электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.[773+55+031.42]

Защита персональных данных в социальных сетях

***Коряковцев А.М.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Якушева Н. А. ст. преподаватель
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
bauman@bmstu.ru

1. Введение

Спустя некоторое время после наступления эпохи Web 2.0 появились Социальные сети. Их возникновение не было прорывом, но помогло значительно упростить общение людей в Сети. Люди стали интенсивнее и больше (этому также, ко всему прочему, способствовало развитие технологий, связанных с передачей и обработкой данных) обмениваться информацией. Средний объем данных, как и количество пользователей сети Интернет в общем, и Социальных Сетей в частности увеличилось в разы по сравнению с прошлыми годами и продолжает увеличиваться. [1] [2]

Однако, у всего есть его оборотная сторона. Несмотря на огромное количество существующих на данный момент методов защиты информации, сеть Интернет предполагает публичный доступ к данным, даже в случае с личными данными пользователя – всякий, кто успешно пройдет систему защиты имеет доступ к данным. Это означает, что эти данными могут быть обращены во вред для самого пользователя, так и для тех, кого касаются эти данные, если попадут в не те руки. При взломе аккаунта, злоумышленник может получить эти данные, а также, использовав их с помощью этого же аккаунта обмануть других пользователей, не подозревающих о том, что аккаунт был взломан. Частота этих взломов угрожающе велика – большинство пользователей ставят легко или относительно легко угадываемые пароли (относительно перебора по словарю) [3]. К тому же, после новостей 2013 года [4] [5] стало известно, что сами сервисы Социальных Сетей и даже государство использует личную переписку, данные в профиле и другую информацию в своих целях, ставя под угрозу при этом свободу слова и неприкосновенность личной жизни.

Количество существующих предложений на данный момент невелико, но вскоре этот рынок систем, ставящих на первый план защищенность данных пользователя, скорее

всего, будет активно осваиваться из-за повышения уровня компьютерной грамотности и возрастающему интересу к этой теме [6]. Реализация таких систем не являет собой научного прорыва, однако, как и в случае с появлением Социальных Сетей, разработка Защищенных Социальных Сетей, может быть новым витком в развитии Интернет.

Цель этой работы это разработать и имплементировать систему защиты персональных данных в Социальных Сетях. Чтобы достигнуть этой цели, необходимо выполнить следующие задачи:

- Разработать механизм защиты данных пользователя Социальной сети
- Разработать алгоритм сокрытия реального отправителя и получателя сообщения
- Разработать систему контроля доступа к приватным и публичным данным для пользователей системы
- Интегрировать систему в привычную программную среду пользователя Социальных сетей

2. Теория и спецификация

2.1. Текущие уязвимости для пользователей Социальных Сетей. Модель «клиент-сервер»

Несмотря на свои явные преимущества перед одноранговой сетью – таких как скорость соединения, надежность доступа и защищенность предоставляемых данных от угроз снаружи – модель «клиент-сервер» обладает рядом недостатков, в частности угроз безопасности. Из-за того, что неизвестно, что происходит с хранящейся на серверах информацией, нельзя узнать, что происходит с удаляемыми данными – сервер может хранить эти данные, несмотря на желание пользователя их удалить. [8]. К тому же, доступ к информации пользователя может получить сотрудник самой Социальной Сети и использовать ее в своих целях. [10]

Также известны случаи взлома серверов известных Социальных Сетей, при которых в открытый доступ попали тысячи паролей от аккаунтов пользователей этих сетей. [3] [7].

Угрозы пользовательской стороне

Благодаря серьезным мерам в обеспечении безопасности своих сервисов, Социальные Сети становятся с течением времени безопаснее от атак на их инфраструктуры, однако компьютер пользователя защищен слабее, что и является

основной причиной взлома пользователя. Из-за уязвимостей браузеров или другого программного обеспечения, злоумышленник может получить доступ к учетной записи пользователя.

