**Secure Communication**

From Wikipedia, the free encyclopedia

(Redirected from [Secure Communication](http://en.wikipedia.org/w/index.php?title=Secure_Communication&redirect=no))

When two entities are communicating with each other, and they do not want a third party to listen to their communication, then they want to pass on their message in such a way that no body else could understand their message. This is known as communicating in a secure manner or **secure communication**. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot know what was said. Other than communication spoken face to face out of possibility of listening, it is probably safe to say that no communication is guaranteed secure in this sense, although practical limitations such as legislation, resources, technical issues (interception and encryption), and the sheer volume of communication are limiting factors to surveillance.

The purpose of this article is to describe the various means by which security is sought and compromised, the differing kinds of security possible, and the current means and their degree of security readily available.

With many communications taking place over long distance and mediated by technology, and increasing awareness of the importance of interception issues, technology and its compromise are at the heart of this debate. For this reason, this article focusses on communications mediated or intercepted by technology.

Also see [*Trusted Computing*](http://en.wikipedia.org/wiki/Trusted_Computing), an approach under present development that achieves security in general at the potential cost of compelling obligatory trust in corporate and governmental bodies.

**Users and needs**

Many forms of everyday communication are "reasonably" secure, thus, we do not assume telephone calls are intercepted when we use them. However in some areas such as online intellectual property rights, legal, criminal, political and commercial communications, this assumption is inadequate.

**History**

In 1898, [Nikola Tesla](http://en.wikipedia.org/wiki/Nikola_Tesla) demonstrated a [radio controlled](http://en.wikipedia.org/wiki/Radio_controlled) boat in [Madison Square Garden](http://en.wikipedia.org/wiki/Madison_Square_Garden) that allowed secure communication between transmitter and receiver.

One of the most famous forms of secure communication was the [Green Hornet](http://en.wikipedia.org/wiki/SIGSALY). During WWII, Winston Churchill had to make vital calls to the President of the United States, Franklin D. Roosevelt. These calls talked about such things as shipping and troop movements. At first, the calls were made using a radio phone as this was thought to be secure. Unfortunately, due to the Nazis having a listening station in Holland they were able to hear every last word. As soon as it was realised they stopped using the radio phone and started work on a whole new system, the Green Hornet. This meant that anyone listening in would just hear white noise but as the only two identical copies were held with the Prime Minister and the President the conversation was clear to them. As secrecy was paramount, the location of the Green Hornet was only known by the people who built it and Winston Churchill, and if anyone did see him entering the room it was kept in, all they would see was the Prime Minister entering a closet labeled 'Broom Cupboard.' It is the said that because of the way the Green Hornet works it is not able to be beaten, even today.

**Nature and limitations of secure communication**

**Types of security**

Security can be broadly categorised under the following headings, with examples:

* Hiding the content or nature of a communication
	+ [Code](http://en.wikipedia.org/wiki/Code)
	+ [Encryption](http://en.wikipedia.org/wiki/Encryption)
	+ [Steganography](http://en.wikipedia.org/wiki/Steganography)
	+ Identity Based
* Hiding the parties to a communication (prevention of identification, or [anonymity](http://en.wikipedia.org/wiki/Anonymity))
	+ "[Crowds](http://en.wikipedia.org/wiki/Crowds)" and similar anonymous group structures. i.e. it is difficult to identify who said what when it comes from a "crowd".
	+ Anonymous communication devices (unregistered [cellphones](http://en.wikipedia.org/wiki/Cellphone), [Internet cafes](http://en.wikipedia.org/wiki/Internet_cafe))
	+ [Anonymous proxies](http://en.wikipedia.org/wiki/Anonymous_proxies)
	+ Hard to trace [routing](http://en.wikipedia.org/wiki/Routing) methods (through unauthorised 3rd party systems, or relays)
* Hiding the fact that a communication takes place
	+ "Security by obscurity" (similar to [needle in a haystack](http://en.wikipedia.org/wiki/Needle_in_a_haystack))
	+ Random traffic (creating random data flow in order that the presence of genuine communication is harder to detect and [traffic analysis](http://en.wikipedia.org/wiki/Traffic_analysis) less reliable)

Each of the three is important, and depending on the circumstances any of these may be critical. For example, if a communication is not readily identifiable, then it is unlikely to attract attention for identification of parties, and the mere fact a communication has taken place (regardless of content) is often enough by itself to establish an evidential link in legal prosecutions. It is also important with computers, to be sure where the security is applied, and what is covered.

