УДК 004.75

РАЗРАБОТКА РАСПРЕДЕЛЕННОЙ СИСТЕМЫ СОВМЕСТНОГО УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ

Чебыкин И.Б. (Университет ИТМО), **Айтуганов Д. А.** (Университет ИТМО)
Научный руководитель – к.т.н., доцент Лукьянов Н.М.
(Университет ИТМО)

В данной работе описывается изучение существующих реализаций систем совместного управления ключами и создание собственной реализации распределенной системы, на основе существующей открытой библиотеке, реализующей протокол для управления криптографическими ключами.

Введение. Совместное управление криптографическими ключами необходимо для того чтобы упростить процедуру шифрования, повышая при этом надежность и безопасность процесса, ввиду отсутствия необходимости хранить ключи в различных местах без контроля над доступом, и сокращения числа ситуаций, когда ключ необходимо передавать по сети. Существует открытый протокол KMIP, который определяет все необходимые операции над ключами, однако у него нет референсной реализации и все решения, которые используют этот протокол либо коммерческие, направленные на решение какой-либо конкретной задачи бизнеса, либо открытые, которые не готовы к эксплуатации в реальной среде. Поэтому актуальной задачей является разработка распределенного сервера совместного управления ключами, который может успешно заменить коммерческие решения.

Основная часть. Несмотря на то, что протокол совместного управления криптографическими ключами (KMIP) является открытым, организация, которая его разработала, не предоставляет референсной реализации, и на рынке существует несколько реализаций как открытых, так и закрытых, с различной степенью готовности реализации протокола. Перед разработкой своей реализации были рассмотрены следующие решения:

- HyTrust KeyControl – коммерческий сервер, полноценно реализущий протокол и обеспечивающий некоторую отказоустойчивость, с несколькими ограничениями, из-за которых не достигается полная прозрачность распределения:
  – При добавлении ключа необходимо вручную подтверждать запись на каждой из реплик;
  – Добавление нового узла возможно только в ручном режиме;
  – Максимально можно хранить до тысячи объектов, включая удаленные;
  – Нет разграничения прав доступа, т. е. все пользователи имеют доступ ко всем объектам и операциям над ними.
- PyKMIP – Открытая реализация протокола, сервера и клиента на языке Python. В данной библиотека реализована большая часть протокола и библиотека покрыта множеством тестов. С другой стороны сервер, развиваемый в рамках данной реализации используется исключительно для тестирования операций протокола и не рекомендуется для использовая в реальных ситуациях, так как сервер не отказоустойчив.

В качестве основы разрабатываемого проекта была выбрана библиотека PyKMIP. В оригинальной реализации каждый сервер использовал для хранилища ключей встроенную базу SQLite, при добавлении или обращении к ключу осуществлялся простой запрос к этой базе. В разработанном модуле этот запрос заменен на запрос в специализированный слой, который помимо запроса в встроенную базу обращается в базы остальных узлов с такой же операцией добавления или обращения к ключу с помощью разработанного алгоритма достижения консистетности данных.

Для связи между разными серверами используется протокол gRPC, сообщения описываются специальным языком для описания данных бинарных протоколов – Protobuf. Также в существующей библиотеке был расширен компонент конфигурации для возможности установки таких параметров как список серверов в распределенной системе, различных настроек максимального времени ожидания ответа и количества повторных запросов.

Выводы. В рамках данной работы, после обзора существующих решений была найдена реализация протокола совместного управления ключами PyKMIP, на основе которой был реализован программный модуль, реализующий распределенную систему управления криптографическими ключами.

Чебыкин И.Б. (автор) Подпись

Лукьянов Н.М. (научный руководитель) Подпись