УДК

УЛУЧШЕНИЕ СХЕМЫ ПОВТОРНОГО ШИФРОВАНИЯ ЧЕРЕЗ ПРОКСИ-СЕРВЕР С ФУНКЦИЕЙ ЗАЩИТЫ РАСПРЕДЕЛЕННОГО ХРАНИЛИЩА

Нгуен Ань Дык (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»).
Донг Суан Тхань (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»).
Научный руководитель – доцент Таранов С. В. (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»).

Распределенная база данных - теперь новая тенденция для хранения и обмена личными данными. Мы с коллегой потратили много времени на изучение и заключение, что можно повысить безопасность распределенной системы хранения данных с помощью повторного шифрования прокси. Повторное шифрование прокси-сервера позволяет прокси-серверу преобразовать зашифрованный текст, вычисленный под открытым ключом Алисы, в тот, который может быть открыт секретным ключом Боба. Существует много полезных применений этого примитива. Мы представляем несколько эффективных схем повторного шифрования прокси-серверов, которые предлагают улучшения безопасности по сравнению с более ранними подходами.

Мы представляем несколько эффективных схем повторного шифрования прокси-серверов, которые предлагают улучшения безопасности по сравнению с более ранними подходами. Основное преимущество наших схем состоит в том, что они являются однонаправленными (то есть Алиса может делегировать Бобу без необходимости делегировать Бобу ее) и не требуют, чтобы делегаторы раскрывали весь свой секретный ключ кому-либо-или даже взаимодействовали с делегатом-для того, чтобы прокси мог повторно зашифровать их шифротексты. В наших схемах доверенность к доверенному лицу устанавливается лишь в ограниченном объеме. Например, он не может расшифровать шифротексты, которые он повторно шифрует, и мы доказываем, что наши схемы безопасны, даже когда прокси.

В этой статье мы исследовали повторное шифрование прокси-сервера как с теоретической, так и с практической точки зрения. Мы описали характеристики и гарантии безопасности ранее известных схем и сравнили их с набором улучшенных схем повторного шифрования, которые мы представляем на билинейных картах. Эти схемы, основанные на сопряжении, реализуют важные новые функции, такие как защита главного секретного ключа делегатора от сговора доверенного лица и делегата. Одним из наиболее перспективных приложений для повторного шифрования прокси-серверов является предоставление прокси-возможностей ключевому серверу конфиденциальной распределенной файловой системы

Таким образом, серверу ключей не нужно полностью доверять все ключи системы, и секретное хранилище для каждого пользователя также может быть уменьшено.

Нгуен Ань Дык (автор)

Таранов С. В. (научный руководитель)