Internet Architecture Board (IAB)
Request for Comments: 7624
Category: Informational
ISSN: 2070-1721

R. Barnes
B. Schneier
C. Jennings
T. Hardie
B. Trammell
C. Huitema
D. Borkmann

August 2015

Конфиденциальность перед лицом всеобъемлющего наблюдения - модель угроз и постановка задачи

Confidentiality in the Face of Pervasive Surveillance:

A Threat Model and Problem Statement

Аннотация

С момента первоначального обнаружения всеобъемлющего наблюдения в 2013 году было раскрыто несколько типов атак на коммуникации Internet. В этом документе приведена модель угроз, которая описывает эти атаки на конфиденциальность в Internet. Мы предполагаем, что атакующие заинтересованы в недетектируемом перехвате без выделения конкретных целей. Модель угроз основана на опубликованной и проверенной информации об атаках.

Статус документа

Этот документ не является спецификацией какого-либо стандарта Internet и публикуется с информационными целями.

Этот документ является результатом работы IAB[1] и представляет информацию, которую IAB считает нужным опубликовать и сохранить. Эта информация выражает согласованную точку зрения IAB. Документы, одобренные для публикации IAB, не рассматриваются в качестве возможных стандартов Internet (см. раздел 2 в RFC 5741).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc7624.

Оглавление

[1] Internet Architecture Board - Совет по архитектуре Internet.

1. Введение

Начиная с июня 2013, Эдвардом Сноуденом (Edward Snowden) были раскрыты для публикации документы о некоторых операциях, выполняемых разведывательными службами в целях использования коммуникаций Internet для негласного получения информации. Эти атаки в значительной степени основаны на использовании известных уязвимостей протоколов. Тем не менее, эти атаки поражали воображение широтой охвата как в плане объёмов отслеживаемого трафика Internet, так и используемых для слежки методов.

Для того, чтобы обеспечить доверие пользователей сети Internet техническое сообщество Internet должно решить вопросы преодоления уязвимостей, использованных в этих атаках [RFC7258]. Целью настоящего документа является более точное описание угроз, создаваемых этими всеобъемлющими атаками, и на основе этих угроз очертить проблемы, которые требуется решить для обеспечения безопасности Internet перед лицом таких угроз.

В оставшейся части этого документа раздел 3 посвящён пассивным всеобъемлющим атакам, которые способны скрытно отслеживать все коммуникации в масштабе Internet, в разделе 4 дано краткое описание обнаруженных атак этого типа и оценки возможностей атакующих для идеализированной ситуации. Отметим, что здесь не предпринимается попытки описать все возможные атаки и основное внимание уделено тем, которые позволяют организовать недетектируемый перехват. В разделе 5 описана модель угроз, разработанная на основе этих атак с основным вниманием на атаки, которые ещё не получили должного внимания со стороны инженерного сообщества Internet.

2. Терминология

В этом документе используется связанная с приватностью и безопасностью терминология, которая описана в [RFC4949] и [RFC6973]. Термины из [RFC6973] включают Eavesdropper (соглядатай), Observer (наблюдатель), Initiator (инициатор), Intermediary (посредник), Recipient (получатель), Attack (атака в контексте приватности), Correlation (сопоставление), Fingerprint (оттиск), Traffic Analysis (анализ трафика), Identifiability (идентифицируемость) и др. Кроме того применяется несколько новых терминов, которые относятся непосредственно к описанным здесь атакам. Отметим отдельно что термины «пассивная» и «активная» в тексте документа не связаны с действиями по организации атак - пассивной считается любая атака, обеспечивающая доступ к потоку трафика, но не меняющая его содержимого, а активные атаки меняют сам поток трафика. Некоторые пассивные атаки включают активный захват и изменение конфигурации устройств, не ограничиваясь простым доступом к среде передачи. Определения новых терминов приведены ниже.

Pervasive Attack - всеобъемлющая атака
: Атака на коммуникации Internet, в которой используется доступ к большому числу точек сети или иные способы предоставления атакующему большого объёма трафика Internet (см. [RFC7258]).

Passive Pervasive Attack - пассивная всеобъемлющая атака
: Атака на основе перехвата, организованная в широком масштабе, при которой перехватываются потоки трафика между парами узлов, но атакующий не может изменять пакеты в перехватываемых потоках, менять обработку пакетов (например, задержку или маршрут), добавлять или удалять пакеты в потоке. Пассивные атаки не могут быть обнаружены конечными точками, чьи данные перехватываются. Это эквивалентно пассивному ответвлению (passive wiretapping), описанному в [RFC4949]. Здесь применяется специальный термин для таких атак, поскольку используемые в них методы шире, нежели обычное «ответвление» трафика, и включают активное воздействие на промежуточные системы.

Active Pervasive Attack - активная всеобъемлющая атака
: Атака, где в дополнение к повсеместному прослушиванию атакующий может изменять, добавлять или удалять пакеты в потоке трафика или оказывать влияние на их обработку. Эквивалент атаки active wiretapping, в соответствии с определением [RFC4949].

Observation - наблюдение
: Информация собирается непосредственно из коммуникационного обмена соглядатаем или наблюдателем. Например, выяснение того, что <alice@example.com> отправляет сообщение <bob@example.com> через сервер SMTP, определённый из заголовков SMTP, является наблюдением.

Inference - логический вывод
: Информация добывается из анализа данных, собранных непосредственно из коммуникаций соглядатаем или наблюдателем. Например, информация о том, что данная страница web доступна по данному адресу IP, полученная путём сравнения размера (в октетах) записей для потока с отпечатками, полученными по известным размерам для связанных ресурсов на вовлечённых web-серверах, будет предположением.

