Принцип разделения: практическая основа конфиденциальности

Пол Шмитт
Гавайский университет / INVISV

Яна Айенгар
Быстро

Кристофер Вуд
Облачное сияние

Барат Рагхаван
ОСК / ИНВИСВ

АБСТРАКТНЫЙ

Трехдесятилетняя борьба за обеспечение конфиденциальности данных в Интернете — ключевого аспекта конфиденциальности коммуникаций — наконец-то позади. Шифрование является быстрым, безопасным и стандартным для всех браузеров, современных транспортных средств и основных протоколов. Тем не менее, долгое время казалось, что конфиденциальность сети не объединяется основными принципами, а представляет собой набор методов и идей, применимых к одинаково широкому спектру приложений, контекстов, уровней инфраструктуры и стеков программного обеспечения.

Здесь мы пытаемся изложить принцип (старый, но редко обсуждаемый как таковой) обеспечения конфиденциальности в интернет-сервисах. Мы исследуем, какие свойства конфиденциальности желательны и достижимы при применении этого принципа. Мы оцениваем несколько классических систем и систем, которые были недавно развернуты с применением этого принципа, и обсуждаем будущие направления обеспечения конфиденциальности сети на основе этих усилий.

КОНЦЕПЦИИ CCS

• Безопасность и конфиденциальность→Псевдонимность, анонимность и неотслеживаемость; Протоколы сохранения конфиденциальности;

КЛЮЧЕВЫЕ СЛОВА

Конфиденциальность в Интернете, анонимность, системная архитектура

Справочный формат ACM:
Пол Шмитт, Яна Айенгар, Кристофер Вуд и Барат Рагхаван. 2022. Принцип разделения: практическая основа конфиденциальности. В *21-й семинар ACM по актуальным темам в сетях (HotNets '22), 14–15 ноября 2022 г., Остин, Техас, США*.ACM, Нью-Йорк, Нью-Йорк, США, 8 страниц. https://дой.орг/10.1145/3563766.3564112

HotNets '22, 14–15 ноября 2022 г., Остин, Техас, США
 ISBN
ACM 978-1-4503-9899-22/2/11. . . 15 долларов США
https://doi.opr/10.1145/3563766.3564112

1 ВВЕДЕНИЕ

Впервые в истории человечества почти каждый человек находится под ежедневным наблюдением – наблюдением не вопреки, *а из-за*, достижения сетевого сообщества. Нарушения конфиденциальности — это многомиллиардная индустрия, которая уже некоторое время является основной бизнес-моделью Интернета [33, 40]. Людям необходима конфиденциальность в повседневной жизни, но конфиденциальность имеет значение не только для личности: общества прогрессируют, когда мы предотвращаем сдерживающие последствия тотальной слежки [15, 24, 25, 31, 34]. Индивидуальный *конфиденциальность*является синонимом организационного *безопасность*: в каждом случае участвующие стороны желают сохранить контроль над своими личными данными и метаданными.

К счастью, как практики, так и исследователи осознали необходимость, как минимум, конфиденциальности данных. TLS используется практически для всех типов связи в Интернете и используется по умолчанию во всех основных браузерах, современных протоколах, таких как QUIC [19, 22] и HTTP/3 [3], и многих других. Несмотря на успех TLS, интернет-коммуникации, тем не менее, сегодня контролируются более тщательно, чем когда-либо прежде, как в сети, так и на конечных точках. Хотя данные шифруются в процессе передачи, важные метаданные обычно просачиваются при передаче (например, IP-адреса, сообщения DNS и т. д.) и на конечных точках (сами конечные точки и их партнерские организации). В то время как на протяжении десятилетий исследовательское сообщество, наряду с многочисленными разрозненными развертываниями, пыталось решить проблему конфиденциальности метаданных связи, шаблоны многократного использования для решения этой проблемы явно отсутствуют в наборе инструментов разработчика протокола.

В этой статье мы обращаем внимание на то, что мы называем *Принцип развязки*. Идея проста, но ранее не была четко сформулирована: для обеспечения конфиденциальности информация должна быть разделена архитектурно и институционально так, чтобы каждая организация имела только ту информацию, которая ей необходима для выполнения соответствующих функций. Архитектурное разделение влечет за собой разделение функций для различных фундаментальных действий в системе, таких как отделение аутентификации (проверка того, кому разрешено использовать сеть) от подключения (установление состояния сеанса для связи). Институциональное разделение влечет за собой разделение оставшейся информации между субъектами, не участвующими в сговоре, такими как отдельные компании или сетевые операторы, или между пользователем и узлами сети. Такое разделение делает поставщиков услуг индивидуально защищенными от взлома, поскольку у каждого из них мало возможностей.

или никаких конфиденциальных данных, которые могут быть потеряны хакерами. Проще говоря, принцип разделения предполагает всегда разделять *кто ты* от *что вы делаете*.

Чаум был одним из первых, кто разработал протоколы и системы конфиденциальности таким образом в серии основополагающих статей [4–6]. Многие системы основаны на идеях Чаума, в том числе некоторые из самых популярных когда-либо созданных систем конфиденциальности, такие как Tor [13]. Однако из-за растущего давления с целью улучшения конфиденциальности в Интернете для конечных пользователей только в последнее десятилетие идеи Чаума начали получать широкое применение и признание.

