УДК 681.3

В. А. Киселенко

АНОНИМИЗАЦИЯ РАБОТЫ В ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ INTERNET

Исследована проблема анонимного доступа к ресурсам сети Internet. Приведена принципиальная схема архитектуры анонимизатора.

В наше время сеть Internet, перестав быть средством общения научного мира и специалистов по компьютерным технологиям, становится доступна обычному пользователю. Все большее число людей разных специальностей и социального статуса начинают пользоваться сетью. Сеть Internet является одной из наиболее интенсивно развивающихся и непрерывно усложняющихся сфер человеческой деятельности [1]. Таким образом, анонимизация работы в этой сети становится актуальной в условиях, когда некоторые организации или хакеры пытаются установить контроль за пользователями сети Internet.

В связи с этим в настоящей работе рассмотрены наиболее оптимальные и безопасные способы работы пользователей в глобальной компьютерной сети Internet.

Целью настоящей работы является исследование проблем анонимного доступа к ресурсам сети Internet и построения принципиальной схемы архитектуры анонимизаторов.

Защита частной жизни человека, пользующегося широкими возможностями доступа к информации в сети Internet, и интенсивный сбор данных, персонально идентифицирующих его личность, — это две конфликтующие друг с другом задачи [2]. Первоначально в конце 80-х годов XX в. в сети Internet появилась возможность анонимного FTP-доступа. Сервис FTP (File Transfer Protocol) позволяет пользователям одной машины получать доступ к файловой системе другой машины и получать (передавать) файл с одной машины на другую [3].

При анонимном FTP-доступе пользователю присваивается имя “anonymous” и пароль, совпадающий с адресом его электронной почты. При входе в систему с правами пользователя “anonymous” можно получить доступ к специально выделенному каталогу, который называется FTP-сервером. На FTP-серверах можно найти базовое программное обеспечение, утилиты и новые версии драйверов, программы испра-

вления (patches) замеченных в коммерческих программах ошибок, документацию, адреса, сборники и многое другое.

С развитием сети Internet и широким распространением web-браузеров сформировалось общее понятие анонимного доступа к информационным ресурсам глобальной сети. В настоящее время доступ к большинству таких ресурсов производится по схеме клиент–сервер.

Каждый доступ к информационному ресурсу обычно представляет собой цепочку событий "запрос — передача данных" (транзакций) между клиентом и сервером. Каждое такое событие характеризуется тремя координатами: адресом клиента, инициирующего запрос, временем подачи/исполнения запроса и адресом абонента, обслуживающего запрос (сервера).

Основные понятия. Анонимизацией запроса называется технология, позволяющая скрывать первые две из рассмотренных выше координат.

Как запрос клиента, так и ответ сервера могут содержать данные о клиенте, т.е. непосредственно информацию о нем, а также алгоритм и структуру данных, специфичную для определенных клиентов. Например, это могут быть аппаратные особенности клиента (разрешение монитора, скорость передачи трафика и др.), а также особенности используемого клиентом программного обеспечения (например, марка браузера, тип операционной системы и т.д.). Технология, позволяющая избегать утечки подобной информации, называется анонимизацией данных [4].

Последовательность транзакций при однократном или многократном использовании сетевого сервиса клиентом называется потоком запросов. Технологию разъединения транзакций в потоке будем называть анонимизацией потоков.

Анонимизация запроса при работе в сети Internet. Поскольку каждая транзакция обязательно имеет три рассмотренные выше координаты, единственный способ анонимизации запроса — это изменение всех или некоторых из этих координат.

Изменение адреса клиента в сети Internet означает изменение его IP-адреса независимо от того, является ли этот адрес принадлежащим пользователю адресом, динамическим адресом, выделяемым пользователю провайдером Internet-услуг, или корпоративным адресом, присваиваемым запросу при входе в глобальную сеть.

Изменение времени подачи/исполнения запроса — это задержка транзакции на некоторый срок (обозначим его T).

Ограничения на изменение координат следующие. Если информация, подлежащая анонимизации, является частью сетевого протокола

или алгоритма взаимодействия с сервером, ее изменение может привести к отказу в обслуживании запроса.

В сетевых сервисах, в которых используется в качестве учетной записи IP-адрес клиента, необходима уникальность измененного IP-адреса, вследствие чего затрудняется процесс анонимизации.