Collaborator - соучастник
: Элемент, являющийся легитимным участником коммуникаций и предоставляющий информацию об этих коммуникациях злоумышленнику (атакующему). Соучастник может способствовать атакующему вольно или невольно (в последнем случае это обусловлено техническим, социальным или иным воздействием со стороны атакующего).

Key Exfiltration - утечка ключей
: Передача атакующему криптографического материала, используемого для шифрования коммуникаций через вольного или невольного соучастника.

Content Exfiltration - утечка содержимого
: Передача содержимого коммуникаций атакующему от вольного или невольного соучастника.

3. Идеализированная пассивная атака

Рассмотрение угрозы, связанной с повсеместной слежкой, начнём с идеализированной пассивной атаки. В этом случае возможности атакующего меньше, нежели были в описанных в прессе случаях нарушения работы Internet, которые рассмотрены в разделе 4. В таких атаках используется пассивный перехват всех данных, но атака остаётся незаметной. Отметим, что до сообщений Сноудена в 2013 году сообщения о представленных здесь возможностях организации атак люди, не связанные с сетевой безопасностью, рассматривали, как параноидальный бред.

В нашем идеализированном случае соглядатай, просматривающий все подряд, имеет подключенный к сети Internet компьютер и способен выполнять перечисленные ниже действия.

- Наблюдать каждый пакет всех коммуникаций на любом интервале в любой сети между инициатором и получателем.
- Статически наблюдать данные в любой промежуточной системе между конечными точками, контролируемыми инициатором и получателем.
- Передавать полученную информацию другим атакующим, но не может оказывать какое-либо воздействие на коммуникации (например, блокирование, изменение, вставка пакетов и т. п.).

Доступные атакующему в нашем идеализированном случае методы включают прямое наблюдение и выводы. Прямое наблюдение включает непосредственный сбор информации из перехватываемых коммуникаций типа идентифицирующего URL содержимого или адресов электронной почты из заголовков прикладного уровня, указывающих конкретных лиц. Логические выводы, с другой стороны, включают анализ собранных данных для получения новой информации типа поиска отпечатков приложений или моделей поведения в наблюдаемом трафике для получения сведений об участвующих в коммуникациях лицах. Применения шифрования обычно достаточно для того, чтобы предотвратить возможность прямого наблюдения (при условии того, что реализации криптографических средств не имеют лазеек, а ключевой материал не скомпрометирован). Однако для логического анализа шифрование не обеспечивает достаточной защиты, особенно в тех случаях, когда анализируются только открытые компоненты коммуникаций типа заголовков IP и TCP для трафика TLS [RFC5246].

3.1. Информация, доступная для непосредственного наблюдения

Протоколы, не использующие шифрования данных, делают эти данные доступными для злоумышленников вдоль всего пути передачи. В соответствии с рекомендациями [RFC3365] большинство таких протоколов поддерживает защищённый вариант с шифрованием содержимого для обеспечения конфиденциальности и эти защищённые варианты распространяются все шире. Важным исключением является протокол DNS [RFC1035], поскольку DNSSEC [RFC4033] не требует защиты конфиденциальности.

Это означает, что до перехода на разрабатываемый рабочей группой IETF DPRIVE[1] протокола [DPRIVE], все запросы и отклики DNS при любых действиях будут доступны для злоумышленников.

При использовании протоколов с промежуточным хранением (store-and-forward) типа SMTP [RFC5321] промежуточные узлы открывают доступ к сохраненным данным захватившим такие узлы злоумышленникам, если при коммуникациях не применяется сквозное шифрование или промежуточный узел не использует шифрование при сохранении данных.

3.2. Информация, полезная для логического анализа

Выводы представляют собой информацию, полученную путём последующего анализа наблюдаемых или подслушанных коммуникаций и/или сопоставления наблюдаемой или перехваченной информации и с данными из других источников. На практике наиболее полезным для атакующего результатом является обнаружение корреляций. Простейшим примером является наблюдение запросов DNS и откликов на них с последующим сопоставлением результатов этого наблюдения с адресами IP, к которым данный источник будет обращаться (например, заголовок "Host:" запроса HTTP/1.1 при работе HTTP по протоколу TLS).

Протоколы, использующие шифрование данных на прикладном или транспортном уровне (например, TLS), по-прежнему оставляют открытыми для злоумышленников заголовки сетевого и транспортного уровня, включающие адреса и номера портов отправителя и получателя. В IPsec ESP[2] [RFC4303] дополнительно шифруются заголовки транспортного уровня, но адреса IP передаются в открытом виде (в туннельном режиме эти адреса указывают конечные точки туннеля). Свойства самих протоколов защиты (например, сеансовые идентификаторы TLS) могут давать злоумышленникам дополнительную информацию для сопоставления и выводов. Хотя смысла в такой информации значительно меньше для атакующего, она все равно может оказаться полезной для анализа действий отдельных пользователей.

Анализ может также повышать качество информации, полученной из источников, отличающихся от наблюдения за трафиком. Например, базы данных о местоположении служат для привязки адресов IP к территориям с целью предоставления дифференцируемых по местам услуг типа контекстной рекламы. Такая информация зачастую обеспечивает точность, достаточную для достоверных предположений с целью идентификации или создания профиля отдельного пользователя.

Социальные сети и СМИ могут быть ещё одним источником более или менее доступной публично информации. Такая информация может оказаться весьма обширной, включая сведения о местоположении людей, их связях с другими людьми и группами, а также деятельности или мероприятиях, в которых человек принимает участие. Кроме того, такую информацию люди обычно публикуют и поддерживают добровольно - обычно они просто не задумываются при этот о защите приватности. Однако сопоставление данных из социальных сетей с результатами непосредственного наблюдения сетевого трафика позволяют создать весьма полную картину деятельности отдельных людей.

Отметим, что при разработке протоколов мало что можно сделать для ограничения возможностей атакующих в поиске отмеченных корреляций и наличие таких источников информации значительно усложняет задачу защиты приватности на уровне протоколов.

