Secret message in a ping: creation and prevention

LAVINIA MIHAELA DINCA
Economic Cybernetics, Statistics and Informatics
Bucharest Academy of Economic Studies
6 Romana Square, district 1, Bucharest, postal code 010374, postal office 22
ROMANIA
lavinia.dinca@gmail.com

Abstract: - The current methods of communication using steganography techniques involve the use of carrier files including network protocols. The current study presents a new method of communication using steganography techniques available today, the carrier being a ping. The study will also present the most effective ways of prevention against this form of secret communication.

Key-Words: - steganography, information hiding, secret communication, ping, intrusion detection system

1 Introduction

Steganography is the art of secret communication. The word "steganography" is derived from the Greek words steganos which means "covered" and graphia which means writing. A usual description of Steganography is "Hiding in plain sight".

The goal of steganography is to hide the existence of the hidden message. The difference between Steganography and Cryptography is that the latter will make the message unreadable, but the existence of secret communication will be there. Steganography on the other part hides the message and "erases" the existence of any communication.

A steganography message is made up of three components: the "carrier", the message, and the key [1]. The carrier (or cover) can be a digital image, an audio file, even a protocol (like TCP/IP packet) which conceals the hidden message.

Sometimes the word steganography is used to refer to information hiding, steganography and watermarking. Some argue that the three terms are similar but not the same; that there are fundamental philosophical differences that affect the requirements, and thus the design, of a technical solution [2].

Common carrier files for steganography are multimedia files (such as: image, audio and video). These types of files are ideal because they can be posted on the specific Internet site (like YouTube, for video files) without arising suspicion.

Besides the "common" carrier files steganography can be used in internet protocols, mobile devices.

In this area: of using steganography in network protocols the most common methods are:

- using the header of a TCP/IP packet (the message is hidden in the header, the data payload of the packet is not altered) – this is the most common method in use today in the area of network steganography
- using html files. Some time ago spaces were used at the end of each html line of code to hide data (one space for 1 and two spaces for 0 or vice versa). Nowadays key attributes and corresponding attributes are used. Example: if the pair of attributes "align" and "width" is used in this order might mean 1 and 0 or vice versa. HTML language has a lot of attributes pairs which can be used in different order. The method of using pair attributes is harder to construct the data concealment system but is also harder to detect.
- using VOIP – a common practice is to hide a small bit of information (so the sound is not altered) into every VOIP packet.

This paper proposes a new method of secret communication using network steganography – *using a ping as the carrier.*

2 Ping common usage and threats

Ping is a computer network administration tool used to test if a host is reachable or alive and to measure the round trip for messages set from the host to destination computer. The ping program was written by Mike Muss in 1983 and named by the sound that a sonar makes, inspired by the whole principle of echo-location [3].

The program was immediately embedded in Berkeley UNIX and quickly became a standard and is used in all OS (UNIX and Windows) nowadays.

2.1 Usage

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (round-trip time) and records any packet loss [4].

ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet [5]. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user [5].

A common mistake people make is assuming ping can be used to calculate internet bandwidth. In a network the bandwidth is the highest speed of the slowest component [6].

The ping command will send a small packet from the host to the destination and will measure the round trip, but it must be clear that:

- ICMP packet is very small and can be send without being split in chucks
- Internet providers have optimised the ping routes so will respond faster
- The Internet traffic is very large and packets must be sent in chucks. At the destination the chucks must be assembled which can take time and imply processing speed.

In conclusion the round trip calculated by ping shouldn't be used to estimate bandwidth.

2.2 Ping command and response types

The basic ping command syntax is:

#ping *[options]* hostname.

Full options for the ping command can be found in the ping man pages, for example in [7] and many other sources.

The most important ICMP message types (sent from by the destination machine) are presented in *Fig.1 Most important ICMP message types.*

A *ping sweep* is the process of pinging all the addresses within a subnet rage. The ping sweep is widely used in the Scanning and enumeration phase of a Penetration Test. During this phase the penetration tester tries to find active machines.

ICMP Message Type	Description and Important Codes
0: Echo Reply	Answer to a Type 8 Echo Request
3: Destination Unreachable	Error message indicating the host or network cannot be reached. Codes: 0—Destination network unreachable 1—Destination host unreachable 6—Network unknown 7—Host unknown 9—Network administratively prohibited 10—Host administratively prohibited 13—Communication administratively prohibited
4: Source Quench	A congestion control message
5: Redirect	Sent when there are two or more gateways available for the sender to use, and the best route available to the destination is not the configured default gateway. Codes: 0—Redirect datagram for the network 1—Redirect datagram for the host
8: ECHO Request	A ping message, requesting an Echo reply
11: Time Exceeded	The packet took too long to be routed to the destination (Code 0 is TTL expired).

