Опыт внедрения SDL-практик в отечественных компаниях

Технический директор ООО НТЦ «Фобос-НТ»
Пономарев Дмитрий Владимирович

Испытательная лаборатория в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 (Аттестат аккредитации испытательной лаборатории № СЗИ RU.0001.01БИ00.Б039)

1. Опыт работы

Регуляторы

и другие...

Научная и инструментальная поддержка

ИСП РАН

Клиенты и партнеры

kaspersky

КОД БЕЗОПАСНОСТИ

NUMA TECHNOLOGY

GIB

PostgresPro

Аладдин

ИВК

BELLSOFT
Java Platform & Applications Experts

ideco

R-Vision
At the root of your security

GIS
ГАЗИНФОРМ СЕРВИС

А·М·Г· ИСКУССТВО НАХОДИТЬ

МВП ЭЛЕМЕЛ

и другие...

2. Оценка ситуации в области информационной безопасности

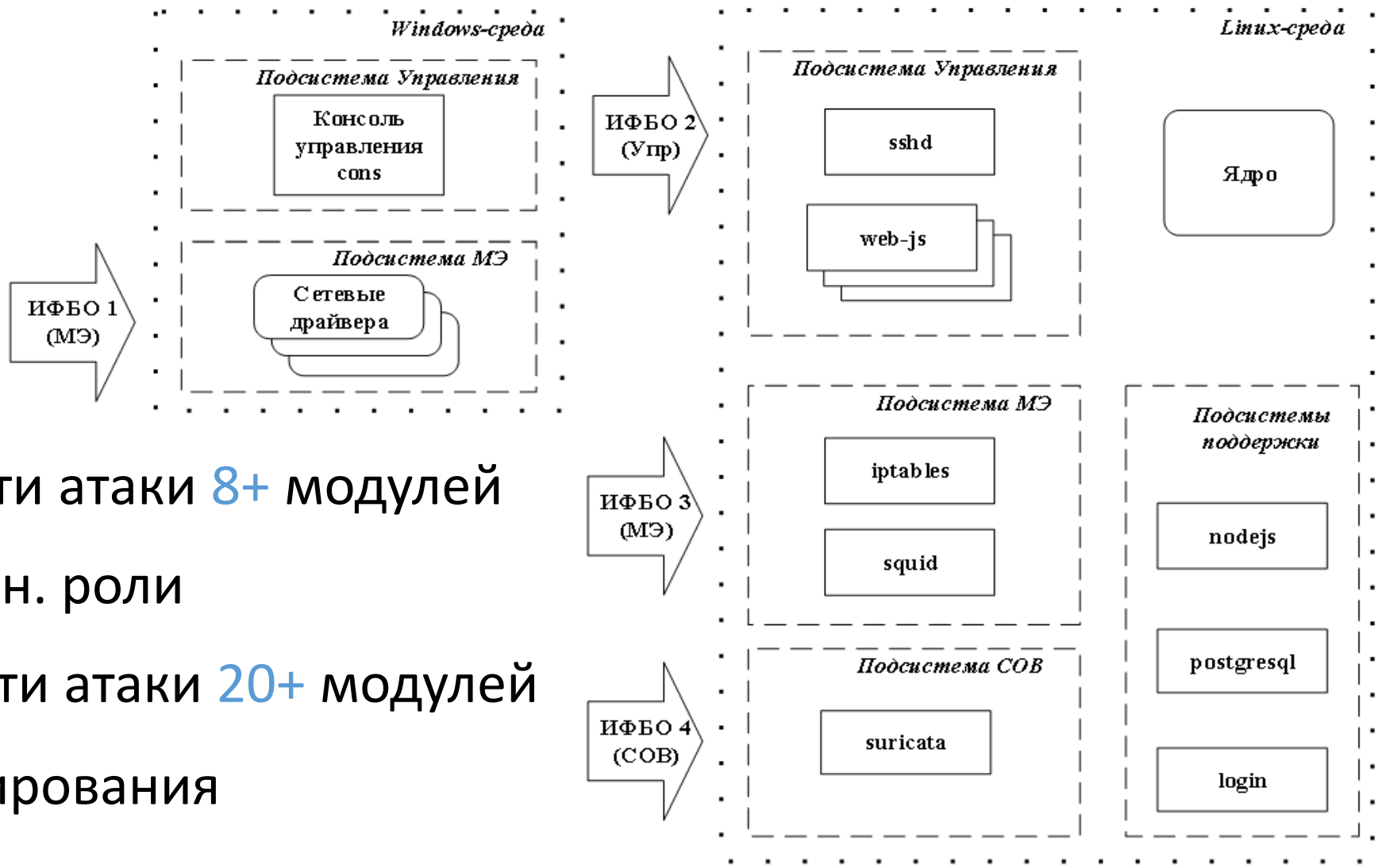
- степень информатизации общества, сложность информационных систем непрерывно увеличиваются
- взят стратегический курс на импортозамещение
- масштабы и сложность киберугроз непрерывно возрастают
- нехватка инженеров и менеджеров в области доверенной разработки
- средства и методики доверенной разработки и обеспечения информационной безопасности активно развиваются
- регуляторы уделяют доверенной разработке и информационной безопасности все большее внимания

