Mapping the Most Significant Computer Hacking Events to a Temporal Computer Attack Model

Renier Heerden, Heloise Pieterse, Barry Irwin

Mapping the Most Significant Computer Hacking Events to a Temporal Computer Attack Model

Renier van Heerden[1,2], Heloise Pieterse[1] and Barry Irwin[2]

[1]Council for Scientific and Industrial Research, Pretoria, South Africa
rvheerden@csir.co.za, hpieterse@csir.co.za
[2]Rhodes University, Grahamstown, South Africa
b.irwin@ru.ac.za

Abstract. This paper presents eight of the most significant computer hacking events (also known as computer attacks). These events were selected because of their unique impact, methodology, or other properties. A temporal computer attack model is presented that can be used to model computer based attacks. This model consists of the following stages: Target Identification, Reconnaissance, Attack, and Post-Attack Reconnaissance stages. The Attack stage is separated into: Ramp-up, Damage and Residue. This paper demonstrates how our eight significant hacking events are mapped to the temporal computer attack model. The temporal computer attack model becomes a valuable asset in the protection of critical infrastructure by being able to detect similar attacks earlier.

Keywords: computer attack model, ontology, network attack prediction

1 Introduction

Computer hacking (also referred as computer cracking) developed in conjunction with the normal usage of computer systems. This paper discusses some of the most significant hacking events and the features that made them unique. The events listed are considered to be significant because of their unique impact, methodology or other properties. The level of significance is an abstract and relative measure. Other attempts to judge the importance of hacking events have been made by Heater [1], Hall [2] and Julian [3].

Research in computer network attack prediction at the Counsel for Scientific and Industrial Research (CSIR) in South Africa has resulted in the development of a Taxonomy and Ontology of computer network attacks. A temporal attack model was developed with the goal of separating the different stages of a computer network attack. The model consists of the following basic stages: Target Identification; Reconnaissance; Attack; and Post Attack. The Attack stage has the following sub-stages: Ramp-up; Damage; and Residue. Research was also organized into strategies for identifying the Reconnaissance and Ramp-up stages. The attack model is a valuable asset in the protection of critical infrastructure as it has the ability to identify attacks at an earlier stage and so improve the responsiveness to incidents.

adfa, p. 1, 2011.

This paper presents the authors' view on the most important hacking events, and cannot in itself be considered absolute. We chose events based on either the uniqueness of the technique used or their unique impact. The attack model is presented in more detail in Section 2. Section 3 describes the most significant hacking events and their characteristics. Section 4 identifies trends in hacking development. Section 5 maps the hacking events to our temporal attack model. Section 6 focuses on the protection of critical infrastructure. Section 7 discusses mayor future hacking events.

2 Attack Model

2.1 Computer Attack Taxonomy and Ontology

A detailed taxonomy that describes computer based attacks has the following classes [4]: actor; actor location; aggressor; attack goal; attack mechanism; automation level; effects; motivation; phase; scope; target; and vulnerability. The taxonomy was then used to describe the following scenarios [4]: denial of service (DoS); industrial espionage; web deface; spear phishing; password harvesting; snooping for secrets; financial theft; amassing computer resources; industrial sabotage; and cyber warfare.

2.2 Temporal Attack Model

The Phase class in Section 2.1 was used to build the Temporal Attack Model. The Target Identification stage represents actions undertaken by an attacker in choosing his/her target. Identification of these actions falls outside the scope of the network attack prediction project, but forms part of the overall attack model. The Reconnaissance stage represents actions undertaken by an attacker to identify potential weak spots. These actions are the earliest indicators of an impending network attack, and occur before any real damage has occurred. Popular reconnaissance actions include network mapping and scanning with tools such as Nmap and Nessus. Google and other search engines can also be used to identify potential weak spots. The Attack stage represents modification of the target system by an attacker. The system can be modified in the following aspects: Confidentiality; Integrity; and Availability.

These aspects are also known as the CIA principles. Confidentiality refers to prevention of disclosure of information to unauthorized individuals or systems. Integrity means that data in a system cannot be modified undetectably. Availability refers to the availability of information when required by the system to serve its purpose. In computing, e-Business and information security, it is necessary to ensure that data, transactions, communications and documents are genuine. It is also important that authentication validates the identities of both parties involved.

In figure 1 the Temporal Attack Model is represented. The Attack stage is subdivided into sub-stages. The first sub-stage is the Ramp-up stage. This sub-stage refers to the preparatory actions performed by an attacker before his/her final goal can be attained. The targeted computer network is modified in this stage, but only in preparation for some other goal. This stage typically includes the installation of backdoors and other malware.

