Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056

Закревский
Игнат Евгеньевич

Создание центра распространения и хранения конфиденциальной информации организаций

АВТОРЕФЕРАТ
на соискание степени магистра технических наук

по специальности 1-98 80 01 Методы и системы защиты информации, информационная безопасность

_____

Научный руководитель
Гурский Александр Леонидович
д.ф.-м.н., профессор

_____

Минск 2018

ВВЕДЕНИЕ

С развитием информационного общества, вопросы, касающиеся защищённого распространения конфиденциально информации приобретают все большую значимость. Неоднократные утечки больших объёмов пользовательских данных из-за плохой организации хранения и распространения конфиденциальной информации подтверждают актуальность этой проблемы. Встаёт вопрос о том, как же правильно хранить такие данные и какие меры предосторожности надо предпринимать, чтобы сохранить их конфиденциальность.

Не смотря на то, что вопрос о хранении конфиденциальных данных актуален для каждого человека, имеющего какие-либо устройства хранения, наиболее остро он стоит в случае больших корпоративных систем. Так, например, скомпрометированный код доступа к базе данных какого-либо интернет-сервиса затронет не одного человека, а значительную группу людей. Утечка базы данных компании GitHub в 2016 году затронула 8 миллионов пользователей, а инцидент с компанией Uber 57 миллионов. На данный момент, число пользователей Facebook превышает 2 миллиарда человек, трудно представить, к каким последствиям может привести компрометация такого объёма данных.

Однако хранение конфиденциальной информации это не только проблемы Интернет-ресурсов. У многих крупных компаний есть необходимость в хранение идентификаторов доступа к своим ресурсам, таким как, корпоративные аккаунты, системы контроля и управления доступом, внутренние базы данных и т.д.

В настоящее время существует множество систем хранения и распространения конфиденциальной информации, однако, существующие системы используют идею мастер-пароля для осуществления всех операций с информацией, которая является точкой отказа всей системы. Разработанная система предлагает отказаться от мастер-паролей, таким образом, компрометация одного пользователя системы не затронет других её пользователей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 13 «Безопасность человека, общества, государства» приоритетных направлений научных исследований Республики Беларусь на 2016-2020 гг., утвержденных Постановлением Совета Министров Республики Беларусь 12 марта 2015 г., № 190. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цели и задачи исследования.

Целью диссертационной работы является исследование проблемы хранения и распределения конфиденциальных данных организаций. Для достижения поставленной цели необходимо решить следующие задачи:

− провести анализ проблем хранения и распределения конфиденциальной информации;

− предложить протокол надёжного хранения и распределения конфиденциальной информации;

− практически реализовать предложенный протокол;

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на 53 научной конференции аспирантов, магистрантов и студентов БГУИР.

Опубликованность результатов диссертации

По результатам исследований, предоставленных в диссертации, опубликовано 2 работы, в том числе 2 статьи в сборниках материалов конференций.

Личный вклад соискателя

В диссертации представлены результаты исследований, выполненных автором. Личный вклад автора состоит в постановке задач исследования, разработке экспериментальных и теоретических методов их решения, в разработке программного комплекса реализующего защищённое хранение и распространение конфиденциальной информации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Хранение защищённой информации пользователей

Хранение паролей в открытом виде является уязвимым вариантом, в случае компрометации БД все пароли скомпрометированы. Поэтому, для хранения паролей их необходимо шифровать.

Для шифрования паролей используется симметричное шифрование AES. Таким образом, когда пользователь создаёт новый секрет, система требует пароль пользователя, для шифрования полученного секрета, этим система нивелирует риски при компрометации БД [18]. Чтобы уменьшить риск вычисления зашифрованной информации (из-за того, что множество секретов шифруются одним и тем же паролём), система генерирует модификатор, который добавляется к пользовательскому секрету.

Предоставление доступа к защищённой информации другим пользователям

Когда речь идёт о хранение паролей для корпоративных систем, необходимо иметь в виду, что подходы, используемые для отдельных пользователей, не подходят.

Одним из самых распространённых вариантов решения такой проблемы является использование мастер-пароля. Такой пароль может устанавливаться на уровне организации или даже всего приложения. Однако, утечка этого ключа ведёт к полной компрометации всей системы.