3.3. Картина идеализированной пассивной атаки

Для демонстрации возможностей атакующего, даже с учётом ограничений, в этом параграфе рассматривается неанонимный шифрованный трафик IP. Подробно рассмотрены некоторые методы анализа для связывания набора адресов с конкретным лицом для иллюстрации сложности защиты коммуникаций от нашего идеализированного злоумышленника. Основная проблема состоит в том, что информацию, полученную даже от протоколов, не связанных с персональными данными, можно сопоставить с другой информацией для получения достаточно полной картины поведения. И нужен для этого лишь один незащищённый канал в цепочке.

[1] DNS Private Exchange - приватный обмен DNS.
[2] Encapsulating Security Payload - инкапсуляция защищённых данных.

3.3.1. Анализ заголовков IP

Отслеживать трафик Internet можно с помощью ответвлений на каналах Internet или установки программ-мониторов на маршрутизаторах Internet. Понятно, что ответвление одного канала или контроль за одним маршрутизатором обеспечит доступ лишь к малой части глобального трафика Internet. Однако, организовав мониторинг множества магистральных каналов или установив программы слежения на множестве маршрутизаторов[1] можно получить достаточно хорошую выборку трафика Internet.

Инструменты типа протокола IPFIX[2] [RFC7011] позволяют администраторам собирать статистику для последовательностей пакетов с некими общими свойствами, которые проходят через сетевое устройство. Наиболее общим набором свойств, используемым в качестве «метрики» потоков, является «пятёрка (five-tuple) из адресов отправителя и получателя, типа протокола и номеров портов на обеих сторонах. Такая статистика обычно применяется для организации трафика, но может служить и другим целям.

Давайте предположим, что адрес IP можно сопоставить с конкретными службами или пользователями. Анализ последовательностей пакетов будет быстро показывать, какие пользователи пользуются какими службами, а также позволит определить одноранговые (peer-to-peer) соединения между пользователями. Анализ изменения трафика с течением времени позволяет обнаружить рост активности определённого пользователя или группы пользователей в случае одноранговых соединений.

3.3.2. Сопоставление адресов IP с пользователями

Сопоставить адреса IP с конкретным пользователем можно разными способами. Например, инструменты типа обратных преобразователей DNS (reverse lookup) позволяют определить имена DNS для серверов. Поскольку адреса серверов обычно достаточно стабильны и серверов существенно меньше, чем их пользователей, злоумышленник легко может организовать и поддерживать свою копию DNS для общеизвестных и популярных серверов с целью ускорения своей работы.

С другой стороны, определение имён (reverse lookup) по адресам IP даёт немного информации. Например, запрос для адреса, который автор использует в домашней сети даст имя c-192-000-002-033.hsd1.wa.comcast.net. Обратные преобразователи DNS обычно дают лишь «грубую» информацию о местоположении и поставщике услуг, которую можно просто найти в базе данных геолокации.

Во многих странах ISP[3] обязаны предоставлять информацию о «владельце» конкретного адреса по запросам правоохранительных органов. Это достаточно эффективно при конкретных расследованиях, но нашему злоумышленнику требуется нечто большее. Это стимулирует атакующих на взаимодействие с ISP для автоматического сопоставления адресов с пользователями.

3.3.3. Отслеживание клиентских сообщений для сопоставления адресов IP

Даже при отсутствии взаимодействия с ISP пользователей зачастую можно идентифицировать с помощью логических выводов. Протоколы POP3 [RFC1939] и IMAP [RFC3501] применяются для получения почты с серверов, а SMTP используется для отправки на серверы почтовых сообщений. Соединения IMAP исходят от клиента и обычно начинаются с аутентификационного обмена, в котором клиент предъявляет отождествляет себя, отвечая на запрос пароля. То же самое происходит в протоколе SIP [RFC3261] и многих системах обмена мгновенными сообщениями через Internet, использующих фирменные протоколы.

Имя пользователя можно увидеть непосредственно, если любой из упомянутых протоколов работает в открытом режиме без шифрования. После этого имя пользователя можно сопоставить с адресов отправителя в пакетах.

3.3.4. Извлечение адресов IP из почтовых заголовков

Протокол SMTP [RFC5321] требует, чтобы каждый транслятор SMTP в цепочке передачи добавлял в почтовый заголовок свою строку Received. Это предназначено для аудита почтовых транзакций, а в некоторых случаях - для того, чтобы отличить нормальную почту от спама. Ниже приведена такая строка, извлечённая из сообщения, полученного недавно в списке рассылки perpass.

```
Received: from 192-000-002-044.zone13.example.org (HELO ?192.168.1.100?) (xxx.xxx.xxx.xxx) by lvps192-000-002-219.example.net with ESMTPSA (DHE-RSA-AES256-SHA encrypted, authenticated); 27 Oct 2013 21:47:14 +0100
Message-ID: <526D7BD2.7070908@example.org> Date: Sun, 27 Oct 2013 20:47:14 +0000 From: Some One <some.one@example.org>
```

Это первый заголовок Received, присоединённый к сообщению первым транслятором SMTP (в целях сохранения приватности значения полей были изменены). Мы видим, что сообщение было отправлено неким пользователем Some One 27 октября с хоста за транслятором NAT (192.168.1.100) [RFC1918], который использует IP-адрес 192.0.2.44. Эта информация остаётся в сообщении и доступна всем получателям рассылки perpass, а также любому злоумышленнику, который просто видит копию сообщения.

Атакующий, который может наблюдать достаточный объем почтового трафика, может регулярно обновлять привязки публичных адресов IP к почтовым идентификаторам пользователей. Даже шифрование трафика SMTP при подаче и трансляции сообщений не сможет воспрепятствовать злоумышленнику получать копии сообщений из списков рассылок типа perpass.

