Анализ исходных кодов эксплойтов и признаков их выполнения для формирования объективных оценок защищенности информационных систем

Е.В. Федорченко, Е.С. Новикова

Лаборатория проблем компьютерной безопасности, СПб ФИЦ РАН

РусКрипто - **21-24 марта, 2023**

Содержание

Мотивация

If you can't measure it, you can't improve it.

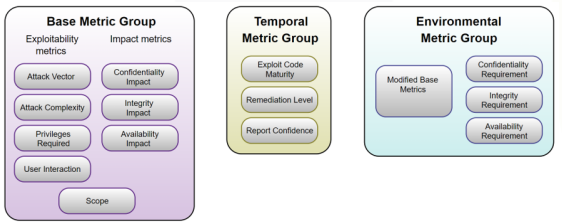
Peter Drucker

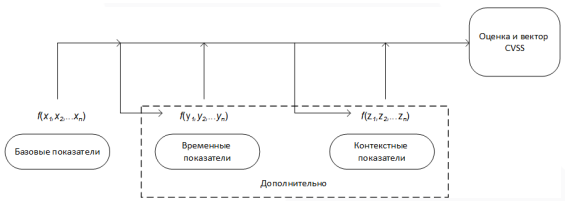
Постановка задачи исследования

Научная проблема

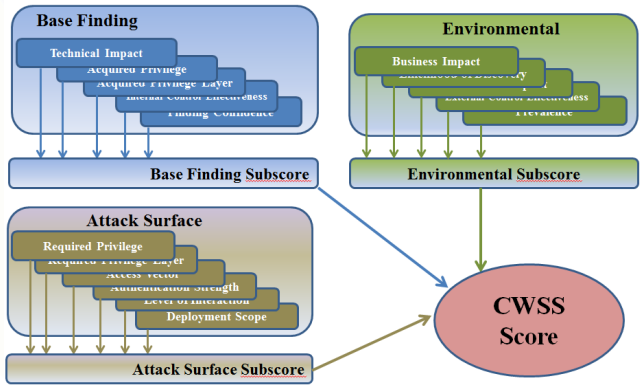
Противоречие между необходимостью в объективных и объяснимых показателях защищенности и тем, что в основе популярных систем оценивания защищенности лежат экспертные оценки.

CVSS:





CWSS:



Другие системы оценки:

- Методика ФСТЭК
- ISO2700*
- Методика OWASP
- NIST 800-30
- TRA
- RRA

Постановка задачи исследования

Цель

Повышение эффективности противодействия киберугрозам за счет формирования понятных, объективных и объяснимых показателей защищенности на основе анализа исходных кодов эксплойтов и обнаружения признаков их реализации в реальном времени.

Методология

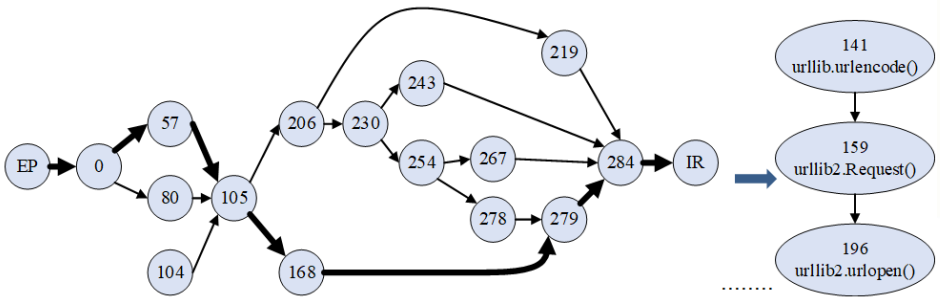
1. Разработка модели выполнения эксплойтов
2. Поиск исходных данных для реализации и анализа предложенной модели
3. Реализация и анализ модели для определения показателей защищенности, основанных на особенностях исходного кода эксплойтов
4. Выбор подхода к формированию тестовой среды для проведения экспериментов
5. Формирование тестовой среды для выполнения эксплойтов и определения признаков их выполнения в системе, для формирования показателей, основанных на признаках выполнения эксплойтов
6. Проведение экспериментов для определения признаков выполнения эксплойтов и определения основанных на них показателей защищенности
7. Разработка методики прогнозирования атакующих воздействий, а также автоматизации принятия решений по повышению защищенности

Подход

Подход:

- излечение данных из EDB
- компиляция исходного кода отдельных эксплойтов;
- декомпиляция;
- построение функциональной семантической модели эксплойтов;
- сравнение моделей и генерация стандартной семантической модели исходного кода эксплойтов для последующего извлечения признаков, которые будут применяться для вычисления показателей защищенности.