**Borderline cases**

A further category, which touches upon secure communication, is software intended to take advantage of security openings at the end-points. This software category includes [trojan horses](http://en.wikipedia.org/wiki/Trojan_horse), [keyloggers](http://en.wikipedia.org/wiki/Keystroke_logging) and other [spyware](http://en.wikipedia.org/wiki/Spyware).

These types of activity are usually addressed with everyday mainstream security methods, such as [antivirus](http://en.wikipedia.org/wiki/Antivirus) software, [firewalls](http://en.wikipedia.org/wiki/Firewall), programs that identify or neutralize [adware](http://en.wikipedia.org/wiki/Adware) and [spyware](http://en.wikipedia.org/wiki/Spyware), as well as web filtering programs such as [proxomitron](http://en.wikipedia.org/wiki/Proxomitron) and [privoxy](http://en.wikipedia.org/wiki/Privoxy) which check all web pages being read and identify and remove common nuisances contained. As a rule they fall under [computer security](http://en.wikipedia.org/wiki/Computer_security) rather than secure communications.

**Tools used to obtain security**

**Encryption**

Main article: [Encryption](http://en.wikipedia.org/wiki/Encryption)

|  |  |
| --- | --- |
|  | [***Cryptography portal***](http://en.wikipedia.org/wiki/Portal%3ACryptography) |

[Encryption](http://en.wikipedia.org/wiki/Encryption) is where data is rendered hard to read by an unauthorised party. Since encryption can be made extremely hard to break, many communication methods either use deliberately weaker encryption than possible, or have [backdoors](http://en.wikipedia.org/wiki/Backdoor_%28computing%29) inserted to permit rapid decryption. In some cases government authorities have required backdoors be installed in secret. Many methods of encryption are also subject to "man in the middle" attack whereby a third party who can 'see' the establishment of the secure communication is made privy to the encryption method, this would apply for example to interception of computer use at an ISP. Provided it is correctly programmed, sufficiently powerful, and the keys not intercepted, encryption would usually be considered secure. The article on [key size](http://en.wikipedia.org/wiki/Key_size) examines the key requirements for certain degrees of encryption security.

The encryption can be implemented in way to require the use of encryption, i.e. if encrypted communication is impossible then no traffic is sent, or opportunisticly. [Opportunistic encryption](http://en.wikipedia.org/wiki/Opportunistic_encryption) is a lower security method to generally increase the percentage of generic traffic which is encrypted. This is analogous to beginning every conversation with "Do you speak [Navajo](http://en.wikipedia.org/wiki/Code_talker)?" If the response is affirmative, then the conversation proceedes in Navajo, otherwise it uses the common language of the two speakers. This method does not generally provide [authentication](http://en.wikipedia.org/wiki/Authentication) or [anonymity](http://en.wikipedia.org/wiki/Anonymity) but it does protect the content of the conversation from [eavesdropping](http://en.wikipedia.org/wiki/Eavesdropping).

**Steganography**

[Steganography](http://en.wikipedia.org/wiki/Steganography) ("hidden writing") is the means by which data can be hidden within other more innocuous data. Thus a watermark proving ownership embedded in the data of a picture, in such a way it is hard to find or remove unless you know how to find it. or, for communication, the hiding of important data (such as a telephone number) in apparently innocuous data (an MP3 music file). An advantage of steganography is [plausible deniability](http://en.wikipedia.org/wiki/Plausible_deniability), that is, unless one can prove the data is there (which is usually not easy), it is deniable that the file contains any. *(Main article:* [*Steganography*](http://en.wikipedia.org/wiki/Steganography)*)*

**Identity based networks**

Unwanted or malicious behavior is possible on the web since it is inherently anonymous. True identity based networks replace the ability to remain anonymous and are inherently more trustworthy since the identity of the sender and recipient are known. (The telephone system is an example of an identity based network.)

