УДК 621.396.677.49

Ю.Ю. КОЛЯДЕНКО, д-р техн. наук, И.Г. ЛУКИНОВ

МОДЕЛЬ ВЫЯВЛЕНИЯ И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ СВЯЗИ НА ОСНОВЕ АППАРАТА МАРКОВСКИХ ПРОЦЕССОВ

Постановка задачи

В настоящее время значительный интерес представляют исследования беспроводных городских телекоммуникационных сетей, в которых имеется центральная станция, координирующая работу абонентских станций. Именно такая сетевая архитектура является основой технологии программных конфигурируемых сетей (SDN). Отличительными особенностями построения беспроводных городских телекоммуникационных сетей являются высокая сложность протокола подуровня управления доступом к среде, отвечающего, в частности, за организацию доступа абонентов к общему каналу связи, а также наличие большого числа неопределенных частей, в которых стандартизированы лишь некоторые механизмы сетевого взаимодействия. Эти особенности технологии SDN, а также ее новизна приводят к необходимости разработки методов повышения защиты информации при множественном радиодоступе абонентов.

Задача обеспечения безопасности становится особенно актуальной для телекоммуникационных сетей, где канал передачи данных часто разделяется между большим количеством пользователей. В беспроводных городских сетях появляется еще одна проблема – общедоступность канала связи.

Информационная безопасность является одной из составляющих гарантоспособности SDN [1 – 5]. Основную угрозу безопасности таких систем представляют уязвимости, прежде всего, программных компонентов. Поиск уязвимостей в программных компонентах является актуальной и ресурсоемкой задачей, которой занимаются крупные компании и исследовательские центры. Информацию об уязвимостях можно получить из общедоступных информационных источников, например Open Source Vulnerability Database (www.osvdb.org), Common Vulnerabilities and Explosures (www.cve.mitre.org), Natioal Vulnerability Database (www.nvd.nist.gov) и других баз данных уязвимостей.

Однако, несмотря на общедоступность информации об уязвимостях программных продуктов, имеющихся данных недостаточно, чтобы количественно оценивать и сравнивать безопасность программных продуктов по одному обобщенному критерию, а также прогнозировать их защищенность от информационных вторжений в будущем. Одна из основных проблем выбора наиболее защищенной конфигурации SDN заключается в сложности количественной оценки уровня информационной безопасности, а также выбора адекватных показателей для оценки, позволяющих в комплексе учесть все факторы, влияющие на успешное проникновение в сеть и размер потенциального ущерба, который может быть нанесен при эксплуатации имеющихся угроз безопасности.

Цель статьи – исследование подходов к оценке и прогнозированию уровня информационной безопасности программных средств SDN на основе моделирования процессов выявления и устранения уязвимостей с использованием аппарата марковских процессов.

Основная часть

Угрозами информационной безопасности являются отказы, нарушающие готовность сети, целостность или конфиденциальность информации. Причинами этих отказов являются уязвимости – специальный вид дефектов, которые активизируются вследствие

злонамеренных действий (хакерских атак, воздействия вирусов, вредоносных программ и др.).

Предварительный анализ процессов обнаружения и устранения уязвимостей показывает, что они могут быть описаны системой массового обслуживания с неограниченной длиной очереди. Параметры системы массового обслуживания могут быть получены и соотнесены с процессами и статистическими данными об обнаружении и устранении уязвимостей следующим образом [5]:

– число обслуживающих каналов n соответствует количеству организаций или групп разработчиков, которые занимаются устранением уязвимости конкретного программного продукта SDN. В простейшем варианте может быть рассмотрен только один обслуживающий орган;

– интенсивность поступления заявок λ, которая соответствует интенсивности обнаружения уязвимостей в рассматриваемом программном продукте SDN может быть получена на основе анализа базы данных уязвимостей CVE (первичной базы) как количество уязвимостей, опубликованных за рассматриваемый промежуток времени (неделя, месяц, год);

– интенсивность обслуживания заявок μ, которая соответствует интенсивности устранения уязвимостей (выпуска обновлений, исправляющих уязвимости), может быть оценена с использованием информации из бюллетеней безопасности, публикуемых компаниями-производителями программного продукта SDN, а также баз уязвимостей NVD и OSVDB (вторичные базы);