3. Некоторые типичные вопросы эксперту

- поверхность атаки? Во внутреннем контуре?? Защитим админ. Мерами
- нам не нужен SDL. OpenSource-решения надёжны
- у нас нет людей, техники, средств под то, что от нас требуют
- статический анализатор Clang Static Analyzer умеет всё
- у нас отличный фаззинг - используем Burp Suite. Почему вы смеётесь..?
- динамический анализ… Фаззинга Burp’ом точно не хватит?
- у нас единственно правильный тулчейн, не трогайте
- какой такой анализ рантайма Java / C# / Python
- ваши методики и требования устарели / невыполнимы / бессмысленны
- нас нигде не учат и спросить не у кого

Типичные ответы квалифицированного эксперта

4. Поверхность атаки на примере межсетевого экрана



Оценка ПА:

- ширина поверхности атаки 8+ модулей
- 4 встроенных админ. роли
- **глубина** поверхности атаки 20+ модулей
- 2 среды функционирования
- код на 4 ЯП, 4+ компилятора

5. Зачем анализировать OpenSource

Сторонние компоненты в составе продукта это ваш код. Если в состав вашего продукта входит 400+ пакета с github, вы отвечаете за всю кодовую базу

Зачем фаззить OpenSource:

- 11 критичных уязвимостей в IDS suricata в 2019 г. Найдены фаззингистом-любителем!

-BDU:2020-04280: уязвимость демона маршрутизации bird, связанная с недостаточной проверкой размера пакетов протокола OSPFv2

6. Люди, техника, средства анализа

Оценочные затраты на внедрение SDL-практик для команды 5-15 разработчиков:

- 1-2 специалиста: (Junior/Middle-разработчик, навыки пентеста, горящие глаза и прямые руки)
- аппаратная платформа-вычислитель (0,5 млн – 1,5 млн)
- инструментальные средства (0 млн – 5 млн)
- 3-6 месяцев на освоение SDL-практик

Инструментальные средства:

- либо доступны в OpenSource, либо недешевы, но стоят своих денег и предоставляют поддержку. Остерегайтесь платных «поделок».
- неформальный критерий хорошего инструмента – международная база клиентов (как минимум - клиенты на свободном рынке)

7. Статический анализ

Анализ на уровне AST и стилистики отдельных модулей трансляции в 2020 году это не достижение, но необходимый минимум.

Возможности статических анализаторов:

- перехват сборки. Учет опций компиляторов, анализ на уровне бит/байт кода после выполнения препроцессинга и оптимизаций
- межмодульный, межпроцедурный контекстно-чувствительный анализ. Построение статических трасс ошибок по объектному коду
- производительность. 2-3 сборки в сутки для 3-4 ГБ исходных кодов
- SMT-решатели. Проверка выполнимости трасс. Символьное выполнение

COVERITY BY SYNOPSYS klocwork PERFORCE SVACE ИСП РАН

8. Динамический анализ (фаззинг) – это интересно

Фаззеры бывают разные: afl, libfuzzer, Crusher (ИСП РАН), Hongfuzz и т.д.

Что фаззим: usermode Windows / Linux, Linux Kernel, Windows driver и т.д

Инструментирование: статическое (gcc, syzygy) / динамическое (DynamoRIO, QEMU, Intel PT) / интерпретационная (python-afl)

Мутации: управление мутациями, stateful fuzzing

Оркестрация: Docker, QEMU и т.п.

Дополнительное инструментирование: санитайзеры, оптимизации

Фаззинг прошивок в дампах памяти

и многое другое …

9. Динамический анализ (помимо фаззинга) – это ещё интереснее

Динамическое символьное выполнение: перевод ассемблерных трасс в набор уравнений и ограничений к ним для генерации данных, открывающих новый путь выполнения программы

Предикаты безопасности: набор ограничений, описывающих срабатывание различных дефектов

Автоматический анализ эксплуатируемости выявленных дефектов

Полносистемная эмуляция и анализ распространения помеченных данных

Модульное и регрессионное тестирование и многое другое …

10. Среды сборки и выполнения

- компиляторы могут порождать эксплуатируемые уязвимости в машинном коде. Инфа 100%

- параметры компиляции могут превращать безопасный исходный код в небезопасный машинный код

- изменения, вносимые в скомпилированный и скомпонованный код дополнительными инструментаторами, могут порождать небезопасный машинный код

- недоверенная среда функционирования, в т.ч. интерпретатор, оптимизирующий JIT-компилятор, сборщик мусора, могут превращать безопасный исходный код в небезопасную программу

11. Методики, обучение, сообщество

- актуальные Методики отечественных Регуляторов задают высокую планку доверенной разработки, конкурируют с мировыми стандартами

- наряду с ужесточением требований к доверенной разработке активно развиваются инструментальные средства и Методики, Регуляторы открыты к позитивной повестке

- в рамках партнерства ФСТЭК России и РАН в лице ИСП РАН проводятся курсы повышения квалификации

- созданы и развиваются Телеграм-ресурсы, посвященные стат. и дин. анализу. **Приглашаем к участию всех заинтересованных**:

@sdl_dynamic @sdl_static @sdl_inform

Благодарю за внимание

Технический директор ООО НТЦ «Фобос-НТ»
Пономарев Дмитрий Владимирович

Испытательная лаборатория в Системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 (Аттестат аккредитации испытательной лаборатории № СЗИ RU.0001.01БИ00.Б039)