УДК 004.056

Т.М. Пестунова, В.В.Селифанов, И.С.Слонкина, Я.В. Юракова

Россия, г. Новосибирск, Новосибирский государственный университет экономики и управления «НИНХ»

АВТОМАТИЗИРОВАННАЯ ТЕХНОЛОГИЯ СОПОСТАВЛЕНИЯ УГРОЗ И УЯЗВИМОСТЕЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В работе решается проблема построения прямых связей между уязвимостями и угрозами информационной безопасности на основе сведений в банке угроз ФСТЭК России [4]. Авторами разработан оригинальный алгоритм для автоматизированного решения данной задачи, реализованный в виде web-приложения. Предложенная технология позволяет существенно снизить трудозатраты и сократить количество ошибок, связанных с человеческим фактором при оценке соответствия угроз и уязвимостей. Ключевые слова: информационная безопасность, угрозы безопасности информации; уязвимости; банк данных угроз ФСТЭК России.

Введение

При идентификации актуальных угроз в различных ИС, как правило, учитываются следующие характеристики: источник угрозы; уязвимости, способствующие ее возникновению; способ реализации угрозы; последствия деструктивного воздействия. Такая форма представления сведений об угрозе используется в «Банке данных угроз безопасности информации» (далее – БДУ) [4]. Он содержит сведения об основных угрозах и уязвимостях, характерных, в первую очередь, для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

Для определения актуальных угроз нужно установить корректные взаимосвязи между характеризующими их параметрами. В работе [5], в частности, представлена структурная модель идентификации угроз, отражающая процесс её реализации от инициирования до последствий. В описании угрозы в БДУ содержатся сведения о типе нарушителя и его потенциале, способе реализации и возможных последствиях, что позволяет построить модель нарушителя и установить взаимосвязи между перечисленными параметрами угрозы.

Качественно иная ситуация имеет место при сопоставлении угроз и уязвимостей, так как соответствующие каталоги представлены в БДУ обособлено. Установление вручную связи между уязвимостями и угрозами в таких условиях является крайне трудоемкой задачей. На сегодняшний день соответствующие каталоги содержат сведения о более, чем 200 угрозах и 16 000 уязвимостях, а сопоставление уязвимости и угрозы можно реализовать только посредством «поиска по тегам» [1]. Создание автоматизированной технологии сопоставления угроз и уязвимостей с использованием БДУ направлено на снижение трудоёмкости процесса создания модели угроз.

Цель работы: разработка алгоритма для автоматизированного анализа и сопоставления угроз и уязвимостей на основе электронного ресурса БДУ и его реализация в виде программного приложения.

1. Алгоритм автоматизированного анализа и сопоставления угроз и уязвимостей

Предлагаемый авторами алгоритм для автоматизированного анализа и сопоставления угроз и уязвимостей, включает шесть этапов.

На первом этапе оператор ИС формирует запрос, содержащий сведения о программном (аппаратном) средстве с указанием формы прохождения процедуры аутентификации, способа и уровня сложности получения доступа.

На втором этапе происходит обработка запроса и осуществляется выборка уязвимостей из БДУ в соответствии с введенными параметрами.

На третьем этапе вычисляется значение базовой метрики вектора «CVSS», основываясь на том факте, что сведения предоставленные оператором на этапе построения запроса полностью коррелируют с полями записи об угрозе в БДУ, за исключением сведений о программном или аппаратном средстве.

На четвертом этапе, исходя из полученных значений базовой метрики вектора CVSS и имеющихся сведений об уязвимости в БДУ, исключаются те угрозы, у которых этот показатель отличен от значения, заданного в 157нновациях об уязвимости. Для расчета значения базовой метрики вектора CVSS используется формула [3]:

$$Base\ Score = RoundUp_1(Minimum[1{,}08\times(Impact + Exploitability), 10]),$$

где $RoundUp_1(Minimum\ [\ ])$ – функция округления (до десятков в меньшую сторону),

Impact – оценка последствий реализации, а именно влияние на конфиденциальность ($Impact_{Conf}$), целостность ($Impact_{Integ}$), доступность ($Impact_{Avail}$) – вычисляется по формуле:

$$7{,}52 \times [ISC_{Base} - 0.029] - 3{,}55 \times [ISC_{Base} - 0{,}02]^{15},$$

где

$$ISC_{Base} = 1-[(1-Impact_{Conf}) \times (1-Impact_{Integ}) \times (1-Impact_{Avail})],$$

Exploitability – оценка нарушителя (вычисляется по формуле:

$$8{,}22 \times Attack\ Vector\ (Способ\ получения\ доступа) \times$$
$$Attack\ Complexity\ (Сложность\ получения\ доступа) \times$$
$$Privilege\ Required\ (Аутентификация)).$$

На пятом этапе осуществляется отсеивание угроз на основе обобщенной матрицы парных сравнений «Типа программного обеспечения» (запись об уязвимости в БДУ) и «Объекта воздействия» (запись об угрозе в БДУ). В качестве критичного значения установлен коэффициент равный 0.5: если на пересечении соответствующих строк и столбцов матрицы результат сравнения не превышает 0.5, угроза отбрасывается, т.к. не связана с выбранным типом программного обеспечения.