– время обслуживания $T_{обсл}$, соответствующее параметру «количество дней риска» [2, 5], который используется при оценке информационной безопасности программного продукта SDN, определяется как усредненный период времени между появлением и устранением отдельных уязвимостей;

– вероятностью обслуживания поступившей заявки Q является вероятность устранения уязвимости, которая теоретически равна единице; на практике же встречаются ситуации, когда отдельные уязвимости отдельных программных компонентов так и не устраняются;

– вероятность отказа $P_{отк}$ показывает вероятность того, что уязвимость не будет устранена;

– среднее число заявок в СМО $z_{ср}$ показывает среднее количество уязвимостей, которые присутствуют в сети в данный момент времени, и для которых еще не выпущено программное обновление. Данный показатель является одним из наиболее важных, поскольку определяет количество потенциальных возможностей для атаки инфокоммуникационной сети:

– среднее число заявок в очереди $r_{ср}$ определяет, сколько в среднем уязвимостей опубликовано и ожидает выпуска обновления для их устранения;

– среднее время пребывания заявки в очереди $t_{оч.ср}$ показывает, сколько в среднем требуется времени для устранения уязвимости с момента ее обнаружения;

– среднее число занятых каналов $k_{ср}$ говорит о том, сколько рабочих групп в среднем заняты устранением уязвимости.

Рассмотренную выше систему массового обслуживания можно представить в виде системы состояний, в которой каждому состоянию будет соответствовать определенное количество обнаруженных уязвимостей, присутствующих в системе, для которых еще отсутствует рекомендация или программное обновление для устранения. Такие уязвимости будем называть активными. Подобные процессы эффективно описываются марковскими цепями. Марковские цепи имеют сравнительно мало инженерных приложений, так как довольно редко на практике моменты возможных переходов системы из состояния в

состояние заранее известны и фиксированы. Гораздо чаще переходы из состояния в состояние могут происходить не в фиксированные моменты времени, а в случайные.

Будем считать, что переходы системы из состояния в состояние осуществляются под воздействием пуассоновских потоков событий (не обязательно стационарных).

Отсутствие последействия в пуассоновском потоке позволяет при фиксированном настоящем (состояние s_i системы в момент t) не учитывать то, когда и как система оказалась в этом состоянии.

Пусть на графе состояний системы S существует стрелка, ведущая из состояния s_i в одно из соседних состояний s_j (рис.1).

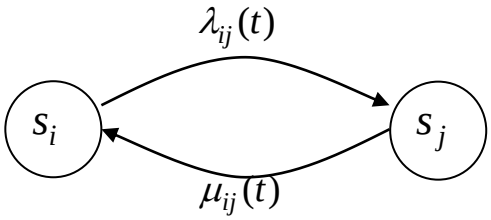

Рис.1. Переход из состояния s_i в одно из соседних состояний s_j под воздействием $\lambda_{ij}(t)$ и $\mu_{ij}(t)$

Будем считать, что переход системы из состояния s_i в состояние s_j осуществляется под воздействием пуассоновского потока событий с интенсивностью $\lambda_{ij}(t)$. Переход из s_i в s_j происходит в момент, когда наступает первое событие потока.

Рассмотрим на оси $0t$ элементарный участок времени Δt, примыкающий к t (рис. 2) и найдем вероятность того, что за время Δt система перейдет из состояния s_i в состояние s_j в предположении, что система находилась в состоянии s_i в момент времени t.

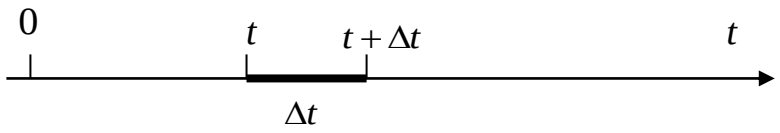

Рис. 2. Элементарный участок времени Δt на оси $0t$

Эта вероятность $p_i(t)=\lambda_{ij}(t)\Delta t$, так как случайная величина равна числу событий потока, попадающих на элементарный участок Δt, имеет математическое ожидание $m=\lambda_{ij}(t)\Delta t$ и с точностью до бесконечно малых высших порядков равна вероятности p_i попадания на элементарный участок одного события.

