ВЫБОР ВАРИАНТА УПРАВЛЕНИЯ ЗАЩИЩЕННОЙ СИСТЕМОЙ

© 2013 г. П.С. КОСТОМАРОВ

Московский институт электроники и математики НИУ ВШЭ
e-mail: Pavel.Kostomarov@gmail.com

Введение

Под процессом обработки информации понимаются действия, связанные с её хранением, преобразованием и передачей. В дополнение к этому, кроме традиционных свойств, которыми обладают автоматизированные системы – надёжности, эффективности, удобства использования и так далее, защищённая система обработки информации должна обладать ещё одним – свойством безопасности, которое является для неё самым главным.

При синтезе оптимального управления процессами обработки информации одной из наиболее важных с практической точки зрения является задача оптимального выбора варианта управления с позиции безопасности защищенных систем [1].

Как и все автоматизированные системы обработки информации, защищённые системы решают задачу автоматизации некоторого процесса обработки информации. Такая система должна соответствовать сложившимся требованиям и представлениям, обеспечивать возможность сопоставления параметров и характеристик для того, чтобы их можно было сравнивать между собой [2].

Таким образом, под защищённой системой обработки информации предлагается понимать систему, которая обладает следующими тремя свойствами:

- осуществляет автоматизацию некоторого процесса обработки конфиденциальной информации, включая все аспекты этого процесса, связанные с обеспечением безопасности обрабатываемой информации;
- успешно противостоит угрозам безопасности, действующим в определённой среде;
- соответствует требованиям и критериям стандартов информационной безопасности.

Предложенный подход рассматривает проблему обеспечения безопасности систем на стыке автоматизации обработки информации и общей безопасности.

Безопасность является качественной характеристикой системы. Её нельзя измерить в каких-либо единицах, или, скажем, нельзя сравнивать безопасность двух систем с однозначным результатом, т. к. он зависит от конкретной ситуации, возникшей в условиях эксплуатации системы. Для объединения всех специалистов, работающих над созданием защищенных систем необходимо определить, что является целью исследований, чего мы хотим добиться в результате и чего в состоянии достичь.

Модели безопасности защищенных систем

Модель безопасности Харрисона-Руззо-Ульмана [3], являющаяся классической дискреционной моделью, реализует произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа. Система обработки информации представляется в виде совокупности активных сущностей – субъектов (множество S), которые осуществляют доступ к информации, пассивных сущностей – объектов (множество O), содержащих защищаемую информацию, и конечного множества

прав доступа $R = \{r_1, ..., r_n\}$, означающих полномочия на выполнение соответствующих действий (например, чтение, запись, выполнение).

Поэтому критерий безопасности формулируется следующим образом: для заданной системы начальное состояние $Q_0 = (S_0, O_0, M_0)$ является безопасным относительно права r, если не существует применимой к Q_0 последовательности команд, в результате которой право r будет занесено в ячейку матрицы M, в которой оно отсутствовало в состоянии Q_0 [3].

Данная модель является наиболее простой в реализации и эффективной в управлении с точки зрения практики построения защищенных систем, не требует никаких сложных алгоритмов и позволяет управлять полномочиями пользователей с точностью до операции над объектом. Ее критерий безопасности является весьма сильным, поскольку позволяет гарантированность недоступности определённого объекта для субъекта, которому изначально не выданы соответствующие полномочия [4].

Дискреционная модель Харрисона-Руззо-Ульмана в своей общей постановке не дает гарантий безопасности системы, однако именно она послужила основой для целого класса моделей политик безопасности, которые используются для управления доступом и контроля за распространением прав во всех современных системах.

Развитие модель Харрисона-Руззо-Ульмана получила в другой дискретной системе – "Типизованная матрица доступа" (Type Access Matrix – далее TAM) [2].

Формальное описание модели TAM включает следующие элементы:

1. конечный набор прав доступа $R = \{r_1, ..., r_i\}$;
2. конечный набор типов $T = \{ t_1, ..., r_g\}$;
3. конечные наборы исходных субъектов $S_0 = \{s_1, ..., s\}$ и объектов $O_0 = \{o_1, ..., o_m\}$, где $S_0 \subseteq O_0$;
4. матрица M, содержащая права доступа субъектов к объектам, и её начальное состояние M_0;
5. конечный набор команд $C = \{ \alpha_i (x_1,. x_k)\}$, включающий условия выполнения команд и их интерпретацию в терминах элементарных операций.

