M. A. Styugin

Protection Systems against Unauthorized Access by Modifying the Structures Awareness Subjects

Keywords: informational structure, mathematical modeling, information security, information limitations, functional invisibility

In this paper, we propose to divide the actual structure of information systems and the subject information structure. An example of such separation on mathematical models of information security is given. It can determine on the basis of mathematical models what subjective images of a system are stable, and define the conditions under which we can confirm that our own subjective image of a system is an objective one. A task of hiding any processes by modifying the structure of information flows in a system is given.

М. А. Стюгин

ПРОТИВОДЕЙСТВИЕ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ ПУТЕМ МОДИФИКАЦИИ СТРУКТУР ИНФОРМИРОВАННОСТИ СУБЪЕКТОВ[1]

Введение

В области моделирования конфликтных систем очень подробно рассматриваются вопросы информированности субъектов конфликта. Информированность играет ключевую роль в определении конфликтных стратегий. Однако вопрос информированности на сегодняшний день недостаточно хорошо освещен в области информационной безопасности. В любых задачах безопасности можно выделить антагонистические интересы защитника и атакующего. От того, насколько адекватно каждый из них видит информационную систему, зависит исход конфликта, а можно сказать, и уровень безопасности системы. Каждый день в мире находят множество новых уязвимостей популярного программного обеспечения. Программное обеспечение, которое сейчас оценивается как безопасное по результатам тестирования, возможно, в ближайшем будущем потребует обновлений для перекрывания уязвимостей. Таким образом, вопрос информационной безопасности какой-либо системы — это практически всегда вопрос информированности. Непопулярность моделирования этих процессов обусловлена тем, что никто пока не изобрел универсального способа обнаружения уязвимостей, да и вряд ли такой способ когда-либо будет получен. В данной работе в связи с информированностью будет рассмотрен другой вопрос: каким образом за счет управления информацией, которую получает злоумышленник в процессе исследования информационной системы, можно сделать систему более безопасной? Очевидно, что перед попыткой реализации несанкционированного доступа злоумышленнику необходимо получить информацию об атакуемой системе. От того, насколько эта информация полна и достоверна, зависит успешность атаки. Также в системе иногда бывает полезно сделать системы логгирования или обнаружения атак невидимыми для потенциального злоумышленника. Возникает вопрос: как можно реализовать данный процесс, если потенциальным злоумышленником может быть легальный пользователь информационной системы, который неизбежно будет иметь доступ ко многим процессам?

Для решения этих вопросов необходимо определить способ формализации информированности субъектов в конфликте, а также обстоятельства, при которых они могут корректировать свой образ системы, приближая его к реальному.

[1] Работа поддержана грантом Президента Российской Федерации МК-1039.2013.9.

Моделирование структуры информированности в системах информационной безопасности

Существует много различных способов математического моделирования систем информационной безопасности. Наиболее популярные из них: дискреционные модели (например, модель Харрисона — Руззо — Ульмана) [1], модели мандатного управления доступом (Белла — Лападулы) [2], модели информационных потоков, ролевого управления доступом. Наиболее общей моделью можно считать модель дискреционного разграничения доступа Харрисона — Руззо — Ульмана (ХРУ). Хотя она и не всегда удобна для определения состояний безопасности реальных систем, почти все основные модели разграничения доступа можно выразить с ее помощью. Таким образом, определив структуры информированности для системы ХРУ, мы в дальнейшем можем определить аналогичные структуры для других моделей.

Кратко представить исходные данные для модели ХРУ можно следующим образом: в системе заданы множество субъектов (S), множество объектов (O), множество категорий доступов (R), матрица доступов субъектов к объектам M и множество команд (C).

$M[s, o] \in R$.

Все команды в системе строятся на ограниченном множестве примитивных операторов (всего их шесть).

Таким образом, у нас есть состояние системы $q = (S, O, M)$, которое в результате выполнения примитивного оператора α может перейти из состояния q в состояние q':

$q \underset{\alpha}{\mapsto} q'$.

