УДК 004.738 (045)

Я. В. Милокум, канд. техн. наук

ВЗАИМОДЕЙСТВИЕ КОНФЛИКТУЮЩИХ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ ПАРАМЕТРИЧЕСКОЙ И СТРУКТУРНОЙ НЕОПРЕДЕЛЕННОСТИ

Национальный авиационный университет, e-mail: janine@ukr.net

Рассмотрено взаимодействие атакующего субъекта и защищаемого объекта в рамках общей теории конфликта. Формулируется задача обнаружения и предотвращения вторжений. Подробно рассмотрен алгоритм последовательного анализа.

Ключевые слова: конфликт, атака, сети, информация, неопределенность, защита.

Введение. В литературе по защите компьютерных сетей существует масса различных определений термина «атака». Специалисты в области безопасности часто трактуют его применительно к конкретной ситуации, специфике сети, её целевому назначению и решаемым задачам. Эти определения имеют узкий характер, отражают некоторые частные характеристики процесса, зачастую являются тавтологичными, а иногда и противоречивыми.

Рассмотрим взаимодействие атакующего субъекта и защищаемого объекта в рамках общей теории конфликта [1; 2]. При использовании данной теории достигается максимальная степень обобщения задачи защиты. Абстрагируясь от множества промежуточных этапов взаимодействия атакующего субъекта и защищаемого объекта, в дальнейшем будем рассматривать связь между потенциальными угрозами и наличием «окон уязвимости» – незащищенных элементов компьютера и/или компьютерной сети, аппаратных и программных модулей, через которые может осуществляться несанкционированный доступ и т. д.

«Атакой» (вторжением, нападением) на информационную систему называется действие или последовательность связанных между собой действий нарушителя, которые приводят к реализации угрозы путем поиска и использования окон уязвимости этой информационной системы [3]. Следовательно, если бы можно было устранить все уязвимости информационной системы, то тем самым была бы исключена и потенциальная возможность реализации атак.

Поскольку устранение всех уязвимостей информационной системы – принципиально недостижимая цель, то и решение задачи предотвращения атак можно рассматривать только в некотором асимптотическом смысле.

Назначение системы обнаружения вторжений состоит в обнаружении, определении попыток вторжения (как реализованных, так и предотвращенных) и прогнозировании связанных с ними угроз, т. е. в мониторинге ситуации. Ввиду противодействия противника (атакующего субъекта) эффективный мониторинг возможен только при правильном сочетании и успешном выполнении комплекса обеспечивающих и организационных мероприятий. Система обнаружения вторжений является неотъемлемой частью общей системы защиты компьютерной сети.

Постановка задачи. Задачу обнаружения и предотвращения вторжений невозможно решить путем адаптации к изменяющимся условиям – пассивного следования за действиями разумного партнера (противника). В условиях, когда неизвестны ни параметры, ни структура связей между атакующими субъектами (параметрическая и структурная априорная неопределенность), реализация активной защиты в системах обнаружения и предотвращения вторжений возможна только в процессе конфликтного управления ситуацией [1; 2].

Рассмотрим наиболее распространенные стратегии противодействия S_{icm} и стратегии обнаружения вторжений S_{ids} для различных задач конфликта.

Стратегии противодействия и атак

1. Разведка:

– определение режима работы системы обнаружения вторжений и ее организации (порядок включения и выключения средств, смены режимов и т. д.);

– определение конфигурации защищаемого объекта (компьютера, компьютерной сети, сетевого узла) и текущих изменений конфигурации;

– технический прогноз скрытых возможностей системы защиты на основании измеренных величин;

– оперативный прогноз скрытых возможностей системы защиты на основании априорных и накопленных данных.

2. Дезинформация:

– имитация ложной обстановки, в которой функционирует объект защиты;

– формирование ложных адресов атакующего субъекта;

– создание виртуальных ложных объектов, якобы взаимодействующих с объектом защиты.

3. Рефлексивное управление (стремление к ситуационному перевоплощению и поиску неразрешимых проблем):

– оценка субъективной вероятности [4] поведения атакуемого объекта и направления его мышления;

– эскалация в атаку (медленное, малозаметное повышение сетевой активности для стимулирования повышения порогов обнаружения и распознавания);

– оперативная эскалация (кратковременная имитация потока атакующих запросов, не достигающих рубежей принятия решений);

– показ группировки атакующих субъектов (с ориентировкой на недоверие);

– силовой шантаж («размножение» атакующих субъектов для дезорганизации управления S_{ids}).

