УДК 004.056.55:004.056.53

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

ОФЛАЙН КОНФІДЕНЦІЙНА КОМУНІКАЦІЯ БЕЗ АДРЕСАЦІЇ У КООРДИНАТНІЙ КРИПТОГРАФІЇ

У запропонованій моделі криптографічний процес інтерпретується як навігація у внутрішньому координатному просторі системи, який динамічно еволюціонує у процесі виконання криптографічних подій. На відміну від класичних моделей, де шифрокод визначається відображенням $Enc_k(m)$, у даному підході шифрокод формується як координатне відображення об'єктів g_i у внутрішньому координатному просторі системи. Шифрокод виступає навігаційною інструкцією, реконструкція якої дозволяє знайти об'єкт g_i у внутрішньому координатному просторі. Будь-якої іншої семантики, крім необхідної для реконструкції координатної події шифрокод не містить. У системі формується вектор події e_t – еквівалентний сформованому шифрокоду c_t, які мають різну форму представлення. Нехай UA_t – компонент відкритого тексту, NA_t – внутрішній ентропійний вектор імітаційних даних, що використовується у випадках відсутності відкритого тексту та визначається розподілом $\mathcal{D}_{\mathcal{NA}}$, що забезпечує маскування структури повідомлення: $NA_t \sim \mathcal{D}_{\mathcal{NA}}$. Внутрішній вектор e_t та зовнішній вектор c_t однієї і тієї ж криптографічної події задаються відображеннями:

$$e_t = \Pi_t^{int}(UA_t, NA_t, \mathcal{E}_t), \quad c_t = \Pi_t^{ext}(UA_t, NA_t, \mathcal{E}_t),$$

де Π_t^{int} – внутрішня (латентна) проєкція, що формує подію e_t у вигляді множини бінарних векторів, Π_t^{ext} – зовнішня проєкція, що формує шифрокод c_t як спостережуване представлення криптографічного процесу, $\mathcal{E}_t$ – операційний стан системи. Еволюція $\mathcal{E}_t$ відображається: $\mathcal{E}_{t+1} = \Psi_t(\mathcal{E}_t, c_t)$, де Ψ_t – фазово-залежне стохастичне відображення, c_t – верифікований шифрокод (подія). Унаслідок унікальності кожної фази: $\forall i \neq j: \Phi_i \neq \Phi_j$ виникає фундаментальна властивість фазової антиколізійності шифрокодів, яка може бути записана у вигляді $m_i = m_j \Rightarrow c_i \neq c_j, \quad c_i = c_j \Rightarrow m_i \neq m_j$. Координатний компонентний простір 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 $G_t^{(c_t)} = \{g_1, g_2, \dots, g_k\}$ – конфігурація індукована шифрокодом. Шифрокод c_t приймається тоді і тільки тоді, коли виконується предикат верифікації: $V_{\mathcal{E}_t}(c_t) \in \{0,1\}, \quad V_{\mathcal{E}_t}(c_t) = 1 \Leftrightarrow G_t^{(c_t)} \subset \mathcal{A}_t$, де $V_{\mathcal{E}_t}$ – функція верифікації, а значення 1 відповідає прийняттю. Верифікація не потребує знання семантики відкритого тексту і базується виключно на логічній узгодженості структури шифрокоду з параметрами фазової симетрії системи. Система працює у логіці «свій / чужий» шифрокод. Нехай $S_t \in \{UA_t, NA_t, UA_t \cup NA_t\}$ – джерело подій у системі, що

визначає формування шифрокодів. Нехай $\{C_t\}_{t\in N}$ – випадковий процес шифрокодів, де N – множина фаз. Тоді виконується рівність розподілів: $\mathcal{L}\left(\{C_t\}_{t\in N}^{(UA)}\right) = \mathcal{L}\left(\{C_t\}_{t\in N}^{(NA)}\right) = \mathcal{L}\left(\{C_t\}_{t\in N}^{(UA\cup NA)}\right)$, де верхній індекс позначає джерело, що індукує процес. Тобто процес шифрокодів є статистично нерозрізнюваним відносно джерела їх формування. Відповідно, для зовнішнього спостерігача взаємна інформація між шифрокодами та джерелом подій дорівнює нулю: $I(c_t; S_t) = 0$. Для офлайн-комунікації використовується спільне сховище шифрокодів, яке можна представити як пул $CCP = c^1, c^2, \dots, c_k$. Користувачі періодично завантажують повний пул шифрокодів та локально верифікують кожний шифрокод c_t: $|S: V_S(c_i) = accept| \leq 1$.

Системи використовують стохастичний механізм обміну шифрокодами рівної, але не фіксованої довжини. Довжина шифрокоду визначається фазовими параметрами системи: $L = G(S_t),\ L \in [L_{min}, L_{max}]$. Це дозволяє виконувати попередню фільтрацію кодів: $V_R(c_i) = reject$, якщо $|c_i| \neq L,\ \ c_i \in CCP_L,\ \ CCP_L = c \in CCP: |c| = L$ – перевіряється лише підмножина пулу CCP_L. Оскільки всі користувачі працюють з одним і тим самим пулом ССР, зовнішній спостерігач не має можливості визначити, який саме шифрокод призначений для конкретного отримувача [1] $Pr\left(R_j|c_i\right) = Pr\left(R_j\right)$. Унаслідок цього розподіл шифрокодів у пулі не залежить від факту комунікації: $L(CCP|C) = L(CCP|\neg C)$, де C – подія інформаційного обміну між будь-якою парою користувачів та $Pr(C|CCP) = Pr(C)$ - тобто спостереження пулу шифрокодів не дає інформації про сам факт комунікації [2]. Ймовірність випадкової успішної верифікації стороннього шифрокоду прямує до нуля: $P\left(V_{S_t}(c_i) = accept\right) \ll 1$. Для будь-якого шифрокоду c_i існує не більше однієї системи, для якої виконується умова $V_{S_t}(c_i) = accept$. Таким чином Координатна криптографія дозволяє реалізувати модель офлайн конфіденційної комунікації без явної адресації, у якій зовнішній спостерігач не може встановити отримувача, напрямок комунікації, обсяг обміну відкритими даними та навіть сам факт інформаційного обміну. Ця інновація реалізує комунікаційну модель, у якій криптографічний захист досягається не лише шифруванням повідомлення, але й структурною невизначеністю самого факту комунікації: $I(CCP; C) = 0$, де I – взаємна інформація. Формально це означає, що для будь-якого алгоритму спостереження A його перевага у визначенні факту комунікації або її учасників на основі спостереження пулу ССР дорівнює нулю: $\forall A: Adv_A(CCP) = 0$.

Список використаних джерел

1. Chaum D. Untraceable electronic mail, return addresses, and digital pseudonyms // Commun. ACM. – 1981. – Vol. 24, № 2. – P. 84–90.

2. Danezis & Diaz — metadata-hiding / traffic analysis resistance; інваріантність розподілів.