В сетевых сервисах, предоставляющих услуги on-line (т.е. с небольшим промежутком времени между запросом и его исполнением, а также между несколькими последовательными запросами), значительно уменьшается задержка T.

Одним из основных способов анонимизации данных является их шифрование. С помощью шифрования трафика не решаются в общем случае проблемы анонимизации запроса, однако можно достичь анонимизации данных в случае, когда у атакующего отсутствует доступ к дешифратору.

Анонимизирующие службы обычно называют анонимизаторами. Можно выделить следующие классы анонимизаторов [4]:

— *локальные* (в пределах выделенного пространства IP-адресов) — позволяют фильтровать возможную утечку данных, изменять алгоритм и структуру запроса, создавать график отложенных (off-line) запросов, а также подменять IP-адрес;

— *публичные* (в сети Internet с открытым или частным доступом) — отчасти позволяют фильтровать утечку данных и изменять структуру запроса, изменять IP-адрес клиента на принадлежащий администраторам сервера (с потерей однозначности IP-адреса), в пределах сервера производить подачу отложенных запросов;

— *распределенные* (в разных точках сети Internet) — помимо возможностей публичного анонимизатора позволяют производить полную подмену IP-адреса клиента и эффективную организацию анонимизации потоков.

В некоторых случаях имеется возможность организации защищенного туннеля между анонимизирующей службой (или клиентом) и сервером. Технология организации такого туннеля требует поддержки со стороны сервера; этот туннель обладает всеми свойствами шифрованного канала.

Анонимизирующий прокси-сервер. Прокси-серверы (англ. proxy — “доверенный, уполномоченный”) изначально используются только для одной цели — снижения трафика в сети. Такой сервер при передаче информации сохраняет ее для того, чтобы при повторном запросе этой информации она не проходила снова своим полным маршрутом, а сразу передавалась от прокси-сервера к пользователю. Основное назначение прокси-сервера — кэшировать (т.е. накапливать и сохранять) передаваемые данные.

Сразу после появления прокси-серверов их стали использовать для анонимного доступа к ресурсам сети следующим образом. Пользователь соединяется с прокси-сервером и передает ему информацию о запрашиваемом объекте (например, о странице на web-сервере). Когда прокси-сервер получает эти данные, он сам запрашивает этот объект (страницу) и после получения передает ее пользователю.

Прокси-сервер, обладая свойством кэширования, позволяет значительно деструктурировать поток запросов (увеличивая интервал T до "времени жизни" кэшируемого ресурса) и, обладая свойством анонимности, позволяет производить подмену IP-адреса.

Большинство прокси-серверов в сети Internet не предоставляют открытого доступа. Однако на сайтах, посвященных взлому и защите от него (как правило, на страницах хакерских сообществ), регулярно публикуются списки доступных анонимизирующих прокси-серверов.

Анонимизирующий сервер предоставляет два принципиально различных вида услуг: изменение политики безопасности и изменение координат запроса, которые осуществляются по-разному на двух участках пути следования сетевого запроса от абонента анонимизатора к конечному серверу: на участке "абонент–анонимизатор" и на участке "анонимизатор–сервер".

Если уровень защиты данных на компьютере абонента анонимизирующего сервера невысок, непосредственное пользование сетевыми службами в сети Internet может быть опасно. Например, при использовании служб с низким уровнем защиты учетных записей возможен перехват этих данных и последующий анализ трафика для их извлечения.

Маршрут прохождения пакета к серверу зависит от координат сервера (в том числе от времени запроса, так как карта маршрутизации в сети Internet постоянно изменяется). При этом вероятность появления перехватчика в какой-нибудь точке маршрута очень велика [5].

Количество возможных маршрутов нельзя предсказать, а следовательно, нужно заранее предполагать утечку информации. Для предотвращения утечки информации необходимы:

— сокращение количества точек потенциальной утечки информации;

— подмена приватных данных в потоке запросов другими (возможно, временными), утечка которых не приводит к возникновению угрозы безопасности абонента.

Рассмотрим способы изменения политики безопасности [6].

