Методический подход к выбору оптимального набора процедур выявления уязвимостей

авторы: Шаров И.А., Язов Ю.К.

Докладчик: доктор техн. наук, профессор Язов Юрий Константинович

Актуальность выбора процедур выявления уязвимостей

В нормативных правовых актах, утвержденных приказами ФСТЭК России, выявление уязвимостей является составной частью процесса организации защиты информации

Необходимость выявления уязвимостей в ПО была определена Советом Безопасности Российской Федерации в 2014 г.

Существующие модели процесса выявления уязвимостей основаны на экспертных оценках :

- не позволяют количественно **оценивать эффективность** исследований
- не позволяют моделировать **совокупность процедур** исследований
- не позволяют обосновывать **целесообразный состав** методов и процедур исследований
- не учитывают **особенности** исследуемого ПО

Более **5000 комбинаций** процедур исследований по выявлению уязвимостей

Методы выявления уязвимостей

Экспертный анализ

- Моделирование атак
- Направленный анализ участков кода
- Анализ документации
- Ранжирование уязвимостей

Динамический анализ

- Фаззинг
- Отслеживание помеченных данных
- Сканирование уязвимостей
- Анализ активности и потоков взаимодействия программы
- Эмуляция оборудования
- Динамическая бинарная трансляция
- Профилирование
- Съём трасс выполнения программы
- Сканирование интерфейсов получения входных данных
- Анализ сетевого трафика

Статический анализ

- Межпроцедурный контекстно-чувствительный анализ
- Формальная верификация
- Анализ, чувствительный к путям выполнения
- Анализ бинарного кода
- Анализ байт-кода
- Синтаксический анализ
- Абстрактная интерпретация
- Оценка метрик сложности программного кода
- Инструментация программного кода
- Извлечение информации из исполняемого кода программы
- Визуализация данных
- Компилирование кода
- Итеративный анализ потока данных
- Аутентификация программного кода

Комбинированный анализ

- Антивирусное сканирование
- Сопоставление статических и динамических маршрутов
- Оценка соответствия исходных кодов программы их исполняемому коду
- Восстановление формата данных
- Символьное выполнение
- Слайсинг
- Анализ тестового покрытия
- Съём микропрограммного кода
- Подтверждение уязвимости

- целевой метод

- вспомогательный метод

Процесс выявления уязвимостей

✓Более 20 наименований исходных данных

✓Более 10 вариаций выполнения вспомогательных процедур

✓Более 30 вариаций выполнения целевых процедур

✓Возможность повторного выполнения процедур

Число сочетаний процедур ограничивается только сложностью архитектуры ПО

Взаимосвязь метода, процедуры и вариаций ее выполнения

Показатели оценки эффективности выявления уязвимостей

Показатель эффективности процедуры

$$\eta_k = \delta_k^{(j)} \cdot (1 - p_k^{(np)}) \cdot C_k \cdot \sum_{r=1}^{R} \nu_r \cdot \theta_r \;\; при \;\; \tau_{всп}^{(k)} + \tau_{цел}^{(k)} \le T_{\lim}$$

Показатель эффективности совокупности процедур

$$\eta^{(j)} = \bigcup_{k=1}^{K} \widehat{\xi_k} = \sum_k \widehat{\xi_k} - \sum_{k<i} \widehat{\xi_k} \cap \widehat{\xi_i} + \sum_{k<i<z} \widehat{\xi_k} \cap \widehat{\xi_i} \cap \widehat{\xi_z} -$$

$$-\ldots + (-1)^{K-1} \cdot \widehat{\xi_1} \cap \widehat{\xi_1} \cap \ldots \cap \widehat{\xi_K}$$

$$при \sum_k \delta_k^{(j)} \cdot \overline{\tau_{всп}^{(k)}} + \sum_k \delta_k^{(j)} \cdot \overline{\tau_{цел}^{(k)}} \le T_{\lim}$$

Пример. Пусть имеются три кортежа процедур,
значения показателей степени исследованности которых равны $\xi_1 = 0,2,\ \xi_2 = 0,3,\ \ \xi_3 = 0,4$

Тогда для совокупности кортежей $\xi^{\{1,2,3\}} = \xi_1 + \xi_2 + \xi_3 - \xi_1 \cdot \xi_1 - \xi_1 \cdot \xi_3 - \xi_2 \cdot \xi_3 + \xi_1 \cdot \xi_2 \cdot \xi_3 = 0,664$

Постановка оптимизационной задача выбора процедур исследований ПО

Исходные данные

Средства автоматизации

ЭТАП 1 — **Формирование перечня процедур выявления уязвимостей и вариаций их выполнения**

Оптимизационная задача № 1

Максимизация эффективности

$$\begin{cases} \eta^{(j)} \to \max\limits_{C_K^{K^{(j)}}}, \forall\, K^{(j)} = \overline{1, K} \\ \sum\limits_{k=1}^{K^{(j)}} \overline{\tau_k} \le T_{\lim} \end{cases}$$

Оптимизационная задача № 2

Минимизация времени исследования ПО

$$\begin{cases} \sum\limits_{k=1}^{K^{(j)}} \overline{\tau_k} \to \min\limits_{C_K^{K^{(j)}}}, \forall\, K^{(j)} = \overline{1, K} \\ \eta^{(j)} \ge \eta_{\lim} \end{cases}$$

ЭТАП 2 — **Выбор оптимального набора процедур**

ЭТАП 3 — **Разработка программы и методик исследований по выявлению уязвимостей**

Спасибо за внимание!

Язов Юрий Константинович