УДК 004.056.55:004.056.53

Соловей В. А., молодший наук. співробітник
Житомирський військовий інститут ім. С. П. Корольова

ЛОГІЧНА АВТЕНТИФІКАЦІЯ БЕЗ ПАРОЛІВ

У цій роботі розглядається механізм логічної автентифікації без використання паролів (LPA) у рамках формальної моделі координатної криптографії (КК). Класичні системи автентифікації базуються на секретних ключах, цифрових підписах, паролях [1], ідентифікованих цифрових відбитках тощо. Запропонований підхід верифікує шифрокод за його структурою відносно очікуваної на цей подієвий момент. Зміст відкритого тексту, що пов'язаний із отриманим шифрокодом (c_t), не має значення для функціонування цього механізму. LPA має логічну природу походження, що пов'язана із опосередкованим механізмом встановлення факту симетрії системи отримувача відносно стану системи автора шифрокоду. Операційний стан визначається як $\mathcal{E}_t = (GIS_t, LTT_t)$, де GIS_t – внутрішній координатний простір, що складається з множини динамічних об'єктів g_i із унікальними параметризованими координатами, а LTT_t – логічний тунель часу, який задає правила асоціації, допустимі операції кодування та функціональний контекст у фазі t. Шифрокод формується параметризованими координатами g_i, які визначаються бієктивними правилами асоціації φ_t^i, для кожного слова, між семантикою слова та одним g_i. Нехай $\mathcal{M}$ - семантика слова відкритого тексту w_n, де $n \in N_t$, ініціює процес формування c_t. Кількість подій у фазі t дорівнює кількості слів N_t. Зазначимо: $\forall w_i, w_j \in N_t, i \neq j$:

$$GIS_t^{(w_i, g_i)} \neq GIS_t^{(w_j, g_j)} \ \wedge \ LTT_t^{\left(\varphi_t^i, \mathcal{M}(w_i)\right)} \neq LTT_t^{\left(\varphi_t^j, \mathcal{M}(w_j)\right)},$$

тобто конфігурації є унікальними для різних слів і відповідних їм семантик.

GIS_t формується з об'єднання активної $\mathcal{A}_t$ та пасивної $\mathcal{P}_t$ множин об'єктів: $\mathcal{A}_t \cap \mathcal{P}_t = \emptyset,\ GIS_t = \mathcal{A}_t \cup \mathcal{P}_t$, при цьому обов'язково: $|\mathcal{A}_t| \ll |\mathcal{P}_t|$. Кожен об'єкт $g_i \in \mathcal{A}_t \cup \mathcal{P}_t$ має унікальні координатні параметри.

Нехай $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – підмножина об'єктів координатного простору, індукована c_t, яка відповідає вибору тільки активних об'єктів $a_i \in \mathcal{A}_t, G_t^{(c_t)} \subset \mathcal{A}_t$. Тоді шифрокод c_t приймається тоді і тільки тоді, коли виконується предикат верифікації: $V_{\mathcal{E}_t}(c_t) \in \{0,1\},\ \ V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t$, де $V_{\mathcal{E}_t}$ – функція верифікації, а значення 1 відповідає прийняттю. Нехай W^1 – множина можливих значень першого слова тексту довжини m біт, причому $|\mathcal{A}_t^1| = |W^1| = 2^m$, де $\mathcal{A}_t^1 \subset \mathcal{A}_t$. Правило асоціації: $\varphi_t^1 : W^1 \to \mathcal{A}_t^1$ кожному $\mathcal{M}(w_1) \in W^1$ ставить у відповідність єдиний об'єкт $a_i \in \mathcal{A}_t^1$. Тоді для слова W^2 визначається відображення $\varphi_t^2 : W^2 \to \mathcal{A}_t^2$. Кількість елементів a_i^1 у множині $\mathcal{A}_t^1$ дорівнює 2^m. Після першої події усі об'єкти множини $\mathcal{A}_t^1$ втрачають поточне правило асоціації φ_t^1, змінюють свої координатні параметри стохастичним чином та отримують нове правило асоціації, яке буде

