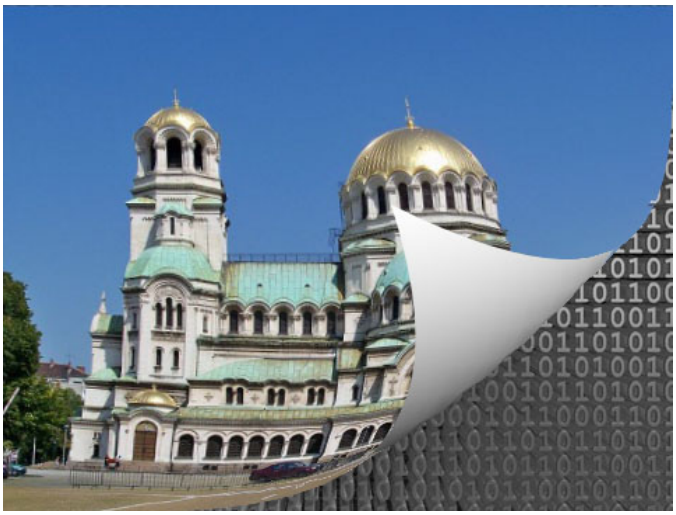
Стеганография

Автор: Фам Т . Киен

Стеганография (на английски: стеганография) е изкуство и наука за писане и предаване на тайни съобщения, така че освен изпращача и получателя, никой да не може да знае за съществуването на съобщението. Тази техника е една форма на сигурност, като съобщения се крият. Думата „стеганография“ има гръцки произход, тя означава „тайнопис“, и е комбинация от две думи Steganos (στεγανός) означава „крие за защита“ и graphein (γράφειν) означава „да пише“. За стеганографичната техника, съобщенията обикновено се появяват под друга форма в процеса на предаване: снимки, статии, пликове, с които съобщенията могат да бъдат написани с невидимо мастило в празно пространство на нормално писмо.

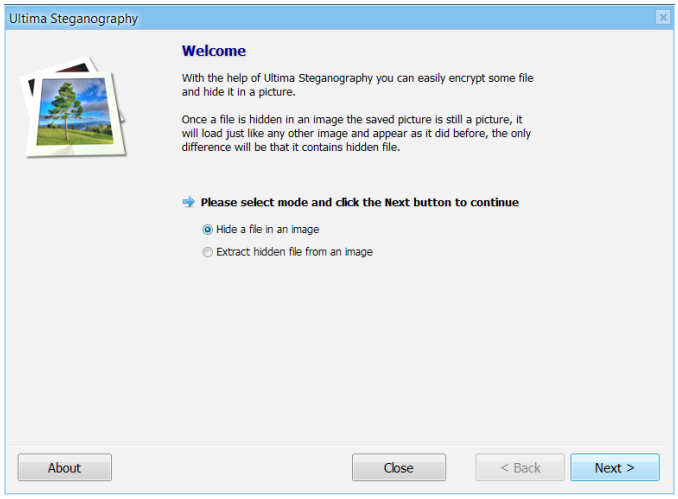


Днес електронната стеганография означава техника за скриване на секретни данни в публични изображения, видео, аудио или текстови файлове. Тази техника е изследвана и широко известна в последното десетилетие като една техника за сигурност. Тайните съобщения се кодират във вътрешната структура на фонови данни (изображение, звук, видео) и се изпращат открито в медиите от изпращача до получателя. След като успешно е получил фонов файл с тайните данни, получателят използва софтуерните си инструменти за декодиране, премахване на фоновия файл и получаване секретните данни на съобщението. Има много такива инструменти. За да се създаде визуалния поглед, тук ще дам пример за криене на тайни данни във фонови файлове посредством използване на два софтуера: “Ultima steganography Version 1.7” за PC и “Steganography” за мобилни телефони, които използват Android операционна система. Тези два софтуера имат сравнително прост интерфейс и е лесен за употреба.

Ultima Steganography

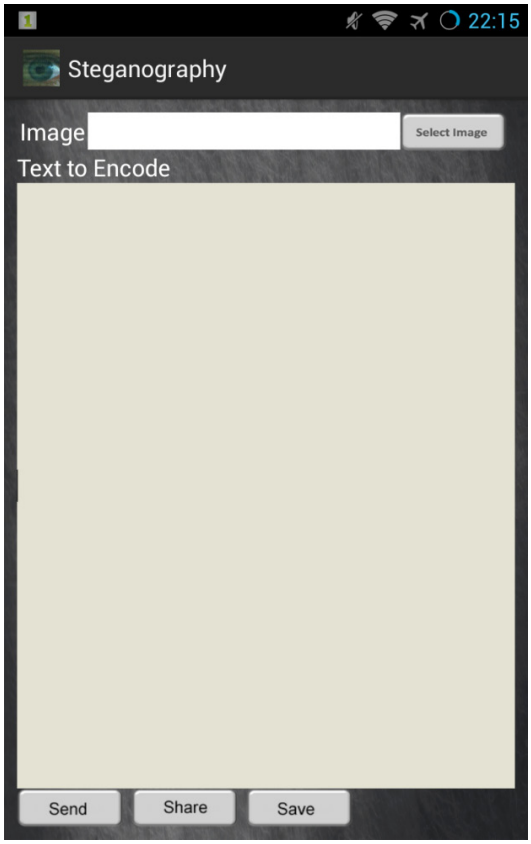
Ultima Steganography Version 1.7 се използва за да се скрият секретни дан-

ни в обикновен поглед. Тези секретни данни могат да бъдат снимка, текстов файл, аудио-видео и др., а фоновите файлове са изображения с графичния формат като PNG, GIF, JPG, JPEG, BMP, TIF, TIFF, ICO, EMF, WMF. След като са скрити тайните данни във вътрешната структура на фоновия файл, те се запазват с парола и се предават чрез медийната среда, например интернет. Получателят също трябва да използва тази програма и трябва да знае паролата за декодиране на файла, за да може да получи секретната информация, която се крие вътре в него.



Steganography

Приложението „Steganography“ на Android устройствата има същото предназначение и начин за използване като на Ultima steganography. Секретните данни са обикновени текстове, които се въвеждат директно и скрити под графичен файлов формат като PNG JPG и др. След кодиране файлът ще бъде препратен чрез медиите като интернет, или чрез изпращане с мултимедийно съобщение от изпращача до получателя.



Мрежова стеганография

Един по-модерен подход, наречен мрежова стеганография, която на практика няма следа за откриване. В тази техника, вместо за вграждане на секретна информация във фонови данни, като JPEG или MP3 формат, програмата за мрежова стеганография крие секретни комуникационни данни в интернет трафика. Тъй като тези програми използват каналите за предаване в кратък период от време, като Voice over Internet Protocol, скритните данни трудно се откриват.

В момента, имаме десетки техники с мрежова стеганография. Това означава, че терористи, престъпници, хакери могат да използват същия метод, за да

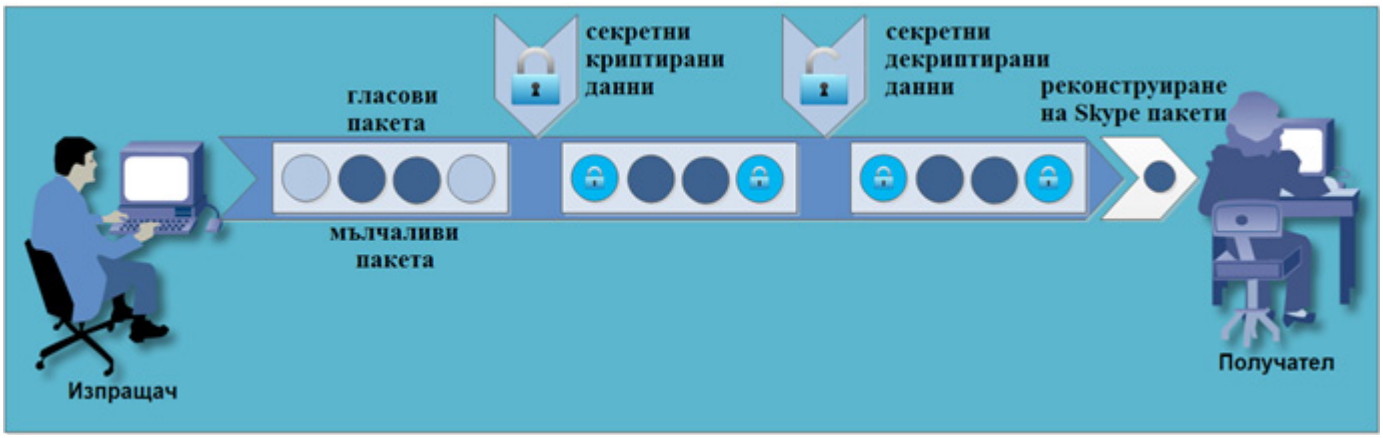
комуникират помежду си и да се избегне намеса от страна на властите. До настоящия момент може да се твърди, че никой не притежава всички инструменти и достатъчно възможности за ефективно откриване на тайните съобщения, които са били изпратени от тази техника.

Благодарение на бързото развитие на интернет, сегашното разпределение на данните и комуникация в интернет става прекалено лесно. Въпреки това, поради неговата отворена структура безопасността при изпращане и получаване на данните в интернет не е висока. Прилагането на стеганографична техника за споделяне на данни и комуникация в интернет е основна тенденция. Тук ние ще разгледаме няколко приложения, където може да бъде приложена мрежова стеганография.

Skype

Skype - VoIP услуга монопол на Microsoft - особено лесно се използва за предаване на скрити съобщения поради неговия начин за капсулиране на звукови данни. Когато някой потребител използва Skype, програмата капсулира звукови данни в пакети. Но за разлика от много други VoIP приложения, Skype продължава да създава звукови пакети (тишините пакети) дори когато потребители мълчат. Това подобрява качеството на разговора, но също така лесно се използва за предаване на тайни съобщения. Тишините пакети лесно също са разпознаваеми, защото имат много по-малък размер - около половината от броя на битовете - от пакети, съдържащи глас на потребителя. В действителност, потребителите могат да използват тези тишините пакети за да скрият и да предават тайна информация.

Една изследователска група за мрежова сигурност във Варшавски политехнически университет, Полша е разработила програма за мрежова стеганография, която позволява на потребителите да определят пакета, който има по-малък размер (тишините пакети) и да заменя техните съдържания с криптирана тайна на данните, наречена SkyDe. За да се направи този разговор, повикващият и повикваният трябва да имат SkyDe програма, инсталирана на компютъра си. Софтуерът ще открие и открадне някои по-малки пакети, като същевременно позволява да минават всички по-големи остана-



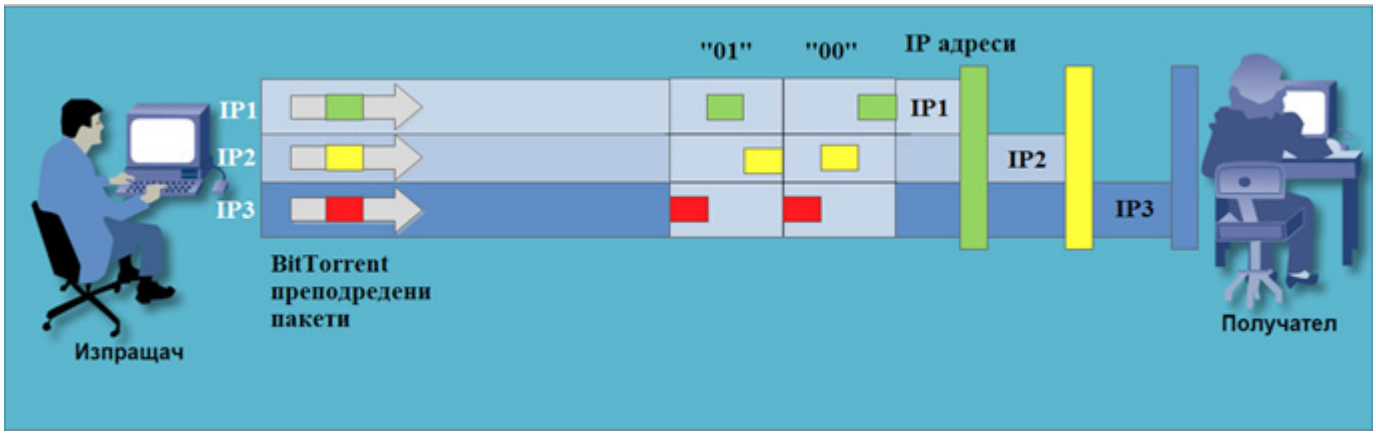
ли пакети, и използва тези малки пакети за да се скрие тайно съобщение. След това Skype запълва пропуските на малките пакети чрез възстановяване на тяхното съдържание, въз основа на съдържанието на съседните пакети. В резултат на това съдържанието на тишините пакети, които се вземат от SkyDe, ще бъдат същите като всички съседни пакети. Това означава, че Skype може да транспортира тайни съобщения, без да причинява забележима промяна в качеството на разговора. В действителност те могат да изпратят около 2 килобита в секунда тайна информация, т.е около 100 текстови страници за 4 минути, без да предизвиква никакви подозрения.

BitTorrent

BitTorrent е протокол за споделяне на ресурси, базиран на система „peer to peer“ и е името на програма за споделяне на ресурси, разработена от Bram Cohen. BitTorrent се използва за сваляне на големи данни без плащане на скъпи разходи за сървър и мрежови трафик. Той е един от най-популярните протоколи за споделяне на файлове в момента. BitTorrent протокол предава стотици трилиони битове в секунда от цял свят. Очевидно, ако искат да скрият тайните данни в тази масивна купчина от данни, която се предава чрез този протокол, ще бъдат много трудно за проследяване и откриване.

Програма StegTorrent се възползва от факта, че потребителите на BitTorrent обикновено споделят един файл от данни (или парчета от файлове) за множество получатели наведнъж, за да се скрие тайни съобщения в BitTorrent транзакции. За провеждане на тайни транзакции чрез използване на BitTorrent, първо получателят трябва да има предварителния контрол над определена група от разпределени компютри, всички от които използват еднакво BitTorrent приложение. Това означава, че тези компютри са притежавани от получателя или тези компютри са били хакнати преди, както получателя и изпращача трябва да знаят всеки компютър от групата и техните IP адреси.

За простота, разгледахме случай при който получателят контролира една група от два компютъра. За да се започне транзакцията, той нарежда на компютъра една заявка за получаване на файлове от другия. В типична-

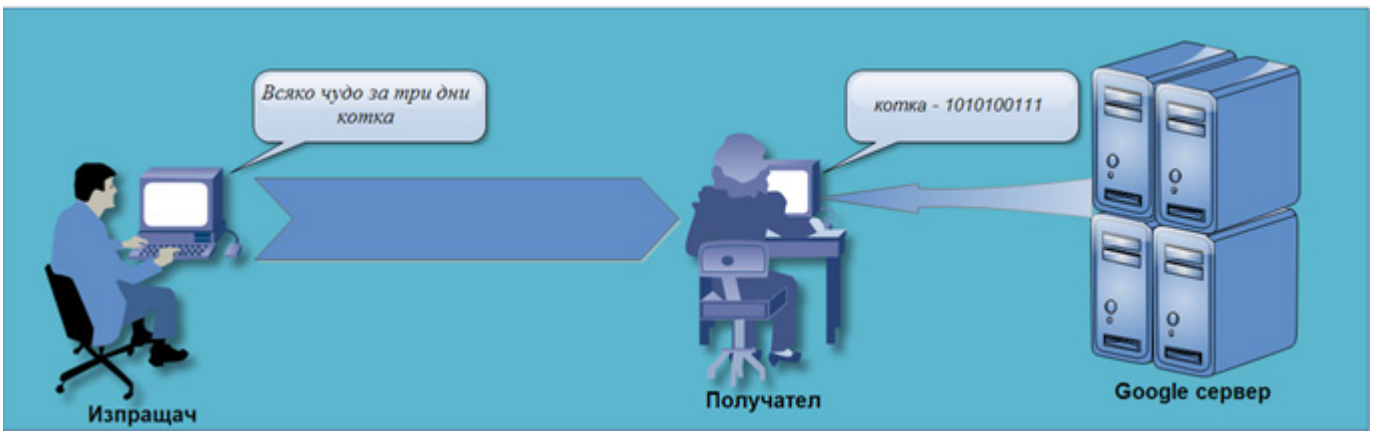


та обикновена транзакция с BitTorrent протокол, програмата на изпращача ще предава пакети от данни в случайния ред, и компютъра на получателя ще ги пренарежда въз основа на насоките, които се носят в него. Въпреки това, като се използва StegTorrent изпращачът пренарежда пакетите за криптиране на определена последователност от битове. По този начин изпращачът може да изпрати до 270 бита секретна информация всяка секунда, използвайки шест IP адреса - достатъчна честотна лента за един разговор с обикновен текст - без да се влошава качеството на разговора или привличане на вниманието.

Google Suggest

Google Suggest и Google Suggest keywords е една възможност за автоматично извършване на търсене, базирана на популярността на ключови думи. Тази функция помага на потребителите на Google да спестят времето си при търсенето не е необходимо да въвеждат всички букви във тяхната ключова дума за търсене. Също така той е много ефективен за търсене на име или уебсайт, когато не се знае пълното му име.

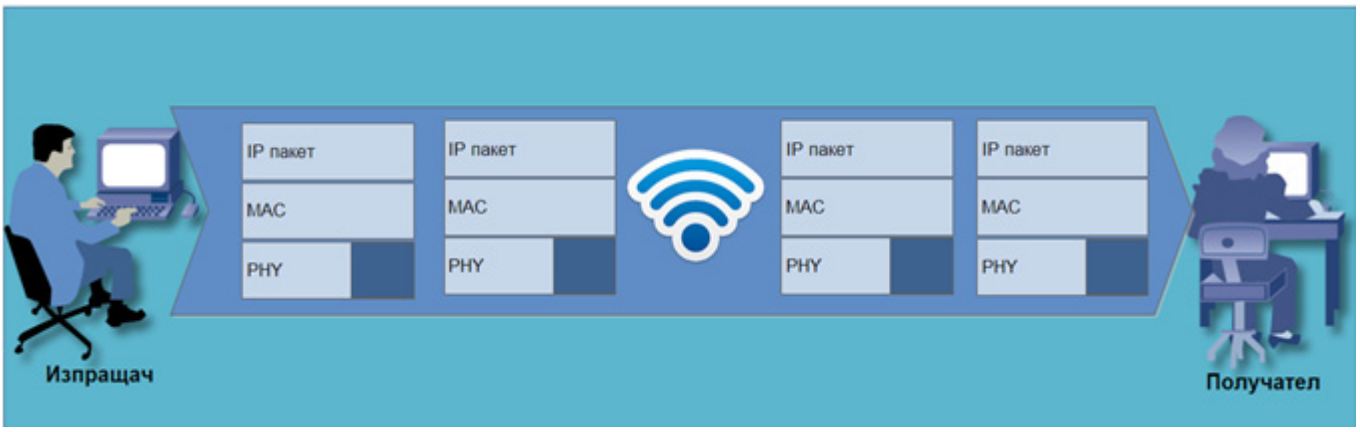
Въпреки това, тази функция също може да се използва за предаване на секретни съобщения. Един инструмент, който се използва за тази цел, е StegSuggest. Неговият принцип на работа е следният: Когато изпращачът иска да изпрати на получателя едно секретно съобщение, първо той трябва да зарази компютъра на получателя със софтуер StegSuggest, така че да може да следи за обмен на мрежов трафик между Google сървъра и браузъра на получателя. След това, когато получателят напише една случайна дума или фраза в полето за търсенето на Google, например, той пише: „Всяко чудо ...“, изпращачът ще блокира данните от сървърите на Google и използвайки StegSuggest инструмента за добавяне на една дума с данни от неговото тайно съобщение в края на всяко от 10 изречения, предложени от Google. Например, ако Google предложи фразата „Всяко чудо за три дни“ изпращачът може да добави „Всяко чудо за три дни *котка*“. Тогава програмата StegSuggest на получателя ще вземе всяка дума, която е добавила преди, и ще преобразува в 10-битова последователност с помощта на справочна таблица. По такъв начин изпра-



щачът може да предава до 100-битов секретна информация всеки път, когато получателят напише една дума или фраза в неговото поле за търсене на Google.

Wi - Fi мрежи

През последните години, безжичната мрежа се развива бързо поради ред предимства, но също така, тя може да се превърне в една среда за предаване на тайни съобщения. В момента, един от най-популярните стандарти на безжична мрежа е IEEE 802.11, който се използва за Wi-Fi мрежа, която използва ортогонална многочестотна модулация (OFDM).



За да се разбере как се скриват данни в OFDM сигнал, трябва да знаем как работи OFDM. Първо, входният поток от данни с висока скорост се разделя в няколко паралелни потока от данни с по-ниска скорост чрез преобразувател S/P (Serial/Parallel). След това всеки паралелен поток се криптира чрез използване на FEC алгоритъм (Forward error correction) и се разполага в смесена поредица. Тези символи постъпват във входа на IFFT блока, който ще изчисли временния период, съответстващ на канала в честотната лента. След това защитените интервали се вмъкнат за да се намали ISI интерференция. Накрая модулатора на предавателна страна преобразува сигнал в по-високи честоти и го предава на канала. В действителност, тази техника рядко разделя различните символи с еднаква дължина, обикновено някои от левите символи са твърде по-малко на брой битове. Поради това, OFDM предавателя добавя допълнителни битове (буферни битове) в тези символи, докато те се впишат в стандартния размер. Поради това „буферните битове“ са безсмислени, изпращачът може да ги заменя с бита на секретни данни, без да влошава качеството на предаваните първоначални данни. Този метод се нарича безжична буферна стеганография, или WiPad. Тъй като броят на буферните битове е относително голям, изпращачът може да изпраща скрити данни дори с много високо качество клипове.

Литература:

[1] Shashikala C., Ajay J., Steganography An Art of Hiding Data, International Journal on Computer Science and

Engineering Vol.1(3), 2009, p. 137-141
[2] Vijaya C., Orthogonal Frequency DivisionMultiplexin,https://www.cresis.ku.edu/~rvc/ documents/862/862_ofdmreport.pdf
[3] New Ways to Smuggle Messages Across the Internet, http://spectrum.ieee.org/telecom/ security/4-new-ways-to-smuggle-messages-across-the-internet
[4] Wojciech M., Krzysztof S., New Ways to Smuggle Messages Across the Internet, IEEE spectrum, 2013
[5] Samuel K., SkyDe Software Sends Hidden Messages in Skype Calls, IEEE spectrum.
[6] Pawel K., Wojciech M., Krzysztof S., StegTorrent: A Steganographic Method for the P2P File Sharing Service, ISBN: 978-1-4799-0458-7
[7] Szczypiorski K., Hiding Data in OFDM Symbols of IEEE 802.11 Networks , ISBN: 978-1-4244-8626-7, Multimedia Information Networking and Security (MINES) International Conference, 2010
[8] Shashikala C., Ajay J., Steganography An Art of Hiding Data. International Journal on Computer Science and Engineering Vol.1(3), 2009, p.137-141, ISSN: 0975-3397
[9] http://enplase.com/pages/Download.html
[10] James C., Steganography: Past, Present, Future, SANS Institute, 2001
[11] Емануил С., Божидар С., Обратими растерни трансформации и тяхното приложение в стеганографията, Научни трудове на Русенския университет-2008, том 47, серия 3.2, p.84-91
[12] http://enplase.com/pages/Ultima+Steganography+description.html
[13] http://www.appszoom.com/android_applications/productivity/steganography_jeyyt_download.html