AKTIV.
CONSULTING

Особенности реализации требований к безопасной разработке ПО **в промышленных организациях**

Александр Моисеев

Ведущий консультант по информационной безопасности AKTIV.CONSULTING

О чем сегодня пойдет речь

1

Обеспечение безопасной разработки ПО в промышленных организациях

2

Реализация проверок безопасности для «унаследованного» ПО

Обеспечение безопасной разработки ПО в промышленных организациях

01

Особенности разработки ПО в промышленных организациях

Бизнес аспекты:

1. Прикладное **ПО управляет** технологическими, производственными процессами
2. **Длительный ЖЦ**
3. Оказывает **влияние на здоровье** человека, экологию, ущерб инфраструктуре
4. Меры ИБ **должны предотвращать ухудшение** эффективности мер ФБ *(ГОСТ Р 59506)*

Технические аспекты:

1. **Специфические** ЯП и протоколы
2. **Повышенные требования** устойчивости к отказам
3. **Долгий цикл** предварительных и приемочных испытаний, оценки
4. соответствия

Возможна связь с безопасностью:

- промышленной
- функциональной безопасностью *(МЭК 61508)*
- зданий и сооружений *(ГОСТ 34332)*
- атомной *(МЭК 63096)*
- машин и механизмов *(Machinery Directive)*
- и т. п.

Эталонная модель ЖЦ ПО ФБ (МЭК 61508)

ЖЦ системы безопасности

ЖЦ ПО системы безопасности

1 Спецификация требований к ПО

2 Планирование подтверждения соответствия безопасности ПО

3 Проектирование и разработка ПО

- Архитектура ПО
- Исходный код
- Детальное проектирование
- Инструментальные средства и ЯП
- Тестирование модулей ПО
- Интеграционное тестирование

4 Интеграция ПАК и ПО

5 Эксплуатация ПО

6 Планирование подтверждения соответствия безопасности системы

к ПНР системы

к эксплуатации системы

Модификация ПО

Верификация ПО

Оценка ФБ ПО

Методы и средства обеспечения безопасности

МЕТОДЫ

- Структурные методы *(CORE, JSD, ...)*
- Прослеживаемость *(прямая и обратная)*
- Стандарты кодирования
- Программирование с защитой
- Формальное доказательство *(методы CCS, CSP, VDM, Z)*

СРЕДСТВА

- Универсальный язык программирования *(UML)*
- Статический и динамический анализ
- Доверенные инструментальные средства
- Функциональное тестирование и тестирование методом «черного ящика»
- Стресс-тестирование

Рекомендуемый набор мер для обеспечения безопасности при разработке

Управление доступом к среде разработки

Формирование рекомендаций по безопасному программированию

Установление требований ИБ в отношении сторонних компонентов и коллективов разработки

