Безопасная разработка и Сертификация. Две стороны одной медали

Дмитрий Пономарев
ООО НТЦ «Фобос-НТ» / ИСП РАН
(@DmitryJustDmitry)

1.1. Актуальность безопасной разработки. Стратегия

Напряженная политическая обстановка. Нарастание информационного, технологического, экономического и пр. давления со стороны «иностранных партнеров». Ограничение доступа к технологиям, повышенные риски кибератак, в том числе уровня APT-группировок.

Комплексная угроза -> Комплексная защита:

1. Триумвират «Образование, Разработка, Инновации».

2. Принцип эшелонированной обороны:
   - физическая и административная защита;
   - привлечение SOC для выявления нестандартных и APT- угроз;
   - межсетевое экранирование, обнаружение вредоносной активности;
   - формирование политик организации и контроль за журналами;
   - проектирование и разработка приложений в парадигме безопасной разработки.

Собственная защищенность программного комплекса – последний рубеж обороны!

1.2. Актуальность безопасной разработки. Требования ФСТЭК России

Приказ №76 «Требования по безопасности информации…», раздел IV, п. 17.

Тестирование, испытания по выявлению уязвимостей и недекларированных возможностей, а также анализ скрытых каналов **проводятся изготовителем в ходе приемочных испытаний средства** и испытательной лабораторией в ходе сертификационных испытаний средства.

Приказ №121 «О внесении изменений в положение о системе сертификации…», п. 12.

При проверке организации производства программных и программно-технических средств защиты информации проверяется внедрение заявителем процедур безопасной разработки программного обеспечения **в соответствии с требованиями по безопасности информации, на соответствие которым проводятся сертификационные испытания**.

а также (*первоисточник уточните у представителя вашей ИЛ*):

«… если по совокупности выполнения пунктов «а» - «д» дана положительная оценка, **исследования ограничиваются верификацией результатов, предоставленных разработчиком**...».

1.3. Актуальность безопасной разработки. Неформально говоря

- парадигма: «отдадим собранный полгода назад комплекс бинарников в испытательную лабораторию, она нам что-то пофаззит, и можно считать испытания пройденными»;
  больше **системно** не работает!

- в настоящий момент требования к количественным и качественным характеристикам SDL- и сертификационных процессов задаются Положением о системе сертификации, Требованиями доверия и Методикой ВУ и НДВ. ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения» носит рекомендательный характер;

- безопасная разработка != «возьмём пару open-source анализаторов для видимости проведения исследований и оформим отчет с 200 000-ю формулировок «*Не эксплуатируемо, потому что не эксплуатируемо*»»:

- безопасная разработка == перманентный процесс, включающий выделенных сотрудников, технику, программные средства (**платные** и бесплатные) и понимание необходимости всего этого сотрудниками компании, от «джуна» до собственника.

Поставленный процесс – залог своевременного получения Сертификата соответствия и конкурентное преимущество XXI века!

2.1. Наш опыт. Друзья и партнеры

- проводим аудит SDL-процессов в АО «Лаборатория Касперского» с тех пор, когда это ещё не было мейнстримом (в течение последних 5 лет):

- помогаем в улучшении SDL-процессов и сертификации компаниям:

  ООО «Айдеко», АО «Аладдин Р.Д.», АО «АМГ БР», ООО «Амикон», ООО «А-Реал Консалтинг», ООО «Базальт СПО», ООО «БеллСофт», ООО «BI.ZONE», ООО «Доктор Веб», ООО «Group-IB», ООО «Газинформсервис», ООО «Гарда Технологии», АО «ИВК», ЗАО «Институт Сетевых Технологий», ООО «Код Безопасности», ООО «НПЦ КСБ», АО «Лаборатория Касперского», ООО «Нума Технологии», ООО «Постгрес Профессиональный», ООО «R-Vision», ООО «Secret Technologies», ООО «Cyberpeak»

  и другим…

- участвовали в пилотных испытаниях по новым требованиям и методикам ФСТЭК России совместно с ИСП РАН, ООО «Код Безопасности» и АО «Лаборатория Касперского» в 2019 году;

- участвуем в подготовке и проведении образовательных курсов ФАУ "ГНИИИ ПТЗИ ФСТЭК России“ на базе ИСП РАН;

- принимаем активное участие в «пилотировании» методик и средств анализа, разработанных ИСП РАН и в развитии сообщества Центра компетенций под эгидой ФСТЭК России и ИСП РАН.

