ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Ю.В. Алейнов

ЗАЩИТА ЛОКАЛЬНЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ ОТ АТАК НАПРАВЛЕННОГО ТИПА ПУТЕМ ИМИТАЦИИ СЕТЕВЫХ РЕСУРСОВ

(Самарский государственный университет)

Актуальность проблемы защиты от сетевых атак в настоящее время не вызывает сомнений. Вместе с ростом количества программного кода растет количество уязвимостей, так называемое сообщество «черных шляп» постоянно открывает новые способы обхода существующих средств защиты. Вместе с тем, все более заметной становится тенденция перехода злоумышленников от стратегии массовых атак, покрывающих большие сегменты сети, к парадигме так называемых направленных (*targeted*) атак [1]. Злоумышленник или группа злоумышленников, действуя максимально осторожно, совершает ряд последовательных частных атак, избирательно компрометируя объекты внутри какой-то определенной, интересующей нарушителя, сети. Тем самым нарушитель закрепляется внутри сети, и на протяжении долгого периода времени может контролировать информационные потоки в ней, извлекая выгоду для себя. Это подчеркнуто в распространенной англоязычной версии термина (*Advanced Persistent Threat, APT*). Обнаружение направленных атак представляет собой задачу особой сложности, учитывая, что при их подготовке и проведении часто используются так называемые уязвимости «нулевого дня», сигнатуры которых еще не содержатся в базах данных большинства систем обнаружения вторжений [2].

Эффективно противостоять направленным атакам можно только используя различные средства и методы защиты сети в комплексе. Одним из заслуживающих внимание методов в данном контексте является применение механизмов обмана. В структуру защищаемой сети внедряются специальные объекты, которые не участвуют в штатных процессах обработки информации, а нужны только для того, чтобы привлечь внимание нарушителя и быть атакованными им. Узлы сети, реализующие такие объекты, называют обманными системами (ОбС, Honeypot). К обманным системам предъявляется обязательное требование – они должны быть неотличимы с точки зрения нарушителя от реальных узлов сети. В таком случае нарушитель на некотором этапе может случайно выбрать в качестве цели для следующей частной атаки ОбС. Любое его взаимодействие с обманной системой должно быть самым подробным образом записано для дальнейшего исследования. Сам же факт обращения к ОбС, откуда бы то ни было, уже является аномалией и поводом

для пристального рассмотрения данной ситуации администратором безопасности [3].

Важным направлением исследований в области применения ОбС для обнаружения нарушителя в сети является выработка принципов размещения таких систем в защищаемой инфраструктуре и определение оптимальных значений их основных параметров. Указанные вопросы освещены в литературе недостаточно полно. Существует ряд исследований, в которых предлагаются способы поиска оптимальной конфигурации ОбС, однако их результаты оказываются неприменимы в условиях направленных атак [4]. Авторы при построении моделей атаки, как правило, допускают возможность свободного доступа нарушителя к любому узлу сети в любой момент времени. Очевидно, в реальности это не так. Нарушитель всегда ограничен в выборе цели для следующей частной атаки. Это обусловлено структурой самой сети и работой средств разграничения доступа на разных уровнях. Пренебрежение данным обстоятельством выглядит оправданным в случае, когда берется во внимание отдельный небольшой участок сети с однородной структурой или рассматривается единственная попытка частной атаки, но при попытке рассмотреть развитие процесса сложного многоступенчатого вторжения в контексте всей сетевой инфраструктуры может привести к ошибочным результатам.

В настоящей статье приведено описание модели направленной атаки на локальную сеть, содержащую обманные системы. На основе описанной модели предложено решение задачи размещения ОбС в сети.

