Cybersecurity: Expanding the Front Lines of Defense

George K. Kostopoulos

New York Institute of Technology
Nanjing University of Posts and Telecommunications
University of Maryland University College
george@kostopoulos.us

Abstract

This paper presents a cybersecurity strategy, implemented by a multi Internet-node SCADA[1], which serves as a defense shield – countermeasure – against *denial-of-service* attacks. The strategy employs the Internet nodes surrounding a server of interest, and uses them as *avant-gard*, monitoring the server's impending traffic, and reporting on the traffic's volume and origin, with possible authorization to selectively or totally block that traffic. In this concept, the Internet nodes are equipped with appropriate software that hold and update a traffic database accessible by the server of interest. Through this node database the server becomes aware of the upcoming traffic, and the node is appropriately instructed by the server. It is believed that such SCADA and node-server communications can create a shield that will effectively protect servers from *denial-of-service* attacks.

Keywords: cybersecurity, network security, artificial intelligence, denial of service, SCADA.

Introduction

As the cyberspace is becoming an integral part of practically every aspect of modern life, so are the threats against its safe and reliable operation are on the increase. Thanks to cryptography, communications content is relatively secure, while the prompt delivery of communications can be impeded by denial-of-service, DoS, attacks. "*Nevertheless, there are security threats* (such as DoS) *which cannot be prevented using cryptographic methods.*" **(Granzer, 2008)**.

Cyber anti-malware have been successfully protecting against *viruses*, however, DoS, attacks appear to remain out of control. Such attacks come in large bursts of thousands of requests saturating typical servers. Most DoS attacks **(Schmidt, 2009)**:

- Saturate server, network or terminal devices through repeated requests that incapacitate the server's resources.
- Inject false messages, such as connect, disconnect or error messages, thus disorienting the server operations.

[1] **SCADA: S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition. Usually, it is a computer based system that oversees a certain well defined operations, and possibly controls them by providing adjusting feedback.

That is, DoS attacks aim at incapacitating or saturating one or more of the target's resources. "*DoS attacks attempt to exhaust the victim's resources. These resources can be network bandwidth, computing power, or operating system data structures."* **(Patrikakis, 2006)**. The Internet has not been designed with the cyber criminals in mind, and is totally vulnerable to sophisticated attacks to the point where *"...even a single attacker is easily able to achieve a complete DoS.*" **(Zhou et al, 2009).**

DoS attacks have become the prime concern of all chief information/and chief information security officers. *"Cyber criminals routinely use the threat of DDOS* (Distributed Denial of Service) *attacks in extortion against on-line businesses."* **(Hunker, 2010)** Also concerned are custodians of Domain Name System, DNS, servers. Saturation of such servers will result in the inaccessibility of thousands of websites. Maintaining an in-PC domain name to IP address converter is always a good policy, although it does not eliminate the vulnerability of a possible DDoS attack. DDoS attacks have been on the increase in frequency and in strength, having reached the level of close to 50Gbps in a single attack. Statistics are as shown in Fig.1. **(Arbor, 2009).** There is a general pessimism over effective DDoS countermeasures with researches believing that *"This is an ongoing problem to which there is no permanent solution in sight."* **(Murphy, 2009).**

