Anonymity in the service of attackers

Guillermo Suarez de Tangil Rotaeche (Researcher), Esther Palomar (Assistant Professor), Arturo Ribagorda Garnacho (Full Professor), Benjamín Ramos Álvarez (Professor)

SeTI - Group of Security of Information Technologies and the Communication,
Department of Computer Sciences, Univ. Carlos III de Madrid
Avda. Universidad 30, 28911 Leganés, Madrid
Teléfono: 0034 91 624 94 22 Fax: 0034 91 624 91 29
gtangil@pa.uc3m.es, {epalomar, arturo, benja1}@inf.uc3m.es

Abstract. Since its conception, malware users have focused on either hiding or camouflaging their identities and their locations in the Internet as a primary objective. To counter this challenge, attackers use traditional techniques based on the manipulation of TCP/IP elements as well as the most modern attack methods conceived to provide anonymity in the Internet. In fact, emergent research on improving network anonymity especially designed to protect well-behaving users lead to malicious users are undoubtedly favoured. In this article, we describe the aforementioned techniques, i.e. those based on traditional concepts and those which apply recent mechanisms used by the attacker in order to protect her identity. Moreover, we discuss the need for providing anonymity to users in the Internet without it implying new vulnerabilities that favor dishonest intentions.

Key Words. Attacker identification, Malware, Anonymity, Attack localization, Hiding the identity.

1. Introduction

Ever since its conception, objectives of what is nowadays known as **malware,** and consequently the malicious behavior of such techniques, has highly evolved. As an example, Creeper [1, p. 10], i.e. one of the first viruses recognized as such, was developed based on a simple purpose: to attract attention. Its behavior was limited to displaying the following message: "I'm creeper... catch me if you can!". Certainly, it was in the 80s when software designs conceived from malicious intentions appear, meanwhile attackers also identify being undetected as a priority. Additionally, this need increased since law courts start judging early authors of virus (see the case of Robert Tappan Morris [14], sentenced in 1990 to four years in jail for creating a virus spread through ARPANET).

The attacker tried to hide her identity and location over the network by seeking impunity on the legal consequences that may be derived from their actions. For example, it is worth mentioning the well-known Denial of Service attack (DoS) and the massive sending of undesired e-mail (called Spam) just to name a few of current dishonest acts.

To protect his identity, the attacker applies several mechanisms generally designed for a specific type of attack. Some of these mechanism are more effective than others, and are more suitable for a certain type of attack while others are not. Therefore, specific mechanisms were developed by means of the manipulation of the lower layers of the protocol stack. Moreover, attackers can determine the required level of anonymity according on the desired impact of the attack. On the other hand, recent mechanisms, aimed at providing anonymity to well-behaving networking users, become a potential tool for misbehavior. In this article, we review both earlier methods as well as the most recent techniques used by attackers to protect their identity.

The reminder of the paper is organized in the following way: First, we briefly survey the traditional techniques in Section 2. Section 3 is focused on the exploration of recent anonymity techniques suitable for masquerading identity and location. Finally, Section 4 presents some conclusions and research directions.

2. Traditional anonymity strategies

As defined in [4], anonymity allows to hide the elements and attributes which identify a transaction and/or the participats within a given interaction. Thus, to remain anonymous, the attacker should attempt to either disguise the elements that characterize the attack or hide the source of its acts. For instance, in the case of a *botnet*, the attacker does not necessarily worry about hiding the activity of bots (i.e. any node controlled by her without the owner's authorization) but indeed should anonymize the communication between her machine and the master engine (i.e. which controls the compromised bots).

2.1. Overview

Nowadays several open tools are free-available on the Web that assist administrators in tracing the source of a network activity without requiring special computational resources or technical knowledge either. Similarly, note that, in general antivirus toolkits provide a friendly interface for monitoring tasks. Attackers must deal with such accessible tools. Similarly, in particular cases, even though it represents a slow process, communication operator authorities and/or Internet Service Providers (ISPs) are involved in jointly contributing the evidences against a given computer crime. This is critical especially when the collaborative countries do not share the computer crime legislation.