Тогда состояние системы описывается четвёркой

$$Q = (S, O, t, M) ,$$

где S, O, и M обозначают соответственно множество субъектов, объектов и матрицу доступа, а $t: O \rightarrow T$ – функция, ставящая в соответствие каждому объекту некоторый тип [2; 3].

Система в модели безопасности Белла-ЛаПадулы, представляется в виде множеств субъектов S, объектов O (множество объектов включает множество субъектов, $S \subset O$) и прав доступа read (чтение) и write (запись). Рассматриваются только эти два вида доступа, и хотя она может быть расширена введением дополнительных прав (например, правом на добавление информации, выполнение программ и так далее), все они будут отображаться в базовые (чтение и запись). Использование столь жёсткого подхода, не позволяющего осуществлять гибкое управление доступом, объясняется тем, что в мандатной модели контролируются не операции, осуществляемые субъектом над объектом, а потоки информации, которые могут быть только двух видов: либо от субъекта к объекту (запись), либо от объекта к субъекту (чтение).

Недостаток основной теоремы безопасности Белла-ЛаПадулы состоит в том, что ограничения, накладываемые теоремой на функцию перехода, совпадают с критериями безопасности состояния, поэтому данная теорема является избыточной по отношению к определению безопасного состояния. Поскольку не имеется никаких определённых ограничений на вид функции перехода, кроме указанных в условиях теоремы, и допускается, что уровни безопасности субъектов и объектов могут изменяться, то можно представить такую гипотетическую систему (она получила название Z-системы), в которой при попытке низкоуровневого субъекта прочитать информацию из высокоуровневого объекта будет происходить понижение уровня объекта до уровня субъекта и осуществляться чтение [5].

Пример применения обобщенного принципа адаптивного управления

Функция перехода Z-системы удовлетворяет ограничениям основной теоремы безопасности, и все состояния такой системы также являются безопасными в смысле критерия Белла-ЛаПадулы, но вместе с тем в этой системе любой пользователь сможет прочитать любой файл, что, очевидно, несовместимо с безопасностью в обычном понимании [1].

Такая трактовка требует формирования обобщенного принципа адаптивного управления – принципа адаптации по прогнозирующей оценке эффективности, который лежит в основе методики выбора вариантов управления.

Пусть в дискретные моменты времени t_i (i=0,…,k) осуществляется выбор одного из заданных N возможных вариантов u(1),…,u(N) управления работой динамической системы с вектором состояния $x(t_i)$ (i=0,…,k) (вектор x(·) размерности n, вектор u(·) размерности m×N m≥1). Эволюция вектора состояния x(·) определяется оператором перехода Ф:

$$\mathbf{x}(t_{i+1}) = \Phi[\mathbf{x}(t_i), \mathbf{u}(t_i), \xi(t_i)], \tag{1}$$

где $\xi(t_i) - 1$-мерный вектор шумов, действующий на систему; $u(t_i)$- вариант управления динамической системой, выбранной на момент t_i.

На траекториях системы (1) задана некоторая (обычно скалярная) функция потерь $L[x(t_i),u(l_i)\ i=0,\ldots,k)]$. Задача выбора вариантов управления состоит в определении вариантов управления $\mathbf{u}(l_{t_i})\,(i = 0,...,k),$ обеспечивающих решение задачи оптимизации

$$M\{L[x(t_i), u(l_{t_i}), \xi(t_i) \quad i = 0,...,k]\} \to \max$$

на множестве допустимых значений

$$\{\mathbf{x}(t_i), \mathbf{u}(l_{t_i}), \quad i = 0,...,k\} \in D. \tag{2}$$

Данная постановка задачи достаточно общая и включает различные частные случаи задач выбора оптимальных вариантов управления. Рассмотрим математические модели адаптивного выбора вариантов управления динамической системой [6].

Пусть динамическая система описывается n-мерным (n>0) вектором x(t,p), где p-m-мерный (m>0) вектор параметров, описывающих структуру, состав и вариант функционирования исследуемой системы. Процесс функционирования протекает в интервале времени $[t_0,t_k]$ (возможно бесконечном); $-\infty<t_0<t_k\le+\infty$. На траекториях динамической системы x(t,p) ($t_0\le t\le t_k$) задан критерий эффективности системы K(p) (векторный, вообще говоря) размерности l(l > 0). Семейство x(t,p) является многомерным случайным процессом, заданным на некотором вероятностном пространстве (Ω,F,P) с полным множеством событий $\{\varpi \in \Omega\}$(ϖ - элементарное событие), F- σ-алгебра, а P- вероятностная мера (вероятность), определенная на множествах из F [1].

