сохранности и установленного статуса использования. Поэтому обеспечение безопасности информации и информационных процессов является обязательной функцией современных информационных систем [2].

Изучая принципы работы и защиты информации от несанкционированного доступа в Wi-Fi сетях становится понятно, что самые первые стандарты имели множество уязвимостей. Однако на их смену приходят новые, более совершенные стандарты, в которых усовершенствованы методы шифрования и аутентификации, благодаря чему, шанс защититься от взлома злоумышленников сильно возрастает.

Пользуясь Wi-Fi сетью следует помнить, что чем сложнее и надёжнее алгоритм шифрования информации, тем дольше она будет обрабатываться и передаваться, вызывая большие задержки в обработке информации [1].

Список использованных источников

1 Остапенко Д. В. Технология защиты информации в сетях Wi-Fi. — [Электронный ресурс]. — Режим доступа: http://bibliofond.ru/view.aspx?id=725189

2 Шамиль Ф., Маклаков В. И. Обеспечение информационной безопасности в системе «1С:Предприятие 8.1» // Сборник тезисов докладов студенческой конференция "IT security for new generation", 29 марта – 30 марта 2010 г., г. Москва, 2010. - С. 80.

ОТСЛЕЖИВАНИЕ ПОСЕЩЕНИЙ НА СЕТЕВЫХ РЕСУРСАХ

Автор: Рязанов Андрей Андреевич, студент 4 курса филиала «Протвино» государственного университета «Дубна»
Научный руководитель: Ковцова Ирина Олеговна, старший преподаватель

Аннотация

В статье рассматриваются вопросы отслеживания посетителей и приватности при посещении сетевых ресурсов. Представлен разбор некоторых популярных способов отслеживания посетителей.

Tracking of network visitors.

This article describes some ways to track visitors on network resources. Opposed to analytic WVT(Website visitor tracking) there discusses about identification of the visitors.

К текущему моменту развитие сетевых технологий достигло огромных высот. Абсолютное лидерство в сфере объединения сетей принадлежит IP-протоколу, обязательной частью которого является *IP*-адресация. Злоумышленники в целях нанесения вреда сетевым ресурсам могут использовать способы сокрытия своего реального *IP*-адреса.

Техническая администрация любых сетевых ресурсов, по большей части, имеет инструменты для отслеживания пользователей. Как правило, всеми ресурсами логируется время, *IP*-адрес и *url* страницы, чего явно недостаточно при использовании пользователем базовых методов анонимизации. Веб-мониторы, используемые веб-мастерами и аналитиками, обычно не предоставляют информацию о конкретных пользователях.

Такие посетители могут быть кликботами, кликающими по рекламным объявлениям ресурса и повышающими траты на рекламу. К тому же подобные

посещения страниц анализируются как нецелевые, что вредит популярности ресурса в поисковых системах. Обычно нецелевыми считаются посещения без кликов менее трёх секунд. В другом случае посетители, пришедшие через рекламные биржи могут быть не целевыми в случаях, когда идёт отображение в рекламных блоках и маленьких или невидимых *iframe*-окнах.

Отслеживание конкретных посетителей и анализ их перемещений могут выявить не оптимальность размещения материалов на ресурсе. Хуже, когда подобные визиты связаны с подбором паролей в техническую часть сайта. Отслеживание всех подозрительных действий часто не просто актуально в рамках ресурса, а необходимо для поддержания его актуальности и работоспособности.

Базовым методом слежения можно считать *cookie*. Конечно эффективнее внедрять их на самой странице, так как в большинстве профессиональных браузеров присутствует и чаще всего активна по умолчанию настройка об отклонении *cookie*-файлов сторонних ресурсов, что техническая администрация может обойти, используя систему перенаправлений, а также - опция по удалению новых *cookie* по окончанию сеанса. В ЕС (Европейский союз) даже есть закон, обязывающий предупреждать об их вреде, что увы не меняет ситуации. По разным данным (в зависимости от тематики ресурса) опцией блокировки сторонних *cookie* пользуется от 3 до 45% посетителей.

