УДК 519.7

ПОБУДОВА КЛЕПТОГРАФІЧНИХ МОДИФІКАЦІЙ ФУНКЦІЙ ХЕШУВАННЯ

Б. А. Коваленко[1, а], А. М. Кудін[1, б]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

У даній роботі розглядаються клептографічні схеми для деяких криптографічних примітивів. Особлива увага в роботі звертається на клептографічні версії алгоритмів хешування. Доцільність досліджень клептографії у контексті функцій хешування визначається двома фактами. По-перше, дослідження клептографічних лазівок в хеш-функціях практично обмежуються лише використанням випадковості хеш-кодів при невідомих відкритих текстах (як в деяких схемах автентифікації). По-друге, функції хешування лежать в основі стійкості безлічі сучасних протоколів. В доповіді наводиться загальна класифікація клептографічних систем, а також одна з можливих схем побудови хеш-функції на основі незбалансованої схеми Фейстеля з лазівкою для ефективного пошуку сильної колізії (другого прообразу)

Ключові слова: Хеш-функція, клептографія, схема Фейстеля, диференційний шлях, колізія

Вступ

Термін "клептографія" ("kleptography") був уведений А. Яном та М. Юном у 1996 році [**?**]. Клептографія вивчає методи побудови в криптосистемах так званих витоків секрету (trapdoor) або ж "лазівок", що дозволяють розробникам отримувати доступ до певної секретної інформації користувачів криптосистем з метою стеження за потенційними злочинцями, шпигунства, збору маркетингової статистики клієнтів. Актуальність досліджень випливає з того, що практично кожен новий стандартизований криптографічний алгоритм залишає питання наявності в ньому закладок чи каналів витоку секрету. Одним з найвідоміших прикладів є алгоритм генерації псевдовипадкових чисел Dual EC DRBG, що дозволятиме розробникам прогнозувати вихід генератора у випадку, якщо вони володіють секретних ключем каналу витоку [**?**].

1. Класифікація та принципи побудови клептографічних систем

Складність класифікації клептографічних систем випливає з того, що немає чітких формальних критеріїв визначення. В певних випадках такі системи можна виявити на підставі очевидної "нелогічності" їхньої побудови або наявності у розробника явної мети її побудови, але також система може мати помилки проектування. Наприклад, до цього часу не можна визначити чи належить алгоритм шифрування DES до клептографічного, оскільки насправді невідомо, чи слабкі параметри безпеки були застосовані навмисне чи це є наслідком недосконалого аналізу.

Модель клептографічної системи включає в себе захищеного каналу передачі інформації, користувачів, зловмисника та розробника, що має канал витоку секретної інформації (trapdoor) від користувачів. При цьому зловмисник не повинен мати змоги порушити захищеність основного каналу передачі. Також ні зловмисник ні користувач не повинні мати змогу порушити захищеність каналу витоку секрету.

Використовуватимемо таку класифікацію клептографічних систем:

За закритістю реалізації:

1) Відкриті стандартизовані реалізації (програмні бібліотеки, схемотехнічні описи, алгоритмічні специфікації).
2) Закриті, здебільшого апаратні реалізації (криптографічні мікроконтролери, апаратні криптомодулі).

За моделлю дослідження каналів витоків:

1) З можливістю подальшого використання (реверсінг програмних компонент, маскованих апаратних компонент, логічний аналіз специфікацій тощо).
2) Без можливості подальшого використання (реверсінг криптографічних контролерів, вбудованої EEPROM-пам'яті тощо).

За рівнем побудови:

1) Модифікація готових криптосистем (додавання каналу витоку).
2) Побудова нових криптоалгоритмів з вбудованими закладками.

За способом впровадження системи:

1) Модифікація працюючих криптосистем на стороні користувача (через троянські програми, кібератаки тощо).
2) Відкрите розповсюдження клептографічних модифікацій алгоритмів (наприклад, у вигляді програмних компонентів).