Определенный на отрезке $[t_0,t_k]$ случайный процесс x(t,p) и возрастающая последовательность σ - алгебр $\{\mathbf{A}_i, t \in [t_0, t_k]\}$($A_{t_i} \subset A_{t_2}$ при $t_1 < t_2\ t_1, t_2 \in [t_0, t_k]$) называются адаптированными, если при каждом $t \in [t_0, t_k]$ процесс x(t,p) является A_t- измеримым. При этом события из A являются предыдущими по отношению к моменту t.

Пусть $\{\mathbf{A}_t, t \in [t_0, t_k]\}$- возрастающее семейство σ- подалгебр σ- алгебры A. Отображение τ нулевого подмножества Ω_τ множества Ω в интервале $[t_0,t_k]$, если удовлетворяет условию{$\tau \le t \in A_i$ при $t \in [t_0,t_k]$}, - момент остановки. Каждому моменту остановки сопоставляется σ- алгебра подмножеств A_τ множества Ω_τ, удовлетворяющих условию $\mathbf{A} \cap \{\tau \le t\} \in \mathbf{A}_t$ при всех $t \in [t_0, t_k]$.

События из A_τ являются предыдущими по отношению к τ. В дискретном по времени случае процесса $(x(t,p)_\tau$ принимает лишь счетное или конечное множество значений) τ есть момент остановки относительно семейства $\{\mathbf{A}_t, t\in[t_0,t_k]\}$тогда, и только тогда, когда $\{\tau = t\}\in \mathbf{A}_i$ при всех t, являющихся значениями τ. Если τ- некоторый момент остановки относительно семейства $\{\mathbf{A}_t, t\in[t_0,t_k]\}$, то моментом остановки будет и любое другое измеримое отображение $\xi(\tau):[t_0,t_k]\to[t_0,t_k]$, удовлетворяющее условию $\xi(t)\ge t$ для всех $t\in[t_0,t_k]$.

Введем отношение порядка в множество возможных моментов, определенных относительно фиксированного возрастающего семейства σ- алгебр $\{A_t\}$, а именно будем говорить, что $\tau_1\le\tau_2$ (τ_1 предшествует τ_2), если $\Omega_{\tau_2}\subset\Omega_{\tau_1}, \tau_1(\omega)\ge\tau_2(\omega), \text{если } \omega\in\Omega_{\tau_2}$. С помощью отношения порядка моментов определяются верхняя и нижняя грани двух произвольных моментов остановки τ_1 и τ_2:

$$\bar{\tau}=\tau_1\vee\tau_2=\mathbf{max}[\tau_1(\omega),\tau_2(\omega)];$$

$$\underline{\tau}=\tau_1\wedge\tau_2=\begin{cases}\tau_1(\omega), \text{если } \omega\in\Omega_{\tau_1}\cap\Omega^c_{\tau_2}=\Omega_{\tau_1}/\Omega_{\tau_2},\\ \mathbf{min}[\tau_1(\omega),\tau_2(\omega)], \text{если } \omega\in\Omega_{\tau_1}\cap\Omega_{\tau_2},\\ \tau_2(\omega), \text{если } \omega\in\Omega^c_{\tau_1}\cap\Omega_{\tau_2}=\Omega_{\tau_2}/\Omega_{\tau_1},\end{cases}$$

причем область определения $\bar{\tau}$ есть $\Omega_{\bar{\tau}}=\Omega_{\tau_1}\cap\Omega_{\tau_2}$. Таким образом определенная функция $\bar{\tau}$ есть функция множества $\Omega_{\tau_1}\cup\Omega_{\tau_2}$.

Если (Ω,A,P) – некоторое вероятностное пространство, τ- момент остановки, определенный на Ω_τ относительно возрастающего семейства $\{\mathbf{A}_t, t\in[t_0,t_k]\}$, и x(t,p) ($t\in[t_0,t_k]$) – случайный (многомерный) процесс, адаптированный к $\{\mathbf{A}_t, t\in[t_0,t_k]\}$, то отображение $x(\tau(\omega),p)$ множества Ω_τ в множество R^n является A_τ -измеримым, если момент остановки τ принимает лишь счетное множество различных значений [1].

