A.K. Kolobova, D.G. Kolobov, A.S. Gerasimov

Steganography from Antiquity to the Present Days

Key words: steganography, digital watermarking, container.
This article deals with the history of steganography and with modern methods and purposes of its application.

А.К. Колобова, Д.Г. Колобов, А.С. Герасимов

СТЕГАНОГРАФИЯ ОТ ДРЕВНОСТИ ДО НАШИХ ДНЕЙ

Введение

Одна из древнейших и до сих пор полностью не решенных проблем настоящего времени –надежная защита информации. Основными направлениями решения этой проблемы занималось две науки: криптография и стеганография. Цель криптографии – сокрытие содержимого сообщения за счет шифрования. Однако наличие зашифрованного сообщения привлекает к нему излишнее внимание. Цель стеганографии – сокрытие самого факта передачи сообщения. Необходимая информация встраивается в какой-нибудь безобидный объект, а затем этот объект передается получателю.

Стеганография в древности

Существует версия [1], что одними из первых начали использовать стеганографию древние шумеры, так как ученые обнаружили множество глиняных клинописных табличек. Особенностью этих табличек были два слоя информации: одна запись покрывалась слоем глины, на котором писалась другая информация. Однако существуют также противники этой теории [2]. Они считают, что это была не попытка сокрытия информации, а просто особенность письма.

В древней Греции для письма использовали деревянные дощечки, покрытые воском. В трактате Геродота «История» описан способ передачи сообщения о плане царя персов Ксеркса захватить Грецию. Сообщение было нацарапано на дощечке под слоем воска, поэтому сама дощечка выглядела как пустая заготовка для письма [3].

Для другого известного метода использовались рабы. Голову раба брили наголо, затем наносили сообщение (в виде татуировки) и ждали, пока волосы снова не отрастут. После этого раб отправлялся к получателю сообщения. Все, что было нужно сделать для получения доступа к сообщению – это снова побрить раба. Однако такой способ передачи информации требовал достаточно большого количества времени и не подходил для срочных сообщений.

Более быстрый способ использовался в Китае. Письма писались на небольших полосках из шелка, затем они скатывались в шарики, покрывались воском и проглатывались человеком, который должен был доставить сообщение [4, 5].

В 1499 году аббат Иоанн Тритемий описал множество способов скрытой передачи данных в своем трактате «Steganographia» [6]. Именно в этой книге впервые было введено понятие стеганографии.

Другим древним методом сокрытия сообщения являлось использование симпатических чернил различного состава. Этот метод можно использовать и сейчас, так как сок лимона и молоко есть в каждом доме. При этом текст, написанный при помощи

этих веществ, невидим до момента его нагревания. Во время Второй мировой войны американские цензоры проверяли все письма на наличие симпатических чернил [7]. Лаборант использовал несколько щеток, закрепленных на одной оси. Каждая щетка была смочена в определенном проявителе. Лаборант водил по письму этим приспособлением с проявителями, которые обладают различные свойства (с их помощью можно было даже обнаружить естественные выделения человеческого тела – пот, жир и т.д.). Также письма просвечивали инфракрасным и ультрафиолетовым светом. Текст, написанный крахмалом, например, светится под воздействием ультрафиолета, но он невидим при электрическом и дневном свете. Инфракрасный свет использовался для выявления цветов, неразличимых при обычном освещении (таким образом можно было увидеть зеленые надписи на зеленом фоне).

Еще одним стеганографическим методом защиты информации являются микроточки. Фотография с информацией (например, фотография разведывательного донесения) уменьшалась до размера точки и вставлялась в безобидный с виду текст вместо точки. Получателю оставалось снова увеличить фотографию и прочитать сообщение. В книге [8] указано, что в 1482 году при создании книги один из монахов вместил 14 стихов из Евангелия от Иоанна в круг диаметром 12 мм.

Существуют и другие методы сокрытия информации, а именно:

запись при помощи колоды карт. Карты укладываются в колоду в определенной последовательности, а затем на боковой стороне колоды пишется сообщение. После чего колода тасуется;

запись внутри вареного яйца. На скорлупе сырого яйца пишется послание, потом определенным образом стирается, но успевает просочиться через скорлупу и при варке отпечатывается на белке;

использование трафаретов, которые кладутся на определенный текст, например на страницу книги, закрывают незначащие буквы и показывают значащие;

узелки на нитках и многие другие.

