Анализ · 16 мая 2026 года

← Предыдущий·Следующий →

Когда никого нет посередине

Шифрование того, что проходит через сервер, защищает содержимое. Отсутствие сервера посередине избавляет от самого вопроса. Это не одно и то же.

Два человека, один разговор

Когда два человека разговаривают лицом к лицу в комнате, никто не обязан обещать, что ничего не слышал. Он не слышал, потому что его там не было. Когда два человека передают бумагу из рук в руки, никому посередине не нужно клясться, что он ее не читал. Посередине никого нет.

Большинство вещей в повседневной жизни работают именно так. Мы не подписываем соглашений о конфиденциальности с воздухом, который передает наш голос, или с бумагой, которую держим. Приватность разговора не зиждется на обещаниях посредника, потому что посредника нет. Это одна из самых сильных форм приватности: не потому, что кто-то или что-то ведет себя хорошо, а потому, что кого-то или чего-то просто нет.

Когда разговор переходит в цифровой канал, это по умолчанию меняется. Обычная модель такова: два человека подключаются к серверу, сервер получает сообщение, шифрует его или хранит зашифрованным и доставляет получателю. Сервер находится посередине. Сервер может быть честным. Он может проходить аудит. Он может работать в благоприятной юрисдикции и соблюдать строгую политику конфиденциальности. Все это может быть правдой. Но сервер находится посередине.

Разница между шифрованием и неиспользованием данных (часть вторая)

В предыдущей статье этой серии мы утверждали, что шифрование содержимого и неиспользование метаданных — это не одно и то же. Стоит четко сформулировать следующий шаг: шифрование того, что проходит через сервер, и отсутствие сервера — это также не одно и то же.

Первая модель — сервер посередине, зашифрованное содержимое — защищает содержимое от оператора сервера, его технического персонала, от внешнего злоумышленника, скомпрометировавшего систему. И это важно. Но это не устраняет сервер. Сервер все еще там. Он продолжает обрабатывать метаданные. Он остается точкой, которая может получить судебный запрос, законное вмешательство, политическое давление или пострадать от утечки данных. Он остается точкой, требующей доверия к кому-либо.

Вторая модель — отсутствие сервера между двумя концами — не защищает зашифрованное содержимое лучше: если криптография надежна, содержимое защищено в обоих случаях. Меняется не содержимое. Меняется то, что вопрос *«что происходит с сервером?»* теряет смысл, потому что нет сервера, о котором можно было бы спрашивать.

Доверие, отсутствие и разница между ними

Доверие может быть заслуженным. Честные компании существуют. Тщательные аудиторы существуют. Законы, защищающие пользователя, существуют. Серьезные сервисы, неукоснительно соблюдающие все вышеперечисленное, существуют. Доверие, когда оно оказывается достойному оператору, — это неплохая сделка.

Но доверие, каким бы прочным оно ни было, остается лишь доверием. Это социальное решение, а не техническое. Компания может сменить владельца. Юрисдикция может сменить правительство. Судебный приказ может прийти завтра. Новая уязвимость может быть обнаружена в следующем месяце. Ничего из этого не происходит по злому умыслу. Это происходит потому, что оператор существует, а всё существующее подвержено случайностям этого мира.

Отсутствие оператора не подвержено этим случайностям. Судебный приказ не может затребовать данные у сервера, которого нет. Злоумышленник не может скомпрометировать сервер, которого нет. Изменение в политике компании не может затронуть данные, которых у компании никогда не было. Ключевая фраза проста: данные, которых нет, нельзя потерять.

О легитимном аргументе серверной стороны

Тот, кто предлагает профессиональный сервис обмена сообщениями с сервером посередине, обычно выдвигает три вполне веских аргумента. Первый: сервер необходим для гарантии доставки, когда получатель не в сети. Второй: шифрование содержимого надежно, поэтому оператор не может его прочитать. Третий: сервис соответствует европейскому законодательству и данные защищены законом.