[а] animantbk@gmail.com
[б] pplayshner@gmail.com

3) Розповсюдження пропрієтарних закритих криптосистем у вигляді апаратних модулів.
4) Лобіювання стандартизації клептографічних криптосистем, нав'язування їхнього використання через правові механізми чи корпоративні політики.

Приклади клептографічних систем:

1) На основі асиметричної криптосистеми: генератор псевдовипадкової послідовності Dual_EC_DRBG, SETUP (Secretly Embedded Trapdoor with Universal Protection – таємно вбудований захищений канал витоку секрету) механізм для протококу Діффі-Хеллмана [**?**].
2) На основі симетричної криптосистеми: метод Пренеля [**?**]. Проте пізніше було доведено [**?**], що схема Пренеля ненадійна, зловмисник може знайти лазівку в реалізації.

2. Клептосистеми на базі хеш-функцій

Функція хешування – це відображення, що перетворює повідомлення довільної довжини у хеш-код фіксованої довжини n, тобто $\Phi : \{0,1\}^* \to \{0,1\}^n$. Криптографічна хеш-функція повинна мати додаткові властивості, основні з яких: стійкість до слабкої колізії, стійкість до сильної колізії та стійкість до побудови прообразу.

Задачі клептосистем на базі хеш-функцій є дещо різноманітнішими від задач клептографії для систем шифрування і включають:

1) Побудова каналу витоку секрету. Секретом є повідомлення, що хешується. Таку схему доцільно реалізовувати за умови, що повідомлення достатньо короткі (наприклад паролі).
2) Створення можливості ефективного пошуку прообразу або другого прообразу для розробника на основі секрету. При цьому користувач та зловмисник не повинні бути в змозі ефективно шукати прообраз, другий прообраз, чи вбудованого секрету для їхнього пошуку.
3) Створення можливості ефективного пошуку слабкої колізії для розробника на основі секрету. При цьому користувач та зловмисник не повинні бути в змозі ефективно шукати колізії чи вбудованого секрету для їхнього пошуку.

2.1. Проектування клептографічної схеми для функцій хешування

Розглянемо функцію хешування на базі схеми Меркла-Дамгарда [**?**], що складається з ланцюжка функцій стиснення, що мають вигляд:

$$F : \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n \quad (1)$$

$$\Phi = F(F(F(F(IV, M_0), M_1), ...), M_k), \quad (2)$$

де $\{M_i\}_{i=0..k}$ – блоки повідомлень.

Розглянемо метод побудови функції хешування, що з має такі властивості:

1) Стійкість до пошуку прообразу: за довільним значенням $H \in \{0,1\}^n$ та фіксованим $IV \in \{0,1\}^n$ неможливо ефективно підібрати M : $\Phi(IV, M) = H$.
2) Стійкість до слабкої колізії: неможливо ефективно підібрати таку пару повідомлень $M_1, M_2 \in \{0,1\}^n$, $M_1 \neq M_2$, $\Phi(IV, M_1) = \Phi(IV, M_2)$.
3) Стійкість по пошуку сильної колізії: користувач та зловмисник не в змозі знайти для заданого $M_1 \in \{0,1\}^n$ таке повідомлення $M_2 \in \{0,1\}^n$, $M_1 \neq M_2$, $\Phi(IV, M_1) = \Phi(IV, M_2)$
4) Наявність секретної інформації, володіючи якою розробник в змозі ефективно знайти для заданого $M_1 \in \{0,1\}^n$ таке повідомлення $M_2 \in \{0,1\}^n$, $M_1 \neq M_2$, $\Phi(IV, M_1) = \Phi(IV, M_2)$.