Повышение уровня защиты. Если пользователь не в состоянии поддерживать необходимый уровень безопасности сетевых запросов на

своем компьютере, это за него может сделать анонимизирующий сервер. При этом возможна утечка информации в канале между абонентом и анонимизирующим сервером. Далее в сети Internet запросы транслируются с необходимой защитой. Путь следования пакета от абонента к анонимизирующему серверу можно проконтролировать административно.

Смещение точки ответственности. Незащищенные запросы к сетевым службам ретранслируются анонимизирующим сервером с заменой данных, утечка которых возможна (например, учетных записей), на некоторые другие. Эти новые данные однозначно соответствуют исходным, при этом сервером гарантируется неразглашение таблицы этого соответствия, проверка безопасности трафика, основанного на использовании таких данных, и сокращение времени валидности этих данных (для уменьшения возможности присвоения учетных записей или длительного анализа трафика). Этот способ обеспечения политики безопасности поддерживается сетевыми почтовыми web-службами, в которых сервер берет на себя основную нагрузку по обеспечению безопасности, а также отвечает за анонимность использования его учетных записей.

Транслирующие оболочки. При использовании публичного, а не локального анонимизирующего сервера необходимо обеспечивать информационную защиту канала "абонент–анонимизатор". Наиболее просто в этом случае обучить пользователя применять какой-либо один способ защиты, а возможные запросы на предоставление сетевых услуг подавать с сервера, преобразуя их при помощи программных оболочек. Чаще всего для защиты используется протокол HTTPS (Secure HTTP), а в качестве оболочки — активная www-страница на сервере. Этот способ используется в дополнение к двум предыдущим, поскольку не оказывает влияния на состояние канала "анонимизатор–сервер".

Если клиент не желает разглашать координаты своего компьютера в сети Internet, он может воспользоваться анонимизирующей службой.

Необходимость в изменении координат запроса. Если стоимость (денежная или временна́я) обслуживания прямого запроса для пользователя при обращении к обычному серверу превосходит сумму стоимости обслуживания запроса с использованием анонимизатора, то этот запрос, безусловно, выгодно осуществлять через анонимизатор. Наименьшая стоимость обслуживания запроса — при использовании прокси-серверов (ретрансляторов запросов) или кэширующих прокси-серверов. В последнем случае помимо изменения координат запросов происходит существенное снижение загрузки канала "анонимизатор–сервер" за счет исполнения запросов абонента с использованием ин-

формации, хранимой на анонимизаторе, который в этом случае подменяет координаты не клиента, а сервера.

Необходимость в сокрытии координат запроса. Во многих случаях пользователю анонимизирующего сервера необходимо сокрытие его исходных координат. Это может потребоваться для следующих целей.

1. Для предотвращения последствий утечки информации. Если использование сервера так или иначе приводит к утечке информации, необходимо, чтобы эта информация была не привязана к исходным координатам абонента. В этом случае будет затруднено использование следующих данных:

— личных данных (учетных записей, адреса электронной почты, паспортных или биографических данных);

— корпоративных данных, т.е. информации о субъекте, административно ответственном за компьютер-абонент (учетных записей, используемых сервисов, графиков работы, структуры, местоположения, деловых контактов и т.п.).

2. Для отсечения обратной связи. При раскрытии реальных координат запроса происходит нарушение анонимности абонента в сети Internet.

Вследствие раскрытия координат абонента может произойти следующее.

Перегрузка сервера (*"спам"*). Если в зоне административной ответственности абонента находится какой-нибудь собственный сервис (например, почтовый), то раскрытие его координат (нередко наряду с частичным раскрытием или успешным моделированием учетных записей) может спровоцировать перегрузку этого сервиса пустыми или вредоносными запросами со стороны.

Взлом системы безопасности пользователя. Раскрытие координат абонента, система безопасности которого не обеспечивает необходимого уровня защиты, может спровоцировать попытку атаки на данные пользователя. Не меньшую опасность представляет раскрытие профиля операционной системы, поскольку при этом атакующему становится ясно, какое средство взлома необходимо применять. Результатом взлома может быть прекращение работы системы или сервера, утечка или изменение данных.

Захват координат компьютера. Раскрытие координат абонента (особенно если оно происходит одновременно с раскрытием некоторой профильной или учетной информации) позволяет атакующему воспользоваться присвоенными данными для получения доступа к сетевым службам, которые производят аутентификацию абонента на основе этих данных. Нередко захват координат сопровождается DOS-атакой (Denial of Service).

