UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by Novática <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*, <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- InfoRewiew, magazine from the Serbian CEPIS society JISA
- Informatica, journal from the Slovenian CEPIS society SDI
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Pliroforiki, journal from the Cyprus CEPIS society CCS
- Tölvumál, journal from the Icelandic CEPIS society ISIP

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Monograph of next issue (April 2010)

"Information Technology inTourism Industry"

(The full schedule of **UP**GRADE is available at our website)

CEPIS UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

Vol. XI, issue No. 1, February 2010

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

Anonymity in the Service of Attackers

Guillermo Suarez de Tangil-Rotaeche, Esther Palomar-González, Arturo Ribagorda- Garnacho, and Benjamín Ramos-Álvarez

Since the inception of malware, the primary objective of its authors has been to either hide or camouflage their identities and locations in the Internet. To do this, 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 this respect, the growing body of research into improving network anonymity intended to protect well-behaved users against malicious users has actually benefited the attackers. In this article, we describe the aforementioned techniques; i.e. those based on traditional concepts and those which apply recent mechanisms used by attackers in order to protect their identity. We also discuss the need to provide anonymity to Internet users without creating new vulnerabilities that open the door to dishonest intentions.

Keywords: Anonymity, Attack Localization, Attacker Identification, Hiding Identity, Malware.

1 Introduction

Since the inception of what is known today as **malware**, its objectives, and consequently the malicious behaviour of such techniques, have evolved considerably. As an example, Creeper [1, p 10], one of the first viruses recognized as such, was developed based on a simple purpose: to attract attention. Its behaviour was limited to displaying the following message: "*I'm creeper... catch me if you can!*". It was in the 80s when software designs conceived with malicious intent first appeared and attackers made remaining undetected their priority. This need for undetectability increased when early authors of viruses started to be put on trial (see the case of Robert Tappan Morris [2], who received a four year sentence in 1990 for creating a virus spread through ARPANET).

Attackers tried to seek immunity from any legal consequences arising from their actions by hiding their identity and location on the Internet. By way of example we might mention the well-known Denial of Service attack (DoS) and the massive sending of undesired e-mail (known as spam), to name but a few of the malicious acts being committed today.

To protect their identity, attackers use several mechanisms usually designed for a specific type of attack. Some of these mechanisms are more effective than others, and are more suitable for a certain type of attack than others. Thus, specific mechanisms were developed by manipulating the lower layers of the protocol stack. Attackers can also determine the required level of anonymity according to the desired impact of the attack. Meanwhile, recent mechanisms aimed at providing anonymity to well-behaved networking users have become a potential tool for misbehaviour. In this article, we review both earlier methods and more recent techniques used by attackers to protect their identity.

The remainder 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 used for masking identity and location. Finally, Section 4 presents some conclusions and research directions.

Authors

Guillermo Suárez de Tangil-Rotaeche graduated as a Computer Engineer from the *Universidad Carlos III de Madrid*, Spain, in 2008. He is a senior researcher in the ICT Security Group (SeTI) of the same university and a member of the CENIT-Segur@ project research team. He is currently working towards his PhD degree. His research interests are focused on the area of automatic intrusion detection using artificial intelligence techniques. His research has produced several contributions in international conferences and journals. <gtangil@pa.uc3m.es>

Esther Palomar-González is an Assistant Professor in the Computer Science Department of the *Universidad Carlos III de Madrid*, Spain. She earned her PhD in Computer Science from the same university in 2008. Before joining the university she worked as a forensic auditor for a well-known firm in the field. Her research interests currently revolve around building secure peer-to-peer and ad hoc systems and include security protocol formalisms by evolutionary computation. <epalomar@inf.uc3m.es>

Arturo Ribagorda-Garnacho is a Telecommunications Engineering and holds a PhD in Computer Science from the *Universidad Politécnica de Madrid*, Spain. He is a Full Professor at the *Universidad Carlos III de Madrid*, leading its IT security research group. He has participated, and currently participates, in several national and European research projects. He has published numerous articles in national and international journals and conferences. <arturo@inf.uc3m.es>

Benjamin Ramos-Álvarez is an Associate Professor in the Computer Science Department at the *Universidad Carlos III de Madrid*, Spain. His research is mainly focused on authentication and non-repudiation issues of electronic signatures. He received his PhD degree in Computer Science from the same university in 1999. <benja1@inf.uc3m.es>

2 Traditional Anonymity Strategies

As defined in [3], anonymity allows the elements and

attributes which identify a transaction and/or the participants in a given interaction to remain hidden. Thus, to remain anonymous, attackers must attempt to either disguise the elements that characterize the attack or hide the source of their acts. For instance, in the case of a *botnet*, attackers do not necessarily worry about hiding the activity of bots (i.e. any node controlled by them without the owner's authorization) but they do need to anonymize communication between their machine and the master engine (i.e. the one which controls the compromised bots).