Некоторые предшествующие подходы не учитывали принцип разделения. Например, VPN и промежуточные устройства переносят доверие с разрозненного набора конечных точек сети (например, веб-сайтов, которые может посещать пользователь, преобразователей DNS, которые может использовать пользователь, и т. д.) к одному доверенному посреднику (например, провайдеру VPN). В зависимости от модели угроз этот дизайн может решить проблемы конфиденциальности конечных пользователей, особенно если сеть еще более ненадежна. Однако здесь единственный доверенный посредник видит всю активность пользователя, связанную с его идентификационными данными, требует большего доверия, чем необходимо, и подвержен утечке данных. Этот шаблон не соответствует принципу разделения. Подобные примеры подтверждают идею о том, что развязка имеет основополагающее значение для конфиденциальности сети.

Далее мы обсудим некоторые общие цели конфиденциальности и способы их достижения, а затем рассмотрим многочисленные системы, предназначенные для достижения этих целей. Некоторые из них являются классическими разработками Чаума, а другие являются основой, на которой мы строим сегодня. Другие включают недавно развернутые коммерческие системы для достижения значимого (хотя и постепенного) повышения конфиденциальности в производственных сетях. Мы также рассматриваем некоторые ловушки, когда развязка либо игнорировалась, либо оказывалась недостаточной для решения проблемы. Наконец, мы обсудим ряд остающихся проблем в области конфиденциальности в Интернете.

2 ПРЕДВАРИТЕЛЬНЫЕ ПРЕДВАРИТЕЛЬНЫЕ ПРЕДСТАВЛЕНИЯ

2.1 Что такое конфиденциальность в Интернете?

Конфиденциальность означает свободу от наблюдения, и нигде это не является более важным, чем в Интернете, где мы должны полагаться на других в передаче нашего трафика. Поскольку конфиденциальность данных, к счастью, в значительной степени решена, проблемы конфиденциальности переместились в другое место: в метаданные трафика (а не в зашифрованные теперь полезные данные) и в конечные точки, где происходит обработка на уровне приложения. Кроме того, существует множество проблем конфиденциальности, связанных с обеспечением отсутствия связи между несколькими потоками трафика от одного пользователя/объекта (в сети) и несколькими идентификаторами (на конечных точках).

Проблемы конфиденциальности существуют во всем сетевом стеке, поэтому решения по обеспечению конфиденциальности также должны быть многоуровневыми. Например, шифрование трафика приложений может обеспечить конфиденциальность содержимого сообщения, однако непривилегированные наблюдатели нижних уровней (например, инфраструктуры IP-маршрутизации) могут легко отслеживать, кто с кем разговаривает. кого, записывая конечные точки IP. Системы, которые придерживаются принципа развязки, должны рассматривать конфиденциальность целостно и учитывать утечку информации через стек.

2.2 Аутентификация, авторизация и субъекты

Конфиденциальность важным образом взаимодействует с механизмами безопасности. Поскольку важность сетевой безопасности возросла, все больше систем полагаются на аутентификацию для подтверждения личности пользователя или устройства и авторизацию для подтверждения уровней доступа, которые должны быть предоставлены. Но аутентификация и авторизация, как в режиме реального времени, так и для последующего использования в судебно-медицинской экспертизе, часто создают неоспоримую запись о том, кто использовал сетевую службу, когда, как и даже почему. Участвующие субъекты одновременно децентрализованы (с использованием аутентификации и авторизации от наиболее важных для безопасности приложений до контекстов с низким уровнем риска) и централизованы (например, OAuth и SSO) с целью использования огромного спектра сервисов.

2.3 Доверие

Конфиденциальность зависит от доверия, которое пользователи должны оказывать интернет-системам, с которыми они взаимодействуют. Когда мы используем системы, мы отдаем нашу конфиденциальность в их руки. За последние 15 лет Интернет стал все более централизованным, при этом большая часть трафика приходится на горстку облачных провайдеров, CDN и поставщиков контента, которые считаются гипергигантами [21]. Например, количество ASN, необходимое для покрытия 50% интернет-трафика, сократилось со 150 в 2009 году [21] до всего лишь 5 в 2019 году [27, 38]. Эта тенденция привела к беспрецедентной централизации доверия и знаний о поведении пользователей в этих организациях. Такая централизация имеет некоторые преимущества для пользователей, поскольку крупные организации иногда способны эффективно защищать пользовательские данные, но это также сопряжено с определенными издержками и последствиями [23, 32].

Большинство сетевых протоколов предполагают сквозную координацию и, следовательно, сквозное доверие. В этом предположении заложена отдельная зависимость от механизмов аутентификации, которые гарантируют, что источник уверен в пункте назначения, с которым он взаимодействует (например, с использованием иерархии сертификатов или других внеполосных механизмов). Пользователи часто неявно или явно выносят суждения о том, следует ли раскрывать конкретную часть данных конкретной службе в определенном контексте, и это суждение требует бесчисленных факторов, которые может учитывать только пользователь. Ключевым моментом является то, что стороны, участвующие в общении, могут и должны иметь доступ к данным и метаданным, а их взаимное доверие к посредникам является ключевым вопросом, который мы рассматриваем в этой статье.

2.4 Принцип разделения

Ранее мы кратко сформулировали принцип разделения как *отделить то, кто ты есть, от того, что ты делаешь*. Чтобы сделать это более

конкретный, чтобы обеспечить возможность анализа, мы определяем▲как конфиденциальная информация пользователя*известный по*какая-то сущность и тому подобное△как неконфиденциальная личность пользователя, как конфиденциальные данные и⊙как неконфиденциальные данные.[1]Мы определяем кортежи из двух или более членов, обычно с одним или несколькими идентификаторами пользователя и одним или несколькими совокупностями пользовательских данных, где кортеж определяет знания некоторого объекта. Анализ разделения состоит из изучения сторон (независимых объектов или субъектов), участвующих в сетевой системе, которая взаимодействует с пользователем или его данными. Система отделена и, таким образом, получает выгоду от конфиденциальности, полученной за счет применения принципа разделения, если*только*пользователь (▲,).Другие объекты могут иметь не более одного из▲или , со всеми остальными записями кортежа как△или⊙.

