWAYS_FALSE: src/storage/storage_util.c:3389
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] REDUNDANT_COMPARISON.ALWAYS_FALSE: src/vbox/vbox_common.c:4817
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] PASSED_TO_PROC_AFTER_RELEASE: src/qemu/qemu_command.c:9786
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] PASSED_TO_PROC_AFTER_RELEASE: src/qemu/qemu_command.c:1561
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] PASSED_TO_PROC_AFTER_RELEASE: src/qemu/qemu_command.c:9787
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] PASSED_TO_PROC_AFTER_RELEASE: src/qemu/qemu_command.c:8911
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] PASSED_TO_PROC_AFTER_RELEASE: src/qemu/qemu_command.c:1517
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] MEMORY_LEAK.EXCEPTION: tools/virt-host-validate-common.c:199
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] MEMORY_LEAK.EX.EXCEPTION: tools/virsh-completer-domain.c:695
Alexey Khoroshilov Добавлен новый комментарий.	[lvc-svace] MEMORY_LEAK.EX.EXCEPTION: src/vbox/vbox_snapshot_conf.c:579

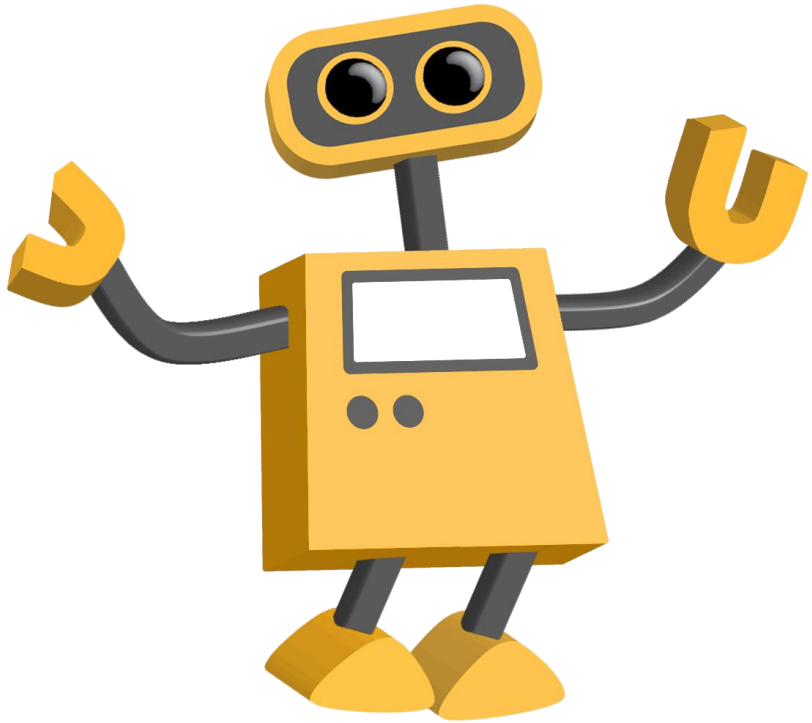
Центр исследования безопасности системного программного обеспечения