Почти также популярно отслеживание через *Flash*. Использование локально-общего хранилища (*Local Shared Objects*), которое предоставляет существенно большие возможности. Так как *Flash* един для конкретного компьютера он позволяет отслеживать пользователя вне зависимости от того, какими браузерами он пользуется. На текущий момент в большенстве браузеров используется специальный интерфейс для удаления *LSO*.

Третьим стандартным методом является отслеживание через *javascript*. Как правило используется *IP*-адрес, точное время на устройстве, версию браузера, разрешение экрана, версию ОС и список шрифтов. С помощью *Flash* можно дополнительно получить информацию об устройствах. По публичным данных *Flash* и *JavaScript* отсутствуют менее, чем у 10% посетителей. Их отсутствие уже обращает на данных посетителей повышенное внимание. Даже если посетитель отключит *Flash* и *java*, то остаётся множество возможностей связать его визиты.

HTML5 Local Storage является стандартным аналогом *Flash LSO*, с помощью которого также можно хранить информацию. Данное хранилище встроено во все современные браузеры, но его недостатками является очистка вместе с *cookies* и отсутствие кросс-браузерности.

Также популярен вариант с использованием браузерных баз данных - *IndexedDB* и *Web SQL Database*, как минимум одна из которых поддерживается в *FireFox*, *Chrorme* и *IE (Internet Explorer)*. Записи в них сохранятся даже при очистке *cookies* и *LSO*. При использовании нескольких вкладок – данные между ними могут быть переданы с помощью обьектной модели документов (*Document Object Model*), в свойстве которой *window.name* можно передать другим страницам до двух магабайт данных, которые доступны любым доменам. Единственным недостатком *DOM*, не позволяющим полностью перейти на него – является потеря данных после завершения сессии.

Достаточно популярен способ отслеживания браузеров через их кеш. Идиентификатор пользователя может быть вставлен в *url*-адрес какого-либо объекта. Браузер запоминает адрес, и при следующем посещении автоматически будет использовать адрес с *id*.

Помимо вставки идентификатора в адрес элемента он может быть зашифрован с самом элементе или его свойствах. Заметить подобное отслеживание многократно

сложнее.

С помощью доступа к истории посещений можно проверить на каких сайтах бывает пользователь. При использовании более пятиста ресурсов можно достаточно точно разделить пользователей на группы по интересам, а в случаях, когда ресурс посещается небольшим кругом лиц – точно выделить посетителя. В случаях если в истории есть данные о социальных сетях – возможна полная деанонимизация пользователя. Посещённые страницы можно определить по наличию их в кеше (по скорости ответа) либо по разнице цветов посещённых ссылок.

В случае, когда js (*JavaScript*) отключен – возможно замаскировать ссылки под капчу (*Completely Automated Public Turing test to tell Computers and Humans Apart*). По публичным данным уже в 2013-м году уже вводилось 320 миллионов капч каждый день. Под капчи могут быть замаскировано посещение основных ресурсов. С помощью ввода пользователем в поле отображаемых символов на основе истории его посещений. Может использоваться кеш *HTTP Strict Transport Security* – с помощью которого можно побитно сохранить *id* посетителя. На основе типов уникального набора запросов к включениям в страницу – браузер будет выдавать конкретного посетителя. С помощью HTML *canvas* можно получить данные о устройстве основываясь на уникальности отображения шрифтов.

Ну и одним из самых выделяющихся способов отслеживания посетителей является модификация *HTTP* запросов. Для хранения идентификатора можно использовать поля *Etag* и *Last-Modified*. При отправке запроса сервер помещает в поле *Etag* – идентификатор пользователя, а в *Last-Modified* – дату последнего изменения. При повторном запросе браузер передаст серверу значения *Etag* и *Last-Modified*. Если пользователь идентифицирован – сервер сообщит о актуальности закешированной страницы.