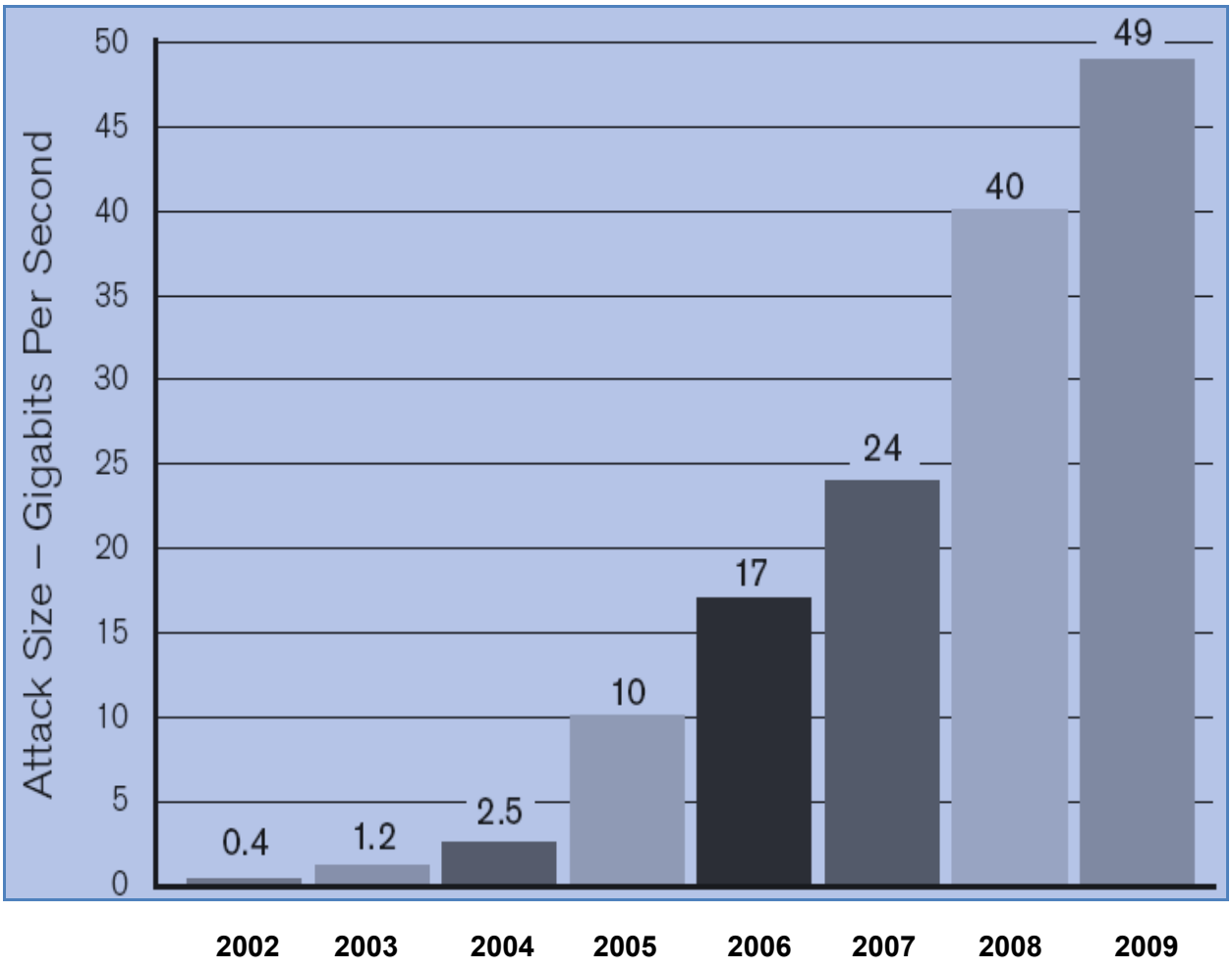

Figure 1: Peek DDoS Attacks in Gbps 2002-2009. Source: Arbor Networks, Inc. **(Arbor,2009)**

The basic topology of a Distributed Denial of Service Attack is illustrated in Figure 2. This is the classic approach where, over a period of time, a cybercriminal infects computers with zombie virus making the ready for a DoS attack at the moment that is chosen by the attacker.