3 СИСТЕМЫ

Теперь мы обсудим классические и новейшие системы, в которых используется принцип разделения. Мы также обсуждаем некоторые предостерегающие истории: системы, которые не используют принцип развязки и, следовательно, полагаются на доверие к третьей стороне для обеспечения конфиденциальности пользователей.[2]

3.1 Классические системы

*3.1.1 Доступ и аутентификация.*Основополагающей работой в системах анонимного доступа и аутентификации являются слепые подписи Чаума [4, 5]. При использовании слепых подписей содержимое сообщения скрыто перед его отправкой на подпись, обычно доверенным центром подписи. Поскольку сообщение скрыто, подписывающий орган не может получить доступ к содержимому сообщения, но подпись подписывающего органа позже может быть проверена третьей стороной, имеющей доступ к открытому содержимому. Слепые подписи обеспечивают несвязность, поскольку подписывающий орган не может связать сообщение, подписанное вслепую, с предыдущим взаимодействием, в результате которого было создано сообщение.

Слепые подписи представляют собой простой пример принципа разделения, поскольку они позволяют пользователям отделить свою личность от своих действий. В случае с цифровой валютой покупки участников не могут быть связаны с личностью. В этой схеме ни продавец, ни банк не могут знать личность покупателя, а просто знают, что представленные деньги действительны. Используя обозначения, введенные в разделе 2.4, анализ разделения для примера цифровой валюты выглядит следующим образом:

Покупатель	Подписывающая сторона (Банк)	Верификатор (Банк)	Продавец
(▲,)	(▲,⊙)	(△, ⊙/)	(△,)

В этом примере подписывающая сторона и проверяющая сторона являются одним и тем же объектом, но использование слепых подписей обеспечивает разделение посредством

[1]Конечно, в действительности невозможно четко классифицировать личность пользователя или данные как конфиденциальные или неконфиденциальные, особенно с учетом того, что объем и размерность рассматриваемых данных увеличиваются. На данный момент мы будем рассматривать их как общепонятные категории, к которым позже добавим оттенки серого.

[2]Мы называем их предостерегающими историями, а не неудачными системами, потому что они все еще могут быть полезны, но использование этих систем не может иметь отношения к реальности. да на архитектурный только свойства системы для обеспечения конфиденциальности аси я n моделей угроз пользователя без доверенных третьих лиц.

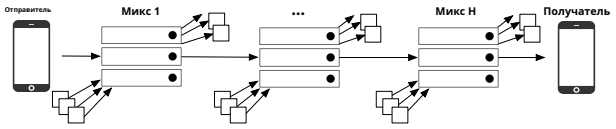

Рисунок 1. Разделение смешанной сети

обеспечение того, чтобы два действия и личность пользователя не могли быть связаны. Также возможно, но не обязательно, разделить подписывающую сторону и проверяющую сторону на две отдельные организации.

*3.1.2 Действующие лица.*Чаум также представил первую архитектуру анонимного общения через Интернет в своей классической статье о смешанных сетях [6]. Этот подход ввел понятие многоскачковой ретрансляции между взаимно несотрудничающими объектами. Перед отправкой сообщение шифруется с использованием открытого ключа микса. Микс расшифровывается с использованием закрытого ключа и пересылается получателю или другому миксу. Эта базовая схема показана на рисунке 1. Конструкция Чаума предотвратила атаки по времени с помощью пакетной пересылки. Микс-сети предлагают несколько форм конфиденциальности метаданных: 1) анонимность отправителя: получатель сообщения не знает личности отправителя; и 2) анонимность отправителя и получателя для сторонних наблюдателей: отправители и получатели могут обмениваться сообщениями, в то время как неглобальные наблюдатели не могут определить, что они оба и общаются друг с другом. Наблюдатели могут знать только то, что данный отправитель или получатель общаются с использованием смешанной сети.

Мик-сети позже были адаптированы Сиверсоном.*и другие.*для интернет-коммуникаций в реальном времени в их работе над луковой маршрутизацией [36], а затем улучшены в популярной системе Tor [13]. Эти системы обеспечивают конфиденциальность метаданных за счет разделения. Здесь идентификаторы (т. е. конечные точки отправителя и получателя) отделены от их поведения при общении (т. е. метаданных, окружающих сообщения или трафик), вплоть до пределов того, что возможно реконструировать или сделать вывод на основе анализа трафика и других побочных каналов. векторы атаки. Анализ развязки для микс-сетей выглядит следующим образом:

Отправитель	Микс 1	…	Микс N	Получатель
(▲,)	(▲,⊙)	…	(△, ⊙)	(△,)

3.2 Современные системы

3.2.1 Паспорт конфиденциальности.

Клиент	Эмитент	Источник
(▲,)	(▲,⊙)	(△,)

Интернет-пользователи, использующие системы повышения конфиденциальности, такие как Tor, часто сталкиваются со многими проблемами со стороны веб-сайтов, требующих доказать, что они являются законными пользователями, а не ботами. В идеале только пользователи lнапример imate клиенты могут успешно реагировать без даты о эти проблемы. К сожалению, такие проблемы часто нарушают конфиденциальность. ЛИ, например, им требуются файлы cookie автоматического он н- подсказки ИЛИ хранения на уровне приложения. Такие техники все ой

Рисунок 2. Отделение Privacy Pass

сервис для получения точной информации о клиенте или отслеживания его с течением времени.