3.3.5. Отслеживание используемых адресов с помощью Web Cookie

Многие web-сайты шифруют лишь малую часть своих транзакций. Достаточно широко применяется протокол HTTPS для передачи идентификационной информации (login), а после этого применяются cookie для связывания последующих открытых транзакций с предъявленным отождествлением пользователя. Технологии cookie также используют различные рекламные службы для быстрой идентификации пользователей и передачи им «персонифицированной» рекламы. Такие cookie полезны, в частности, для рекламных служб, которые хотят отслеживать пользовательскую активность даже при смене тем адреса IP.

---

[1] Например, в точках обмена трафиком. *Прим. перев.*
[2] IP Flow Information Export - экспорт информации потоков IP.
[3] Internet Service Provider - поставщик услуг Internet.

Поскольку cookie передаются в открытом виде, атакующий может создать базу данных с сопоставлениями cookie с адресами IP в трафике, не являющемся HTTPS. Если адрес IP уже идентифицирован, cookie можно также привязать к отождествлению пользователя. После этого, если те же cookie появляются с другими адресами IP, эти адреса также связываются с определенным ранее отождествлением пользователя.

3.3.6. Модели сопоставления адресов на базе графов

Атакующий может отслеживать трафик с IP-адреса, который ещё не связан с конкретным пользователем, на разные публичные службы (например, web, электронная почта, игровые серверы) и использовать картину наблюдаемого трафика для сопоставления этого адреса с другими адресами, имеющими аналогичную картину. Например, два любые адреса, подключающиеся к одним серверам IMAP или webmail, одному и тому же набору предпочтительных web-сайтов и игровых серверов примерно в одинаковое время, могут быть связаны с одним человеком. Сопоставленные адреса можно будет связать с конкретным человеком, используя один из описанных выше методов с перемещением по «графу сети» для расширения множества атрибутированного трафика.

3.3.7. Отслеживание идентификаторов канального уровня

Технологии канального уровня стека протоколов типа Ethernet или Wi-Fi используют адреса MAC[1] для идентификации получателей на канальном уровне. MAC-адреса выделяются в соответствии со стандартами IEEE 802 так, чтобы устройство можно было уникально идентифицировать в глобальном масштабе. Если к канальному уровню имеется открытый доступ, атакующий может организовать прослушивание и отслеживание адресов. Например, злоумышленник может отслеживать трафик беспроводных сетей в публичных зонах Wi-Fi. Простые устройства позволяют организовать мониторинг и показывать присутствие MAC-адресов. Для раскрытия идентификаторов канального уровня устройство даже не требуется подключать к сети. Активное детектирование сервиса раскрывает MAC-адрес пользователя, а иной раз и идентификаторы SSID[2] ранее посещённых им сетей. Например, некоторые методы типа использования скрытых SSID требуют от мобильных устройств широковещательное передачи идентификатора сети вместе с идентификатором устройства. Такая комбинация может дополнительно раскрывать пользователя для аналитических атак, поскольку включает комбинацию MAC-адреса, проверяемого SSID, времени и текущего местоположения. Например, активная проверка пользователем полууникального SSID на вылете из того или иного города, скорей всего говорит о том, что он покидает этот город и его больше не будет в месте расположения соответствующей точки доступа. С учётом того, что уже давно существуют базы данных о MAC-адресах точек доступа для целей геолокации, атакующий может без проблем создать базу данных, связывающую идентификаторы канального уровня и время с устройствами и идентификаторами пользователей , применяя эту базу для отслеживания перемещений устройств и их владельцев. С другой стороны, если в сети Wi-Fi не применяется шифрования или злоумышленник способен расшифровать трафик, анализ позволит также сопоставить MAC-адреса с адресами IP. Дополнительный мониторинг с использованием описанных выше методов позволит сопоставить адреса MAC и IP с отождествлением пользователя. Например, подобно web cookie, адреса MAC могут служить для отождествления и могут быть использованы для связывания пользователя с разными адресами IP.

4. Известные примеры крупномасштабных атак

Реальная ситуация существенно мрачнее того, что показано выше при анализе идеализированного атакующего. Благодаря утечке секретных документов в некоторые СМИ, стало известно о некоторых операций, проводимых резведслужбами США и Англии, в частности US NSA[3] и UK GCHQ[4]. В этих документах раскрываются методы, которые эти службы применяли для атаки на приложения Internet с целью получения конфиденциальной информации о пользователях. Нет никаких оснований предполагать, что такую деятельность вели лишь правительства США и Англии - просто они попались первыми. Отметим, что эти отчёты полезны прежде всего в качестве иллюстрации возможностей повседневной слежки на момент публикации откровений Сноудена в 2013 году.

Во-первых, отчёты подтверждают развёртывание крупномасштабной системы перехвата и сбора трафика Internet, что служит подтверждением наличия всеобъемлющего пассивного наблюдения, в котором, как минимум, имеются возможности описанного выше идеализированного злоумышленниками. Например, как описано в [pass1], [pass2], [pass3] и [pass4]:

- система XKEYSCORE в NSA имеет доступ к данным от множества точек доступа и выполняет поиск по таким селекторам, как адреса электронной почты в масштабе десятков терабайтов данных в сутки;
- система Tempora в GCHQ имеет доступ приблизительно к 1500 основных кабелей на территории Соединённого королевства;
- программа MUSCULAR в NSA перехватывает данные из кабелей между центрами обработки основных сервис-провайдеров;
- имеется несколько программ широкомасштабного сбора cookie в трафике web и данных о местоположении мобильных устройств типа смартфонов.

Однако описанные в упомянутых отчётах возможности существенно превосходят описанные выше возможности идеализированного злоумышленника. Они включают взлом криптографических протоколов, в том числе расшифровку защищённых с помощью TLS сессий Internet [dec1] [dec2] [dec3]. Например, проект NSA BULLRUN был направлен на нарушение работы шифровальных систем разными способами, включая преднамеренное изменение криптографических программ на оконечных системах.

