УДК 004.056

Шыхалиев Р.Г.
Институт Информационных Технологий НАНА, Баку, Азербайджан
ramiz@science.az

ОБ ОДНОЙ МОДЕЛИ ЭКРАНИРОВАНИЯ ВЗАИМОУВЯЗАННЫХ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ ПРОСТРАНСТВ С ИСПОЛЬЗОВАНИЕМ СЕТЕЙ ПЕТРИ

В статье предложена модель экранирования взаимоувязанных корпоративных информационных пространств. Для моделирования использованы Сети Петри. СП хорошо подходят для моделирования систем экранирования ВУКИП, которые предписывают политику контроля доступа на основании правил фильтрации. Построенная модель может использоваться для имитации и тестирования системы экранирования ВУКИП и проверки корректности политики безопасности, осуществляемой ею. Также эта модель может быть использована как основа для проектирования средств анализа систем экранирования ВУКИП.

Ключевые слова: *Сети Петри, взаимоувязанные корпоративные информационные пространства, экранирование, правила фильтрации, пакет.*

Введение

Необходимым условием создания информационного общества в любой стране является формирование единого государственного корпоративного информационного пространства и интеграция его в глобальное мировое информационное пространство. В связи с этим очень существенным представляется формирование взаимоувязанных корпоративных информационных пространств (ВУКИП). ВУКИП – это территориально-распределенная информационная структура, являющаяся совокупностью взаимосвязанных и взаимодействующих корпоративных информационных пространств (КИП) на базе единых корпоративных стандартов, которая обеспечивает доступ к информации пользователей в рамках их полномочий, в каком бы КИП они ни оказались. В контексте информационной безопасности каждое КИП имеет свою политику безопасности.

Определяющим фактором при формировании ВУКИП, на которое необходимо обратить внимание, является обеспечение информационной безопасности. Для решения этой задачи необходимо в рамках ВУКИП создать такую среду, которая обеспечит защиту корпоративного сетевого пространства, информационных ресурсов и предоставление пользователям возможности безопасной работы с информационными ресурсами, в каком бы КИП они ни находились. Средством, позволяющим создать такую среду, является межсетевой экран (МСЭ). Обычно МСЭ располагается между двумя сетями, имеющими различные политики безопасности, и контролирует все информационные потоки, проходящие через него. Основной задачей МСЭ является пресечение попыток несанкционированного доступа (НСД) в защищаемую сеть и выполнение следующих функций:

- контроль доступа;

- протоколирование информационных потоков;
- сокрытие топологии защищаемой сети;
- реагирование на НСД.

Эти задачи широко описаны в [1–3]. В совокупности выполнение этих задач делает МСЭ полным.

Экранирование ВУКИП достигается путем установления МСЭ в местах подключения данного КИП к открытым информационным пространствам (например, Internet) и другим КИП. Экранирование – функция МСЭ, позволяющая поддерживать безопасность объектов внутреннего информационного пространства, игнорируя несанкционированные запросы из внешнего информационного пространства. Основными элементами описания экранирования ВУКИП являются:

- информационные пакеты (информационный трафик);
- субъекты информационного взаимодействия;
- объекты информационного взаимодействия;
- правила фильтрации (перечень условий, по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов, и перечень действий, производимых МСЭ по регистрации и/или осуществлению дополнительных защитных функций);
- критерии фильтрации (параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи пакета в соответствии с заданными правилами разграничения доступа (правилами фильтрации).

Несмотря на то, что МСЭ широко применяется для обеспечения информационной безопасности КИП, необходимо подчеркнуть, что многие вопросы, связанные с организацией и проектированием системы для экранирования таких распределенных информационных пространств, как ВУКИП, пока еще остаются нерешенными. Так как для ВУКИП требуется стратегия экранирования, существенно отличная от используемых в отдельно взятых КИП. Исходя из этого, при экранировании ВУКИП необходимо решить ряд основных задач, к которым относится анализ корректности политики безопасности, осуществляемой МСЭ, описание функциональных возможностей МСЭ, формализация процесса экранирования и т.д.

Статья посвящена вопросу формализации процесса экранирования ВУКИП. При формализации процесса экранирования ВУКИП целесообразно использовать свойства Сети Петри, что позволяет решать задачи моделирования и анализа процесса экранирования.

