"HENRI COANDA"
AIR FORCE ACADEMY
ROMANIA

GERMANY

"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY
SLOVAK REPUBLIC

INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER
AFASES 2011
Brasov, 26-28 May 2011

TEST BED FOR CYBER-ATTACKS MITIGATION

Július BARÁTH*, Marcel HARAKAĽ*

*Department of informatics, Armed Forces Academy of General Milan Rastislav Štefánik, Liptovský Mikuláš, Slovakia

Abstract: The paper use Georgian case as a real example of cyber-attack, shows methods used to paralyse *country institutions and the effects achieved. The case initiated the need to create test environment for simulation and understanding of this phenomena, serving as test bed for research, experimentation and exercising. Possible use and further extensions of test bed are mentioned*

.

Keywords: *cyber-attacks, network infrastructure, test bed.*
MSC2010*: 68M11, 68M15.*

1. INTRODUCTION

Massive penetration of computers in business, industry, government, schools and homes with broadband connection, availability of knowledge and tools creates a framework for better utilization of resources both for legal and illegal (crime) use. OECD average fixed (wired) broadband subscriptions per 100 inhabitants, from June 2010, is 24,20% (1) and is expected to rise. Business, industry, government, schools and individuals relay on computers, services and connectivity, so attacks against reliability and availability of them can lead to serious problems. Recent cyber-attacks have shown that the threat is real and all representative national bodies together with industry should take practical steps to prepare response solutions, prevent losses and mitigate threats. Because cyber defence is a broad area starting from policy and ending with elementary bits of information, broader view about the topic can be found in (2), (3).

The first part of the paper will use Georgian case as real example of cyber-attack; will show methods used to paralyse country institutions and effects achieved. The case initiated the need to create test environment for simulation and understanding of this phenomena, serving as test bed for research and experimentation. Simulation and experimentation in cyber security is an emerging area and some ongoing activities can be found in (4) (5) (6).

The last part of the paper describes the proposal of cyber defence test bed architecture and its possible use.

2. FACTS – GERORGIAN CASE

The facts of the Georgian cyber-attacks have been collected from the Estonian Computer Emergency Response Team (CERT-EE) and distinguished IT security websites, verified with the Georgian Embassy in Estonia, and compared with international media. The majority of the materials referred to in the facts section and all materials referred to in the analysis part are open-source and summarized in (7).

On August 7, 2008, following separatist provocations, Georgian forces launched a surprise attack against the separatist forces. On August 8, Russia responded to Georgia's act by military operations into Georgian territory, which the Georgian authorities viewed as Russia's military aggression against Georgia. By late August, before the Russian invasion into Georgia commenced, cyber-attacks were already being launched against a large number of Georgian governmental websites, making it among the first cases in which an international political and military conflict was accompanied – or even preceded – by a coordinated cyber offensive (7).

US-CCU analysis of Georgian cyber campaign (8) concluded that:

- attacks were carried out by civilians with little or no direct involvement on the part of the Russian government or military,
- the organizers of the cyber-attacks had advance notice of Russian military intentions and timing,
- social networks operating over the internet were the main tool used to recruit those carrying out the attacks,
- the civilian cyber attackers were aided and supported in their efforts by Russian organized crime,
- the total number of individual civilian cyber attackers involved in the campaign against Georgia was much greater than in the campaign against Estonia, although the total number of computers involved was much smaller.

3. METHODS USED

Georgia cyber-attacks were relatively simple by nature and benefited from massive human cyber-attackers participation. Attacks were targeted on poorly maintained and inadequately secured servers, services and communication infrastructure with less bandwidth.

1. First wave of attacks was carried out by botnets and command and control systems that were ready before Russian invasion.
2. Later the chief method used to maintain and expand the cyber campaign was a series of postings on websites using cyber-attack tools and the lists of suggested targets for attack.
3. The types of cyber-attacks used against Georgia were limited to denials of service and website defacements, but these relatively unsophisticated types of attacks were carried out in a very sophisticated manner.
4. At least one of the website defacements was prepared specifically for use against Georgia more than two years before the attacks.
5. Cyber attackers refrained from carrying out the sorts of attacks that would have done lasting physical damage to the Georgian critical infrastructure, even though some of those involved in planning the cyber campaign may have had some idea of how to carry out such attacks (8).

Georgia itself had no procedures and cyber-defence teams at place to face the challenge. One of the very first steps made by the officials was to contact Estonian government and get in touch with network of cyber-security experts, followed by installing access-lists on boundary routers, but only effective response to attacks was to move important web sites to foreign countries with appropriate internet bandwidth connection. It is important to note, that those countries also had great difficulty in running Georgian sites due to volume of attacks.