Fig.1 Most important ICMP message types [8]

A network administrator can configure a firewall not to answer ICMP requests, but the ICMP response type will show that there is a filtering device in place preventing response to ICMP requests.

2.3 Ping of death

Ping of death is a well known vulnerability for this protocol. A ping of death (short POD) is a denial of service attack on a computer that uses a malicious ping to crash the target computer. This malicious ping is created by sending an IP packet larger than 65,536 bytes which are allowed by the IP protocol. Ping of death attacks were particularly nasty because the identity of the attacker sending the oversized packet could be easily spoofed and because the attacker didn't need to know anything about the machine they were attacking except for its IP address [9].

This vullnerability was very easy to exploit during early implementations of TCP/IP protol, thus by 1997 all OS have included patches to fobit the ping of death.

2.4 ICMP packet structure

The common ICMP packet structure is depicted below:

ISBN: 978-1-61804-081-7

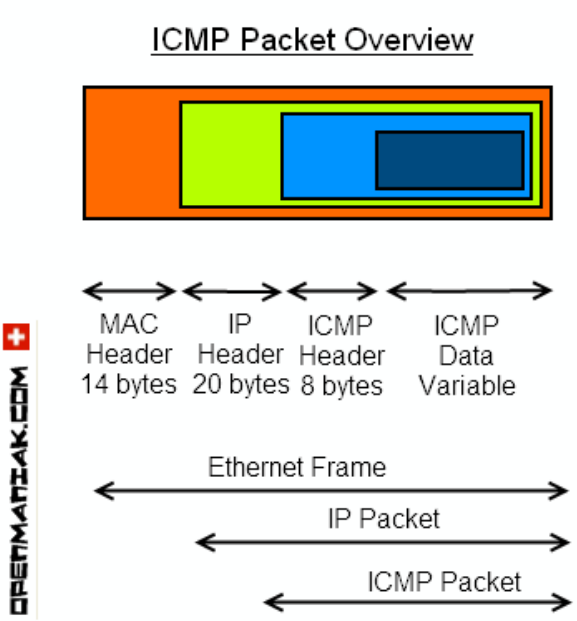

Fig.2 ICMP packet overview [10]

Form the picture above it is obvious that in order to embed secret messages in a ping the *Data variable* (or the data payload) must be modified. If other fields the ICMP packet is changed the protocol will not function properly and might not reach its intended destination.
The RFC 972 [11] that regulates the ICMP protocol doesn't specify what the data payload of the ICMP should be. This makes it ideal for modification since is not regulated and will not affect protocol function.

3 Creating the stego ping

There are a lot of networking tools available (both commercially and open source) that allow a system administrator to send a specially crafted data payload with a ping, including files.
This method is useful in troubleshooting data loses. A normal ping can arrive at its destination with no packet losses, but one with payload might experience packet loses. – in this case there is a problem with data packets in the network.
In order to create the stego ping a tool that creates a ping data payload will be used. The message will be hidden in the data payload.
Small files should be used as carrier files due to the fact that ICMP is in essence a small packet send to test if a system is alive and that a big package, deviating from the norm, will attract attention.
Carrier files like audio, video, images can't be used, the best option being text files and small jpeg files.
In steganography the strength of an algorithm is measured by a series of factors such as:

- *Hiding capacity* represents the size of information that can be hidden compared to the length of the message.
- *Perceptual transparency* represents how much information can be hidden in a host file without visible alteration of that file or loss in quality.
- *Security* – the difficulty of detecting the hidden information. Usually security relates with capacity – if a large amount of information is hidden in a cover medium it will be easier to detect.
- *Robustness* is the ability of embedded data to remain intact if the host image undergoes transformation such as lossy compression, scaling, rotating etc.
- *Tamper resistance* refers to the difficulty for an attacker to forge or to replace the message once it has been embedded into the host file.

It is clear that hiding capacity is influenced by the length of the carrier file it self. We can't hide more information in bytes that exceed the carrier medium size. If we hide information in a carrier file the resulting stego file will be bigger in size.
For this test the same small message will be hidden in both text and image file, which is: *A test for a stego ping*.

3.1 Creating the image file

The selection of the cover image is very important. As best practice the images downloaded from the internet shouldn't be used as they are. Before using a downloaded image, the image should be altered by image editing tools such as: resizing, reversing the colours etc. This way there is no "original" copy of the carrier file that can be used to be compared with. Even if the embedded message can't be extracted from the stego file, if there is an original file to be compared with it's enough to attract suspicion that a secret message is being transmitted.
The best cover images are the ones with many details, which don't have large portion with the same colour.
For creating the stego image Invisible Secrets 4 was used, with hide only option, no encryption. The following file was generated:

ISBN: 978-1-61804-081-7

Fig.3 Stego file containing the secret message

The original file size was 69.0 kB and the resulting stego file (containing the secret message) was 69,2 kB.