Современная стеганография

До конца XIX века криптография и стеганография развивались параллельно в рамках одной науки – тайнописи. Криптография отделилась от стеганографии после формулирования правила Кирхгоффа о принципах построения криптографических систем. Оно заключается в том, что секретным является не сам алгоритм, а лишь набор конкретных параметров без снижения стойкости алгоритма ниже допустимой величины [9]. Криптография превратилась в полноценную науку из совокупности особенных методов. Она основывается на теории вероятности, математической статистике, теории числовых полей.

В настоящее время стеганография используется для решения следующих основных задач:

защита авторских прав;

отслеживание каналов утечки информации;

защита конфиденциальной информации от несанкционированного доступа;

создание секретных каналов передачи информации;

преодоление систем мониторинга;

камуфляж программного обеспечения.

Современную стеганографию можно разделить на три раздела [10].

1. Классическая стеганография. Она включает в себя все методы, не связанные с компьютерными системами. Примеры применения классической стеганографии приведены в предыдущем разделе.

2. Компьютерная стеганография – направление классической стеганографии, основанное на особенностях компьютерной платформы и использования специальных свойств компьютерных форматов данных.

3. Цифровая стеганография – направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты. При этом возникают некоторые искажения файлов-контейнеров. Обычно методы цифровой стеганографии используют избыточность изображений, видео или аудио.

Компьютерная стеганография

Компьютерная стеганография появилась благодаря развитию компьютерных систем. Особенности компьютерной стеганографии учитывают работу с данными, особенности файловых систем и хранения в файловых системах. Примером может быть использование пробелов в машинописном тексте (напечатанном на компьютере). Пробел обозначается символом с кодом 32, но вместо него можно использовать символ с кодом 255. В таком случае кодом может служить использованный пробел. Один из пробелов будет обозначать 0, другой – 1.

Кроме того, довольно распространенной практикой в информационной безопасности стала установка скрытого программного обеспечения, применяемая как в законных, так и незаконных целях. Подобное программное обеспечение позволяет достигать различных целей: от логирования нажатий клавиатуры до слежения и получения удаленного доступа к системе.

За последние несколько лет случилось несколько инцидентов [11], получивших широкую огласку в мировой прессе – в первую очередь благодаря вирусам Duqu, Stuxnet и Flame, в составе которых были использованы руткит-технологии. Причем существует версия, что Stuxnet является разработкой израильских военных, направленных против ядерной программы Ирана. Данный вирус, который можно было найти не только на компьютерах обычных пользователей, спровоцировал инцидент на иранских заводах, осуществляющих разделение изотопов урана, запустив среди ночи песню одной из рок-групп, а также выведя из строя некоторые элементы системы. Общий итог – несколько версий данного вируса вывели из строя более 4000 центрифуг, а также затормозили ядерную программу Ирана на 1,5 года. Обнаружить и локализовать вирус смогли далеко не сразу как раз благодаря тому, что он был отлично скрыт от исследователей с помощь различных методов сокрытия.

Цифровая стеганография

Цифровая стеганография представляет собой наибольший интерес, с точки зрения защиты информации, как наиболее перспективное направление.

Ярким примером является сетевая стеганография, где в качестве носителей скрываемых данных используются протоколы модели OSI. В данной области имеются два основных направления передачи информации:

изменение заголовков;

изменение очередности пакетов (включая потерю пакетов).

Безусловно, даже в данном случае возможны различные гибридные методы сокрытия. В качестве примера можно привести метод LACK (Lost Audio Packets Steganog-

raphy) – в данном случае происходит передача данных за счет преднамеренных задержек пакетов. Причем речь идет в первую очередь о сигнальных пакетах, которые используются для установления стегоканала, а затем о пакетах с полезной для пользователей нагрузкой.

Однако наиболее распространеннй способ применения цифровой стеганографии – цифровые водяные знаки и идентификаторы. Цифровой водяной знак – это специальная метка, незаметно внедряемая в изображение или другой сигнал (контейнер) с целью тем или иным образом контролировать его использование [10]. Идентификаторы – те же цифровые водяные знаки, которые используются для отслеживания каналов утечки информации. На сегодняшний момент существует несколько открытых решений по встраиванию цифровых водяных знаков для обеспечения защиты авторских прав, например, [12–14]. Однако многие из них не являются устойчивыми к некоторым распространенным преобразованиям файла-контейнера или сильно искажают файл-контейнер. Чем более устойчив водяной знак, тем больше искажений он вносит. Сейчас перед специалистами стоит задача нахождения баланса между двумя указанными факторами.