**Anonymized networks**

Recently, anonymous networking has been used to secure communications. In principle, a large number of users running the same system, can have communications routed between them in such a way that it is very hard to detect what any complete message is, which user sent it, and where it is ultimately going from or to. Examples are [Crowds](http://en.wikipedia.org/wiki/Crowds), [Tor](http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29), [I2P](http://en.wikipedia.org/wiki/I2P), [Mixminion](http://en.wikipedia.org/wiki/Mixminion), various [anonymous P2P](http://en.wikipedia.org/wiki/Anonymous_P2P) networks, and others.

**Anonymous communication devices**

In theory, an unknown device would not be noticed, since so many other devices are in use. This is not altogether the case in reality, due to the presence of systems such as [Carnivore](http://en.wikipedia.org/wiki/Carnivore_%28FBI%29) and [Echelon](http://en.wikipedia.org/wiki/ECHELON) which can monitor communications over entire networks, and the fact that the far end may be monitored as before. Examples include [payphones](http://en.wikipedia.org/wiki/Payphone), [Internet cafe](http://en.wikipedia.org/wiki/Internet_cafe), etc.

**Methods used to "break" security**

**Bugging**

Main article: [Covert listening device](http://en.wikipedia.org/wiki/Covert_listening_device)

The placing covertly of monitoring and/or transmission devices either within the communication device, or in the premises concerned.

**Computers (general)**

Main article: [Computer security](http://en.wikipedia.org/wiki/Computer_security)

Any security obtained from a computer is limited by the many ways it can be compromised - by hacking, [keystroke logging](http://en.wikipedia.org/wiki/Keystroke_logging), [backdoors](http://en.wikipedia.org/wiki/Backdoor_%28computing%29), or even in extreme cases by monitoring the tiny electrical signals given off by keyboard or monitors to reconstruct what is typed or seen ([TEMPEST](http://en.wikipedia.org/wiki/TEMPEST), which is quite complex).

**Laser reading of windows**

Main article: [Laser microphone](http://en.wikipedia.org/wiki/Laser_microphone)

In certain cases individuals have had private spoken communications intercepted by means of laser. This usually involves a sensitive laser directed at a window, capable of picking up the tiny glass movements caused by sounds, and conversion back to speech.

**Systems offering a degree of secure communication**

**Anonymous cellphones**

Cellphones can easily be obtained, but are also easily traced and "tapped". There is no (or only limited) encryption, the phones are traceable - often even when switched off - since the phone and SIM card broadcast their International Mobile Subscriber Identity ([IMSI](http://en.wikipedia.org/wiki/IMSI)). It is possible for a cellphone company to turn on some cellphones when the user is unaware and use the microphone to listen in on you, and according to James Atkinson, a [counter-surveillance](http://en.wikipedia.org/wiki/Counter-surveillance) specialist cited in the same source, "Security-conscious corporate executives routinely remove the batteries from their cell phones" since many phones' software can be used "as-is", or modified, to enable transmission without user awareness and the user can be located within a small distance using signal [triangulation](http://en.wikipedia.org/wiki/Triangulation) and now using built in GPS features for newer models.

**Landlines**

Analogue landlines are not encrypted and are trivially tapped. Such tapping requires physical access to the line which is easily obtained from a number of places, e.g. distribution points, cabinets and the exchange itself. Tapping a landline in this way would also enable the attacker to make calls which appear to originate from the tapped line.

