УДК 34::62

ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СТЕГАНОГРАФИИ

[1] Ж.Мусаев

Аннотация. Эта статья является кратким введением в стеганографию и отвечает на вопросы: что такое стеганография, как ее можно использовать, и ее значение для безопасности информации. Конечно же, наряду с шифрованием, стеганография является одним из основных методов сохранения конфиденциальной информации.

Ключевые слова. Криптография, стеганография, безопасность, шифрование, утилиты.

В процессе исследования стеганографии в рамках компьютерной безопасности, становится очевидным, что она, по существу, является чем-то новым, так как возникла еще во времена древнего Рима. К примеру, в древнем Риме и Греции тексты обычно писались на воске, которым заливали каменные таблички. Если отправитель информации хотел скрыть сообщение (например, в целях военной тайны) он использовал стеганографию: воск скребался, и сообщение либо вставлялось, либо писалось прямо на таблице, затем воск наливался поверх послания. Таким образом, скрывалось не только значение сообщения, но и оно общее существование.

Dictionary.com пишет, что стеганография (также известная как "*steg*" или "*stego*") - это «искусство написания цифр или букв, которые не понятны никому, кроме человека, у которого есть ключ - cryptography».

В компьютерный мир стеганография вошла как метод сокрытия определенного сообщения в другом (которое есть заведомо большим), таким образом, что невозможно увидеть присутствие или смысл скрытого сообщения. А если сказать по точнее, то стеганография это в скрытие самого факта информации. Например в нынешнее время стеганографию используют через программные обеспечения мультмедийном формате, а именно через картинки, музыку или видеофайлы.[1, № 3]

Для чего используется стеганография?

Как и большинство утилит по безопасности, стеганография может использоваться для разных целей. Законные цели включают водяные знаки на изображениях в целях защиты прав собственности. Цифровые подписи (также известны как fingerprinting (отпечатки), указывают в основном на объекты, защищенные законом об авторском праве) являются обычными для стеганографии, так как содержатся в файлах, являясь частью их, и потому сложно обнаружимы обыкновенным человеком. Стеганография может также использоваться для замены одностороннего значения хэша (когда берется длина вводимой переменной и создается статическая длина строки на выходе, для того, чтобы подтвердить, что вводимая переменная не была изменена). Также стеганография может быть использована для добавления меток на онлайновые изображения (как тикеры для баннеров). Наконец, стеганография может использоваться для сохранения ценной информации, в целях защиты данных от возможного саботажа, кражи или несанкционированного просмотра.

К сожалению, стеганография может быть также использована для незаконных целей. Например, при попытке украсть информацию, существует возможность скрыть ее в другом файле, или файлах и послать ее в виде невинного письма или лифайла. Более того, люди, чье хобби – коллекционирование порнографии, и что еще хуже, на своем винчестере, могут использовать стеганографию для сокрытия доказательств. И как говорилось ранее, он нам может использоваться в целях террористов как средство скрытого общения. Конечно же применение стеганографии может быть как законным так и незаконным.[2, с. 288]

Инструменты стеганографии

Существует масса инструментов пригодных для стеганографии. Важное различие, которое должно быть сегодня проведено среди доступных инструментов стеганографии – это те, которые стеганографируют, и те, что стеганализируют (метод обнаружения стеганографии и уничтожения первоначального сообщения). Стеганализ основывается на этом аспекте, поскольку расшифровка сообщения без ключа является проблематичной.

Подробное рассмотрение инструментов стеганографии не входит в рамки данной статьи. Хотя существует очень много источников для получения инструментов стеганографии в Интернете. Рекомендуем в поисках подобных средств обратится в соответствующий раздел на нашем сайте.

Для знакомства со средствами стеганографии рекомендуем сайт Нейла Джонсона (*Neil Johnson's Steganalysis site*). Также можно посетить сайт Нильса Провоса (*Niels Provos*), хотя он в данный момент переезжает, как и тот, следить за его развитием.

Большое количество утилит работают под разными ОС - *Windows, DOS, Linux, MacOS, Unix*: вам будет из чего выбирать.