Семантическая модель исходных кодов эксплойтов:



Применение:

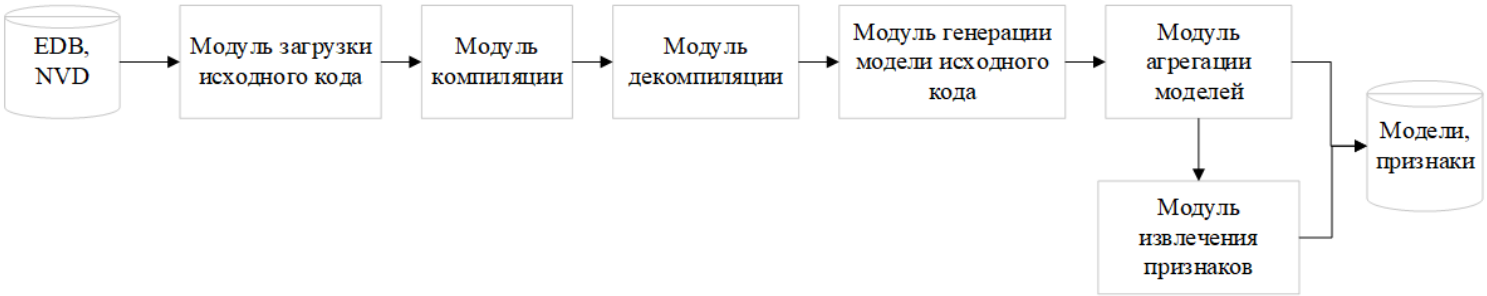
- выявления наиболее часто используемых фрагментов злонамеренного кода и вычисления статистических показателей на их основе;
- вычисления вероятностей перехода от одного фрагмента кода к другому;
- выявления признаков выполнения фрагментов кода в системе, их сопоставления концептам модели для последующего прогнозирования шагов кибератаки.

Другие модели:

- абстрактное синтаксическое дерево (Abstract Syntax Tree, AST),
- абстрактный семантический граф (Abstract Semantic Graph, ASG),
- граф потока управления (Control Flow Graph, CFG),
- граф зависимостей программы (Program Dependence Graph, PDG),
- граф свойств кода (Code Property Graph, CPG)

Реализация

Основные компоненты модуля анализа исходного кода эксплойтов:



Исходные данные: база эксплойтов “Exploit DataBase” (EDB).

Типы эксплойтов в EDB:

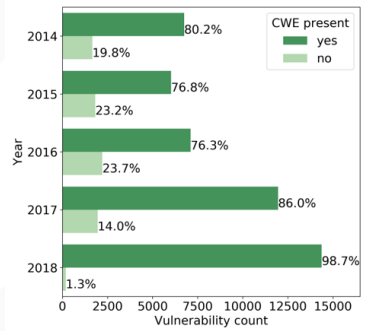
- 4292 веб приложений (webapps),
- 1829 на отказ в обслуживании (dos),
- 1078 эксплойтов, исполняемых локально (local),
- 1030 эксплойтов, исполняемых удаленно (remote),
- 287 шелл-кодов (shellcode).

Статистика эксплойтов в EDB по платформе:

- 531 эксплойтов для аппаратных платформ;
- 3610 эксплойтов для операционных систем;
- 132 эксплойтов для программных платформ;
- 3432 эксплойтов для веб платформ, и
- 1646 неопределенных.