Постановка задачи

Безотносительно к используемым МСЭ, на основе которых осуществляется экранирование ВУКИП, экранирование в первую очередь определяется множеством пакетов U и множеством правил фильтрации (политиками безопасности КИП) R.

Пусть $R=\{r_1, r_2, ..., r_n\}$ – множество правил фильтрации и $U=\{u_1, u_2, ..., u_m\}$ – множество пакетов. Для каждого правила фильтрации $r_i \in R,\ i=\overline{1,n}$ определены

множества входных и выходных пакетов, обрабатываемых данным правилом, т.е. задана матрица взаимосвязей правил фильтрации и пакетов. Требуется представить процесс экранирования ВУКИП с помощью СП, определенной набором $N=\{P,T,F,W,M_0\}$.

Модель экранирования ВУКИП

Сети Петри – это набор $N=\{P,T,F,W,M_0\}$, где P – непустое конечное множество состояний; T – непустое конечное множество переходов;

$F: P\times T\to\{0,1\}, W: T\times P\to\{0,1\}$ – функции инцидентности;

$M_0: P\to\{0, 1, 2, \ldots\}$ – начальная разметка СП [4].

Графически СП представляется в виде ориентированного графа. Множество вершин графа образует множество $P\bigcup T$. Вершина-состояние p и вершина-переход t соединяются дугой (p, t), если $F(p, t)=1$, и дугой (t, p), если $W(t, p)=1$. Вершины-состояния помечаются целыми неотрицательными числами, а при графическом изображении СП – соответствующим числом маркерных точек.

Если все состояния сети обозначить последовательно символами $p_1, p_2, \ldots, p_n$, то разметка представляется в виде n-мерного вектора M, координаты которого равны числу маркерных точек в соответствующих состояниях.

Функционирование СП заключается в переходе от одной разметки к другой. Смена разметок происходит в результате срабатывания одного из переходов. Переход t может сработать при разметке M, если

$$M(p)-F(p,t)\geq 0,\quad \forall p\in P. \qquad (1)$$

Это означает, что каждое входное состояние перехода t помечено хотя бы одной маркерной точкой.

В результате срабатывания некоторого перехода t, удовлетворяющего условию (1), разметка M заменяется $M': \forall p\in P, M'(p)=M(p)-F(p,t)+W(t, p)$, т.е. при срабатывании перехода из каждого его входного состояния удаляется и в каждое выходное состояние добавляется одна маркерная точка и говорится, что разметка M предшествует M' и обозначается $M\xrightarrow{t}M'$.

Функционирование СП можно представить в виде графы достижимости, вершинами которой являются отдельные разметки сети. Две вершины M и M' графы достижимости соединяются дугой, помеченной символом t, если $M\xrightarrow{t}M'$.

Для того чтобы представить процесс экранирования ВУКИП с помощью СП, сначала поставим в соответствие каждому пакету $u_j\in U,\ j=\overline{1, m}$ вершину-состояние p_j СП N. Множество состояний p_j обозначим P, $P=\{p_j,\ j=\overline{1, m}\}$.

Каждое правило фильтрации $r_i\in R,\ i=\overline{1, n}$ поставим в соответствие с переходом t_i сети. Множество переходов обозначим T, $T=\{t_i, i=\overline{1, n}\}$.

Выполнение условий правила фильтрации r_i соответствует срабатыванию перехода t_i.

В соответствии с матрицей взаимосвязи правил и пакетов соединяем дугами элементы множества P и T, т.е. устанавливаем взаимосвязи между элементами этих множеств. Элемент $p_j \in P,\ j=\overline{1,m}$ соединяется с элементом $t_i \in T, i=\overline{1,n}$ дугой (p_j, t_i), если пакет $u_j \in U,\ j=\overline{1,m}$ является входным пакетом правила $r_i \in R,\ i=\overline{1,n}$, и дугой (t_i, p_j), если он является выходным для правила $r_i \in R,\ i=\overline{1,n}$. Поскольку пакет ВУКИП может являться входным для нескольких правил фильтрации, то для восстановления маркерных точек состояния $p_j \in P,\ j=\overline{1,m}$ после срабатывания перехода $t_i \in T, i=\overline{1,n}$ необходимо также построить дуги (t_i, p_j) для таких t_i и p_j, для которых существует дуга (p_j, t_i).