Принципы работы стеганографии

Чтобы показать, насколько легка стеганография, мы начнем с загрузки более чем популярной бесплатной утилиты - F5, затем и спробуем утилиту под названием *SecurEngine*, которая прячет сообщение в большом текстовом файле и напоследок познакомимся с программкой, которая скрывает файлы в MP3 формате – так называемая - *MP3Stego*. Также мы протестируем коммерческий продукт *Steganos Suite*.

F5 была разработана Андреасом Вестфилдом (*Andreas Westfield*) и работает как *DOS* клиент. Также была разработана «парочка» *GUI*: первая утилита - *"Frontend"*, созданная Кристианом Вонном (Christian Wohne), и вторая - *"Stegano"*, чьим автором является Томас Бьель (*Thomas Biel*). Мы и спытывали F5, *beta version 12*. Оказалось, очень легко закодировать сообщение в формате *JPEG*, даже когда релиз немецкий. Пользователь очень легко может это сделать, следуя инструкциям мастера, указывая путь к картинке (мы использовали простой текстовый файл, созданный в блокноте), вводя ключевое слово. Как вы можете сами убедиться, сложно сказать под двумя следующим картинкам, содержатся ли в них вложенное сообщение или нет.

Конечно же, вложенный файл был очень маленьким (состоял всего из одной строки *"This is a test. This is only a test."*), а кто-то слишком много пикселей пришлось заменить, чтобы спрятать сообщение. А что будет, если мы попытаемся спрятать большой документ? F5 работает только с текстовыми файлами. При попытке спрятать более объемный «вордовский» файл, то хоть программа и восприняла его, но восстановить не сумела. Тем не менее, большие файлы похоже тоже можно, как и маленькие, вкладывать в изображения.[3, с. 272]

SecurEngine не выглядит, как профессиональная утилита, которая способна спрятать текст в изображении. Когда мы спрятали своем маленькое сообщение в большом текстовом файле, то обнаружили лишний символ («я») в конце зашифрованного файла. Такого символа не было в оригинале. SecurEngine позволяет пользователям лишь спрятать изображение и (или) зашифровать. Пробное предложение было закодировано и декодировано без всяких проблем. *SecurEngine*

т акжев ключает вс ебя н струменты д ляб олее н адежного у ничтожения ф айлов.

У тилита *M P3Stego*, к оторая п озволяет п рятать д анные в файлах ф ормата *MP3*, с работала о чень хорошо. Процесс ш ифрования п роисходит т аким о бразом: в ы ш ифруете ф айл (екстовый н апример), к ак *W AV* файл, который з атем преобразовывается в формат *M P3*. Е динственная п роблемка, к оторая в озникла – ч тобы з ашифровать д анные б ольшого р азмера, н еобходимо и метьп ропорциональный к к оличеству д анных файл. Например, маленькое с ообщение, к оторое мы и с пользовали в предыдущих о пыта х оказалось с лишком б ольшим для *WAV* ф- айла (размер *WAV* -ф айла составлял 121KB, а т екстового файла – 36 байт). Д ля з авершения о пыта пришлось сократить текстовый файл д о 5 байт – т олько слово «*t est*». Мы нашли с оответствующий ф айл размером 627 KB. К онечный MP3 ф айл з анял 57KB.

Steganos S uite – это к оммерческий п акет, объединивший м ножество у тилит. В д ополнение к и зящной й деструктивной ф ункции т рассировки (д ля Интернета) и у тилиты д ля у ничтожения ф айлов, п рограммат акже е о бладает т ак н азываемым ф айловым м енеджером, ч то п озволяет пользователям ш ифровать и с крывать ф айлы н а с воем в инчестере. Пользователь в ыделяет п апку и ли ф айл, к оторые с ледует сокрыть и ф айл – « носильщик» информации - о бязательно г рафический и ли м узыкальный. П рограммат акже п озволяет с амим п ользователям с оздавать ф айлы п ри п омощи м икрофона и ли с канера. Е сли у в ас н ет п одходящего ф айла, в строенный ф айловый м енеджер умеет и скать нужный ф айл н а в ашем в инчестере. Эта утилита, в о тличие о т т е х, к оторые м ы т естировали, с пособна р аботать с р азными файловыми форматами (*d ll*, *dib*). Так что, если в ам н еобходим качественный п родукт для шифрования информации, то в ам придется в ыложить деньги з а к оммерческий п акет.[4, с. 153]

С теганография и б езопасность

К ак р анее у поминалось, с теганография я вляется э ффективным м е тодом с окрытия д анных и з а щиты и х о т н есанкционированного или н е ж елаемого п росмотра. Н о в се ж е э то л ишь о дин из с пособов з ащиты информации. Возможно, лучше было бы использовать с теганографию с овместно с д ругими м етодами сокрытия д анных, что с делало бы в озможным м ногоуровневую б езопасность. Далее п риведены н екоторые и з альтернативных методов с окрытия данных.