2.2. Наш опыт. Как сформировать команду

- поставить цель и **проявить политическую волю**;

- сформировать команду профессионалов:
  - на внедрение SDL-практик в компании с командой 5-15 разработчиков необходимо 1-2 выделенных SDL-специалиста: Junior/Middle-разработчик по каждому ЯП, используемом в продукте, навыки пентеста и общее представление об анализе уязвимостей, devops-навыки, «горящие глаза» и «прямые руки»;
  - свободных Security Champion на рынке **нет**. Но такого специалиста реально **вырастить**;

- создать инфраструктуру: аппаратная платформа-вычислитель (1 млн. – 6 млн.), в том числе возможна аренда в облаке;

- развернуть необходимые инструментальные средства (до 5 млн. в год);

- запустить процесс и подождать 6-12 месяцев (срок на базовое освоение и внедрение SDL-практик).

Освоение полезного и сложного инструментария нужно начинать вчера!

2.3. Наш опыт. Опыт наших друзей из Аладдин Р.Д (ресурсоемкость)

Тезисы вебинара «Разработка безопасного ПО для предприятий КИИ, АСУ ТП, гос. структур» доступного по адресу https://www.youtube.com/watch?v=2TCscvm66aA

2.4. Наш опыт. Практики безопасной разработки

Требуемые практики безопасной разработки (**выборочно**):

- моделирование и проектирование безопасной архитектуры;
- анализ безызбыточности внешних интерфейсов и прав доступа к ресурсам;
- статический анализа исходного кода;
- статический анализа конфигураций модулей и контейнеров;
- использование безопасных тулчейнов (компиляторы, линковщики и их параметры);
- использование безопасных сторонних и заимствованных компонентов (**в том числе рантайм-компонент и интерпретаторов/ВМ**);
- динамический анализ – модульное и функциональное тестирование (подтверждение известного);
- динамический анализ – фаззинг-тестирование (поиск неизвестного);
- динамический анализ – выявление побочных взаимодействий со средой функционирования;
- динамический анализ – анализ утечек чувствительных (помеченных) данных;
- тестирование на проникновение.

Автоматизация практик безопасной разработки (встраивание в CI/CD).
Обучение студентов и сотрудников в парадигме безопасной разработки.

2.5. Наш опыт. Технологии безопасности ИСП РАН

«На поршневом самолёте нельзя улететь на луну.
Даже если «сейлы» утверждают обратное» ©

- статический ММКЧ-анализ с динамическим учетом параметров компиляции/компоновки и использованием доказательных возможностей SMT-решателей (**SVACE**);
- динамический фаззинг-анализ: низкоуровневого кода, с использованием технологий символьного выполнения и предикатов безопасности, с возможностями сбора покрытия по базовым блокам низкоуровневого кода, с возможностями оркестрации и мн. др. (**CRUSHER**);
- широчайший спектр технологий полносистемной интроспекции, в том числе для анализа распространения помеченных данных и определения поверхности атаки (**БЛЕСНА …**);
- анализ и создание компонентов сборочной системы (**БЕЗОПАСНЫЙ КОМПИЛЯТОР**);
- и многое, многое другое: https://www.ispras.ru/technologies.

А также, Центр верификации Linux (при поддержке государственных и частных организаций), ведущий работы по исследованию, повышению защищенности и стандартизации Linux-ядер.