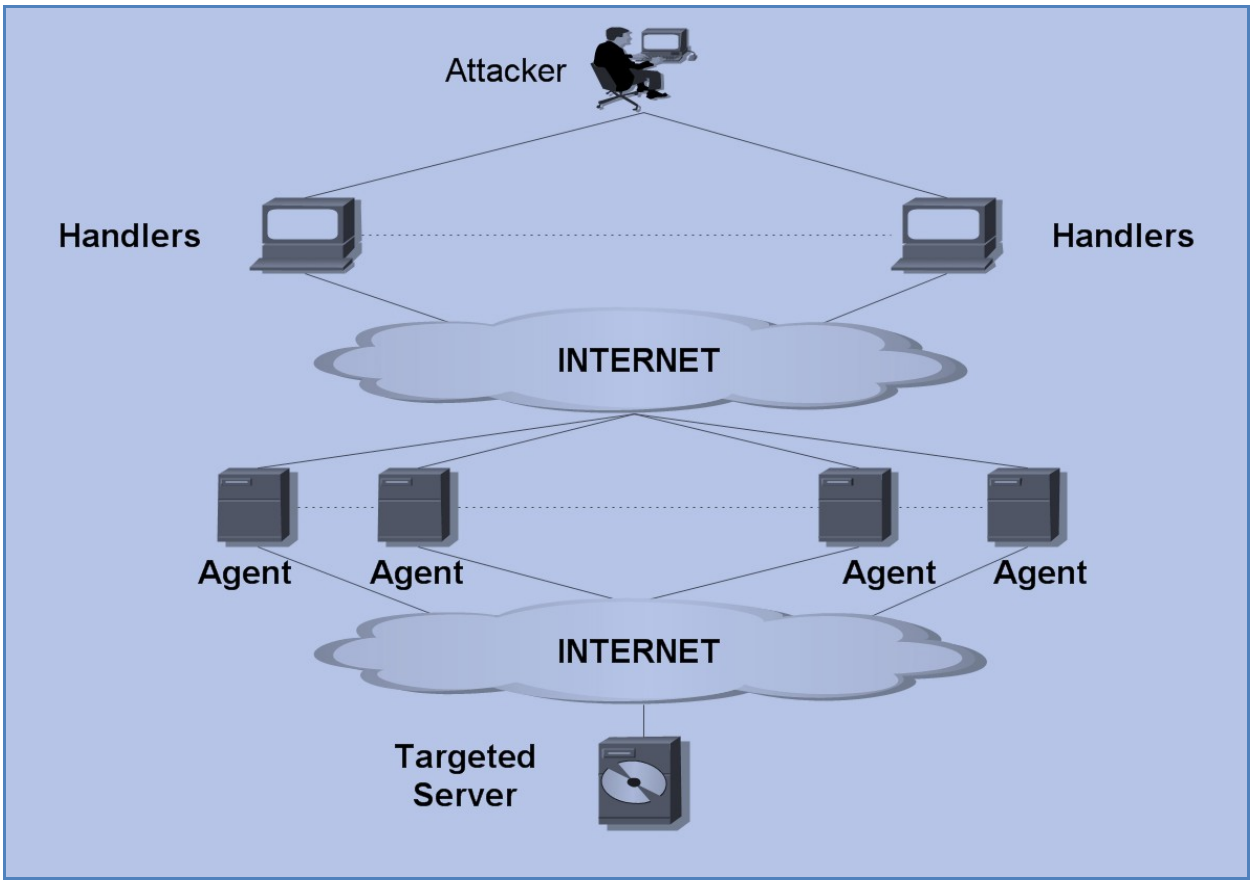

Figure 2 Basic Topology of a Distributed Denial of Service Attack.

Countermeasures

DoS countermeasures start with the detection of a potential attack, proceed with an assessment of the attack's potential, and end with the necessary actions that need to be taken. Such actions include delay or rejection of suspected packets, and forward and backward notifications of the Internet nodes about the suspected DoS attack. "*Although no "silver bullet" solution to the problem of denial of service attacks currently exists, various countermeasures can make attacks far more difficult to successfully devise and execute*." **(Karig, 2001).** The increased networks speed coupled with the equally increased size of computer memory and storage, now allows for the incorporation of advanced algorithms in the network nodes where traffic can be monitored, assessed and controlled.

The deployment of such algorithms in Internet nodes can collectively create a *traffic forecasting* system where destination servers will be informed of the impending traffic its volume and equally important its origin.

Presently, there is neither such system in place, nor is there any *"...comprehensive method to protect against all known forms of DDoS attacks.*" **(Specht et al, 2008)**. Significant research activity has been in progress that points to the need for an Internet SCADA. **(Daniel et al, 2001) (Krugel, 2002) (Wood et al, 2002).**

Any Internet SCADA system has to be of a well-defined scope, of measurable effectiveness, of controllable complexity and of practical scalability, focusing on an early-warning type of DoS detection. In DoS countermeasures *"...header analysis is the foremost method used in (the) detection..."* of potential DoS attacks **(Xiong, 2004).** This analysis aims at identifying an origin-to-destination relationship using a variety of packet traceback techniques. **(Chao, 2005) (Rohit, 2005).** However, the real vulnerability remains with the high volume brute force DoS attacks.

The Proposed Concept

The suggestion in this paper is that special artificial intelligence software be embedded in the Internet nodes, so that collectively, and in cooperation with corresponding software in the server-of-interest, will serve as an Internet SCADA able to detect and prevent potential DoS attacks. Figure 3 illustrates a server-of-interest surrounded by Internet nodes. There is a two-way priority communication between the Node Artificial Intelligence Monitoring Software, NAIMS, and the destination server's Server Global Traffic Analysis Software, SGTAS.

