УДК 621.391(075.8)

Воробьев Антов Александрович
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Аспирант
E-Mail: zeromem@mail.ru

Трещев Иван Андреевич
ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»
Россия, Комсомольск-на-Амуре
Заведующий кафедрой «Информационная безопасность автоматизированных систем»
Кандидат технических наук
E-Mail: kalkt@yandex.ru

О подходе к построению таксономии уязвимостей технических систем

Аннотация. В данной работе проведен обзор классификаций уязвимостей, атак и инцидентов связанных с ними в технических системах. Освещены подходы к классификации Аттансио, Андерсона, Хэнсмена, Бишопа и других к категорированию уязвимостей технических систем. Предлагается модифицированная многомерная таксономия уязвимостей систем.

Ключевые слова: информационная безопасность; уязвимость; атака; инцидент.

Введение

Защита информационных ресурсов от угроз безопасности на сегодня является одним из приоритетных направлений, как отдельного предприятия, так и государства в целом.

На сегодня регулирование деятельности по защите информации на автоматизированных объектах информатизации в Российской Федерации осуществляет Федеральная служба по техническому и экспортному контролю России (ФСТЭК) при поддержке ГНИИИ ПТЗИ ФСТЭК России, которая разработала ряд руководящих(РД) и нормативных документов(НД). Среди последних, основополагающими являются документы о базовой модели угроз информационных систем персональных данных (ИСПДн) и ключевых систем информационной структуры (правительственные объекты и объекты, непосредственно влияющие на обороноспособность государства). В соответствии с РД и НД, частным случаем угрозы является понятие уязвимости, применяемое к информационным системам (ИС), - "свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации" или "некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации"[1].

Количество и разнообразие различных технических систем(ТС) с течением времени становится необозримым вследствие всеобщего проникновения науки в современную жизнь человека, что приводит к необходимости разработки их классификаций с целью систематизации информации.

Интерес к данной систематизации порождается двумя связанными между собой причинами. Во-первых, наличие классификации объектов анализа в определенной области знаний является значимым акселератором скорости ее познания. Во-вторых, через разработку классификаций устанавливаются «интеллектуальные» границы области знаний.

Однако в областях системотехники для оценки производительности технических систем используются показатели качества, которые представляются нефункциональными к системе требованиями. Примером данных показателей являются показатели безопасности, надежности, развёртываемости, модернизируемости, защищенности, уязвимости и др.

В частности, в области информационных технологий под уязвимостью понимается недостаток в вычислительной системе, используя который возможно нарушить ее целостность и вызвать некорректную работу. Попытка реализации уязвимости называется атакой.

Классификация уязвимостей

С целью изучения и анализа областей знаний о технических системах, исследователи предлагают различные виды классификаций. Формально, задача классификации состоит в создании системы категорирования, а именно, – в выделении категорий и создании классификационной схемы, как способа отнесения элемента классификации к категории.

При использовании заданной терминологии, неизбежно возникают разночтения между понятиями классификация и классификационная схема. Для устранения данного недостатка, в дальнейшем, используется термин «таксономия». Данный термин имеет греческое происхождение: от слов taxis – порядок и nomos – закон [1].

Таксономия [2] – это «классификационная схема, которая разделяет совокупность знаний и определяет взаимосвязь частей». Таким образом, вопрос выделения универсальной классификационной схемы технических систем остается открытым.

Вследствие данного факта, исследователями приводятся классификационные схемы, охватывающие лишь малую часть предметной области, на которую они ориентируются.

К примеру, в области информационных технологий, при оценке их уязвимости к внешним факторам, выделяются три группы таксономий:

- таксономии атак;
- таксономии уязвимостей;
- таксономии инцидентов.

К проблеме классификации атак имеется несколько подходов. Классически атаки разделяют на категории в зависимости от производимого эффекта:

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- отказ в обслуживании (нарушение доступности информации).

Главным недостатком подобной классификации является слабая информативность (а, следовательно, и применимость), так как по информации о классе атаки практически невозможно получить информацию об ее особенностях. Однако, эффект атаки является важным ее свойством и данный параметр в том или ином виде применяется в ряде таксономий.

Другим подходом к классификации является классификация уязвимостей аппаратного и программного обеспечения информационно–вычислительных и телекоммуникационных систем. Однако данный подход является слишком узким и зачастую не отражает в должной мере специфику атаки, поэтому применяется, в основном, лишь для специальных классов задач (при тестировании программного обеспечения и др.).