- **Шифрование** – процесс преобразования информации посредством ряда м атематический операций. Результатом

шифрования является зашифрованный текст. Зашифрованные данные могут быть прочитаны лишь при условии наличия необходимого ключа. Шифрование прячет данные, но усложняет их

- **Скрытые директории (*Windows*)** - *Windows* предлагает возможность скрытия файлов. Использовать эту возможность очень легко: просто в свойствах папки или файла проставить атрибут «скрытый» и надеяться, что никто не отобразит в сетипы файлов в эксплорере.
- **Скрытые директории (*Unix*)** – на платформах ***Unix*** в существующих директория, содержащих множество файлов, как, например, */dev* или создав свою директорию, в названии которой использовав три точки, (обычно используют одни лишь).
- **Скрытые каналы** – Некоторые утилиты используются для передачи шифрованных данных, которые внешне выглядят как обыкновенный сетевой трафик. Одна из таких утилит – *Loki* – способна скрывать данные в ICMP трафике. [5, с 135]

Защита от теганографии

К сожалению, все методы, о которых мы говорили, могут также использоваться с целью незаконных, несанкционированных или нежелательных действий. Возможность определения или предупреждения утечки информации является тривиальной задачей. Если кто-то решил для скрытия данных использовать стеганографию, то единственным способом обнаружения является активное наблюдения за специальными файлами и удача. Иногда активные меры безопасности могут дать ответ на поставленный вопрос – жесткие политики на установку несанкционированного программного обеспечения.

Использование уже имеющихся утилит для контроля над сетевым трафиком также может оказаться полезным. Системы обнаружения вторжения могут помочь администратору в определении нормального трафика и, таким образом, увидеть аномалии, например, при передаче больших картинок по сети. Если администратор подготовлен к такому виду аномальной активности, это может помочь в дальнейшем расследовании. Находящиеся на каждой машине системы обнаружения вторжения также могут помочь во обнаружении аномального скопления изображений и (или)

В исследовании, проведенным Стефаном Хетцлем (*Stefan Hetzel*) на его сайте, идет речь о двух методах стеганографии, которые, в свою

очередь, являются средствами обнаружения ее. Это – визуальная и статистическая атака. «Идея статистической атаки – сравнение частоты распределения цветов для возможного носителя скрытой информации и теоретически ожидаемая частота распределения цветов для файла-носителя с скрытой информации». Это возможно не самый быстрый метод защиты, но если слив возникают подозрения насчет такого рода деятельности, то этот метод может быть самым эффективным. Специально для JPEG файлов существует утилита *Stegdetect*, которая способна определять следы стеганографии в этих файлах. Родственная утилита к *Stegdetect*, с названием *Stegbreak* способна расшифровывать и находить возможную информацию в подозрительном файле.

Стеганография – одна из самых увлекательных и эффективных методов сокрытия данных, которые использовались за всю историю человечества. Методы, способны разоблачить хитрые тактики злоумышленников несовершенны, но радует то, что такие методы существуют. Есть очень много причин, по которым следует использовать стеганографию (подписи, пароли, ключи), но главная – это легкость в обращении и сложность при обнаружении. Чем больше вы знаете о методах стеганографии, тем больше у вас шансов не попасть впросак.

Список литературы

1. Быков С.Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии - СПб.: Защита информации. Конфидент. 2000, № 3.
2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.«МК-Пресс», 2006. — 288 с.
3. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. — М.«Солон-Пресс», 2002. — 272 с.
4. Бабаш А. В., Материалы к лекции по теме «Криптография в древние времена».
5. Громов В. И., Энциклопедия безопасности 2000 года 3-ое издание.