**Anonymous Internet**

Main article: [Anonymity](http://en.wikipedia.org/wiki/Anonymity)

Using a third party system of any kind (payphone, Internet cafe) is often quite secure, however if that system is used to access known locations (a known email account or 3rd party) then it may be tapped at the far end, or noted, and this will remove any security benefit obtained. Some countries also impose mandatory registration of Internet cafe users.

[Anomymous proxies](http://en.wikipedia.org/wiki/Anonymous_proxy) are another common type of protection, which allow one to access the net via a third party (often in a different country) and make tracing difficult. Note that there is seldom any guarantee that the [plaintext](http://en.wikipedia.org/wiki/Plaintext) is not tappable, nor that the proxy does not keep its own records of users or entire dialogs. As a result anonymous proxies are a generally useful tool but may not be as secure as other systems whose security can be better assured. Their most common use is to prevent a record of the originating [IP](http://en.wikipedia.org/wiki/IP_address), or address, being left on the target site's own records. Typical anonymous proxies are found at both regular websites such as Anonymizer.com and spynot.com, as well as on proxy sites which maintain up to date lists of large numbers of temporary proxies in operation.

A recent development on this theme arises when wireless Internet connections ("[Wi-fi](http://en.wikipedia.org/wiki/Wi-fi)") are left in their unsecured state. The effect of this is that any person in range of the base unit can [piggyback](http://en.wikipedia.org/w/index.php?title=Piggybacking_(Internet_access)&action=edit&redlink=1) the connection - that is, use it without the owner being aware. Since many connections are left open in this manner anyway, situations where piggybacking might arise (wilful or unaware) have successfully led to a defense in some cases, since it makes it difficult to prove the owner of the connection was the downloader, or had knowledge of the use to which unknown others might be putting their connection. An example of this was the Tammie Marson case, where neighbours and anyone else might have been the culprit in the sharing of copyright files. Conversely, in other cases, people deliberately seek out businesses and households with unsecured connections, for illicit and anonymous Internet usage, or simply to obtain free [bandwidth](http://en.wikipedia.org/wiki/Bandwidth_%28computing%29).

