Взаимосвязь автоматных моделей безопасных информационных систем без скрытых каналов передачи данных

В. Г. Гукасян (МГУ имени М. В. Ломоносова, Москва)

Построены отображения между автоматными моделями информационных систем, описанными в работах Московитца — Костича и Грушо — Шумицкой, сохраняющие свойства безопасности.

Ключевые слова: автоматные модели, скрытые каналы, модель невлияния, вероятностное невлияние.

1. Введение

Большинство современных систем является многопользовательскими, причем пользователи различаются по глубине прав доступа и возможности выполнения некоторых действий. Поэтому остро стоит вопрос изучения разграничения этого доступа и поиска возможных каналов передачи информации между пользователями с различными правами доступа. Понятие невидимости данных высокого уровня для пользователей низкого уровня тесно связано с понятием невлияния. В широком смысле невлияние означает невозможность для одного пользователя своими действиями влиять на работу другого пользователя. В противном случае, если один пользователь может воздействовать на другого, появляется вероятность компрометации секретных данных по такому каналу передачи данных между различными уровнями доступа.

В работе [?] исследуется невлияние и возможность передачи данных между уровнями в терминах информационных потоков. В работе [?] вводится автоматная модель и дается определение безопасной системы в автоматных терминах. Далее в работе [?] автоматная модель изменяется, добавляется вероятностное распределение, вводится определение невидимости по вероятности и формулируется достаточное условие для его существования.

В данной работе исследуется взаимосвязь моделей, введенных в работах [?] и [?].

2. Модели компьютерных систем

В данном разделе будут более подробно описаны модели, построенные в работах [?] и [?].

2.1. Модель А (Грушо — Шумицкая)

Компьютерная система моделируется абстрактным автоматом A, $A = A(X, S, Y, \delta, \lambda)$, где X, S, Y — конечные непустые множества, представляющие собой, соответственно, входной алфавит, множество состояний и выходной алфавит, $\delta : S \times X \to S$ — функция переходов, $\lambda : S \times X \to Y$ — функция выходов.

Рассматривается следующая автоматная модель двухуровневой компьютерной системы.

Пусть $X = X_H \times X_L, X_H \bigcap X_L = \varnothing$, где X_H и X_L — множества входов для пользователей уровней H (High) и L (Low), соответственно. Далее везде будем предполагать, что имеется только один пользователь каждого уровня, и назвать их H и L. Аналогично, пусть $S = S_H \times S_L$, $Y = Y_H \times Y_L$. Будем обозначать Low-компоненты элементов индексом L: x_L, s_L, y_L. Аналогично обозначим и High координаты. Также введем обозначения координатных функций δ_H и $\delta_L(s, x)$: $\delta(s, x) = (\delta_H(s, x), \delta_L(s, x))$ и аналогично λ_H и λ_L. Множества X_H, X_L, Y_H, Y_L могут содержать среди своих элементов пустые слово e_H и e_L. При этом будем считать, что $\delta(s, (e_H, e_L)) = s$ и $\lambda(s, (e_H, e_L)) = (e_H, e_L)$. Если из контекста ясно, какому множеству принадлежит пустое слово, будем опускать нижний индекс.

Определение 1. Пусть $s^1, s^2 \in S$. Определим отношение эквивалентности $\sim$, полагая $s^1 \sim s^2$, если $s^1_L = s^2_L$. Обозначим $S/_\sim$ фактормножество относительно отношения $\sim$; класс эквивалентности, содержащий s, $s \in S$, будем обозначать $[s]$.

Аналогично определим отношение эквивалентности на множестве Y.

Определение 2. Будем говорить, что L не видит H, если функция $\tilde{\delta}$: $S/_\sim \times X_L \to S/_\sim$, определяемая формулой

$$\tilde{\delta}([s], x_L) = [\delta(s', (x_H, x_L))],\ x_H \in X_H,\ s' \in [s],$$

и функция $\tilde{\lambda}\colon S/_\sim \times X_L \to Y/_\sim$, определяемая формулой

$$\tilde{\lambda}([s], x_L) = [\lambda(s', (x_H, x_L))],\ x_H \in X_H,\ s' \in [s],$$

корректно определены.

Система, удовлетворяющая определению 2, считается безопасной.

2.2. Модель B (Московитц — Костич)

Опишем модель, построенную в работе [?], на которую ссылаются авторы работы [?].

Система описывается автоматом без выхода $B = (S, \Sigma, \delta)$, где

1) S — конечное непустое множество состояний. Каждое состояние задается как вектор значений и S — совокупность возможных векторов.
2) Σ — входной алфавит.
3) $\delta : S \times \Sigma \to S$ — функция переходов.
   Для пустого входа e полагаем $\delta(s, e) = s$.