Утечка информации, вызванная «человеческим фактором»

Естественно, что иногда информация, предназначенная не для сторонних людей, становится известной по причине неосторожного обращения человека с этой информацией. А иногда даже данные, которые, на первый взгляд, не являются тайной, могут использоваться во вред пользователю. Несмотря на все меры безопасности, нельзя сбрасывать со счетов «человеческий фактор». [9]

2.2. Основная информация о системе

Разрабатываемая система представляет собой набор независимых между собой модулей, каждый из которых отвечает за одну из нескольких задач:

- Авторизация и профилирование
- Шифрование данных и обмен ключами
- Взаимодействие с пользователями системы и Социальной Сети
- Графический интерфейс (GUI)
- Интерфейс Социальной Сети

Работу системы обеспечивает модуль-драйвер. Сообщения между модулями могут проходить как напрямую, так и через модуль-драйвер. Схема взаимодействий показана на рис. 3.

2.3. Использованные алгоритмы шифрования и обмен ключами

В системе непосредственно для шифрования используется алгоритм AES (Advanced Encryption Standard) размером ключа 128, 192 или 256 бит [12]. Ключ задается пользователем. Для подписи всех сообщений используется алгоритм шифрования RSA размером ключа 1024 или 2048 бит. Однако в будущем, необходимо отказаться от использования RSA из-за постоянного уменьшения времени, необходимого для взлома закрытого ключа. [13] Ассиметричное шифрование с использованием эллиптических кривых – *ECDH* или ГОСТ. может стать заменой *RSA*.

Обмен ключами *RSA* может происходить 4 различными способами: (предполагается, что Социальная Сеть является не доверенным каналом)

1) По сторонним каналам. В таком случае система не принимает никакого участия в обмене ключей.

2) По доверенным каналам. Двум пользователям A и B известен открытый ключ *RSA* пользователя C, и этот пользователь поддерживает обмен ключами, то оба этих пользователя могут передать свои ключи через пользователя C.

3) По не доверенным каналам с использованием общей секретной информации. Такая информация может использоваться для стеганографических текстов или обмена по протоколу обмена ключей *Diffie-Hellman*. Система, знающая секретную информацию, сможет расшифровать ключ *RSA* из такого сообщения.

4) По не доверенным каналам с использованием медиа-контента. Данный механизм удобен только в том случае, если процесс обмена происходит за достаточно короткое время, за которое возможный человек посередине не успеет подделать эту информацию. Может быть использована визуальная информация, такая как фото или видео, или аудиозапись голоса пользователя. В таком случае ответственность за распознавание ключа лежит на пользователе.

Обмен симметричными ключами для обмена данными происходит после успешного обмена публичными ключами *RSA*. Зашифрованный по алгоритму шифрования *RSA* симметричный ключ посылается как системное сообщение.

2.4. Авторизация и профилирование

Данные о пользователе, которые ранее сохранялись с Сети, теперь хранятся локально у владельца учетной записи. Профиль зашифрован симметричным шифрованием AES с пользовательской длиной ключа. Данные о пользователе включают в себя контактный лист пользователя и других известных ему людей, доступные данные об этих людях, их открытые ключи RSA и все ключи переговоров AES. Пользователь может выбрать, какие данные будут доступны для всех – для пользователей Социальной Сети и системы, а какие данные могут быть доступны только для пользователей системы. Таким образом может быть создан контроль доступа к профильным данным как для каждого отдельного пользователя, так и для различных групп пользователей по различным критериям одновременно.

2.5. Users interactions: peer-to-peer data exchange based on TOR Network

Для безопасного обмена данными через небезопасную сеть (по причинам, описанным в пункте 2.1) использована модификация анонимной гибридной сети *TOR* [11]. Чтобы начать работу в сети, необходимо знать *ID* и публичный *RSA* ключ хотя бы одного уже существующего пользователя этой защищенной сети. Также для общения друг с другом, обеим сторонам необходимо договорится об общем *AES* ключе их беседы. (см.

2.3.). Для начала передачи данных используется *Onion Routing* – передача данных через посредников. Как и *TOR*, эффективность работы данной сети напрямую зависит от количества ее пользователей. [11]

Используются следующие **Системные сообщения** для поддержания работы системы:

1) *GET_KEY* (*user ID*) – главное сообщение

2) *GET_PROFILE* – сообщение-запрос на данные о профиле от принимающей стороны.