Results of military invasion supported by cyber-attacks were devastating. Cyber-attacks made governmental, financial, business and news media websites unreliable, unavailable or misused for propaganda. In such situation, government was not able to inform Georgian population properly about what to do and how to defend against invasion. All sites able to inform about the current situation, including foreign media were under attack during the whole invasion. International audience was informed with delay, and because the actual size and scope of invasion was unclear, international support was delayed too. Due to success of cyber-attacks, physical destruction of news media and communication facilities was not necessary. Money transfers between domestic banks and abroad was impossible; disruptions and uncertainty made a business transactions and orders difficult.

4. SIMULATION TEST BED PROPOSAL

The idea for creation of test bed for cyber-attacks mitigation is not new at Department of Informatics and should be taken as an extension of currently used network security lab and existing network security course. Up to now, we have used network security lab to evaluate and teach how to secure network devices (switches, routers, wireless access points), configure firewalls (router based and adaptive security appliances), create virtual private networks, and reliably authenticate users and devices in small-scale scenarios - Figure 1.

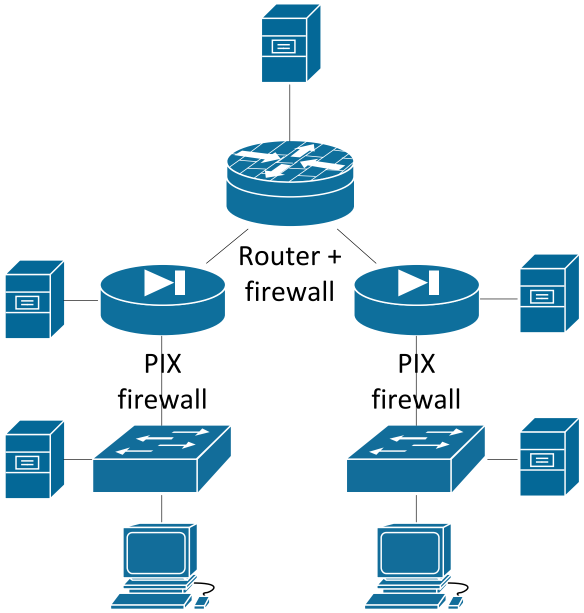

Figure 1. Network security lab topology.

Not enough attention was paid to secure application servers, user hosts and other network devices (network printers, physical access control devices, cameras etc.), to enforce defined security policy globally and collect, analyse and archive security logs globally.
The goal of proposed test bed is to provide a scientific platform to evaluate the impact of new technologies to cyber defence and move us from a reactive to a proactive stage.

The goals should be characterised as follows:

- support scalable experimentation with heterogeneous technical infrastructure isolated from public internet,
- guarantee containment, confidentiality and integrity of test bed environment,
- provide collaborative and exploratory environment for discoveries and innovation,
- create the library of attack tools, Denial of Service, security scanners with source code and more (for example (9)),
- create the library of methods used to discover and mitigate threats,
- provide the place to conduct cyber response exercises.

To illustrate possible topology for experimentation see - Figure 2. The topology consists of ACE - Cisco ACE Application Control Engine application switch for increasing the availability, performance, and security of data centre applications, ACS - Cisco Secure Access Control System - complement of existing infrastructure to enhance visibility and control across the domain. It offers central management of access policies for device administration and for wireless and wired 802.1X network access scenarios. Cisco Security Monitoring, Analysis and Response System (MARS) is used for identifying threats on the network by "learning" the topology, configuration, and behavior of your environment and making precise recommendations for threat mitigation, including the ability to visualize the attack path and identify the source of the threat. The Cisco IronPort S-Series Web Security Appliance employs advanced tools including acceptable-use-policy controls, reputation filtering, malware filtering, data security, and application visibility and control to protect web servers. Traffic analysis is realised using both hardware (Fluke EtherScope) and software analysers. Attacker site consists of software traffic generators, sniffers and attack tools (MPack, Neosploit, ZeuS, Nukesploit P4ck, Phoenix etc.).

In the first scenario there is an attacker site represented by the cluster of traffic generators and reconnaissance tools guided by human attacking victim web site trying DDoS attack over one or more internet connections. Victim site can be configured to be purely secured with the lack of protection or secured and well maintained. Using analyses tools, protocol inspectors and other tools will enable to:

- measure how much traffic is needed to defeat different server operating systems and web server applications,
- measure server response times to legitimate requests made from non-attacker sites,
- collect signatures of attacks,
- evaluate counter actions made by site administrator,
- evaluate counter actions made by ISP provider,
- collect and analyse logs from network devices, servers and applications and more.

