УДК:004.7

Как следят социальные сети

Тенетилова К.К., Госуниверситет-УНПК, 11-ИБ

Diaspora — социальная сеть, созданная на добровольные пожертвования в 2010 г. по инициативе четырех студентов Нью-Йоркского университета как альтернатива Facebook, не обладающей, по мнению многих пользователей, достаточным уровнем конфиденциальности личных данных. Представляет собой распределенную децентрализованную сеть с открытым исходным кодом. Вместо контролируемых одной организацией вычислительных центров задача управления переносится на частные некоммерческие. Данная схема подразумевает работу большого числа персональных компьютеров с запущенными на них копиями управляющей программы, а также намного большего количества пользователей, обращающихся к сети только через браузер, доверяя содержать свои аккаунты владельцам серверов.

Главным отличием Диаспоры от других социальных сетей является факт принадлежности прав на пользовательскую информацию лишь самому пользователю. В проекте реализована возможность работы под псевдонимом, возможно бесследное удаление любой загруженной ранее информации, включая весь аккаунт.

Принципом функционирования Диаспоры является хранение данных пользователей не на удаленных серверах компании, а на личных компьютерах пользователей. Эта информация подвергается многократному шифрованию, в результате которого получение доступа к каким-либо данным при попытке несанкционированного доступа крайне затруднительно.

В Диаспоре использован криптографический контроль доступа, главным недостатком которого является практически не реализуемая возможность лишения каких-либо прав пользователя, ранее ими обладавшего. Для выполнения этой задачи необходим ресурсоемкий и долгий

процесс перешифрования всей информации новым ключом и распространение его среди всех членов группы за исключением лишенного прав на получение информации. В обратном случае наделения нового члена группы правами доступа достаточно передать ему ключи от всех старых файлов.

При отсутствии задачи регистрации на каком-либо конкретном сайте зарегистрировать аккаунт, называемый в Диаспоре seed («зерно»), можно на располагающемся в США крупном сервере https://diasp.org. На официальном сервере разработчиков проекта https://joindiaspora.com регистрация возможна только по приглашению одного из участников. Причина этого заключается в работе данного сайта в режиме закрытого альфа-тестирования. Полный же список серверов доступен по адресу https://podupti.me.

Каждый пользователь обладает возможностью запуска собственного сервера социальной сети, называемого pod («стручок») и позволяющего контролировать личные данные на основе полного доступа к ним. Необходимым условием является постоянное подключение к стабильной выделенной линии.

При выборе для регистрации одного из серверов вход на сайт в дальнейшем возможен только через него. Причина этого заключается в том, что схема распределенной социальной сети подразумевает хранение всех данных пользователя на том сервере, на котором была произведена регистрация его аккаунта. Вместе с тем, между зарегистрированными на различных серверах пользователями через шифрованный канал возможно как общение посредством личных сообщений, так и чтение и комментирование записей друг друга. [1]

Рассматривая перспективы развития проекта, можно отметить следующие возможные проблемы, связанные с ростом числа пользователей сети. Поды (pod – пользовательский сервер в Дисапоре) могут быть использованы мошенниками для сбора информации о пользователях в целях

использования ее в корыстных или криминальных целях, а также ее возможной перепродажи заинтересованным лицам. Возможно исчезновение хранимого не на защищенных от сбоев и проникновений серверах Google+ или Facebook, а на персональных компьютерах пользователей. Возникновение проблем в случае появления желания у пользователя переехать с одного пода на другой. Возможность массового распространения спама. Меньшая, в сравнении с доступной пользователям ресурсов с выделенным центром, скорость распределенной децентрализованной схемы.

Несмотря на позиционирование проекта как полноценной альтернативы Facebook, массового притока пользователей за полтора года существования проекта не произошло. Причинами этого явились как объяснимые на начальных этапах развития недоработки, так и привычка пользователей к социальным сетям, на которых они уже зарегистрированы, при отсутствии достаточного количества свободного времени на изучение новой.

Вместе с тем, учитывая перспективы развития информационной сферы, описываемые многими аналитиками как отказ от дальнейшего совершенствования персональных компьютеров с переводом всей вычислительной составляющей процесса в сеть, следует особенно подчеркнуть главную особенность Диаспоры. Если данный вариант развития будет реализован, одним из наиболее действенных способов обеспечения конфиденциальности личных данных станет распределенная социальная сеть, примером которой является Диаспора.

