УДК 004.35

СЕМАНТИЧЕСКАЯ БЕЗОПАСНОСТЬ И НЕРАЗЛИЧИМОСТЬ

Храпов А.С.
студент магистратуры 2 курс
кафедры «Компьютерные системы и технологии»,
Национальный исследовательский ядерный университет «МИФИ»
Россия, г. Москва
Кинаш В.М.
студент магистратуры 2 курс
кафедры «Компьютерные системы и технологии»,
Национальный исследовательский ядерный университет «МИФИ»
Россия, г. Москва
Малков Л.В.
студент магистратуры 2 курс
кафедры «Стратегического планирования и методологии управления»,
Национальный исследовательский ядерный университет «МИФИ»
Россия, г. Москва
Дождев А.И.
студент магистратуры 2 курс
кафедры «Стратегического планирования и методологии управления»,
Национальный исследовательский ядерный университет «МИФИ»
Россия, г. Москва

Аннотация: Данная статья описывает такие свойства криптографической системы, как семантическая безопасность (SEM) и неразличимость (IND). Рассмотрена связь этих свойств с уровнем защищенности криптографической системы.

Ключевые слова: семантическая безопасность, неразличимость, криптографические системы, информационная безопасность.

STRUCTURE OF COMPILER FOR ONT-TIME PROGRAMS

Hrapov A.S.

graduate student, second course

Department of Computer Systems and Technologies,

National Research Nuclear University MEPhI

Moscow, Russia

Kinash V.M.

graduate student, second course

Department of Computer Systems and Technologies,

National Research Nuclear University MEPhI

Moscow, Russia

Malkov L.V.

graduate student, second course

Department of Strategic planning and management methodologies,

National Research Nuclear University MEPhI

Moscow, Russia

Dozhdev A.I.

graduate student, second course

Department of Strategic planning and management methodologies,

National Research Nuclear University MEPhI

Moscow, Russia

Annotation: This article is about semantic security and indistinguishability – highly significant properties of cryptographic systems. Also, this article contains a definition of relationship between these properties and secure level of system.
Key words: semantic security, indistinguishability, cryptographic system, information security.

Введение

Семантическая безопасность (semantic security - SEM) и неразличимость (indistinguishability - IND) являются одними из самых важных свойств защищённой системы. Рассмотрение этих свойств является чрезвычайно важным при анализе уровня безопасности системы [1]. Наиболее часто угрозу безопасности представляют атаки открытым текстом (Known-plaintext attack – CPA). Эти атаки базируется на знании некоторых данных о криптосистеме, например, знании открытых ключей, кусков засекреченного текста, как с наличием расшифрованного текста, так и без него [2]. Далее рассмотрены классические понятия безопасности для схем шифрования, защищенных от выбранных атак открытым текстом. Отдельно стоит отметить возможность применения описанных свойств для анализа уровня безопасности систем на базе нейронных сетей [3, 4].

Базовые понятия

Начнём с введения обозначений, которые будут использованы на протяжении всей работы.

Скажем, что функция f: N $\rightarrow$ R полиномиально ограничена, если существует полином p и значение $\bar{n} \in$ N такое, что: для каждого $n \geq \bar{n}$ имеем $f(n) \leq p(n)$; в этом случае просто напишем $f = \mathrm{poly}(n)$. Говорят, что функция ε: N $\rightarrow$ R пренебрежимо мала, тогда и только тогда, когда для каждого полинома

p существует $n_p \in N$ такое, что $\varepsilon(n) \leq \frac{1}{p(n)}$ для каждого $n \geq n_p$; в этом случае $\varepsilon = negl(n)$. Здесь и далее $n \in N$ использовано в качестве параметра безопасности.

Схема шифрования с секретным ключом представляет собой тройку вероятностных алгоритмов полиномиального времени (Gen, Enc, Dec), работающих в пространстве сообщений $M = \{0, 1\}^m$ (где $m = poly(n) \in N$), которые удовлетворяют следующим двум условиям [5]:

1. Алгоритм генерации ключа $Gen(1^n)$ на вход параметра безопасности n в унарных выходах битовой строки k.

