Определение оптимальных параметров проактивной защиты сервиса электронной почты от сетевой разведки

А. А. Горбачев, e-mail: infosec23.00@mail.ru

Краснодарское высшее военное училище
им. генерала армии С.М. Штеменко

Аннотация. *Проактивная защита сервиса электронной почты информационных систем различного назначения осуществляется за счет использования механизмов фрагментации ответных откликов почтовых серверов на запросы средств сетевой разведки, имитируя канал связи низкого качества. Статья содержит порядок определения соответствующих оптимальных параметров проактивной защиты.*

Ключевые слова: *электронная почта, сетевая разведка, проактивная защита, оптимизация.*

Введение

Применение различных методов сетевой разведки для исследования информационно-телекоммуникационных систем, таких как, использование уязвимостей в общесистемном программном обеспечении, подмена сетевых адресов, организация компьютерных атак направлены на осуществление анализа сетевого трафика, таблиц маршрутизации, сетевой топологии и конфигурации сетевого оборудования, а также сетевого сканирования с целью определения структуры, алгоритмов функционирования телекоммуникационного оборудования, перечня используемого программного обеспечения, средств защиты информации и других сведений [1-9].

Наряду с наиболее распространенными реактивными средствами защиты информационных систем, основанных на применении принципов фильтрации и идентификации шаблона вредоносного воздействия существуют проактивные средства защиты, такие как: средства маскирования структуры инфо-коммуникационной системы, средства маскирования информационного обмена распределенной информационной системы, средства, использующие временной и вычислительный ресурс злоумышленника («сетевые ловушки») [10-22].

Определение оптимальных параметров функционирования средств проактивной защиты клиент-серверных информационных сетей

© Горбачев А. А., 2022

позволит обеспечить требуемый уровень эффективности защиты в условиях ресурсных ограничений.

1. Качественная постановка задачи

Принцип работы проактивных средств защиты сервиса электронной почты основан на фрагментации ответных откликов почтового сервера на d фрагментов, направляемые в ответ на запросы средств сетевой разведки через промежутки времени T (рисунок 1).

Также существует возможность направления почтовым сервером дополнительных промежуточных (многострочных) откликов или отправка откликов с кодом временной или постоянной ошибки.

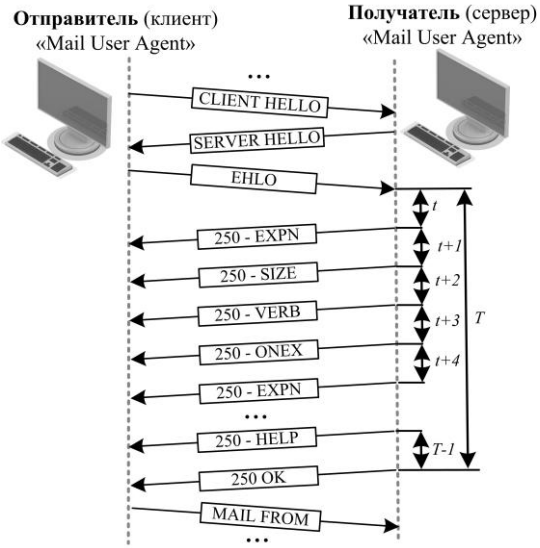

Рис. 1. Принципиальная схема работы проактивной защиты сервиса электронной почты

С целью бескомпроматного расходования ресурсов средств сетевой разведки указанные параметры проактивной защиты являются случайными величинами, имеющими в общем случае произвольные распределения.

С одной стороны, расчет эффективности (результативности) проактивной защиты сервиса электронной почты осуществляется с использованием математической модели функционирования сервиса электронной почты в условиях сетевой разведки, разработанной на основе математического аппарата случайных процессов, в частности,

рекуррентных моделях первого порядка (марковские процессы с дискретным пространством состояний и непрерывным временем).

С использованием вышеуказанной математической модели определяется вид целевой функции, определяющей выбор соответствующих оптимальных параметров проактивной защиты.

С другой стороны, формирование дополнительных фрагментов ответных откликов приводит к увеличению служебного трафика и как следствие к дополнительному использованию пропускной способности канала связи. В связи с чем, при формировании условий определения оптимальных параметров проактивной защиты следует учитывать степень использования среды передачи данных.

2. Формализованная постановка задачи

Моделируемая система характеризуется внешними и внутренними параметрами S_i, Λ_{ij}, где S_i – состояния сервиса электронной почты, характеризующие этап процесса передачи сообщений электронной почты, λ_{ij} – интенсивности потоков событий, инициирующие переход из состояния i в состояние j.

