Глава II.

Компьютерная стеганография

 В предыдущей главе мы дали определения всем основным понятиям в стеганографии, рассмотрели её методы до изобретения компьютеров и выявили её отличия от криптографии. Но каковы принципы нынешней, компьютерной, стеганографии?

 В современной компьютерной стеганографии можно выделить четыре основных положения:

* Методы скрытия должны обеспечивать аутентичность и целостность файла.
* Предполагается, что противнику полностью известны возможные стеганографические методы.
* Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации - ключа.
* Даже если факт скрытия сообщения стал известен противнику, извлечение самого секретного сообщения должно представлять сложную вычислительную задачу.

 В настоящее время стеганографические системы активно применяются для решения различных задач. Давайте рассмотрим их более подробно.

 Во-первых, данные системы используются для незаметной передачи информации. Это классическая задача стеганографии. Она не требует пояснений.

 Во-вторых, с помощью стеганографических систем можно не только скрытно передавать информацию, но и хранить её. Данная задача реализуется на носителях информации, а не в каналах связи. Причем многие носители обладают большой избыточностью, которую можно использовать. Похожей задачей является недекларированное хранение информации.

Многие информационные ресурсы позволяют хранить данные только определенного вида. Однако можно использовать стеганографию для хранения данных в других форматах.

 Ещё стеганографические системы можно использовать для защиты исключительного и авторского прав. Благодаря данным системам существует возможность определить уникальный идентификатор покупки, дату/время покупки и другую информацию. С их помощью можно защитить каждую копию контента от несанкционированной публикации, продажи или использования.

 Технология защиты подлинности документов может быть такая же, как и для защиты авторского права. Только в данном случае стеганография используется не для подтверждения авторства, а для подтверждения подлинности документа. Документ, не содержащий стеганографические водяные знаки считается «ненастоящим», поддельным. Подробнее о водяных знаках написано в третьей главе.
 В системе электронного документооборота можно использовать индивидуальный отпечаток внутри \*.odt, \*.docx и иных документах при работе с ними пользователем. Для этого должны быть написаны специальные приложения и/или драйверы, которые установлены и работают в системе. Если данная задача выполнена, то с помощью индивидуального отпечатка можно будет опознать, кто работал с документом, а кто нет. В данном случае стеганографию нельзя делать единственным критерием, но как дополнительный фактор идентификации участников работы с документом она может быть полезна.
 Стеганография может быть применима для предотвращения утечек информации. В отличие от индивидуального отпечатка, в данном применении стеганографии при создании документа, содержащий конфиденциальный характер, вкрапляется определенная метка. При этом метка не изменяется, вне зависимости от количества копий и/или ревизий документа. Для того, чтобы извлечь метку необходим стегоключ. Стегоключ, разумеется, держится в тайне. DLP-система, перед одобрением или отказом выдать документ вовне, проверяет наличие или отсутствие водяного знака. Если знак присутствует, то система не разрешает отправлять документ вовне системы.

 Стеганография может быть применима для доставки какого-либо управляющего сигнала системе. Если система может находится в различных состояниях и мы желаем, чтобы противник даже не догадался о том, что система перешла в другое состояние, мы можем воспользоваться стеганографией. Использование только криптографии, без стеганографии, может дать противнику информацию о том, что что-то изменилось и спровоцировать его на нежелательные действия. Данная задача невероятно актуальна в военной сфере. Данная задача может быть актуальной и для преступных организаций. Соответственно, правоохранительные органы должны быть вооружены определенной теорией по данному вопросу и способствовать развитию программ, алгоритмов и систем по противодействию данного применения стеганографии.
 Стегосообщение может содержать данные, подтверждающие корректность передаваемых данных контейнера. Задача подтверждения достоверности является актуальной, если противник имеет необходимость подделать данные контейнера; по этой причине данное применение не нужно путать с защитой подлинности документов. Данная проблема имеет множество классических решений, в том числе криптографических. Использование стеганографии является ещё одним способом решить данную проблему.
 Существует ряд документов, для которых важна целостность. Ее можно осуществить резервированием данных. Порой существует необходимость иметь документы в таком виде, чтобы невозможно было одну информацию отделить от другой информации. Это могут быть медицинские снимки, содержащие информацию об имени, фамилии и иных данных пациента, или скриншот игры WoW, в который внедряется имя пользователя, время снятия и адрес сервера. Стеганография также в состоянии справиться с данной задачей.

 Стеганографическое отслеживание в некоторой степени похоже на индивидуальный отпечаток, только цель стоит иная — поймать злоумышлинника, который «сливает» информацию. В реальном мире можно привести примером «меченные деньги». Они используются правоохранительными органами, для того чтобы преступник, получивший деньги за какую-либо незаконную деятельность, не мог бы потом заявить, что эти деньги были у него до сделки.

 Методы стеганографии для каждого типа информации свои. Наиболее популярный тип, используемый стеганографией – изображение.

 Стеганографические методы, используемые при работе с изображениями, делятся на две группы.

 Методы первой группы предполагают небольшую модификацию изображений. Данные методы обычно используют побитную модификацию, например, изменение наименьшего по значению бита. Эти методы относят к числу простых, они легче поддаются декодированию и допускают потерю информации при тех или иных преобразованиях файла-носителя, скажем, при сжатии. Из трех наиболее популярных алгоритмов сжатия изображений: BMP, GIF и JPEG — чаще используют первые два. Они отличаются меньшими потерями.

 Методы второй группы используют трансформацию изображений. В методах этой группы используют тригонометрические преобразования или наложения, незаметные для глаз. Эти методы более устойчивы, вложенная информация не теряется при преобразованиях, поэтому их чаще всего применяют при создании цифровых водяных знаков. Обычно при этом используются файлы формата JPEG.

 Метод скрытых гарнитур шрифтов в некоторой степени похож на побитную модификацию изображений. Делаются малозаметные искажения в очертаниях букв, которые будут нести смысловую нагрузку. Так, в документ Microsoft Word можно вставить похожие символы, содержащие скрытое послание.

 Сообщения можно передавать и в звуковом формате. Их можно послать, используя шумовое кодирование. Оно будет трудно определимо на фоне аппаратных шумов в телефонной линии или сетевых кабелях.