Если известны, все интенсивности пуассоновских потоков событий, переводящих систему из состояния в состояние, то можно составить систему дифференциальные уравнения для вероятностей состояния.

Пусть для любой пары состояний s_i, s_j известна интенсивность $\lambda_{ij}(t)$ пуассоновского потока событий, переводящая систему из состояния s_i в любое другое состояние s_j ($i\neq j$), будем полагать эту интенсивность равную нулю, если непосредственный переход из состояния s_i в состояние s_j невозможен.

Обозначим $p_i(t)$ – вероятность того, что в момент времени t система находится в состоянии s_i ($i=1,2,...,n$). Теперь придадим t приращение Δt и найдем вероятность $p_i(t+\Delta t)$

того, что в момент $t+\Delta t$ система будет находиться в состоянии s_i. Обозначим это событие A: $A=\{S(t+\Delta t)=s_i\}$.

Как это событие может произойти? Двумя способами: либо произойдет событие B, состоящее в том, что в момент t система уже была в состоянии s_i, и за время Δt не вышла из этого состояния; либо произойдет событие C, состоящее в том, что в момент t система была в одном из соседних s_j, из которых возможен переход в s_i, и за время Δt перешла из состояния s_j в s_i.

Очевидно, $A = B + C$. Найдем вероятности событий B и C. Согласно правилу умножения вероятностей вероятность события B равна вероятности $p_i(t)$ того, что система в
момент t была в состоянии s_i, умноженной на условную вероятность того, что за время Δt она не выйдет из этого состояния, т.е. в суммарном потоке событий, выводящих систему из состояния s_i, не появится ни одного события.

Так как суммарный поток событий, выводящий систему из состояния s_i, как и все его слагаемые, – пуассоновский с интенсивностью, равной сумме интенсивностей слагаемых потоков: $\sum_{j=1}^{n} \lambda_{ij}(t), i \neq j$, то условная вероятность того, что на участке Δt появится хотя бы одно событие (приближенно) $p_i(t) = \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t, i \neq j$, а условная вероятность противоположного события $1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t$.

Таким образом,

$$P(B) = p_i(t)\left[1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t\right]. \quad (1)$$

Найдем теперь вероятность события C. Представим его в виде суммы несовместных вариантов:

$$C = \sum_j C_j, \quad (2)$$

где суммирование распространяется на все состояния s_j, из которых возможен непосредственный переход в s_i. События C, в силу ординарности потоков, можно считать несовместными. По правилу сложения вероятностей

$$P(C) = \sum_j P(C_j). \quad (3)$$

По правилу умножения вероятностей $P(C_j) = p_j(t)\mu_{ji}(t)\Delta t$, откуда

$$P(C) = \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t \quad (i \neq j). \quad (4)$$

Следовательно,

$$P(A) = P(B) + P(C) = p_i(t)\left[1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t\right] + \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t$$

Таким образом,

$$p_i(t + \Delta t) = p_i(t)\left[1 - \sum_{j=1}^{n} \lambda_{ij}(t)\Delta t\right] + \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t. \quad (5)$$

Вычитая из (5) $p_i(t)$, получим приращение функции на участке $t, t + \Delta t$:

$$p_i(t+\Delta t) - p_i(t) = \sum_{j=1}^{n} p_j(t)\mu_{ji}(t)\Delta t - p_i(t)\sum_{j=1}^{n}\lambda_{ij}(t)\Delta t\,.$$

Деля приращение функции на приращение аргумента Δt и устремляя $\Delta t \to 0$, получим для вероятностей $p_i(t)$ систему обыкновенных дифференциальных уравнений с переменными коэффициентами

$$\frac{dp_i(t)}{dt} = \sum_{j=1}^{n} p_j(t)\mu_{ji}(t) - p_i(t)\sum_{j=1}^{n}\lambda_{ij}(t)\ . \qquad (6)$$

Эти уравнения называются уравнениями Колмогорова. Первая сумма в правой части формулы (6) распространяется на те значения j, для которых возможен непосредственный переход из состояния s_j в s_i, а вторая – на те значения, для которых возможен непосредственный переход из состояния s_i в s_j.