Начальное состояние системы ХРУ q^0 является безопасным относительно некоторого права доступа $r \in R$, когда невозможен переход системы в состояние, в котором право доступа r появилось бы в ячейке матрицы доступов M, до этого r не содержавшей.

Это классическое определение системы ХРУ, данное в [1]. Для того чтобы определить структуру информированности субъектов системы, необходимо определить для каждого субъекта множество наблюдаемых им множеств S, O и M. То есть субъект может быть дезинформирован о других участниках системы, а также относительно доступов, которые имеют субъекты в системе, в том числе и своих собственных.

Таким образом, для каждого субъекта в S определим субъективное состояние системы:

$\forall s_i \in S \ \exists q_i = (S_i, O_i, M_i)$,

где S_i — множество субъектов, которые, по мнению i-го субъекта, присутствуют в системе, O_i — множество объектов в представлении i-го субъекта, M_i — матрица доступов, которые, по мнению i-го субъекта, присутствуют в системе. Субъективное состояние системы q_i определяет образ системы, который есть у i-го субъекта. Он может в той или иной степени соответствовать реальности. Как и раньше, оставляем состояние системы $q = (S, O, M)$ как объективное. То есть это состояние системы, соответствующее действительности. Подобную систему ХРУ назовем системой ХРУ с информированностью (ХРУИ).

Теперь, для того чтобы проанализировать систему на предмет безопасности, нам необходимо каким-то образом из этого множества состояний получить одно состояние $q^* = (S^*, O^*, M^*)$. Данное состояние системы назовем «приведенным». Особенность его в том, что оно однозначно определяет динамику (переходы) системы в рамках установленных команд и примитивных операторов.

Очевидно, что $S^* = S$, так как вне зависимости от представлений участников системы совершать переходы будут только реальные субъекты. Приведенное множество объектов можно определить следующим образом:

$O^* = O \cap (O_1 \cup ... \cup O_n)$.

То есть из объективного множества объектов мы выкидываем те, которые не содержатся в образах субъектов системы.

Приведенная матрица доступов задается по следующей схеме:

$$\begin{gathered} i = 1...n,\ j = 1...m, \\ \neg\exists M_i[s_i, o_j] \Rightarrow M^*[s_i, o_j] = \varnothing, \\ \exists M_i[s_i, o_j] \Rightarrow M^*[s_i, o_j] = M_i[s_i, o_j] \cap M[s_i, o_j]. \end{gathered} \quad (1)$$

То есть, определяя приведенную матрицу доступов, мы учитываем для каждого субъекта только его представления о своих собственных доступах, так как представления о доступах других участников системы не будут влиять на ее динамику.

В результате мы можем определить безопасное состояние системы с учетом структуры информированности субъектов.

Определение 1. Начальное состояние системы ХРУИ, заданное объективным состоянием q^0 и субъективными состояниями q_i^0, $i = 1...n$ (для системы из n субъектов), является безопасным относительно некоторого права доступа $r \in R$, когда невозможен переход системы из приведенного состояния q^* в состояние, в котором право доступа r появилось бы в ячейке матрицы доступов M^*, до этого r не содержавшей.

Устойчивость структуры информированности

Каждый из субъектов каким-то образом определяет свою исходную структуру информированности. Для нас неважен сам процесс получения этой структуры, так как процесс получения новых знаний мы не сможем смоделировать. Существенным для нас будет то, насколько эта структура устойчива. То есть в дальнейшем субъект может изменить свое видение системы, если получаемая информация расходится с его образами.