Поверхность атаки



Автоматизация определения поверхности атаки





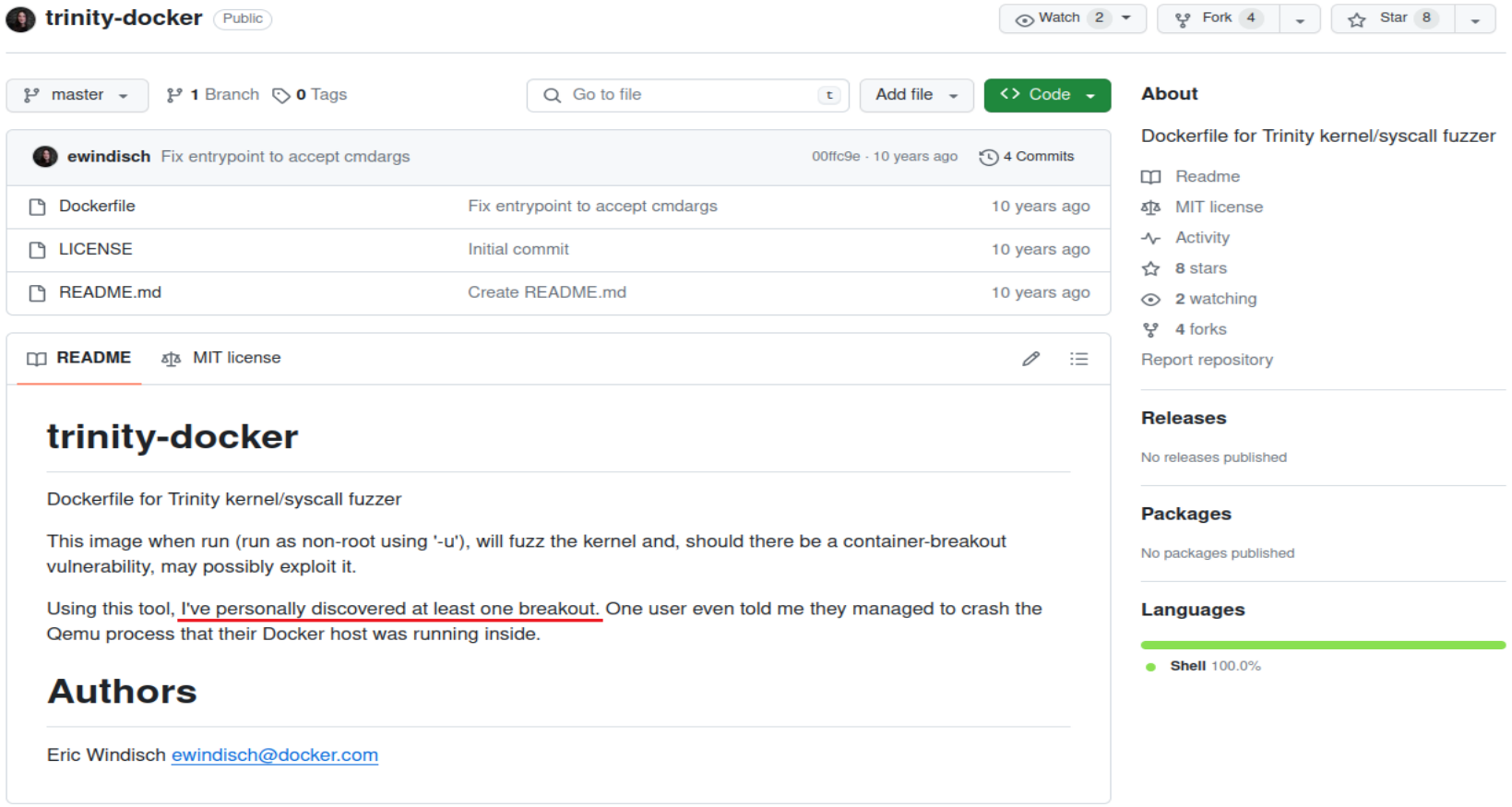
Применение философии фаззинга для тестирования изоляции Podman контейнеров (и не только)

Леонид

инженер ООО НТЦ «Фобос-НТ»

студент МГТУ Баумана

Стратегия фаззинг-тестирования Podman контейнеров



trinity-docker Public

Watch 2 | Fork 4 | Star 8

master | 1 Branch | 0 Tags | Go to file | Add file | Code

ewindisch Fix entrypoint to accept cmdargs — 00ffc9e · 10 years ago — 4 Commits

Dockerfile	Fix entrypoint to accept cmdargs	10 years ago
LICENSE	Initial commit	10 years ago
README.md	Create README.md	10 years ago

README | MIT license

trinity-docker

Dockerfile for Trinity kernel/syscall fuzzer

This image when run (run as non-root using '-u'), will fuzz the kernel and, should there be a container-breakout vulnerability, may possibly exploit it.

Using this tool, I've personally discovered at least one breakout. One user even told me they managed to crash the Qemu process that their Docker host was running inside.