Все потоки, переводящие систему S из одного состояния в другое, являются простейшими (стационарными пуассоновскими). Системы, в которых происходит такой процесс, называют простейшими системами. Для простейшей системы вероятности состояний определяются уравнениями Колмогорова с постоянными коэффициентами. Применим преобразование Лапласа к решению системы уравнений Колмогорова. Обозначим изображение вероятности состояния $p_i(t)$ функцией $\pi_i(x)$

$$p_i(t) \to \pi_i(x)\,. \qquad (7)$$

Тогда системе уравнений Колмогорова для вероятностей состояний будет соответствовать система уравнений для их изображений:

$$x\pi_i(x) = \sum_{j=1}^{n}\pi_j(x)\mu_{ji} - \pi_i(x)\sum_{j=1}^{n}\lambda_{ij} + p_i(0)\,, i = 1,2,...,n\,. \qquad (8)$$

Откуда

$$\pi_i(x) = \frac{\sum_{j=1}^{n}\pi_j(x)\mu_{ji} + p(0)}{x + \lambda_i}, \qquad (9)$$

где $\lambda_i = \sum_{j=1}^{n}\lambda_{ij}$.

Таким образом, вместо системы однородных дифференциальных уравнений с постоянными коэффициентами для вероятностей состояний получена система однородных алгебраических уравнений с постоянными коэффициентами для изображений вероятностей состояний.

Эту систему нужно решать с учетом нормировочного условия:

$$\sum_{i=1}^{n} p_i(t) = 1\,. \qquad (10)$$

Следовательно, одно из уравнений можно заменить на

$$\sum_{i=1}^{n}\pi_i(t) = \frac{1}{x}, \qquad (11)$$

которое является изображением нормировочного условия.

Зная интенсивности λ_{ij} и μ_{ij} появления событий, порождаемых потоком, можно сымитировать случайный интервал между двумя событиями в этом потоке:

$$\tau_{ij} = -\frac{1}{\lambda_{ij}}\ln(r)\,,\ \tau_{ji} = -\frac{1}{\mu_{ij}}\ln(r)\,.$$

где τ_{ij} – интервал времени между нахождением системы в i-м и j-м состоянии; r – равномерно распределенное от 0 до 1 случайное число, которое берется из генератора случайных чисел (ГСЧ).

Далее, очевидно, система из любого i-го состояния может перейти в одно из нескольких состояний j, $j + 1$, $j + 2$, …, связанных с ним переходами.

В j-е состояние она перейдет через τ_{ij}; в $(j + 1)$-е состояние она перейдет через τ_{ij+1}; в $(j + 2)$-е состояние она перейдет через τ_{ij+2} и т. д.

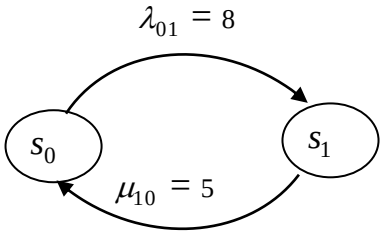

Рис. 3. Граф состояний

Ясно, что система может перейти из i-го состояния только в одно из этих состояний, причем в то, переход в которое наступит раньше.

Поэтому из последовательности времен: τ_{ij}, τ_{ij+1}, τ_{ij+2} и т.д. надо выбрать минимальное и определить индекс j, указывающий, в какое именно состояние произойдет переход.

Рассмотрим пример. Пусть поступают заявки на обнаружения уязвимостей.

Обозначим состояния (рис.3): s_0 – нет заявки, s_1 – поступила заявка. Зададим интенсивности потоков:

λ_{01} = 8 заявок в минуту; μ_{10} = 5 обработанных заявок в минуту.

Будем считать, что система в начальный момент находилась в состоянии s_0.