Здесь необходимо отметить различие понятия устойчивости структуры информированности, вводимого в данной статье, и термина, используемого в теоретико-игровом моделировании (например, [3]). В теоретико-игровом моделировании устойчивость структуры информированности определяется действием (или бездействием) других участников конфликта. В нашем случае каждый из субъектов самостоятельно анализирует собственный информационный образ путем воздействия на систему и получения обратной связи. То есть в теоретико-игровом моделировании структура информированности неустойчива, если субъект наблюдает действия других участников, не соответствующие его представлениям. В нашем понимании структура информированности неустойчива, если субъект при исследовании системы наблюдает обратную связь, не соответствующую его представлениям. Таким образом, структура информированности каждого конкретного субъекта устойчива, если в процессе взаимодействия с системой он не наблюдает обратную связь, противоречащую его образу системы.

Здесь для нас будут существенны два процесса: способ воздействия на объект и получение обратной информации от него, то есть контроль изменения его состояния. Для описания этих процессов необходимо ввести в системе информационные потоки между субъектами и объектами.

Определение 2. Если состояние объекта o_1 в момент времени t_n влияет на состояние другого объекта в момент времени t_{n+1}, то между данными объектами существует информационный поток по направлению от объекта o_1 к объекту o_2.

Соответственно, информационные потоки также можно разделить на субъективные и объективные. Объективный поток существует, если один объект реально влияет на другой, субъективный поток существует, если один объект влияет на другой в представлении i-го субъекта. Состояние некоторых объектов субъект может контролировать, то есть, он может наблюдать несоответствие субъективных и объективных информационных потоков. Это отвечает неустойчивой структуре информированности. Можно анализировать информационные потоки вне зависимости

от модели доступов в системе [4]. Однако для наглядности мы будем ориентироваться именно на нее с предположением, что никаких других информационных потоков, кроме получения доступов из множества R, в системе нет. Возьмем для примера множество $R = \{read, write, append, execute\}$. Тогда согласно определению информационного потока можно сопоставить данным категориям доступа соответствующие информационные потоки (рис. 1).

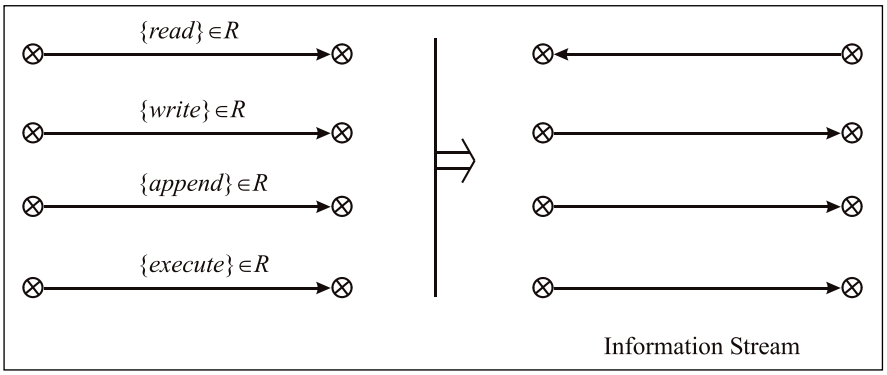

Рис. 1. Приведение доступов к информационным потокам

Посредством этого мы можем получить матрицу информационных потоков $I[s,o]$, которая формируется по следующему принципу:

$$\{write\} \in M[i,j] \text{ or } \{append\} \in M[i,j] \text{ or } \{execute\} \in M[i,j] \text{ or } \{read\} \in M[j,i] \Leftrightarrow$$
$$\Leftrightarrow I[i,j] = 1$$

В результате мы получаем матрицу смежности ориентированного графа. Данный граф представляет собой информационные потоки в системе. Обозначим его как Г.

Поскольку в нашей системе существуют объективная матрица доступа и множество субъективных, необходимо аналогичным образом разделить и графы. Будем далее рассматривать систему только с одним субъектом, без ограничения общности.

$\Gamma = (O \cup \{s\}, V)$,

где O — множество объектов в системе, s — субъект (исследователь), V — множество ребер графа (информационных потоков). Здесь мы выделили вершину $\{s\}$ — это субъект, с позиции которого мы смотрим на систему.