Authors

Eric Windisch ewindisch@docker.com

About

Dockerfile for Trinity kernel/syscall fuzzer

Readme
MIT license
Activity
8 stars
2 watching
4 forks
Report repository

Releases

No releases published

Packages

No packages published

Languages

Shell 100.0%

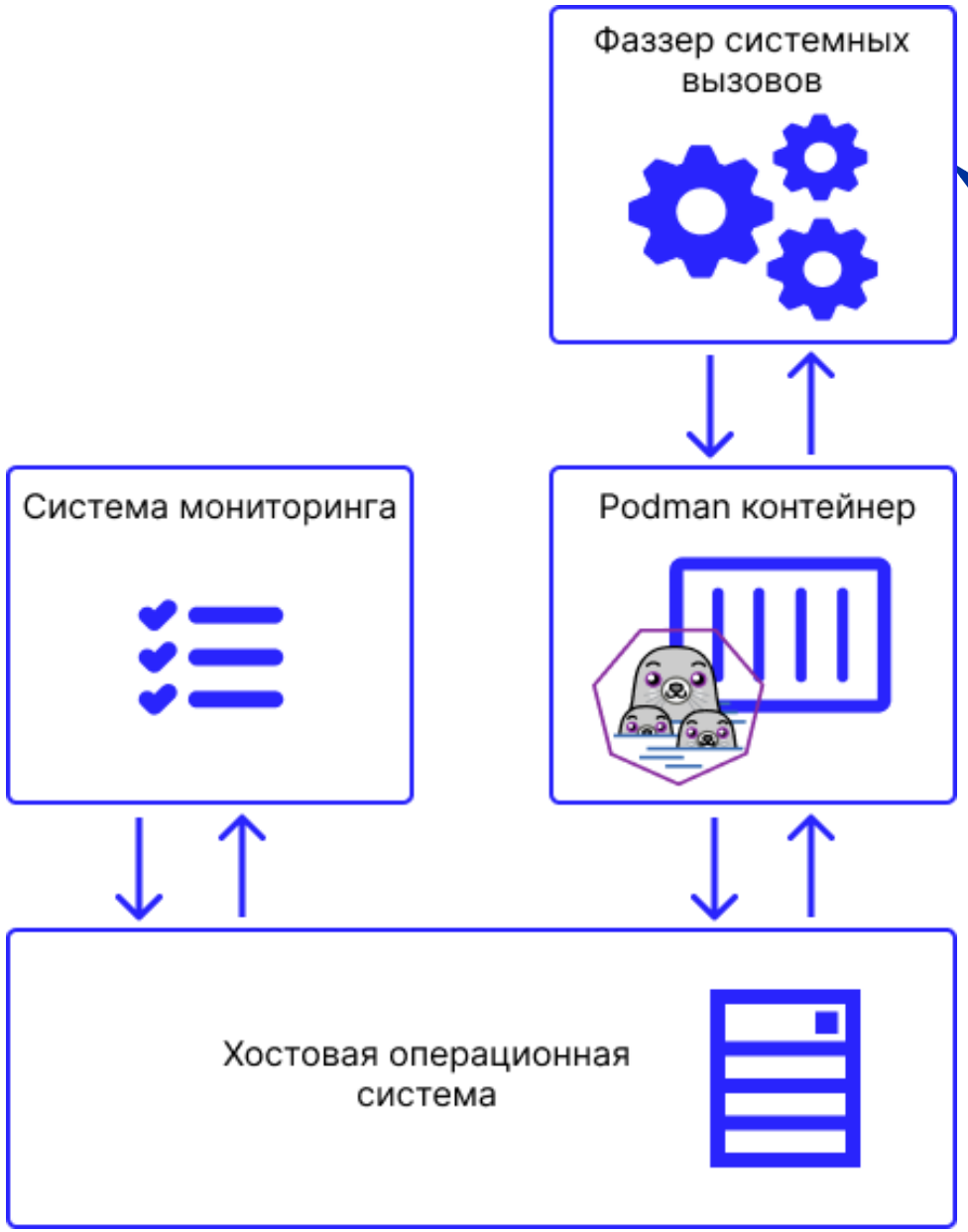
https://github.com/ewindisch/trinity-docker