Другим возможным вариантом классификации является деление на основе начального доступа, которым обладает атакующий. Таким образом, категория, к которой принадлежит атака, зависит от начальных привилегий атакующего.

В силу необходимости практической применимости таксономий, наиболее выгодными считаются комбинированные подходы, которые в некоторой степени реализуют все вышеописанные методы. Однако, способы комбинирования методов могут быть различны.

Один из способов комбинирования приводится в своей работе Хэнсмэн, – все анализируемые параметры разносятся отдельно и считаются попарно некоррелированными[3]. Для достижения данной цели, автор использует концепцию «измерений.

Главную цель, которую преследовал Хэнсмэн, была разработка «прагматичной таксономии, которая полезна при ведении непрерывной работе над атаками» [3].

Первоначально производилась разработка таксономии древовидной структуры, подобно классификациям природного царства, – более общие категории находятся выше по высоте дерева, а нижние по высоте представляют более подробное описание категорий. Но на практике, в применении подобных классификационных схем имеется ряд неудобств. Во–первых, атаки зачастую несут смешанный характер. То есть складывается ситуация, при которой одна атака тесно зависит от другой или вложена в нее. Данная проблема, с одной стороны, решается путем введения межузловых ссылочных дуг между вершинами дерева, то есть при заполнении классификационной схемы образуется нагруженный граф. Однако это неизбежно сводится к беспорядку в структуре и сложностям при классификации. С другой стороны, возможно введение рекурсивных деревьев, где каждый лист дерева также является деревом. Но данное решение также сводится к беспорядочному росту структуры, и ограничению их применения. Во–вторых, атаки, не имеют обширного числа общих черт, вследствие чего имеют место сложности в формулировке классификационных групп верхних уровней. Действительно, у вредоносных программ типа «черви» или «вирусы» имеется

достаточного много общих черт, однако непосредственных аналогий с атаками типа DoS(Denial of Service – отказ в обслуживании) и троянскими программами у них немного. Данная проблема ведет к разрастанию дерева на некоторое количество несвязанных между собой категорий, то есть до леса.

Иной подход к созданию таксономий заключается в виде использования списочных структур. Таксономии, основанные на списочных структурах, представляются как совокупность списков категорий атак. С одной стороны, возможна организация общих классов категорий атак, с другой – возможно создание объемного количества списков, каждый из которых детально описывает уникальный класс категорий. Данные подходы также слабо применяются на практике, так как для первого случая организуются наборы крайне обобщенных категорий атак, а во–втором случае, детализация списков категорий бесконечна.

В предлагаемой Хэнсмэном таксономии используется иной подход, основанный на концепции «измерений» Бишопа. Введение «измерений» позволяет комплексно рассматривать каждую атаку отдельно. В таксономии рассматривается четыре измерения для классификации атак:

1. первое (базовое) измерение используется для категорирования атаки относительно классов атак на основе вектора атаки. Под вектором атаки понимается метод, с помощью которого атака достигает своей цели. При отсутствии подходящего вектора, атака классифицируется в ближайшую по смыслу категорию;
2. вторым измерением, атака классифицируется по цели атаки. Степень детализированности измерения достигается указанием конкретной версии продукта, например Linux Kernel 3.5.1rc–1, или же покрывается определенным классом возможных целей, например Linux Kernel;
3. третье измерение используется для описания уязвимостей и эксплоитов, которыми реализуется данная атака. Измерение представляется списоком номеров CVE(Common Vulnerabilities and Exposures) известных уязвимостей по классификации проекта CVE.

Дополнительно, в таксономии Хэнсмэна предполагается ситуация, когда на момент классификации атаки не существует ее описания (CVE–номера) уязвимости. В этом случае, предлагается использовать общие классы категорий атак процессной таксономией компьютерных и сетевых атак Ховарда [3], – уязвимость в реализации (логические ошибки в текстах программ), уязвимость в проекте, уязвимость в конфигурации. В данной таксономии рассматривается в качестве центрального понятия инцидент – совокупность атакующего, атаки и цели атаки. Главным ее отличием является наличие структурных элементов: инцидентов и события, – совокупности действия и целевого объекта. Предусматривается возможность комбинирования событий. Таким образом, в инциденте возможно вложение последовательность атак. Полезным свойством таксономии Ховарда является возможность описания неатомарных (составных) атак и учет их сценариев проведения.