використовуватись у наступній фазі φ_{t+1}^{i}. Тому виконується: $a_i \in \mathcal{A}_t^i \Rightarrow a_i \notin \mathcal{A}_t^j \Rightarrow a_i \notin \mathcal{A}_{t+n}^j$, $i \neq j$. За умови сталості параметра m виконується: $|\mathcal{A}_t^1| = |\mathcal{A}_t^2| = \cdots = |\mathcal{A}_t^i| = 2^m$, для всіх фаз та подій системи. Успішна верифікація шифрокоду забезпечує збереження симетрії у подальшій фазовій еволюції систем:

$$V_{\mathcal{E}_t}(c_t) = 1 \Rightarrow \left(G_t^{(c_t)} \subset \mathcal{A}_t\right) \Rightarrow \mathcal{E}_{t+1}^{Alice} = \mathcal{E}_{t+1}^{Bob}, \quad \forall t \in N.$$

Ймовірність P_{err} того, що модифікований шифрокод успішно пройде верифікацію визначається $p_t = \frac{|\mathcal{A}_t|}{|GIS_t|} \Rightarrow P_{err} = \left(\frac{|\mathcal{A}_t|}{|GIS_t|}\right)^k$, де k – кількість слів у координатних подіях реконструкції $G_t(c_t) = \{g_1, g_2, \dots, g_k\}$. Якщо кожне слово додає нову координатну подію перевірки, то ймовірність помилкової автентифікації зменшується експоненційно. Інформаційна характеристика LPA – ентропія автентифікації $H_{LA} = -\log P_{err}$, тому: $H_{LA} = k \log\left(\frac{|GIS_t|}{|\mathcal{A}_t|}\right)$. Це означає, що ентропія LPA лінійно зростає зі збільшенням кількості координатних подій перевірки.

Після кожної операції кодування конфігурація змінюється:

$$GIS_{t+1} = \Psi(GIS_t, LTT_t, c_t) \Rightarrow LTT_{t+1} = \Omega(GIS_{t+1}, LTT_t, c_t),$$
$$\mathcal{E}_{t+1} = (GIS_{t+1}, LTT_{t+1}), \mathcal{E}_i \neq \mathcal{E}_j \Rightarrow c_i \neq c_j.$$

Таким чином ЛБА виконує роль подієвого механізму синхронізації фазової еволюції $\mathcal{E}_t$, без використання секретних ключів або паролів.

Якщо задано допустиму ймовірність помилкової автентифікації δ, то: $P_{err} = \delta$, $\left(\frac{|\mathcal{A}_t|}{|GIS_t|}\right)^k = \delta$, $\frac{|\mathcal{A}_t|}{|GIS_t|} = \delta^{1/k}$, розмір простору: $|GIS_t| = \frac{|\mathcal{A}_t|}{\delta^{1/k}}$.

Розмір $|GIS_t|$ повинен бути таким, щоб забезпечити задану стійкість.

Якщо шифрокод має k слів та m бітові слова, то $|\mathcal{A}_t| = k\,2^m$, тоді: $|GIS_t| = \frac{k\,2^m}{\delta^{1/k}}$. Але при заданому $|GIS_t|$ маємо: $\left(\frac{|\mathcal{A}_t|}{|GIS_t|}\right)^k \to 0 \quad (k \to \infty)$.

Якщо треба розрахувати k при заданій структурі GIS_t та заданому δ, тоді: $k \geq \frac{\log \delta}{\log\left(\frac{|\mathcal{A}_t|}{|GIS_t|}\right)}$ – формула мінімальної довжини шифрокоду.

ЛБА має логічну природу $V_{\mathcal{E}_t}(c_t) = f(GIS_t, LTT_t, c_t)$ залежить виключно від криптографічного стану $\mathcal{E}_t$ та не спирається на семантику відкритого тексту $\mathcal{M}$: $V_{\mathcal{E}_t}(c_t) \not\equiv f(\mathcal{M})$, $c_t \to G_t(c_t) \to V_{\mathcal{E}_t}(c_t) \to \mathcal{E}_{t+1}$.

ЛБА має історично-залежний характер, тому еволюція $\mathcal{E}_t$ має немарковську властивість. Нехай Ф оператор формування LTT, тоді:

$$LTT_t = \Phi(c_{t-1}, c_{t-2}, \dots) \to V_{\mathcal{E}_t}(c_t) = f(GIS_t, \Phi(c_{t-1}, c_{t-2}, \dots), c_t),$$
$$\Rightarrow V_{\mathcal{E}_t}(c_t) \Rightarrow \mathcal{E}_{t+1}.$$ Висновок: ЛБА є подієвою системою з пам'яттю.

Список використаних джерел

1. Bellare M., Pointcheval D., Rogaway P. Authenticated key exchange secure against dictionary attacks // EUROCRYPT. – 2000.

2. Shannon C. A mathematical theory of communication // Bell System Technical Journal. – 1948. – Vol. 27. – P. 379–423.