2. Для всех k в диапазоне $Gen(1^n)$ и любого сообщения $x \in M$ алгоритмы Enc (шифрование) и Dec (дешифрование) удовлетворяют $Pr[Dec(k, Enc(k, x)) = x] = 1$, где вероятность принимается за внутренние броски монет Enc и Dec.

Запишем K для диапазона $Gen(1^n)$ (пространство ключей) и $Enc_k(x)$ для Enc(k, x).

Классические понятия безопасности: IND-CPA и SEM-CPA

Понятия IND-CPA и SEM-CPA могут быть определены как игра между соперником C и противником A. Во-первых, C генерирует легитимный ключ $k \leftarrow Gen(1^n)$, который он использует на протяжении всей игры. Игра начинается с первого этапа обучения. Фаза вызова следует, когда A получает вызов. После следует второй этап обучения, и, наконец, A должен вывести решение. Этапы обучения определяют тип атаки, а этап вызова - понятие, захваченное игрой.

M - распределение сообщений, а P является частью вычислений противника, которая предсказывает функцию f, а S является информацией о состоянии, которая передается от запрашивающего к алгоритму распределения и прогнозирования. Также это определение даже позволяет

выводу функции *f* зависеть от информации, которую злоумышленник узнает из своих выбранных запросов открытого текста [6].

Последующие определения ссылаются на эту игровую среду.

Этап обучения CPA: A разрешено адаптивно запрашивать у C шифрование сообщений по своему выбору. C отвечает на запросы, используя ключ *k*. Это эквивалентно утверждению, что A получает (парного оракула доступа - шифрования) PPT, которое было инициализировано с помощью ключа *k*.

Этап вызова IND: A определяет шаблон запроса, состоящий из двух сообщений равной длины x_0, x_1, и отправляет его в C. Претендент C выборочно случайным образом выбирает случайный бит $b \leftarrow \{0, 1\}$, и отвечает с шифрованием $\mathrm{Enc}_k(x_b)$. Цель A - угадать *b*. При этом симметричная схема шифрования (K, ε, D) безопасна для последнего вызова IND-CPA тогда и только тогда, когда для каждого PPT A, который выполняет серию вызовов своего оракула, в котором два запроса одинаковы и заканчивается одним вызовом, в котором они могут отличаться, функция

$$\epsilon(\mathrm{k}) = \Pr\left[\mathrm{A}^{\varepsilon_{\mathrm{K}}\left(\mathrm{Select}(\cdot,\cdot,0)\right)}\left(1^{\mathrm{k}}\right) = \mathrm{b} \middle| \mathrm{K} \leftarrow \mathrm{K}\left(1^{\mathrm{k}}\right)\right]$$

$$-\Pr\left[\mathrm{A}^{\varepsilon_{\mathrm{K}}\left(\mathrm{Select}(\cdot,\cdot,1)\right)}\left(1^{\mathrm{k}}\right) = \mathrm{b} \middle| \mathrm{K} \leftarrow \mathrm{K}\left(1^{\mathrm{k}}\right)\right]$$

пренебрежимо мала, когда $\mathrm{Select}(\mathrm{M}^0, \mathrm{M}^1, \mathrm{b}) = \mathrm{M}^{\mathrm{b}}$ при $\mathrm{b} \in \{0, 1\}$.

Этап вызова SEM: A отправляет C шаблон запроса (S_m, h_m, f_m), состоящий из многоразмерной схемы S_m, задающей распределение по открытым текстам длиной m бит функции извещения h_m: $\{0,1\}^m \rightarrow \{0,1\}^*$ и целевой функции f_m: $\{0,1\}^m \rightarrow \{0,1\}^*$. Претендент C отвечает парой ($\mathrm{Enc}_k(x)$, $h_m(x)$), где x выбирается в соответствии с S_m. Задача A состоит в том, чтобы вывести $f_m(x)$.

