УДК *004.056.5*

МЕТОД ЗАЩИТЫ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ НА ОСНОВЕ ГЕНЕРАЦИИ ЛОЖНЫХ СЕКРЕТОВ С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ

И.А.Лепесий, Е.С.Романович
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В работе предложен метод защиты криптографических ключей на основе внедрения ложных сегментов, сгенерированных с помощью машинного обучения. Традиционные методы защиты часто неприменимы в облачных системах. Схема включает разделение ключа, генерацию ложных сегментов через генеративно-состязательные сети и их перемешивание. Использование машинного обучения обеспечивает правдоподобное распределение битов. Это усложняет задачу злоумышленника при компрометации хранилища, делая перебор комбинаций сегментов вычислительно нецелесообразным из-за экспоненциального роста числа ложных вариантов.
Ключевые слова: криптография; криптографическая защита; AES-256; разделение ключа; машинное обучение; медовое шифрование; разделение секрета; генеративно-состязательные сети; ложные данные; информационная безопасность.

METHOD OF PROTECTING CRYPTOGRAPHIC KEYS BASED ON GENERATION OF FALSE SECRETS USING MACHINE LEARNING

I.A. Lepesy, E.S. Romanovich
Educational Institution "Belarusian State University of Informatic and Radioelectronics", Minsk, Republic of Belarus

Abstract. This paper proposes a method for protecting cryptographic keys based on the embedding of false segments generated using machine learning. Traditional security methods are often inapplicable to cloud systems. The scheme involves key splitting, generating false segments using generative adversarial networks, and shuffling them. Machine learning ensures a plausible bit distribution. This complicates the attacker's task when compromising the storage, making brute-force segment combinations computationally infeasible due to the exponential growth of false combinations.
Keywords: cryptography; cryptographic protection; AES-256; key splitting; machine learning; honey encryption; secret sharing; generative adversarial networks; decoy data; information security.

Введение

В современных условиях цифровой трансформации криптографические алгоритмы, такие как AES-256, обеспечивают надежную защиту данных при передаче и хранении. Однако безопасность системы часто определяется не стойкостью алгоритма шифрования, а защищенностью ключевой информации. Инциденты, связанные

с утечкой баз данных, приводят к тому, что злоумышленник получает доступ к зашифрованным ключам или их компонентам.

Основная часть

Традиционные методы защиты, такие как аппаратные модули безопасности или доверенные исполняющие среды, не всегда применимы в распределенных облачных системах из-за высокой стоимости и сложности интеграции. Альтернативным подходом является концепция «медового шифрования», предполагающая наличие ложных данных, которые выглядят правдоподобно для атакующего. И в создании этих ключей может помочь машинное обучение(далее – МО)

Предлагаемая схема защиты включает три основных этапа:

1. Разделение ключа. Ключ шифрования K длиной 256 бит разделяется на m сегментов (например, m=3) с использованием схемы разделения секрета или побайтового распределения.

2. Генерация ложных сегментов. Для каждого реального сегмента генерируется n ложных сегментов. Критически важно, чтобы распределение битов в ложных сегментах соответствовало распределению в реальных ключах.

3. Перемешивание и хранение. Реальные и ложные сегменты перемешиваются и сохраняются в хранилище. Метаданные, указывающие на принадлежность сегмента к реальному ключу, не хранятся явно, а восстанавливаются только при успешной аутентификации пользователя.

Для генерации ложных сегментов оптимально использовать генеративно-состязательной сети. Архитектура включает: генератор – принимает на вход случайный шум z и выдает вектор битов длиной 85 бит (при разделении 256 бит на 3 части). Дискриминатор: Обучается различать реальные сегменты ключей) и сгенерированные векторы.

Заключение

В работе предложен метод защиты криптографических ключей, основанный на внедрении ложных сегментов, сгенерированных с помощью машинного обучения. Использование МО в криптографии огромный потенциал в помощи криптографу. Это усложняет задачу злоумышленника при компрометации хранилища ключей, так как перебор комбинаций сегментов становится вычислительно нецелесообразным из-за экспоненциального роста числа ложных вариантов.

Список использованных источников

1. Алпайдин, Э. Машинное обучение: новый искусственный интеллект / Э. Алпайдин. – М. : Альпина Паблишер, 2017. – 208 с.
2. Основы криптографии / А. П. Алфёров [и др.]. – М. : Гелиос АРВ, 2005. – 430 с.

References

1. Alpaidin, E. Machine Learning: A New Artificial Intelligence / E. Alpaidin. – Moscow : Alpina Publisher, 2017. – 208 p.
2. Fundamentals of Cryptography / A. P. Alfyorov [et al.]. – Moscow : Helios ARV, 2005. – 430 p.

Сведения об авторах

Романович Е.С., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», egor.romanovich.00@inbox.ru
Лепесий И.А., маг. воен. наук, старший преподаватель кафедры тактической и общевоенной подготовки, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», dljatebja1@mail.ru

Information about the authors

Romanovich E., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", egor.romanovich.00@inbox.ru

Lepesiy I., Master of Military Sciences, Senior Lecturer, Educational Institution "Belarusian State University of Informatics and Radioelectronics", dljateb-ja1@mail.ru