Модель направленной атаки на сеть, содержащую обманные системы

Процесс развития направленной атаки на сеть можно рассматривать как последовательность частных атак, каждая из которых характеризуется своим источником и целевым узлом. Нарушитель, контролирующий узел-источник атаки, инициирует сетевое соединение между ним и выбранной целью. В ходе передачи данных через это соединение нарушитель эксплуатирует какие-либо из имеющихся на целевом узле уязвимостей для получения контроля над ним. Допустим, что нарушитель тщательно готовит каждую частную атаку, при этом он имеет достаточно опыта и ресурсов, чтобы она была гарантированно успешной. В случае если целевой узел является реальной системой, он переходит под контроль нарушителя и может использоваться им в дальнейшем в качестве источника следующих частных атак. Если в качестве цели для частной атаки нарушителем была выбрана ОбС, то будем считать, что атакой на нее нарушитель обнаруживает себя и служба безопасности сети делает дальнейшие его действия невозможными, то есть, развитие направленной атаки останавливается.

Рассмотрим влияние внутренней структуры сети на развитие направленной атаки. Во-первых, разные узлы сети могут принадлежать разным зонам межсетевого экрана, что, в зависимости от его настроек, способно повлиять на возможность обмена данными между ними. Во-вторых, сетевое соединение между двумя узлами сети возможно установить только в случае

поддержки ими обоими одного и того же сетевого протокола. При этом некоторые протоколы подразумевают, что сообщающиеся стороны выполняют различные роли (так называемое клиент-серверное взаимодействие). Поддержка протоколов и правильное распределение ролей при сетевом взаимодействии обеспечивается установленным на узлах программным обеспечением (ПО) [5]. Таким образом, список установленного на сетевых узлах ПО и его конфигурация так же, как и правила межсетевого экрана, влияют на возможность установления сетевого соединения. Другими словами, выбор на некотором этапе нарушителем некоторого подконтрольного ему узла в качестве источника частной атаки определяет множество доступных в рамках этой атаки целей. Кроме того, список установленного ПО на сетевых узлах влияет и на выбор конкретной цели для частной атаки из нескольких возможных. Нарушитель будет атаковать в первую очередь те узлы, программное обеспечение которых содержит наиболее известные для него уязвимости или уязвимости, которые наиболее просто использовать. Итак, можно выделить два основных признака различия узлов в сети с точки зрения нарушителя:

1. расположение узла относительно межсетевого экрана и правила фильтрации трафика для его зоны;
2. список программного обеспечения, функционирующего на узле.

Будем считать идентичными для нарушителя сетевые узлы, находящиеся в одной зоне межсетевого экрана и имеющие одинаковый список установленных программ, независимо от того, реальные ли это системы или ОбС. Вероятность проведения частной атаки на такие узлы из одного и того же источника, независимо от его выбора, будем считать одинаковой. Таким образом, фактически задается отношение эквивалентности сетевых узлов с точки зрения нарушителя. Множества эквивалентных узлов будем называть доменами эквивалентности.

Пусть $\{d\}_1, d_2, \ldots, d_n\}$ – разбиение всего множества узлов сети на домены эквивалентности. Рассмотрим процесс развития направленной атаки в сети. Время положим дискретным. Будем полагать, что за один шаг происходит одна частная атака. Зафиксируем некоторый номер шага t. Пусть S_t и D_t – случайные величины, равные номерам доменов эквивалентности, содержащих соответственно источник и целевой узел частной атаки на шаге с номером t. Согласно сделанным предположениям относительно критериев выбора нарушителем целей для частных атак, условная вероятность $P(D_1 t = j \mid S_1 t = i), 1 \le i, j \le n$ не зависит от t. Обозначим эту вероятность p_{ij}. Матрица $M = (p_{ij})_{i,j=1}^{n}$ таким образом является инвариантной по времени характеристикой сети. Вероятность $P(S_t = i), 1 \le i \le n$ – это вероятность выбора в качестве источника частной атаки на шаге с номером t узел из домена d_i. Очевидно, эта вероятность зависит от того, какие на данном шаге узлы находятся под контролем нарушителя. А это, в свою очередь, определяется тем, на какой из узлов была направлена частная атака на предыдущем шаге.