Эксперты утверждают, что Facebook отслеживает людей далеко за пределами собственного сайта и абонентской базы, так как все больше и больше сторонних сайтов используют кнопку «Мне нравится» и Facebook Connect. Исследователь приводит примеры того, как кнопка «Мне нравится» на любой странице может собирать информацию о пользователе и отправлять ее на Facebook.

Первый пример включает пользователей, у которых уже есть аккаунт на Facebook: Когда учетная запись создана, Facebook выдает cookies, содержащие уникальный идентификатор (ID) пользователя. Эти cookies способствуют отображению имени пользования в поле для логина при повторных визитах. При входе на Facebook через другое устройство используются временные cookies, которые заменяются cookies с тем же ID после входа в аккаунт». Это позволяет разным устройствам входить в аккуант с одним и тем же cookies. Каждый раз когда пользователь посещает Facebook, cookies отправляются HTTP-запросом на данный сайт. В результате чего Facebook знает кто хочет войти еще перед тем, как введен логин. Но cookies посылаются не только тогда, когда пользователь хочет зайти на Facebook, они посылаются каждый раз когда посещается сайт с кнопкой «Мне нравится».

«Facebook получает информацию о пользователе, включая его ID, через cookies. Когда же пользователь кликает на кнопку, он обеспечивает Facebook деталями логина и сообщением о том, что ему «нравится», опубликованном на страничке в профиле», — пишет Роозендааль. Но информация о пользователе отправляется на Facebook независимо от того, была ли кнопка «Мне нравится» реально активирована или нет. Все это достаточно пугающе – но не очень удивительно, потому что за Facebook давно закрепилась репутацией шпиона, который следит за своими пользователями.

Второй этап включает интернет пользователей, у которых нет аккаунта на FaceBook.Даже если у вас нет аккаунта на Facebook, вы далеко не защищены от сбора информации о вас. Если пользователь не имеет аккаунта на Facebook, cookies и ID пользователя недоступны. В этом случае HTTP GET запрос кнопки «Мне нравится» не выдает cookies. Тем не менее, когда посещается сайт, имеющий Facebook Connect, это приложение заводит cookies. С этого момента посещение других сайтов с кнопкой «Нравится» уже запрашивает данные пользователя из cookies». Это значит, что Facebook стащил еще одну порцию ценной информации, не спрашивая разрешения.

Если учесть, что 40 миллионов уникальных посетителей просматривали сайты с Facebook Connect за один только март 2009 года, и эти самые cookies действительны в течение двух лет, становится понятно почему и как распространяются данные пользователей.

Имея cookies можно отследить практически все действия в сети. Каждый сайт, который включает какое-либо содержимое Facebook, будет инициировать взаимодействия с его серверами, раскрывая информацию о посещаемом сайте вместе с cookies. Даже если вы никогда не были на Facebook – стоит вам зарегистрироваться и вся ваша история будет доступна социальной сети. При регистрации ваш временный ID посылается на Facebook как часть запроса для загрузки страницы, и сервер отвечает созданием уже нового идентификатора для зарегистрированного пользователя, связывая его со всеми вашими доступными данными.

Связь между этим старым и новым идентификатором совершается (тайно) серверами Facebook. Это значит, что вся собранная в прошлом информация о пользователе может быть привязана к только что созданному, чистому аккаунту на Facebook. С этого момента любые запросы содержимого Facebook будут сопровождаться уникальным ID пользователя[2]

Эксперты обнаружили уязвимость в соцсети, которая приводит к тому, что на сторонних сайтах проявляется информация о предпочтениях пользователей, о которых те упоминали лишь в личных сообщениях. По словам представителей сети, это стало побочным эффектом сканирования URL в личных сообщениях на предмет их проверки на наличие вредоносного контента. Как отметили эксперты, этим же грешит Gmail, который уже давно собирает всю информацию о пользователях, которую те оставляют в сервисах Google. Тем не менее, поисковый гигант делает это в соответствии со своим пользовательским соглашением, а вот Facebook не заявлял о том, что будет читать личную переписку.

Специалисты по кибербезопасности объясняют, что система сканирует личные сообщения, выбирая в них суждения, касающиеся чего-либо, например, чайника. И затем, зайдя в какой-либо интернет-магазин, можно увидеть под чайником свое мнение о нем.

Тем не менее, как говорят в Facebook, такой эффект является лишь единичной ошибкой, и никто не сможет увидеть информацию о личных сообщениях другого пользователя в открытом доступе. Сейчас данная уязвимость устраняется, сообщает mir24.tv.