Входной алфавит состоит из всевозможных команд, которые может ввести каждый пользователь. Координаты состояния интерпретируются как доступная пользователям информация о системе. Пользователям доступны различные/неполные данные о системе в зависимости от прав доступа. Пусть имеется два пользователя: пользователь с низкими правами (Low) видит только ограниченную часть координат вектора состояний, пользователь с высокими правами (High) видит весь вектор.

Определение 3. Автомат называется двухуровневым, если входной алфавит Σ представляется как объединение двух непересекающихся множеств: $\Sigma = \Sigma_H \sqcup \Sigma_L$, а множество состояний — как $S = S_H \times S_L$.

Определение 4. Состояния $s^1, s^2 \in S$ называются эквивалентными, пишем $s^1 \sim s^2$, если их Low-компоненты равны.

Таким образом, S разбивается на классы эквивалентности. Класс эквивалентности, содержащий s, $s \in S$, будем обозначать $[s]$. Обозначим отображение, разбивающее S на классы эквивалентности, $\pi : S \to S/_\sim$.

Также вводится функция $Z_L\colon \Sigma^* \to \Sigma_L^*$, которая из последовательности входов оставляет только команды пользователя Low.

Определение 5. Система, задаваемая автоматом $B = (S, \Sigma, \delta)$, называется безопасной, если:

1) Отображение $\tilde{\delta} : S/_\sim \times \Sigma_L^* \to S/_\sim$, определяемое формулой $\tilde{\delta}([s], w_L) = [\delta(s, w_L)]$, где $[s] \in S/_\sim$ и $w_L \in \Sigma_L^*$, корректно определено.
2) $\pi \circ \delta = \tilde{\delta} \circ (\pi \times Z_L)$.
   В левой и правой части равенств стоят отображения $S \times \Sigma^* \to S/_\sim$. Иными словами, диаграмма ниже коммутативна:

$$\begin{array}{ccc} S \times \Sigma^* & \xrightarrow{\delta} & S \\ {\scriptstyle \pi \times Z_L}\downarrow & & \downarrow{\scriptstyle \pi} \\ S/_\sim \times \Sigma_L^* & \xrightarrow[\tilde{\delta}]{} & S/_\sim \end{array}$$

2.3. Взаимосвязь моделей

Обозначим через $\mathbb{A}$ и $\mathbb{B}$ множества автоматов, описанных в терминах моделей A и B, соответственно. Сами автоматы будем также обозначать A и B.

Будем далее обозначать входы модели B как x'_L и x'_H, опуская явное указание действующего пользователя, где это не вызывает путаницы.

2.3.1. Отображение из модели B в модель A

Построим отображение $F : \mathbb{B} \to \mathbb{A}$. Каждому автомату $B(S', \Sigma', \delta') \in \mathbb{B}$ сопоставим автомат $A(X, S, Y, \delta, \lambda) \in \mathbb{A}$ по следующим правилам:

1) входами автомата A будет прямое произведение возможных команд пользователей Low и High,
2) выход равен состоянию, в который переходит автомат после действий пользователей,
3) новое состояние после входа (x_H, x_L) эквивалентно состоянию автомата B после последовательного ведения команд x_L и x_H.

Замечание 1. Заметим, что сопоставленный таким образом автомат A удовлетворяет следующим равенствам:

$\forall s \in S, x \in X$:

$$\begin{array}{l} \delta(s, (x_H, x_L)) = \delta(\delta(s, (e, x_L)), (x_H, e)) = \delta(s, (e, x_L)(x_H, e)), \\ \lambda(s, (x_H, x_L)) = \lambda(\delta(s, (e, x_L)), (x_H, e)) = \lambda(s, (e, x_L)(x_H, e)). \end{array} \quad (1)$$

Обозначим множество автоматов, удовлетворяющих условию (**??**), за $\overline{\mathbb{A}}$.

Утверждение 1. $\overline{\mathbb{A}} \neq \mathbb{A}$.

Теорема 1. *F — инъективный гомоморфизм из множества $\mathbb{B}$ в $\overline{\mathbb{A}}$, сохраняющий свойство безопасности/небезопасности, а также функционирование автомата, как отображения из множества состояний и входных слов в множества состояний:*

$$\begin{array}{ccc} S' \times \Sigma^* & \xrightarrow{\delta'} & S' \\ {\scriptstyle F_S \times F_X}\downarrow & & \downarrow{\scriptstyle F_S} \\ S \times X^* & \xrightarrow[\delta]{} & S \end{array}$$