On the other hand, the localization process becomes enormously hard as attackers employs *proxy* and *zombie* (like bots) nodes. As stated before, it is a common practice that the attacker recruits several compromised computers as some kind of gateway between her machine and victims. Various *proxy* methods are the following [2]: Generic Port Routing (e.g. GRE tunneling [3]), HTTP proxy, Socks proxy, and IRC (Internet Relay Chat) channels. I addition, since the proliferation of weakly encrypted wireless networks (WEP [5]), attackers can get easily anonymous locations.

Regarding legal concerns, there is an emerging interest in providing a global legal framework against the use of malware [1, p. 81]. There are also several working groups, such as those created by the International Consumer Protection and Enforcement Network (ICPEN), aimed at integrating the information exchange on cybercrime within different countries.

Next sections outline the security vulnerabilities in TCP/IP communications, which provide attackers with different levels of anonymity.

2.2. TCP/IP vulnerabilities

TCP/IP was originally designed focusing on the provision of high levels of reliability as well as prevailing the interconnectivity among heterogeneous systems and networks. However, several security properties had to be incrementally addressed by later solutions such as *IPSec*, and IPv6. In particular, most TCP/IP vulnerabilities exist due to the existence of an underlying trust on the source address of IP packets as a mechanism to authenticate the source of the connection.

For instance, it is simple enough to discover, even modify, the participant nodes of a given interaction using appropriate traffic analysis tools, e.g. *sniffers*. We refer the interested reader to further details on the *IP Spoofing* attack [19] which is a common tactic used in a DoS attack. Thus, TCP/IP protocol suite presents a set of security problems inherited from its design, which provides a few security weak points that attackers use in order to hide their identities, among others. The interested reader may consult Ref.[6] for a comprehensive analysis of the security problems associated with the family of TCP/IP protocols.

2.3. Manipulation of TCP/IP elements

We have identified two main strategies commonly applied by attackers aimed at being undetected. On the one hand, the attacker is focused on prevent a trace-back mechanism by means of hiding its actions. Thus, the victim will not be able to realize that an attack is being carried out [7]. This strategy is based on the application of anti-detection methods. As an example, work in [8] presents the use of mechanisms like *FIN Scanning* to avoid recording TCP sessions.

On the other hand, the attacker may directly inject fake information into the IP packets. The classic attack of *IP Spoofing* is classified within this strategy, in which the attacker replaces the source address of the IP packet with a fake one establishing a forged connection from an innocent network host (see Figure 1). In this context, the attacker sends packets without showing any evidence of her authorship. However, this strategy also presents some limitations, e.g. the attacker will not be able to receive any packet back. In this case, it is only possible to launch DoS attacks and, occasionally, *port scanning* [9, p. 195].