За основу візьмемо схему функції стиснення, схожу на функцію стиснення хеш-функції MD5:

1) Вхід алгоритму: початкове заповнення $\{Q_i\}_{i=-3..0}$, блоки повідомлення $\{M^i\}_{i=0..k}$.
2) Для $i = 1..n$ відбуваються перетворення:
$$Q_{i+1} = F_i(Q_i, Q_{i-1}, Q_{i-2}) \oplus Q_{i-3} \oplus C_i \oplus M_j^i \quad (3)$$
де $F : \{0,1\}^{32\times 3} \to \{0,1\}^3 2$ – нелінійне перетворення, C_i – раундові константи.
3) Виходом функції стиснення буде значення $Q_{-3} \oplus Q_{k-3}, Q_{-2} \oplus Q_{k-2}, Q_{-1} \oplus Q_{k-1}, Q_0 \oplus Q_k$.

Розглянемо метод побудови закладки:

1) Розробник фіксує довільні різниці для блоку повідомлень: $\delta M_j \in \{0,1\}^{32}$ та різниці робочих станів $\{\delta Q_i \in \{0,1\}^{32}\}_{i=1..k-4}$, $\{\delta Q_i = 0\}_{i=-3..0,k-3..k}$. Ці параметри являються секретом розробника для обчислення другого прообразу.
2) Подамо нелінійну підстановку F у вигляді булевих функцій для компонент
$$F(x) = \langle f_0(x), ..., f_{31}(x)\rangle, f : \{0,1\}^{32\times 3} \to \{0,1\}$$
3) Для раундів $i = 1..n$ виконуються кроки 4-6.
4) Для кожного $\delta T[j], \delta T \equiv \delta Q_{i+1} \ominus \delta Q_{i-3} \ominus \delta M^i, j = 0..31$ будується функція $f_j^i(\delta x)$, $\langle Q_i, ..., Q_{i-2}\rangle \equiv x$, $\delta x = \langle \delta x_0, ..., \delta x_{95}\rangle$, $\delta x_i \in \{0,1\}$.
5) Будується дві множини індексів $I_0 = \{i|\delta x_i = 0\}$, $I_1 = \{i|\delta x_i = 1\}$.
6) Функція f_j^i будується у вигляді $f_j^i = \bigoplus_{j\in I_1} x_j \cdot D_j \oplus D \oplus \gamma$, де $\{D_j = 1\}$ – тотожні ДНФ формули випадково згенеровані на основі атомів $\{x_j\}_{j\in I_0}$, D – довільно згенерована формула на основі атомів $\{x_j\}_{j\in I_0}$, параметр $\gamma = T[j]$ у випадку коли $|I_1|$ – парне, інакше $\gamma = T[j] \oplus 1$.

Для пошуку високойморвірного диференціального шляху побудованої функції зловмиснику(користувачу) потрібно знайти раундові різниці. Перша різниця формується виключно з δM_0, тож зловмисник має розглядати всі можливі 2^{32} варіантів різниць. Наступна різниця δF_1 формується гарантовано (за умови, що ми розглядаємо правильну δQ_1), проте уже значення δQ_2 потребує розглядати усі можливі M_1. Отже для отримання різниць перших двох раунді потрібен уже перебір 2^{64} значень M_0, M_1. Розмірковуючи подібним чином можна показати, що для отримання різниць $Q_i, i \geq 3$ необхідно здійснювати перебір 2^{96} значень.

Зловмисник може піти іншим шляхом – спробувати знайти найбільш імовірні диференціали для кожної нелінійної функції F_i. Тоді для кожного значення $Q_i[j] \in \{0,1\}$ зловмисник шукатиме δx. Проте ця задача у загальному випадку буде NP-повною та експоненційною від розміру вектора x, задача зводиться до задачі 3-ДНФ.

Висновки

В доповіді наведені задачі клептографії та класифікація клептографічних систем. В результаті проведених досліджень були визначені задачі клептографії стосовно функцій хешування. Окрім утворення каналу витоку секрету, додатково з'являються задачі побудови алгоритмів хешування, що дозволяють розробнику, який володіє секретом, ефективно будувати колізії. В даній роботі була продемонстрована схема з клептографічної хеш функції, що окрім криптографічних властивостей має також секрет, що дозволяє розробнику будувати диференційні шляхи ймовірності 1 (тобто успішно проводити атаку пошуку сильної колізії).