Privacy Pass [11, 12] решает эту проблему, применяя принцип развязки для отделения аутентификации, чувствительной к конфиденциальности, от авторизации. В частности, клиенты, которым предлагается представить доказательства, отвечают с низкой достоверностью.*жетоны*произведено надежным эмитентом. Эмитент, в свою очередь, представляет токены только тем клиентам, которые могут успешно доказать свою легитимность. Это взаимодействие показано на рисунке 2. Таким образом, токены*передача*доверие со стороны эмитента, который узнает конфиденциальную информацию от клиента, но ничего об услуге (или происхождении)[3], сервису (или источнику), который изучает только неконфиденциальную информацию пользователя.

3.2.2 Незаметный DNS.

Клиент	резольвер	Забывчивый решатель	Источник
(▲,)	(▲,⊙)	(△, ⊙/)	(△,)

Почти всем подключениям к Интернету предшествует поиск DNS. Таким образом, рекурсивные преобразователи DNS, обычно управляемые интернет-провайдерами или поставщиками облачных услуг, могут привязывать поведение просмотра (DNS-запросы) к отдельным пользователям (IP-адресам и/или идентификаторам уровня приложения). Предыдущая работа показала, что DNS-трафик может выявить использование веб-сайта пользователями даже при подключении через Tor [16]. Чтобы уменьшить объем доступной информации в иерархии DNS, протоколы Oblivious DNS (ODNS [29] и ODoH [35]) применяют принцип развязки, разделяя знания между организациями.

Исходный протокол ODNS [29] шифрует и запутывает запросы, которые отправляются рекурсивному DNS-провайдеру пользователя. Затем запутанные запросы достигают ничего не подозревающего преобразователя — сервера, настроенного в качестве авторитетного сервера для запутанных запросов и хранящего ключи шифрования, необходимые для расшифровки исходного запроса. Затем этот сервер действует как рекурсивный преобразователь для запроса открытого текста. Конечным результатом является то, что обычный рекурсивный преобразователь пользователей может узнать личности пользователей (▲), но не может наблюдать за их DNS-запросами (⊙),в то время как забывчивый преобразователь может видеть запросы ( ), но не личности пользователей (△). Если рекурсивный преобразователь и забывчивый преобразователь управляются двумя организациями, не вступающими в сговор, конфиденциальность пользователей сохраняется.

Oblivious DNS over HTTPS (ODoH) [35] был вдохновлен ODNS и отделяет информацию о DNS-запросах с помощью Oblivious Proxy (рекурсивного преобразователя в ODNS) для обработки HTTP-запросов, содержащих зашифрованные DNS-запросы, которые отправляются в Oblivious Target (забывчивый преобразователь в ODNS), который является преобразователем DNS через HTTPS. Как и в случае с ODNS, конфиденциальность пользователей сохраняется до тех пор, пока Oblivious Proxy и Oblivious Target управляются организациями, не вступающими в сговор.

3.2.3 Довольно хорошая конфиденциальность телефона.

Пользователь	ПГПП-ГВ	НГК
(▲,▲,)	(▲,△,⊙)	(△,△,)

Pretty Good Phone Privacy (PGPP) [30] использует принцип развязки для достижения анонимности местоположения в сотовой архитектуре. Традиционно архитектура сотовой связи опирается на международный идентификатор мобильного абонента (IMSI), постоянный глобально уникальный идентификатор, который хранится на SIM-карте для функций выставления счетов и аутентификации, а также мобильности и подключения. Поскольку выставление счетов и аутентификация эффективно создают привязку между IMSI и личностью пользователя, их последующее использование и физическое перемещение можно легко отслеживать (и продавать [8, 9, 20, 39]) просто в результате работы сотовой сети.

PGPP отделяет выставление счетов и аутентификацию от ядра сотовой связи (NGC), изменяя его для использования протокола сверхзабывчивой аутентификации на внешнем сервере, PGPP-GW, которым может управлять вторая организация, оставляя при этом мобильность и функции связи в ядре, как они есть сегодня. Путем изменения выставления счетов (и человеческой личности пользователя)▲) и аутентификации, изменяются IMSI, которые мы обозначаем как неконфиденциальные сетевые идентификаторы.△ которые идентичны или периодически перемешиваются. Это гарантирует отсутствие связи с отдельными пользователями при их подключении и перемещении по сети.

Здесь разложение▲в▲ и▲ иллюстрирует, как различные компоненты пользовательских данных могут быть видны системным объектам и при этом могут анализироваться в нашей структуре.

3.2.4 Многостороннее реле.

Пользователь	Реле 1	Реле 2	Источник
(▲,)	(▲,⊙)	(△, ⊙/)	(△,)

В 2021 году Apple запустила сервис iCloud Private Relay [1], в котором используется прокси-архитектура, подобная классической микс-сети Чаума и последующим системам, таким как Tor; мы называем их услугами многосторонней ретрансляции (MPR). Private Relay отличается от предыдущих систем в двух ключевых аспектах: 1) использованием HTTP вместо пользовательских протоколов и 2) использованием хорошо подготовленной коммерческой сетевой инфраструктуры всего с двумя переходами, а не многопереходной добровольной сети децентрализованных узлов. Служба использует прокси-архитектуру с двумя вложенными туннелями HTTP CONNECT от клиента: первый к первому ретранслятору (управляется Apple), а второй через первый ко второму ретранслятору (управляется одним из трех независимых поставщиков инфраструктуры). Второй ретранслятор выдает соединение с исходным сервером от имени пользователя.

