МОДЕЛИ И АЛГОРИТМЫ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ РАБОЧИХ СТАНЦИЙ И КОРПОРАТИВНЫХ СЕРВЕРОВ

Бозорова Феруза Хайдар қизи [*]

[*] *Магистр, Факультет кибербезопасности, Ташкентский университет информационных технологий имени Мухаммада аль-Хоразмий, Узбекистан*

Аннотация: *В последнее время системы обнаружения вторжений (IDS) были внедрены для эффективного защищенные сети. Использование нейронных сетей и машинного обучения для обнаружения и классификации вторжения являются мощными альтернативными решениями. В этой исследовательской работе оба метода Gradient спуск с импульсом (GDM) на основе обратного распространения (BP) и градиентный спуск с импульса и адаптивного усиления (GDM / AG) используются для обучения нейронные сети для работы как IDS. Чтобы проверить эффективность двух предложенных обучения , IDS на основе нейронной сети строится с использованием предложенного алгоритма обучения - риттмы . Эффективность обоих алгоритмов проверяется с точки зрения скорости сходимости к достичь системного обучения и затраченного времени обучения, используя различные настройки нейронной сети параметры . Результат показал, что алгоритм обучения BP на основе GDM/AG превосходит алгоритм обучения BP на основе GDM.*

Ключевые слова :*Системы обнаружения вторжений (IDS) Нейронные сети (NN) Обратное распространение (BP)*

Аннотация: *В настоящее время информационная безопасность организаций имеет большое значение в связи с тем, что доля участия человека на этапе принятия решений планирования и управления их деятельностью перемещается в область автоматизированных систем. Автоматизированным системам инвентаризации переданы не только отдельные заводы и другие узкоспециализированные производства, но и целые отрасли и министерства. Например, хорошо известна история Министерства обороны США, где использование автоматизированной системы для закупки продовольствия и другого невоенного оборудования давало некоторым поставщикам несправедливое преимущество, пусть даже явно завышенное. цена товара. Программное обеспечение, содержащее ошибки, представляет серьезную угрозу не только для отдельных субъектов хозяйствования, но и для всего государства. Еще одним бичом современного ПО является наличие недокументированных возможностей и дополнительных функций, которые могут быть использованы в злонамеренных целях «знающими» людьми. При сочетании этих механизмов с легальными возможностями различного программного обеспечения в организации*

высока вероятность получения несанкционированного доступа к конфиденциальной информации (АНА). Тогда ущерб и потери будут зависеть только от совершенства комплекса мер по борьбе с разрушительным воздействием нападающих.

Ключевые слова: *Информационный комплекс, Подсистема, Автоматизированная система, Связь между параметрами, Нарушитель, Модель Нарушителя, атака.*

Введение . Для многих систем концепция безопасности заключается в том, чтобы ограничить возможность внесения изменений в свои данные тем или иным образом. Таким образом, любое нарушение безопасного режима работы автоматизированной или автоматической системы (далее - АС) в первую очередь связано с нештатным изменением внутреннего состояния АС, т.е. если изначально информация в ¬АС обладает свойствами конфиденциальности, достоверности и доступности, то потеря любого из этих свойств объясняется изменениями, произошедшими в АС.

Именно с этой точки зрения предлагается анализ информационной системы, т.е. рассмотреть возможность несанкционированной модификации внутреннего состояния некоторой АС путем внутреннего или внешнего воздействия на нее. Преимуществом такого подхода является его универсальность по отношению к функциям защиты данных в АС. При необходимости можно уделить внимание анализу информационной системы для обеспечения конфиденциальности информации или ее достоверности или доступности, в любом случае меняются только параметры модели, но ее структура остается неизменной.

В настоящее время комплексный анализ систем на предмет несанкционированного изменения данных или их отсутствия затруднен отсутствием строгого математического аппарата, позволяющего проводить такую работу. Отсутствие строгого математического аппарата анализа объясняется сложностью взаимосвязей внутри систем и наличием непредсказуемых эффектов (человеческий фактор и др.). Выходом часто является построение логических моделей при существенном ограничении изучаемых параметров и влияющих факторов систем. В связи с этим многие важные особенности систем остаются вне поля зрения исследователей.