3.1. SDL и ускорение процессов сертификации. Опыт наших друзей

BELLSOFT
Java Platform & Applications Experts

- дифференциальный фаззинг компиляторов виртуальной машины Java;
- полная автоматизация основных видов тестирования, генерация артефактов во всех средах;
- более 50 патчей в апстрим по итогам испытаний;

- единая пакетная база для множества архитектур (x86, X86_64, Elbrus, ARM7, ARM8, PowerPC) в рамках репозитория «Сизиф»;
- централизованные применение патчей и обновлений и тестирование по всему стеку пакетов во всех архитектурах;
- 4х-кратный рост SDL-команды за 1.5 года;

ИВК®
ИВК

base alt

3.2. SDL и ускорение процессов сертификации. Опыт наших друзей

- создание, имплементация и предоставление в общий доступ набора AppSec-инструментов BugBane, предназначенного для повышения эффективности борьбы с рутиной в процессах динамического фаззинг-тестирования;

- практически первыми приступили к анализу сложных пакетов (OpenSSL) с доведением найденных багов до подачи в апстрим;

- комплекс работ по анализу защищенности виртуальных машин C#, в частности, анализ и сокращение на 1/3 пакетной базы netcore 3.1;

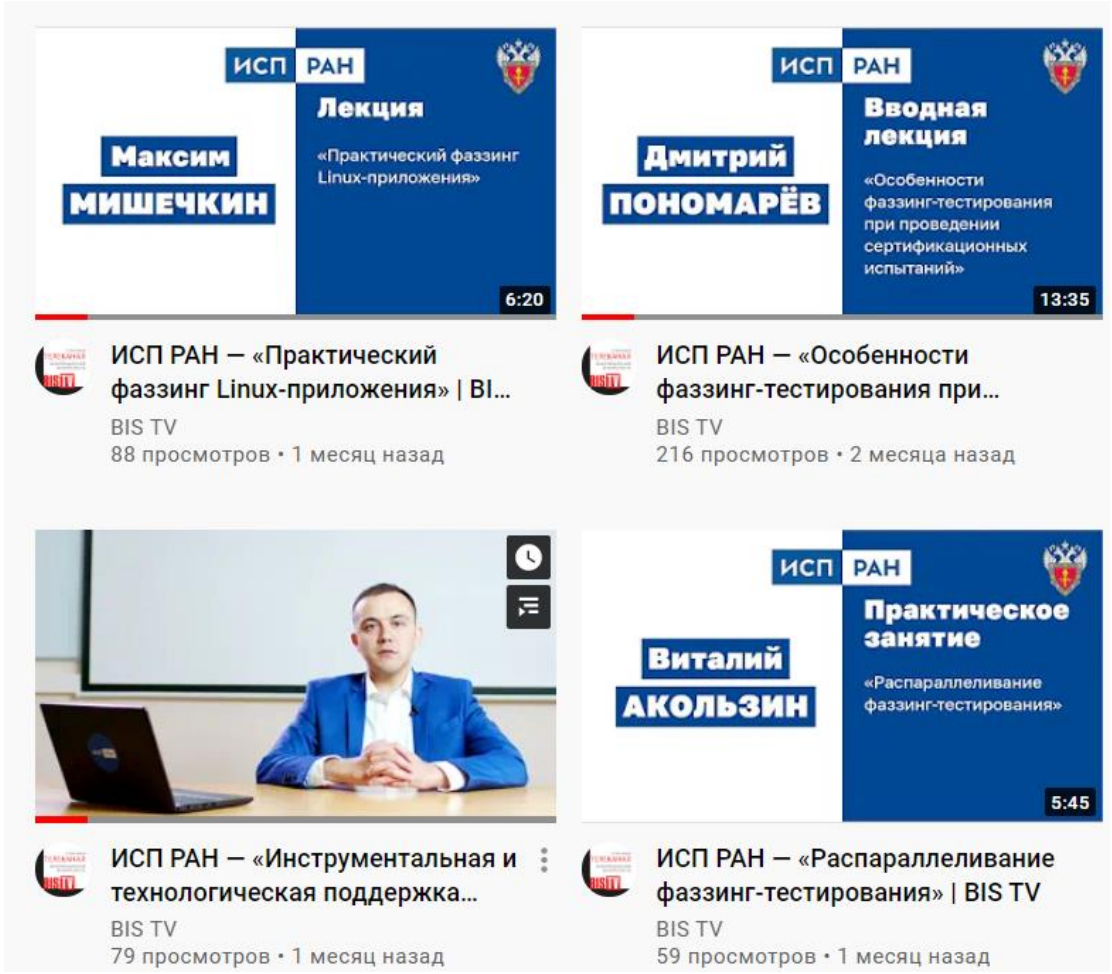
3.3. SDL и ускорение процессов сертификации. Опыт наших друзей