Отмеченные в отчётах возможности включают прямой взлом (компрометацию) промежуточных систем и соглашения с сервис-провайдерами в части широкомасштабного доступа к данным и метаданным [dir1] [dir2] [dir3] без необходимости захвата трафика из кабельных линий. Например, программа NSA PRISM обеспечивала АНБ доступом ко многим типам пользовательских данных (например, электронная почта, чат, VoIP).

[1]Media Access Control - управление доступом к среде.
[2]Service Set Identifier - идентификатор набора услуг.
[3]National Security Agency - Агентство национальной безопасности (АНБ).
[4]Government Communications Headquarters.

Упомянутые в отчётах возможности включают также элементы активных всеобъемлющих атак.

- Вставка устройств для организации MITM[1]-атак на транзакции Internet [TOR1] [TOR2]. Например, система NSA QUANTUM использует несколько разных технологий захвата соединений HTTP от вставки ложных откликов DNS до перенаправлений HTTP 302.

- Установка в конечные системы специальных компонент (имплантов) для преодоления средств защиты и анонимности [dec2] [TOR1] [TOR2]. Например, QUANTUM применяется для направления пользователей на сервер FOXACID, который, в свою очередь, обеспечивал доставку и установку специального импланта для компрометации браузеров у пользователей Tor.

- Использование имплантов NSA Advanced Network Technology в сетевом оборудовании множества основных производителей, включая Cisco, Juniper, Huawei, Dell и HP [spiegel1].

- Использование бот-сетей из взломанных и захваченных хостов [spiegel2].

Масштабы угрозы выходят за рамки сети, как таковой, и захватывают процессы разработки технических стандартов. Например, есть подозрение, что модификации NSA для генератора случайных чисел DUAL_EC_DRBG (RNG) были специально сделаны так, чтобы АНБ могло предсказывать результат работы генератора. Этот RNG был сделан частью стандарта NIST SP 800-90A и NIST подтверждает участие NSA. Сообщают также, что АНБ платило RSA Security по контракту, в результате которого была разработана кривая, используемая по умолчанию в линейке продукции RSA BSAFE.

Мы используем термин «всеобъемлющая атака» (pervasive attack) [RFC7258] для описания этих операций в целом. Атрибут «всеобъемлющая» был выбран потому, что атаки организуются для сбора всех данных, какие доступны, и применения к ним логического анализа, нацеленного уже более конкретно. Это означает, что все или почти все коммуникации в Internet являются целями таких атак. Для достижения такого масштаба атаки должны быть повсеместными в физическом смысле - они воздействуют на большинство коммуникаций Internet. Атаки всеобъемлющи и в смысле содержимого, поскольку захватывают и поглощают любую информацию, которую можно извлечь из протокола. В технологическом смысле всеобъемлющий характер атак означает, что в них используется множество разных уязвимостей в различных протоколах.

Ещё раз важно подчеркнуть, что атаки этого типа могут использовать многие организации, хотя «пойманы за руку» были только NSA и GCHQ. Поскольку для организации таких атак требуются значительные ресурсы, это доступно в большинстве случаев организациям, работающим на государства. Например, китайская система фильтрации Internet, известная, как Great Firewall of China, использует методы, похожие на программу QUANTUM, и обеспечивает широкий охват китайского сегмента сети Internet. Таким образом, правовые ограничения любого государства на организацию всеобъемлющего мониторинга не могут избавить от риска всеобъемлющих атак на Internet в целом.

5. Модель угроз

С учётом упомянутых выше разоблачений требуется рассмотреть более широкую модель угроз.

Всеобъемлющая слежка направлена на сбор информации из большого числа коммуникаций Internet, анализ собранных данных для идентификации нужной информации в отдельных коммуникациях, а также сопоставление информации из связанных между собой коммуникаций. Такой анализ иногда может получить дополнительные преимущества от расшифровки зашифрованных данных и раскрытия анонимности коммуникаций. Поэтому атакующие стремятся получить доступ к большим объёмам трафика Internet и ключевому материалу, требуемому для расшифровки любого трафика, который может быть зашифрован. Даже при недоступности ключей факт наличия коммуникаций и их шифрования может служить исходной информацией для анализа, несмотря на то, что злоумышленник не способен расшифровать данные.

Отмеченные выше атаки показали новые возможности доступа как к трафику, так и к ключам шифрования. Они также показали, что масштабы слежки достаточно велики для того, чтобы можно было найти кросс-корреляции в трафике Internet – раньше такая угроза в масштабах Internet в целом просто не рассматривалась.

5.1. Возможности атакующих

Класс атаки	***Возможности***
Пассивное наблюдение	Прямой сбор данных в процессе передачи
Пассивный анализ	Логические выводы из неполных/нешифрованных данных
Активная	Изменение/вставка данных в процессе передачи
Статическая утечка ключей	Однократное или редкое получение ключей
Динамическая утечка ключей	Получение сеансового ключевого материала
Утечка содержимого	Доступ к данным без перехвата

При анализе безопасности протоколов Internet обычно рассматривается два класса атак - пассивные всеобъемлющие атаки, когда атакующий может просто «прослушивать» трафик, проходящий через сеть, и активные всеобъемлющие атаки, в которых атакующий в дополнение к сбору пакетов может изменять или удалять их.

В контексте пассивной всеобъемлющей слежки эти атаки приобретают дополнительную значимость. В прошлом предполагалось, что такие злоумышленники обычно действуют на периметре сетей, где организовать атаку проще. Например, в некоторых ЛВС практически любой узел может организовать пассивное прослушивание других узлов или вставку пакетов для организации активной атаки. Однако сейчас, как мы знаем, пассивные и активные всеобъемлющие атаки переместились в направлении ядра сети, что значительно расширило сферу охвата и возможности атакующих.