4. Организационные мероприятия:

– комплексное применение атак разных классов;

– прорыв системы защиты под прикрытием имитационных атак;

– ослабление управления S_{ids} путем длительного применения изнуряющих атак (атаки типа «отказ в обслуживании»);

– подавление пропускной способности (применение атак с других сетевых сегментов с более высокой скоростью передачи данных или распределенные атаки).

Стратегии защиты

1. Разведка:

– контроль потоков атак;

– определение характеристик атак;

– выявление эскалации в атаку;

– изучение и прогнозирование типовых (рабочих) ситуаций;

– изучение и прогнозирование организационных мероприятий атакующего субъекта;

– изучение и прогнозирование потенциальных объектов атак, не входящих в сферу влияния защищаемого объекта.

2. Маскировка:

– скрытие эффективных методов защиты, применение типовых режимов работы в простых ситуациях;

– имитация активности системы защиты;

– имитация «спокойствия» – отсутствие реакции на организационные мероприятия атакующего субъекта.

3. Рефлексивное управление:

– демонстрация «затягивания» в эскалацию атаки (обманные системы создания псевдосервисов, цель которых заключается в воспроизведении хорошо известных уязвимостей как приманки для злоумышленника);

– демонстрация растерянности – беспорядочная смена приёмов защиты и режимов работы защищаемого объекта;

– демонстрация благополучия – применение простых решений, несмотря на противодействие и атаки;

– демонстрация «мгновенной реакции» – изменение режима (не обязательно целенаправленного) при любом изменении обстановки;

– истощение ресурса ответных мер атакующего субъекта (выделение большей доли общего ресурса на меры защиты, заказ большего ресурса у провайдера для защищаемого объекта, подключение к своей защите лояльных партнеров и т.д.).

1. Организационные меры:

– объединение независимых объектов атаки (лояльных партнеров) для создания защищаемой группировки и реализации общей стратегии защиты;

– рациональное использование энергоинформативности системы (оптимизация распределения ресурсов на обмен данными и на защиту).

В системе защиты, основанной на теории конфликта, предполагаются активные действия по отражению атаки. Здесь рассматриваются теоретические модели и методы анализа, прогноза развития конфликта и оптимизации последовательностей защитных действий.

Самым эффективным видом атаки является распределенная. Атака происходит сразу из нескольких точек, что приводит к резкому возрастанию нагрузки на каналы передачи, сетевые узлы и к выведению атакуемого узла из строя из-за перегрузки интенсивным потоком заявок (сообщений, запросов, ложных данных и пр.). Из-за многомерности пространства априорных данных значительно усложняются задачи обнаружения вторжений, распознавания аномальных ситуаций и выработки оптимальных решений. Логично, что в ситуации распределенной атаки наиболее эффективной является распределенная система защиты – привлечение к решению задачи совместной защиты лояльных партнеров – как тех, которые обслуживаются тем же провайдером, так и тех, которые обслуживаются другими провайдерами и, возможно, находятся в разных сегментах сети.

Поэтому в дальнейшем будем рассматривать именно распределенную систему защиты, которая при очевидных упрощениях может быть сведена к сосредоточенной системе или к совокупности сосредоточенных систем защиты, не связанных между собой.

Элементы системы защиты периодически опрашиваются для проверки их состояния. Элемент срабатывает, если появится достаточно интенсивный сигнал, который превысит пороговый уровень β_{0l} . Если сработал один или несколько элементов, система защиты переходит в режим повышенной готовности. В этом режиме могут включаться дополнительные ресурсы сети для детального анализа состояния.

По результатам предварительного анализа информации выбирается адекватный метод (методы) первичной защиты:

– возврат запросов без их модификации (отказ от получения трафика),

– занесение отправителя в «черный список»,

– перенаправление входящих запросов на адрес злоумышленника;

– разрыв соединения с атакующим узлом;

– реконфигурация межсетевых экранов и сетевого оборудования для блокирования всех запросов с атакующего адреса;

– посылка сообщения интернет-провайдеру с целью блокирования злоумышленника;

– другие.

Одновременно информация передается в базу данных более высокого уровня иерархии (региональную базу данных – РБД).