Вектор $\{p_i(t)\}$ выходных характеристик математической модели представляет собой вероятность пребывания системы в состоянии i в момент времени t.

Вектор искомых оптимальных управляющих параметров u(d, T).

Начальное (краевое) условие представляет собой распределение вероятностей пребывания системы в состояниях в начальный момент времени.

Допустимые значения вектора выходных характеристик математической модели, вектора управляющих параметров, исходя из физических и ресурсных ограничений.

Ресурсные ограничения по увеличению количества промежуточных откликов/фрагментов определяются посредством оценки коэффициента использования среды передачи данных:

$$\rho = \frac{1}{V}\frac{\gamma d}{T}, \qquad (1)$$

где, γ – величина дополнительных служебных данных на 1 дополнительный промежуточный отклик/фрагмент, [бит]; V – выделенная скорость передачи данных, [бит/с].

Уравнение объекта управления представляет собой систему линейных дифференциальных уравнений Колмогорова, представляет собой выражение 2.

Решение вышеуказанных уравнений осуществляется с использованием аналитических и численных методов. В частности,

явные, неявные методы Рунге-Кутта 8 порядка, многошаговый метод Адамса 8-го порядка, метод Гира и т.д. С учетом современных возможностей средств вычислительной техники все вышеуказанные методы имеют приемлемую временную сложность (средняя продолжительность вычисления) 10^{-2} с и достаточную точность (относительная погрешность ниже 10^{-5}).

$$\begin{cases} \frac{dp_1}{dt} = p_2\lambda_{21} + p_4\lambda_{41} + p_6\lambda_{61} + p_8\lambda_{81} + p_9\lambda_{91} - p_1\lambda_{12}, \\ \frac{dp_2}{dt} = p_1\lambda_{12} - p_2(\lambda_{21} + \lambda_{23} + \lambda_{24}), \\ \frac{dp_3}{dt} = p_2\lambda_{23} + p_4\lambda_{43} - p_3(\lambda_{34} + \lambda_{35}), \\ \frac{dp_4}{dt} = p_2\lambda_{24} + p_3\lambda_{34} - p_4(\lambda_{41} + \lambda_{43} + \lambda_{45}), \\ \frac{dp_5}{dt} = p_3\lambda_{35} + p_4\lambda_{45} - p_5(\lambda_{56} + \lambda_{57}), \\ \frac{dp_6}{dt} = p_5\lambda_{56} - p_6(\lambda_{61} + \lambda_{67}), \\ \frac{dp_7}{dt} = p_5\lambda_{57} + p_6\lambda_{67} + p_9\lambda_{97} - p_7(\lambda_{78} + \lambda_{79}), \\ \frac{dp_8}{dt} = p_7\lambda_{78} - p_8(\lambda_{81} + \lambda_{89}), \\ \frac{dp_9}{dt} = p_7\lambda_{79} + p_8\lambda_{89} - p_9(\lambda_{91} + \lambda_{97}). \end{cases} \quad (2)$$

Тогда формализованная постановка задачи по максимизации вероятности удержания средства сетевой разведки при обеспечении заданного значения коэффициента использования среды передачи данных может быть представлена выражением:

$$J[u] = p_{уд}(u \mid \rho \le \rho^{кр}) \to \max . \quad (3)$$

3. Результаты расчетов

Решение указанной оптимизационной задачи может быть реализовано с использованием различных методов линейной и нелинейной оптимизации, в частности, в работе используется метод случайного поиска с адаптацией, обеспечивающий приемлемую относительную точность (10^{-5}), временную (средняя продолжительность вычисления 2,18 с) и пространственную сложность (используемый

объем памяти 182 Мб). Для описанного выше примера со значением $\rho^{кр}$=0,001, V=10 Мбит/с значение целевой функции составляет величину J=0,997, а набор оптимальных параметров реализации проактивной защиты сервиса электронной почты представляет собой вектор {d, T }={89 шт.; 0,21 с}. Определение оптимальных параметров проактивной защиты сервиса электронной почты от сетевой разведки при различных ресурсных ограничениях представлено на рисунках 1 и 2:

