УДК 002.5:681.3

В.А. Михеев, М.М. Репин

ИССЛЕДОВАНИЕ ВОЗМОЖНЫХ АТАК НА АЛГОРИТМ «КОМПЛЕКСНАЯ ЗАЩИТА СТЕГАНОГРАФИЧЕСКИХ СООБЩЕНИЙ»

Рассмотрены виды возможных атак на алгоритм «Комплексная защита стеганографических сообщений». Проанализированы основные виды нарушителей и этапы подготовки к атаке. На основе анализа наиболее часто применяемых на практике атак построен возможный сценарий развития атаки на алгоритм КЗСС и приведены рекомендации для устранения возможных угроз.

Современные стеганографические системы; файл-контейнер; множественная инкапсуляция; криптоанализ.

V.A. Mikheev, M.M. Repin

THE INVESTIGATION OF POSSIBLE ATTACKS ON CPSM

In the article all possible attacks on algorithm "Complex protection of steganographic messages" are considered. Principal types of attackers and stages of preparation for attack are analysed. On the basis of the analysis of most used in practice attacks the possible scenario of development of attack to algorithm CPSM is constructed and there are recommendations for elimination of possible threats are resulted.

Modern steganography system; the file-container; multiple encapsulation; cryptoanalysis.

Алгоритм «Комплексная защита стеганографических сообщений» (КЗСС), рассмотренный в [1], позволяет обеспечить защиту стегосообщения от различных видов атак. В то же время существует возможность, что с помощью модификаций и расширений, атаки, которые не представляют опасности, станут актуальными.

Для выявления опасных атак рассмотрим известные типы атак на стегоалгоритмы и выделим представляющие наибольшую опасность для алгоритма КЗСС.

Нарушитель, осуществляющий атаку, может быть пассивным, активным и злоумышленным.

Пассивный нарушитель может обнаружить стегоканал и прочитать сообщения, но только при условии, что система шифрования имеет недостаточную криптостойкость или вообще не применяется. Сама возможность обнаружения стегоканала ставит под вопрос устойчивость всей стегосистемы.

В отличие от пассивного, активный нарушитель может угрожать целостности стеганосообщения. Это позволяет определить факт вмешательства, но существуют области, где это может быть серьезной угрозой, например когда сообщение содержит информацию, получение которой критически важно для абонента в определенное время, по прошествии которого информация теряет свою ценность.

Особенностью злоумышленного нарушителя является то, что он способен не только разрушать, но и создавать ложные стеганосообщения.

Рассмотрим виды атак, которые может предпринять нарушитель для реализации угроз.

Первый и самый простой вид атак, это субъективная атака. Она заключается в поиске скрытых сообщений с помощью просмотра изображений или прослушивания аудиозаписей. Данная атака обычно применяется на начальных этапах вскрытия стегосистемы.

На этапе первичного анализа также проводятся следующие мероприятия [5]:

1. Первичная сортировка стегоматериалов по внешним признакам.
2. Выделение стегоматериалов с известным алгоритмом встраивания.

3. Определение использованных стегоалгоритмов.
4. Проверка достаточности объема материала для стегоанализа.
5. Проверка возможности проведения анализа по частным случаям.
6. Аналитическая разработка стегоматериалов. Разработка методов вскрытия стегосистемы.
7. Выделение стегоматериалов с известными алгоритмами встраивания, но неизвестными ключами и т.д.

Из криптоанализа нам известны следующие разновидности атак на шифрованные сообщения [6]:

- атака с использованием только шифрованного текста;
- атака с использованием открытого текста;
- атака с использованием выбранного открытого текста;
- адаптивная атака с использованием открытого текста;
- атака с использованием выбранного шифрованного текста.

По аналогии с криптоанализом в стегоанализе можно выделить следующие типы атак, актуальных для алгоритма КЗСС [5]:

- Атака на основе известного заполненного контейнера. В этом случае у нарушителя есть одно или несколько стеганосообщений. В последнем случае предполагается, что встраивание скрытой информации осуществлялось одним и тем же способом. Задача злоумышленника может состоять в обнаружении факта наличия стегоканала (основная), а также в его извлечении или определения ключа. Зная ключ, нарушитель получит возможность анализа других стегосообщений.
- Атака на основе выбранного скрытого сообщения. В этом случае злоумышленник имеет возможность предлагать для передачи свои сообщения и анализировать получающиеся стеганосообщения.
- Адаптивная атака на основе выбранного скрытого сообщения. Эта атака является частным случаем предыдущей. В данном случае злоумышленник имеет возможность выбирать сообщения для навязывания адаптивно, в зависимости от результатов анализа предыдущих стеганосообщений.