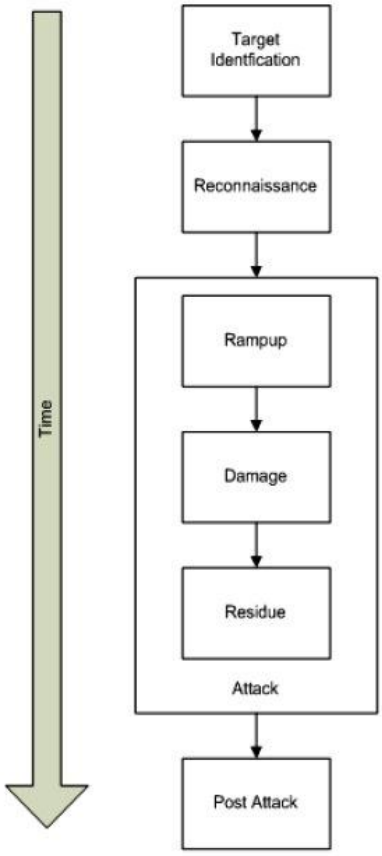

Fig. 1. Temporal Network Attack Model.

The Damage sub-stage refers to actions undertaken by an attacker during the achievement of his/her final goal. In this sub-stage the network is damaged according to the Information Security CIA principles. For example when an attacker launches a Distributed Denial of Service (DDoS) attack on a network, the Damage sub-stage is entered as soon as the attack is launched. The action of installing DDoS attack software falls under the Ramp-up stage.

The Residue sub-stage refers to unintended communications and actions by malware after an attack has been completed. For example, computers that have incorrect time settings may attack their target at a later date and/or time than when the original coordinated attack was planned. This is also noticed in DDoS attacks.

The Post-Attack Reconnaissance stage refers to scouting and other similar reconnaissance actions performed by an attacker after completion of the Attack stage. The attacker's goal in this stage is to verify the effects of his/her attack and to assess whether the same methodology can be used again in the future.

3 Significant Hacking Events

We consider the following to be the most significant hacking events.

Brain Virus: The world's first computer virus was created by two brothers, Basit and AmjadFarooqAlvi, in Lahore, Pakistan [5]. This was a boot sector virus since it only affected boot records [6]. The Brain virus marked the area where the virus code was hidden as having bad sectors [7]. It occupied a part of the computer memory and infected any floppy disk that was accessed. It hid itself from detection by hooking into the INT13. When an attempt was made to read the infected sector, the virus simply showed the original sector. This resulted in a change to the volume label.

Morris Worm: On 2nd November 1988 a Cornell graduate student, Robert Tappan Morris, unleashed the first computer worm [8]. It started as a benign experiment with a simple bug in a program, but the worm replicated much faster than anticipated [9]. By the following morning it had infected over 6000 hosts [10]. The worm could not determine whether a host had already been infected or not and as a result distributed multiple copies of itself on a single host. The exponential increase in data load eventually tipped off the system administrators and the worm was discovered.

CIH Virus: The CIH virus, also referred to as the Chernobyl or E95.CIH virus, first appeared in June 1998 [7]. It was created by a Taiwanese college student called Chen Ing-Hau [11]. It possessed a destructive payload with the purpose to destroy data. On release, the virus attempted to override a portion of the hard disk as well as the flash ROM of the PC. It infected over a million computers in Korea at the time [7].

I-LOVE-YOU Worm: The I-LOVE-YOU worm first appeared on May 4, 2000 in the form of an e-mail with the subject: I-LOVE-YOU [7]. It was created by a student named Onel de Guzman, and originated from Manila, Philippines. The worm code was written using Visual Basic and processed by the WScript engine [12]. It targeted computers using Internet Explorer and Microsoft's Outlook. Within a few hours it had spread worldwide via e-mail by making use of Outlook addresses of infected users. It exploited human curiosity, enticing people into opening an untrusted email.

Code Red Worm: The Code Red worm appeared on July 12, 2001. It exploited a buffer-overflow vulnerability in Microsoft's IIS web servers [13]. Upon infection of a machine, it checked whether the date was between the first and the nineteenth of the month. If so, a random list of IP addresses was generated and each machine on the list was probed to infect as many other machines as possible. Proper propagation of the worm failed due to a code error in the random number generator [14]. On 19 July a second version of the Code Red worm appeared that infected computers at a rate of 200 hosts per minute [9].

