Подход к оценке защищенности критических документов на основе профиля компетенций злоумышленника

Ф. В. Бушмелев[1], Т. В. Тулупьева[2]
СПбГУ, СПИИРАН
[1]fedebushe@gmail.com, [2]tvt100a@mail.ru

А. А. Азаров
СПИИРАН
artur-azarov@yandex.ru

***Аннотация*. В статье рассматривается подход к оценке защищенности кричных документов, хранимых в информационной системе, на основе данных о профиле компетенций злоумышленника и профиле уязвимостей пользователя. Рассматривается модель процесса, при которой злоумышленник с помощью доступных ему методов воздействия на пользователей информационных систем (социоинженерных атакующих воздействий на пользователей) пытается получить доступ к таким документам. Рассматривается агрегированная оценка вероятности получения такого доступа через социоинженерные атакующие воздействия на различных пользователей информационной системы.**

Ключевые слова: социоинженерные атаки; информационная безопасность; защита информации; критические документы

I. Введение

В 20 веке было сделано множество важных открытий. Все они вошли в повседневную жизнь людей. Одним из итогов таких открытий стало формирование компьютерных систем, которые хранят, обрабатывают и передают информацию. Столь стремительный темп развития информационных технологий заставляет все больше внимания уделять вопросам информационной безопасности. Причинами этого служит то, что за последние годы, в значительной мере увеличилось число атак на информационные системы. Всё больше требуется средств и временных затрат для расследования и устранения последствий от подобного рода атак.

Сегодня вопрос по обеспечению безопасности и конфиденциальности информации стоит наиболее остро. Большая часть исследований, направленных на решение этой проблемы, имеет программно-технический характер [7, 8]. Надо отметить, что имеются очень серьезные наработки по этому вопросу, получены значимые результаты, но исследования продолжаются с не меньшей интенсивностью.

К сожалению, не смотря на все вышеупомянутые достижения, СМИ в изобилие рассказывают о самых разных и необычных инцидентах, связанных с нарушениями информационной безопасности [1, 9]. Когда поднимается вопрос о защищенности информационной системы, чаще всего имеют ввиду программно-технические аспекты, забывая, что пользователь также является субъектом информационной системы и имеет непосредственное влияние на уровень ее защищенности. Таким образом, становится актуальной проблема по защите пользователей, и как результат – информации, от социоинженерных атак, т.е. атак, основной целью которых является персонал информационных систем.

Для всестороннего изучения вопросов связанных с социоинженерными атаками командой исследователей Лаборатории теоретических и междисциплинарных проблем информатики Санкт-Петербургский института информатики и автоматизации РАН был разработан прототип программного комплекса, моделирующий социоинженерные атакующие воздействия на пользователей информационной системы [2, 4]. В основе лежит набор моделей: «критические документы – информационная система – персонал – злоумышленник». Дальнейшая цель исследования заключается в определении уровня защищенности информации, хранимой в информационной системе, на основе имеющихся сведений об уровне проявления уязвимостей пользователей этой системы.

Задача, решенная в этой статье – рассмотрение подхода (раздел I), вариативности его интерпретаций в зависимости от структуры социоинженерной атаки (раздел II), и обработка полученных результатов (раздел III). Данный подход позволит получить вероятностные оценки компетенций злоумышленника и вероятностные оценки получения им несанкционированного доступа к критическим документам через социоинженерные атакующие воздействия на различных пользователей информационной системы.

II. Описание подхода к оценке

Как было отмечено ранее, важным аспектом в анализе защищенности информационной системы является возможность вывода оценок защищенности критичных документов, хранимой в данной системе. Очевидно, что

Работа выполнена в рамках проекта по государственному заданию СПИИРАН № 0073-2018-0001, при финансовой поддержке РФФИ, проект №18-37-00323; и проект №18-37-00340

определение критичности документов – отнесение их к той или иной категории по уровню критичности – может быть осуществлено различными способами. Одним из часто используемых методов выделения категорий критичности информации, хранящейся в системе, является финансовая оценка возможного ущерба, который может быть нанесен при получении несанкционированного доступа злоумышленника к некоторому критичному документу.

Для оптимальной оценки защищенности критичной информации предлагается принимать в рассмотрение не только степень выраженности уязвимостей пользователей информационных систем, но и вероятностные оценки сил и средств, которыми обладает злоумышленник. Будем считать, что социоинженерная атака была успешно проведена, и доступ к некоторому документу злоумышленником получен. Необходимо установить какими минимально возможными ресурсами мог обладать такой злоумышленник. Для этого будем использовать модель «злоумышленник», одной из составляющей которого является профиль компетенций злоумышленника (ПКЗ): набор пар «степень владения атакующим действием» – «максимальная степень владения атакующим действием».