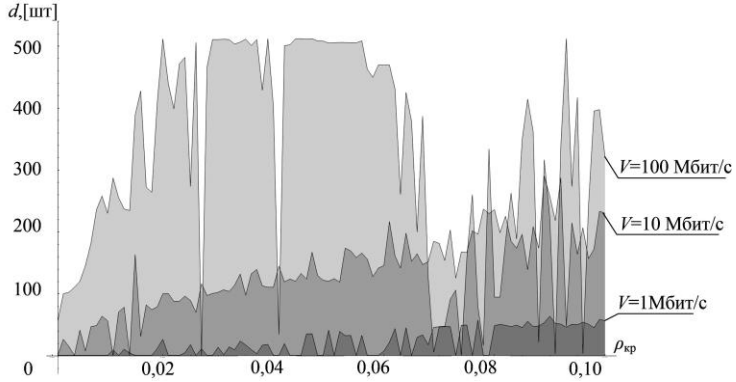

Рис. 2. Принципиальная схема работы проактивной защиты сервиса электронной почты

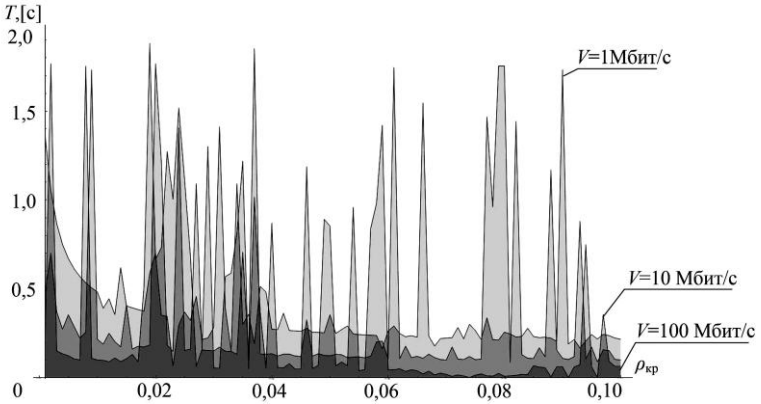

Рис. 3. Принципиальная схема работы проактивной защиты сервиса электронной почты

Заключение

Таким образом, определение оптимальных значений параметров проактивной защиты сервиса электронной почты в условиях воздействия средств сетевой разведки позволяет установить наиболее эффективный режим работы средств проактивной защиты с учетом ресурсных ограничений.

Литература

1. Соколовский, С. П. Концептуализация проблемы проактивной защиты интегрированных информационных систем / С. П. Соколовский, Д. Н. Орехов // Научные чтения имени профессора Н.Е. Жуковского : сб. тр. участников VIII Междунар. научно-практической конф. "Научные чтения имени профессора Н. Е. Жуковского" (Краснодар, 20–21 декабря 2017 г.). – Краснодар, 2018. – С. 47–52.
2. Способ защиты вычислительных сетей [Текст] : пат. 2696330 Российская Федерация : МПК G 06 F 21/50, G 06 F 21/60, H 04 L 9/00 / Соколовский С. П. [и др.] ; заявитель и патентообладатель Краснодарск. высш. воен. училище. – № 2018128075 ; заявл. 31.07.18 ; опубл. 01.08.19, Бюл. № 22. – 30 с.
3. Максимов, Р. В. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей / Р. В. Максимов, С. П. Соколовский, И. С. Ворончихин // Труды СПИИРАН. – 2020. – Т. 19. – № 5. – С. 1018-1049.
4. Соколовский, С.П. Модель конфликта в информационной сфере / С. П. Соколовский, С. Р. Шарифуллин, Е. С. Маленков // VIII Международная научно-практическая конференция молодых ученых, посвященная 57-й годовщине полета Ю.А. Гагарина в космос : сборник научных статей "VIII Международная научно-практическая конференция молодых ученых, посвященная 57-й годовщине полета Ю.А. Гагарина в космос" (Краснодар, 12-13 апреля 2018 г.). – Краснодар, 2018. – С. 299-304.
5. Катунцев С. Л. Моделирование способа обфускации идентификаторов сетевых устройств в интересах минимизации компрометирующих признаков средств проактивной защиты вычислительных сетей / С. Л. Катунцев, Д. Н. Орехов, С. П. Соколовский // Научные труды Кубанского государственного технологического университета. – 2018. – № 3. – С. 239-248.
6. Душкин, А. В. Способ распознавания вредоносных воздействий на информационную систему / А. В. Душкин, В. Н. Похващев, С. П. Соколовский // Телекоммуникации. – 2011. – № 10. – С. 25-28.