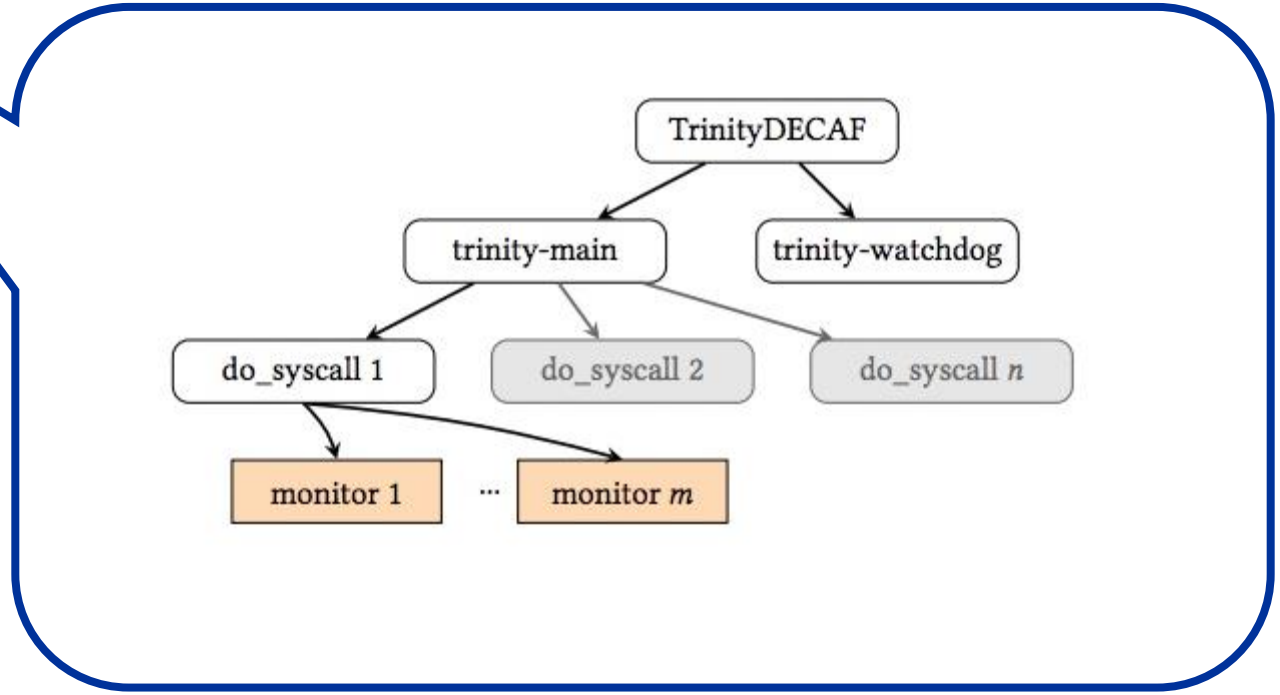
Стратегия фаззинг-тестирования Podman контейнеров

Критические состояния

Нарушение ограничений по потреблению ресурсов (cgroups)	• Потребление памяти больше лимита (> 110%) • Использование ЦП больше лимита (> 110%) • Количество дочерних процессов превосходит установленное значение
Побег из пространства имён	• Запущенный контейнер не должен порождать процесс в родительском пространстве имён
Чтение или запись в запрещённые места на хосте	• Запущенный контейнер не должен читать/записывать в недоступные места хостовой системы
Приобретение новых прав	• Контейнер не должен повышать свои привилегии (capabilities)

