Шуваева А.М., Яковлев А.В.

ФОРМАЛЬНОЕ ОПИСАНИЕ СИСТЕМЫ ОБНАРУЖЕНИЯ ТРОЯНСКИХ ПРОГРАММ НА ОСНОВЕ СЕТИ ПЕТРИ

(Тамбовский государственный технический университет)

Троянские программы созданы для осуществления несанкционированных пользователем действий, направленных на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей [1,2]. В отличие от вирусов и червей, представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения.

Основным признаком, по которому различают типы троянских программ, являются их несанкционированные действия – те, которые они производят на заражённом компьютере. Вербальное описание троянских программ строится с помощью элементов сигнатур, таких как *Backdoor.Win32.Bredavi.asq, Packed.Win32.Katusha.b, Backdoor.Win32.Throd.a* и *Trojan-PSW.BAT.Labt.c* [2,3]. Для представления сигнатур атак будем использовать семантические сети.

Семантическая сеть – это ориентированный граф, вершины которого – понятия, а дуги – отношения между ними [4]. Узлы в семантической сети обычно соответствуют объектам, концепциям, событиям или понятиям. Логический вывод (поиск решения) на семантической сети заключается в том, чтобы найти или сконструировать подсеть, удовлетворяющую некоторым условиям.

Детектирование угрозы в такой сети будет выполняться следующим образом. В результате последовательного прохождения по вершинам такой сети определяются компоненты сигнатуры, совокупность которых характеризует конкретную атаку. Структура разработанной семантической сети, позволяет значительно сократить время формирования цепочки соответствующих компонентов сигнатур, на основе группировки характеризующих определенный класс атак компонент и выделения наиболее важных из них на верхний уровень сети. При анализе некоторых отдельных компонент сигнатуры, например, размера файла или содержания поля, может быть использована нечеткая логика или синтаксический анализ текста на степень совпадения с сигнатурой. Такой подход позволит обнаружить вирусы, в которые внесены некоторые изменения, т.е. присутствуют элементы эвристического анализа.

Представим систему обнаружения вторжений в виде сети Петри с последующим ее анализом для получении важной информации о структуре и динамическом поведении моделируемой системы. Эта информация может использоваться для оценки моделируемой системы и выработки предложений по ее усовершенствованию.

Сети Петри - это аппарат для моделирования динамических дискретных систем и определяется как пятерка <P, T, I, O, μ>, где P и T – конечные множе-

ства позиций и переходов, I и O – множества входных и выходных функций, μ – маркировка [5].

Известно [5], что сеть Петри выполняется посредством запусков переходов. Переход запускается удалением меток из его входных позиций и образованием новых меток, помещаемых в его выходные позиции. Переход может запускаться только в том случае, когда он разрешен. Формально работа сети Петри описывается множеством последовательностей запусков и множеством реализуемых маркировок.

Каждому виду атак соответствует конкретная сеть Петри, которая моделирует процесс ее обнаружения. Для успешного детектирования атаки необходима совокупность условий. Если эти условия существуют, то можно говорить о том, что атака точно обнаружена. Но если их нет, или они присутствуют частично, то можно говорить о том, что атака отсутствует, либо присутствует с некоторой долей вероятности соответственно.

Введем следующие обозначения для элементов сети Петри, рассматриваемой в данной работе:

конечное множество позиций:

P = { p0,p1, p2, p3, p4, p5, p6, p7, p8, p9, p10, p11, p12, p13, p14, p15, p16, p17, p18, p19, p20, p21, p22, p23, p24, p25, p26, p27, p28, p29, p30, p31, p32, p33 }.

конечное множество переходов:

T = {t0,t1,t2,t3,t4,t5,t6,t7,t8,t9,...,t31,t32,t33,t34,t35,t36, t37,t38,t39, ..., t51,t52,t53,t54,t55,t56,t57,t58,t59,...,t71,t72,t73,t74,t75,t76,t77,t78,t79,t80}.

