ZRÍNYI MIKLÓS NEMZETVÉDELMI EGYETEM

GYÁNYI SÁNDOR

Official and author’s review of PhD thesis titled

Methods of Denial of Service attacks and applicable ways of defense

Scientific advisor:

Prof. Dr. Kovács László

Budapest
2011

The scientific problem

During the operation of computers connected to the public communication networks, sometimes strange phenomena can be observed which may cause slow down or breakdown of the computer operations. In many cases, after examining of the malfunction, it turns out that it caused by intentional attacks, so called Denial of Service (DoS) attacks, based on system overload. In these cases the first step must be the recognition of the attack method, because the applicable way of defense based on that. In case of a DoS or a Distributed DoS (DDoS) attack defense methods are aimed at keeping the operation at a minimum level, until the hosts participating in the action are being deactivated or the originator of the incident stops its activities. Even keeping the minimum operation level can be difficult, because most of the information systems do not have sufficient redundancy, which endure the multiples of the normal operation strain.

In my research I analyzed the attack methods on information infrastructures and found that they have become more complex. Different kinds of malicious software, which could have been well distinguished earlier, are getting blurred. Thus, new threats came into existence, which are used by cyber criminals as well as different political organizations.

Besides activities aimed at tapping network traffic or taking over target devices new methods came to the front which undermine target operations. There is no universal defense method against these attacks. During modern DDoS actions there are so many hosts appear as attacker that the widely used packet filtering cannot be applied any more. In another generally used method the target tries to put more resource into the action than the capacity used by the attacker, and survive the action this way. However, I have my doubts about the possibility of such implementation and its economic aspects.

The best solution would be to identify the launcher of a DDoS attack and forced him to stop the action. It would be easy if attackers were using their own resources, but they try to avoid it – for obvious reasons. Developers of viruses and other harmful software provide solutions which make it hard to identify the perpetrator. Modern computer malwares have functions which allow the infected computer – or any other equipment, connecting to a computer network – to get commands from a central controller. These equipment are organized as networks and forming botnets which are capable of performing DDoS attacks. A botnet includes many host members; therefore it is not easy to deactivate it, especially when the attack is already in progress. I consider that it is very important to identify them before the start of an attack, when the investigator is not under time pressure.

Aims of research

My goal was to research of Denial of Service attack methods and applicable countermeasures against DoS-capable devices. To achieve this I set the following tasks:

1. To examine the different types of computer attacks, their threats and the potential damages, the connection of computer attacks and warfare, terrorism.

2. To determine the effects of DoS attacks, the security methods used against them, the feasibility of business continuity measures and their effectiveness correlated to the necessary resource usage. Identify and categorize the DoS and DDoS threats of the information infrastructures operating on the internet.

3. To examine the other functions of botnets from the aspects of traces that can lead to identification of infected hosts of malicious networks.

4. To find a method which suitable to identification the malicious bots without the violation of the other owners' privacy rights.

5. To define the basic functions of a system that could identify and deactivate the malicious hosts responsible for DDoS attacks, and to examine the possible organizational framework.

Applied research methods

I carried out extensive investigations in the Hungarian and also in the international scientific literature. Because of nature of the topic and the fast improvements of technology, my research was based mainly on the electronic, and to a lesser degree, the printed literature. With systematizing and processing the references I expanded my knowledge needed to achieve my research aims. In some cases, if it was possible, I made tests and experiments with computer networks in practice, and with the results I supported my statements.

I regularly participated – as a student as well as a lecturer – at professional conferences, and I systematically published the results of my researches in professional journals.

At my workplace I cooperated in many research and development projects, which helped my professional development.

Structure of the thesis

I split my thesis into four chapters:

The first chapter illustrates the methods of attacks on information infrastructures, their categories, particularly the vulnerabilities of critical infrastructure. I analyze the implications of the military aspects of these actions, domestic and international incident management processes. I show possible course of action and consequences with the help of an imaginary complex cyber attack on our country.

The second chapter analyses the damaging ability of cyber attacks, especially DoS attacks, and the potential protection methods against such actions. It categorizes the different kinds of attack techniques and the targeted system layers. I classify the most common techniques into the defined categories to facilitate relevant countermeasure selection.

In the third chapter I analyze the operation of botnets, their proliferation-related information. I review botnet evolution, actual and potential applications from computer criminals', terrorists' and military organizations' point of view.

In the fourth chapter I point out that service breakdowns inevitably occur during a DDoS attack, so prevention activities are very important. I describe the results of my own experiments, which allows easy identification of the infected members of botnets, using existing data only.