3.2 Creating the text file

There are several methods of hiding data into documents. The well known ones are:

- *Open text methods* such as inter-sentence spacing, end of line spacing, inter-word spacing. These methods are not reliable if the document is in an editable format, because the hidden message can be removed by simple text formatting.
- *Syntactic method* – punctuation manipulation to hide information.
- *Semantic method* – this method uses synonyms for primary and secondary value. For example, the word "beautiful" could be considered primary and "exhilarating" secondary. Whether a word has primary or secondary value bears no relevance to how often it will be used, but primary words will be read as ones, secondary words as zeros when decoding [12].
- *New file generation* – new files are generated in order to create the message. This latest method described is the best way to hide information inside documents because it doesn't use o cover document, but rather creates one. A popular program that can do that is: spammimic [13].

For this test the last method will be used (new file generation). Using spammimic the following spam message was generated:

Dear Friend , You made the right decision when you signed up for our database ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1623 ; Title 5 , Section 308 . Do NOT confuse us with Internet scam artists ! Why work for somebody else when you can become rich in 20 MONTHS ! Have you ever noticed most everyone has a cellphone and nearly every commercial on television has a .com on in it , Well, now is your chance to capitalize on this . We will help you process your orders within seconds & process your orders within seconds . You can begin at absolutely no cost to you ! But don't believe us ! Ms Anderson who resides in Washington tried us and says "I was skeptical but it worked for me" ! We are licensed to operate in all states , If not for you then for your loved ones - act now . Sign up a friend and you get half off . Thank-you for your serious consideration of our offer ! Dear Business person ; This letter was specially selected to be sent to you ! If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail . This mail is being sent in compliance with Senate bill 1620 ; Title 6 ; Section 306 . This is not a get rich scheme . Why work for somebody else when you can become rich within 63 MONTHS . Have you ever noticed people love convenience & people are much more likely to BUY with a credit card than cash ! Well, now is your chance to capitalize on this . We will help you increase customer response by 160% & increase customer response by 170% . You can begin at absolutely no cost to you . But don't believe us ! Ms Ames who resides in New Jersey tried us and says "Now I'm rich, Rich, RICH" ! We assure you that we operate within all applicable laws ! We beseech you - act now ! Sign up a friend and you'll get a discount of 10% ! God Bless .

Fig.4 – Generated spam message

The spam message was saved into a text file that will be used in the test. The size of the text file is 1,83 kB.

3.3 Tool used to create the stego ping

NetScanTools Pro 10.96 Demo version is one of the tools available that can send a data file as attachment to a ping. NetScanTools Pro 10.96 Demo has several network tools available but for the purpose of the test Ping – *Enhanced* was used with the options depicted in the picture below:

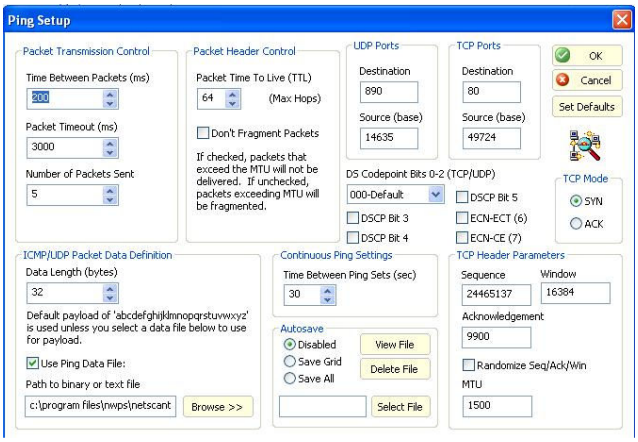

Fig.5 – Ping options

The stego ping is now ready to be sent. In the method described there are two distinctive stego pings: one carrying the jpeg data file and the other one with the text file.

4 Prevention against the stego ping

The best method of prevention against this steganography method is to configure the firewall to filter (not respond) to ICMP packets. This way the ping packet will be dropped and not received. This solution is very useful for external pings – a ping outside the local network.

