БЕЗОПАСНЫЕ СПОСОБЫ ОБЩЕНИЯ В СЕТИ

Переходим к самой печальной части нашего рассказа. Хотя почти для каждого типа онлайнкоммуникаций есть защищенные решения, для их применения придется убедить твоего собеседника в том, что «так нужно». Как подсказывает опыт фанатов Jabber, сделать это без вмешательства крупных компаний невозможно. Поэтому данный обзор несет скорее футуристический характер — если все это найдет спрос, возможно, кто-нибудь когда-нибудь научится на этом зарабатывать.

ЗАЩИЩЕННЫЕ СООБЩЕНИЯ

Для пересылки защищенных сообщений разработан криптографический протокол OTR (Off-the-Record). Для создания сильного шифрования протокол использует комбинацию алгоритмов AES, симметричного ключа, алгоритма Диффи — Хеллмана и хеш-функции SHA-1.

Основное преимущество OTR перед другими средствами шифрования — это его применение на лету, а не после подготовки и оправления сообщения. Он был разработан Никитой Борисовым и Яном Голдбергом. Для использования в сторонних приложениях разработчики протокола создали клиентскую либу. Поэтому, чтобы защитить передачу данных по IM-каналам, можно воспользоваться специально предназначенными для защиты приложениями.

Один из подобных проектов — Cryptocat; это веб-аппликация с открытым исходным кодом, написанная на JS. Имеются расширения для Chrome, Firefox и Safari. Кроме того, есть клиентское приложение, но только для OS X. Криптокат шифрует сообщения на клиенте и передает их доверенному серверу. Для этого на стороне клиента используется симметричное шифрование сообщений и файлов с использованием AES-256 и выбранного ключа. Для каждого чата генерируется новый ключ.

Другие участники разговора — до десяти человек в комнате — смогут прочитать их, только если сами правильно введут тот же самый ключ. Для надежной передачи ключей используется алгоритм Диффи — Хеллмана, для генерации уникальных отпечатков при аутентификации — хеш-функция Whirlpool, а для проверки целостности сообщений — HMAC-WHIRLPOOL. Метод работы с ключами превращает Cryptocat в систему совершенной прямой секретности, в которой даже потеря закрытого ключа не может скомпрометировать ключ сессии. Лог переписки удаляется через 30 минут отсутствия активности, а сам сервис работает с постоянным SSL-шифрованием.

Еще один проект подобного рода — Bitmessage, написанный Джонатаном Уорреном на питоне. Bitmessage — это децентрализованная P2P-программа для обмена зашифрованными сообщениями между двумя и/или несколькими юзерами. Она использует сильную криптографию, которая надежно защищает абонентов от прослушивания на уровне интернет-провайдера или на сервере. Стоит заметить, что криптографическая система практически в точности копирует схему, которая используется в P2P-системе Bitcoin, однако направлена на обмен сообщениями. Особенность Bitmessage состоит в том, что факт общения двух пользователей практически невозможно доказать: сообщение передается не напрямую от пользователя А к Б, а рассылкой всем участникам сети (подобный подход реализован в Tor). При этом прочитать его может только тот пользователь, с которым установлено соединение и который обладает корректным ключом для расшифровки.

Последним проектом этого ряда, который мы рассмотрим, будет TorChat. Сеть TorChat представляет собой свободную

децентрализованную высокоанонимную криптозащищенную систему обмена мгновенными сообщениями и файлами. Весь код открыт, а следовательно, проверяем. TorChat в основе своей использует анонимную сеть Tor, но это полностью обособленный проект. Анонимность передачи данных целиком возлагается на скрытые сервисы Tor, TorChat, по сути, лишь надстройка к ним, занимающаяся обработкой сообщений. Криптозащита соединения двух пользователей также обеспечивается скрытыми сервисами Tor посредством асимметричного шифрования по стандарту RSA. Изначально TorChat был написан на питоне, клиент для OS X, соответственно, на Objective C. В начале 2012 года был запущен проект jTorChat, разрабатываемый на Java. Пока в нем не реализована вся функциональность оригинального TorChar, к примеру отсутствует передача файлов.

INFO

Хотя на мобильных устройствах можно использовать веб-интерфейсы рассмотренных мессенджеров, в разработке находится средство обмена мгновенными сообщениями,

специально заточенное под мобилы (https://heml.is).

t₮ŞŘŖŨţŖŵ t₮ŭŨŖ

Широкую известность получило самозакрытие почтового сервиса lavabit.com, которым воспользовался Сноуден. Сервис был закрыт после того, как спецслужбы предъявили требования предоставить доступ к хранимым данным.