Итак, каждому домену $d_i, 1 \le i \le n$ поставим на шаге с номером t в соответствие упорядоченную тройку целых чисел (r_i, h_i, a_i^t), где r_i – количество реальных, h_i – обманных систем, а a_i^t – количество подконтрольных нарушителю (зараженных) узлов в домене. Состояние процесса развития направленной атаки в сети на шаге t можно полностью описать вектором $\bar{a}_t = (a_1^t, a_2^t, \dots, a_n^t)$. Пусть $\bar{a}'$ и $\bar{a}''$ – два состояния процесса. Найдем вероятность перехода между этими состояниями. Согласно принятой модели, на каждом шаге совершается ровно одна частная атака, в ходе которой либо происходит компрометация одной реальной системы из некоторого домена сети, либо процесс останавливается. Таким образом, для состояния $\bar{a}'$ существует максимум $n+1$ возможных переходов. Пусть $\Delta\bar{a}_k = (0,0,\dots,\underset{k}{1},0,\dots 0) \in \mathbf{Z}^n$, а $\bar{a}'' = \bar{a}' + \Delta\bar{a}_k$. Тогда вероятность перехода $P(\bar{a}' \to \bar{a}'')$ равна вероятности атаки на соответствующем шаге реального узла, лежащего в домене эквивалентности d_k:

$$P(\bar{a}' \to \bar{a}'') = P\left(a_k^{t+1} = a_k^t + 1\right) = \frac{r_k - a_k^t}{h_k + r_k} \sum_{i=1}^{n} P(S_t = i) p_{ik} \quad (1)$$

Распределение случайной величины S_t на каждом шаге полностью определяется списком скомпрометированных узлов сети. Пусть экспертным путем задана некоторая весовая функция $w: [\![d]\!]_1, d_2, \dots, d_n\} \to \mathbf{R}$, ставящая в соответствие каждому домену эквивалентности в сети числовое значение приоритета при выборе узла-источника атаки. Тогда вероятность выбора источника из конкретного домена можно записать следующим образом:

$$P(S_t = i) = \frac{w(d_i)}{\sum_{s: a_s^t \neq 0} w(d_s)} \quad (2)$$

Подставляя (2) в (1), получим окончательное выражение для вероятности перехода:

$$P(\bar{a}' \to \bar{a}'') = \frac{r_k - a_k^t}{h_k + r_k} \sum_{i=1}^{n} \frac{w(d_i)}{\sum_{s: a_s^t \neq 0} w(d_s)} p_{ik} \quad (3)$$

Вероятность остановки процесса на шаге t определяется следующим выражением:

$$P_{stop}^t = \sum_{k=1}^{n} \left(\frac{h_k}{h_k + r_k} \sum_{i=1}^{n} \frac{w(d_i)}{\sum_{s: a_s^t \neq 0} w(d_s)} p_{ik} \right) \quad (4)$$

Из (3) и (4) видно, что вероятности перехода между состояниями процесса зависят только от текущего состояния, следовательно, процесс изменения вектора $\bar{a}$ со временем является цепью Маркова. Общее количество состояний процесса равно $m = \prod_{i=1}^{n} r_i$. Хотя, таким образом, для размера матрицы переходов справедлива оценка $O\left([\![\max_{1 \le i \le n} r_i^n]\!]\right)$, она является весьма разреженной. Каждая ее строчка содержит не более $n+1$ ненулевых элементов. При реализации операций с данной матрицей необходимо это учитывать для более эффективного использования вычислительных ресурсов. Пусть Q – матрица

переходов рассматриваемого процесса. Пусть также $\bar{p}_0 = (p_0^1, p_0^2, \ldots, p_0^m)$ – вектор вероятностей нахождения системы в каждом из возможных состояний на шаге с нулевым номером, а вектор $\bar{p}_t = (p_t^1, p_t^2, \ldots, p_t^m)$ описывает распределение вероятностей нахождения процесса в каждом из возможных состояний на шаге с номером t. В силу марковского свойства процесса справедливо следующее выражение:

$$\bar{p}_t = \bar{p}_0 Q^t. \quad (5)$$

Вероятность P_{stop}^t остановки процесса на шаге с номером t находится из выражения (5) как одна из компонент вектора $\bar{p}_t$. Очевидно, эта вероятность должна входить в состав показателя эффективности обнаружения нарушителя с помощью обманных систем.