Также существуют атаки, которые не имеют прямых аналогов в криптоанализе:

- Атака на основе известного пустого контейнера. Если он известен злоумышленнику, то путем сравнения его с предполагаемым стеганосообщением он всегда может установить факт наличия стегоканала. – Атака на основе выбранного пустого контейнера. В этом случае злоумышленник способен заставить абонента пользоваться предложенным ему контейнером. Например, предложенный контейнер может иметь большие однородные области (однотонные изображения), и тогда будет трудно обеспечить секретность внедрения.
- Атака на основе известной математической модели контейнера или его части. При этом атакующий пытается определить отличие подозрительного сообщения от известной ему модели. Например допустим, что биты внутри отсчета изображения коррелированы. Тогда отсутствие такой корреляции может служить сигналом об имеющемся скрытом сообщении. Задача внедряющего сообщения заключается в том, чтобы не нарушить статистики контейнера. Внедряющий и атакующий могут располагать различными моделями сигналов, тогда в информационно-скрывающем противоборстве победит имеющий лучшую модель.

Для противодействия перечисленным видам атак, а также их возможным модификациям, алгоритм КЗСС содержит в себе несколько ступеней защиты. Реализация атаки на КЗСС возможна только при использовании комплексного подхода.

Рассмотрим математическую модель стеганосистемы, на которой построен КЗСС. Процесс тривиально стеганографического преобразования описывается зависимостями:

Ψ – процесс скрытия информации;

D – процесс извлечения скрытой информации;

$$\Psi: C \times M \to S; \tag{1}$$

$$D: S \to M, \tag{2}$$

где $S = \{(c_1, m_1), (c_2, m_2), \dots, (c_n, m_n), \dots, (c_q, m_q)\} = \{s_1, s_2, \dots, s_q\}$ – множество контейнеров-результатов (стеганограмм). Необходимые условия: 1. Отсутствие "пересечения", то есть, если $m_a \neq m_b$ причем $m_a, m_b \in M$, а $(c_a, m_a), (c_b, m_b) \in S$, то $E(c_a, m_a) \cap E(c_b, m_b) = \emptyset$.

$$|C| \geq |M|. \tag{3}$$

Стороны должны знать алгоритмы прямого (Ψ) и обратного (D) стенографического преобразования.

На основании этого, под стеганосистемой будем понимать совокупность $\sum = (C, M, S, \Psi, D)$ контейнеров, сообщений и преобразований, которые их связывают.

Надежность стеганосистемы будем описывать случайностью избирания контейнера c из множества C с вероятностью P_c.

Основой КЗСС служит алгоритм разбиения [2], в основу которого ложится цель сведения вероятности обнаружения наличия скрытых сообщений к минимуму. Основой является создание большой избыточности контейнеров, которая позволит отвлечь внимание от скрытой информации, так как изменение распределения P_c при встраивании секретных сообщений будет минимально.

На вход поступает соотношение Q. Функция $Z(Q) = S_1, S_2 \dots S_n$ осуществляет разбиение Q и зашифровывание получившихся блоков. В стеганокодере осуществляется распределение шифроблоков по контейнерам, причем в различных файлах должно использоваться их одинаковое число. Для повышения надежности при передаче можно использовать инверсию функции Z к сообщению Q.

$$\bar{Z}(Q) = S_n \dots S_2, S_1. \tag{4}$$

На выходе стеганокодера мы получаем контейнеры с дублированием, что повышает вероятность успешного декодирования.

Атака на данную часть алгоритма подразумевает несколько условий. Основным и самым главным является условие осведомленности злоумышленника о возможности осуществления передачи стеганосообщений и о предполагаемом стегоканале. Второе условие, это предположение о возможном разбиении исходного сообщения. И третьим условием является знание о критическом числе перехваченных контейнеров, которое позволит получить часть стеганосообщения. Целью атаки является получение полного стеганосообщения.

Допустим, что исходное сообщение разбито на τ частей и распределено по $K(\tau)$ контейнерам. Критическое число перехваченных контейнеров, при расшифровке которых становится возможно получение части исходного сообщения, – $N(\tau)$, $X(\tau)$ – число сообщений, потеря которых не критична для расшифровки.

Тогда часть $\tau = K(\tau) - X(\tau)$. При известном значении этих параметров атака становится вероятной.

Вторым шагом предполагаемой атаки, при условии, что злоумышленнику удалось получить критическое число стегоконтейнеров, является преодоление множественной инкапсуляции. Основным параметром этого этапа защиты является глубина инкапсуляции p. Если исключить возможность сговора или прямой утечки значения данного параметра, то существует два пути развития атаки. Первый путь – это последовательное расшифровывание стегоконтейнеров до получения удовлетворительного результата. При этом способе атаки есть возможность получить беспорядочный набор данных при нескольких первых расшифровках, что может быть последствием как недостаточным раскрытием глубины p, так и недобором критического числа контейнеров на первом шаге. Более быстрым способом является проба некоторого фиксированного p, с учетом того, что увеличение глубины дает существенное увеличение размера стеганосообщения. Сопоставив размер перехваченных контейнеров с примерным значением p, можно существенно упростить расшифровку.