Материалы . Информационные системы с возможностью анализа исходного кода дают больше свободы для изучения их параметров безопасности, поскольку позволяют тщательно искать потенциальные уязвимости. Напротив, проприетарное ПО представляет собой «черный ящик», поэтому наличие в нем уязвимостей вероятно и, как правило, связано с противоправными действиями, т.е. нарушение законов об авторском праве и интеллектуальной собственности. Таким образом, при определении параметров безопасности подсистем CI мы руководствуемся

известными уязвимостями для каждой подсистемы. При таком подходе понимаются ситуации, когда настройки безопасности позволяют реализовать угрозу, вызванную уязвимостью. ¬Тогда основной задачей будет определение максимальной атаки с точки зрения последствий, которая может быть осуществлена через те или иные уязвимости.

Методы . во-первых, мы пытаемся определить, какие процессы следует описывать с помощью математической модели, а во-вторых, что следует обнаружить при решении описываемой ею задачи. Рассмотрим подробнее события, происходящие при запуске НРД. Первоначально злоумышленник выбирает подсистему «жертва», то есть определяет направление атаки. ¬Затем он влияет на параметры некоторых доступных ему подсистем, тем самым вызывая изменения в других подсистемах. Он распространяется от одной подсистемы к другой, в конечном итоге вызывая изменения в желаемой подсистеме. Перенос изменений из одной подсистемы в другую определяется несколькими факторами:

1. Сроки передачи изменений. После согласованного изменения параметров затрагиваемого набора и до момента изменения нужного параметра проходит ненулевое время, которое соответствует интервалу времени передачи изменения для данного параметра.

2. Вероятность обнаружения изменения параметра. При несанкционированном изменении одного или нескольких параметров может быть нарушена логика работы всей или отдельных функциональных частей подсистемы, имеется возможность обнаружения нарушения параметров данной подсистемы. Соответственно, эту вероятность следует учитывать при анализе комиссии UA на персональном компьютере.

Результаты . К методике расчета оптимальной атаки на IQ предъявляются особые требования: во-первых, по скорости нахождения решения, во-вторых, по точности результата. Это следует из простого рассуждения о том, что безопасность CI необходимо анализировать во временных рамках, намного меньших, чем время любой успешной атаки. Только в этом случае можно будет гарантировать предсказание атаки на основе обнаруженных частичных изменений параметров подсистем.

Таким образом, алгоритм решения задачи поиска оптимальной атаки должен, прежде всего, обеспечивать сложность, близкую к полиномиальной [5], т.е. время нахождения указанного решения должно зависеть только от числа неизвестных в задаче и зависеть от него как полином конечной степени, а во-вторых, оно должно обладать хорошей устойчивостью [4], т.е. исключить «ротацию» алгоритма при определенных значениях констант и параметров задачи. Важна способность алгоритма работать с параллельным выполнением своих шагов, или возможность «распараллелить» свою работу. При возможности параллельного расчета отдельных шагов алгоритма его практическая ценность резко возрастает, т.е. Возможности

распределенных вычислительных сетей значительно превышают вычислительную мощность одной. Сказанное подчеркивается тенденцией развития современных суперкомпьютеров, в которых микропроцессоры все чаще используются для домашнего использования, но основное внимание уделяется их количеству и скорости передачи данных между ними. С этой точки зрения можно сформулировать дополнительные требования к алгоритму:

1. Алгоритм должен иметь «свободные» шаги, расчет которых не зависит от других шагов даже в пределах одной итерации алгоритма;

2. «Свободные» шаги алгоритма должны характеризоваться скалярной величиной, упрощающей оценку той или иной итерации алгоритма.

При соблюдении этих условий очень легко разработать распределенный алгоритм, в котором отдельные вычислительные шаги выполняются параллельно на разных компьютерах.

Обратите внимание, что искомое решение должно быть целым числом, т.е. дополнительно к указанным свойствам алгоритма добавлено условие целочисленности решения. Это следует из рассмотрения ограничений математической модели с точки зрения техники работы с изменением параметров подсистем. В рассматриваемом случае учитывается только факт изменения некоторого параметра и оценивается влияние этого явления на другие параметры, но величина изменения остается за рамками задачи. Такой подход значительно упрощает математическую модель.

следует рассмотреть метод нахождения значений констант модели. ¬Следует учитывать, что до сих пор не существует единой методики решения возникающих здесь трудностей, их можно классифицировать следующим образом:

1. Нахождение параметров подсистем, необходимых для ИК-безопасности. Предполагается, что сложно выделить и разделить механизмы взаимодействия процессов передачи и обработки данных при работе подсистемы. ¬в том числе сложность выделения подсистем, ведь даже если рассматривать одну изолированную автоматизированную систему, состоящую из нескольких подсистем, задача определения функций каждой подсистемы тривиальна из-за отсутствия полного описания их взаимодействия.