В определении семантической безопасности не требуется, чтобы вероятность победы A в игре всегда была незначительной. Вместо этого вероятность успеха A сравнивается с вероятностью симулятора S, который играет в ограниченную игру: с одной стороны, S не получает этапов обучения. С другой стороны, на этапе вызова S не получает зашифрованный текст, а только вывод функции извещения. Это использование симулятора делает то, с чем трудно работать в доказательствах, так как нужно создать симулятор для каждого возможного A, чтобы доказать безопасность схемы.

Схема шифрования секретного ключа A считается защищенной с помощью SEM-CPA, если для любого вероятностного противника A за полиномиальное время существует вероятностный имитатор S за полиномиальное время, такой, что шаблоны запроса, создаваемые S и A, распределяются одинаково и вероятность успеха выигрыша A в игре, определяемой фазами обучения CPA и фазой вызова SEM (рассчитанной по монетам A, Gen и S_m), пренебрежимо близок (по n) к вероятности успеха S выигрыша в уменьшенной игре.

В безопасности IND-CPA, важно, чтобы ε_K была рандомизированной или с состоянием; в противном случае, если S записывает все пары (открытый и зашифрованный текст,), тогда распределение M может быть просто запрошено по всем открытым текстам, а предиктор P может просто посмотреть в своем списке зашифрованных текстов свой второй аргумент, вернув соответствующий открытый текст. Однако, эта атака потерпит неудачу, если ε_K будет возвращать разные значения при каждом использовании. Подобная схема также предотвращает атаки на блокчейн-системы [7].

Результаты

Семантические модели безопасности - то, чего хотят добиться от схемы шифрования: злоумышленник, получивший зашифрованный текст, не может ничего узнать о зашифрованном сообщении, которое он не мог бы также узнать из своего знания о распространении сообщения и, возможно, существующей дополнительной информации (смоделированной h_m).

Заключение

Рассмотренные в статье свойства безопасности информационных систем являются чрезвычайно важными при анализе уровня защищённости системы. Системы, отвечающие семантической модели безопасности, устойчивы к атакам на основе открытых текстов.

Библиографический список

1. Gagliardoni T., Hülsing A., Schaffner C. Semantic security and indistinguishability in the quantum world //Annual Cryptology Conference. – Springer, Berlin, Heidelberg, 2016. – С. 60-89.
2. Beame P. Cryptography: курс лекций. URL: https://courses.cs.washington.edu/courses/cse599b/06wi/ . Дата обращения: 15.12.2018
3. Стрелец А.И., Протопопова Ю.Д., Тоичкин Д.В., Ключникова Б.В. Анализ тензорных процессоров на предмет эффективности применения для расчёта систолических массивов нейронных сетей. Форум молодых ученых. – 2018. – № 7 (23). – С. 916.
4. Стрелец А.И., Протопопова Ю.Д., Тоичкин Д.В., Ключникова Б.В. Использование нейронных сетей на основе многослойного персептрона

для прогнозирования условий протекания химических реакций. – 2018. – № 7 (23). – С. 930.

5. Bagherzandi A. et al. Relations between semantic security and indistinguishability against cpa, non-adaptive cca and adaptive cca in comparison based framework //arXiv preprint cs/0508110. – 2005.
6. Bagherzandi A., Mohajeri J., Salmasizadeh M. Comparison Based Semantic Security is Probabilistic Polynomial Time Equivalent to Indistinguishability //IJ Network Security. – 2008. – Т. 6. – №. 3. – С. 354-360.
7. Стрелец А.И., Протопопова Ю.Д., Иванников В.С., Тимофеев К.В. Решение проблемы двойной траты в системе электронного валютного управления на базе технологии блокчейн. – 2018. – № 7 (23). – С. 925.

Оригинальность 96%