Показатель эффективности обнаружения нарушителя – это комплексная величина, производная от частных показателей результативности, оперативности и ресурсоемкости процесса обнаружения [6]. Результативность обнаружения определяется наличием контакта нарушителя и ОбС. В качестве показателя оперативности можно рассматривать выполнение условия обнаружения нарушителя прежде некоторого шага t_{max}. Наконец, показателем ресурсоемкости естественно считать истинность предиката $\sum_{i=1}^{n} h_i \le h_{max}$, где h_{max} – максимально допустимое число ОбС в сети, которое рассчитывается исходя из ограничений на вычислительные ресурсы. Интегральным показателем эффективности обнаружения нарушителя (E) может выступать вероятность одновременного попадания в зону допустимых значений всех трех частных показателей. В качестве него таким образом можно рассматривать вероятность $P(t_{stop} \le t_{max})$ остановки процесса не позднее шага t_{max}, которая, очевидно, равна $P(t_{stop} \le t_{max}) = \sum_{j=1}^{t} P_{stop}^j$, где P_{stop}^j – вероятность остановки атаки на шаге с номером j.

Итак, соотношение (5) позволяет непосредственно вычислить значение показателя эффективности обнаружения нарушителя в зависимости от размещения ОбС в сети. Это можно записать следующим образом:

$$E = E(\bar{h}, \bar{r}, M, t_{max}, h_{max}), \quad (6)$$

где $\bar{r} = (r_1, r_2, \ldots, r_n)$ – вектор размещения реальных систем в сети, а $\bar{h} = (h_1, h_2, \ldots, h_n)$ – вектор размещения ОбС. Если положить все аргументы, кроме вектора $\bar{h}$, неизменными, то можно переписать (6) следующим образом: $E = E(\bar{h})$. Оптимальным будем называть такое размещение $\bar{h}_{opt}$, которое удовлетворяет условию $E(\bar{h}_{opt}) = \max_{\bar{h} \in \mathbb{Z}^n} E(\bar{h})$.

Алгоритм поиска оптимального размещения обманных систем в сети

Очевидно, что при добавлении любого количества ОбС в любой домен эквивалентности вероятность контакта нарушителя с ОбС может лишь увеличиваться. Другими словами, функция векторного аргумента $E(\bar{h})$ монотонно возрастает по всем направлениям роста последнего. Кроме того, заметим, что функция E ограничена сверху, поскольку имеет смысл

вероятности. Отсюда ясно, что для любого направления роста аргумента приращение функции ΔE будет уменьшаться при увеличении аргумента. Зафиксируем некоторое начальное размещение $\bar{h}_0 = (h_1^0, h_2^0, \dots, h_n^0)$ в пространстве $\mathbf{N}^n$. Выберем направление максимального роста аргумента и будем двигаться вдоль него. Ясно, что рано или поздно найдется такое направление роста аргумента, отличное от выбранного, что приращение функции по этому направлению станет превышать приращение функции по направлению движения. Изменив направление движения так, чтобы приращение функции было максимально возможным, будем продолжать движение. При удачном выборе исходного размещения $\bar{h}_0$, в конце концов, получим такое размещение $\bar{h}$, которое обеспечивает максимум вероятности контакта с учетом ограничений на максимальное число ОбС и максимальное время обнаружения нарушителя. Удачным выбором $\bar{h}_0$ очевидно будет являться такой, при котором функция E будет принимать максимальное возможное значение для всех вариантов аргумента с фиксированным общим числом ОбС: $\bar{h}_0 = \underset{\sum h_i = const}{\operatorname{argmax}} E(h_1, h_2, \dots, h_n)$. В качестве h_0 удобнее всего взять точку $(0,0,\dots,0)$, поскольку это единственная точка, удовлетворяющая условию $\sum_{i=1}^{n} h_i = 0$. Для ненулевого же количества ОбС всегда существует больше одного варианта размещений. Таким образом, можно предложить следующий общий алгоритм нахождения оптимального размещения ОбС.