Подслушивание и наблюдение в более широких масштабах упрощает организацию пассивных атак с анализом данных - пассивный атакующий с доступом к значительной части Internet может анализировать собранный трафик для получения более детального представления о поведении отдельных субъектов, нежели это возможно при сборе данных в одной точке. Даже обычное представление о том, что шифрование осложняет проведение пассивных всеобъемлющих атак, частично утрачивает силу, поскольку атакующий может логически вывести нужные связи из

[1]Man-in-the-middle - перехват данных с участием человека для из анализа и модификации. *Прим. перев.*

сопоставления данных большого числа сессий (например, связывая шифрованные и нешифрованные сеансы одного хоста или сравнивая «отпечатки» трафика между известными и неизвестными шифрованными сеансами). Сведения о системе NSA XKEYSCORE показывают пример такого типа атак.

В активной всеобъемлющей атаке злоумышленник также имеет возможности, превосходящие возможности локальной активной атаки. Атаки с измерением потоков часто ограничены топологией сети (например, атакующий должен иметь возможность видеть целевую сессию, а также включать в неё свои пакеты). Атакующий с возможностью повсеместного изменения потоков и доступом к множеству точек в ядре Internet способен преодолеть топологические ограничения и организовать атаки со значительно более широким охватом. Размещение в ядре сети, а не на её периметре может также позволить активному атакующему менять маршрутизацию целевого трафика для организации прослушивания и вставки пакетов. В активных всеобъемлющих атаках могут также применяться результаты пассивных атак для обнаружения уязвимых хостов.

Хотя это и не связано напрямую с зоной распространения атаки, злоумышленники, способные организовать всеобъемлющую активную атаку, зачастую способны также обмануть аутентификацию, традиционно применяемую для защиты от таких атак. Аутентификация в Internet зачастую выполняется с помощью доверенных органов типа удостоверяющих центров (CA[1]), которые «заверяют» подлинность представления web-сайтов. Атакующий с достаточными ресурсами может создать «удостоверяющий центр», который будет «заверять подлинность» нужных для атаки сайтов. Если стороны обмена данными доверяют множеству удостоверяющих центров для заверения конкретного отождествления, такую атаку можно организовать путём «подчинения» одного из таких центров (пресловутое «слабое звено»). Подмена или захват удостоверяющих центров позволяет организовать успешную активную атаку даже при наличии проверки подлинности.

Кроме трёх отмеченных классов атак (наблюдение, анализ и активное воздействие), сообщалось о проекте BULLRUN по взлому шифрования и проекту PRISM по получению данных от сервис-провайдеров, что позволяет предположить ещё три класса атак:

- статическая утечка ключей;
- динамическая утечка ключей;
- утечка содержимого.

Эти атаки основаны на сотрудничестве с провайдерами, предоставляющими организаторам атак некоторую информацию - ключи или данные. Такие атаки обычно не включаются в рассмотрение разделов «Вопросы безопасности» протоколов IETF, поскольку они выходят за рамки протоколов.

Термин «утечка ключей» (key exfiltration) означает передачу ключевого материала, используемого для шифрованных коммуникаций от соучастника (провайдер) к атакующему. Под статической утечкой мы понимаем однократную или эпизодическую (редкую) передачу ключей, которые обычно используются в течение продолжительного срока. Например, к этой категории относится передача сервис-провайдером секретного ключа, соответствующего сертификату HTTPS в разведслужбу.

Термин «динамическая утечка ключей» относится к атакам, в которых соучастник регулярно передаёт атакующему ключевой материал (например, сеансовый ключ). Это не обязательно предполагает частое взаимодействие с атакующим, поскольку передача ключевого материала может быть виртуальной. Например, если конечную точку изменить так, чтобы атакующий мог предсказать состояние её генератора псевдослучайных чисел, этот атакующий сможет самостоятельно создавать нужные сеансовые ключи даже без коммуникаций до начала сеанса.

Утечкой содержимого мы называем атаки, в которых соучастник просто обеспечивает атакующему нужные тому данные или метаданные. В отличие от утечки ключей такая атака не требует от организатора сбора данных в сети. Для утечки используются скорее статические данные, нежели передаваемые через сеть. Это расширяет спектр доступных злоумышленнику данных, поскольку он может видеть их изменение, а не просто фрагмент, перехваченный в процессе передачи через сеть.

Утечки могут быть организованы с помощью атаки на одну из взаимодействующих сторон (например, злоумышленник похитит ключи или содержимое, прикинувшись нужным партнёром). В таком случае подвергшаяся атаке сторона может не знать (по крайней мере, на уровне людей) о том, что она является соучастником другой атаки. Здесь просто используются технические активы одной из сторон для «соучастия» в действиях атакующего (путём предоставления ключей или содержимого) без ведома и согласия их владельца.

Любая сторона, имеющая доступ к ключам или незашифрованным данным, может стать таким соучастником. Хотя обычно в качестве невольных соучастников выступают конечные точки коммуникаций (с шифрованием для защиты каналов), промежуточные точки недостаточно надёжно зашифрованных коммуникаций также могут стать соучастниками утечек, предоставляя атакующим доступ к коммуникациям. Например, в документе, описывающем программу NSA PRISM, сказано, что АНБ имеет доступ к пользовательским данным непосредственно на серверах, где они хранятся в открытом виде. В таких случаях оператор сервера выступает соучастником даже против своей воли. В программе NSA MUSCULAR множество соучастников предоставляет атакующим доступ к кабелям, соединяющим центры обработки данных, используемые такими компаниями, как Google и Yahoo. Поскольку обмен данными между центрами обработки ведётся без шифрования, соучастие промежуточных узлов позволяет АНБ собирать незашифрованные пользовательские данные.