Датчики могут сработать и по ложному сигналу, когда попытки несанкционированного доступа (НСД) на самом деле не было. Поэтому в РБД для исключения ложных вызовов необходимо обрабатывать поступившую информацию по некоторому оптимальному алгоритму. Рассматриваемая задача относится к классу задач проверки статистических гипотез [5]. Для принятия решения, оптимального по некоторому критерию, необходимо выполнить соответствующие преобразования над принятой смесью полезного сигнала, мешающих сигналов и (помех) и шумов. Существует большое количество статистических критериев оптимальности, однако известно [6], что все они приводят к стандартной процедуре вычисления отношения правдоподобия (ОП) или его монотонной функции (обычно вычисляют логарифм ОП) и сравнения результата с порогом β_{0i}:

$$L(x_i) = \frac{W(x_i / s_{1i})}{W(x_i / s_{0i})} \gtrless \beta_{0i}$$

или

$$l(x_i) = \ln \frac{W(x_i / s_{1i})}{W(x_i / s_{0i})} \gtrless \ln \beta_{0i} \ ,$$

где $W(x_i / s_{1i})$ – условная плотность вероятности входной смеси при условии наличия полезного сигнала (попытка НСД); $W(x_i / s_{0i})$ – условная плотность вероятности при условии отсутствия полезного сигнала (отсутствие попытки НСД, ложное срабатывание системы обнаружения).

По результатам обработки могут быть приняты следующие решения.

1. При использовании алгоритма с фиксированным объемом выборки $N_b = \text{const}$ и пороговым уровнем β_{ci}, который устанавливается в устройстве оптимальной обработки РБД:

– $\beta_0 < \beta_{ci}$ – ложная тревога;

– $\beta_0 > \beta_{ci}$ – попытка НСД.

2. При использования алгоритма последовательного анализа с переменным объемом выборки $N_b = \text{var}$, нижним β_{ci} и верхним B_{ci} пороговыми уровнями, которые устанавливаются в устройстве оптимальной обработки РБД:

– $\beta_0 < \beta_{ci}$ – ложная тревога;

– $\beta_0 > \text{B}_{ci}$ – попытка НСД;

– $\beta_{ci} < \beta_0 < \text{B}_{ci}$ – продолжение наблюдения.

Рассмотрим алгоритм последовательного анализа более подробно. Поскольку сигналы и помехи являются случайными величинами, объем выборки до принятия какого-либо решения также является случайной величиной и заранее не фиксируется. Интуитивно ясно, что чем меньше нижний порог и чем выше верхний порог, тем больше (в среднем) будет ожидаемый объем выборки и, соответственно, время наблюдения до момента принятия решения. Однако проблема выбора порогов является одной из центральных и наиболее сложных в теории проверки статистических гипотез [6]. Выбор порогов осуществляется в соответствии с неравенствами

$$\beta_{ci} \ \geq \min \left(\frac{1 - P_{\text{обн}}}{1 - P_{\text{лт}}}, \frac{P_{\text{обн}}}{P_{\text{лт}}} \right); \qquad (1)$$

$$\mathrm{B}_{ci} \le \max\left(\frac{1-P_{\text{обн}}}{1-P_{\text{лт}}}, \frac{P_{\text{обн}}}{P_{\text{лт}}}\right), \qquad (2)$$

где $P_{\text{обн}}$ – вероятность правильного обнаружения НСД; $P_{\text{лт}}$ – вероятность ложной тревоги, среднее время последовательного анализа является минимальным и меньшим, чем время анализа с выборками фиксированного объема (при тех же показателях качества обнаружения).

На практике интерес представляют условия высокой вероятности правильного обнаружения $P_{\text{обн}} > (0,9...0,99)$ и малой вероятности ложной тревоги $P_{\text{лт}} << 0,5$. Тогда неравенства (1) и (2) упрощаются:

$$\beta_{ci} \ge \left(\frac{1-P_{\text{обн}}}{1-P_{\text{лт}}}\right);$$

$$\mathrm{B}_{ci} \le \left(\frac{P_{\text{обн}}}{P_{\text{лт}}}\right).$$

Выражения для математических ожиданий требуемых объемов выборок n до принятия решения имеют следующий вид [7]:

– по гипотезе H_0 (отсутствие попытки НСД)

$$m_0\{n \mid H_0\} = \frac{(1-P_{\text{лт}})\ln\frac{1-P_{\text{обн}}}{1-P_{\text{лт}}} + P_{\text{лт}}\ln\frac{P_{\text{обн}}}{P_{\text{лт}}}}{m_{10}};$$