множество входных позиций перехода:

I(t0)={p0}, I(t1)={p0}, I(t2)={p1}, I(t3)={p1}, I(t4)={p2}, I(t5)={p2}, I(t6)={p2}, (t7)={p2}, I(t8)={p4}, I(t9)={p4}, I(t10)={p4}, I(t11)={p4}, I(t12)={p3}, I(t13)={p3}, I(t14)={p3}, I(t15)={p3}, I(t16)={p3}, I(t17)={p5}, I(t18)={p6}, I(t19)={p7}, I(t20)={p8}, I(t21)={p9}, I(t22)={p6}, I(t23)={p7}, I(t24)={p8}, I(t25)={p9}, I(t26)={p5}, I(t27)={p5}, I(t28)={p10}, I(t29)={p11}, I(t30)={p12}, I(t31)={p13}, I(t32)={p13}, I(t33)={p10}, I(t34)={p11}, I(t35)={p12}, I(t36)={p13}, I(t37)={p5}, I(t38)={p5}, I(t39)={p5}, I(t40)={p14}, I(t41)={p14}, I(t42)={p14}, I(t43)={p15}, I(t44)={p15}, I(t45)={p15}, I(t46)={p16}, I(t47)={16}, I(t48)={p16}, I(t49)={p16}, I(t50)={p16}, I(t51)={p17}, I(t52)={p14}, I(t53)={p15}, I(t54)={p16}, I(t55)={p17}, I(t56)={p5}, I(t57)={p18}, I(t58)={p19}, I(t59)={p20}, I(t60)={p21}, I(t61)={p22}, I(t62)={p23}, I(t63)={p24}, I(t64)={p18}, I(t65)={p19}, I(t66)={p20}, I(t67)={p21}, I(t68)={p22}, I(t69)={p23}, I(t70)={p24}, I(t71)={p26}, I(t72)={p28}, I(t73)={p28}, I(t74)={p27}, I(t75)={p29}, I(t76)={p31}, I(t77)={p30}, I(t78)={p25}, I(t79)={p32}, I(t80)={p33}.

множество выходных позиций перехода:

O(t0)={p1}, O(t1)={p2}, O(t2)={p4}, O(t3)={p25}, O(t4)={p3}, O(t5)={p3}, O(t6)={p3}, O(t7)={p3}, O(t8)={p3}, O(t9)={3}, O(t10)={p3}, O(t11)={p25}, O(t12)={p5}, O(t13)={p5}, O(t14)={p5}, O(t15)={p5}, O(t16)={p25}, O(t17)={p6}, O(t18)={p7}, O(t19)={p8}, O(t20)={p9}, O(t21)={p27}, O(t22)={p26}, O(t23)={p26}, O(t24)={p26}, O(t25)={p26}, O(t26)={p25}, O(t27)={p10}, O(t28)={p11}, O(t29)={p12}, O(t30)={p13}, O(t31)={p27}, O(t32)={p27},

O(t33)={p26}, O(t34)={p26}, O(t35)={p26}, O(t36)={p26}, O(t37)={p14}, O(t38)={p14}, O(t39)={p14}, O(t40)={p15}, O(t41)={p15}, O(t42)={p15}, O(t43)={p16}, O(t44)={p16}, O(t45)={p16}, O(t46)={p17}, O(t47)={17}, O(t48)={p17}, O(t49)={p17}, O(t50)={p17}, O(t51)={p27}, O(t52)={p26}, O(t53)={p26}, O(t54)={p26}, O(t55)={p26}, O(t56)={p18}, O(t57)={p19}, O(t58)={p20}, O(t59)={p21}, O(t60)={p22}, O(t61)={p23}, O(t62)={p24}, O(t63)={p27}, O(t64)={p26}, O(t65)={p26}, O(t66)={p26}, O(t67)={p26}, O(t68)={p26}, O(t69)={p26}, O(t70)={p26}, O(t71)={p28}, O(t72)={p25}, O(t73)={p27}, O(t74)={p29, p30}, O(t75)={p30, p31}, O(t76)={p33}, O(t77)={p32}, O(t78)={p33}, O(t79)={p33}, I(t80)={p0}.

начальная маркировка:

μ_0={1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0}.

Сеть Петри, моделирующая процесс обнаружения троянских программ представлена на рис. 1.