4. Четвертое измерение используется для классификации атаки по наличию и виду полезной нагрузки (payload) или реализуемого эффекта. В большинстве случаев, в результате своей работы, с атакой привносится дополнительный эффект. Например, «вирус», используемый для установки «потайного входа» (backdoor) очевидно остается «вирусом», но несет в качестве полезной нагрузки программу «потайного входа».

В 1995 году, Бишоп [4] предложил классификацию относительно уязвимостей для UNIX–систем. Отличительная особенность его работы заключается в создании принципиально новый схемы классификации. Шесть «осей координат» представляются компонентами[4]:

1. Природа уязвимости – описывается природа ошибки в категориях протекционного анализа;
2. Время появления уязвимости;
3. Область применения – что может быть получено через уязвимость;
4. Область воздействия – на что может повлиять уязвимость;
5. Минимальное количество – минимальное количество этапов, необходимых для атаки;
6. Источник – источник идентификации уязвимости.

Авторами предлагается использовать комбинированный подход к классификации уязвимостей, в котором для построения таксономии выделяются категории классификаций элементов области знания, где каждая категория со своими компонентами «проецируется» на некоторую ось многомерного пространства, причем каждому отсчету оси соответствует своя компонента категории. В предлагаемой таксономии используется n-мерное пространство, где каждому измерению соответствует категория атаки, а отсчетами по осям являются компоненты категорий атак. Данный подход является обобщением идей, предложенных Бишопом и Хэнсмена, существенно расширяя их в области использования многомерных пространств. Каждая атака на конкретную техническую систему, представляет из себя, точку введенного пространства и для каждой системы мы имеем собственное пространство. Для оценки угроз могут использоваться классические многомерные метрические пространства с существующими метриками, например метрика Хаусдорфа.

Заключение

Комбинированный подход к классификации уязвимостей прослеживается и в нормативно–распорядительной документации ФСТЭК России. В классификации уязвимостей, предлагаемой базовой моделью угроз ИСПДн, также применяется комбинированный подход, основанный на идеях работ Ховарда, Хэнсмэна, Бишопа и др.

Более того, для систематизации уязвимостей в соответствии с классификацией на практике, в документах предлагается использовать существующие зарубежные базы данных(БД) уязвимостей в качестве источников информации. Наиболее распространенной базой данных об уязвимостях является БД National Vulnerability Database(NVD), которая основывается на объединении информации из более ранних баз данных (CPE, CVE, и др.).

Предложенная авторами таксономия является перспективной с точки зрения практического применения и возможности оценки наиболее актуальных угроз.

ЛИТЕРАТУРА

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия – Телеком, 2004. 280 с.
2. Варлатая С.К., Шаханова М.В. Программно–аппаратная защита информации: учеб. пособие. Владивосток: ДВГТУ, 2007. 318 с.
3. Hansman S. A taxonomy of network and computer attacks methodologies // University of Canterbury. New Zealand. 2003.
4. Bishop M and Bailey D, "A Critical Analysis of Vulnerability Taxonomies," Department of Computer Science, University of California at Davis, Technical Report CSE–96–11, 1996.

Anton Vorobyev
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: zeromem@mail.ru

Ivan Treschev
Komsomolsk-on-Amur state technical University
Russia, Komsomolsk-on-Amur
E-Mail: kalkt@yandex.ru

An approach to the construction of a taxonomy of vulnerabilities of technical systems

Abstract. In this paper, a review of the classification of vulnerabilities, attacks and incidents related to technical systems. Covered approaches to classification Attansio, Anderson Hensmena, Bishop and others to the categorization of vulnerabilities of technical systems. A modified multi-dimensional taxonomy of system vulnerabilities.

Keywords: Information security; vulnerability; attack; incident.

REFERENCES

1. Maljuk A.A. Informacionnaja bezopasnost': konceptual'nye i metodologicheskie osnovy zashhity informacii. M.: Gorjachaja linija – Telekom, 2004. 280 s.
2. Varlataja S.K., Shahanova M.V. Programmno–apparatnaja zashhita informacii: ucheb. posobie. Vladivostok: DVGTU, 2007. 318 s.
3. Hansman S. A taxonomy of network and computer attacks methodologies // University of Canterbury. New Zealand. 2003.
4. Bishop M and Bailey D, "A Critical Analysis of Vulnerability Taxonomies," Department of Computer Science, University of California at Davis, Technical Report CSE–96–11, 1996.