ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 24 МАТЕМАТИКИ Выпуск 5
2017

О. В. Баева, В. В. Мкртичян (Ростов-на-Дону, ЮФУ ИММиКН).
Алгоритм поиска подмножества коалиции динамической схемы цифровых отпечатков пальцев в программном обеспечении.

Пусть $\mathbb{X}$ — множество программ; $\mathbb{U} = \{u_1; \ldots; u_n\}$ — множество пользователей $x(\in \mathbb{X})$, $n = |\mathbb{U}|$; $d(\in \mathbb{N})$; $l = d(n-1)$. Рассмотрим такие множества $P = \{p_1; \ldots; p_l\} \subset \mathbb{N}$ и $Q = \{q_1; \ldots; q_l\} \subset \mathbb{N}$, что $P \bigcap Q = \varnothing$, и матрицу $\Gamma(n, d)$, каждый элемент $w_{i,j}$ которой равен q_j, если $j < (i-1)d + 1$, и p_j в противном случае. Строки $\Gamma(n, d)$ обозначим $\{w^{(1)}, \ldots, w^{(n)}\}$.

Пример. Пусть $n = 3, d = 3$. Тогда $l = 9$, и $\Gamma(4, 3)$ имеет вид:

$$w^{(1)} = (\ p_1,\ p_2,\ p_3,\ \ p_4,\ p_5,\ p_6),$$

$$w^{(2)} = (\ q_1,\ q_2,\ q_3,\ \ p_4,\ p_5,\ p_6),$$

$$w^{(3)} = (\ q_1,\ q_2,\ q_3,\ \ q_4,\ q_5,\ q_6).$$

Пусть π — непустая перестановка l элементов, известная распространителю программы, но неизвестная пользователям, и $\mathbb{W} = \{\pi w^{(1)}; \ldots; \pi w^{(l)}\} \subset \mathbb{N}^l$ — множество цифровых отпечатков пальцев (ЦОП).

Пусть $\mathbb{I}$ — множество вводов в $x \in \mathbb{X}$, а $f_x : \mathbb{N} \times \mathbb{I} \to \mathbb{X}$ и $g : \mathbb{X} \times \mathbb{I} \to \mathbb{N}$ действуют по СТ-алгоритмам внедрения и извлечения элемента ЦОП соответственно [1]. $\mathbb{K} = \mathbb{I}^l$ — множество ключей, $k = (k_1; \ldots; k_l) \in \mathbb{K}$.

Пусть $M : \mathbb{U} \to \mathbb{W}$ — биективное отображение, $R : \mathbb{N}^l \to \mathbb{U} \cup \{?\}$ — сюръективное отображение. Если вектор $v \in \mathbb{N}^l \pi w^{(j)} \in \mathbb{W}, j \in \{1, 2, \ldots, n\}$, то $R(v) = u_j$, иначе $R(v) = '?'$.

Рассмотрим схему ЦОП следующего вида: $\xi = (\mathbb{X}, \mathbb{U},\ \mathbb{W},\ \mathbb{K},\ E,\ D,\ M,\ R)$, где $E : \mathbb{X} \times \mathbb{U} \times \mathbb{K} \to \mathbb{X}$ и $D : \mathbb{X} \times \mathbb{K} \to \mathbb{N}^l$ действуют соответственно по алгоритмам, определенным следующим образом: $E(x, u, k) = x'$ — программа с внедренным $w = M(u)$, каждый элемент которого встроен по алгоритму f_x при помощи элементов ключа k; $\pi^{-1}(D(x'', k)) = w'$ — извлеченный ЦОП из программы x'', являющейся пиратской копией программы x.

В [2] представлен алгоритм поиска непустого подмножества множества коалиции, создавшей пиратскую копию программы. Построим аналогичный алгоритм для динамической схемы ЦОП, описанной выше.

Функция веса $t(w)$ равна количеству совпадений $w_j = p_j$ для всех $j \in \{1, 2, \ldots, l\}$. Пусть $\Sigma = P \cup Q$ и $w = (w_1, \ldots, w_l) \in \mathbb{N}^l$. Пусть

$$w|_{B_m} = \{w_{d(m-1)+1}; \ldots; w_{d(m-1)+d}\}, \quad \text{где} \quad m \in \{1, 2, \ldots, n-1\}.$$

Для $2 \leqslant s \leqslant n-1$ определим $w|_{R_s} = w|_{B_{s-1}} \cup w|_{B_s}$.

Алгоритм.
Вход: $w \in \Sigma^l$ — пиратский ЦОП.
Выход: $C_0 \subset \mathbb{U}$.

1. $C_0 := \varnothing$, s:=2.
2. Если $t(w|_{B_1}) > 0$, добавить u_1 в C_0.

3. Если $t(w|_{B_{n-1}}) < d$, добавить u_n в C_0.
4. $k := t(w|_{R_s})$. Добавить u_s в C_0, если

$$t(w|_{B_{s-1}}) < \frac{k}{2} - \sqrt{\frac{k}{2}\log\frac{2n}{\varepsilon}},$$

5. $s := s + 1$; если $s < n$, вернуться на шаг 4.

Теорема. *Пусть* $n \geqslant 3$, $\varepsilon > 0$ *и* $d = 2n^2\log(2n/\varepsilon)$, $C (C \subset \mathbb{U})$ *— коалиция из не более чем* c *пользователей, создавшая* $w \in \Sigma^l$), *и* $A : \Sigma^l \to \mathbb{U}$ *действует по алгоритму. Тогда схема* ξ *является* c*-защищенной с ошибкой* ε, *т. е.* $\mathbf{P}\{A(w) \in C\} = 1 - \varepsilon$.

СПИСОК ЛИТЕРАТУРЫ

1. *Collberg C. S.*, *Thomborson C.*, *Townsend G. M.* Dynamic graph-based software fingerprinting. — ACM Transactions on Programming Languages and Systems (TOPLAS), 2007, v. 29, N. 6, p. 35:1–35:67.
2. *Boneh D.*, *Shaw J.* Collusion-secure fingerprinting for digital data. — IEEE Trans. Inform. Theory, 1998, v. IT-44, is. 5, p. 1897–1905.