УДК 004.056; 004.415.24

Буценко Ю. П., Савченко Ю. Г. *Национальный технический университет Украины «Киевский политехнический институт» им. Игоря Сикорского*

СУЩЕСТВУЕТ ЛИ ИДЕАЛЬНОЕ СТЕГАНОГРАФИЧЕСКОЕ СОКРЫТИЕ ИНФОРМАЦИОННОГО ОБМЕНА?

Предлагается некоторый гипотетический (но легко реализуемый практически) сценарий тайной передачи сообщения, которая принципиально не может быть выявлена. Сценарий базируется на необходимости предварительного согласования между абонентами ключевой информации на основе так называемого “книжного шифра”, а сама передача скрываемого сообщения реализуется с помощью пустого контейнера, поэтому не может быть выявлена.

***Ключевые слова*:** стеганоанализ, “книжный шифр”, пустой контейнер

Butsenko Ju. P., Savchenko Ju. H. Is there a perfect steganographic hiding of information exchange? We consider the classical problem of steganography – organization of maximal hidden (secret) information transmission via insecure channels. There is a fundamentally important aspect in this task,i.e.protection from identification of hidden messages in a transmitted container. Existing steganalysis methods provide analysts with sufficiently effective tools to identify hidden embedding in different file types, therefore protection from detection of steg-message transmission is primary and most urgent. Some hypothetical (but easily realized in practice) script for the transmission of hidden message,which in principle cannot be detected, is proposed. The script is based on the need for prior coordination of key information between subscribers on the basis of the so-called "book cipher" and the transmission of hidden messages is realized using an empty container, so that it cannot be detected.

***Keywords*:** steganalysis, "book cipher", empty container

На вопрос, вынесенный в заголовок, по мнению авторов, можно дать уверенный положительный ответ. Такое, возможно, провокационное утверждение базируется на возможности использования некоторого гипотетического (но реализуемого практически) сценария скрытой от любого наблюдателя передачи сообщения.

Основная идея стеганоанализа в целом базируется на существовании некоторых закономерностей, связывающих отдельные фрагменты файла – контейнера. Как правило, такие закономерности могут быть выявлены только на статистическом уровне. Однако, если они существуют, то их можно и обнаружить. Отсюда можно сделать вывод, что статистический анализ достаточно ограниченной области контейнера может дать информацию о наличии (отсутствии) скрываемого тайного сообщения. Наиболее популярную группу методов составляют именно статистические методы. Наиболее простой из них состоит в χ -квадрат атаке, то есть в вычислении величины

$$\chi^2 = \sum_{i=1}^{n} \frac{(x_{\text{емп}}^{(i)} - x_{\text{теор}}^{(i)})^2}{x_{\text{теор}}^{(i)}} ,$$

где $x_{\text{емп}}^{(i)}$ та $x_{\text{теор}}^{(i)}$ − характеристики виявлених в контейнере закономерностей, которые относяться, соответсвенно, к общим закономерностям и фрагментов, “подозреваемых” в наличии встроенной скрываемой информации. Недостатком такого похода является резкое падение его эффективности при использовании стеганосистем с кодированием адресов встроенных битов и уменьшение объема вложения. Для других методов встраивания скрываемых сообщений, например, спектральных, то в этих случаях также существуют эффективные статистические (вероятностные) методы стеганоанализа, которые позволяют с высокой достоверностью обнаружить симптомы подозрения в модификации соответствующего файла-контейнера.

Прежде чем изложить предлагаемый сценарий, зафиксируем следующие базовые условия, общепринятые в стеганографии.

Акту передачи стегосообщения ***обязательно*** должен предшествовать этап согласования между отправителем и получателем сообщения некоторой адресной информации, указывающей местонахождение скрытого в контейнере вложения. Без выполнения этого этапа получатель ***не имеет никаких преимуществ*** перед стегоаналитиком условного противника. Это условие является принципиально важным и, как правило, принимается по умолчанию и без обсуждения. Предварительный этап выполняется либо по закрытому криптоканалу (“предварительному сговору”), либо путем согласования ключа по алгоритму Деффи-Хеллмана и передачей адресной информации опять-таки по криптоканалу.

Основная задача и цель стегонаграфических методов состоит в ***сокрытии*** самого ***акта передачи*** скрываемого сообщения. Задачу же ***защиты содержания*** сообщения успешно решается шифрованием. Поэтому все усилия стеганоанализа направлены на ***выявления*** наличия ***скрытого вложения*** в контейнере. Этой практически единственной и главной задаче стегоанализа посвящено большое число методов и работ. Более чем полный перечень публикаций по стеганоанализу содержится в [1], значительная часть из них базируется на анализе статистических параметров содержимого контейнера, например, [2-4].

После фиксации этих, по сути, ограничительных постулатов стеганографии рассмотрим предлагаемый сценарий идеального (на наш взгляд) стеганографического сокрытия. И еще раз подчеркнем, что первый этап передачи ключевой адресной информации принимается по умолчанию абсолютно надежным с точки зрения возможности вскрытия. Об этом свидетельствуют результаты применения современных алгоритмов и стандартов шифрования на протяжении уже нескольких десятилетий.

Предлагаемый сценарий рассмотрим на таком простом примере.

В качестве контейнера выберем, например, текстовый файл. Пусть предназначенное для передачи скрываемое сообщение также является текстовым файлом в том же алфавите. В соответствие с алгоритмом “книжного шифра” сформируем последовательность адресов, эквивалентных последовательности символов стегановложению. Выбранный произвольно текстовый файл является контейнером, а сформированная на его основе последовательность − адресной информацией, которая передается получателю на предварительном этапе.