The proposed method works very well inside a firewall because pings can be sent to internal

ISBN: 978-1-61804-081-7

machines. The person for whom the message is intended might have a packet capture in place that will pick up the stego pings and decipher them.
Inside a network is not common practice to block pings by firewalls. In order to prevent this type of communication an Intrusion Detection System (IDS) must be installed.
An IDS is a software application or specialized software equipment that automates the process of monitoring a computer system or network and alerts the administrator about suspect behavior.
There are experts that don't believe in IDS efficiency but in general they add a new layer of security. Secure systems are impossible because it entails securing a system for both present and future threats (14).
IDS are classified by different methods such as:

- By Response type:
  - *Active* – known as IPS – Intrusion prevention system can be configured to take active actions such as: block suspected attacks in progress without any intervention from a network administrator.
  - *Pasive* – can be configured only to monitor and analyze traffic, the network administrator will take the required actions
- By enviroment type:
  - *Network based* – ussualy a newtok sensors placed at varius points in a network. This IDS capture and analyse network packets in order to detect and attack
  - *Host based* – agents (small programs) are installed on individual systems. A host based IDS can monitor only the hosts it is installed on.
- By engine type:
  - *Knowledge based (signature based)* – a database of known system vulnerabilities, intrusion techniques etc is used to detect possible intrusions
  - *Behavior based* – a baseline of normal system behavior is used to identify possible intrusions.

Large enterprises have complex IDS already installed with agents in critical nodes. The medium small enterprises usually don't have IDS installed. For the purpose of security in general (in particular for prevention against the method described in this paper) small and medium enterprises should install an IDS. There are a lot of commercially available IDS that range from a variety of prices. A very popular and complex open source IDS is S*nort* which is platform independent and ideal for small and even medium enterprises.

5 Conclusion

This paper examined the possibility of using the ping command for sending messages using steganography. The proposed method is very easy to implement because it uses available tools on the internet: some commercial some freeware.
The proposed method used NetPro Tools 10 (demo version) to generate the stego ping – a ping that sends a data payload consisting of a file with data hidden in it. Two types of files were created:

- a jpeg file – the secret message was embedded in the file using Invisible Secrets 4.
- a text file – the text contained in the file was generated with the spammimic program, freely available from the internet.

The best type of file to be used is a text file, because a normal ping has a small payload.
The methods of prevention should be classified into two distinct categories:

- *External* (pings from outside the internal network). The best method of prevention is to configure the firewall to filter ICMP requests this way the ping will not receive the intended destination.
- *Internal* (ping from inside the network). Since is not practical to filter ICMP packets from internal network suspicious pings need to be analyzed. The best way to do that is to install an Intrusion Detection System (even a lightweight one) that will monitor traffic and report anomalies based on configured rules.

This type of secret communication is not very dangerous because: most firewalls are setup to block ICMP request and the amount of data that can be sent in (without attracting any suspicion) is very small.

References:

1. Kesslet, Gary C, An Overview of Steganography for the Computer Forensics Examiner, *Forensic Science Communications*, 2004.
2. Ingemar J. Cox; Matthew L. Miller; Jeffrey A. Bloom; Jessica Fridrich; Ton Kalker, Digital

Watermarking and Steganography, *Morgan Kaufmann*, 2008, 978-0-12-372585-1.
3. Muuss, Mike, The Story of the PING Program, *http://ftp.arl.army.mil.* [Online] [Cited: 12 03, 2011.] http://ftp.arl.mil/mike/ping.html.
4. Ping, *Wikipedia.* [Online] [Cited: 12 04, 2011.] http://en.wikipedia.org/wiki/Ping.
5. ICMP, *Searchnetworking.* [Online] [Cited: 12 10, 2011.] http://searchnetworking.techtarget.com/definition/ICMP.
6. J.C. Kessels, The Ping Fallacy. *Numion.* [Online] [Cited: 12 10, 2011.] http://www.numion.com/faq/ping.html.
7. ping(8) - Linux man page. [Online] [Cited: 12 12, 2011.] http://linux.die.net/man/8/ping.
8. Walker, Matt, *Certified Ethical Hacker.* s.l. : McGraw-Hill, 2011. 978-0-07-177229-7.
9. Ping of death [Online] [Cited: 12 10, 2011.] http://searchsecurity.techtarget.com/definition/ping-of-death.
10. Ping. *Openmaniack.* [Online] [Cited: 12 10, 2011.] http://openmaniak.com/ping.php.
11. RFC 792 - Internet Control Message Protocol, *http://www.ietf.org.* [Online] [Cited: 12 23, 2011.] http://www.ietf.org/rfc/rfc792.txt.
12. Kipper, Greg, Investigators guide to Steganography, *Auerbach Publications*, 2004.
13. [Online] [Cited: 01 04, 2011.] https://www.spammimic.com/.
14. Pfleeger, C. F., & Pfleeger, S. L**,** Security in computing (3rd edition), *Upper Saddle River* , NJ: Pearson, 2003.