При использовании услуги MPR личность пользователя (его идентификатор сетевого уровня) известна Реле 1, но его запрос (данные)

[3]Мы используем*источники целевой серверили услуга*В этом документе термин взаимозаменяемо означает, например, веб-сервер, с которого клиент запрашивает контент.

неизвестно, поскольку оно скрыто в зашифрованном потоке. Реле 2 не знает о пользователе, кроме как об анонимном члене сетевой совокупности, но может узнать ограниченную информацию о запросе пользователя (например, полное доменное имя исходного сервера). Наконец, Origin узнает только о запросе пользователя.

3.2.5 Частная совокупная статистика.

Клиент	Агрегатор	Коллектор
(▲,)	(▲,⊙)	(△, ⊙)

Приложения, начиная от программной телеметрии и заканчивая отслеживанием и составлением отчетов об инфекционных заболеваниях, должны собирать статистические данные. Один из наивных подходов — отправлять входные данные на один (доверенный) сервер, который вычисляет агрегат. Однако это не является конфиденциальным, поскольку один сервер видит конфиденциальные данные клиента вместе с его личностью.

Один из подходов заключается в сокрытии конфиденциальной информации, идентифицирующей клиента, от сервера с помощью Oblivious HTTP, обобщения ODoH; клиенты будут отправлять зашифрованные отчеты на сервер сбора через прокси-сервер, тем самым отделяя сетевую идентичность клиента (IP-адрес) от его индивидуального вклада. Хотя это улучшает общее состояние конфиденциальности системы, оно по-прежнему раскрывает заинтересованным сторонам больше, чем необходимо. В частности, один сервер, действующий и как агрегатор, и как сборщик данных, видит все отдельные элементы данных.

Дальнейшее применение принципа развязки может улучшить ситуацию. В частности, измерение с сохранением конфиденциальности (PPM) [14] — это недавняя попытка IETF стандартизировать протоколы для частного вычисления совокупной статистики, а Prio [7] — один из конкретных примеров протокола PPM. PPM использует многосторонние вычисления между объектами, не участвующими в сговоре, для частного расчета совокупного результата. В этом случае только клиент видит конфиденциальные данные, тогда как другие стороны в системе видят только совокупные (неконфиденциальные) выходные данные, рассчитанные на основе многих входных данных клиента.

3.3 Поучительные истории

Клиент	VPN-сервер	Источник
(▲,)	(▲,)	(△,)

Помимо систем, которые имеют ключевые недостатки конфиденциальности (например, из-за отсутствия внимания к конфиденциальности), существует множество примеров систем, которые направлены на защиту конфиденциальности, но создают новые уязвимости и новые точки наблюдения. Такие системы часто не могут отделить конфиденциальную информацию и, таким образом, обеспечивают конфиденциальность только при условии доверия к какому-либо сетевому объекту.

Классические примеры включают централизованный VPN и службы обработки данных. Цели как VPN (например, защита «точка-точка» и периметра), так и служб безопасности (например, промежуточных устройств для предотвращения фишинга) часто отличаются от целей конфиденциальности, которые мы обсуждаем в этой статье. Тем не менее, направляя весь трафик через одну доверенную сторону, такие системы создают единый центр наблюдения.

TLS Encrypted ClientHello (ECH) [28] — еще один пример протокола, который не полностью реализует принцип развязки. С помощью ECH клиенты TLS шифруют конфиденциальную информацию при подтверждении связи TLS с сервером TLS, который завершает соединение. Это позволяет скрыть конфиденциальную информацию от ненадежной сети. Однако ECH не меняет информацию, которую видит сервер TLS.

4. ДИСКУССИЯ

В этом разделе обсуждаются фундаментальные предположения и соответствующие соображения, которые позволяют разумно применять принцип разделения на практике. Также обсуждается влияние принципа развязки на системы реального мира.

4.1 Отсутствие сговора

Системы, которые придерживаются принципа разделения, часто полагаются на предположение, что несколько организаций не будут вступать в сговор против пользователя. В этом случае активное соединение требует активного сговора между участниками. Конечно, идеальная конструкция системы не требует такого предположения. Однако на практике создание таких идеальных протоколов, повышающих конфиденциальность, затруднено, учитывая неявное доверие, присущее сложным вычислительным системам всех видов, — проблема, столь же старая, как классическая атака Томпсона (и, вероятно, намного старше) [37]. Все пользователи, даже самые искушенные, полагаются на услуги, предлагаемые относительно немногими, что обязательно дает этим службам возможность понять личность и поведение пользователей. Кроме того, практичные решения, которые можно сразу развернуть, могут обеспечить значительный рост конфиденциальности при несколько смягченном наборе требований к доверию. Конфиденциальность есть и останется движущейся целью. Таким образом, мы можем воспользоваться преимуществами постепенного улучшения конфиденциальности по мере их появления.

4.2 Степени разделения

Как показывает статистика Private Relay и Private Aggregate, *степень* информация, от которой отделена информация, может улучшить состояние конфиденциальности системы. Например, добавление большего количества ретрансляторов в Private Relay может улучшить защиту системы от атак по времени или сговора. Действительно, Tor воплощает этот подход, допуская схемы с 3 и более переходами, хотя и с более высокими затратами производительности. Аналогично, добавление большего количества агрегаторов в PPM может помочь в борьбе с атаками по сговору. На практике отделение в конечном итоге достигает точки, когда оно обеспечивает ограниченную отдачу от конфиденциальности за большие деньги. Добавление большего количества прыжков в Private Relay и агрегаторов в PPM увеличивает нагрузку на систему и в конечном итоге снижает производительность. В конечном счете, любая система, основанная на принципе разделения, должна учитывать компромисс между затратами и выгодами в отношении степени разделения.