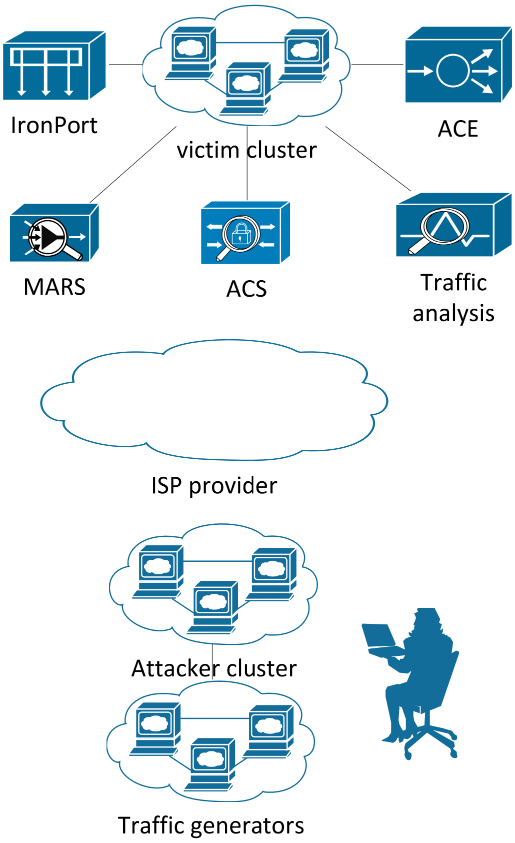

Figure 2. WEB attack scenario using test bed.

The second scenario can address attempts to modify content of the web pages. Here victim has to detect that attempt was made to modify content, identify attacker site, take necessary steps to restore original content and secure web server. Although scenario may be seen as trivial, without proper backup plan, policies for monitoring and skilled administrators it will be difficult and stressful to succeed.

The third scenario can simulate worm attack targeted to network infrastructure. Again there is need to detect and react timely and properly.

5. CONCLUSION

Cyber-defence is an important area of national and international interest and to coop with challenges successfully an active participation of government, commercial sector, research and academia is needed. National and international organizations play an active role in creating laws addressing cyber-crime and forming computer emergency response teams.

Department of Informatics participate in activities related to network security and extends scope of interest to cyber-defence. Test bed for cyber-attacks mitigation is our contribution toward better understanding of current state-of-art in the area and attempt to provide a platform for evaluating and exercises. Although the test bed is an important part of the approach to safer cyber-space it is also necessary to keep our eyes and ears open, and possibly be informed about activities discussed in hacker forums, social networks, etc.

We feel that modelling and simulation is another important approach towards understanding of cyber-attacks in larger scale scenarios. The interconnection between simulators and real devices can bring more realistic view of the situation as well.

Finally yet importantly, deeper understanding of cyber-security issues and lessons learned from cyber-defence exercises will be beneficial for both active serving military professionals and cadets, prepared for serving in armed forces and oriented to national and international security.

BIBLIOGRAPHY

1. OECD Broadband Portal. *Directorate for Science, Technology and Industry.* [Online] [Dátum: 24. February 2011.] http://www.oecd.org/sti/ict/broadband.

2. **Knapp, Kenneth J, [ed.].** *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions (Advances in Information Security and Privacy).* Hershey : Information Science Reference, 2009. 978-1605663265.

3. **Clarke, Richard A. and Knake, Robert.** *Cyber War: The Next Threat to National Security and What to Do About It.* New York : Ecco, 2010. 978-0061962233.

4. *The DETER project: Advancing the science of cyber security experimentation and test.* **Mirkovic, J, et al., et al.** Waltham, MA : s.n., 2010. Technologies for Homeland Security. pp. 1-7. 978-1-4244-6047-2.

5. GENI. *The Global Environment for Network Innovations.* [Online] 2011. [Cited: February 24, 2011.] http://www.geni.net/.

6. Information and Infrastructure Integrity Initiative. *Pacific Northwest National Laboratory.* [Online] 2011. [Cited: February 24, 2011.] http://i4.pnl.gov/.

7. **Tikk, Eneken, et al., et al.** *Cyber Attacks Against Georgia: Legal Lessons Identified.* Tallin : CCDCOE, 2008.

8. **Bungarner John.** Overview by the US-CCU of the Cyber Campaign Against Georgia in august of 2008. *US Cyber Consequences Unit.* [Online] August 2009. [Dátum: 24. February 2011.] http://www.usccu.us/.

9. Attack tool kit. *Computer technik security.* [Online] 2011. [Cited: February 24, 2011.] http://www.computec.ch/projekte/atk/.