2.1 Overview

Nowadays several open tools are freely available on the Web which help administrators trace the source of a network activity without requiring either special computational resources or technical knowledge. In general, antivirus toolkits provide a friendly interface for monitoring tasks, and attackers need to find a way to get around these readily available tools. Also, in some particular cases, even though it is a slow process, communication operator authorities and/or Internet Service Providers (ISPs) are jointly involved in providing evidence to prove that a particular computer crime has been committed. This is especially critical when collaborating countries do not share the same computer crime legislation.

However, the localization process becomes enormously difficult when attackers employ *proxy* and *zombie* (like bots) nodes. As mentioned earlier, it is common practice for attackers to recruit several compromised computers as a kind of gateway between their machines and those of their victims. Among the various *proxy* methods used are the following [4]: Generic Port Routing (e.g. GRE tunnelling [5]), HTTP proxy, Socks proxy, and IRC (Internet Relay Chat) channels. In addition, since the proliferation of weakly encrypted wireless networks (WEP [6]), attackers can easily obtain anonymous locations.

With regard to 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 information exchange on cybercrime between different countries.

The following paragraphs outline the security

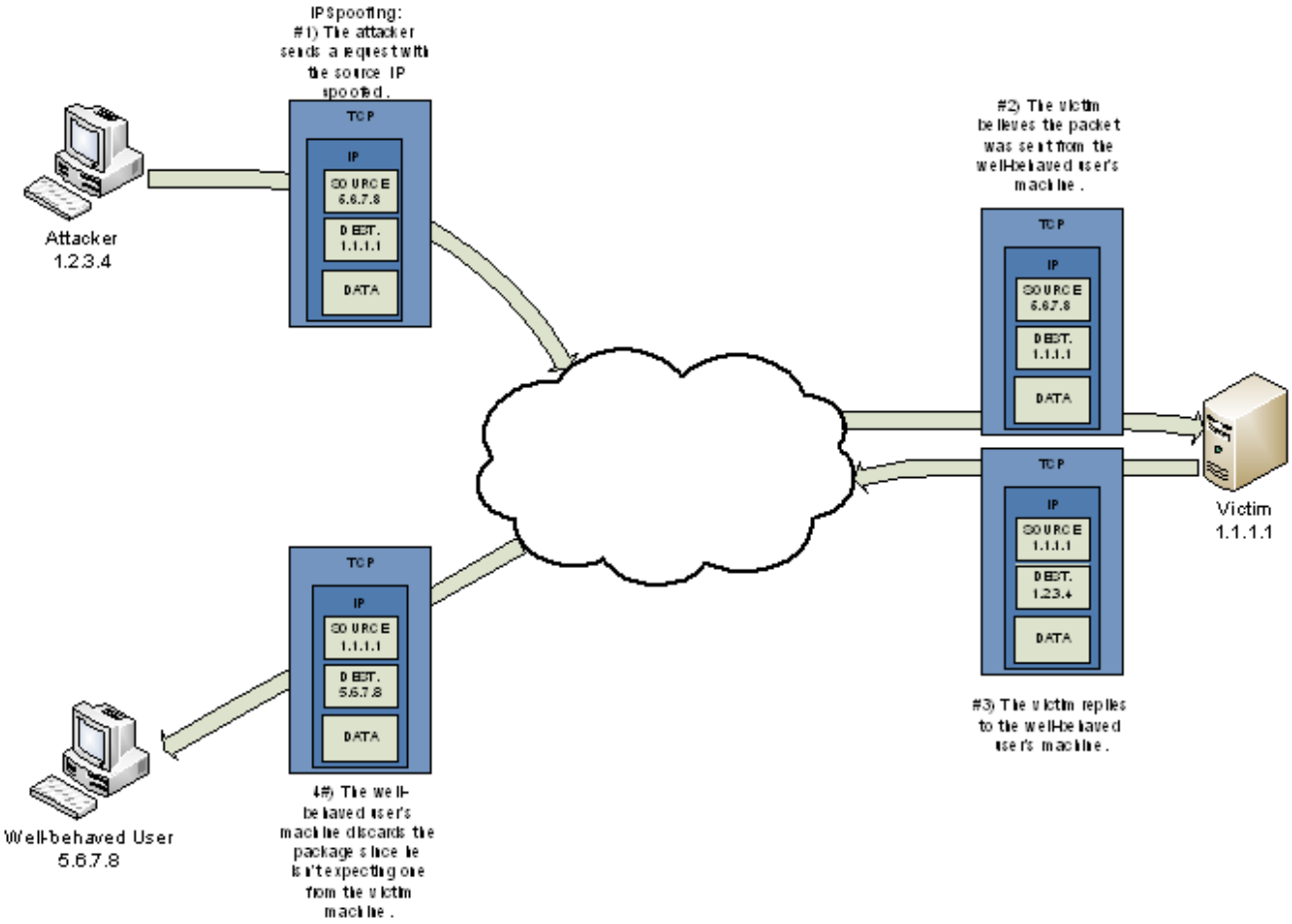

Figure 1: IP Spoofing. The figure shows how the attacker spoofs the source field of the IP packet so it will not be stated as a source of communication.

vulnerabilities in TCP/IP communications, which provide attackers with different levels of anonymity.

2.2 TCP/IP Vulnerabilities