3) *GET_OPTIONS* (тип опций) – сообщение-запрос о возможностях, которые предоставляет принимающая это сообщение сторона: перенаправление сообщения, задержка сообщения, средняя пропускная способность и т.д.

4) *OP_RESULT* (тип сообщения) (возвращаемый код) [дополнительные данные] – ответ на любое из вышеперечисленных сообщений.

2.6. Message structure

Чтобы обеспечить безопасную передачу между пользователями сети, используется механизм луковичной и чесночной передачи данных, которые были разработаны в анонимных сетях TOR и I2P соответственно. Главная цель этих алгоритмов – скрыть реального получателя и отправителя сообщения. В луковичной передачи сообщение шифруется текущим ключем шифрования и к этому сообщению к началу добавляется системная информация, зашифрованная алгоритмом RSA. Если в сети находятся свободные и доступные для перенаправления сообщения пользователи сети, то сообщение будет перенаправлено несколькими из этих пользователей, выбранных случайным образом. В таком случае сообщение инкапсулируется в другое как обычное сообщение по описанному выше алгоритму столько раз, сколько на пути сообщения встречается перенаправляющих точек. Каждая перенаправляющая точка расшифровывает только свою часть сообщения, в котором будет указан следующий получатель сообщения. Процесс продолжается до тех пор, пока не дойдет до получателя сообщения. Луковичны алгоритм схож с данным, за исключением того, что оперирует несколькими сообщениями одновременно. Иллюстрация луковичной передачи приведена для трех перенаправляющих точек:

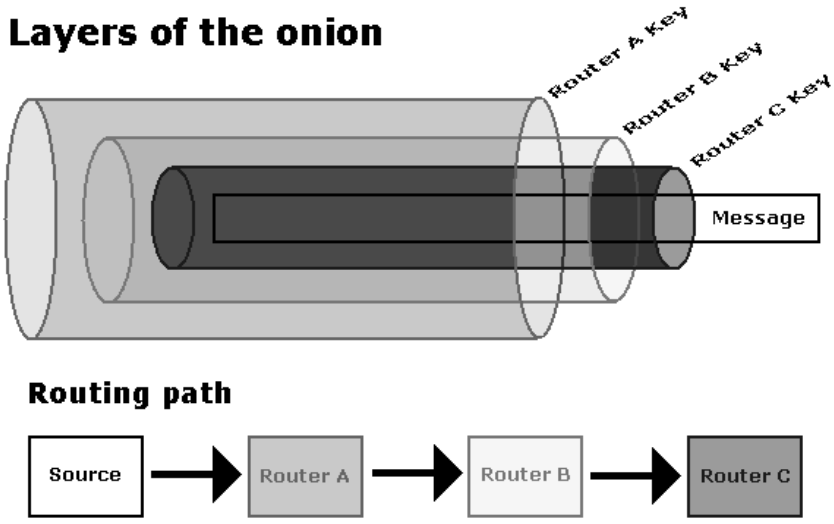

Рис. 1. Диаграмма луковичного сообщения

RSA Encrypted	*AES Encrypted*
MSG_FLGS [2 bytes]	User data
MSG_DEST [4 bytes]	
MSG_SRC [4 bytes]	
MSG_SIZE [4 bytes]	

Рис. 2. Структура луковичного сообщения

MSG_FLGS – системные флаги. Используются для укзаания типа шифрования, вознможности задержки сообщения, чесночной передачи данных и т.д.

MSG_DEST – получатель сообщения.

MSG_SRC – отправитель сообщения.