– по гипотезе H_1 (попытка НСД)

$$m_1\{n \mid H_1\} = \frac{(1-P_{\text{обн}})\ln\frac{1-P_{\text{обн}}}{1-P_{\text{лт}}} + P_{\text{обн}}\ln\frac{P_{\text{обн}}}{P_{\text{лт}}}}{m_{11}},$$

где m_{10} и m_{11} – математическое ожидание корреляционных интегралов по гипотезам H_0 и H_1 соответственно. Отношение $\frac{m_{11}}{m_{10}}$ можно трактовать как логарифм отношения (полезный сигнал)/(помеха и шум) по мощности.

Судя по результатам проведенных расчетов, требуемый объем выборки слабо зависит от вероятности ложной тревоги, более существенно зависит от вероятности правильного обнаружения и сильнее всего зависит от энергетических характеристик сигналов и помех.

Поскольку данные характеристики являются случайными и существенно меняются в процессе работы системы защиты, можно ожидать, что будут случаться ситуации, когда процедура последовательного анализа окажется слишком длительной. В таких случаях используют правило усеченного последовательного анализа. При объеме выборки $n \le n_{\max}$, где $n_{\max}$ – заранее устанавливаемый максимально допустимый объем выборки, устанавливаются два порога, с которыми сравнивается ОП. Если же значение $n_{\max}$ достигнуто, а решение не принято, ОП сравнивается с одним порогом, как в алгоритме с фиксированным объемом выборки. Третий порог устанавливается внутри области между первым (нижним) и вторым (верхним) порогами. Метод оптимального выбора третьего порога пока не разработан. Поэтому рекомендуется подбирать его экспериментальным путем для конкретных условий работы системы защиты. Кроме того, необходимо предусмотреть возможность регулировки порогов в процессе работы.

Выводы. В условиях непрекращающегося роста потенциальных угроз, организации атак распределенного типа логичным выходом из сложившейся ситуации является ответная организация распределенных систем активной защиты – группировок, включающих достаточно большое количество лояльных партнеров и работающих согласованно под управлением иерархической системы управления объектами защиты.

Для предупреждения существующих и прогнозируемых угроз, успешного отражения атак на начальном этапе их организации нецелесообразно применять адаптивные системы защиты из-за их постоянного запаздывания как минимум на один шаг. В распределенных системах защиты предлагается использовать методы конфликтного управления с прогнозированием развития ситуации и коррекции по результатам ее текущего анализа.

Список литературы

1. *Дружинин В. В.* Введение в теорию конфликта / В. В. Дружинин, Д. С. Конторов, М. Д. Конторов. – М.: Радио и связь, 1989. – 288 с.
2. *Дружинин В. В.* Конфликтная радиолокация / В. В. Дружинин, Д. С. Конторов. – М.: Радио и связь, 1982. – 124 с.
3. *Лукацкий А. В.* Мир атак многообразен // Сетевой. – №1. – 2001 http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=4781
4. *Де Гроот М.* Оптимальные статистические решения / Де Гроот М. – М.: Мир, 1974. – 491 с.
5. *Сосулин Ю. Г.* Теория обнаружения и оценивания стохастических сигналов / Ю. Г. Сосулин. – М.: Сов. радио, 1978. – 320 с.
6. *Левин Б. Р.* Теоретические основы статистической радиотехники / Б. Р. Левин. – М.: Сов. радио, 1968. – Кн. 2. – 504 с.
7. *Леман Э.* Проверка статистических гіпотез / Э. Леман. – М.: Наука, 1979, – 408 с.

Я. В. Милокум

Взаємодія конфліктуючих інформаційних систем в умовах параметричної та структурної невизначеності

Формулюється задача виявлення і запобігання вторгнень. Вирішується задачі виявлення вторгнень в інформаційних системах в рамках загальної теорії конфлікту. Докладно розглядається алгоритм послідовного аналізу.

Ya. V. Milokum

Co-operation of the conflicting informative systems is in the conditions of self-reactance and structural vagueness

The interaction between the attacker and the subject of the protected object within the general theory of conflict. Formulated the problem of detecting and preventing intrusions absorption. Discussed in detail the algorithm of sequential analysis.