5.2. Стоимость атак

Класс атаки	***Стоимость и риск для атакующего***
Пассивное наблюдение	Пассивный доступ к данным
Пассивный анализ	Пассивный доступ к данным и обработка
Активная	Активный доступ к данным и обработка
Статическая утечка ключей	Однократное взаимодействие
Динамическая утечка ключей	Постоянное взаимодействие, изменение кода
Утечка содержимого	Постоянное и интенсивное взаимодействие

[1]Certificate Authority.

Каждый из описанных в предыдущем параграфе типов атак сопряжён с некоторыми расходами и рисками. Эти издержки отличаются для разных атак и их понимание будет полезно для противодействия всеобъемлющим атакам.

В зависимости от типа атаки злоумышленник может быть подвержен некоторому риску от простой потери доступа до ареста и тюремного заключения. Однако для возникновения этих негативных для злоумышленника последствий он должен быть обнаружен и идентифицирован. Поэтому в первую очередь рассмотрим риск раскрытия и опознания атакующего.

Организация всеобъемлющей пассивной атаки в некотором смысле является простейшим делом. Базовым требованием является наличие у атакующего физического доступа к среде передачи и способа считывания данных из этой среды. Например, атакующий может сделать ответвление (tap) оптического кабеля, организовать «зеркало» порта в коммутаторе или просто прослушивать беспроводные сигналы. Потребность в ответвлениях для физического доступа или близость к каналам подвергает атакующего риску обнаружения. Например, отвод оптического кабеля или «зеркальный» порт могут быть обнаружены оператором за счёт роста затухания в оптическом кабеле или изменения конфигурации коммутатора. Естественно, пассивные всеобъемлющие атаки могут организовываться при содействии сетевых операторов, но и в этом случае имеется риск раскрытия взаимодействия оператора с атакующим.

Во многих отношениях организация активных всеобъемлющих атак похожа на организацию пассивных атак, но требует некоторых дополнений. Для активной атаки требуется более надёжный доступ в сеть, поскольку в таких атаках требуется не только считывать данные из среды, но и передавать данные в сеть. В приведённом выше примере с беспроводной сетью атакующему придётся выступать не только в качестве приёмника, но и в качестве приемопередатчика, что существенно повышает риск обнаружения (например, с помощью методов радиопеленгации). Активные атаки также более заметны на верхних уровнях сетевого стека. Например, атакующий, который пытается использовать подставные сертификаты, может быть обнаружен с помощью Certificate Transparency [RFC6962].

С точки зрения сложности для пассивной всеобъемлющей атаки требуется только извлечение информации из сети и её сохранение. Активные атаки, напротив, зачастую зависят от временных параметров для отправки в активные соединения пакетов от атакующего. Поэтому для активной всеобъемлющей атаки в ядре сети требуется оборудование, способное работать со скоростью среды (примерно 100 Гбит/с - 1 Тбит/с для ядра сети) для оценки возможности атаки и размещения связанных с атакой пакетах в высокоскоростных потоках трафика. Утечки основаны на пассивных всеобъемлющих атаках для доступа к шифрованным данным и получении от соучастника ключей для их расшифровки. В результате атакующий принимает на себя расходы и риск обнаружения пассивной всеобъемлющей атаки, а также дополнительный риск обнаружения за счёт взаимодействия с соучастником.

Активные атаки могут существенно различаться по связанным с ними расходам. Например, для активных MITM-атак требуется доступ в одну или несколько точек коммуникационного пути, позволяющий целиком видеть сессию и иметь возможность изменения или отбрасывания легитимных пакетов и вставки пакетов от атакующего. Похожие, но более слабые активные атаки MOTS[1] требуют доступа лишь к одной стороне сессии. В активной MOTS-атаке злоумышленнику достаточно возможности вставки или изменения трафика на сетевом элементе, к которому он имеет доступ. Хотя это может не дать полного контроля над сессией (как в MITM-атаке), злоумышленник может выполнить множество мощных атак, включая вставку пакетов, которые способны разорвать сессию (например, TCP RST), передачу подставных откликов DNS для перенаправления соединений TCP на нужный атакующему адрес (например, «DNS response race»), организацию перенаправления HTTP за счёт наблюдения TCP/HTTP на целевом адресе и вставки пакетов данных TCP с перенаправлением HTTP, а также другие зловредные действия. Например, система названная исследователями Great Cannon [great-cannon], может работать в полном режиме MITM для организации очень сложных атак, которые могут менять содержимое в процессе передачи, хотя общеизвестная система Great Firewall в China относится к типу MOTS и фокусируется на блокировке доступа для некоторых типов трафика и адресатов за счёт вставки пакетов TCP RST.

В этом смысле риск при организации статической утечки ключей ниже, чем при динамической. Для организации статической утечки атакующему достаточно один или несколько раз вступить во взаимодействие с соучастником - в идеальном случае достаточно разово получить секретный ключ. Для динамических утечек атакующий должен достаточно часто взаимодействовать с соучастником. Как отмечено выше, эти взаимодействия могут быть реальными контактами людей (например, встречи на конференциях) или виртуальными (например, внесение изменений в программы для сбора ключей. В обоих случаях существует риск разоблачения (например, сотрудники компании-соучастника могут отметить частое участие определённого человека в конференциях или подозрительные изменения программного кода).

Риск при организации утечки содержимого похож на риск при динамической утечке ключей. В контексте атаки с утечкой содержимого для злоумышленника также сохраняются издержки и риск, присущие пассивным всеобъемлющим атакам. При этом риск обнаружения взаимодействий с соучастников может оказаться даже выше. Объем содержимого коммуникаций обычно значительно (на несколько порядков) превышает объем ключей, используемых для шифрования. Поэтому в случае организации утечки содержимого возрастает риск связанный с обнаружением значительной загрузки каналов.

