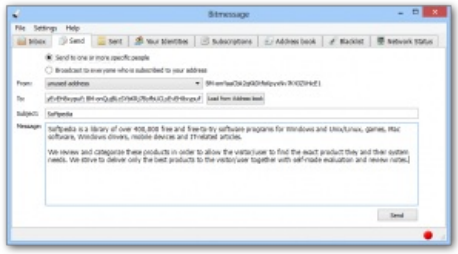
Bitmessage — Urbanculture

Криптоконспирология

Bitmessage — криптографическая программа для обмена текстовыми сообщениями, использующая распределенную P2P-сеть. Написана на языке Python. Имеет открытый исходный код. Адреса Bitmessage представляют собой случайный набор символов, с префиксом BM-. Реализована поддержка многопользовательских конференций. Программа пока является beta-версией, последняя версия 0.4.4.

Логотип BM

Как это работает?



Пользовательский интерфейс

У каждого пользователя и у каждой конференции есть адрес и пара ключей. При отправке сообщения пользователь шифрует содержимое ключом получателя или конференции, затем сообщение распространяется среди всех участников p2p-сети. Те, кто имеет соответствующий секретный ключ могут расшифровать содержимое, остальные просто хранят его и передают другим участникам сети. По умолчанию каждый хранит сообщения в течении 2 дней с момента его получения. В настройках можно отрегулировать время хранения сообщений и насколько старые сообщения можно получать. Для защиты от спама перед отправкой каждый клиент должен проделать определенную вычислительную работу, прежде чем сообщение отправится в сеть, то есть массовая рассылка будет достаточно медленной. В настройках клиента можно указать объем вычислений в относительной форме, который необходим для получения вами сообщения, либо для длинного, либо короткого.

Чаны или каналы

Многопользовательские конференции — чаны или каналы — имеют общий ключ для нескольких пользователей. То есть отправленное в чан будет получено и расшифровано всеми его участниками. Основной идентификатор чана — его имя, то есть зная только имя можно стать участником. Модерация чанов невозможна, т.к. все участники имеют равные права, никто не может прекратить распространение сообщений от определенного участника или остановить распространение конкретного сообщения. Адрес чана будет являться личным адресом каждого из его участников, то есть в в конференцию можно отправлять сообщения от имени конференции. Таким образом достигается дополнительная анонимность. Анонимность не является обязательной, то есть отправителем может стать и лично пользователь. Для этого в поле «от» можно выбрать свой адрес. Свои каналы есть у некоторых популярных сервисов, таких как 2ch.hk, 2ch.ru (ныне навеки усопшиего), habr, hiddenchan, vestichan (редакция газеты «Вестник I2P»), aibchan. Также есть множество национальных и тематических каналов. Список активных каналов периодически рассылается по подписке.

Проблема имен

Использование хэшей в качестве имен создает проблему запоминания и обмена адресами. В программе есть возможность интеграции с namecoin, для создания удобочитаемого имени, которая не получила поддержки пользователей. Тратить драгоценную криптовалюту для шифропанка есть на что помимо имени в BM. Разработчики не предпринимают каких-либо действий по решению данной проблемы. Но большинство тех, кто пользуется, данная ситуация устраивает.

Передача нетекстового контента

Работа с изображениями и документами в системе не поддерживается. Есть возможность отображать html-версию сообщения, то есть можно использовать картинки, закодированные с помощью base64 с `<img>`. При этом объем изображения увеличивается на 20-30%, объем вычислительной работы для шифрования и отправки становится значительным. Практически воскрес из мертвых uue-формат данных, который использовался в этом вашем фидо, но опять же используется редко и единицами из тех единиц, которые сидят в конференциях.

Анонимность

Анонимность — один из ключевых вопросов для такого рода приложений. Сервис не требует дополнительных данных для регистрации, генерировать адреса может каждый клиент самостоятельно. Для обеспечения дополнительной безопасности есть поле настроек прокси, сервис отлично работает через Tor. IP-адрес каждой ноды публичный, то есть его будут знать все, кто установил соединение с ней.

Получить информацию о пересылаемом содержимом можно только имея секретный ключ получателя, то есть сервис достаточно анонимен. Разработчики рекомендуют периодически менять личные адреса и не использовать один и тот же адрес для переписки с реальными и виртуальными знакомыми.

Атмосфера конференций

Зависит исключительно от тематики конференции и сайта, который ее породил. Так конференции посетителей имиджборд скатываются к типичным для двача оскорблениям, конференции мигрировавших пользователей скрытосетей являют миру пример вежливости и недоверия. А так ничего нового, это интернет — тут могут послать нахуй. При том абсолютно безнаказанно.

См. также

- Tor
- I2P
- RetroShare

Сссылки

- Официальный сайт программы

Примечания