Управление уязвимостями в сегменте разработки и продуктовой среде

Тестирование на проникновение

Фаззинг

Реализация проверок безопасности для «унаследованного» ПО

02

Проблематика

Неподдерживаемый код

Нет документации к ПО

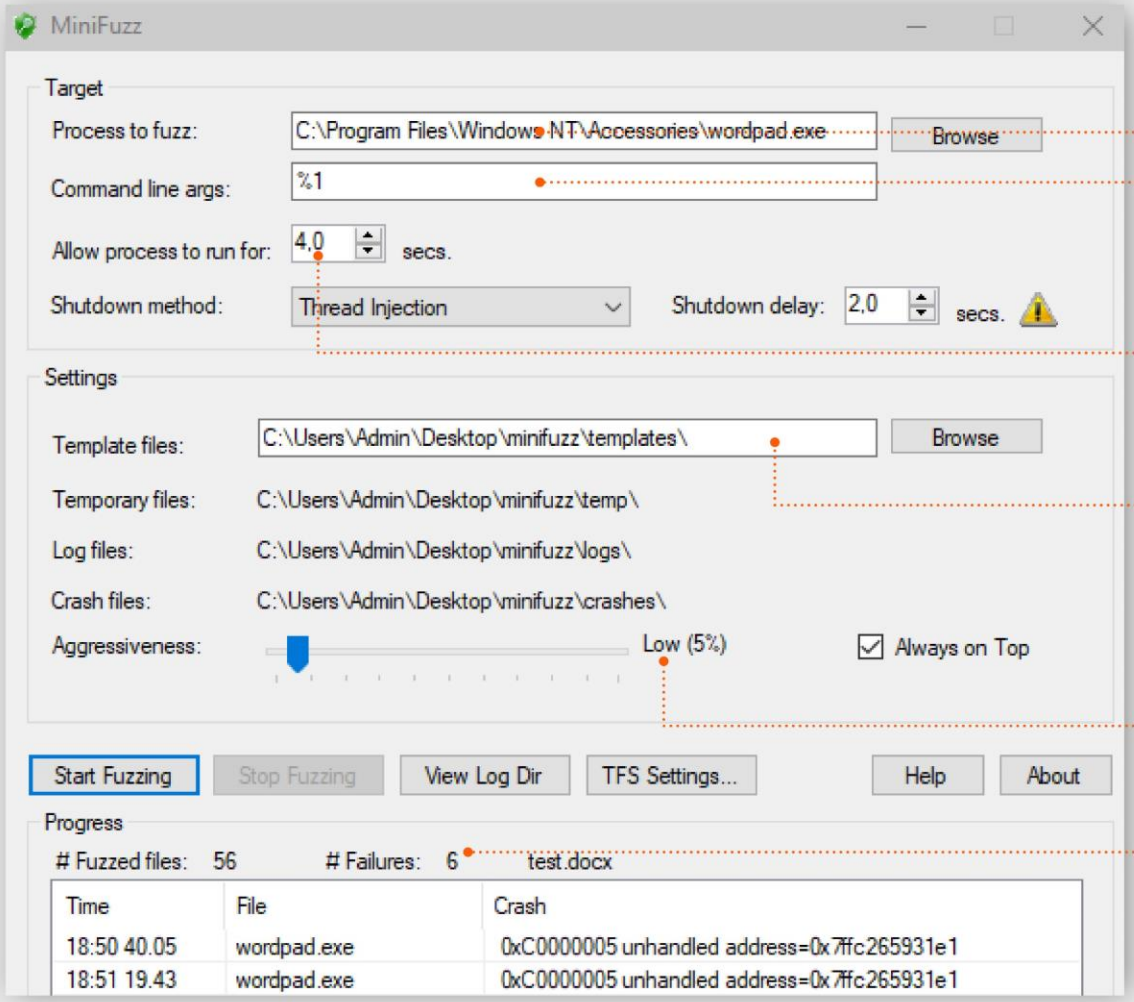
Используются устаревшие версии ЯП, библиотек

Не используются технологии защиты кода (DEP, ASLR, safe stack и т.п.)

Исследование исполняемого файла
методом «серого ящика»

1 **Статический анализ «1/2»** **Динамический анализ «1/2»**	Поиск нетипичных артефактов или поведения
2 **Фаззинг**	Локализация ошибок
3 **Статический анализ «2/2»** **Динамический анализ «2/2»**	Дизассемблирование и отладка

Попытка вызвать ошибку (на примере фаззера файлов MiniFuzz)



Полный путь до приложения

Передаваемые тестируемому приложению опции командной строки

Время функционирования приложения до принудительного завершения

Путь до папки с файлами шаблонами

Степень искажения файла шаблона

Счетчик ошибок

В качестве резюме

01

При внедрении БРПО для ЗО КИИ важно учитывать **отраслевую специфику и практики,** связанные с промышленной и функциональной безопасностью

02

Часть свидетельств безопасности ПО может содержаться в имеющейся **проектной документации**

03

Для проверок безопасности «унаследованного» ПО необходимо применять **методы** «**серого ящика**»

04

Для тренировки навыков написания безопасного кода разработчикам нужна постоянная **тренировка практик security**

05

Рекомендуем дополнить регуляторные требования **собственными проверками** безопасности *(управление секретами, SCA/OSA, SBOM, автоматизированные проверки безопасности в CI/CD и т.д.)*

Разработка нового ПО как правило осуществляется с привлечением уже существующего задела *(заимствованные компоненты и библиотеки, легаси код, и т.п.)* **и требует проведения композиционного анализа**

AKTIV.
CONSULTING

Александр Моисеев

Ведущий консультант по информационной безопасности AKTIV.CONSULTING

moiseev@aktiv.consulting