Учет трафика (в том числе легальный). Многие сетевые службы ведут учет трафика запросов, произведенных конкретным пользователем. Данные такого учета могут использоваться для начисления оплаты за услуги, для прекращения предоставления услуг (если объем обработанных запросов превышает определенную величину), для регулирования общего трафика (например, пользователи, подающие небольшое количество запросов, получают более высокий приоритет) и т.п.

Анализ трафика. В случае, если проведена деанонимизация потока запросов, содержание и структура потока могут служить источником утечки данных; в случае полного перехвата потока резко повышается вероятность дешифровки запросов, особенно при использовании слабого алгоритма шифрования, передаче ключей в симметричной схеме шифрования и обмене ключами с возможностью атакующему встроиться в поток в качестве ретранслятора — шифровании по алгоритму с открытым ключом. Кроме того, даже нерасшифрованный поток содержит в себе (возможно, косвенно) информацию о программном наполнении клиентского компьютера, графике работы, списке используемых служб и т.п.

В настоящее время существуют различные мнения об актуальности использования анонимизаторов. С одной стороны, анонимизаторы дают единственную реальную возможность свободной работы в сети Internet; с другой стороны, такие серверы, напротив, содействуют раскрытию приватной информации, так как позволяют контролировать проходящие через них потоки данных.

Таким образом, использование анонимизаторов приводит к накапливанию значимой информации в них (что является опасным для пользователя), но при этом обеспечивается анонимность работы во всем остальном пространстве сети Internet.

Архитектура анонимизатора. Прежде всего, при создании анонимизатора следует учитывать, что он не является основным средством для обеспечения тотальной анонимности. Такой сервер, например, не может обеспечить безопасность данных пользователя при наличии определенных классов следящих устройств. В качестве таких устройств могут выступать как достаточно простые программные средства (например, сканеры клавиатуры, которые ведут журнал всех нажатий клавиш в определенном сеансе связи), так и весьма сложные электронные следящие устройства (например, удаленные сканеры излучения мониторов). В данном случае анонимизатор является программно-аппартным средством, обеспечивающим защиту только от деанонимизации. Принципиальная схема работы анонимизатора представлена на рис. 1.

Рис. 1. Принципиальная схема работы анонимизатора

Анонимизаторы могут быть двух видов. Для работы одного вида анонимизаторов требуются только стандартные программные средства. Для работы другого вида анонимизаторов требуется установка дополнительного программного обеспечения. Каждый вид имеет свои достоинства и недостатки, при этом анонимизаторы разных видов могут использоваться одновременно.

В любом случае при разработке анонимизатора его следует разделить на две логически независимые части: принимающую заказы и выполняющую эти заказы. Данные первой его части придется раскрыть, поскольку они необходимы пользователю. Вторую же часть анонимизатора желательно реализовать в таком виде, чтобы она имитировала в сети машину обычного пользователя.

Далее при разработке архитектуры анонимизатора следует учитывать, что даже при использовании всех описанных выше способов обеспечения анонимности пользователя она все же может быть раскрыта. Защита пользователя может быть ослаблена, если сервер, к которому пользователь обращается с целью получения информации, получит возможность воздействовать на машину пользователя.

Архитектура разработанного анонимизатора представлена на рис. 2; здесь анонимизатор 1 предназначен для работы с компьютерами клиен-