Estonia Hack Attack: Early in 2007, a series of politically motivated cyber-attacks struck Estonia [16]. The attacks included web defacements and DDoS attacks on Estonia government agencies, banks and Internet Service Providers. The attacks followed the removal of a bronze statue in Tallinn, which commemorated the dead from the Second World War [17]. At the time of the attacks, Estonia was one of the leading nations in Europe with regards to information and communication technologies [16]. This can be considered an example of cyber warfare and its potential effects.

Conficker Worm: The Conficker was the first worm to penetrate cloud technology [15], [18]. It first appeared in November 2008 and quickly became one of the most infamous worms to date. The Conficker worm controlled over 6.4 million computer systems and also owned the world's largest cloud network at the time. As a result of the infrastructure of a cloud, the worm could propagate much faster, infect a broader range of hosts and cause greater damage. Conficker has not been used as an attack weapon since, and it is speculated that it might have been a precursor to Stuxnet.

Stuxnet Worm: Stuxnet was one of the most complex threats ever analysed [19]. The primary purpose of Stuxnet was to target industrial control systems such as gas pipelines and power plants with the goal of reprogramming the programmable logic controls (PLCs) of the systems to enable an attacker to control them. Stuxnet was also the first to exploit four zero-day vulnerabilities as well as compromise two digital certificates. As of September 29, 2010, Iran had the greatest number of infected computer systems. Stuxnet has shown that direct-attack attempts on critical infrastructures are no longer a myth but a definite possibility. Stuxnet actions can be considered an act of war, but no one has officially claimed responsibility for it.

4 Trends

Although our selection of significant hacking events is subjective and does not represent a comprehensive list, some interesting trends can be identified. Firstly, the monetary impact of each event is shown in figure 2. The vertical scale represents an estimation of the effect. Effects are classified as follows: 5 – severe financial impact; 4 – significant financial impact; 3 – major financial impact; 2 – minor financial impact; and 1 – negligible financial impact. On the horizontal scale, the attacks are listed in chronological order.

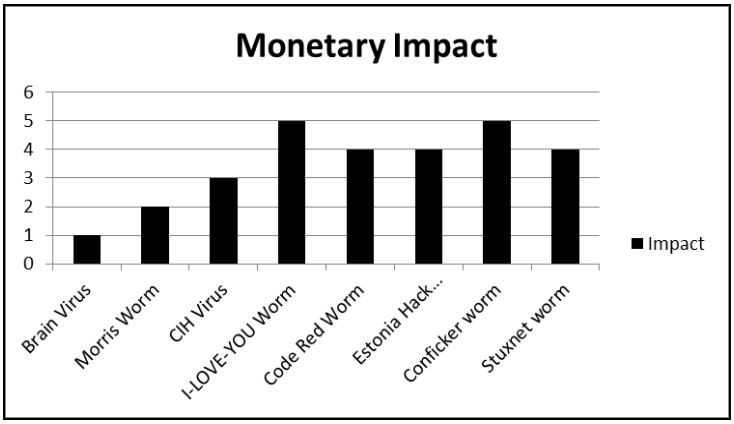

Fig. 2. Monetary impact of hacking events.

Figure 3 lists the most common countries of origin of hacking events. Most events surprisingly originate from the Philippines. Figure 4 illustrates the number of events per continent, with Europe and Asia at the top of the list.

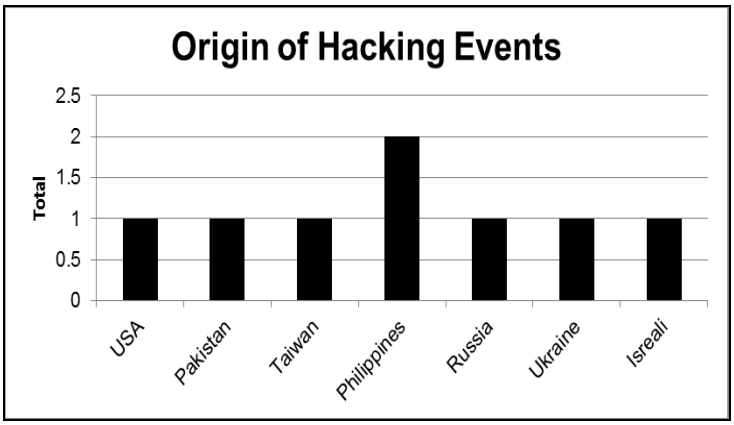

Fig. 3. Countries of origin of hacking events.

