Критика заблуждения о маршрутизации Briar

Арс Либрев 05.10.2023

Уже довольно давно мне задавали вопрос в нашем чате Telegram о маршрутизации Briar. Является ли он на самом деле децентрализованным. При этом ссылались на эту заметку, где говорится, что, якобы, Briar, на самом деле использует маршрутизирующий сервер, а разработчики Briar, говоря о децентрализации, вводят пользователей в заблуждение. Поскольку мой ответ затерялся в чате, а та публикация может сбить с толку еще кого-то, я решил сделать полноценную заметку, изложив в ней то, что выяснил про Briar.

Для начала стоит заметить, то если бы данный мессенджер связывался через сервер, а не непосредственно между собеседниками, то не работала бы связь через Wi-Fi и Bluetooth, при отключенном доступе к Интернету. Однако она работает прекрасно.

То, что автор опуса, на который мне дали ссылку, назвал «маршрутизирующим сервером» никакой не сервер в том смысле, какой в это слово вкладывается при разговоре о серверных инструментах. Это специальное приложение Briar headless, которое выставляет REST API с интегрированным HTTP-сервером вместо традиционного пользовательского интерфейса. Об этом четко сказано на соответствующей странице документации. «Сервер» в данном случае, это не некий удаленный сервак, а часть приложения отвечающая за создание соединения. Этот http-сервер, если на то пошло, есть на любом компьютерном устройстве. То есть, это приложение, которое позволяет создавать методы обмена данными между пирами по протоколу HTTP. Принцип изложен, например, в этой статье. Поскольку статьи о REST API часто сосредотачиваются на взаимодействии клиентов с сервером, поясню, что его можно использовать и в случае, когда нет центрального сервера, - сервером выступает устройство с клиентом. На это указано в этой статье. Глубоко в нее не вникал, но суть понятна.

Автор опуса пишет, что разработчики Briar, назвали «маршрутизирующий сервер» пиром, чтобы запутать пользователей, и те не поняли, что речь идет о «сервере». На самом деле, если почитать документацию Briar, обнаруживается, что они все устройства с установленным приложением называют пирами. Если Вы установили себе на устройство Briar, то оно становится пиром - пиром распределенной сети Briar. Если же применить логику автора опуса, то оказывается, что у Briar нет пользователей - одни сервера.

Далее, если у Briar таки есть «маршрутизирующий сервер», то почему информация о нем не всплывает нигде в подробнейшем описании протокола работы Briar? Ни в быстром обзоре протокола. Ни в описании подключения между контактами. Ни в описании формата структурирования данных. Ни в описании подключения по QR. Ни в описании протокола ключей подключения. Ни в описании протокола обнаружения собеседников. Ни в протоколе безопасности транспортного слоя. Ни в протоколе синхронизации данных.

Серьезно, я потратил часы на чтение, вообще-то не шибко мне интересных, технических деталей и не обнаружил там никаких «серверов», хоть «маршрутизирующих», хоть еще каких. Да, там везде фигурируют пиры, - как я и сказал, разработчики так называют устройства с приложением Briar, участвующие в связи через него. Это совершенно ясно из контекста. Видно, что связь действительно осуществляется непосредственно между участниками.

Конечно можно включить конспирологию и предположить, что разработчики все написали специально не правильно, а настоящий протокол с использованием «сервера» держат в тайне. Но тогда не понятно, почему эти разработчики оставили страницу про этот самый «безголовый» сервер? Почему об этом инструменте подробно написано здесь. Почему допускают существование у них страниц с обсуждением его разработки и использования? Например, этой страницы. И этой. А еще этой. И еще этой. Зачем же так палить «сервер», существование которого так тщательно скрывается в документации о протоколах? Либо разработчики-заговорщики настолько невнимательны и непоследовательны, либо никакого «маршрутизирующего сервера» нет. Серьезно, нигде в приведенных обсуждения невозможно найти ничего, что указывало бы на то, что речь идет о выделенном сервере, через который идет переписка пользователей. Ясно, что речь идет про нечто, позволяющее создавать определенный интерфейс для взаимодействия участников сети. Обсуждаемый инструмент удобен, например, для создания ботов, о чем упомянуто здесь.

Можно было бы еще много чего накидать, но есть ли смысл? Домыслы, изложенные в крайне грубом виде, не стоят того времени, что потрачено на изучение материалов и самого этого опуса.

Под конец, еще раз скажу - если бы Briar не производил связь непосредственно между собеседниками, а делал это через сервер, была бы невозможна связь сугубо через Wi-Fi и Bluetooth при выключенном соединении с Интернетом. Однако она есть. Пусть тот кто верит в «сервер» Briar потрудится объяснить это. Благодарю всех, кто смог дочитать это до конца.