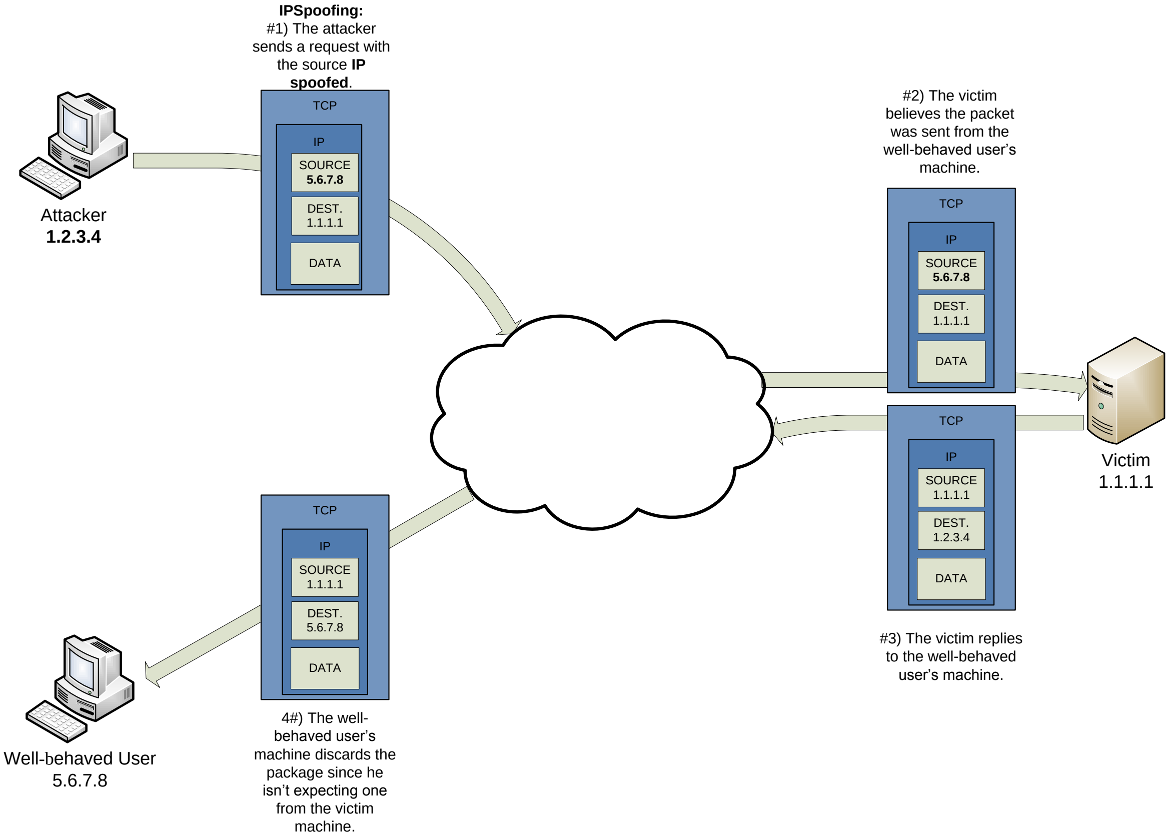
IPSpoofing:
#1) The attacker sends a request with the source IP spoofed.
Attacker
1.2.3.4
TCP
IP
SOURCE
5.6.7.8
DEST.
1.1.1.1
DATA
#2) The victim believes the packet was sent from the well-behaved user's machine.
TCP
IP
SOURCE
5.6.7.8
DEST.
1.1.1.1
DATA
Victim
1.1.1.1
TCP
IP
SOURCE
1.1.1.1
DEST.
1.2.3.4
DATA
#3) The victim replies to the well-behaved user's machine.
TCP
IP
SOURCE
1.1.1.1
DEST.
5.6.7.8
DATA
Well-behaved User
5.6.7.8
4#) The well-behaved user's machine discards the package since he isn't expecting one from the victim machine.

Figure 1: IP Spoofing. The figure shows how the attacker spoofs the Source field of the IP packet so it won't be stated as a source of communication.

3. Current anonymity strategies

As a result of the emerging needs imposed by users of IT, research on anonymity over the Internet has attracted an increasing attention in recent years. In this section, we outline current anonymity techniques as well as the related attacks.

3.1. Current Anonymity approaches

In general, a classification of the current anonymity techniques relies on establishing what must be kept anonymous during the communication, i.e. the identity of the interacting parties or the interaction as a whole. Classification proposed in [4] identifies two different strategies according to the network routing protocol: *relay* and *random routing*.

In relay routing, the anonymity strategy is based on centralizing the routing information into a certain relaying node which acts as a proxy. *Anonymizer* for HTTP traffic [18] is a popular mechanism within this category. However, the concept of *Mix network* introduced by David Chaum in [10] is the building block for most anonymity systems. A mix network establishes every transmission through a set of routers (or proxy servers) by means of encrypting every message hop-by-hop with the corresponding key of each router. The message is re-encrypted and layered.

In random routing, *Tor network* (TCP based Onion Routing) is one of the most popular approach. Each hop each router agrees a symmetric key to repeatedly uncover the message. Figure 2 shows a Tor network scenario and the construction of messages transmitted among the Tor nodes. *Mixmaster*, *Buses*, *Mixonion*, *MorphMix*, *PIPENET*, *Babel* and *Tarzan* are well-known examples of this technology.