Так, например, можно рассмотреть систему, в которой для передачи пароля от одного пользователя другому необходим ввод паролей обоих пользователей (пароль автора секрета для расшифровка зашифрованного секрета и пароль пользователя, которому предоставляется секрет, для дальнейшего шифрования секрета), в таком случае, для организации доступа к паролю множеству людей придётся N раз ввести пароль автора секрета.

Хранение паролей в открытом виде является небезопасным, если БД будет скомпрометирована, то будут скомпрометированы и все пароли, к которым было необходимо предоставить доступ.

Следующий вариант – это хранение паролей в памяти процесса, обрабатывающего запросы от пользователя. К сожалению, и на этот тип хранения существует множество атак, например – через дамп областей памяти веб-сервера.

Таким образом, можно прийти к выводу, что хранение шифрованных данных в открытом виде не является допустимым вариантом. Вместо того, чтобы хранить секретную информацию в открытом виде, лучше её зашифровать. Однако встаёт вопрос о выборе подходящего ключа. Можно использовать один ключ на проект, но и этот вариант является неподходящим. Множество шифрограмм зашифрованных одним и тем же ключом -- уязвимый вариант для криптоаналитика. Более того, в случае компрометации одного единственного ключа, скомпрометированными являются все записи системы.

Существует ещё вариант с разделением БД на две, в одной хранятся уже персональные пароли каждого из пользователей, а во второй – заявки на предоставление доступа. Таким образом снижается риск потери части паролей, однако это все ещё не решает проблему хранения.

Одним из вариантов решения проблемы является использование одноразовых паролей. Таким образом: в БД не хранятся незащищённые пароли, в случае компрометации БД криптоаналитик не сможет найти общие характерные особенности шифра, в случае компрометации устройства пользователя – ещё есть парольная защита, в случае компрометации и парольной защиты – будут скомпрометированы данные только одного пользователя.

В виду того, что двухфакторная авторизация является де-факто стандартом для серьёзных защищённых систем, пользователь, как правило, уже обладает подтверждённым источником одноразовых паролей. Это может быть как телефон, специальное приложение или устройство, предоставляющее одноразовые пароли.

Вместо стандартных одноразовых паролей, система генерирует пароли на основе времени, то есть время является параметром для генерации. Таким образом, риск компрометации пароля становится ещё меньше.

Для разграничения доступа различным пользователям к информации используется мандатное управление доступа.

Система реализует физическое разделение базы данных, использующихся для хранения информации различной степени секретности.

ЗАКЛЮЧЕНИЕ

В ходе работы была спроектирована и разработана система для хранения и распространения конфиденциальных данных организаций с использованием одноразовых паролей основанных на интервалах времени и алгоритмов симметричного шифрования.

В процессе работы над данным дипломным проектом были рассмотрены основные принципы разработки программных средств с использованием языка Ruby и фреймворка Ruby on Rails. В результате был создан полноценный программный продукт.

Разработанный проект имеет большой потенциал в связи с отсутствием аналогов на белорусском рынке и востребованностью организациями возможности криптостойкого хранения конфиденциальных данных.

Программный модуль может быть легко внедрен на различных предприятиях в виду гибкости его настройки и малых требований предоставляемых им к вычислительным ресурсам.

При разработке проекта была приобретена экспертиза в области использования программных интерфейсов, предоставляемых современными библиотеками, а также в области тестирования и логирования ошибок.

В качестве возможных вариантов улучшения данного проекта следует назвать использование более криптостойких алгоритмов шифрования для увеличения надежности системы и использование программных механизмов генерации паролей для снижения стоимости использования системы.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Закревский, И. Е. Использование вероятностных структур данных при работе с большими объёмами данных / И. Е. Закревский // Телекоммуникационные системы и сети: материалы 53-й научной конференции аспирантов, магистрантов и студентов (Минск, 2–6 мая 2017 г.). – Минск: БГУИР, 2017. – С. 98.

2-А. Закревский, И. Е. Использование вероятностных структур при работе с большими объемами данных / И. Е. Закревский // Технические средства защиты информации : тезисы докладов XV Белорусско-российской науч.-техн. конф. (Минск, 6 июня 2017 г.). – Минск : БГУИР, 2017. – С. 49.