На шестом (заключительном) этапе формируется итоговая таблица, содержащая сведения об угрозах и уязвимостях, способствующих её реализации и актуальных для данной ИС.

2. Программная реализация алгоритма

Разработанный алгоритм реализован в виде программного приложения «ThreVulSec», написанном на языке «Python 2.7.8» с использованием поискового движка «ElasticSearch». В таблице 1 приведены основные сведения о программной реализации. Выбор движка обусловлен его быстродействием и стойкостью к высоким нагрузкам. Дополнительно реализована функция сохранения полученных результатов на рабочей станции в формате «xlsx».

При инсталляции «ThreVulSec» на персональный компьютер в зависимости от операционной системы должен быть установлен «Python 2.7.8» (для Unix-систем) или интерпретатор «Python 2.7.8» (при работе в MS Windows). Далее следует загрузить модули «ElasticSearch 1.7.2», «JRE 7», «Flask». Установка производится путем запуска файла «control/setup.py».

Перед первым запуском программы оператор должен обновить базу данных посредством запуска скрипта «control/renewDB.py». Далее обновление производится по мере необходимости.

При появлении новых типов программного обеспечения обновление обобщенной матрицы парных сравнений выполняется путем запуска «control/match_table». Заполнение матрицы происходит с использованием метода экспертной оценки [2]. По умолчанию используется обобщенная матрица парных сравнений, заполненная разработчиками. Оператор ИС должен выбрать из раскрывающегося списка следующие данные: название программного продукта или аппаратной платформы; его версию; производителя (вендора), способ получения доступа с оценкой сложности его получения; сведения о процедуре прохождения аутентификации.

3. Пример расчёта

Апробация была проведена на множестве примеров, один из них представлен ниже. В примере рассматривается web-браузер Firefox версии до 45.0.

Для сравнения осуществлялся поиск прямых связей между уязвимостями и угрозами вручную («поиска по тегам»), в результате которого выявлена 41 уязвимость. Для поиска угроз по каждой уязвимости составлялся список тегов, затем осуществлялся поиск угроз. В частности, для одной из уязвимостей потребовалось оценить 11 угроз на соответствие. В процессе анализа угрозы УБИ.001-005 и УБИ.009-010 были отброшены из-за несоответствия типа программного обеспечения и объекта воздействия. Посредством более детального анализа сведений об угрозах УБИ.007-008 был сделан вывод об их неактуальности для рассматриваемой уязвимости. В результате только 2 из 11 найденных угроз оказались актуальными – при относительно общих формулировках тегов в результатах поиска часто выводятся угрозы, не связанные с рассматриваемой уязвимостью. При вводе уточнённых формулировок тегов множество угроз становилось неполным или вообще пустым (например, при использовании тега «произвольный код», встречающегося в описании уязвимости, угроз в БДУ обнаружено не было). В целом, время, затрачиваемое на сопоставление всех угроз и уязвимостей «вручную» составило более 2 часов. Использование разработанного программного приложения «ThreVulSec» позволило выполнить всю работу за 20 секунд при более качественном выборе перечня угроз, тем самым существенно сократив трудозатраты оператора и повысить качество полученных результатов.

Выводы

Разработана автоматизированная технология, включающая алгоритм автоматизированного анализа и сопоставления угроз и уязвимостей, реализующее его программное приложение «ThreVulSec», а также рекомендации по его использованию, который использован для определения актуальных угроз безопасности информации на основе БДУ.

Сравнительный анализ «поиска по тегам» вручную и предложенной технологии показал значительное сокращение времени на анализ угроз и уязвимостей при её применении. Повышение качества анализа угроз достигается за счёт направленного автоматического поиска по заданным параметрам используемых информационных технологий, а также уменьшения ошибок, связанных с человеческим фактором. Примерами таких ошибок являются субъективная оценка соответствия угрозы найденной уязвимости, неточное определение ключевых слов (тегов) для поиска, невнимательность оператора по причине переутомленности от работы с большим количеством данных и ряд других.

Литература

1. Селифанов В.В., Слонкина И.С., Юракова Я.В. Определение актуальных угроз безопасности информации в информационных системах, используя Банк данных угроз (bdu.fstec.ru) // Электронные средства и системы управления (ЭсиСУ-2016): Материалы XII Международной научно-практической конференции. – Томск, 2016. – №2 – с. 67-69.

2. Ельмеев В.Я. Прикладная социология: Очерки методологии / Ельмеев В.Я., Овсянников В.Г. — 2-е изд., испр. и доп. — СПб.: Изд-во С.-Петербургского государственного университета, 1999. — 276 с.

3. First (Forum of Incident Response and Security Yeams) – Common Vulnerability Scoring System [Электронный ресурс]. – URL: https://first.org/cvss (Дата обращения: 12.01.2016 г.)

4. Банк данных угроз ФСТЭК России. [Электронный ресурс], – URL: https://bdu.fstec.ru.

5. Курносов К.В., Пестунова Т.М. Модель идентификации угроз виртуальной инфраструктуры // Сб. трудов научно-практ. конфер. Росинфоком – 2016. «Информационная безопасность в современном обществе». – Новосибирск: ФГБОУ СибГУТИ, 2016. – с. 45-49.