MSG_SIZE – размер сообщения. Это поле используется в ситуациях, когда к концу сообщения добавлена криптографическая соль, или если это сообщение содержит еще одно или несколько сообщений (чесночная передача данных)

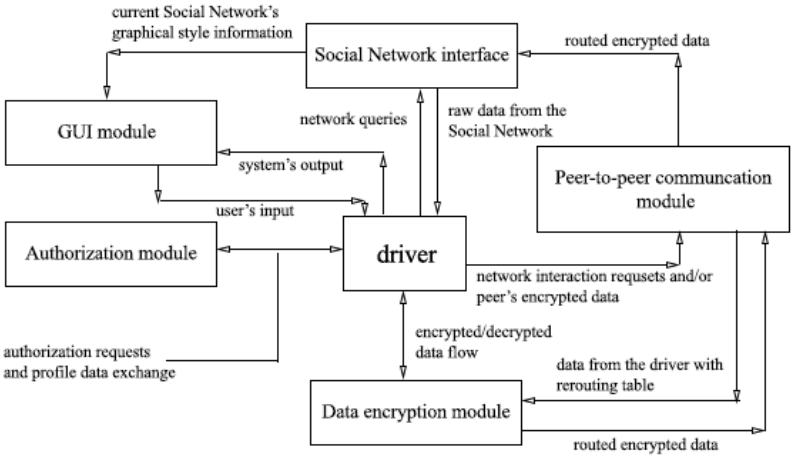

Рис. 3. Взаимодействие модулей. Raw data («Сырые» данные) – необработанные данные, которые были получены или отправлены из/в Социальную сеть

3. Реализация

Форма веб-плагина в качестве реализации этой системы была рассмотрена в качестве наиболее подходящей, так как такая реализиация позволяет экономить время и усилия и сконцентровать их только на разработку всех особенностей программы. Mozilla Firefox был выбран в качестве браузера, для которого реализовывается данная система по трем причинам:

1) Браузер Mozilla Firefox – популярный браузер, которым пользуются более 100 миллионов пользователей.

2) Дополнения к Mozilla Firefox используют язык Javascript – ООП язык и поддерживаемых практически во всех современных браузерах.

3) Mozilla Firefox предлагает стабильный и удобный SDK для разработки собственных плагинов к браузеру с детальной документацией и примерами реализации.

3.1. Текущая реализация

Текущая реализация еще до сих пор на стадии разработки. На данный момент реализована лишь небольшая часть спецификации системы, описанной в этой работе. Главная проблема в размере работы и в осознанном избегании любых *API*, которые предоставляют Социальные Сети. Текущая стабильная весрия веб-плагина поддерживает защиту приватных сообщений в Социальной Сети «Вконтакте» - широко известной Социальной Сети в странах СНГ. Обладая небольшим функционалом, он уже способен защищать обмен информацией между пользователями:

Рис. 4. Encrypted messages with the plug-in activated

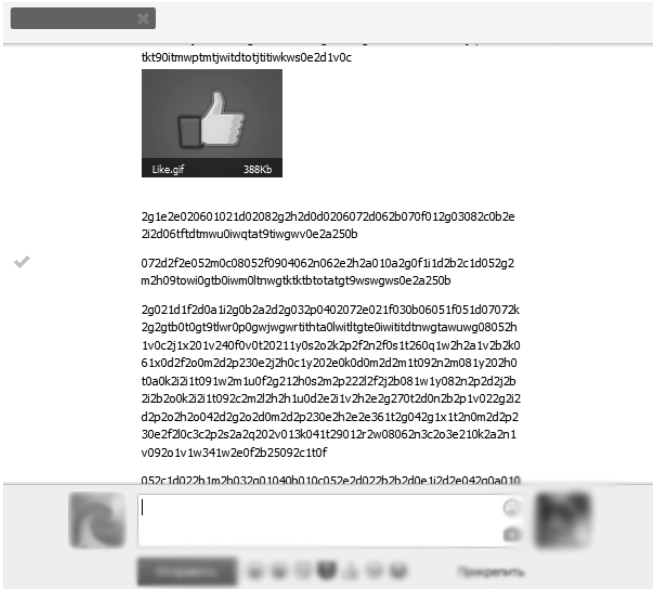

Рис. 5. Encrypted messages with the plug-in deactivated

Исходный код веб-плагина можно найти здесь:
https://github.com/FakeEmperor/social_network_secure
Стабильная версия плагина на данный момент:
https://addons.mozilla.org/ru/firefox/addon/ssn_project/