2.3.2. Отображение из модели A в модель B

Теперь построим отображение $G' : \mathbb{A} \to \mathbb{B}$. Отображение G' будем получать как композицию двух других отображений:

$$G' = G \circ \overline{G}, \text{ где}$$

- $\overline{G} : \mathbb{A} \to \overline{\mathbb{A}}$
  Отображение $\overline{G}$ сопоставляет каждому автомату $A \in \mathbb{A}$ автомат $\overline{A} \in \overline{\mathbb{A}}$, совпадающий с автоматом A на входах вида (x_H, e) и (x_L, e). Рассмотрим разбиение множества $\mathbb{A}$ на классы эквивалентности (класс эквивалентности автомата A будем обозначать [A]):

$$[A] = \{T \in \mathbb{A} \mid \forall x_H \in X_H, x_L \in X_L, s \in S\colon$$

$$\begin{aligned} \delta_A(s,(e,x_L)) &= \delta_T(s,(e,x_L)), \\ \lambda_A(s,(e,x_L)) &= \lambda_T(s,(e,x_L)), \\ \delta_A(s,(x_H,e)) &= \delta_T(s,(x_H,e)), \\ \lambda_A(s,(x_H,e)) &= \lambda_T(s,(x_H,e))\}. \end{aligned}$$

Замечание 2. Заметим, что по определению множества $\overline{\mathbb{A}}$ для любого автомата $A \in \mathbb{A}$ существует ровно один автомат $\overline{A} \in \overline{\mathbb{A}}$, лежащий в $\overline{A} \in [A]$. Обозначим такой автомат через $\overline{A}_{[A]}$.
Тогда

$$\overline{G}(A) = \overline{A}_{[A]}.$$

- $G : \overline{\mathbb{A}} \to B$
  Отображение G будет строиться ниже.

Каждому $A(X, S, Y, \delta, \lambda) \in \overline{\mathbb{A}}$ сопоставим автомат $B(S', \Sigma', \delta') \in \mathbb{B}$ по следующим правилам:

- входы автомата B — объединение команд пользователей High и Low,
- множество состояний — прямое произведение множеств состояний и выходов автомата A,
- переход по входу x'_L эквивалентен переходу в автомате A по входу (e, x'_L).

Замечание 3. Функция δ' не зависит от Y:

$$\forall y_1, y_2 \in Y, s \in S, x' \in \Sigma' : \delta'((s, y_1), x') = \delta'((s, y_2), x').$$

Теорема 2. *Построенное отображение G — инъективный гомоморфизм из $\overline{\mathbb{A}}$ в $\mathbb{B}$, сохраняющий свойство безопасности/небезопасности, а также конфигурации автоматов:*

$$\begin{array}{ccc} S \times X^* & \xrightarrow{\delta \times \lambda} & S \times Y \\ {\scriptstyle G_S \times G_{\Sigma'}}\downarrow & & \downarrow{\scriptstyle G_{SY}} \\ S' \times \Sigma^* & \xrightarrow[\delta']{} & S' \end{array}$$

2.3.3. Степень соответствия между моделями A и B

Покажем, что отображения F и G в некотором смысле обратны друг другу.

Определение 6. Определим отображение d, удваивающее состояния автомата $B \in \mathbb{B}$:

$$d((S', \Sigma', \delta')) = ((S', S'), \Sigma', (\delta', \delta')).$$

Отображение d переводит автомат $B \in \mathbb{B}$ в точно такой же, но у которого вместо состояния s' теперь состояние вида (s', s'), входной алфавит и переходы остаются теми же.

Замечание 4. Очевидно, что для любого $B \in \mathbb{B}$, автоматы B и $d(B)$ изоморфны.

Утверждение 2. $G \circ F(B) = d(B)$, $B \in \mathbb{B}$.

2.3.4. Отображение из модели A в модель B, сохраняющее свойство безопасности

Построенное выше отображение G в некотором смысле обратно отображению F и при этом конфигурации автомата $A \in \mathbb{A}$ при функционировании будут повторяться автоматом $G(A)$ (по модулю отображения G). Но важным ограничением отображения G является то, что оно определено не на всем множестве $\mathbb{A}$, а только на $\overline{\mathbb{A}}$. В данном разделе мы построим отображение M любого автомата $A \in \mathbb{A}$ в $\mathbb{B}$, сохраняющее свойство безопасности.

Для любого автомата $A(X, S, Y, \delta, \lambda) \in \mathbb{A}$ отображением M сопоставим автомат $B(S', \Sigma', \delta') \in \mathbb{B}$ по следующим правилам:

- входы — объединение команд пользователей High и Low,
- множество состояний — прямое произведение множеств S, Y и X автомата A,
- переход по входу x'_L эквивалентен переходу в автомате A по входу (x^s_H, x'_L), где x^s_H — компонента состояния, соответствующая X_H.

Теорема 3. *M является инъективным отображением, сохраняющем свойство безопасности/небезопасности.*

Список литературы

[1] Goguen J. A., Meseguer J. Security policies and security models // Proceedings of the IEEE Symposium on Security and Privacy. — 1982. — P. 11–20.

[2] Moskowitz I. S., Costich O. L. A classical automata approach to noninterference type problems // Proc. Computer Security Foundations Workshop V, IEEE Press. — 1992. — P. 2–8.

[3] Грушо А. А., Шумицкая Е. Л. Модель невлияния и скрытые каналы // Дискретная математика. — 2002. — Т. 14. Вып. 1. — С. 11–16.