В рассматриваемой задаче будет использовано представление информационной системы, приведенное в [3, 5]. На рис.1 приведен пример графа социальных связей пользователей информационной системы, где узлы — это пользователи, обладающие всеми характеристиками модели «персонал», в том числе моделью профиля уязвимостей пользователя (ПУП): набор пар «уязвимость» – «выраженность уязвимости»; а дуги графа – это вероятности перехода социоинженерной атаки от пользователя к пользователю.

Перестроим граф для визуализации предлагаемого подхода. Преобразуем граф к корневому, корнем которого будет являться критический документ, а сыновьями пользователи, имеющие к нему доступ, а их сыновья, пользователи, связанные с помощью дуг и т.д. Например, пусть пользователи 1,4 и 8 имеют доступ к критичному документу. Тогда граф может быть представлен в виде рис. 2.

Рассмотрим алгоритм предлагаемого метода. Установив метку текущего положения в корень, будем двигаться вниз, вычисляя возможные точки входа для атаки.

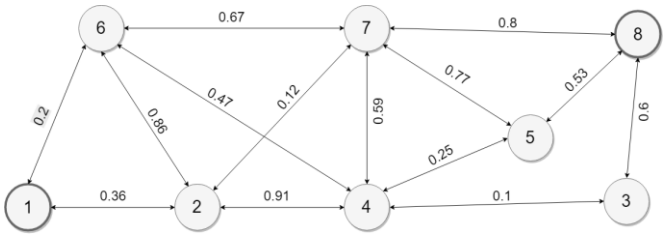

Рис. 1. Пример графа межличностных связей персонала информационной системы.

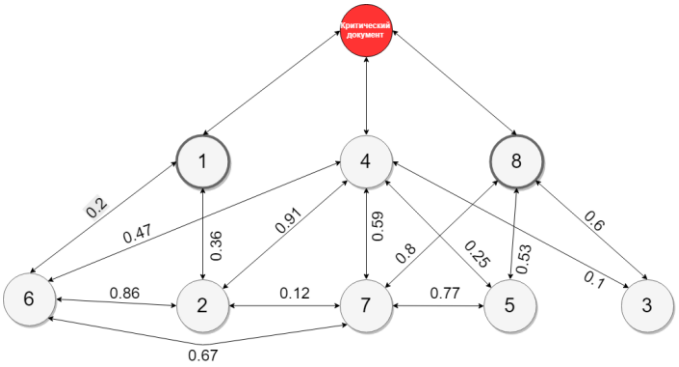

Рис. 2. Пример преобразованного графа межличностных связей персонала с выделением некоторого критического документа

Для корня необходимо рассмотреть всех соседей на некотором расстоянии s от него, где $s \in [0, V-1]$, V – мощность множества вершин графа. Достигнув некоторой вершины, высчитывается вероятностные оценки параметров ПКЗ.

III. Вариативность подхода

Обнаружив вершины, связанные с корнем, непосредственно формируем запись $\left\langle id_r^s, \{K_i, D(K_i)\}_{i=1}^m, p_r^s \right\rangle$, где id_r^s – уникальное имя злоумышленника, а r – последовательность вершин длины $s+1$, $\{K_i, D(K_i)\}_{i=1}^m$ – ПКЗ, $D(K_i)$ – степень владения i-м атакующим действием, а p_r^s – вероятность достижения данной конфигурации степеней владения атакующими действиями последовательности r. Для описания метода, рассматриваемого в этой статье, предполагаем, что пользователь уже успешно атакован злоумышленником, и им уже получен доступ к критичной информации, которой обладает пользователь. То есть, не умаляя общности мы считаем, что вероятность этого события 1. Тогда, имея ПУП – из информационной системы, информацию о влиянии атакующих действий на уязвимости [6] и прочие сведения, необходимо будет решить экстремальную задачу и найти $D(K_i)$, иными словами: При $P_j = 1$, необходимо найти такие значения $D(K_i) \to \min$, где P_j – вероятность того, что j-й пользователь был успешно атакован.

Важно отметить, что подход может иметь несколько вариаций для расчета p_r^s и $D(K_i)$ в зависимости от условий организации атаки. Не умаляя общности, рассмотрим следующее.

Злоумышленник на всем пути, успешно атакует каждого пользователя по цепочки. Напомним, мы идем от корня к листьям, от документа к первому вхождению. При переходе по дуге приходится вести расчет $D(K_i)$ для каждого пользователя, и модифицировать значение с учетом ранее полученной выраженности компетенции.

