УДК 003.26

РАЗРАБОТКА СЕТЕВОЙ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ «S&R»

Лалетин П.Ю., Переверзев В.С., Шуршилов А.А.
научный руководитель канд. техн. наук Шниперов А.Н.
Сибирский федеральный университет

Стеганография занимает свою нишу в обеспечении безопасности: она не заменяет, а дополняет криптографию. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты. Среди основных причин наблюдающегося всплеска интереса к стеганографии можно выделить принятые в ряде стран ограничения на использование сильной криптографии, а также проблему защиты авторских прав на художественные произведения ,интеллектуальную собственность и т.д. в цифровых глобальных сетях.

Стеганография - это метод организации связи, который собственно скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

В настоящее время в связи с бурным развитием вычислительной техники и новых каналов передачи информации появились новые стеганографические методы, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т. п. Это дает нам возможность говорить о становлении нового направления - компьютерной стеганографии.

Существует множество направлений современной стеганографии, таких как компьютерная стеганография, цифровая стеганография, сетевая стеганография, каждое со своими методами и алгоритмами. Каждое направление используется в зависимости от ситуации и имеющихся ресурсов.

Основными стеганографическими понятиями являются сообщение и контейнер. Сообщение – это секретная информация, наличие которой необходимо скрыть. Контейнером называется не секретная информация, которую можно использовать для скрытия сообщения. В качестве контейнера могут выступать обычный текст, файлы мультимедийного формата, сетевые протоколы и, даже, задержки передачи сообщений.

Существует множество программ и работ по методам цифровой стеганографии, где контейнерами являются мультимедиа-объекты и небольшое количество по сетевой. Идеей к разработке сетевой стеганографической системы стал контейнер случайных(псевдослучайных) данных, в котором недоказуема передача секретного сообщения.

Целями разработки стеганографической системы явились: проблема передачи ключей и актуальная проблема скрытой аутентификации. Система работает с помощью протокола SSL. Данный протокол широко используется в приложениях, работающих с сетью Интернет, таких как Веб-браузеры, работа с электронной почтой, обмен мгновенными сообщениями и IP-телефония (VoIP). Основные потребители данной системы – организации с филиалами, для передачи им секретных ключей или коротких сообщений, а также пользователям нуждающимся в таком комплексе для иных нужд. Система является клиент-серверной надстройкой над открытым программным обеспечением OpenSSL.

Разработан протокол передачи скрытых коротких сообщений (ключей) с использованием веб-сервера поддерживающий защищенное соединение HTTPS, в сегменте случайных данных протокола HandShake (TSL/SSL).

TLS дает возможность клиент-серверным приложениям осуществлять связь в сети таким образом, чтобы предотвратить прослушивание и несанкционированный доступ.

Когда соединение только устанавливается, взаимодействие идёт по протоколу TLS handshake. На этом этапе в фазе переговоров нас интересуют два сообщения, на которых основана система:

• Клиент посылает сообщение ClientHello, указывая последнюю версию поддерживаемого TLS протокола, случайное число и список поддерживаемых методов шифрования и сжатия, подходящих для работы с TLS;

• Сервер отвечает сообщением ServerHello, содержащим: выбранную сервером версию протокола, случайное число, посланное клиентом, подходящий алгоритм шифрования и сжатия из списка предоставленного клиентом;

Именно случайные числа отправляемые и клиентом и сервером мы будем использовать, как стеганоканал.

Алгоритм работы стеганографической системы

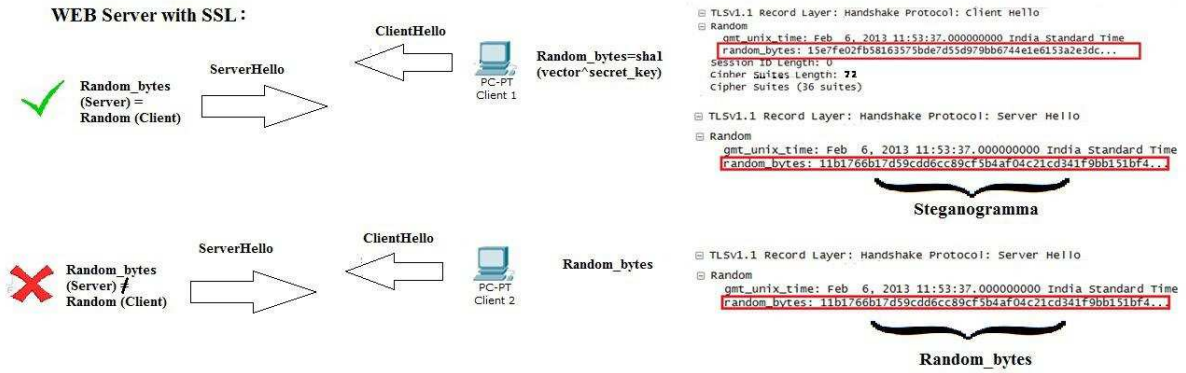
В состав системы клиентской и серверной части системы входят следующие конфигурационные файлы(.packet .vector .key .secret) содержащие данные:

.*vector* – вектор инициализации (число для установки соединения).