Conclusions

Computer networks have greater and greater effect on our lives, so defense of these networks – not only critical information infrastructure, but other areas, too – is more and more important. Public networks and connected hosts together form a virtual space – the so-called cyberspace – where dangerous activity takes place. The most common computer network –the internet – is used by terrorists, cyber criminals for information exchange, data theft and destruction of IT systems. Changes in military doctrines indicate that armies are getting more attention in cyberspace, so potential damage of a cyber attack is increasing significantly. A cyber incident can escalate and may evolve to an armed conflict between nations.

New computer malwares have appeared that risk not only IT systems but other critical infrastructures, too. As a new threat, large-scale networks have showed up, capable of coordinated actions. I examined previous cyber attack statistics and found that 22% of the known incidents applied a specific method called Denial of Service (DoS). Distributed versions of DoS (DDoS) and especially the reflective DDoS attack methods are extremely effective. Several large-scale events occurred where the target was under attack for a few weeks, thus service outage and financial loss was significant. After analyzing of these attacks I came to the conclusion that the first step of defense must be the realization of the fact that the target is under attack. For recognizing the action the knowledge of attack methods and their characteristics is very important, so I set up a simple and understandable framework, based on the most frequently used procedures. These procedures classified in three main classes:

- DoS attacks.
- DDoS attacks.
- Reflective DDoS attacks.

Reflective DDoS actions, especially the reflective DNS types, are the most powerful attack, thus fighting against them is more difficult.

For categorizing the classes of attacks I proposed the ISO OSI reference model layers depending on the layer of the target in which the attacker wants to overload the processes.

The analysis of countermeasures proves that maintaining the service continuity – preventing losses – under a DDoS attack is not possible using rational amount of resources. Since during an attack the resources of the attacker and the target fight each other, the target should be prepared in advance of an attack with unknown intensity. In contrast, the attacker must use resources slightly bigger than the target's resources. In addition, the attacker's botnet can be easily extended with new members, increasing the power of the action. IT systems are scaled for the normal operation load with rational redundancy. It is very uneconomic to allocate highly greater resources for the systems than necessary; however there is a chance that greater resources wouldn't be enough for extremely high loads.

Another popular method is traffic filtering, after the identification of malicious data stream the victim tries to keep the attacker hosts from reaching the target. After studying the DDoS and reflective DDoS techniques I found that traffic filtering is not feasible against certain attacking methods, because filtering may block the proper operation of IT systems as well.

This proves that passive defense mechanisms – increasing resource and filtering traffic – need irrational amount of resources; therefore it is more effective to find and shut down attacker hosts.

The widely used reactive protection methods – seeking to terminate the attack – based on cooperation of service providers. Although this method is effective but in this case the time factor is a problem. If the attack includes a large number of malicious hosts, long time is needed to identify of involved service providers and shut the hosts down with their help. Delay of terminating the attack is increasing the losses. Therefore I focused on research of the methods which allows seeking and neutralizing the malicious bots before DDoS attacks begin.

Illustrating the risks of DDoS attacks I prepared a scenario of a hypothetical complex cyber attack carried out only in cyberspace. I identified the actions against critical information infrastructures, namely the energy service and telecommunications as the main elements. I evaluated IT security weaknesses of mobile communication devices, primarily mobile phones as dangerous tendency.

With the analysis of DDoS cases I found that networks made of infected computers under central control – called botnets – are responsible for that kind of attacks. After examining the distinct botnet architectures partitioned by the method of command and control channel, I found that there are procedures for host discovery. However, these methods are often monitoring the user's network traffic and therefore may violate privacy rights. Besides, they require installation of special devices in the computer network. I assumed that botnets were capable of other tasks beside the DDoS attacks, so I examined these tasks, too. I proved that these tasks leave traces which allow the identification of the network addresses of malicious hosts, this way it can be possible to track and neutralize botnets. I concluded that beside data and identification theft, unsolicited mail – SPAM – sending is the most popular task of a botnet. This is relatively safe revenue for botnet owners, which results massive SPAM-flood. In my opinion this activity is one of the easiest ways of finding a botnet host.

After reviewing TCP protocol used by electronic mail transfer I determined that network address spoofing techniques were not effective, therefore log entries made by electronic mail servers contain the valid address of the mail-sender clients. Most of internet service providers have SPAM filter in their mail system, thus addresses of senders are available on a daily basis, and no extra equipment is needed.

Botnets are the overwhelming majority of SPAM senders, so the network address of an unsolicited electronic mail sender is an address of an infected member of a botnet. I have created an experimental model which is capable of tracking down botnet members by examining the mail server's activity log. To demonstrate the viability of the model's functions I implemented a computer program and analyzed approximately one and a half million SPAM records. Comparing these results and a GeoIP database I demonstrated that botnet members can be located even geographically if accurate and up to date databases are available. In my opinion the database containing the internet service providers' data would be more efficient.

