Стеганография — Urbanculture

Криптоконспирология

Стеганография — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. Главная задача сделать так, чтобы человек не подозревал, что внутри передаваемой информации, не представляющей внешне абсолютно никакой ценности, содержится скрытая ценная информация. Тем самым стеганография позволяет передавать секретную информацию через открытые каналы, скрывая сам факт её передачи. Криптография защищает сообщение, делая его бесполезным в случае перехвата, а стеганография стремится сделать саму передачу сообщения скрытой. Криптография и стеганография могут применяться вместе: тогда сообщение сначала шифруется, а потом скрытно передается. Если применять криптографию без стеганографии, то остается риск, что наблюдатель, перехвативший сообщение, силой заставит отправителя или получателя его расшифровать.

Окно программы Xiao steganography

Компьютерная стеганография

Наиболее часто для сокрытия инфы используются графические файлы. Существует множество разных по своей сложности методов сокрытия, но наиболее простым является так называемый метод битовых плоскостей. Суть его заключается в следующем. Как известно, любое изображение представляет собой совокупность точек. Каждая точка цветного изображения кодируется комбинацией из 3-х байт, задающих уровень красного (R), зелёного (G) и голубого цветов (B) — RGB. Если в этой комбинации изменить самый последний бит, или пару — тройку битов, цвет хоть и получится отличным от исходного, но настолько незначительно, что даже самый острый глаз не заметит никакой разницы. Это и используется для того, чтобы путём изменения битов точек встроить в изображение любые данные, которые предварительно ещё и шифруются, после чего можно спокойно передавать такую картинку (*стегофайл*), не представляющую никакой ценности для ФСБ, ЦРУ, М6, Моссада (нужное подчеркнуть) через открытый канал. Стегофайл нельзя обрабатывать в графическом редакторе как картинку, иначе скрытая информация может быть разрушена. С осторожностью их надо загружать на файловые хостинги, поскольку они тоже при загрузке могут обрабатывать изображения.

Видишь няшу? к этой картинке прикреплен архив с imagecrypt. Ты можешь скачать его и воспользоваться, но это не по-мужски

Недостатком метода битовых плоскостей является то, что объём встраиваемых данных напрямую зависит о размера изображения, чем больше размер, — тем больше данных можно в него встроить. Как вариант решения этой проблемы данные встраиваются в различные служебные поля и переменные формата, необязательно графического. Объём текста может быть практически любым, но подобная вставка очень легко разоблачается, достаточно лишь посмотреть значения служебных полей. Метод битовых плоскостей можно обнаружить, используя статистические методы. Если проверять специальной программой все изображения, среди которых может оказаться стегофайл, то его можно найти.

Практическая реализация

В настоящий момент есть множество программ, которые способны создать стегофайлы из картинок, mp3-файлов и файлов различных форматов видео. Также есть достаточно простые способы сделать стегоконтейнер без узкоспециализированного софта. На еще том дваче практиковался формат rarjpg. При этом архив и картинка просто склеивались, архиватор обрабатывает архив, а просмотрщик изображений — картинку. Ничего не подозревающий анонимус видит картинку, тот кто знает о скрытом содержимом, открывает архиватором. Такие стегоконтейнеры безразмерны, но при попытке засунуть слишком много такую конструкцию выдаст размер. Также существует множество скриптов для поиска.

Imgcrypt.png

Также в качестве стегоконтейнера может послужить книга в формате epub. Формат представляет собой zip-архив с упакованными туда фрагментами. Просмотрщик обрабатывает файлы оглавления, стили из таблицы стилей, картинки и xhtml-файлы с содержимым. При этом он игнорирует все файлы, на которые нет ссылок из файлов с контентом. Добавить можно всё, включая исполняемые файлы программ и архивы. Такие стегоконтейнеры легко вычисляются по объему

данных, который явно превышает объем необходимый для книги. Также данные в нем будут потеряны при конвертации или автоматической оптимизации книги. Но проверку на целостность они успешно проходят. Данный вариант неприменим к файлам формата docx и odt.При наличии встроенного туда файла, просмотрщик или текстовый редактор выдает предупреждение.

Более серьезные поделки, которые изменяют младшие биты rgb-палитры, имеют серьезные ограничения на размер содержимого, при этом обеспечивают более надежную стеганографию. Одной из наиболее популярных программ является steghide. Программа не очень удобна из-за того, что требует использования командной строки. В настоящее время разработан и графический интерфейс, который рапространяется отдельно. Более серьезным иструментом является OpenPuff, который имеет возможность работать с разными форматами контейнеров и позволяет использовать несколько ключей. Слабая половина анонимусов (да, да, та самая у которой дыра в причинном месте) облюбовала ImageCrypto, небольшую и малопопулярную программку на Java. Причина проста — нет необходимости создавать текстовый файл отдельно, можно постить прямо в окно программы, рядом ввести пароль. Также сразу показывается емкость картинки-контейнера — нет необходимости гадать о вместимости. На основе ImageCrypto в политаче 2ch.hk на непостоянной основе существует тянский стегочат. Такой же, только более дохлый существует в криптаче.

Комбинированные стегоконтейнеры. Используются при наличии угрозы поиска стеганографии в определенном типе файлов. Так комбинированный контейнер может представлять собой книгу epub, куда встроено изображение со стегосодержимым. Для большей безопасности стегосодержимое может быть частью заранее подготовленной иллюстрации.