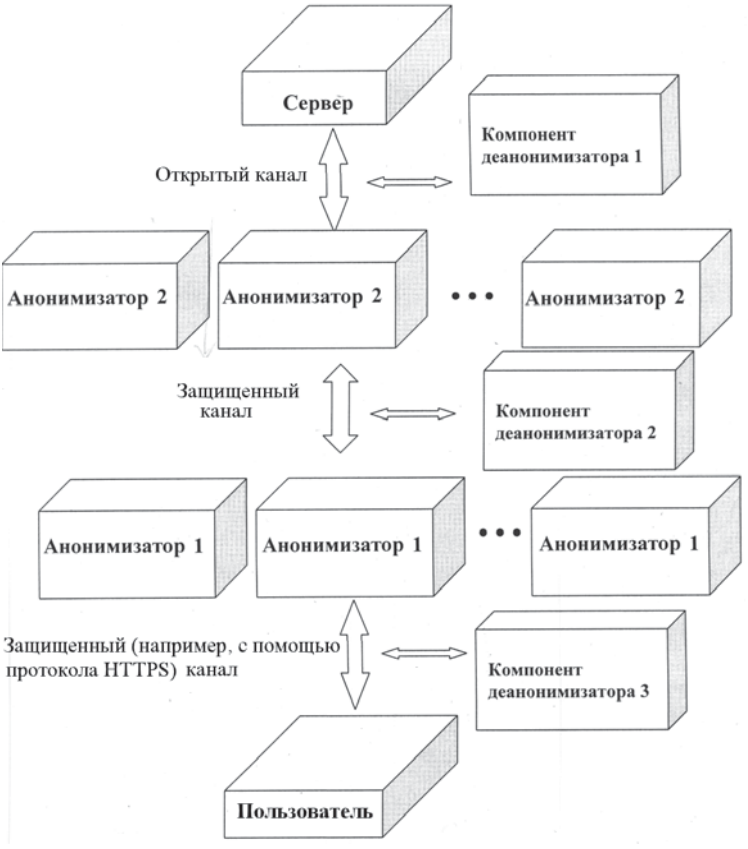

Рис. 2. Улучшенная архитектура анонимизатора

тов, а анонимизатор 2 — для работы с компьютерами анонимизаторов в сети Internet.

Таким образом, в настоящей работе определены основные понятия, касающиеся анонимной работы в сети Internet; рассмотрены различные виды общедоступных анонимизаторов (прокси-серверов); проанализированы способы сокрытия истинных координат пользователей сети Internet; разработана архитектура анонимизатора.

СПИСОК ЛИТЕРАТУРЫ

1. NUA Internet Surveys. – http://www.nua.ie/surveys/.
2. Войскунский А. Е., Бабанин Л. Н., Арестова О. Н. Социальная и демографическая динамика сообщества русскоязычных пользователей компьютерных сетей. Гуманитарные исследования в Интернете / Под ред. А.Е. Войскунского. – М.: Можайск-Терра, 2000. – С. 141–191.
3. Агентство “monitoring.ru” // http://www.monitoring.ru.
4. http://www.anonimyzer.com.

5. http://www.leader.ru/secure/who.html.

6. http://www.privasec.com.

Статья поступила в редакцию 25.03.2004

Владислав Андреевич Киселенко родился в 1962 г., окончил в 1983 г. Московский военный институт. Преподаватель Академии военных наук. Автор 10 научных работ в области компьютерной безопасности.

V.A. Kiselenko (b. 1962) graduated from the Moscow Military Institute in 1983. Teacher of Academy of Military Sciences. Author of 10 publications in the field of computer safety.

УДК 681.3

Н. В. Медведев

КОНЦЕПЦИЯ ОТКРЫТЫХ СИСТЕМ И ЗАДАЧА АУТЕНТИФИКАЦИИ В ЛОКАЛЬНЫХ СЕТЯХ

Рассмотрена задача обеспечения безопасности локальных компьютерных сетей, решаемая с помощью специализированных программных средств — протоколов сетевой аутентификации. Показаны возможности таких протоколов для подтверждения полномочий пользователей сети при организации доступа к информационным ресурсам на примере протокола сетевой аутентификации Kerberos.

Протокол сетевой аутентификации. За последние десятилетия значительно возросла роль компьютерных вычислительных систем и сетей. С их помощью обрабатываются огромные объемы различной информации. Также в последнее время многократно увеличилась степень открытости компьютерных сетей, их размеры и уровень их взаимозависимости, появились распределенные системы обработки информации колоссального размера. В связи с этим возникает необходимость разграничения доступа к обрабатываемой, передаваемой и хранимой информации с учетом специфики систем. Для решения задач этого типа был разработан протокол сетевой аутентификации Kerberos. В настоящей работе рассматриваются основные способы функционирования данного протокола, а также его расширений в операционной системе MS Windows 2000.

Протокол Kerberos является протоколом сетевой аутентификации, с помощью которого решается следующая задача: в открытой, незащищенной сети, в узлах которой находятся некоторые субъекты — пользователи, необходимо обеспечить их взаимную аутентификацию (т.е. подтверждение их полномочий). Протокол аутентификации Kerberos