Полную альтернативу Lavabit найти сложно (кроме self-hosted решений), но в качестве более-менее защищенного сервиса можно предложить VFEmail (https://vfemail.net). Он сканирует каждое пришедшее письмо и его вложения в поисках вирусов и спама. Если была обнаружена малварь, письмо блокируется на шлюзе и не попадает на сервер. Почтовый сервер поддерживает серые и черные списки, а для определения спама используется заслужившая признание система SpamAssassin. Работа с VFEmail идет посредством стандартных протоколов POP, IMAP, SMTP, а веб-интерфейс реализован по защищенному SSL-каналу. Как и большинство современных почтовых служб, VFEmail поддерживает открытие в браузере Microsoft Office документов. Однако за полученную секретность переписки приходится платить. Правда, есть бесплатный, так называемый «медный аккаунт», предоставляющий пользователю 50 Мб серверного пространства для писем. Для увеличения места надо купить другой, более совершенный аккаунт.

СОЦИАЛЬНЫЕ СЕТИ

Вообще, соцсети слабо вяжутся с концепцией анонимности и приватности переписки. Эти сервисы стали источником информации о лицах всех возрастов: люди пишут в соцсети все о себе, своих близких и друзьях, выкладывают жизненные фото и видео. Можно ограничить доступ к этим сведениям, но это не преграда для спецслужб — известны случаи, когда по запросу властей им передавались интересующие их данные о пользователях. Безусловно, соцсети — зло! Но иногда хочется поделиться чем-то с родными или рассказать о достижении близким друзьям. Поэтому даже соцсети играют положительную роль.

Чтобы защитить свои приватные данные от посторонних глаз, можно воспользоваться свободными защищенными аналогами. У них, конечно, гораздо меньше юзеров — 15-летних школьниц, фоткающихся с айфонами, но тем лучше. И чем больше пользователей будут понимать значимость приватности информации, а к этому все идет, тем большее их число будет переходить в защищенные соцсети.

Одна из таких сетей — Friendica (friendica.com). Проект был начат в 2011 году Майком Макгривином. Friendica — свободная социальная сеть с открытым исходным кодом, дислоцирующимся на GitHub. Она предоставляет широкий выбор коннекторов для разнообразных социальных сетей: как традиционных (Facebook, Twitter), так и новых (Diaspora, Identi.ca). Кроме того, с помощью Friendica

Friendica — страшненькая, зато свободная

ГОЛОСОВОЙ И ВИДЕОЧАТ

С мгновенными текстовыми сообщениями мы анонимны, а что насчет голосового и видеообщения? Skype принадлежит Microsoft, а она (по документам Сноудена) была уличена в передаче сведений спецслужбам.

Поэтому нужны другие варианты. Одним из них стал проект Tox (tox.im) — открытая и свободная альтернатива Skype. Он использует похожую на Skype P2P модель организации взаимодействия в сети для распространения сообщений, использующую криптографические методы для идентификации пользователя и защиты транзитного трафика от перехвата. Поддерживается обмен текстовыми сообщениями, голосовая связь, видеозвонки и передача файлов. Работа организована через простой и типичный для IM-клиентов графический интерфейс.

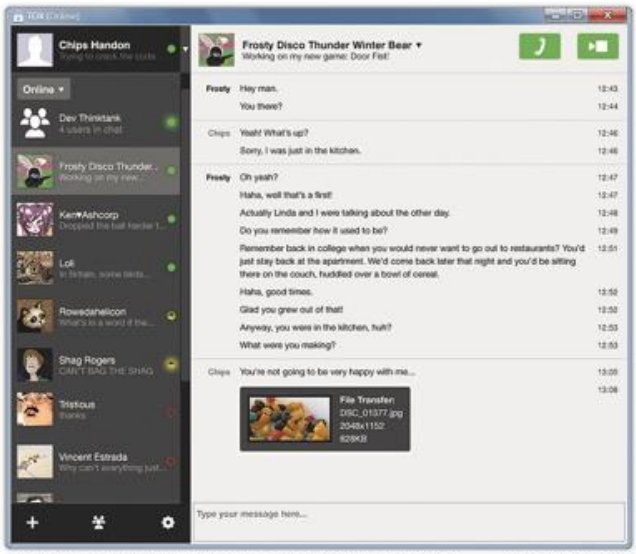
Одна из ключевых задач проекта — обеспечить приватность и тайну переписки, в том числе защиту от возможного анализа трафика. Для обеспечения адресации пользователей используется распределенная хеш-таблица (DHT), работа с которой организована в стиле BitTorrent. Канал связи организуется при помощи надстройки над протоколом UDP с реализацией сеансового уровня (Lossless UDP).