3.2. Future realization features

Although, as it was stated, current realization is a little part from the designed project, and is available only for Firefox users, it is coded on a cross-platform and cross-browser programming language and can be easily ported on other browsers, and even developed as a

standalone application. Future updates will include more features to fulfill the tasks stated in this paper:

Несмотря на то, что, как уже было сказано, текущая реализация имплементирует малую часть описанной системы, и может быть доступна только для пользователей браузера Mozilla Firefox, ее исходный код был написан на кроссплатформенном языке, что позволяет легко адаптировать код под другие браузеры и даже разработать самостоятельное приложение. Следующие обновления призваны сократить разрыв до минимума между текущей спецификацией системы и ее реализацией.

1. В данный момент разрабатывается

- Имплементация луковичной и чесночной передачи данных.
- Защита данных профиля: локальная копия данных профиля.
- Больше различных видов защиты данных: данные в группах и сообществах в Социальных сетях, шифрование медиа-данных, шифрование комментариев и других видов обмена данными.
- Поддержка новых социальных сетей: *Google+* и *Facebook*

2. Будущие нововведения

- Стеганография
- Защищенные файловые потоки и внедрение VoIP-потоков
- Поддержка мобильных платформ: Android, iOS, Windows Mobile.
- Расширения и веб-плагины для других браузеров: Google Chrome, Opera.

4. Заключение

Проблема защиты персональных данных в Социальных Сетях – большая и не прекращающая расти проблема для любого пользователя Сети. В данной работе описан один из методов защиты этих данных и права на тайну личной переписки. В то же время, описанный подход максимально просто для управления пользователем и насколько это возможно, минимизирует нагрузку на него, тем самым практически не изменяя его поведение в сети. Хотя на данный момент описанный подход еще не до конца реализован, текущая реализация уже может быть использована для защиты персональных данных.

Список литературы

1. Smith A., Brenner J. 72% of Online Adults are Social Networking Site Users. Available at: http://pewinternet.org/~/media//Files/Reports/2013/PIP_Social_networking_sites_update_PDF.pdf, accessed 21.01.2014.

2. Internet Usage Statistics. Available at: http://www.internetworldstats.com/stats.htm, accessed 21.01.2014.
3. 2 million stolen login credentials discovered for Facebook, Google, LinkedIn, Twitter, other sites. Available at: http://www.csoonline.com/article/744185/2-million-stolen-login-credentials-discovered-for-facebook-google-linkedin-twitter-other-sites, accessed 21.01.2014.
4. Privacy Suit Against Facebook a warning for business. Available at: http://www.csoonline.com/article/745293/privacy-suit-against-facebook-a-warning-for-businesses, accessed 21.01.2014.
5. U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. Available at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, accessed 22.01.2014.
6. Study finds online privacy concerns on the rise. Available at: http://news.yahoo.com/study-finds-online-privacy-concerns-rise-040211677.html, accessed 22.01.2014.
7. CNN's Twitter, Facebook Hacked by Syrian Electronic Army. Available at: http://www.webpronews.com/cnns-twitter-facebook-hacked-by-syrian-electronic-army-2014-01, accessed 22.01.2014.
8. Facebook Facing $138,000 Fine for Holding Deleted User Data. Available at: http://mashable.com/2011/10/21/facebook-deleted-data-fine/, accessed 22.01.2014.
9. Касперский Е. Соцсети сыграли решающую роль в похищении сына. Режим доступа: http://www.rg.ru/2011/05/18/kasperskii-site-anons.html, accessed 22.01.2014.
10. Anonymous Facebook Employee: Everything You Do Is Tracked And Stored Forever. Available at: http://www.informationliberation.com/?id=28581, accessed 22.01.2014.
11. Dingledine R., Mathewson N., Syverson P. Tor: The Second-Generation Onion Router. Available at: https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf accessed 22.01.2014.
12. Committee on National Security Systems (System Security for the 21st Century). Available at: http://cryptome.org/aes-natsec.htm, accessed 22.01.2014.
13. Dates for Phasing out MD5-based signatures and 1024-bit moduli. Available at: https://wiki.mozilla.org/CA:MD5and1024, accessed 22.01.2014.