4.3 Рекомендации по развертыванию

Хотя принцип развязки применяется в первую очередь к проектированию протоколов и архитектуре системы, его действие может быть ограничено практическими соображениями.

вопросы реализации. Например, рассмотрим атаки с анализом трафика в контексте смешанных систем, таких как Tor. Шифрование защищает конфиденциальность данных, но не защищает от других атрибутов данных приложения, таких как размер и временные метки данных во время передачи. Конкретные системы, такие как Tor, делают все возможное, чтобы смягчить эти типы атак, в том числе за счет использования пакетов постоянного размера и добавления дополнительных помех, чтобы усложнить анализ трафика на практике. Однако за подобные улучшения приходится платить, поскольку они снижают общую производительность системы и увеличивают сложность протокола. Подобные компромиссы хорошо известны в сфере технологий повышения конфиденциальности [10].

Современные процессоры и микросхемы безопасности обеспечивают аппаратную поддержку начальной загрузки доверенных сред выполнения (TEE). TEE позволяют пользователю безопасно и конфиденциально выполнять обработку от его имени на оборудовании, которым он не владеет и не контролирует напрямую. Обычно такое оборудование может криптографически подтвердить программное обеспечение, работающее в TEE (тем самым гарантируя подлинность программного обеспечения), гарантировать, что память и поток выполнения зашифрованы для чтения только TEE, и обеспечить некоторую степень защиты от несанкционированного доступа к локальным устройствам. и удаленные атаки. TEE перемещает локус доверия, в котором программное обеспечение работает, к производителю оборудования, неся в себе неявное обещание, что поставщик оборудования вряд ли нацелится на конкретного пользователя в неизвестном облаке, поскольку у него, вероятно, нет прямого стимула для этого. Таким образом, TEE являются разумным механизмом, обеспечивающим развязку на практике. Действительно, CACTI [26] — предотвращение CAPTCHA посредством интеграции TEE на стороне клиента — представляет собой систему, аналогичную Privacy Pass, которая использует TEE для целей сохранения конфиденциальности. Аналогично, Phoenix [17] использует TEE для реализации сервисов, подобных CDN (например, кэширования, межсетевых экранов веб-приложений и т. д.), при этом CDN не видит каких-либо конфиденциальных данных.

4.4 Регрессии в реальном мире

Развернутые в настоящее время системы часто требуют, чтобы метаданные пользователя функционировали правильно, и отделение личности пользователя от его действий может либо разрушить, либо разрушить эти системы. Например, системы потокового видео применяют DRM (управление цифровыми правами) на основе приблизительного местоположения пользователя путем определения IP-адреса пользователя, который запутывается в таких системах, как Private Relay. Чтобы эти системы могли продолжать работать правильно, некоторый объем пользовательских метаданных должен быть виден исходному серверу. Хотя обмен этими метаданными может осуществляться с сохранением конфиденциальности, как это делается в Private Relay, это нарушает принцип развязки.

В более широком смысле, системы, использующие принцип развязки, расширяют возможности пользователей и, следовательно, могут уменьшить контроль над объектами, которые ранее имели доступ к конфиденциальной информации. Однако контроль не всегда используется деструктивно; сетевые операторы часто полагаются на пользовательскую информацию для управления своими сетями, что в конечном итоге служит пользователю.

5 К БОЛЕЕ ЧАСТНОМУ ИНТЕРНЕТУ

Несмотря на то, что за последние несколько лет был достигнут значительный прогресс во внедрении технологий сохранения конфиденциальности, подобных тем, которые мы обсуждали ранее, еще предстоит сделать гораздо больше.

5.1 Архитектурное разделение

Идея невступающих в сговор субъектов является старой в сфере безопасности: часто модель атаки предполагает, что некоторые субъекты не делятся определенной частной информацией или иным образом не вступают в сговор, обеспечивая гарантии безопасности или конфиденциальности. Разделение объектов, ответственных за сетевой трафик, основано на чем-то похожем. Однако существуют и юридические соображения: когда сетевой провайдер или облачная служба видит только часть сетевого подключения, по самой своей природе эта организация не может раскрыть те части, которые она не видит, и, таким образом, у нее есть нечто большее, чем просто правдоподобное отрицание. Поставщики услуг не могут получить доступ к разделенной информации без незаконного сговора друг с другом (и, вероятно, изменения программного обеспечения для этого), обеспечивая более надежную защиту пользователей своих услуг.

Отсутствие сговора может быть более эффективным как системное свойство, если пользователь может динамически объединять услуги или распределять их использование между несколькими поставщиками. Например, пользователь может улучшить конфиденциальность DNS, распределяя свои запросы по нескольким преобразователям, тем самым ограничивая информацию, доступную о данном пользователе на каждом из них [18]. Будущие архитектуры сервисов, такие как EI [2], которые предусматривают наличие нескольких объектов в Интернете, предлагающих компонуемые услуги, могут дополнительно обеспечить динамическую адаптацию и построение разделенных систем.