Based on the experience of my model I proposed a possibility of a proactive system. I have concluded that the most appropriate solution is a government-coordinated system with cooperation of domestic internet service providers. The ISPs collect the botnet members' addresses and after preprocessing functions – such as filtering out the duplicates – they send to the coordinating organization. This organization makes data processing and separate domestic ISP addresses from foreign addresses. After this step, there is possible to send lists of own infected host addresses to the domestic or to foreign ISPs directly. This process id is highly automated and based on data already available. The infected hosts' list contains only anonym network addresses thus I do not see any privacy concerns.

New scientific achievements of the thesis

1. By analyzing attack and defense methods used in practice I proved that continuity of service under a DDoS attack can be ensured only by using too much resource. That is why these kinds of defense methods alone are not efficient.

2. I worked out a categorization of DDoS attack methods which can make more effective defensive actions against those attacks.

3. After analyzing the operation of botnets causing Denial of Service attacks, I created a botnet member detection method with the help of passive data collection technique.

4. I created an experimental model for analyzing the operation of botnet clients (traces of spam sending) and localizing them. With this experimental model I proved how the

(spam sending) hosts used for DDoS attacks can be traced and neutralized proactively, without violating human or data protection rights.

5. I worked out the basics of a realizable system which can identify botnet clients by the above mentioned methods, and neutralizes them with the help of Internet Service Providers.

Practical usability of thesis

In my thesis I examined the most recent cyber threats, especially the different kinds of Denial of Service attacks and the responsible botnets. I propose to use my whole dissertation in higher education, in computer network subjects.

The classified DoS attack descriptions can help to reduce the response time to select the relevant countermeasures; therefore they can be used as supplementary material in trainings.

In the implementation of the proposed proactive system my thesis can be used as a reference document.

Publications

Reviewed publications in Hungarian

[1] DDoS támadások és az ellenük való védekezés
(Hadmérnök, February of 2008)
http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles7/gyanyi_rw7.html
ISSN 1788-1919

[2] Cyber-támadások elleni védekezés és a válaszcsapások lehetőségei
(Hadmérnök Volume III., Issue 2., June of 2008. 114-128p)
ISSN 1788-1919

[3] Botnetek felkutatása a térinformatika segítségével
(Hadmérnök Volume IV., Issue 3., September, 248-257p)
ISSN 1788-1919

[4] Elektronikus hadviselés a civil világban 1.
(Biztonság, 2008/5 36-38p)
ISSN 0864-9189

[5] Elektronikus hadviselés a civil világban 2.
(Biztonság, 2008/6 36-40p)
ISSN 0864-9189

[6] Informatikai WLAN-hálózatok zavarása
(Bolyai Szemle, April of 2009., 119-132p)

Publication in English

[7] Next Generation Viruses
28th International Conference June 3-4, 2010.
Sience in Practice kiadvány, Subotica, Serbia

Curriculum Vitae

First name:	Sándor
Last name:	Gyányi
Date of Birth:	9 January, 1969.
Education:	Zrínyi Miklós National Defence University, PhD student (2007 -) MsC in Information Engineering, University of Miskolc (2007) Electrical engineer degree, Kandó Kálmán Faculty of Electrical Engineering (1990) Radio and Television technician, Pataky István Vocational School (1987)
Work experience:	University of Óbuda, tutor (2010 -) Budapest Tech Polytechnical Institution, tutor, (2003 - 2009) Aspect Kft, manager (2001. július 1.–2002. szeptember 30.) Mixim Kft, manager (1991. október 1.–2001. június 30.) Matrix Kft, senior auditor (2002–2005) Veritan Kft, senior auditor (2006–)
Language skills:	English, general intermediate (B2) combined (C) Certificate No.: CA060-26933 876393. Russian, general basic (B1) combined Certificate No.: EJ010-76511 1179648
Professional activities:	1. Teaching (Information Technology; Communication networks; Telecommunication; Digital systems; Operations and Security of IT Systems) 3. Research and development, consulting: Developing of a PSTN testing equipment; GTS billing accuracy and security audit (Veritan Kft); Pantel-Technocom SLA accounting system development; Pantel-Technocom Call Data Record collecting system development;

Fővárosi Gázművek electronic metering system development;
Matáv RT billing accuracy and security audit (Matrix Kft);
Pannon GSM billing accuracy and security audit (Matrix Kft);
T-Mobile billing accuracy and security audit (Matrix Kft);
Emitel billing accuracy and security audit (Matrix Kft);
E-szignó digital signature application security audit (Matrix Kft);

Specialities:

Security of Computer Networks
DDoS attacks
Botnet detection
Digital Signal Processing