Мобильный мессенджер Hemlis

Для идентификации каждого пользователя используется специальный публичный ключ, который также применяется как открытый ключ для шифрования. Отдельно генерируется закрытый ключ для расшифровки сообщений, зашифрованных с использованием идентификатора / открытого ключа. Для организации коммуникаций требуется соединение к пиру (каждый клиент сети является пиром), который может быть определен вручную или найден автоматически (доступна функция поиска пиров в локальной сети).

Код Tox написан на языке Си и распространяется под лицензией GPLv3. Поддерживаются платформы Linux, Windows и OS X. Для организации шифрования используется библиотека libsodium. Функциональность разработки пока находится на уровне серии тестовых прототипов, консольного клиента, написанного с использованием библиотеки ncurses, и графического клиента на базе Qt5.

Кроме того, в GNU создается альтернатива под названием GNU Free Call. Этот проект нацелен на разработку и внедрение по всему миру безопасных и самоорганизующихся коммуникационных сервисов. В качестве базового протокола в GNU Free Call будет использоваться SIP, поддержка которого обеспечена при помощи VoIP-сервера GNU SIP Witch. Коммуникационная



Tox — открытый аналог Skype

сеть построена с использованием P2P-технологий и имеет топологию mesh-сети, в которой каждая клиентская точка сети связана через соседние клиентские точки. Конечной целью проекта является формирование VoIP-сети, напоминающей Skype по возможностям и удобству использования.

С технической стороны для реализации проекта в GNU SIP Witch, кроме функции маршрутизации SIP-звонков, будет обеспечена поддержка работы в роли защищенного VoIP-прокси, добавлена возможность хранения кеша хостов и выполнения функций обмена маршрутами с соседними узлами mesh-сети. Поддержка VoIP-прокси позволит упростить построение пользовательских интерфейсов и создание приложений для мобильных устройств, поскольку обеспечит поддержку приема и выполнения звонков с любых SIP-совместимых программных телефонов.

Ударяться в панику из-за слежки не имеет смысла. Есть защищенные решения всех привычных служб: электронной почты, мгновенных сообщений, голосового/видеочата, соцсетей

Клиентское ПО для работы всети GNU Free Call будет поддерживать широкий спектр разнообразных программных платформ. Сеть будет иметь полностью децентрализованную структуру, не привязанную к отдельным управляющим серверам.

ИТОГИ

Как видишь, ударяться в панику из-за тотальной слежки не имеет никакого смысла. Существуют защищенные решения всех привычных служб: электронной почты, мгновенных сообщений, голосового/видеочата, соцсетей. Если воспользоваться ими, то никакой Большой Брат (или скромная спецслужба) не залезет в твои дела. Никто не в состоянии остановить распространение информации в интернете!

Используй все возможности Сети в своих целях!

Diaspora выглядит уже получше

можно обмениваться письмами и читать RSS-ленты. Если в Friendica сделать фото закрытым, то оно на самом деле будет в привате и никто (кроме, естественно, владельца и избранных им лиц) не сможет получить к нему доступ.

В настоящее время идет разработка следующей версии соцсети под названием Red (что с испанского означает «сеть»). По словам авторов, во время разработки Friendica были осознаны детали и обкатаны механизмы разработки соцсетей, поэтому следующий проект станет еще лучше и будет избавлен от фундаментальных недостатков первой версии.

Еще одна защищенная социальная сеть, на которую мы обратим внимание, — это Diaspora (https://joindiaspora.com). Данная сеть базируется на трех принципах. В отличие от традиционных соцсетей, где данные хранятся в одном дата-центре, то бишь централизованно, в Diaspora, как и во многих защищенных в вебе продуктах, данные хранятся децентрализовано. В этом случае данные хранятся не на центральном сервере, а на подах (pod) — компьютерах тех пользователей, кто предоставил их для этой цели. Второй принцип, конечно же, свобода, кто мог сомневаться? Третий принцип — секретность. Никто, кроме тебя, не имеет доступа к твоим данным, а кто может их просматривать, определяешь ты сам, устанавливая разрешения. И они действуют глобально, то есть никто их не нарушит.