7. Соколовский, С. П. Применение адаптивных нечетких систем в вопросах разработки средств выявления несанкционированных воздействий на информацию / С. П. Соколовский, Н. А. Усов // Информатика: проблемы, методология, технологии : материалы XVI Международной научно-методической конференции (Воронеж, 11-12 февраля 2016 г.). – Воронеж, 2016. – С. 259-264.

8. Результаты анализа способов компрометации средств защиты информации / А. Л. Гаврилов [и др.] // Технические и технологические системы : материалы девятой Международной научной конференции «ТТС-17» (Краснодар, 22-24 ноября 2017 г.). – Краснодар, 2017. – С. 117–121.

9. Душкин, А. В. Особенности оценки времени противодействия несанкционированным воздействиям на информационные телекоммуникационные системы / А. В. Душкин, М. Ю. Петшауэр, С. П. Соколовский // Информация и безопасность. – 2009. – № 2. – С. 305-308.

10. Максимов, Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи / Р. В. Максимов, Л. С. Выговский // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2008. – № 3(60). – С. 166-173.

11. Максимов, Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи / Р. В. Максимов, Л. С. Выговский // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2009. – № 1(72). – С. 181-187.

12. Устройство поиска информации [Текст] : пат. 2219577 Российская Федерация : МПК G 06 F 17/40 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Краснодарск. высш. воен. училище. – № 2002111059/09 ; заявл. 24.04.2002 ; опубл. 20.12.2003, Бюл. № 1. – 27 с.

13. Способ выбора безопасного маршрута в сети связи (варианты) : пат. 2331158 Российская Федерация : МПК H 04 L 12/28 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Военная академия связи. – № 2007103774/09 ; заявл. 31.01.2007 ; опубл. 10.08.2008, Бюл. № 22. – 34 с.

14. Максимов, Р. В. Модель случайных помех интегрированным системам ведомственной связи / Р. В. Максимов // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. – 2008. – № 3(60). – С. 151-155.

15. Максимов, Р.В. Этюды технологии маскирования функционально-логической структуры информационных систем / И. И. Иванов, Р. В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции (Санкт-Петербург, 11–12 октября 2017 г.). – Санкт-Петербург, 2017. – С. 147-154.

16. 7. Максимов, Р.В. Спецификация функциональной модели для расширения пространства демаскирующих признаков в виртуальных частных сетях / И. И. Иванов, Р. В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации : Труды всеармейской научно-практической конференции (Санкт-Петербург, 11–12 октября 2017 г.). – Санкт-Петербург, 2017. – С. 138-147.

17. Соколовский, С. П. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров / С. П. Соколовский, И. С. Ворончихин, А. Д. Гритчин // Решетневские чтения : Материалы XXIII Международной научно-практической конференции, посвященной памяти генерального конструктора ракетно-космических систем академика М.Ф. Решетнева (Красноярск, 11–15 ноября 2019 г.). – Красноярск, 2019. – С. 447-448.

18. Способ сравнительной оценки структур информационно-вычислительной сети : пат. 2408928 Российская Федерация : МПК G 06 F 21/20 H 04 L 12/28 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Военная академия связи. – № 2009129726/08 ; заявл. 03.08.2009 ; опубл. 10.01.2011, Бюл. № 1 – 16 с.

19. Способ (варианты) и устройство (варианты) защиты канала связи вычислительной сети : пат. 2306599 Российская Федерация : МПК G 06 F 21/00 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Военная академия связи. – № 2006114272/09 ; заявл. 26.04.2006 ; опубл. 20.09.2007, Бюл. № 26 – 56 с.

20. Способ мониторинга безопасности автоматизированных систем : пат. 2355024 Российская Федерация : МПК G 06 F 15/00 G 06 F 17/00 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Военная академия связи. – № 2007105319/09 ; заявл. 12.02.2007 ; опубл. 10.05.2009, Бюл. № 13 – 15 с.

21. Способ защиты вычислительных сетей : пат. 2649789 Российская Федерация : МПК H 04 L 12/801 H 04 L 29/06 H 04 L 9/32 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Краснодарск. высш. воен. училище. – № 2017125677 ; заявл. 17.07.2017 ; опубл. 04.04.2018, Бюл. № 10 – 25 с.

22. Способ защиты вычислительных сетей : пат. 2696330 Российская Федерация : МПК G 06 F 21/50 G 06 F 21/60 H 04 L 09/00 / Максимов Р. В. [и др.] ; заявитель и патентообладатель Краснодарск. высш. воен. училище. – № 2018128075 ; заявл. 31.07.2018 ; опубл. 01.08.2019, Бюл. № 22 – 30 с.