Desudesutalk

Юзерскрипт, написанный куклофагами для реализации стеганографии посредством картинок. За основу взята программа F5, также добавлена возможность шифровать сообщения с помощью PGP. Скрипт приобрел определенную популярность благодаря форсу на окточане, старом хидденчане и и мелкобордах. Также скрипт активно форсился на aibchan. Используется в большинстве своем не только куклами, а всеми желающими убрать от разбушевавшейся мочи свои кривотолки. Помимо пароля от стегоконтейнера и ключей участников есть еще ключ броадкаста, при изменении которого можно создать автономную группу и общаться в ней. В настоящий момент функционал по мнению большинства является избыточным — большая часть пользователей использует стандартный стег-пароль и ключ броадкаста.

Существует также целая стеганографическая имиджборда — Наноборда, её картинки разбросаны во многих местах и собираются в единую базу. К созданию этой борды приложил руку и автор Desudesutalk. Примечательно, что Desudesutalk способен работать внутри Наноборды, создавая новый уровень глубины.

Стеганография IRL

Действия, предназначенные для того, чтобы физически скрыть наличие сообщения, практиковались веками. Сообщениями были и порядок расположения объектов, их цвет, форма, стиль или количество. Например, в античности был случай, когда сигналом к началу действий послужили две переданные золотые монеты, хотя чаще средством передачи сообщений были одежда или какие-то предметы, от съёмных рукояток кинжалов и потайных карманов до чемоданов с двойным дном. Использование стеганографических методов было столь широким, что «черные кабинеты», в которых задерживалась и изымалась почта, проверяли не только письма, но и пересылаемые по почте вещи. В качестве примера стеганографического метода защиты информации можно привести колоду игральных карт, сложенную в определённом порядке, с надписью сбоку на колоде. После записи сообщения карты перетасовываются и прочитать его сможет только тот, кто знает нужный порядок. Также, в качестве тайника использовались даже курительные трубки. В полости стенок чаши пряталось сообщение, затем оно прикрывалось внутренней частью чаши, при этом эту трубку можно было курить, не опасаясь за сохранность сообщения, при этом имея возможность быстро его уничтожить, слегка повернув внутреннюю часть чаши. Многие подобные методы используются и сейчас.

Невидимые чернила

Невидимые чернила — это специальные жидкости или химические препараты, используемые для сокрытия существования записей. О подобной жидкости, изготовленной из молочая, писал ещё Плиний Старший в «Естественной истории» в I веке нашей эры, в дальнейшем они применялись вплоть до конца Второй мировой войны, после чего от них почти полностью отказались, сменив их на микроточки, хотя и сейчас они иногда используются. Известная легенда про то, как Ленин, сидя в тюрьме, писал сообщения молоком из чернильницы, сделанной из хлебного мякиша, тоже из этой области (чтобы прочесть такое сообщение, бумагу надо нагреть).

Такие чернила бывают двух видов: симпатические и органические. Первые представляют собой химические растворы, которые становятся невидимыми при высыхании и проявляются при добавлении к ним некоторых реагентов. Органическая же группа представлена легкодоступными веществами, такими как уксус, лимон, молоко. Они становятся видимыми, если их осторожно нагреть, ими обычно пишут между строк или на чистом листе бумаги. Во время Первой мировой войны шпионы рисовали символ, обозначавший, к примеру, тип вооружения, невидимыми чернилами, давали им высохнуть, а затем

наклеивали поверх него смоченную только по краям марку, что является хорошим примером технической и физической стеганографии.

Изготовить невидимые чернила можно, используя следующие пары «раствор — проявитель»:

- медный купорос и хлорид натрия[1] — метол-гидрохинон
- двухромовокислый калий и соляная кислота — метол-гидрохинон
- дихлорид ртути — метол-гидрохинон
- сулема — тиосульфат натрия или нашатырный спирт.
- Фенолфталеин — любая щелочь.
- Крахмал — йод. В простейшем случае письмо пишут выжатым из картофеля соком (в нём много крахмала). Текст появится при смачивании письма слабой настойкой йода.
- И, наконец, более продвинутый вариант скрытописьма. Текст пишется обычной шариковой ручкой, затем обрабатывается раствором марганцовки. Следы от маранцовки в свою очередь удаляются перикисью водорода. Подобный текст становится виден в ультрафиолете.

Также в качестве подобных чернил можно использовать сок цитрусовых или лука: просто макните тонкую кисточку в сок и напишите своё сообщение на волокнистой бумаге. Сообщение станет видимым, если нагреть его лампой, феном или утюгом. Ещё можно писать молоком по высокосортной бумаге, затем проявлять сообщение золой или растолченным графитом из карандаша. Да, да, известная легенда про то, как Ленин, сидя в тюрьме, писал сообщения молоком из чернильницы, сделанной из хлебного мякиша, тоже из этой области.

Шумоподобные радиосигналы

При использовании шумоподобных сигналов с отношением сигнал/шум<1 и уникальных кодовых комбинаций можно скрывать факт передачи сообщения.

См. также

- Криптография
- Отрицаемое шифрование

Примечания

1. ↑ Для тех, кто плохо учил химию в школе: хлорид натрия — NaCl — это самая обычная пищевая соль