- глубокая контейнеризация и автоматизация процессов сборки, статического анализа и динамического тестирования;
- постоянная обратная связь по применению и улучшению статического анализатора SVACE, доведение 20+ выявленных багов до апстрима;

- создание фреймворка автоматизации модульного и фаззинг-тестирования и генерации отчетов;
- полная автоматизация проверок функций безопасности и генерации отчетов;
- создание собственного фреймворка структурного фаззинга.

4.1. Научная и методическая поддержка. Курсы Центра компетенций

- курсы ФСТЭК России по динамическому и статическому анализу на базе ИСП РАН - Программы №31 и №34 НОУ ДПО «ЦПКС ТЗИ»;
- видеолекции ИСП РАН по динамическому анализу (https://www.youtube.com/hashtag/фаззинг);
- подготовка курсов ФСТЭК России по архитектурному анализу на базе ИСП РАН;
- вебинары по инструментам и практикам их промышленного внедрения (https://nextcloud.ispras.ru/s/asFDqnGcWZiDKf4).



4.2. Научная и методическая поддержка. Чаты Сообщества Центра компетенций

@sdl_inform – канал, общие вопросы и новости о мероприятиях

@sdl_static – чат, статический анализ и вопросы использования svace

@sdl_dynamic – чат, динамический анализ

@sdl_community – чат, вопросы разделения типовых активностей по анализу интерпретаторов/виртуальных машин и иных сторонних компонентов

@sdl_flood – неофициальный ресурс

В любом деле важны энтузиасты – не стесняйтесь задавать вопросы и делиться своим опытом!