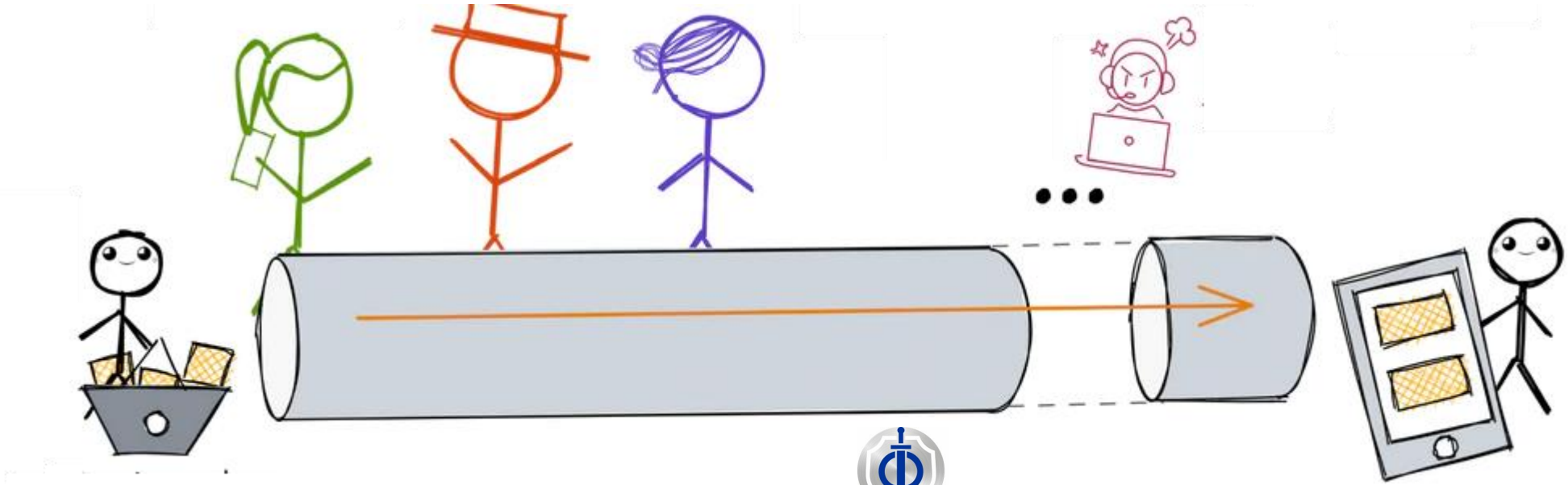
Стратегия фаззинг-тестирования Podman контейнеров





Аудит - сторонний взгляд на процессы разработки

- Подготовка к аудиту
- Сбор данных и информации
- Анализ данных и информации
- Формулирование выводов и рекомендаций