5.2 Будущие направления

Остается множество сетевых систем, которые могут извлечь выгоду из развязки, и такая работа (включая разработку систем, ориентированных на конфиденциальность и решающих новые проблемы, возникающие в разъединенных системах) может и должна продолжаться. Однако принцип разделения не является панацеей от всех проблем конфиденциальности пользователей. Что он действительно гарантирует, так это то, что распространенные нарушения конфиденциальности пользователей требуют нарушения самого принципа. Например, правительство может потребовать, чтобы все ретрансляторы в Private Relay вступили в сговор для получения конфиденциальной пользовательской информации, но это вынуждает систему нарушить принцип развязки.

В конечном счете, ценность отделения состоит в том, что оно переносит нарушения конфиденциальности в публичное, юридическое или социальное пространство, а не в техническую конструкцию системы, которая, как мы считаем, является подходящим пространством для таких разговоров.

БЛАГОДАРНОСТИ

Большое спасибо Томми Поли и анонимным рецензентам.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

[1] Яблоко. 2021. Обзор частного реле iCloud. https://www.яблоко.com/privacy/docs/iCloud_Private_Relay_Overview_Dec2021.PDF. (декабрь 2021 г.).

[2] Хари Балакришнан, Суджата Банерджи, Исраэль Сидон, Дэвид Каллер, Дебора Эстрин, Итан Кац-Бассетт, Арвинд Кришнамурти, Мерфи Мак-Коли, Ник МакКаун, Ауроджит Панда, Сильвия Ратнасами, Дженнифер Рексфорд, Майкл Шапира, Скотт Шенкер, Ион Стойка, Дэвид Тенненхаус, Амин Вахдат и Эллен Зегура. 2021. Оживление публичного Интернета путем его расширения. *СИГКОММ Компьютер. Коммун. Преподобный.* 51, 2 (май 2021 г.), 18–24.

[3] М. Бишоп. 2022. HTTP/3. *Рабочая группа по интернет-инжинирингу, предложенный RFC 9114* (2022).

[4] Дэвид Чаум. 1983. Слепые подписи для неотслеживаемых платежей. В *Достижения в криптологии*. Springer, 199–203.

[5] Дэвид Чаум. 1984. Система слепой подписи. В *Достижения в криптологии*. Springer, 153–153.

[6] Дэвид Л. Чаум. 1981. Неотслеживаемая электронная почта, обратные адреса и цифровые псевдонимы. *Коммун. АКМ* 24, 2 (1981), 84–90.

[7] Генри Корриган-Гиббс и Дэн Боне. 2017. Prio: Частное, надежное и масштабируемое вычисление совокупной статистики. В *14-й симпозиум USENIX по проектированию и внедрению сетевых систем (NSDI 17)*. 259–282.

[8] Джозеф Кокс. 2019. Я дал охотнику за головами 300 долларов. Затем он нашел наш телефон. https://материнская плата.порок.com/en_us/article/nepxbz/i-gave-abounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile. (январь 2019 г.).

[9] Джозеф Кокс. 2019. Сталкеры и сборщики долгов выдают себя за полицейских, чтобы обманом заставить крупную телекоммуникационную компанию передать им данные о местонахождении мобильных телефонов. https://www.порок.com/en_us/article/panvkz/stalkers-debt-collectorsbounty-hunters-impersonate-cops-phone-location-data. (март 2019 г.).

[10] Дебаджьоти Дас, Себастьян Мейзер, Эсфандиар Мохаммади и Аникет Кейт. 2018. Трилемма анонимности: строгая анонимность, низкая нагрузка на полосу пропускания, низкая задержка — выберите два. В *Симпозиум IEEE 2018 по безопасности и конфиденциальности (SP)*. IEEE, 108–126.

[11] Алекс Дэвидсон, Ян Голдберг, Ник Салливан, Джордж Танкерсли и Филиппо Вальсорда. 2018. Privacy Pass: анонимный обход интернет-проблем. *Труды по технологиям повышения конфиденциальности* 2018 (06.2018), 164–180.

[12] А. Дэвидсон, Дж. Айенгар и К. А. Вуд. 2022. *Конфиденциальность Архитектурный Рамки.* Интернет-Черновик. Интернет Инженерное дело Оперативная группа. https://www.IETF.org/archive/id/draft-ietf-privacypass-архитектура-03.html Работа в процессе.

[13] Р. Дингледин, Н. Мэтьюсон и П. Сайверсон. 2004. Tor: луковый маршрутизатор второго поколения», Симпозиум по безопасности USENIX. (2004).

[14] Тим Геогеган, Кристофер Паттон, Эрик Рескорла и Кристофер А. Вуд. 2022. *Протокол распределенного агрегирования для измерения с сохранением конфиденциальности.* Интернет-проект черновика-ietf-ppm-dap-00. Рабочая группа по интернет-инжинирингу. https://дататрекер.IETF.org/doc/html/draft-ietf-ppmdap-00 Работа продолжается.

[15] Джон Гиллиом. 2001. *Надзиратели за бедными: наблюдение, сопротивление и пределы конфиденциальности.* Издательство Чикагского университета.

[16] Бенджамин Грешбах, Тобиас Пуллс, Лора М. Робертс, Филипп Винтер и Ник Фимстер. 2017. Влияние DNS на анонимность Tor. В *Симпозиум по безопасности сетей и распределенных систем, NDSS*. Сан-Диего, Калифорния.

[17] Стивен Херциг, Кристина Гарман и Дэйв Левин. 2020. Достижение бесключевого доступа {CDN} с помощью конклавов. В *29-й симпозиум по безопасности USENIX (USENIX Security 20)*. 735–751.