Собственно акт передачи тайного сообщения состоит в пересылке получателю ***пустого*** контейнера. Очевидно, ни один метод стеганоанализа не сможет выявить в пустом контейнере каких-либо модификаций, свидетельствующих о присутствии посторонних вложений. Поэтому, по мнения авторов, можно утверждать, что такой сценарий реализует ***идеальное*** стеганографическое сокрытие информационного обмена, поскольку акт передачи невозможно обнаружить.

В дискуссии при обсуждении предлагаемого сценария чаще всего возникает такое возражение. При его реализации, по сути, стеганографический информационный обмен подменяется криптографическим при использовании архаичного на сегодня «книжного» шифра. В этом случае уже после первого предварительного этапа обмена получатель (и стеганоаналитик противника) может извлечь скрытое вложение. Но ведь это возможно только в том случае, когда будет известен файл пустого контейнера!

Для сравнения рассмотрим “параллельно” обычный стеганографический сценарий и сценарий “пустого контейнера”.

Обычный сценарий	Сценарий с пустым контейнером
Этап 1. Загрузка контейнера. Формирова-ние последовательности адресов модифици-рованных битов контейнера и передача получателю последовательности по закры-тому либо криптографическому каналу.	***Этап 1.*** Формирование последовательности адресов битов (байтов) выбранного контейнера, соответствующих вложению, и передача ее получателю по закрытому либо криптографическому каналу.
Этап 2. Передача загруженного контейнера по открытому каналу	***Этап 2.*** Передача пустого контейнера по открытому каналу

Легко видеть, что различие между сценариями лишь, в отсутствии, фактически, загрузки в передаваемом получателю контейнере.

Следует также отметить, что, в принципе, передача пустого файла контейнера не является обязательной при наличии у получателя некоторой условной библиотеки контейнеров, которые по предварительному согласованию между получателем и отправителем могут быть использованы в информационном обмене. В этом случае получателю достаточно сообщить идентификатор файла. Важно также, что в отличие от классической стеганографии в рассматриваемом сценарии могут быть использованы в качестве контейнеров текстовые файлы, что по многим причинам является предпочтительным и удобным технологически.

Не останавливаясь на других особенностях использования пустого контейнера для передачи скрытых сообщений, в заключение заметим, что авторам хотелось бы, чтобы данное краткое сообщение рассматривалось, в основном, как приглашение к обсуждению и дискуссии.

Список используемой литературы

1. Кошкина Н. В. Обзор и классификация методов стегоанализа / Н. В. Кошкина // Управляющие системы и машины. –2015. – №3. – С. 3-12.

2 Губенко Н. Е. Анализ особенностей методов цифровой стеганографии для защиты информации, передаваемой по открытым каналам / Н. Е. Губенко, Д. С. Сипаков // Информатика и кибернетика. – 2015. – № 2. – С. 28-37.

3. Andrew D. Ker. Steganalysis of LSB Matching in Grayscale Images / Andrew D. Ker // IEEE signal processing letters. – June 2005. – Vol. 12, No. 6.

4. Буценко Ю. П. Статистический подход к выявлению скрытого сообщения в стегоконтейнерах графического и аудио формата / Ю. П. Буценко, Н. С. Греков, Ю. Г. Савченко // Сучасний захист інформації. – 2015. – №1.

References

1. Koshkina N. V. Review and classification of steganography methods // Upravliaiushchiie sistemy i mashiny. – 2015. – №3. – PP. 3-12.

2 Hubenko N. Ye., Sipakov D. S. Analysis of features of methods of digital steganography for a protection information, transferrable on the open channel // Informatika i kibernetika. – 2015. – № 2. – PP. 28-37.

3. Andrew D. Ker. Steganalysis of LSB Matching in Grayscale Images / Andrew D. Ker // IEEE signal processing letters. – June 2005. – Vol. 12, No. 6.

4. Butsenko Yu. P., Hrekov N. S., Savchenko Yu. H. Statistical mrthod to the exposure of the hidden graphic and audio report in stegocontainers // Suchasnyi zakhyst informatsii. – 2015. – №1.

Автори статті

Буценко Юрій Павлович – кандидат фізико-математичних наук, доцент кафедри математичного анализу і теорії ймовірностей, Національний технічний університет України «Київський політехнічний інститут» імені Ігоря Сікорського, Київ. Тел. +380 (50) 207 34 42. E-mail: armchairdoc@yandex.ua.

Савченко Юлій Григорович – доктор технічних наук, професор кафедри звукотехніки і реєстрації інформації, Національний технічний університет України «Київський політехнічний інститут» імені Ігоря Сікорського, Київ. Тел.: +380 (95) 838 97 69. E-mail: ssaavvaa@ukr.net.

Authors of the article

Butsenko Yurii Pavlovych – candidate of sciences (physics and mathematics), associate professor of probability theory and mathematical analysis department, Ihor Sikorsky National Technical University of Ukraine “Kiev Polytechnic Institute”, Kyiv. Tel.: +380 (50) 207 34 42. E-mail: armchairdoc@yandex.ua.

Savchenko Yulii Hryhorovych – doctor of sciences (technic), professor of chair of sound technologies and information registration department, Ihor Sikorsky National Technical University of Ukraine “Kiev Polytechnic Institute”, Kyiv. Tel. +38 (095) 838 97 69. E-mail: ssaavvaa@ukr.net.

Дата надходження
в редакцію: 18.12.2016 р.

Рецензент:
доктор технічних наук, професор М. А. Віноградов
Національний авіаційний університет, Київ