Достаточно эффективно описать поведение многоэтапного функционирования динамических систем позволяет сформированная в теории случайных процессов методика марковских моментов. Рассмотрим задание многоэтапного функционирования динамической системы x(t,p) с помощью некоторой последовательности марковских моментов (моментов остановки) $\tau_1,\ldots,\tau_N$, где N- число отдельных этапов функционирования системы. Этапы определяются выполнением различных целевых операций, вследствие которых меняются условия функционирования системы. Чаще всего это происходит за счет того, что система функционирует в различных областях $B_1,B_2,\ldots,B_N$ фазового пространства. Марковские случайные моменты $\tau_1,\ldots,\tau_N$ определяются моментами времени первого попадания в множества $B_1,B_2,\ldots,B_N$ соответственно. Множества B_i (i=1,…,N) попарно не пересекаются: $\mathbf{B_i}\cap\mathbf{B_k}=0\,(\mathbf{j,k=1,...,N})$. Предположим, что вначале семейство множеств $B_1,B_2,\ldots,B_N$ удовлетворяет свойству невозвратности по времени функционирования:

$$\mathbf{P}\{\mathbf{x}(t_1,\mathbf{p})\in\mathbf{B_i}\,|\,\mathbf{x}(t_2,\mathbf{p})\in\mathbf{B_k}\}>0, l<k(l,k=1,...,N); t_1,t_2[t_0,t_k], t_1<t_2.$$

Здесь $P\{\cdot\}$ – вероятность, заданная на фазовом пространстве траекторий рассматриваемой динамической системы.

Сформулированное условие означает, что совокупность множеств $B_1,B_2,\ldots,B_N$ определяет “поступательное” функционирование системы. Возвращение на предыду-

щие этапы невозможно, возможны переходы на этапы функционирования, имеющие несоседние индексы (отличающиеся более чем на единицу):

$$\mathbf{P}\left\{\mathbf{x}(t_1,\mathbf{p})\in \mathbf{B}_1 \middle| \mathbf{x}(t_2,\mathbf{p})\in \mathbf{B}_k\right\}>0,$$
$$|l-k|>1, l\geq k; t_1, t_2\in[t_0, t_k], t_1<t_2. \quad (3)$$

Последнее соотношение означает наличие нескольких альтернатив в ходе функционирования системы, возможность невыполнения некоторых этапов функционирования, частичное решение целевой задачи и т. д. [7].

Заключение

При решении задачи выбора вариантов управления защищенными системами необходимо учитывать следующие особенности:

- сложность структуры и режимов функционирования;
- сложность и изменение целевых задач в процессе функционирования;
- многофакторный и заранее непредсказуемый характер условий функционирования.

Все это приводит к необходимости привлечения адаптивных систем управления. Внедрение их связано в первую очередь с развитием современных средств вычислительной техники, позволяющих реализовать управление в реальном масштабе времени. В современных системах управления стремятся рационально сочетать принципы программного (автономного) управления и управления с обратной связью. Адаптация понимается как способность защищенной системы гибко реагировать на факторы, сопутствующие реальному процессу функционирования.

СПИСОК ЛИТЕРАТУРЫ

1. *Болнокин В.Е.* Адаптивное управление на базе нечетких регуляторов и нейросетевой технологии: Монография/ В.Е. Болнокин, Хо Д. Лок. – Воронеж: Издательство «Научная книга», 2012. – 280 с.
2. *Васин В.А., Ивашов Е.Н., Степанчиков С.В.* Защищенные структуры для систем кодирования и криптографии // Вопросы защиты информации. 2012.– № 4, с. 38 – 46.
3. *Harrison M., Ruzzo W., Uhlman J.* Protection operating systems // Communications of the ACM, 1976.
4. *Harrison M., Ruzzo W.* Monotonic protection system// Foundation of secure computation, 1978.
5. *Leonard J. LaPadula and D. Elliot Bell.* Secure Computer Systems: A Mathematical Model // MITRE Corporation Technical Report, 2547, V. II, 31 May 1973.
6. *Ciaran Bryce* Lattice-Based Enforcement of Access Control Policies // Arbeitspapiere der GMD (Research Report), N. 1020, August 1996.
7. *John McLean* The Specification and Modeling of Computer Security // Computer, 23(1): 9-16, January 1990.