Каким браузером воспользуется пользователь, желающий остаться анонимным? Явно не *Safari*, у которого приём *cookies* не отключается даже в приватном просмотре. Использование семейства браузеров *Google* – также маловероятно, так как данная компания никогда не скрывала, что отслеживает посетителей в рекламных целях. *Internet Explorer* и *Microsoft Edge* в свете последних пользовательских соглашений от *Microsoft* – однозначно отпадают, так как последняя официально разрешает себе собирать и хранить все данные включая парольные комбинации и даже полную информацию по банковским картам. Использование устаревших браузеров – также не вариант. Регулярно открывающиеся уязвимости не способствуют приватности. Остаётся *FireFox* и специальные браузеры.

В случае *FireFox* используется *stun*-уязвимость, позволяющая выявить все назначенные *IP* адреса, которые укажут на все подсети, по которым вас модно будет опознать, не говоря о том, что данный протокол идёт в обход прокси-серверов, ну а специальные браузеры также не смогут спасти от анализа истории посещений и *fingerprint'*ов.

Да, можно отключить *Flash*, что отключит *LSO* и несколько затруднит *fingerprint*. Для избавления от *HTML5 LS* достаточно отказаться от *JavaScript* или *cookies*, что сделает невозможным использование современных приложений и повредит отображению большинства сайтов. От изменения *HTTP*-заголовков можно использовать прокси, переписывающие их. Кешу редиректов нет реально действующего способа, позволяющего уйти от отслеживания. Избавление от кеша *HSTS* делает браузер уязвимым к атакам со стороны.

Часть ресурсов предоставляет статистику, что *Flash* отключен менее, чем у половины процента их пользователей. Для полной коллекции уникальных характеристик можно попробовать использовать *TOR*. Плагин *Disconnect* не

оптимизирован под Российские условия. *Ghostery* – продаёт информацию о своих пользователях, *Self-Destructing Cookies* – очищает хранилища по завершении сессии, *NoScript* – блокирует *JavaScript* и *Flash*, но ничто из этого не способно противостоять грамотной комбинации следящих утилит.

На текущий момент не существуют приватности в её традиционном понимании в сети. Большинство попыток лишь усугубляют положение, но большинство пользователей просто не знает об этом, а на большинстве ресурсов – ограничиваются неким базовым стандартным набором. Так кто же получает пользу? Те, кто знает и применяет эти знания. Те, кто продаёт информацию о вас практически вам самим, зарабатывая на этом деньги. И нет никакой гарантии, что однажды взломав их к злоумышленникам не попадёт полное наше досье и все наши деньги.

Источники:

1) http://digishare360.com/blog/ - SEO. Marketing. Analitic.
2) http://sadda.ru/ - Капча. AdSence.
3) http://habrahabr.ru/post/216751/ - HSTS.
4) https://nakedsecurity.sophos.com/ - HSTS – supercookies. Fingerprint.
5) http://lurkmore.to/Капча - о психологическом влиянии, восприятии и причинах использования Капч.

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ОБЕСПЕЧЕНИЮ ЭФФЕКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ

DEVELOPMENT OF RECOMMENDATIONS FOR THE CREATIONS OF EFFECTIVE INFORMATION SECURITY IN ELECTRONIC DOCUMENT

Автор: Епифанов Сергей, 5 курс УЦ «Интеграция» МАИ.
Руководитель: ктн, доцент Красоткин Юрий Иванович, доцент МАИ.

Аннотация

В данной работе рассмотрены достоинства и недостатки электронного документооборота, а так же предложены рекомендации по совершенствованию безопасности электронного документооборота, как технической составляющей так и организационной.

In this paper we discussed the advantages and disadvantages of electronic document management, and proposed recommendations for improving the security of electronic documents, technical component and organizational.

Электронный документ (ЭД) — документ, созданный с помощью средств компьютерной обработки информации, который может быть подписан электронной подписью (ЭП) и сохранён на машинном носителе в виде файла соответствующего формата.

Сегодня 100% документов в офисе создается в электронном виде, но до сих пор более 80% созданных документов распечатываются (для согласования, ознакомления, запуска в работу). Разве может такой формат быть эффективным? Кажется, что внедрение системы электронного документооборота (СЭД) – самое разумное действие со стороны лиц принимающих решение [2].

Но у каждого новшества есть свои достоинства и недостатки [1].