The Implementation

The above concept is implemented by two software components. One is the server global traffic analysis software, SGTAS, hosted in the server-of-interest. The other is the node artificial intelligence monitoring software, NAIMS, which is installed in designated Internet nodes that are expected to handle traffic for the server-of-interest. Together, they form a SCADA that oversees the traffic of interest and regulates the flow averting possibilities of server saturation.

Presently, the Internet is merely a global grid of interconnected routers that facilitate the end-to-end communication between Internet clients and Internet servers, without any cybersecurity potential. While administering this traffic, the Internet nodes access data that may result into most valuable information. Based on statistical assessments, and other packet observations, the above proposed SCADA will be able to monitor related traffic and dynamically establish criteria able to possibly recognize suspected DoS attack.

In the NAIMS, a respective traffic profile is maintained and continuously updated. The profile is parametrically defined basically by the volume of packets per unit time, using a sliding time window of the immediately past activity. Based on that rate, and on other parameters set up by the SGTS, an assessment is made on the integrity of each of the received packets. The NAIMS will be looking for unusual packets bursts and will be notifying the server's corresponding SGTS accordingly.

The central software in the server will be continuously receiving traffic reports from the satellite software and will be developing projections and assessments as to the impending traffic toward that server. Besides creating statistics, the central software will be directing the nodes as to how to treat the requests before they reach the server. The NAIMS to SGTS communications will be bypassing any node queue thus maximizing speed of decision making.

Worth noting is that the geographical spread of the Internet nodes may be often overlapping areas of neighboring countries, where "*Collective cyber defense – passive or active – is altogether consistent* . . . (with other forms of collective defense)…." **(Smith, 2010).**

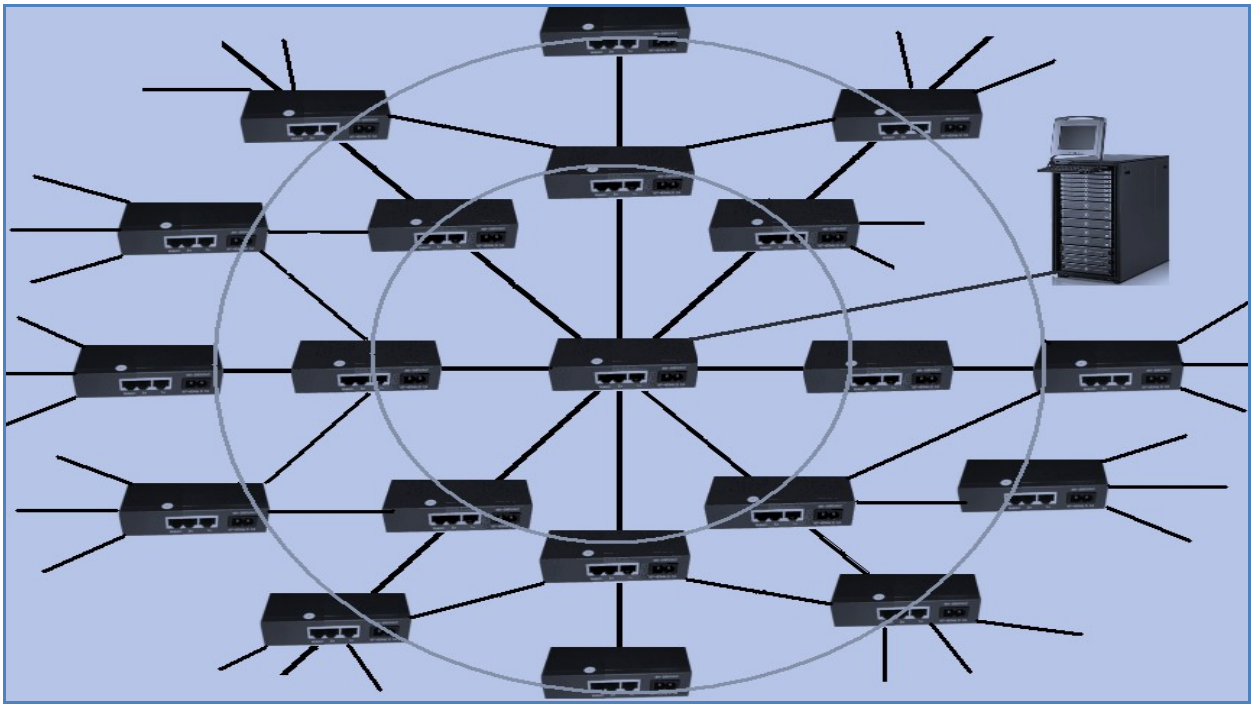

Figure 3. Server-of-interest surrounded by Internet nodes. There is a two-way priority communication between the Node Artificial Intelligence Monitoring Software, NAIMS, and the destination server's Server Global Traffic Analysis Software, SGTAS.