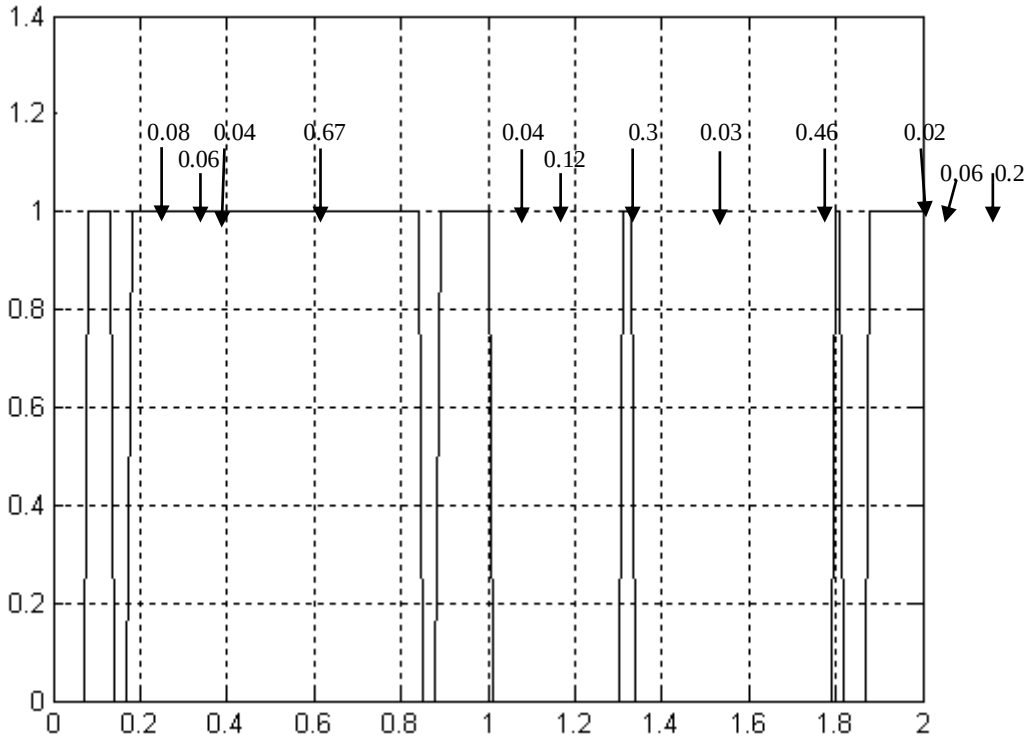

Рис. 4. Временная диаграмма поступления заявок на обнаружение уязвимостей

С помощью имитационного моделирования получена временная диаграмма поступления заявок на обнаружение уязвимостей (рис. 4). Таким образом, зная интенсивности потоков,

можно в реальном масштабе времени моделировать процессы поступления заявок на обнаружение уязвимостей.

Заключение

Информационная безопасность является одной из составляющих гарантоспособности SDN. Основную угрозу безопасности таких систем представляют уязвимости, прежде всего, программных компонентов. Поиск уязвимостей в программных компонентах является актуальной и ресурсоемкой задачей, которой в последнее время занимаются крупные компании и исследовательские центры.

Анализ процессов обнаружения и устранения уязвимостей показывает, что они могут быть описаны системой массового обслуживания с неограниченной длиной очереди. Разработана модель выявления и устранения уязвимостей в программно-конфигурируемых сетях связи на основе аппарата марковских процессов. С помощью данной модели, зная интенсивности потоков, можно в реальном масштабе времени моделировать процессы поступления заявок на обнаружение уязвимостей.

Список литературы: 1. *Avizienis, A.* Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J. C. Lapri, B. Randel // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11–33. 2. *Щеглов, А. Ю.* Безопасность современных ОС «в цифрах» [Электронный ресурс] / А. Ю. Щеглов. – Режим доступа: http://blogs.csoonline.com/days_of_risk_in_2006 (2006). 3. *15th Annual* CSI/FBI Computer Crime and Security Survey. Executive Summary. – CSI, FBI, 2010. – 17 p. 4.*Vulnerability* Disclosure Framework:Final Report and Recommendations by the Council. – Washington : NIAC, 2004. – 52 p. 5. *Белобородов, А. Ю.* Применение аппарата теории массового обслуживания для исследования процессов выявления и устранения уязвимостей программных средств / А. Ю. Белобородов, А. В. Горбенко, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – ISSN 1814-4225. – Харків.- 2014. – С.65-69

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.03.2017