СПИСОК ЛИТЕРАТУРЫ:

1. Попов М. Вперед в прошлое. Криптография // Мир фантастики. 2007. № 50.
2. Барабаш А. Стеганография. Древняя тайнопись в цифровую эпоху [Электронный ресурс] // Режим доступа к журналу: http://www.webcitation.org/66M340RTC (дата обращения: 02.09.2015).
3. Youssef Bassil Steganography & the Art of Deception: A Comprehensive Survey // Int. J Latest Trends Computing, 2013. Vol. 4. №. 3. P. 128–139.
4. Judge J.C.Steganography: past, present, future // SANS Institute publication, 2001.
5. Moulin P., Koetter R. Data-hiding codes // Proceedings of the IEEE, 2005. Vol. 93. Issue 12. P. 2083–2126.
6. Shumaker Wayne. Renaissance Curiosa: John Dee's Conversations With Angels, Girolamo Cardano's Horoscope of Christ , Johannes Trithemius and Cryptography, George Dal (Medieval and Renaissance Texts and Studies). Mrts. 1983.
7. Бабаш А.В. Шанкин Г.П. Зарождение криптографии. Материалы к лекции по теме «Криптография в древние времена». М.: Гелиос АРВ, 2002.
8. White William. The microdot: History and application. Philips Publications. 1992.
9. Фомичев В.М. Дискретная математика и криптология. Курс лекций. М.: Диалог-МИФИ, 2003.
10. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОН-Пресс, 2002.
11. Kim Zetter Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Crown. 2014.
12. Alphatec Watermarking Suite [Электронный ресурс] // Режим доступа к журналу: http://download.cnet.com/Alphatec-Watermarking-Suite/3000-6675_4-10314119.html (дата обращения: 03.09.2015)
13. Giovanni Content Management Suite [Электронный ресурс] // Blue Spike Inc [Офиц. сайт] – Режим доступа к журналу: http://www.bluespike.com/technology/ (дата обращения: 03.09.2015)
14. Technology Partners [Электронный ресурс] // Equilibrium [Офиц. сайт] – Режим доступа к журналу: http://www.equilibrium.com/partners/technology-partners/ (дата обращения: 03.09.2015)

REFERENCES:

1. Popov M. Vpered v proshloe. Kriptographiya // Mir fantastiki. 2007. № 50.
2. Barabash A. Steganographiya/ Drevnyaya tainopis v cifrovuyu epokhu: http://www.webcitation.org/66M340RTC
3. Youssef Bassil. Steganography & the Art of Deception: A Comprehensive Survey // Int. J Latest Trends Computing, 2013. Vol. 4. №. 3. P. 128–139.
4. Judge J.C. Steganography: past, present, future // SANS Institute publication, 2001.
5. Moulin P., Koetter R. Data-hiding codes // Proceedings of the IEEE, 2005. Vol. 93. Issue 12. P. 2083–2126.
6. Shumaker Wayne .Renaissance Curiosa: John Dee's Conversations With Angels, Girolamo Cardano's Horoscope of Christ, Johannes Trithemius and Cryptography, George Dal (Medieval and Renaissance Texts and Studies). Mrts. 1983.
7. Babash A.V., Shankin G.P. Zarozhdeniye kriptographii. Materialy k lekcii po teme «Kriptographiya v drevniye vremena». M.: Gelios ARV, 2002.
8. White William, The microdot: History and application. Philips Publications. 1992.
9. Fomichev V.M. Diskretnaya matematika i kriptologiya. Kurs lekcij. M.: Dialog-MEPHI, 2003.
10. Gribunin V. G., Okov I. N., Turintsev I. V. Tsifrovaya steganografiya. M.: SOLON-Press, 2002.
11. Kim Zetter Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon. Crown. 2014.
12. Alphatec Watermarking Suite http://download.cnet.com/Alphatec-Watermarking-Suite/3000-6675_4-10314119.html
13. Giovanni Content Management Suite http://www.bluespike.com/technology/
14. Technology Partners. Equilibrium http://www.equilibrium.com/partners/technology-partners/