УДК 004.773
AMS MSC2020: 94D99

Методические рекомендации по оптимизации параметров системы аутентификации на основе использования универсальных хэш-функций и случайных цепочек бит

Яковлев В. А.[*], **Савинова С. А.**[**], **Гатчин Ю. А.**[**], **Поляков В. И.**[**], **Чикалов Н. В.**[**]

[*]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича
[**]Университет ИТМО

Аннотация. В статьях [3,4] предлагается метод аутентификации на основе использования универсальных хэш-функций и случайных цепочек бит. Настоящая статья является продолжением и содержит методические рекомендации по оптимизации параметров предложенной системы аутентификации.

Ключевые слова: хэш-функции, случайные цепочки бит, аутентификация, оптимизация.

Введение

Разработанный способ аутентификации ключа [3, 4], распределяемого методом Диффи – Хеллмана, требует методики оптимизации параметров.

В предложенном ранее способе аргументы функций являются дискретными, иными словами — в результате испытания принимают значения с определенными вероятностями. Поэтому для оптимизации используется метод дихотомии и метод перебора [1].

Исходными данными в такой системе аутентификации являются: длина ключа n_0, вероятность отличия бит в аутентифицирующих

последовательностях p_m, требуемая вероятность ложного отклонения [2] $P_f < P_f^{\text{треб}}$, требуемая вероятность ложной аутентификации [2] $P_d < P_d^{\text{треб}}$.

Необходимо определить следующие оптимальные параметры: длину подблока аутентификации m, длину аутентификатора v.

При выборе определяемых параметров необходимо обеспечить требуемые вероятность ложного отклонения аутентификации и вероятность ложной аутентификации, а также минимизировать общую длину аутентификаторов всех блоков сообщения.

1. Основные определения

Определение 1. *Аутентификация — это процедура проверки подлинности.*

Хэш-функция — это функция, реализующая определенный алгоритм и выполняющая преобразование массива входных данных произвольной длины в битовую строку фиксированной длины.

Случайные цепочки бит — это двоичные последовательности, которые пользователи получают по дополнительному каналу.

Оптимизация — это процесс максимизации выгодных характеристик.

Вероятность ложной аутентификации — это вероятность события, которое наступает, когда злоумышленник подменяет подблоки ДХ-значения и осуществляет подбор к ним аутентификаторов таким образом, что число неправильно подобранных аутентификаторов плюс число неправильно принятых блоков из-за несовпадения случайных цепочек бит не больше чем пороговое значение.

Вероятность ложного отклонения — это вероятность события, которое наступает, когда число неправильно аутентифицированных блоков больше установленного порогового значения из-за несогласованности случайных цепочек бит.

2. Основные результаты

Удалось разработать методику, по которой удается определить оптимальные параметры системы, при которых расчетные значения ложного отклонения и ложной аутентификации не превышают 10^{-6}.

Методика включает в себя следующие разделы:

1) Оценка величины возможного отличия ложного сообщения от истинного и оценка вероятности формирования такого сообщения.
2) Оценка максимально вероятного количества ложных подблоков в последовательности.
3) Построение зависимостей вероятности ложного отклонения последовательности в отсутствие навязывания для различных длин блоков и определение допустимого порога стирания.
4) Построение зависимости ложной аутентификации для различных длин подблоков и длине аутентификатора равной длине подблока.
5) Анализ значений вероятностей ложного отклонения и ложной аутентификации для различных значений порогового значения, длины подборка и длины аутентификатора.
6) Использование способа увеличения безошибочности аутентифицирующих последовательностей за счет использования процедуры помехоустойчивого кодирования.
7) Проведение оптимизации длины аутентификатора.
8) Расчет требуемой длины ключа для аутентификации всего сообщения.

В качестве доказательства применимости данной методики рассмотрен подробно пример ее использования и получения оптимальных параметров.

Заключение

В работе разработана методика оптимизации системы аутентификации значений Диффи – Хеллмана. Подробно рассмотрен пример, который демонстрирует эффективность данной методики. Выбрав должным образом параметры системы аутентификации можно обеспечить малые значения вероятности ложной аутентификации и вероятности навязывания ложного ключа, при этом минимизировав суммарную длину всех аутентификаторов, что и говорит о достижении поставленной оптимизационной задачи.

Список литературы

[1] *Гребенникова, И. В.* Методы оптимизации : учебное пособие. — Екатеринбург : УрФУ, 2017. — 148 с.

[2] *Феллер, В.* Введение в теорию вероятностей и ее приложения : в 2 томах. Т. 2. / Пер. с англ. Р. Л. Добродушина, А. А. Юшкевич, С. А. Молчанова. — 2-е изд. — Москва : Мир, 2017. — 748 с.

[3] *Яковлев, В. А.* Аутентификация сеансового ключа на основе универсальных хэш-функций и случайных цепочек бит / В. А. Яковлев, С. А. Савинова // i-methods — Информатика, вычислительная техника и управление. — 2020. — Т. 12, №4. — URL: http://intech-spb.com/wp-content/uploads/archive/2020/4/2_jakovlev_cavinova.pdf

[4] *Яковлев В. А.* Аутентификация ключей, распределяемых методом Диффи – Хеллмана, на основе использования универсальных хэш-функций и помехоустойчивого кодирования // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). Сборник научных статей VIII Международной научно-технической и научно-методической конференции. — 2019. — Т. 4, №2. — С. 762–767.

Библиографическая ссылка

Методические рекомендации по оптимизации параметров системы аутентификации на основе использования универсальных хэш-функций и случайных цепочек бит / В. А. Яковлев, С. А. Савинова, Ю. А. Гатчин [et al.] // Всероссийская научная конференция «Математические основы информатики и информационно-коммуникационных систем». Сборник трудов. — Тверь : ТвГУ, 2021. — С. 285–289. https://doi.org/10.26456/mfcsics-21-40

Сведения об авторах

1. Виктор Алексеевич Яковлев
Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. Профессор

Россия, 193232, проспект Большевиков д.22, к.1
E-mail: viyak@bk.ru

2. Светлана Алексеевна Савинова
Университет ИТМО. Магистрант

Россия, 197101, Кронверкский проспект, д.49, литер А.
E-mail: savinova-sveta@mail.ru

3. Юрий Арменакович Гатчин
Университет ИТМО. Профессор

Россия, 197101, Кронверкский проспект, д.49, литер А.
E-mail: gatchin1952@mail.ru

4. Владимир Иванович Поляков
Университет ИТМО. Доцент

Россия, 197101, Кронверкский проспект, д.49, литер А.
E-mail: v_i_polyakov@mail.com

5. Никита Вячеславович Чикалов
Университет ИТМО. Магистрант

Россия, 197101, Кронверкский проспект, д.49, литер А.
E-mail: nik.chikalow2011@yandex.ru