Функционирование СП определяется в каждый момент времени расположением маркерных точек в вершинах-состояниях. Переход $t_i \in T, i=\overline{1,n}$ может сработать, если все его входные состояния $p_j \in P,\ j=\overline{1,m}$, для которых существует дуга (p_j, t_i), имеют хотя бы по одному маркеру.

Определим исходную разметку построенной СП. Те пакеты, которые не являются выходными ни для одного правила фильтрации, называются входными пакетами системы экранирования ВУКИП. Каждое состояние СП, соответствующее входному пакету системы экранирования ВУКИП, помечается маркерной точкой. Полученный таким образом вектор M_0 и будет исходной разметкой сети.

Таким образом, модель экранирования ВУКИП может быть формализована с помощью СП, заданной набором $N=\{P,T,F,W,M_0\}$, где $P=\{p_j,\ j=\overline{1,m}\}$ – множество состояний сети (пакеты ВУКИП); $T=\{t_i, i=\overline{1,n}\}$ – множество переходов сети (правила фильтрации пакетов);

$$F(p,t)=\begin{cases}1, \textit{ если состояние } p\in P \textit{ связано с переходом } t\in T \textit{ дугой } (p,t),\\ 0, \textit{ в противном случае};\end{cases}$$

$$W(t,p)=\begin{cases}1, \textit{ если переход } t\in T \textit{ связан с состоянием } p\in P \textit{ дугой } (t,p),\\ 0, \textit{ в противном случае};\end{cases}$$

$M_0(p)=\{0/1\},\ \forall p$ – исходная разметка сети.

При срабатывании переходов СП начальная разметка изменяется. Пусть разметка M_l достижима от разметки M_k. Тогда $M_k(p) \le M_l(p)$, т.е. $\forall p \in P,\ M_k(p) \le M_l(p)$. Это следует из того, что для любого перехода $t_i \in T, i=\overline{1,n}$ выполняется условие $\forall p \in w(t_i): F_k(p,t_i)=W_l(t_i,p)=1$.

Конечной разметкой M_z назовем такую разметку СП, для которой $M_z(p) > 0, \forall p \in P$. Такая разметка соответствует окончанию функционирования СП или окончанию фильтрации пакетов.

Любой путь в графе достижимости, приводящий из исходной разметки к конечной, называется возможным. Возможный путь, удовлетворяющий всем ограничениям на функционирование системы экранирования и, соответственно, на функционирование СП, называется допустимым.

Теперь определим тип СП, построенной для моделирования системы экранирования ВУКИП. При экранировании ВУКИП каждое правило фильтрации срабатывает один раз, поэтому и переходы СП срабатывают один раз. Каждый пакет (состояние) является результатом срабатывания одного правила фильтрации (перехода). При начальном маркировании сети каждое ее входное состояние помечается только одним маркером, т.е. $\forall p \in P : M_0(p) \le 1$.

Рассмотрим произвольное состояние СП p. Как известно, изменение числа маркерных точек в состоянии p при срабатывании перехода t производится по следующему правилу:

$$M'(p) = M(p) + W(t, p) - F(p, t).$$

Если изменение разметки произошло при срабатывании перехода t, для которого состояние p является входным (т.е. $F(p, t) = 1$), то число маркерных точек в состоянии p не изменится, так как в этом случае $W(t, p) = 1$ по построению СП. Если же состояние p является выходным для перехода t, то число маркерных точек увеличится на единицу. Поскольку такой переход единственный для состояния p и он срабатывает один раз, то $M'(p) = 1$. Если состояние p не связано с переходом t, то $W(t, p) = 0$ и $F(p, t) = 0$ и, следовательно, $M'(p) = M(p)$. Таким образом, построенная СП, моделирующая работу системы экранирования ВУКИП, является безопасной.

Проблема распознавания живучести и безопасности СП довольно сложна, так как это решение связано с большими вычислительными трудностями из-за того, что производится построение и просмотр графы достижимости.

Для проверки того, что СП, моделирующая работу системы экранирования ВУКИП, является живой, предлагается следующий алгоритм.