Следует также отметить, что в трёх последних случаях организации утечек соучастник также рискует быть раскрытым в части его взаимодействия со злоумышленником. Это может повлечь дополнительные расходы для атакующего на побуждение соучастника к содействию в атаке. Соответственно, область применения таких атак ограничивается возможностями найти для них соучастников. Если атакующий представляет правительственную организацию, он может вынудить на сотрудничество организации и людей в своей стране, но поиск иностранных соучастников может оказаться более сложным.

Как было отмечено выше, соучастники атак с утечками могут оказаться невольными - атакующий может просто украсть ключи или данные для организации атаки. В некотором смысле риск при таком подходе похож на риск при активном использовании соучастников. В статическом случае атакующему требуется сохранять своё присутствие в системах соучастника. Основным отличием является то, что риск в этом случае связан скорее с автоматическим обнаружением (например, системой детектирования вторжений), нежели с разоблачением людьми.

[1] Man-on-the-side - человек на одной стороне.

6. Вопросы безопасности

Этот документ описывает модель угроз для атак со всеобъемлющей слежкой. Защита от таких атак будет рассмотрена в других документах.

7. Литература

7.1. Нормативные документы

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <http://www.rfc-editor.org/info/rfc6973>.

7.2. Дополнительная литература

[dec1] Perlroth, N., Larson, J., and S. Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web", The New York Times, September 2013, <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>.

[dec2] The Guardian, "Project Bullrun -- classification guide to the NSA's decryption program", September 2013, <http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide>.

[dec3] Ball, J., Borger, J., and G. Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security", The Guardian, September 2013, <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>.

[dir1] Greenwald, G., "NSA collecting phone records of millions of Verizon customers daily", The Guardian, June 2013, <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

[dir2] Greenwald, G. and E. MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", The Guardian, June 2013, <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

[dir3] The Guardian, "Sigint -- how the NSA collaborates with technology companies", September 2013, <http://www.theguardian.com/world/interactive/2013/sep/05/sigint-nsa-collaborates-technology-companies>.

[DPRIVE] Bortzmeyer, S., "DNS privacy considerations", Work in Progress, draft-ietf-dprive-problem-statement-06[1], June 2015.

[great-cannon] Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R., and V. Paxson, "China's Great Cannon", The Citizen Lab, University of Toronto, 2015, <https://citizenlab.org/2015/04/chinas-great-cannon/>.

[pass1] Greenwald, G. and S. Ackerman, "How the NSA is still harvesting your online data", The Guardian, June 2013, <http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection>.

[pass2] Ball, J., "NSA's Prism surveillance program: how it works and what it can do", The Guardian, June 2013, <http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google>.

[pass3] Greenwald, G., "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", The Guardian, July 2013, <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>.

[pass4] MacAskill, E., Borger, J., Hopkins, N., Davies, N., and J. Ball, "How does GCHQ's internet surveillance work?", The Guardian, June 2013, <http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <http://www.rfc-editor.org/info/rfc1035>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <http://www.rfc-editor.org/info/rfc1918>.

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, DOI 10.17487/RFC1939, May 1996, <http://www.rfc-editor.org/info/rfc1939>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, DOI 10.17487/RFC3365, August 2002, <http://www.rfc-editor.org/info/rfc3365>.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, DOI 10.17487/RFC3501, March 2003, <http://www.rfc-editor.org/info/rfc3501>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <http://www.rfc-editor.org/info/rfc4303>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[1] Работа опубликована в RFC 7616. *Прим. перев.*

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <http://www.rfc-editor.org/info/rfc6962>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <http://www.rfc-editor.org/info/rfc7011>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

[spiegel1] Appelbaum, J., Horchert, J., Reissmann, O., Rosenbach, M., Schindler, J., and C. Stocker, "NSA's Secret Toolbox: Unit Offers Spy Gadgets for Every Need", Spiegel Online, December 2013, <http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html>.

[spiegel2] Appelbaum, J., Gibson, A., Guarnieri, C., Muller-Maguhn, A., Poitras, L., Rosenbach, M., Schmundt, H., and M. Sontheimer, "The Digital Arms Race: NSA Preps America for Future Battle", Spiegel Online, January 2015, <http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html>.

[TOR1] Schneier, B., "How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID", Schneier on Security, October 2013, <https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html>.

[TOR2] The Guardian, "'Tor Stinks' presentation -- read the full document", October 2013, <http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document>.

Члены IAB на момент одобрения публикации

Jari Arkko (председатель IETF)
Mary Barnes
Marc Blanchet
Ralph Droms
Ted Hardie
Joe Hildebrand
Russ Housley
Erik Nordmark
Robert Sparks
Andrew Sullivan
Dave Thaler
Brian Trammell
Suzanne Woolf

Благодарности

Спасибо Dave Thaler за список атак и их классификацию, руководителям направления Security Stephen Farrell, Sean Turner и Kathleen Moriarty за инициирование и поддержку обсуждения всеобъемлющих атак в IETF, Stephan Neuhaus, Mark Townsley, Chris Inacio, Evangelos Halepilidis, Bjoern Hoehrmann, Aziz Mohaisen, Russ Housley, Joe Hall, Andrew Sullivan, IEEE 802 Privacy Executive Committee SG и IAB Privacy and Security Program за их предложения.

Адреса авторов

Richard Barnes
Email: rlb@ipv.sx

Bruce Schneier
Email: schneier@schneier.com

Cullen Jennings
Email: fluffy@cisco.com

Ted Hardie
Email: ted.ietf@gmail.com

Brian Trammell
Email: ietf@trammell.ch

Christian Huitema
Email: huitema@huitema.net

Daniel Borkmann
Email: dborkman@iogearbox.net

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru