

# Overview of covert communications through networks

Michael A. Caloyannides \*  
Mitretek Systems, Falls Church, VA

## ABSTRACT

Covert communications through digital networks are a small subset of covert channel communications through all other networks such as human contacts, postal, telephone, ham radio and other networks. The repertoire of options available to anyone for covert communications through digital networks is limited only by imagination; covert communications are therefore inherently uncontrollable.

**Keywords:** Covert communications, data hiding, anonymity, confidentiality, privacy, interception.

## 1. BACKGROUND

Viewed as a potential pathway for covert communications, a network of computers is fundamentally no different than any other network, be that a network of social or professional contacts, a postal network, a telephone network, an ATM cash-dispensing bank network, or any other.

Covert communications can occur either through the commission of an act or through the omission of an expected act; not saying “good night” when one usually says good night conveys the message “I am angry with you” in an oblique way. The same goes for a multitude of time-honored social gestures such as the firmness of a handshake, a lover’s longing look, pregnant pauses in speech, and the like. In a different context, the popular literature is full of stories of individuals who communicate brief messages covertly by chalking marks on public road signs, of auction bidders who communicate their bid by scratching their ear, and of just about any profession by engaging in some pre-agreed signaling that is intended to be unnoticed by all other than the intended recipient of the message.

Whereas it is easy to communicate pre-agreed messages, the process of covertly conveying extended messages requires a channel and a means of sending the extended message in a manner that will not alert anyone other than the intended recipient. This brings up the fundamental question that must be answered specifically for each requirement for covert communications, namely “hide exactly what and from whom and under what constraints and assumptions?”

Covert channels have been extensively analyzed in the open literature; an excellent publication available online ([www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-030.html](http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-030.html)) is a 1993 unclassified publication by NSA, “A Guide to Understanding Covert Channel Analysis of Trusted Systems”. A keyphrase search for “Covert Channels” or for “Covert Communications” on the Internet results in an extensive amount of other papers on covert channels. The present paper will not repeat any of this extensive work; instead, this paper will focus on the practical aspects of “so, now what?”

### 1.1 Hide what and from whom?

There are numerous elements of a communication that aspires to remain “covert”; depending on the specifics of each situation, one may wish to hide one or more of these aspects. Each such aspect has its own repertoire of possible solutions. Does one want to hide:

- a) *The content* of the communication?

- b) *The source of the communication?*
- c) *The identity of intended recipient of the communication?*
- d) *The fact that the communication is occurring in the first place?*

Similarly, in the case of digital computer networks, there are numerous different entities that one may wish to hide any or all of the above aspects from. Does one want to hide one or more of these aspects from:

- a) Network operators, such as the Internet Service Provider, corporate network system administrator, etc.?
- b) Inquisitive neighbors, fellow employees, family members, etc.?
- c) Law enforcers, security services, etc.?
- d) Computer- and network-forensics specialists?
- e) Keystroke interception software and hardware?
- f) Commercially available hardware for intercepting unintended (Van Eck) emanations from a computer terminal?
- g) Legal or illegal taps on the communications channel?
- h) Overhead cameras that image one's keyboard or computer monitor?

For each of these threats to communications that aspire to be covert, one must also assess the level of competence and motivation of the individuals involved; an overnight self-anointed "computer forensics expert" poses a very different threat from one who is experienced and who has access to computer forensics microscopy. Related to this is an element of chance, too: is a potential threat monitoring (or recording) the right sensors at the exact time the covert communication is taking place?

## **1.2 Hide it how often and for how long?**

It is clearly far more likely that an act that aspires to remain covert, such as a communication over a computer network, will stay covert if it is done once only than if it is done again and again. Similarly, it is far more likely that such an act will remain undetected "for a short while" than that it will remain undetected for ever.

If, for example, one is only trying to protect the content of a tactical message and for only a few minutes, run-of-the-mill encryption is likely to be adequate because the data being protected is perishable anyway. Stated differently, the engineering design of a means for covert communications over computer networks must take into consideration how often such communication is to occur and how long it is necessary that it remain covert.

## **1.3 Communicate over what distance and under what technical constraints?**

"Distance" in the case of computer networks is relevant mostly in a binary sense: Are the two communicating parties able to access the same network or does a gap have to be bridged along the way? If the latter, then a large submenu of possibilities and constraints opens up that has to be addressed.

Other ancillary constraints that impact the engineering design of a path for covert communications over computer networks include but are not limited to:

- a) Level of access to the network. Depending on which technical means are decided on, varying degrees of access to software and hardware will be needed; these can range from minimal all the way to "root" access.
- b) Data rate and amount of data. Is the required covert data rate and overall amount of covert data a very small (say,  $10^{-9}$ ) percentage of the overt data rate and amount being handled through the intended communications path, or is it comparable? Hiding one byte in a terabyte is trivial; hiding a megabyte in another megabyte is not.

- c) Immediacy requirements. Is it required that the covert data be communicated “right here and now” or can it wait for a technically opportune situation to present itself? Is the intended recipient of the data assumed to be always ready and available or must that intended recipient be alerted to receive the data through yet some other covert means?

#### 1.4 “Yes, but can you *guarantee* it will be covert?”

No; nobody ever can. We all play subject to the same laws of physics. The intended recipient of a covert communication through a computer -or any other- network has no magical wand to use that an interceptor cannot have as well. Obviously, if the interceptor has the same knowledge and equipment as the intended covert recipient, he/she is then indistinguishable from the intended covert recipient. What makes something “covert” is merely a combination of human, and *not* technical, factors, and these human factors pertain to the interceptor and not to the aspiring covert communicator. These factors include:

- a) Little or no suspicion that a covert communication may be taking place.
- b) Little or no motivation to pursue that possibility.
- c) Little or no competence in pursuing that possibility.
- d) Little or no equipment to pursue that possibility.
- e) Little or no knowledge of how that covert communication may be taking place.
- f) Little or no likelihood that the interceptor is monitoring or recording the right sensor at the right time.

Since all of these factors pertain to the interceptor and not to the aspiring covert communicator, there is little that the latter can do to “guarantee covertness”; the best that the covert communicator can do is to exercise good judgment based on experience and knowledge of relevant human, administrative and technical issues. If the covert communication is intended to be used on a repeated basis, one would obviously benefit from also having some means, technical or otherwise, of becoming aware if past covert communications have alerted some interceptors, in which case one will no longer have the benefit of items (a) through (f) above.

## 2. YES, BUT HOW?

Computer networks provide a multiple infinity of ways to communicate covertly; the menu of choices is limited only by one’s combined imagination and technical knowledge. It must be emphasized yet once more that one must first answer the very fundamental question of “hide exactly what and from whom and under what conditions?” discussed in section above. There is no “one size fits all” solution and never will be.

If one merely wants to hide the content of a message, powerful encryption is available for free worldwide.

If one wants to hide the identity of the intended recipient, then one can do the computerized equivalent of placing a classified ad in the local newspaper, namely, posting a message on any of the 100,000-some Usenet newsgroups read by millions of individuals worldwide.

If one wants to hide the identity of the sender, one can –among other ways- avail oneself of the multitude of anonymous Internet remailers, such as the “mixmaster” remailers that resist traffic analysis as well, or use someone else’s networked computer terminal. The use of anonymous remailers and sender-identity obfuscation is not for the amateur <sup>(1)</sup>. Again, the “hide from whom?” issue must be carefully addressed as the mere connectivity to such a remailer can be incriminating enough in some situations.

If one wants to hide the origin of a digitized file, and assuming that the file could not have come from only a handful of sources, then one has to consider the possibility that the file in question may have been

digitally watermarked. Finding and “washing” a watermark does not prove that there is no other watermark as well.

If one wants to hide even the fact that a communication is occurring in the first place, then the choices are largely between two generic classes of approaches:

- a) “Fly under the radar”, in the sense of aspiring not to be noticed, by being non-alerting.
- b) “Hide in plain view”, in the sense of masquerading as part of legitimate data traffic, i.e. appearing to be what one is not. This comes under the general class of “data hiding” which is a very scholarly pursuit with its own yearly technical conferences and publications. Steganography is a major subclass of data hiding. It has been around since time started and has gained notoriety during the last decade. Recall, for example, the microdots of Von Kanaris of World War II fame, or the situation when emperors of yesteryear shaved the heads of a slave, wrote a message on the shaved head, waited for the hair to grow and then sent the slave to the intended recipient of the message who reversed the process.

Possibilities are limitless and can could include, for example, appending or inserting data anywhere where this does not affect the operation of the network or its files, protocol-based schemes, font-related schemes, schemes involving the distribution of software within the network, etc., etc. One well-known example is that of “Easter eggs”, namely, the common practice whereby programmers insert code in commercial software without their respective employer’s knowledge; those software users who know which uncommon sequence of keystrokes and mouse-clicks to use, can then see the hidden messages –usually humorous- that the mischievous programmers hid inside the commercially distributed software.

In view of the broad market for such services for non-technical users, numerous commercial services have sprung up that provide varying degrees of protection for the content of emailed messages, and/or for hiding the identity of the originator or intended recipient from one or more would-be types of interceptors; these include Safe Mail (<https://www.safe-mail.net>), COTSE (<https://www.cotse.net>), and others; many have ceased operation, too, such as PrivacyX and Zero Knowledge Systems’ “Freedom 2”.

Even conventional SSL web browser connections allow end-to-end encryption, although they have their share of security problems, such as:

- a) The SSL certificate of the web site is often that of the web hosting service and not that of the presumed proprietor of the web site.
- b) The fact that there is an ongoing SSL connection may be damning enough to seal the fate of a user in some situations; furthermore, unless the user is particularly technology-savvy, his/her hard disk will contain more than enough evidence that can be readily found by a computer forensics investigator.
- c) Most individual users’ SSL “certificates” are worthless in certifying an individual’s identity, since most can be obtained freely for the asking.

## **2.1 Now, about that “steganography”...**

Steganography is one of the many ways of “hiding data in plain view”. Its notoriety is mostly due to the worldwide availability of rather simplistic software that assert that they hide data undetectably within digitized images and sound files; most –though not all- of those simplistic tools alter the least significant bit on the premise that the human eye and ear cannot tell the difference. While this is true, it is also true that the interceptor is neither the human eye nor the human ear but software that do high order statistics on the cover files and often readily detect tell-tale anomalies suggestive of steganographically hidden content.

But steganography transcends such simplistic tools and can be any technique at all that hides data within other data. As such, the often heard assertions that either “our steganography software is secure” or “we can detect all steganography” only makes a statement about such asserters’ competence.

### 3. BUT SHOULDN'T ALL THIS BE ILLEGAL OR AT LEAST DISREPUTABLE?

No. For the following reasons:

- a) Covert communications has a long and honorable history. Recall Paul Revere (“One if by land, two if by sea...”) as well as most of this Nation’s founding fathers during this Nation’s formative years. It is also essential to the functioning of freedom-seeking groups in patently oppressive totalitarian regimes. Even today, it is essential in such essential functions as allowing informants to pass information to the US about illegal drug dealings, and other situations.
- b) Anonymity is just as deeply ingrained in this Nation’s history. The Federalist Papers were signed with pseudonyms, and the US Supreme Court has repeatedly affirmed the importance of anonymity in facilitating the freedom of speech. It is also indispensable in such social situations as contacts with suicide prevention facilities, “whistle blowing” about illegal conduct, etc.
- c) Data hiding in general and the much maligned steganography in particular is at the heart of digital watermarks that protect the intellectual property rights of individuals in this digital age when artwork, copyrighted music and video are routinely traded over the Internet.
- d) Encryption in the private sector is essential to secure commerce –which includes every businessman regardless of the size of the business-, to medical professionals who must comply with the laws on medical record confidentiality, and to every individual who must rightly protect from identity theft. In short, it is essential to the functioning of society today.

Any technology, be that automobiles, prescription medicines, or kitchen knives can be and has been used for unintended illegal purposes. Bank robbers and terrorists have regularly escaped with cars and have communicated using telephones, yet nobody seriously contemplates banning either.

Covert communications through computer networks, too, can be and have been used for unintended illegal purposes as well, but it would be just as ludicrous to ban those as it would be to ban automobiles or prescription medicines. Additionally, given that there is an infinity of ways to conduct covert communications through computer networks, a ban on such techniques will be no more effective than a ban on bad weather.

### REFERENCES

1. a) Michael Caloyannides, “Computer Forensics and Privacy”, Artech House Publishers, ISBN: 1580532837 August 2001

b) Michael Caloyannides, “Effective Encryption for Privacy”, John Wiley Publishers, ISBN: 0-471-48657-4, May 2002.

\* [Michael.Caloyannides@Mitretek.org](mailto:Michael.Caloyannides@Mitretek.org); Mitretek Systems, 3150 Fairview Park Drive South, Falls Church, VA 22042-4519