**Programs offering more secure communications**

* [Skype](http://en.wikipedia.org/wiki/Skype) - secure voice over Internet, secure chat. Uses 128-bit AES (256-bit is the standard) and 1024-bit asymmetrical protocols to exchange initial keys (which is considered relatively weak by [NIST](http://en.wikipedia.org/wiki/NIST)). Proprietary. No information on backdoors. An article in 2004 suggested that Skype has relatively weak encryption, but more recent analyses, one by invitation and one by [reverse engineering](http://en.wikipedia.org/wiki/Reverse_engineering) presented at [DEF CON](http://en.wikipedia.org/wiki/DEF_CON) 2005, both conclude that Skype uses encryption effectively. Criticism focuses upon its proprietary "black box" design, its relatively short (1536 bit) keys, excessive bandwidth use of user [supernodes](http://en.wikipedia.org/wiki/Supernode_%28networking%29), and excessive trust of other computers able to "speak Skype". *(See* [*Skype#Security*](http://en.wikipedia.org/wiki/Skype#Security)*)*
* [Zfone](http://en.wikipedia.org/wiki/Zfone) is an [open source](http://en.wikipedia.org/wiki/Open_source) secure voice over Internet program, by [Phil Zimmermann](http://en.wikipedia.org/wiki/Phil_Zimmermann), the creator of [PGP](http://en.wikipedia.org/wiki/Pretty_Good_Privacy). As of [April 2006](http://en.wikipedia.org/wiki/April_2006) it is being [beta tested](http://en.wikipedia.org/wiki/Beta_testing) prior to release.
* [pbxnsip](http://en.wikipedia.org/wiki/Pbxnsip) is a SIP-based PBX that uses TLS and SRTP for encrypting the voice traffic. In contrast to other proprietary protocols, the protocol is open so that devices from independent vendors can be used. The encryption includes the relay of [Instant Messaging](http://en.wikipedia.org/wiki/Instant_Messaging) and [Presence](http://en.wikipedia.org/wiki/Presence) information as well as the management interface.
* Secure [IRC](http://en.wikipedia.org/wiki/IRC) and web chat - Some IRC clients and systems use security such as [SSL](http://en.wikipedia.org/wiki/Secure_Sockets_Layer). This is not standardised. Likewise some web chat clients such as Yahoo Messenger use secure communications on their web based program. Again the security of these is unverified, and it is likely the communication is not secured other than to and from the client.
* [Trillian](http://en.wikipedia.org/wiki/Trillian_%28instant_messenger%29) - offers secure IM facility, however appears to have weaknesses in key exchange which would enable a "man in the middle" attack with ease. Proprietary, no information on backdoors.
* [Off-the-Record Messaging](http://en.wikipedia.org/wiki/Off-the-Record_Messaging) is a plugin which adds end-to-end encryption and authentication as well as [Perfect forward secrecy](http://en.wikipedia.org/wiki/Perfect_forward_secrecy) to instant messaging. It is not a separate protocol but runs under most every [IM](http://en.wikipedia.org/wiki/Instant_messaging_%26_messengers) protocol.
* [WASTE](http://en.wikipedia.org/wiki/WASTE) - open source secure IM, high strength "end to end" encryption, within an anonymised network.
* Secure [email](http://en.wikipedia.org/wiki/Electronic_mail) - some email networks such as "[hushmail](http://en.wikipedia.org/wiki/Hushmail)", are designed to provide encrypted and/or anonymous communication. They authenticate and encrypt on the users own computer, to prevent transmission of plain text, and mask the sender and recipient. [Mixminion](http://en.wikipedia.org/wiki/Mixminion) provides a higher level of anonymity by using a network of anonymizing intermediaries, (similar to how [Tor](http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29) and [crowds](http://en.wikipedia.org/wiki/Crowds) work above).
* [CryptoHeaven](http://en.wikipedia.org/w/index.php?title=CryptoHeaven&action=edit&redlink=1) - [secure email](http://en.wikipedia.org/wiki/E-mail_encryption), secure instant messaging, secure file storage and [sharing](http://en.wikipedia.org/wiki/File_sharing). Provides end-to-end encryption with [AES](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard) standard. Publicly available client [source code](http://en.wikipedia.org/wiki/Source_code) in [Java](http://en.wikipedia.org/wiki/Java_%28programming_language%29) language.

**See also**

**General background**

* [Secure computing](http://en.wikipedia.org/wiki/Secure_computing)
* [Opportunistic encryption](http://en.wikipedia.org/wiki/Opportunistic_encryption)
* [Mass surveillance](http://en.wikipedia.org/wiki/Mass_surveillance)
* [Secure messaging](http://en.wikipedia.org/wiki/Secure_messaging)

**Software selections and comparisons**

* [Comparison of VoIP software](http://en.wikipedia.org/wiki/Comparison_of_VoIP_software)
* [Comparison of instant messaging clients](http://en.wikipedia.org/wiki/Comparison_of_instant_messaging_clients)
* [Anonymous P2P](http://en.wikipedia.org/wiki/Anonymous_P2P)

**Other**

* [Freenet](http://en.wikipedia.org/wiki/Freenet)
* [Hepting vs. AT&T](http://en.wikipedia.org/wiki/Hepting_vs._AT%26T) (a 2006 lawsuit in which the [Electronic Frontier Foundation](http://en.wikipedia.org/wiki/Electronic_Frontier_Foundation) alleges [AT&T](http://en.wikipedia.org/wiki/AT%26T) allowed the [NSA](http://en.wikipedia.org/wiki/NSA) to tap the entirety of its clients' Internet and [Voice over IP](http://en.wikipedia.org/wiki/Voice_over_IP) communications)
* [NSA warrantless surveillance controversy](http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy)
* [Kish cypher](http://en.wikipedia.org/wiki/Kish_cypher)