2. Определение взаимосвязей между параметрами. Основная проблема здесь заключается в сложности выбора подмножеств параметров, изменения которых достаточны для аппроксимации желаемого изменения. Задача усложняется разницей во времени, необходимом для завершения процесса изменения нужного параметра.

3. Определение числовых значений величин, связанных с изменением параметров. Характеризуется неспособностью правильно оценить конкретный механизм или алгоритм, используемый для доступа к параметру. Например, при изменении пароля администратора он отправляется на сервер в виде

одностороннего хеш-значения с длиной результата 64 бита. Исходя из высокой оценки, т.е. не зная криптографических свойств алгоритма хеширования, можно сказать, что вычислительная сложность подбора пароля по хеш-значению составляет не менее 2 63 вычислений хеш-значений перечисленного множества паролей. Однако, если, например, в качестве хеш-функции используется 2-й дополнительный модуль, такой внешней оценки безопасности хэш-функции может оказаться недостаточно.

Учитывая изложенное, в метод определения значения констант математической модели необходимо добавить элементы корректировки, когда полученные значения корректируются поправочными коэффициентами.Таким образом, БЗ находится непосредственно через плащ . оборудования и программного обеспечения с учетом характеристик можно более точно рассчитать константы математической модели, что позволяет более точно находить уязвимости в ВИК.

Вывод : Приведена методика разделения информационного комплекса на компоненты подсистемы, позволяющая объективно оценить значимость каждой подсистемы для нарушителя и, как следствие, оценить уровень защищенности выделенной. подсистема. Приведены критерии выбора «безопасных» параметров подсистем, что позволяет найти для них цифровые свойства в модели. Показана и показана методика нахождения коэффициентов математической модели вида к подсистемам и параметрам из определенного участка ИС. ¬В результате появится возможность выявления уязвимостей в комплексе для решения проблемы ПА и обеспечения безопасной работы информационного комплекса.

1. Получена математическая формализация происходящих процессов. Данная математическая модель позволила сформулировать задачу поиска оптимального и, следовательно, наиболее вероятного способа несанкционированного доступа.

2. Задача оптимальной атаки на информационный комплекс представлена как основная задача линейного программирования, что ограничивает все значение переменных этой задачи, что позволяет использовать разработанный математический аппарат линейной теории. целочисленное программирование для ее решения.

3. Программно выполняются несколько модификаций точного алгоритма решения сформулированных задач оптимальной атаки - алгоритм перебора L-класса. Реализация программного обеспечения была подвергнута вычислительному эксперименту, на основании которого были сделаны выводы о возможности использования конкретных алгоритмов для получения результатов при исследовании информационных систем того или иного размера.

4. По результатам вычислительных экспериментов с точным алгоритмом был предложен новый приближенный алгоритм, который применялся для решения задач, подходящих для сетей крупных предприятий с числом узлов более 120 (общее

количество серверов и рабочих станций), поскольку точный Алгоритм позволил найти искомое решение, не дает .¬

5. На основе практического применения разработанной методики получены рекомендации по совершенствованию системы безопасности корпоративной сети, что позволило сократить количество агентов мониторинга сетевого трафика на 30%, было уменьшено количество правил межсетевого экрана, что привело к их увеличению . ¬проводимость. Все это позволило снизить затраты на поддержание политик сетевой безопасности.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Лукацкий А.В. Обнаружение атаки. – СПб.: БХВ – Петербург, 2021. – 624 с.: ил.

2. Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика; Электронинформ, 2017. - 368 с.: ил.

3. Кристофид Н. Теория графов - алгоритмический подход. - М.: Мир, 2018. -432 силы.

4. Волков И.К., Загоруйко Е.А. Операционные исследования: учебник для вузов / Под ред. ПРОТИВ. Зарубина, А.П. Крищенко. М.: МГТУ им. издатель. Н.Э. Баумана, 2020. -436 с.

5. Гэри М., Джонсон Д. Вычислительные машины и неразрешимые проблемы : Пер. с английского. - М.: Мир, 2021. - 416 с., ил.

6. Колоколов А.А. Дискретные методы оптимизации: Учебник. - Омск: ОмГУ, 2018. - 76 с.