В системе задан объективный граф Г и субъективный граф Γ_s.

$\Gamma = (O \cup \{s\}, M)$ — объективный граф;

$\Gamma_s = (O_s \cup \{s\}, M_s)$ — субъективный граф.

Субъективный граф не всегда является устойчивой структурой. Субъект может обнаружить несоответствие отправляемых данных и получаемой обратной связи от системы. В некоторых случаях он может не получать вообще никакой обратной связи, а в некоторых ее не ждать. Процесс исследования не всегда приведет его к объективным данным [5].

Правило 1. Структуры без обратной связи всегда устойчивы.

Если в рамках субъективного графа субъект не имеет обратной связи по каким-либо объектам или не имеет способов воздействия на них, то такая структура всегда является устойчивой.

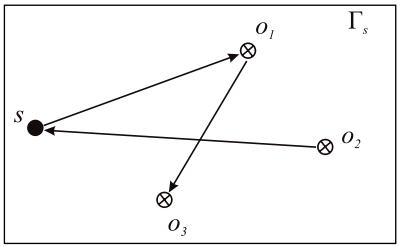

Рис. 2. Структура без обратной связи

Субъективный граф, показанный на рис. 2, является устойчивым, так как не имеет обратной связи ни по одному объекту. Субъект может воздействовать на объекты o_1 и o_3, но не может получать от них информации. Может получать информацию от объекта o_2, но не может на него воздействовать.

Обратная связь в графе есть, если есть сильная связность (путь в одну и другую стороны) субъекта и вершин в графе. Наблюдая несоответствие обратной связи, субъект может корректировать свой субъективный граф.

Определение 3. Назовем кольцом обратной связи Γ_s^k совокупность ребер $M_s^k \subseteq M_s$ сильносвязных вершин $O_s^k \subseteq O_s$ в графе Γ_s с субъектом s.

Правило 2. Если вычитание из субъективного кольца обратной связи Γ_s^k объективного кольца обратной связи Γ^k составляет непустое множество, то такая структура является неустойчивой.

Пример неустойчивой структуры в графе приведен на рис. 3.

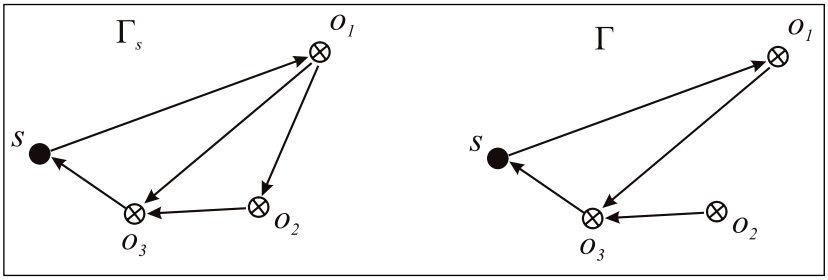

Рис. 3. Неустойчивый субъективный граф по правилу 2

Неустойчивые структуры разрушаются, образуя новый граф.

Определение 4. Преобразование графа информационных потоков с неустойчивой структурой к устойчивому графу называется приведением, а полученный граф — приведенным.

Правило 3. Неустойчивый граф Γ_s по правилу 2 приводится к устойчивому графу Γ_s^* по формуле:

$$\Gamma_s^* = \Gamma_s \setminus (\Gamma_s^k \setminus \Gamma^k) = \left(O_s \setminus (O_s^k \setminus O^k) \cup \{s\}, M_s \setminus (M_s^k \setminus M^k)\right) = \left(O_s^* \cup \{s\}, M_s^*\right). \quad (2)$$

Правило 4. Существует информационный поток к одному из объектов кольца обратной связи субъективного и объективного графов (Γ_s^k является устойчивым), который присутствует в объективном графе, но отсутствует в субъективном, то есть $\exists (o_1, o_2) \in M, (o_1, o_2) \notin M_s, o_2 \in O_s^k, o_2 \in O^k$. Такой граф является неустойчивым.