Furthermore, *Crowds*, *Freenet* and *Onion Routing* are also random routing based systems aimed at protecting sources' location by sending fragments of the IP packet through random paths.

3.2. Attacks based on recent anonymity strategies

We briefly describe the related attacks based on the application of recent anonymity methods mentioned above, as follows:

- Tor-based attacks: Work in [11] presents an experimental analysis of the malicious use of IRC (i.e. the protocol used by most *botnet* master machine to communicate with bots) channels by *bots* which receive instructions from TOR nodes. In fact, most IRC operators have decided to avoid the access to TOR networks [12].

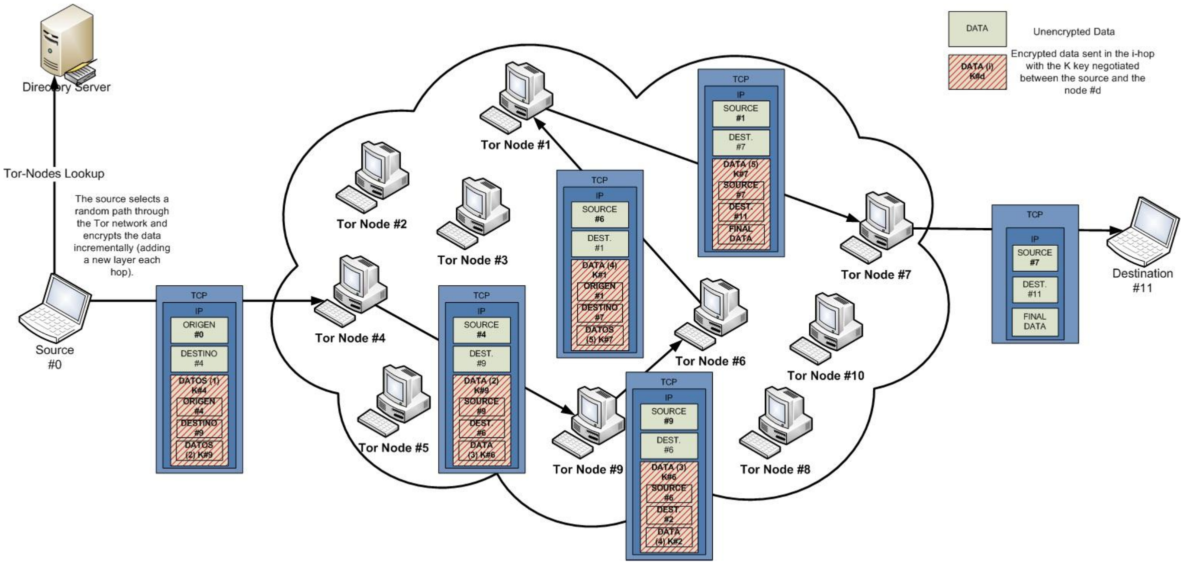

Figure 2: Tor network. The source establishes an anonymous communication with the destination through a set of randomly chosen nodes, and incrementally encrypts the message, i.e. adding a layer each hop.

- Potential attacks based on *Anonymizer*: Several trojans, such as Bobax [13], provide attackers with web services to use the tools designed for HTTP anonymity like *Anonymizer*. In this context, the anonymity level is determined by the security policies defined on the proxy. In this way, the location of the attacker could be traced whether any of the following situations occur: (1) the server records the client sessions, or (2) legal authorities require all the traces.

- Attacks based on *Buses*: *Buses* shares functionalities with Tor network most in the way that messages are layered-encrypted. However, unlike Tor, routes are not created at random as well as messages are sent to next hops in a list (--- this operation is similar to a circular bus-line where every packet is forwarded to the next hop). Moreover, work presented in [17] proposes a malware implementation using Buses. Experimentation presents several results: Buses shows a higher performance efficacy than those networks based on random routing, the same anonymity levels, and a lower latency than Mix networks.

