

ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

ГОСТ Р 56939-2024

Вебинар 7. Моделирование угроз и разработка описания поверхности атаки



ПРЕДСТАВИМСЯ!

Спикеры и гости вебинара



АЛЕКСАНДРА УВАРОВА

DEVELOPER ADVOCATE, C++ DEVELOPER

- Разработчик C++ части анализатора PVS-Studio.
- Рассказываю про качество кода и безопасную разработку на конференциях
- Пишу технические и научные статьи



ВИТАЛИЙ ПИКОВ

ЭКСПЕРТ В ОБЛАСТИ ИТ, ИБ, ПРЕПОДАВАТЕЛЬ

- Стаж преподавательской работы более 10 лет
- Заслуженный доцент Российского нового университета, преподаватель высшей школы
- Microsoft Certifications Earned: MCT, MCPS, MCSA, MCTS
- Автор более 30 научных публикаций



ЕКАТЕРИНА РУДИНА

АНАЛИТИК ДЕПАРТАМЕНТА ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ
«ЛАБОРАТОРИИ КАСПЕРСКОГО»

- Эксперт в области кибербезопасности
- Специализируется на исследовании угроз и моделировании рисков
- Обеспечивает аналитическую поддержку по вопросам стандартов и нормативных требований
- Активно участвует в развитии отраслевых норм в сфере защиты информации и киберфизических систем

Доклад:

Моделирование угроз и оценка поверхности атаки
в контексте РБПО



kaspersky

О ЦИКЛЕ ВЕБИНАРОВ

«Вокруг РБПО за 25 вебинаров»



ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ: ГОСТ Р 56939-2024

- Организуют УЦ МАСКОМ и ООО «ПВС» (PVS-Studio)
- ГОСТ Р 56939-2024 описывает 25 процессов, необходимых для реализации разработки безопасного ПО, поэтому и 25 вебинаров
- Мы открыты к сотрудничеству по разбору тем, пишите нам!

ЗАПИСИ ПРЕДЫДУЩИХ ВЕБИНАРОВ



pvs-studio.ru/ru/webinar/rbpo/

О ПРОЦЕССЕ

5.7 Моделирование угроз и разработка описания поверхности атаки



5.7.1 ЦЕЛИ

1. Создание условий для снижения количества недостатков, связанных с особенностями реализации архитектуры ПО и логики его функционирования, выработка мер по нейтрализации угроз безопасности, связанных с особенностями реализации архитектуры
2. Уточнение модели угроз и описания поверхности атаки по результатам разработки кода и его изменений.

5.7.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

1. Выполнить первичное моделирование угроз ПО и разработать меры по их нейтрализации.
2. Выполнить первичное описание поверхности атаки.
3. Сформировать перечень целей для дальнейших исследований безопасности ПО.
4. Выполнять уточнение модели угроз периодически или при определенных событиях.
5. Выполнять уточнение описание поверхности атаки периодически или при определенных событиях.
6. При уточнении поверхности атаки анализировать её методом идентификации интерфейсов ПО.
7. Уточнять перечень целей для исследований безопасности с учетом изменений в архитектуре, модели угроз и анализе поверхности атаки.

5.7.3 АРТЕФАКТЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

1. Модель угроз должна включать:
 - Описание угроз, объект воздействия, возможные последствия.
 - Рекомендуется учитывать ГОСТ Р 58412, БДУ ФСТЭК, STRIDE, OWASP, DREAD.
2. Перечень мер по нейтрализации угроз должен быть приоритизирован по критичности ущерба.
3. Описание поверхности атаки должно включать потенциальные области воздействия на систему.
4. Перечень целей должен содержать модули и интерфейсы ПО, составляющих поверхность атаки, подлежащих дополнительному анализу.

5.7.3 АРТЕФАКТЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

5. Уточнённая модель угроз должна учитывать новые угрозы, актуальные для выполненных изменений.
6. Уточнённое описание поверхности атаки, должно включать перечень функциональных подсистем ПО и их интерфейсов, составляющих поверхность атаки.
7. Уточнённый перечень целей для проведения дальнейших исследований безопасности ПО должен содержать описание функциональных подсистем, модулей ПО, их интерфейсов.

ЗАЧЕМ ОПРЕДЕЛЯТЬ ПОВЕРХНОСТИ АТАКИ?

- Современные программные системы содержат огромные объёмы собственного и стороннего кода.
- Просто невозможно и избыточно педантично изучать и проверить весь код.
- Необходимо выделить функции/модули, которые взаимодействуют с внешним миром и, скорее всего, будут подвергаться атаке.



[Зачем искать поверхность атаки
для своего проекта](#)

КАКОВЫ ОСНОВНЫЕ СПОСОБЫ ОПРЕДЕЛЕНИЯ ПОВЕРХНОСТИ АТАКИ?

- Привлечение эксперта
- Инструменты поиска точек входа
- Динамический анализ кода
- Статический анализ кода



ПРИМЕНЕНИЕ СТАТИЧЕСКИХ АНАЛИЗАТОРОВ КОДА

Терминология ГОСТ Р 71207-2024: анализ помеченных данных (п.3.1.3):

Статический анализ, при котором анализируется течение потока данных от источников до стоков.

1. Под источниками понимаются точки программы, в которых данные начинают иметь пометку — некоторое заданное свойство. Под стоками понимаются точки программы, в которых данные перестают иметь пометку.
2. Распространённая цель анализа помеченных данных — показать, что помеченные данные не могут попасть из источников — точек ввода пользователя в стоки — процедуры записи на диск или в сеть. Факт такого попадания означает утечку конфиденциальных данных.

ВЫЯВЛЕНИЕ НЕДОСТОВЕРНЫХ ДАННЫХ

ГОСТ Р 71207-2024 (п.7.6):

- Если статический анализатор для поиска ошибок применяет анализ помеченных данных, должна быть предоставлена возможность конфигурации анализа: должны задаваться процедуры-источники и процедуры-стоки чувствительных данных.

В PVS-Studio реализована требуемая стандартом разметка истоков и стоков данных для всех поддерживаемых языков (C, C++, C#, Java).



[Механизм пользовательских аннотаций](#)

СТАТИЧЕСКИЕ АНАЛИЗАТОРЫ

- Могут находить потенциальные уязвимости, которые связаны с поверхностью атаки
- Могут проследить распространение данных и детектировать их небезопасное использование, зная, что определённая функция является источником, приемником или валидатором зараженных данных.

ПЕРЕДАЮ СЛОВО
СЛЕДУЮЩЕМУ СПИКЕРУ



Сделай свой проект
чистым и безопасным
вместе с PVS-Studio



VOKRUG_RBPO25



Получи 10% скидку
на курсы «М БРПО»
в Учебном Центре «МАСКОМ»



VOKRUG_RBPO25