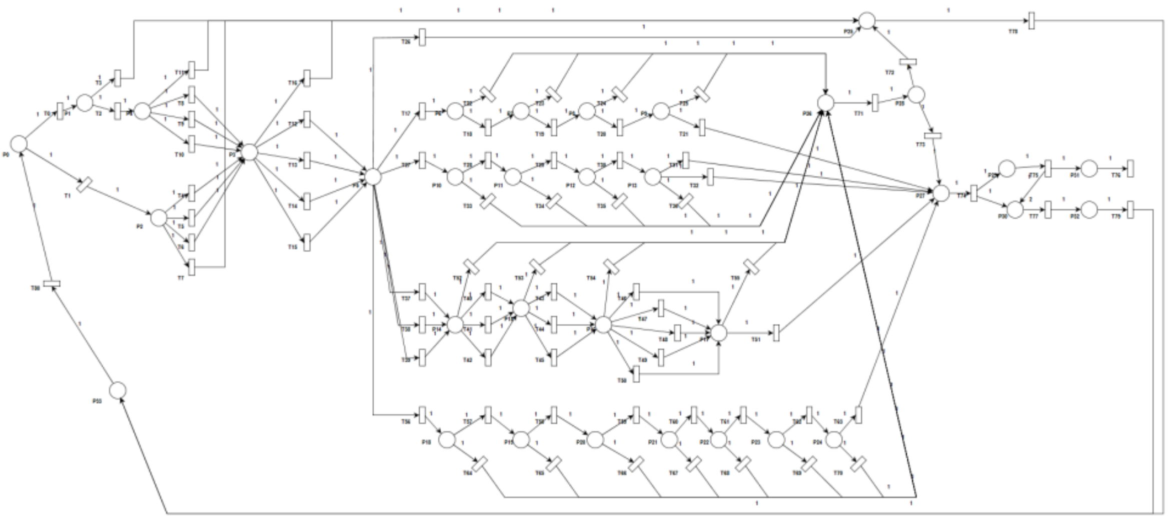

Рис. 1. Сеть Петри, демонстрирующая обнаружение троянских программ

К статическим свойствам сети относятся: конечное множество позиций, конечное множество состояний, множество входных позиций переходов, множество выходных позиций переходов, начальная маркировка, дерево достижимости [5]. Дерево достижимости представляет все достижимые маркировки сети Петри, а также – все возможные последовательности запусков её переходов.

Полный анализ сети Петри можно провести с помощью изучения и анализа ее динамических свойств: достижимость, ограниченность, активность, обратимость и достижимость тупиковой разметки [5]:

- достижимость: маркировка μn достижима из маркировки μ0, если существует последовательность запусков, приводящих от μ0 к μn.

- ограниченность: сеть Петри называется K– ограниченной, или просто ограниченной, если для любой маркировки, достижимой от маркировки μ0, количество фишек в любой позиции не превышает некоторого числа K, то есть μ(p) ≤ K для любого p и любой маркировки μ, принадлежащей R(μ0).

- активность: сеть Петри активна, если независимо от достигнутой μ0 маркировки, для любого перехода существует последовательность дальнейших запусков, приводящая к его запуску;

- обратимость и базовое состояние: сеть Петри обратима, если для любой маркировки μ из R(μ0) маркировка μ0 достижима от μ.

- достижимость тупиковой разметки: делает дальнейшее срабатывание любого перехода в данной сети невозможным [5].

Проанализировав поведенческие свойства модели для сетевых червей, а именно достижимость, ограниченность, активность, обратимость и достижимость тупиковой разметки, можно сделать следующие выводы о:

- достижимости (заданная маркировка в сети принадлежит к множеству маркировок, достижимых в сети и существует последовательность запусков);

- 2-ограниченности (количество меток в любой позиции является ограниченным, в модели в любой позиции имеется не более двух меток);

- активности (последовательность запусков существует для любого перехода, приводящая его к запуску);

- обратимости и отсутствию достижимости тупиковой разметки.

Детектирование угрозы невозможно пока она себя никак не проявит, следовательно, необходимо некоторое время, в течение которого она выполнит свои деструктивные функции. После этого атаку необходимо блокировать, чтобы она не достигла своего логического завершения.

Таким образом, без использования СОВ время реакции на атакующее воздействия зависит от должностной инструкции администратора по безопасности и чаще всего составляет не менее 24 часов. Такой подход не позволяет оперативно реагировать на атаку и тем более предотвратить ее. Использование разработанной системы обнаружения вторжений позволит значительно снизить время реакции на атакующие воздействия и в значительной мере позволит сократить нанесенный системе ущерб.

Литература

1. Лукацкий, А.В. Обнаружение атак / А.В. Лукацкий. – СПб: Питер, 2006. – 680 с.

2. Описания детектируемых объектов. Securelist [Электронный ресурс]. – Режим доступа: http://www.securelist.com/ru/descriptions.

3. Троянские программы. Securelist [Электронный ресурс]. – Режим доступа: http://www.securelist.com/ru/threats/detect/trojan-programs.

4. Представление и использование знаний: пер. с япон. / Х. Уэно [и др.]. – М.: Мир, 1989. – 220 с.

5. Питерсон, Дж. Теория сетей Петри и моделирование систем. / Дж. Питерсон. – М.: Мир, 1984. – 264 с.