1. Задать начальное размещение $\bar{h} = \bar{h}_0 = (0,0,\dots,0)$.
2. Для каждого $\overline{h'} = \bar{h} + \Delta\bar{h}_i$, где $\Delta\bar{h}_i = (0,0,\dots,\underset{i}{1},0,\dots,0)$ вычислить $E_i = E(\bar{h} + \Delta\bar{h}_i)$
3. Найти $j = \underset{i \in [1,n]}{\operatorname{argmax}} E(\bar{h} + \Delta\bar{h}_i)$
4. Положить $\bar{h} = \bar{h} + \Delta\bar{h}_j$
5. Если $\sum_{i=1}^{n} h_i < h_{\max}$, то перейти к шагу 2. Иначе – возврат $\bar{h}$.

Заключение

В статье рассмотрен вопрос поиска оптимального размещения обманных систем в локальной информационной сети (ИС) с целью обнаружения нарушителя. Рассмотрена стохастическая модель, описывающая процесс последовательных контактов нарушителя с элементами ИС, среди которых присутствуют ОбС. Показан способ вычисления показателя эффективности обнаружения. Предложена схема алгоритма, позволяющего синтезировать оптимальное с точки зрения данного показателя размещение обманных систем в ИС.

Литература

1. Sood, A.K., Enbody, R.J. Targeted Cyberattacks: A Superset of Advanced Persistent Threats // Security & Privacy, Vol.11 , № 1, IEEE, 2013.

2. Aaron Beuhring, Kyle Salous, "Beyond Blacklisting: Cyberdefense in the

Era of Advanced Persistent Threats", IEEE Security & Privacy, Vol.12, №5, IEEE, 2014

3. И. В. Котенко, М. В. Степашкин. Обманные системы для защиты информационных ресурсов в компьютерных сетях // Труды СПИИРАН, Вып. 2, т. 1. — СПб.: СПИИРАН, 2004.

4. Bringer M.L., Chelmecki, C.A., Fujinoki H A Survey: Recent Advances and Future Trends in Honeypot Research. // International Journal of Computer Network & Information Security. 2012. №4.

5. В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы - СПб: Питер, 2001.

6. Морозов Л.М., Петухов Г.Б., Сидоров В.Н. Методологические основы теории эффективности: Учебное пособие. – Л.: ВИКИ им. А.Ф, Можайского, 1982. – 236с.

М.Е. Бурлаков

О НЕКОТОРЫХ МОДЕЛЯХ ОПТИМИЗАЦИИ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ ГЕНЕТИЧЕСКИМИ АЛГОРИТМАМИ

(Самарский государственный университет)

В настоящее время в информационной среде все больше находят свое применение искусственные нейронные сети (ИНС). Выделяют множество таковых областей: системы обнаружения вторжений, системы предотвращения вторжений, интеллектуальные экспертные системы, системы прогнозирования [1] и т.д. Для каждой реализации той или иной системы, проектируется и применяется конкретное решение, оптимально отвечающее поставленной задаче. Однако вопрос повышения эффективности уже выбранного решения на основе искусственной нейронной сети является крайне актуальным. Не существует общего алгоритма подбора оптимальных параметров искусственной нейронной сети (вес нейрона, общая топология ИНС, функция активации). Одним из методов, предложенных для решения данной задачи, является применение генетических алгоритмов (ГА).

Генетические алгоритмы

Генетические алгоритмы – одно из направлений исследований в области искусственного интеллекта, занимающееся созданием упрощенных моделей эволюции живых организмов для решения задач оптимизации [1]. Генетические алгоритмы – эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путём случайного подбора, комбинирования и вариации искомых параметров с использованием механизмов, аналогичных естественному отбору в природе [2]. Другими словами ГА - представляет собой адаптивный поисковый метод, который основан на селекции лучших элементов в популяции, подобно эволюционной теории Ч. Дарвина.