Пример неустойчивого графа по правилу 4 показан на рис. 4.

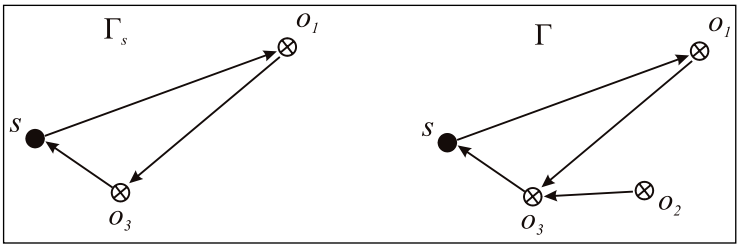

Рис. 4. Неустойчивый граф по правилу 4

Правило 5. Для неустойчивого графа по правилу 4 приведенный граф Γ_s^* строится по следующему принципу:

$$\Gamma_{add} = \left\{(o_i, o_j) \mid (o_i, o_j) \in M, (o_i, o_j) \notin M_s, o_j \in O_s^k, o_j \in O^k\right\}$$
$$\Gamma_s^* = \Gamma_s \cup \Gamma_{add} \quad (3)$$

Теорема 1. Последовательным применением преобразований (2) и (3) к любому субъективному графу информационных потоков мы получаем приведенный (устойчивый) граф.

Теорема 2. Граф, не содержащий сильносвязных вершин с вершиной $\{s\}$, всегда устойчив.

Оценка объективности системы

В реальных конфликтах мы можем анализировать только субъективные информационные потоки, так как сами являемся участниками системы, находимся внутри нее. Отсюда для исследователя достаточно важно решить задачу оценки того, насколько его субъективный граф соответствует объективному.

В общем случае эта задача не имеет решений, однако при введении определенных ограничений может быть решена.

Теорема 3. Если все объекты (вершины графа) в системе являются общим правилом и Γ_s^k приведенного графа субъекта Γ_s^* содержит все вершины, то $\Gamma_s^* = \Gamma$.

Динамика системы

Выше мы рассмотрели только статичное состояние автомата ХРУИ, которое исследуется субъектом. Однако со временем состояние системы может меняться. Автомат ХРУИ переходит из состояния в состояние в результате выполнения примитивного оператора $q \underset{\alpha}{\mapsto} q'$, что является одним шагом работы системы. Без ограничения общности будем рассматривать здесь динамику системы на одном шаге.

Проведенный анализ устойчивости структур по последним двум разделам был сделан по ориентированным графам субъективных структур I_s. Для того чтобы сформировать на их основе устойчивые матрицы доступов $\hat{M}_k$, необходимо сделать следующие преобразования:

$$\{write\} \in \hat{M}_k[i,j] \Leftrightarrow \{write\} \in M_k[i,j] \text{ and } I[i,j] = 1,$$

$$\{read\} \in \hat{M}_k[i,j] \Leftrightarrow \{read\} \in M_k[i,j] \text{ and } I[j,i] = 1,$$

$$\{append\} \in \hat{M}_k[i,j] \Leftrightarrow \{append\} \in M_k[i,j] \text{ and } I[i,j] = 1,$$

$$\{execute\} \in \hat{M}_k[i,j] \Leftrightarrow \{execute\} \in M_k[i,j] \text{ and } I[i,j] = 1$$

Для получения приведенного состояния системы $q^* = (S^*, O^*, M^*)$ необходимо в формуле (1) использовать только устойчивые матрицы доступа. Тогда формула (1) будет выглядеть следующим образом:

$$i = 1...n, j = 1...m,$$

$$\neg\exists\hat{M}_i[s_i, o_j] \Rightarrow M^*[s_i, o_j] = \varnothing,$$

$$\exists\hat{M}_i[s_i, o_j] \Rightarrow M^*[s_i, o_j] = \hat{M}_i[s_i, o_j] \cap \hat{M}[s_i, o_j].$$

В результате путем корректировки структур информированности субъектов системы мы можем, в соответствии с определением 1, *перевести систему из небезопасного состояния в безопасное*.