TCP/IP was originally designed for the purpose of providing high levels of reliability while maintaining interconnectivity between heterogeneous systems and networks. However, several security properties had to be incrementally addressed by later solutions such as *IPSec*, and IPv6. Most TCP/IP vulnerabilities exist due to the existence of an underlying trust in the source address of IP packets as a mechanism for authenticating the source of the connection.

For instance, it is simple enough to discover, and even modify, the participant nodes of a given interaction using appropriate traffic analysis tools, e.g. *sniffers*. We refer interested readers to further details on the *IP Spoofing* attack [7], which is a common tactic used in a DoS attack. Thus, the TCP/IP protocol suite presents a series of security problems inherited from its original design, which provides a number of security weak points that attackers use in order to hide their identities. Interested readers may like to consult [8] 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 aiming to remain undetected. On the one hand, attackers try to prevent a trace-back mechanism by hiding their actions. Thus, the victim will not be able to realize that an attack is being carried out [9]. This strategy is based on the application of anti-detection methods. As an example, work in [10] presents the use of mechanisms such as *FIN Scanning* to prevent TCP sessions from being logged.

On the other hand, the attacker may directly inject fake information into the IP packets. The classic attack of *IP Spoofing* is an example of this type of 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). Thus, attackers send packets without showing any evidence of their 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* [11, p 195].

3 Current Anonymity Strategies

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

3.1 Current anonymity approaches

In general, to classify current anonymity techniques we first need to establish what must be kept anonymous during the communication; i.e. the identity of the interacting parties or the interaction as a whole. The classification proposed in [3] 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 [12] is a popular mechanism in this category. However, the con-