.*key* – ключ системы (для шифрования).

.*packet* – номер следующего пакета(количество переданных/полученных сообщений).

.*secret* – у сервера еще не переданная секретная информация, у клиента уже полученная.



Сервер и клиент имеют ключ (28 байт) и вектор инициализации псевдослучайной последовательности (28 байт).

• Клиент посылает сообщение **ClientHello**, где в поле **Random_bytes** передается хэш-функция SHA224 от сложения строк хранящихся в файлах .vector и .key у клиента

• Сервер отвечает сообщением **ServerHello.** В случае, если значение поля Random_bytes отправленное клиентом совпадает с результатом хеш-функции SHA224 сложения строк хранящихся в файлах .vector и .key на сервере, в поле random_bytes ответного сообщения сервер записывает стеганограмму, предварительно шифруя её с помощью специального алгоритма, описанного ниже, для неотличимости случайных данных и данных содержащих секретную информацию. Структура стеганограммы - 1 байт счетчик номера пакета взятого из файла .packet, 27 байт сообщение взятое из файла .secret(первые 27 байт) хранящегося на сервере.

Инкрементирует счетчик номера пакета, и записывает его в файл .packet. Выставляет новый вектор инициализации - равный полю random_bytes пришедшему от клиента, заменяет им файл .vector.

• Клиент получает сообщение, дешифрует его, если счетчик номера пакета в поле Random_bytes равен числу хранящемуся в файле .packet, записывает информацию в файл .secret, записывает в файл .vector свой вектор инициализации равный ранее отправленным данным в random_bytes.

Процедура повторяется до тех пор, пока нужная информация не будет передана.

Алгоритм шифрования:

Для шифрования используется функция сложения по модулю два, являющаяся обратимой. Размер криптоключа — 28 символов, ключ получается из текущего вектора инициализации и секретного ключа сторон и равен SHA224(mix(vector+secret_key)), где mix функция перемешивания символов. Выбран текущий алгоритм из-за своей простоты, а так же из-за постоянного изменения ключа и его размера равному размеру сообщения.

Анализ работы программы

Объем передаваемых секретных данных равен 27 байт за соединение. Количество соединений не ограничено. Например файл содержащий N символов будет передан за N/27 соединений. Но следует учитывать, что с возрастанием количества соединений проделываемых системой возрастает вероятность обнаружение противником стеганоканала. В разработанной системе предполагается, что секретное сообщение будет передано не более чем за три соединения, чтобы поддерживать заданный уровень защищенности и скрытности стеганосистемы.

Преимуществами разработанной системы S&R являются следующее:

- Недоказуемость - так как сообщение передается в поле случайных данных.
- Возможность использовать нашу систему как механизм скрытой аутентификации

Недостатки:

- Малый объем данных передаваемых с помощью одного сообщения
- Необходимость доработки методов повышающих отказоустойчивость системы

Заключение

Относительно нашего проекта хотелось бы сказать, что все поставленные задачи выполнены, а так же сохранено главное преимущество системы – недоказуемость её использования, система соответствует всем общепринятым положениям стеганосистем, и представляет собой готовый программный продукт. В нашей работе, мы показали, что для сокрытия информации могут использоваться уже устоявшиеся механизмы и методы, в нашем случае это процесс инициализации защищенного соединения, тем самым, область для применения, создания стеганосистем можно назвать безграничной.

В рамках развития проекта необходимо избавить её он недостатков и разработать дружественный интерфейс встраиваемый в браузер и модуль для современных веб-серверов.

1. http://ru.wikipedia.org/wiki/TLS (17.12.2013)
2. Request for Comments 5057 “Transport Layer Security (TLS) Session Resumption without Server-Side State”
3. Request for Comments 1750 “Randomness recommendations for security”
4. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика — К.: МК-Пресс, 2006.
5. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. — 2-е изд. — М.: Горячая линия — Телеком, 2013.