Частный случай:

Примером вариативности может послужить социоинженерная атака, передающаяся посредствам инсайдерской атаки. Мы по-прежнему считаем, что документ успешно захвачен злоумышленником, имеется некая цепочка из $s+1$ узлов, тогда $p_r^s = \prod_{t \in r} p_t$, где p_t – вероятность передать атаку от пользователя к пользователю, t – пара смежных вершин из цепочки r. Подобная вероятность получается в результате инсайдерской атаки, где злоумышленнику необходимо атаковать только одного пользователя, в цепочке его номер будет последним, и дальнейшее распространение атаки происходит без значимых затрат для злоумышленника. Вычисление $D(K_i)$ потребуется выполнить только один раз.

IV. Агрегация записей

Агрегация записей идет с самого первого шага алгоритма. Можно выделить несколько свойств:

- Если при формировании записей с длиной цепочки записи длины $s+1$ вероятность p_r^s меньше порогового значения, например, 0.05, тогда эта запись не учитывается.
- Ввиду того, что для длинных цепочек, например длины 5 и более, вероятность p_r^s так же будет меньшее порогового значения, такие записи учитываться так же не будут.
- Мы получаем новую цепочку длины $s+2$ путем рассмотрения возможных цепочек длины $s+1$, и перехода из текущей вершины в любую из смежных к ней, которая была не посещена ранее. Для всех новых цепочек создаются записи.
- После получения всех возможных цепочек, производится склеивание записей с одинаковыми конечными звеньями цепочек. И после производится агрегация для всех записей, ведущих к рассматриваемому критическому документу.

После завершения работы алгоритма, будет получена одна запись с вероятностными оценками профиля компетенций злоумышленника.

Также приходится иметь в виду тот факт, что современные информационные системы могут насчитывать сотни, и даже тысячи сотрудников, а каждый шаг алгоритма требует существенных временных затрат, даже на оборудовании высокой вычислительной мощности, не говоря обо всем подходе в целом. Для частичного решения данной проблемы видится возможным несколько вариантов оптимизации:

- Предварительно использовать алгоритм обхода графа в глубину с некоторыми модификациями. При обходе вычисляется ПКЗ, и каждой дуге присваивается $(K_i, \overline{D(K_i)})$, где $\overline{D(K_i)}$ – разница между наборами $D(K_i)$ инцидентных этой дуге вершин. И уже при непосредственной работе алгоритма можно получить результат посредствам простого суммирования.
- Использовать представление набора моделей «критические документы – информационная система – персонал – злоумышленник», где используется деление пользователей по контролируемым зонам. Поэтому, можно осуществлять распределенную обработку по таким зонам.

Заключение

В ходе исследования был получен подход, позволяющий сформировать вероятностные оценки профиля компетенций злоумышленника достаточного для достижения им критичной информации определенного уровня критичности.

Список литературы

[1] Phil Muncaster. UK Fraud Attacks Hit 20 Million in Q2. [Электронный ресурс] // URL: https://www.infosecurity-magazine.com/news/uk-fraud-attacks-hit-20-million-in/ (дата обращения 16.03.2018)

[2] Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищённости персонала информационных систем от социоинженерных атак //Информационно-управляющие системы. 2016. №4. С. 77–84.

[3] Абрамов М.В., Азаров А.А., Фильченков А.А. Распространение социоинженерной атаки злоумышленника на пользователей информационной системы, представленных в виде графа социальных связей // Сборник докладов Международной конференции по мягким вычислениям и измерениям (SCM-2015). Санкт-Петербург. Том 1–2. 2015. С. 329–332.

[4] Азаров А.А., Абрамов М.В., Тулупьева Т.В., Фильченков А.А. Применение вероятностно-реляционных моделей комплекса «критичные документы – информационная система – пользователь – злоумышленник» для анализа защищенности пользователей информационных систем от социо-инженерных атак // Нечеткие системы и мягкие вычисления. 2015. Т. 10. № 2. С. 209–221.

[5] Азаров А.А., Тулупьев А.Л., Соловцов Н.Б., Тулупьева Т.В. Ускорение расчетов оценки защищенности пользователей информационной системы за счет элиминации маловероятных траекторий социоинженерных атак // Труды СПИИРАН. 2013. 2(25). С. 171-181.

[6] Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки. Проблемы анализа. СПб.: Наука, 2016. 352 с.

[7] Котенко И.В., Степашкин М.В. Перспективные направления исследований в области компьютерной безопасности. // Защита информации. 2006. N 2. С. 46-57.

[8] Котенко И.В., Степашкин М.В., Богданов В.С. Системы-имитаторы: назначение, функции, архитектура и подход к реализации. // Изв. вузов. Приборостроение, Т. 49. 2006. N.3. С. 3-8.

[9] Митник К.Д., Саймон В.Л. Искусство обмана. М.: Компания АйТи, 2004. 416 с.