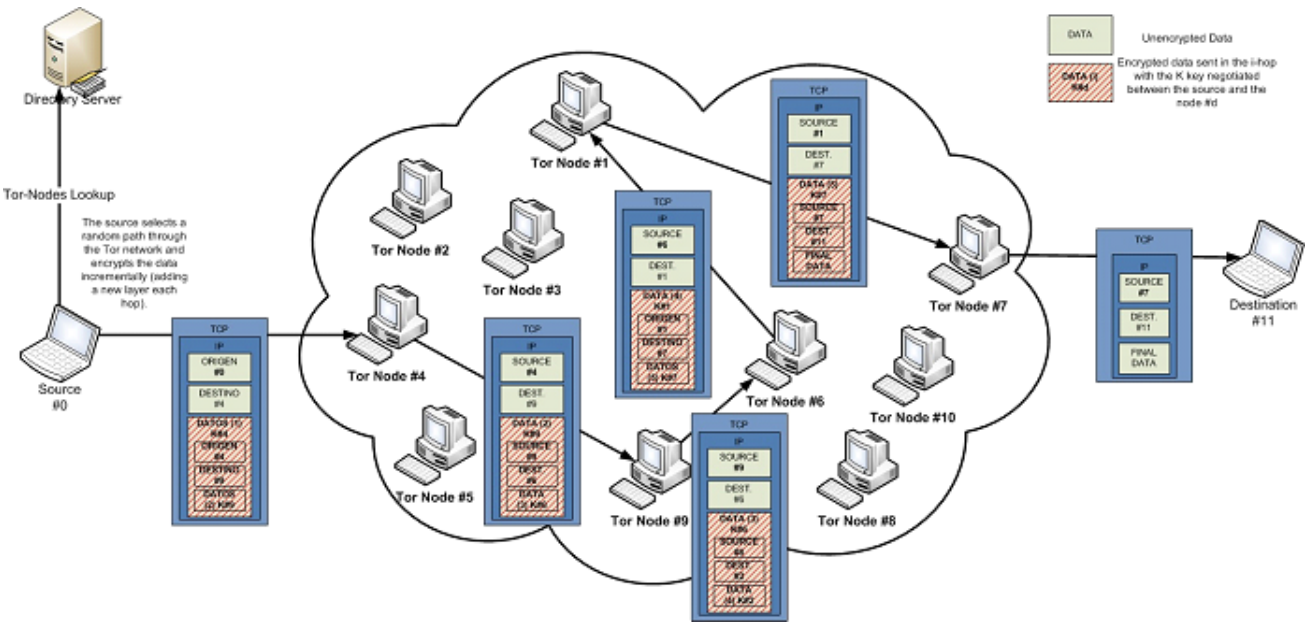

Figure 2: Tor Network. The source establishes an anonymous communication with the destination through a set of randomly chosen nodes, and incrementally encrypts the message by adding a layer each hop.

cept of *mix network* introduced by David Chaum in [13] is the building block for most anonymity systems. A mix network establishes every transmission through a set of routers (or proxy servers) by 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 approaches. For each hop each router agrees a symmetric key to progressively unwrap the message. Figure 2 shows a Tor network scenario and the construction of messages transmitted between Tor nodes. *Mixmaster*, *Buses*, *Mixonion*, *MorphMix*, *PIPENET*, *Babel* and *Tarzan* are well-known examples of this technology.

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

3.2 Attacks based on Recent Anonymity Sstrategies

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

- Tor-based attacks: Work in [14] 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 prevent access to Tor networks [15].
- Potential attacks based on *Anonymizer*: Several trojans, such as Bobax [16], provide attackers with Web services to use tools designed for HTTP anonymity such as *Anonymizer*. Thus the anonymity level is determined by the security policies defined on the proxy. In this way, the location of the attacker can be traced whenever any of the following situations occur: (1) the server records the client sessions, or (2) legal authorities require all traces.
- Attacks based on *Buses*: *Buses* shares functionalities with Tor networks in the way that messages are layered-encrypted. However, unlike Tor, routes are not created at random and messages are sent to the next hop in a list (this operation is similar to a circular bus-line where every packet is forwarded to the next hop). Work presented in [17] proposes a malware implementation using Buses. Experimentation presents several results: Buses shows a higher performance efficacy than networks based on random routing, the same anonymity levels, and a lower latency than mix networks.

4 Conclusions

In recent years, anonymity on the Internet has attracted considerable interest. On the one hand, honest users require anonymity in order to protect their privacy and, on the other hand, anonymity provides 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 Internet users. As these techniques proliferate and consolidate on the Web, new vulnerabilities are discovered indirectly, especially in social-based applications.

In [18][19] 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 it is true that we have not found in relevant literature many indicators that attackers are benefiting from the technologies described in Section 3, we still consider them as a potential tool for masking dishonest actions. For instance, the authors of [17] propose an implementation of malicious software based on anonymity networks.

In summary, in this paper we discuss the need for an integral solution that provides anonymity while preventing 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] A. Plonk, A. Carblanc et al. Working Party on Information Security and Privacy: Malicious software (malware). A security threat to the internet economy. CERT. Report No.: DSTI/ICCP/REG(2007)5/FINAL (2008). <http://www.olis.oecd.org/olis/2007doc.nsf/ENGREFCORPLOOK/NT00005F0E/$FILE/JT03244862.PDF>.

[2] R.B. Standler. Judgment in U.S. v. Robert Tappan Morris (2002). <http://www.rbs2.com/morris.htm>.

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

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

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

[6] S. Fluhrer, I. Mantin, A. Shamir. 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.

[7] M. Tanase. IP spoofing: an introduction. Security Focus (2003) <http://www.securityfocus.com/infocus/1674>.

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

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

[10] M.V. Mahoney, P.K. Chan. An analysis of the 1999 darpa/lincoln laboratory evaluation data for network anomaly detection. Proceedings of the 6th International

Symposium on Recent Advances in Intrusion Detection, Florida, USA, Springer-Verlag (2003), pp. 220-237.

[11] M. Zalewski. Silence on the wire: a field guide to passive reconnaissance and indirect attacks. William Pollock, 2005.

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

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

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

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

[16] J. Stewart. Bobax Trojan Analysis (2004) <http://www.secureworks.com/research/threats/bobax/>.

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

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

[19] Torproject. Abuse Faq (2009) <http://www.torproject.org/faq-abuse.html.en#What AboutCriminals>.