Дальнейшая динамика системы также может быть подвержена анализу информационных структур. При переходе системы $q \underset{\alpha}{\mapsto} q'$ меняется объективное состояние системы, но при этом субъективные состояния системы могут не измениться.

Правило 6. Субъективные состояния системы $q_i = (S_i, O_i, M_i)$ при выполнении оператора α меняются тогда и только тогда, когда граф информационных потоков I_i становится неустойчивым.

Очевидно, что и приведенное состояние системы не всегда будет меняться под действием команд перехода системы. Если мы определим множество всех возможных матриц доступа в системе как 2^M, то на данном множестве мы можем задать подмножества невидимых

преобразований $M_i^{inv} \subseteq 2^M$ для каждого из субъектов. Переходы системы в эти состояния не меняют субъективные матрицы доступов субъектов. Данные переходы становятся в системе «невидимыми».

По аналогии с системой Харрисона — Руззо — Ульмана, мы можем рассматривать и другие модели, такие как Белла — Лападулы [2], ролевого управления доступом [6] и пр.

Выводы

Анализ структур информированности в системах информационной безопасности позволяет ответить на множество важных вопросов, таких, например, как:

- в каких случаях администратор безопасности может утверждать, что его собственная структура информированности является истинной, то есть его образ системы адекватен;
- каким образом можно дезинформировать потенциальных злоумышленников о структуре информационной системы, чтобы сформировать у них устойчивый субъективный образ, то есть ситуацию, когда субъект, взаимодействуя с системой, не наблюдает диссонанса со своим субъективным образом.
- определение структуры информационных потоков в системе, при которых процедуры администрирования безопасности становятся невидимыми для нежелательных субъектов.

Все это позволяет дополнительно снижать риски от потенциальных угроз несанкционированного доступа в информационных системах, а также объективно их оценивать (в случае получения истинной структуры информированности).

СПИСОК ЛИТЕРАТУРЫ:

1. *Harrison M., Ruzzo W., Ullman J.* Protection in operating system // Communication of ACM. 1976. № 19 (8). P. 461–471.
2. *Bell D. E., LaPadula L. J.* Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford. Mass.: MITRE Corp., 1976.
3. *Чхартишвили А. Г.* Рефлексивные игры: трансформация структур информированности // Проблемы управления. 2008. № 5. С. 43–48.
4. *Al-Fedaghi S., Al-Saqabi K., Thalheim B.* Information Stream Based Model for Organizing Security // Availability, Reliability and Security. 2008. ARES 08. Third International Conference.
5. *Styugin M.* Protection against System Research // Cybernetics and System. 2014. Vol. 45. Issue 04. P. 362–372.
6. *Sandhu R.* Role-Based Access Control, Advanced in Computers // Academic Press. 1998. Vol. 46.

REFERENCES:

1. *Harrison M., Ruzzo W., Ullman J.* Protection in operating system // Communication of ACM. 1976. № 19 (8). P. 461–471.
2. *Bell D. E., LaPadula L. J.* Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford. Mass.: MITRE Corp., 1976.
3. *Chkhartishvili A. G.* Reflexivnie igri: transformatsiia structur informirovannosti // Problemi upravlenia. 2008. № 5. P. 43–48.
4. *Al-Fedaghi S., Al-Saqabi K., Thalheim B.* Information Stream Based Model for Organizing Security // Availability, Reliability and Security. 2008. ARES 08. Third International Conference.
5. *Styugin M.* Protection against System Research // Cybernetics and System. 2014. Vol. 45. Issue 04. P. 362–372.
6. *Sandhu R.* Role-Based Access Control, Advanced in Computers // Academic Press. 1998. Vol. 46.