Связи:

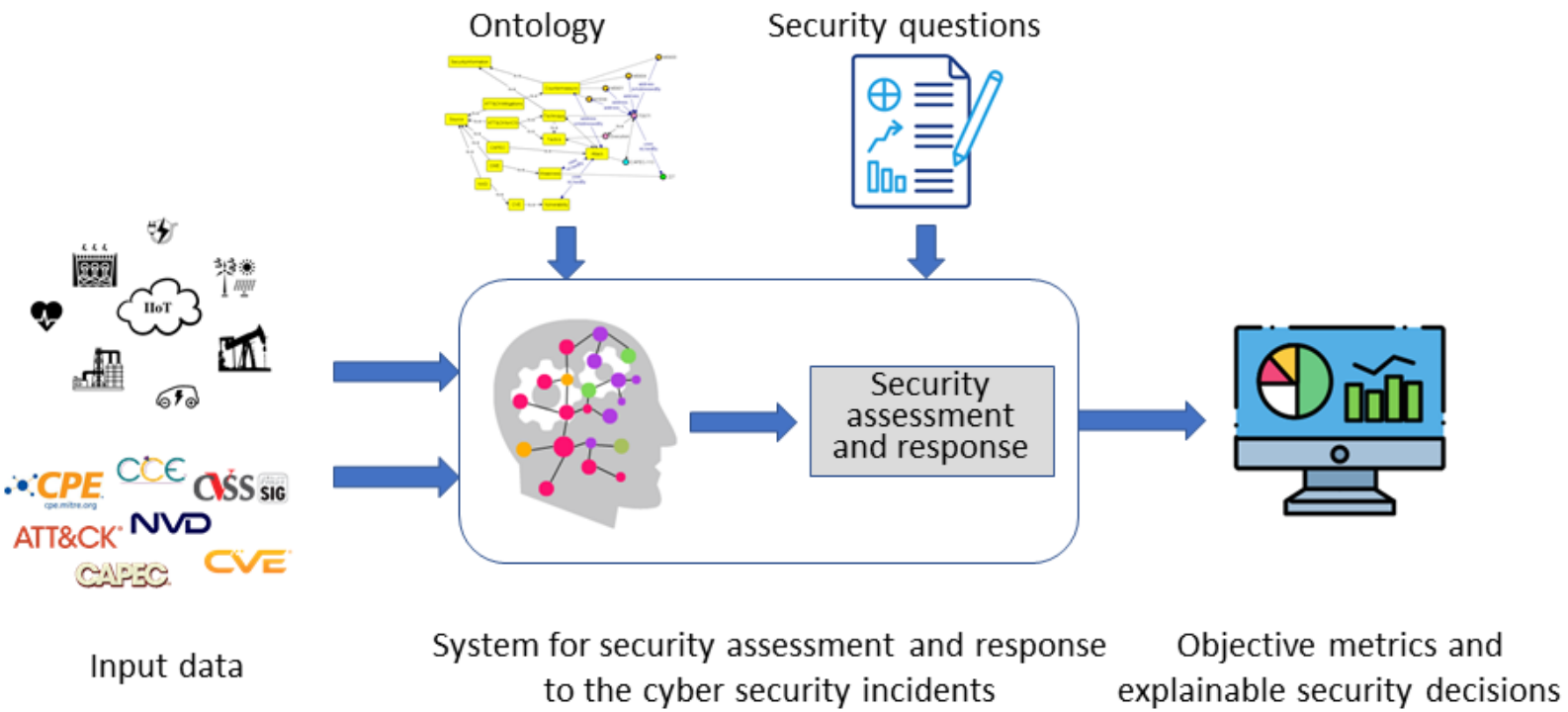
462 (%) эксплойта (Python) имеют связи с CVE.



Результаты

- Предложен подход к анализу исходных кодов эксплойтов и признаков их выполнения для формирования объективных оценок защищенности информационных систем
- Выполнены первые четыре этапа подхода
- ведется формирование тестовой среды для выполнения эксплойтов и определения признаков их выполнения в системе, для формирования показателей, основанных на признаках выполнения эксплойтов
- Проведение экспериментов позволит определить признаки выполнения эксплойтов и определить следующую группу показателей защищенности на их основе
- Показатели лягут в основу методики прогнозирования атакующих воздействий, а также автоматизации принятия решений по повышению защищенности.

Будущие исследования



Спасибо за внимание!

Контактная информация:

Е. В. Федорченко: doynikova@comsec.spb.ru

Е. С. Новикова: esnovikova@etu.ru

Исследование выполнено за счет гранта Российского научного фонда (проект No 23-21-00498)