Все три аргумента верны. Ни один из них не меняет сути дела. Это правда, что сервер позволяет хранить сообщения для отложенной доставки; также правда, что отложенную доставку можно решить иначе, с помощью протоколов прямой связи между устройствами, совершенствуемых десятилетиями и работающих сегодня. Это правда, что шифрование содержимого при передаче надежно в серьезных сервисах. И правда, что европейское законодательство защищает пользователей больше, чем во многих других местах.

Вопрос не в том, легальны ли сервисы с сервером посередине, безопасны ли они или защищают ли они содержимое. Они могут быть такими, они легальны и обычно безопасны. Вопрос в том, что наличие сервера посередине — это архитектурный выбор, а не техническая необходимость. И каждый выбор имеет последствия. Архитектура с сервером посередине неизбежно создает субъекта, которому нужно доверять. Архитектура без сервера посередине — нет.

Что говорит закон и что делает архитектура

GDPR не требует конкретной архитектурной модели. Он требует результатов: минимизации данных, ограниченности целей, защиты данных на этапе проектирования и по умолчанию, способности продемонстрировать соответствие. Сервис с сервером посередине может соответствовать всем этим требованиям. Сервис без сервера посередине соответствует многим из них самой своей конструкцией, а не декларацией. Абсолютная минимизация — не собирать ничего, что не является строго необходимым для доставки сообщения — тривиальна, когда нет сервера, который мог бы что-то собрать.

Для повседневного нечувствительного использования серверная архитектура вполне разумна, а доверие к серьезному оператору — это допустимый вариант. Для других целей — тех, что подразумевают профессиональную тайну, деонтологическую ответственность, касаются особо чувствительной информации — отсутствие точки доверия является не роскошью, а структурным преимуществом.

Для профессионального читателя

К вопросам, которые стоит задать профессиональному сервису связи, уже знакомым по предыдущим статьям этой серии, добавляется еще один архитектурный вопрос:

1. Шифрует ли он содержимое при передаче? (Вероятно, да.)
2. Создает ли он и хранит ли метаданные о том, с кем и когда я общаюсь? (Вероятно, да.)
3. Есть ли сервер на пути между моим устройством и устройством получателя?
4. Если есть: кто им управляет, в какой юрисдикции и что должно произойти, чтобы он выдал данные обо мне?
5. Если нет: предыдущие вопросы теряют смысл.

Разница между этими двумя категориями — это разница не в степени, а в типе. Когда приходит время объяснить это клиенту, пациенту или коллеге, самая честная формулировка будет и самой простой: в одном случае кто-то есть посередине; в другом — нет.

Эта статья закрывает начальный цикл Cuadernos Lacre. Поговорив о шифровании, метаданных и профессиональной тайне, мы завершаем архитектурную картину: шифрование содержимого и отсутствие сервера посередине — это разные вещи. И то, и другое может быть законным; только одно устраняет необходимость в доверии.

Источники и дополнительная литература

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Основополагающий текст принципа, согласно которому гарантии системы должны быть реализованы на концах, а не в промежуточном канале.
- Регламент (ЕС) 2016/679, ст. 25 — защита данных на этапе проектирования и по умолчанию.
- Регламент (ЕС) 2016/679, ст. 5.1.c — принцип минимизации данных.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Главы об архитектурах, минимизирующих сбор данных самой своей конструкцией.

← ПредыдущийGDPR и профессиональный обмен сообщениями: почему большинство нарушает правила, не зная об этомСледующий →CUADERNOS_LIST_SCHREMS_TITLE

Недавние материалы

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Возьмите эту статью с собой туда, где она вам понадобится.

↓ Markdown ↓ Простой текст ↓ PDF

Файл будет загружен на ваше устройство. Оттуда вы можете сохранить его, импортировать в Solo2 или поделиться им где угодно. Cuadernos не решает место назначения за вас.

Сургучная печать · SHA-256 30f0b65b2157e1c39dee87e9b029d8268fe9b8347bf9c7e1854b203843e10ea4

Cuadernos Lacre · Издание Menzuri Gestión S.L. ·
текст R.Eugenio · под редакцией команды Solo2.