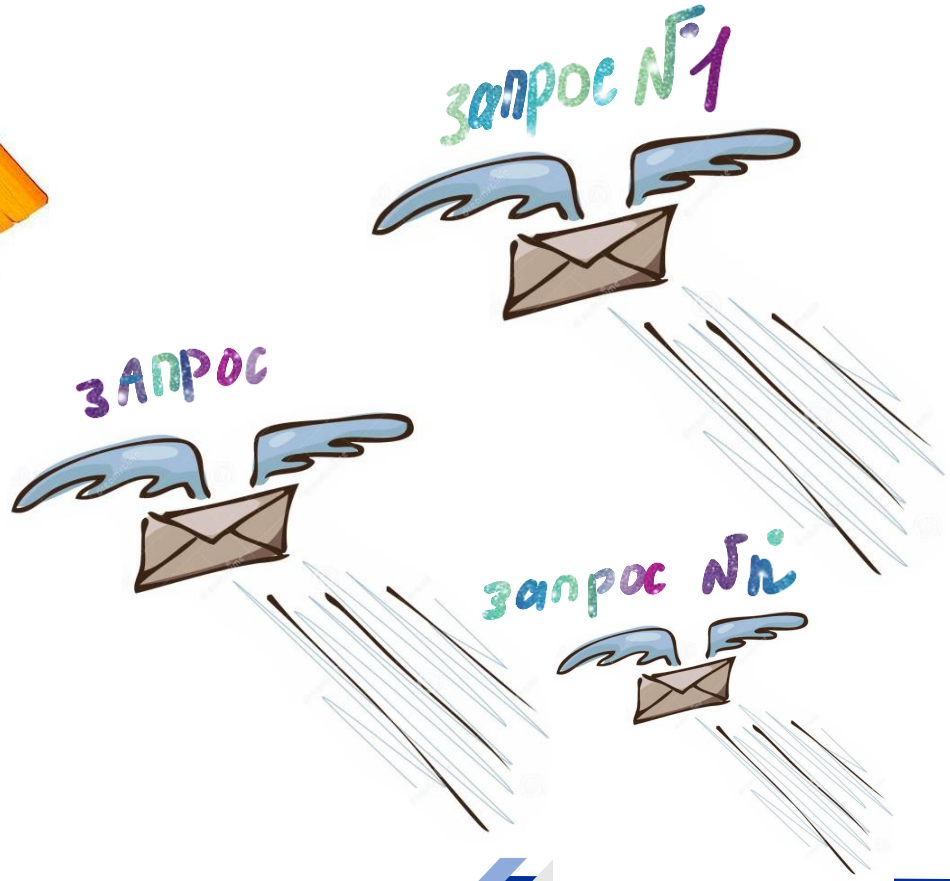
Аудит - двигатель безопасной разработки

Елена

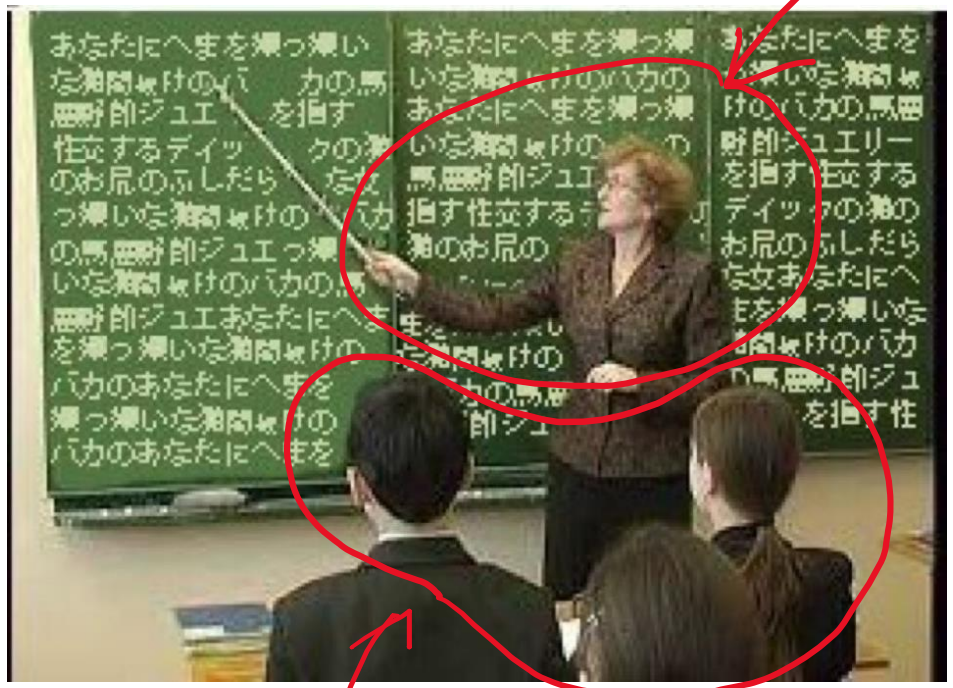
инженер ООО НТЦ «Фобос-НТ»

студент МГТУ Баумана

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР



это мы вам помогаем



это вы нам с интересом внимаете

История из жизни...

ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56939— 2016

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

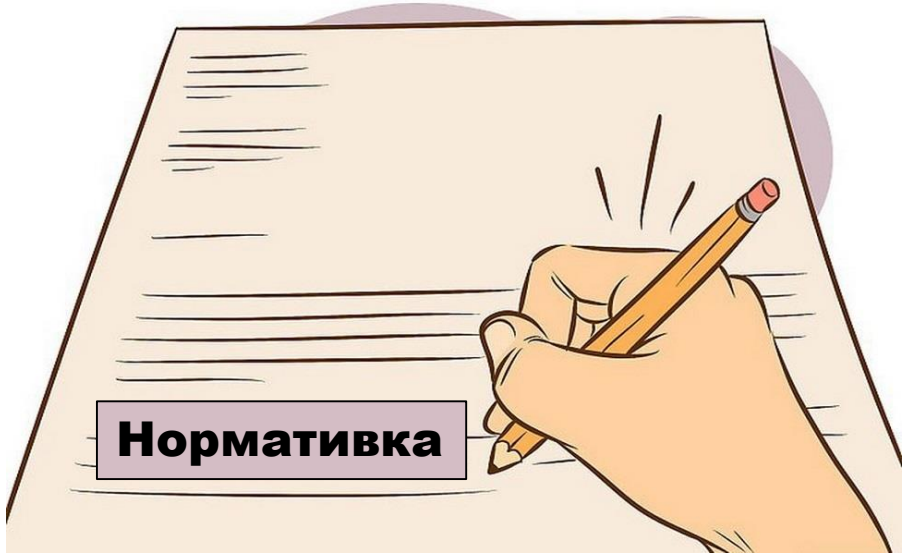
Москва
Стандартинформ
2018

+

+

Дмитрий Владимирович
Пономарев

kaspersky



Дмитрий Владимирович Пономарев

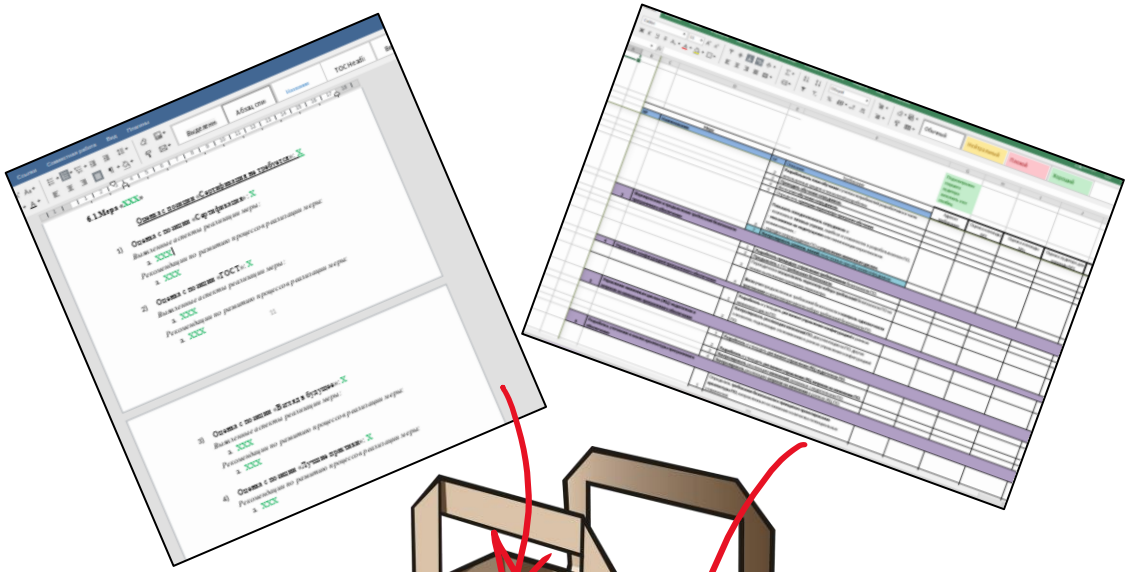
старший аудитор

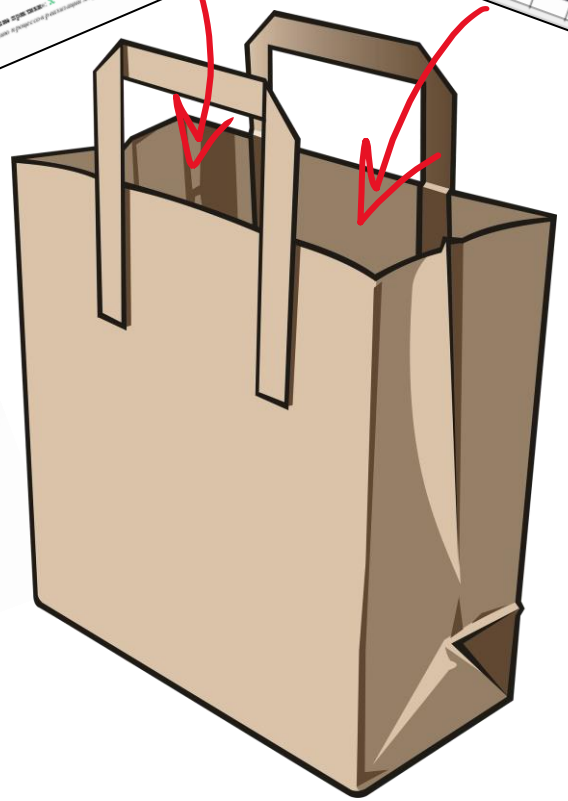
старший техпис

младший техпис

младший аудитор

Фобос-НТ
НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР





=


ГОСТ
ГОСТ
ГОСТ


ГОСТ
ГОСТ
ГОСТ


Методика
ВУ и НДВ


Тут нужен
аудит РБПО

“До скорой встречи!” :)