[18] Остин Хаунсел, Пол Шмитт, Кевин Борголте и Ник Фимстер. 2021. Шифрование без централизации: распределение DNS-запросов между рекурсивными преобразователями. В *Материалы семинара по прикладным сетевым исследованиям (ANRW '21)*.

[19] Яна Айенгар и Мартин Томсон. 2021. QUIC: мультиплексированный и безопасный транспорт на основе UDP. *Рабочая группа по интернет-инжинирингу, RFC 9000* (2021).

[20] Кейт Кэй. 2015. Бизнес в области передачи данных стоимостью 24 миллиарда долларов, о котором телекоммуникационные компании не хотят говорить. https://пословица.com/article/datadriven-marketing/24-million-data-business-telcos-discuss/301058/?mod=article_inline. (26 октября 2015 г.).

[21] Крейг Лабовиц, Скотт Икель-Джонсон, Дэнни Макферсон, Джон Оберхайде и Фарнам Джаханян. 2010. Междоменный интернет-трафик. В *СИГКОММ 2010*. Нью-Дели, Индия.

[22] Адам Лэнгли, Алистер Риддок, Алисса Уилк, Антонио Висенте, Чарльз Красич, Дэн Чжан, Фань Янг, Федор Куранов, Ян Светт, Джанардхан Айенгар и др. 2017. Транспортный протокол quic: проектирование и развертывание в масштабе Интернета. В *Труды ACM SIGCOMM*.

[23] Тай Лю, Зейн Тарик, Джей Чен и Барат Рагхаван. 2017. Барьеры на пути свержения интернет-феодализма. В *Материалы 16-го семинара ACM по актуальным темам в сетях*. 72–79.

[24] Ребекка Маккиннон. 2013. *Согласие сетевых пользователей: всемирная борьба за свободу Интернета*. Основные книги (AZ).

[25] Роберт В. Макчесни. 2013. *Цифровое отключение: как капитализм настраивает Интернет против демократии*. Новая Пресса, The.

[26] Ёшимичи Накацука, Эрджан Озтюрк, Эндрю Паверд и Джин Цудик. 2021. {CACTI}: предотвращение капчи посредством интеграции {TEE} на стороне клиента. В *30-й симпозиум по безопасности USENIX (USENIX Security 21)*. 2561–2578.

[27] Энрик Пуйоль, Ингмар Поезе, Йоханнес Зервас, Георгиос Смарагдакис и Аня Фельдманн. 2019. Масштабное управление трафиком гипергигантов. В *КОНЕКСТ 2019*. Орландо, Флорида.

[28] Эрик Рескорла, Кадзухо Оку, Ник Салливан и Кристофер А. Вуд. 2022. *Клиент с шифрованием TLS Здравствуйте!.* Интернет-проект Draft-ietf-tls-esni-14. Рабочая группа по интернет-инжинирингу. https://дататрекер.IETF.org/doc/html/draft-ietf-tls-esni-14 Работа продолжается.

[29] Пол Шмитт, Энн Эдмундсон, Эллисон Мэнкин и Ник Фимстер. 2019. Oblivious DNS: практическая конфиденциальность DNS-запросов. *Труды по технологиям повышения конфиденциальности* 2019 (04.2019), 228–244.

[30] Пол Шмитт и Барат Рагхаван. 2021. Довольно хорошая конфиденциальность телефона. В *USENIX Безопасность 2021*. виртуальный.

[31] Брюс Шнайер. 2012. *Лжецы и аномалии: обеспечение доверия, необходимого обществу для процветания.* Джон Уайли и сыновья.

[32] Брюс Шнайер. 2012. Когда дело доходит до безопасности, мы возвращаемся к феодализму. *Шнайер о безопасности* (2012).

[33] Брюс Шнайер. 2015. *Данные и Голиаф: скрытые битвы за сбор ваших данных и контроль над своим миром*. WW Нортон и компания.

[34] Брюс Шнайер. 2018. Наблюдение убивает свободу, убивая экспериментирование. https://www.проводной.com/story/mcsweeneys-excerpt-theright-to-experiment/. (ноябрь 2018 г.).

[35] Судиш Синганамалла, Суфанат Чунхапанья, Джонатан Хойланд, Марек Вавруша, Таня Верма, Питер Ву, Марван Файед, Куртис Хеймерл, Ник Салливан и Кристофер Вуд. 2021. Забывчивый DNS через HTTPS (ODoH): практическое улучшение конфиденциальности DNS. *Труды по технологиям повышения конфиденциальности* 2021 (10 2021), 575–592.

[36] Пол Ф. Сайверсон, Дэвид М. Гольдшлаг и Майкл Дж. Рид. 1997. Анонимные соединения и луковая маршрутизация. В *Слушания. Симпозиум IEEE 1997 г. по безопасности и конфиденциальности (кат. № 97CB36097)*.. IEEE, 44–54.

[37] Кен Томпсон. 1984. Размышления о доверии. *Коммун. АКМ* 27, 8 (1984), 761–763.

[38] Мартино Тревизан, Данило Джордано, Идилио Драго, Марко Меллия и Маурицио Мунафо. 2018. Пять лет на грани: просмотр Интернета из сети интернет-провайдера. В*KONEKST 2018*. Ираклион, Греция.

[39] Зак Уиттакер. 2018. Операторы сотовой связи в США продают доступ к данным о местоположении вашего телефона в реальном времени. https://www.зднет.com/article/us-cellcarriers-selling-access-to-real-time-location-data/. (14 мая 2018 г.).

[40] Шошана Зубофф. 2015. Большое другое: капитализм наблюдения и перспективы информационной цивилизации.*Журнал информационных технологий*30, 1 (2015), 75–89.