В официальном заявлении Facebook говорится о том, что каждая ссылка, которая отправляется в личном сообщении, проверяется на содержание спама, поэтому роботы Facebook имеют доступ ко всему контенту, отправляемому пользователями, но, тем не менее, никто из людей не читает эти сообщения.[3]

Переполох начался в Интернете, когда летом 2011 года социальная сеть Facebook включила систему автоматического распознавания лиц. В результате стало возможным анализировать лица на загруженных фотографиях, а сервис захотел узнавать от пользователей, как зовут того или иного человека. Защитники персональных данных и гражданских прав были вне себя от возмущения. Новая функция расценивалась ими не только как вопиющее нарушение прав на личную информацию, но и дальнейший шаг к усилению тотального контроля. Социальную сеть Facebook, в которой насчитывается более 850 млн активных пользователей, можно считать самой большой картотекой лиц на нашей планете — а значит, и самой желанной приманкой для охотников за информацией.

Ежедневно в соцсеть загружается около 300 млн фотографий. Опция по распознаванию лиц на фотографиях, по версии компании, была запущена для того, чтобы помочь пользователям находить и обозначать друзей на фотографиях. Специальная программа анализирует снимки и предлагает пользователю различные варианты имен того или иного знакомого. В США

тестирование этой опции началось в декабре 2010 года, причем сразу с автоматической отметки пользователей на фотографии (без запроса их согласия), что вызвало протест у правозащитников.

Летом 2011 года опция заработала по всему миру, спровоцировав ответные действия со стороны властей нескольких стран, особенно европейских. В Гамбургском ведомстве по защите информации, например, заявили, что функция распознавания лиц в Facebook нарушает немецкий закон о неприкосновенности частной жизни, и пригрозили соцсети штрафами. Но это не остановило соцсеть.

Летом 2012 года Facebook приобрела израильскую Face.com, специализирующуюся на технологии распознавания лиц. Технология Face.com позволяет автоматически находить лица и узнавать уже известных сервису людей. Достаточно несколько раз указать человека на снимках, и сервис будет предлагать пользователю варианты того, кто изображен на новой фотографии, после чего пользователю останется выбрать нужное имя. [4]

Еще одна проблема кажется на первый взгляд странной, потому что у нее технологические корни. В последние два года наблюдается тенденция к использованию сокращенных URL-адресов. Например, большинство ссылок в социальной сети Twitter используют сервис сокращения URL t.co. Переходя по ссылке в twitter, пользователь сначала попадает на сервис сокращенных URL, а затем автоматически перенаправляется по целевому адресу. А это значит, что о переходе становится известно третьей компании. По сути, весь пользовательский трафик проходит через одну точку — t.co, что позволяет компании иметь мощные аналитические возможности для анализа поведения пользователей в Интернете.

Другая проблема — в том, что пользователь не знает, куда попадет, если сокращает URL. В обычной ситуации в браузере можно посмотреть, куда ведет ссылка: если она указывает на личный сайт компании, опасаться не

стоит, а если ведет на неизвестный сайт, нужно быть более осторожным. Но в ситуации, когда все идет на t.co, или на любой другой «сокращатель» URL, пользователю заранее неизвестно, куда он реально попадет. Хуже того, до последнего времени в половине «сокращателей» URL пользователь мог быть перенаправлен вовсе не на http, а на любой объект, для которого существует URL. Например, на зловредный javascript.[5]

Список литературы:

1. Diaspora. [Электронный ресурс]: (с изм. и доп.)- Режим доступа: http://ru.wikipedia.org/wiki/Diaspora; (дата обращения 26.11.12)
2. Сбор данных за пользователем. [Электронный ресурс]: (с изм. и доп.)- Режим доступа: http://www.xakep.ru/post/54130/?print=true; (дата обращения 27.11.12)
3. Face book читает личные сообщения. [Электронный ресурс]: (с изм. и доп.)- Режим доступа: http://www.mk.ru/science/article/2012/10/05/757620-facebook-vtayne-ot-polzovateley-rasstavlyaet-layki.html; (дата обращения 26.11.12)
4. Сбор данных через фотографии. [Электронный ресурс]: (с изм. и доп.)- Режим доступа:22sib.ru/articles/tag/системы; (дата обращения 26.11.12)
5.Сбор данных через переход по ссылкам. [Электронный ресурс]: (с изм. и доп.)- Режим доступа:http://i-business.ru/blogs/17157; (дата обращения 26.11.12)