1. Определить начальную разметку сети, т.е. построить вектор M_0, $i = 0$.
2. Если все координаты вектора M_i равны единице, перейти к п.6, в противном случае – к п.3.
3. Определить множество переходов сети T_i, такое, что $t \in T_i$, если $\forall p \in w(t) : M_i(p) > 0$.
4. Если $T_i = \varnothing$, то перейти к п.7, в противном случае – к п.5.
5. $M_{i+1} = M_i$. Изменить разметку сети M_{i+1} следующим образом: $\forall p \in \bigcup_{t \in T_i} f(t) : M_{i+1}(p) = 1$, $i = i + 1$. Перейти к п.2.

6. Сеть Петри определяется как живая. Останов.
7. Сеть Петри не является живой. Останов.

Таким образом, при корректном выборе необходимых множеств правил фильтрации и пакетов на этапе предварительного анализа СП, моделирующая данную систему экранирования ВУКИП будет правильной.

Заключение

Статья представляет модель экранирования ВУКИП. При формализации процесса экранирования ВУКИП использованы свойства СП, которые позволяют решать задачи моделирования и анализа процесса экранирования. Сети Петри обеспечивают нас теоретической основой и средствами описания, построения, имитации и анализа систем экранирования ВУКИП.

Модель на основе СП может быть основным инструментом доказательства соответствия системы экранирования ВУКИП заданной политике безопасности. Кроме того, модель может использоваться для имитации и тестирования системы экранирования ВУКИП и проверки корректности осуществляемой ею политики безопасности. Также эта модель может быть использована как основа для проектирования средств анализа систем экранирования ВУКИП.

Литература

1. Алгулиев Р.М., Шыхалиев Р.Г. Методы и технологические аспекты экранирования взаимоувязанных корпоративных информационных пространств. Баку: Элм, 2003 – 106 с.
2. Оглтри Т. Firewalls. Практическое применение межсетевых экранов: Пер. с англ. – М.: ДМК Пресс, 2001 – 400 с.
3. Польман Н., Кразерс Т. Архитектура брандмауэров для сетей предприятия: Пер. с англ. – М.: Издательский дом «Вильямс», 2003 – 432 с.
4. Котов В.Е. Сети Петри. – М.: Наука, 1984 .– 160 с.

UOT 004.056
Şıxəliyev R.H.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

ramiz@science.az

Petri şəbəkələri əsasında qarşılıqlı əlaqəli korporativ informasiya fəzalarının ekranlaşdırılması modeli haqqında

Qarşılıqlı əlaqəli korporativ informasiya fəzalarının (QƏKİF) ekranlaşdırılması modeli təklif edilmişdir. Modelləşdirmə üçün Petri Şəbəkələri (PŞ) istifadə edilmişdir. QƏKİF-nın ekranlaşdırılması sisteminin modelləşdirilməsi üçün PŞ ən yararlı riyazi aparatdır. Gurulmuş model QƏKİF-nın ekranlaşdırılması sisteminin imitasiyası, testləşdirilməsi və həçinin onun həyata keçirilən təhlükəsizlik siyasətinin korrektliyinin yoxlanması üçün istifadə edilə bilər. Həmçinin bu model QƏKİF-nın sistemin analizi vasitələrinin layihələndirilməsi üçün əsas kimi istifadə edilə bilər.

Açar sözlər. *Petri şəbəkələri,qarşılıqlı əlaqəli korporativ informasiya fəzaları, ekranlaşdırılma, süzmə qaydaları, paket.*

Shikhaliyev R.H.
Institute of Information Technology ANAS, Baku, Azerbaijan
ramiz@science.az

About a model of firewalling the interconnected corporative information areas using Petri Nets

In paper the model of firewalling of interconnected corporative information areas (ICCIA) is offered. For modelling are used Petri Nets (PN). The PN are a good approach for modelling of firewalling systems of ICCIA which enforce a policy of the access control on the basis of a filtration rules. The proposed model can be used for imitation and testing of system of firewalling ICCIA and check of a correctness of a security policy, carried out by it, also this model can be used as a basis for designing tools for the analysis of firewalling systems of ICCIA.

Key words: *Petri nets, interconnected corporative information areas, firewalling, filtration rules, packet.*