4.3. Научная и методическая поддержка. Сообщество Центра компетенций

- репозиторий сообщества Crusher: https://github.com/ispras/crusher

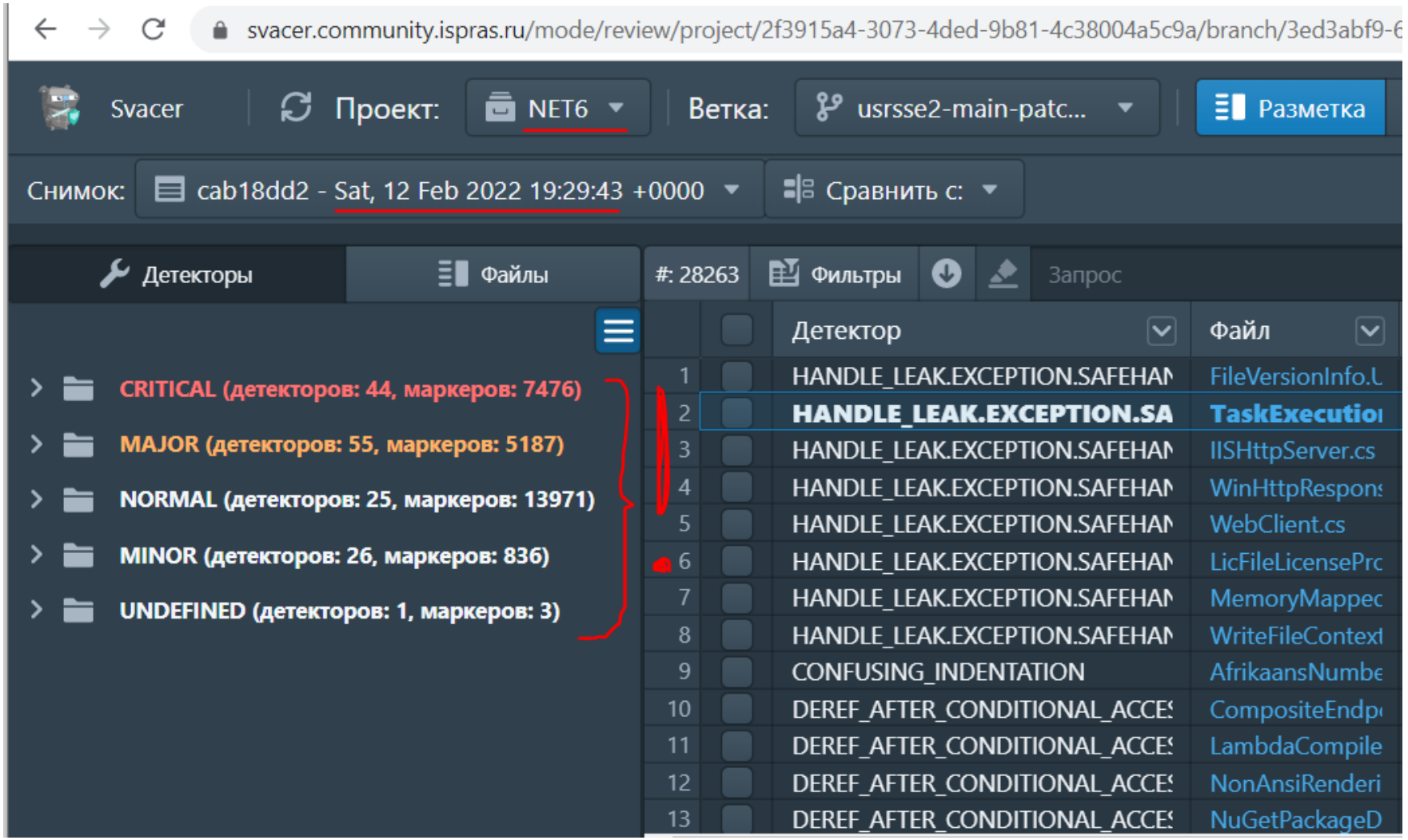
- тезисы встреч Сообщества Центра компетенций по разработка и апробации дорожной карты **пилотного проекта** интеграции практик разделения обязанностей по анализу заимствованных пакетов в существующие процессы безопасной разработки и сертификации: https://disk.yandex.ru/d/FkIL1_ojYj4a5g

- адреса community-репозиториев:
  - https://svacer.community.ispras.ru/
  - https://gitlab.community.ispras.ru/support/wiki
  - https://gitlab.community.ispras.ru/static
  - https://gitlab.community.ispras.ru/dynamic

- обучающие материалы по основам статического и динамического анализа в Community-репозитории (отдельная благодарность коллегам из **ИЛ ЦБИ** за помощь и участие в подготовке материалов): https://cloud.msk.fobos-nt.ru/index.php/s/qTk6s6JfT3A42Yz

и многое, многое другое!

5.1. Что дальше? Пример первичной разметки виртуальной машины и SDK .NET 6



Много, НО – НАДО. Решать фундаментальные задачи совместно проще и эффективнее!

5.2. Что дальше? Процессы, уже идущие в настоящий момент

- разработка и обновление ГОСТов по Безопасной разработке, Статическому и Динамическому анализу, Безопасной компиляции и т.д.;
- разработка и обновление Требований безопасности и Профилей защиты;
- автоматизация и стандартизация определения ширины и глубины поверхности атаки в процессе безопасной разработки продуктов и их сертификации;
- стандартизация использования системных компонент (ядра, системное ПО, компоненты виртуализации и контейнеризации, компоненты сборочной системы);
- обеспечение целостности результатов работы анализаторов с помощью цифровых подписей;
- стандартизация материалов сертификационных испытаний, уход от «бумажной безопасности»

и многое, многое другое!

Благодарю за внимание!

Дмитрий Пономарев
ООО НТЦ «Фобос-НТ» / ИСП РАН
(@DmitryJustDmitry)