Третий этап атаки подразумевается только при необходимости не только перехватить и прочитать стеганосообщение, но и модифицировать его для осуществления дезинформации. Для защиты от нарушения целостности в КЗСС применяется электронная цифровая подпись (ЭЦП) контейнеров. Так как КЗСС не дает жестких рекомендаций по использованию конкретных алгоритмов, то возможные атаки и их сложность необходимо оценивать для каждого конкретного случая отдельно.

Таким образом, алгоритм КЗСС обеспечивает надежную защиту от различных видов атак. Его модульная структура позволяет в зависимости от целей усиливать защиту критических показателей, путем применения различных алгоритмов шифрования, а разбиение сообщения существенно понижает требования к пропускной способности канала передачи.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Михеев В.А. Репин М.М.* Способ многоконтейнерной стеганографической защиты информации с разделением исходного сообщения на части и множественной инкапсуляцией // Материалы XI Международной научно-практической конференции «Информационная безопасность-2010» (Часть I). – Таганрог: Изд-во ТРТУ,2010. – С. 88-90.
2. *Михеев В.А., Николаев А.В., Репин М.М.* Способ многоконтейнерной стеганографической защиты информации с разделением исходного сообщения на части // Вопросы защиты информации. – М.: ВИМИ, 2009. – № 4 (87). – С. 32-35.
3. *Михеев В.А. Репин М.М.* Анализ алгоритмов подсчета числа рациональных точек эллиптической кривой // Материалы XI Международной научно-практической конференции «Информационная безопасность-2010» (Часть I). – Таганрог: Изд-во ТРТУ, 2010. – С. 91-92.
4. *Михеев В.А.,Репин М.М.* Анализ алгоритмов подсчета числа рациональных точек эллиптической кривой // Вопросы защиты информации. – М.: ВИМИ, 2010. – № 3. – С. 17-22.
5. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
6. *Schneier B.* Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York // John Wiley and Sons, 1996.

Михеев Вячеслав Алексеевич
Организация: Открытое акционерное общество «Концерн радиостроения «Вега»».
E-mail: mikheev@vega.su.
121170, г. Москва, Кутузовский проспект, 34.
Тел.: 84992490585, факс: 84959331563.

Репин Максим Михайлович
E-mail: bmstu.iu8@gmail.com.
Тел.: 84992494429, факс: 84959331563.

Mikheev Viatcheslav Alexeevich
The deputy director of Joint-Stock Company «Radio Engineering Corporation «VEGA».
E-mail: mikheev@vega.su.
34, Kutuzov avenue, Moscow, 121170, Russia.
Phone: +74992490585, fax: +74959331563.

Repin Maxim Mixajlovich
E-mail: bmstu.iu8@gmail.com.
Phone: +74992494429; fax: +74959331563.

УДК 681.03.245

Л.К. Бабенко, Е.А. Ищукова

ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ УПРОЩЕННОЙ ФУНКЦИИ ХЭШИРОВАНИЯ SHA*

Рассмотрены основные подходы к анализу современных функций хэширования с использованием метода дифференциального криптоанализа на примере упрощенных версий функции SHA. Подходы, рассмотренные для анализа функции SHA, могут быть легко использованы для анализа других современных функций хэширования.

Функция хэширования; дифференциальный криптоанализ; разность; вероятность.

L.K. Babenko, E.A. Ischukova

DIFFERENTIAL CRYPTANALYSIS OF SHA-LIKE HASH FUNCTIONS

In article highlights of hash functions differential cryptanalysis on an example of algorithm SHA are considered. The technique of carrying out of the differential analysis of SHA hash function and also other hash functions having a similar structure is offered.

Hash function; differential cryptanalysis; difference; probability.

Как известно, криптография призвана решать задачи обеспечения конфиденциальности, целостности, аутентификации, невозможности отказа от авторства, неотслеживаемости с использованием математических методов. Для решения ряда данных задач используются криптографические функции хэширования (hash-functions) [1]. Хэш-функции – это функции, предназначенные для сжатия произвольного сообщения или набора данных, записанного, как правило, в двоичном алфавите, в некоторую битовую комбинацию фиксированной длины, называемую сверткой. В криптографии хэш-функции применяются для решения двух основных задач:

- построения систем контроля целостности данных при их передаче или хранении;
- аутентификации данных.

В 1989 г. Р. Меркль (Ralph C. Merkle) и И. Дамгорд (Ivan Damgaard) [1] независимо предложили итеративный принцип построения криптографических функций хэширования. Данный принцип позволяет свести задачу построения хэш-функции на множестве сообщений различной длины к задаче построения отобра-

* Работа поддержана грантом РФФИ № 09-07-00245-а.