4. Conclusions

In recent years, anonymity in the Internet have attracted considerable interest. On the one hand, honest users require anonymity in order to protect their privacy and, on the other hand, anonymity represents a perfect tool for misbehaving. Thus, anonymity techniques have evolved as well. In this article, we have reviewed both traditional and recent techniques designed to provide anonymity to users on the Internet. As these techniques proliferate and consolidate on the Web, new vulnerabilities are discovered indirectly, especially in social-based applications.

In [15, 16] authors argue that recent anonymizing networks do not represent potential threats to privacy, since attackers already have tools that provide anonymity (see Section 2). However, although we certainly have not found in the literature many indicators that attackers are getting benefits from the technologies described in Section 3, we still consider them as a potential tool for masquerading dishonest actions. For instance, authors in [17] propose an implementation of malicious software based on anonymity networks.

In summary, we discuss in this paper the necessity of an integral solution that provides anonymity meanwhile prevent malicious users from taking advantage of it. In this context, the proposal mentioned before [17] also defines a solution based on involving users in the secure identification of encrypted messages.

References

1. Plonk, A., Carblanc, A., et Grupo de Trabajo de Seguridad de la Información y Protección de la Privacidad: Software malicioso (*malware*) una amenaza de seguridad para la economía de internet. CERT. Report No.: DSTI/ICCP/REG(2007)5/FINAL (2008)

2. Ianelli, N., Hackworth, A.: Botnets as a vehicle for online crime. The International Journal of FORENSIC COMPUTER SCIENCE, Vol. 2, No. 1 (2007) 19-39

3. Hanks, S., Li, T., Farinacci, D., Traina, P.: Generic routing encapsulation (GRE). RFC Editor United States (2000) RFC2784

4. Bertolín, J.A., Bertolín, G.A.: Identificación y análisis del anonimato en comunicaciones electrónicas. Revista Española de Electrónica Nº 627 (2007) 32-45

5. Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the key scheduling algorithm of rc4. Lecture Notes in Computer Science (2001) 1-24 Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography.

6. Bellovin, S.: Security problems in the TCP/IP protocol suite. ACM SIGCOMM Computer Communication Review, Vol. 19, No. 2 (1989) 32-48

7. Tan, K.M.C., McHugh, J., Killourhy, K.S.: Hiding intrusions: From the abnormal to the normal and beyond. In proceedings of the 5th International Workshop on Information Hiding, London, UK, Springer-Verlag (2003) 1-17

8. Mahoney, M.V., Chan, P.K.: An analysis of the 1999 darpa/lincoln laboratory evaluation data for network anomaly detection. In proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Florida, USA, Springer-Verlag (2003) 220-237

9. Zalewski, M.: Silence on the wire: a field guide to passive reconnaissance and indirect attacks. William Pollock (2005)

10. Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, Vol. 24, No. 2 (1981) 84-88

11. Dagon, D., Gu, G., Zou, C., Grizzard, J., Dwivedi, S.J., Lee, W., Lipton, R.: A taxonomy of botnets. Unpublished paper (2005)

12. Torproject: List of irc/chat networks that block or support tor (2009) https://wiki.torproject.org/noreply/TheOnionRouter/BlockingIrc

13. Stewart, J.: Bobax trojan analysis (2004) http://www.secureworks.com/ research/threats/bobax/.

14. Standler, R.B.: Judgment in U.S. v. Robert Tappan Morris (2002) http://www.rbs2.com/morris.htm

15. Shue, C., Gupta, M.: Hiding in Plain Sight: Exploiting Broadcast for Practical Host Anonymity. In proceedings of Hawaii International Conference on System Sciences (HICSS) (2010)

16. Torproject: Abuse faq (2009) http://www.torproject.org/faq-abuse.html.en#WhatAboutCriminals

17. Hirt, A., Aycock, J.: Anonymous and malicious. Berlin. In: 15th Virus Bulletin International Conference. Vol. 2, Citeseer (2005)

18. Boyan, J., The Anonymizer: Protecting User Privacy on the Web. In: Computer-Mediated Communication Magazine, Vol. 4, No. 9 (1997)

19. Tanase, M.,: IP spoofing: an introduction. In: Security Focus (2003) http://www.securityfocus.com/infocus/1674