Conclusion

All technology supported services have started minimal in size and functionality and progressively have grown into powerful and useful social resources. Similarly, the Internet started as a text messaging platform and has grown into being an integral part of everyone's life. Today, the functionality level of the Internet nodes can be compared to that of the mobile phones of the Nineties – minimal and non-intelligent. For the Internet nodes, the next step is to go beyond the packet-passing stage and to collectively become an infrastructure that supports server security and load projections, at least as a start. As a system, the Internet nodes is an underutilized resource. Once intelligence is entered into them, the functionalities will become unlimited, as has been with practically all other technologies.

References

Arbor (2009) Worldwide Infrastructure Security Report V, Arbor Networks,Inc, http://www.arbornetworks.com/dmdocuments/ISR2009_EN.pdf (2009)

Chao, Gong, (2005)"Single Packet IP Traceback in AS-level Deployment Scenario" http://www.utdallas.edu/~ksarac/research/publications/GLOBECOMM05.pdf

Daniels, Thomas E. and Spafford,(2001) "Network Traffic Tracking Systems:Folly in the Large?" , Proceedings of the 2000 Workshop on New Security Paradigms, Feb. 2001

Granzer, Wolfgang, (2008) "Denial-of-Service in Automation Systems" (p.468) https://www.auto.tuwien.ac.at/~wgranzer/etfa2008_dos.pdf

Hunker, Jeffrey, (2010) Cyber war and cyber power –Issues for NATO doctrine, NATO Defense College, Research Paper No.62 November 2010 p.7 http://www..ndc.nato.int/download/downloads.php?icode=230

Karig, D and Lee,R.,(2001) "Remote Denial of Service Attacks and Countermeasures". Princeton University Department of Electrical Engineering Technical Report CE-L2001-002, October 2001. p.15 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.6.4098&rep=rep1&type=pdf

Krugel, C.(2002) Network Alertness: "Towards an Adaptive, Collaborative Intrusion Detection System'. PhD dissertation, Vienna University of Technology, 2002.

Murphy, A. et al,(2009) "Denial of Service and Countermeasures" Networks and Telecommunications Research Group, NTRG, Department of Computer Science, Trinity College Dublin, Ireland (2009) http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group2/

Patrikakis et al,(2009) "Distributed Denial of Service Attacks", CISCO The Internet Protocol Journal - Volume 7, Number 4 http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

Rohit Jain, (2005) IP Traceback to Prevent Denial of Service Attack http://www.rohitj.net/research/files/ip_traceback.pdf

Schmidt, Andreas C., (2009)"Securing VoIP Networks using graded Protection Levels" (p.3). http://subs.emis.de/LNI/Proceedings/Proceedings17/GI-Proceedings.17-7.pdf (2009)

Smith, David J., (2010) Georgia 2008: Why We Need National and NATO Cyber Defense Policies, Georgian Cyber Security and ICT Innovation Conference 2010, Tbilisi, Georgia November 10,2010. http://www.amcham.ge/photos/giti-2010-10-10/11.pdf p.5

Specht, Stephem M. and Lee, Ruby B. (2008), "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures", (p. 5). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.133.4566&rep=rep1&type=pdf

Wood, A. D. and Stankovic, J. A.(2002), DoS in Sensor Networks. IEEEComputer, 35(10):54-62, 2002

Xiong, Jin. (2004) "Analysis of Four Distributed Denial of Service Counter-measures" http://www.rh.edu/~rhb/cs_seminar_2004/SessionA2/xiong.pdf (p.1)

Zhou, Xing et al,(2009) "Evaluation of Attack Countermeasures to Improve the DoS Robustness of RSerPool Systems by Simulations and Measurements" (p.11). http://tdrwww.exp-math.uni-essen.de/dreibholz/rserpool/rserpool-publications/KiVS2009.pdf