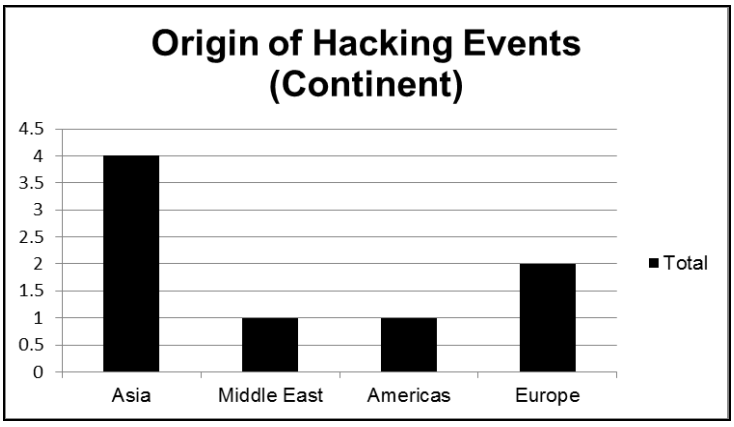

Fig. 4. Hacking events per continent.

In most hacking events, small malware of between 1,000 and 100,000 bytes were utilized. The significant exception is Stuxnet, with a size of over 1.5 megabytes. The progressive increase in bandwidth and computer memory size will likely lend itself to the use of bigger malware (figure 5).

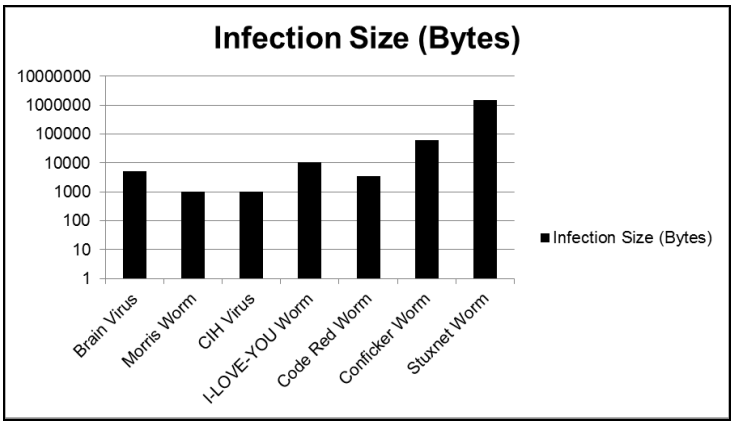

Fig. 5. Infection size in bytes.

5 Attack Model Map

The following sections describe how the most significant hacking events map to the Attack Model in Section 3.

5.1 Brain Virus

- Target Identification: Experimentation with 5.25 inch floppy disks.
- Reconnaissance: Exploring and experimenting with the DOS File Allocation Table (FAT) file system on the floppy disks.
- Ramp-up: Writing and inclusion of malicious code on a 5.25 inch floppy disk.
- Damage: Changing the volume label to read either Brain or ashar.
- Residue: The changed disk label and the message left in infected boot sectors.
- Post attack: Using the same technique to infect hard disks.

5.2 Morris Worm

- Target Identification: Experimenting with the ARPANET.
- Reconnaissance: Scanning the ARPANET network for flaws and vulnerabilities.
- Ramp-up: Writing the experimental program which includes the source code for the worm.
- Damage: The release of the experimental program on the ARPANET.
- Residue: A machine being infected multiple times rather than only once.
- Post attack: Experimenting with the possibility of a worm in different environments.

5.3 CIH Virus

- Target Identification: Exploring the gaps left in PE (Portable Executable) files.
- Reconnaissance: Experimenting with PE file formats under Windows 95, 98 and ME for potential vulnerabilities.
- Ramp-up: Writing the CIH virus code.
- Damage: Spreading of the CIH virus on computers, and destroying certain PC's BIOS, thus disabling PC use.
- Residue: No unintended attacks caused by the virus in this case.
- Post attack: Verifying the effects of the virus by means of scouting.

5.4 I-LOVE-YOU Worm

- Target Identification: Exploring and experimenting with the Windows operating system and Microsoft Outlook.
- Reconnaissance: Using well-known search engines to search for potential weaknesses in the Windows operating system and Microsoft Outlook.
- Ramp-up: Writing the I-LOVE-YOU worm code.
- Damage: The worm led to an effective DoS attack.
- Residue: Only hidden files with .mp2 and .mp3 extensions.
- Post attack: Searching for other additional weaknesses in the Windows operating system and Microsoft Outlook.

5.5 Code Red Worm

- Target Identification: Exploring the Microsoft IIS server configurations.
- Reconnaissance: Using well-known search engines to search for potential vulnerabilities in the IIS server software.
- Ramp-up: Writing the Code Red worm code and identifying a buffer overflow vulnerability in the software.
- Damage: Launching a DoS attack against randomly selected server IP addresses.
- Residue: The worm used a static seed as its random number generator and so generated identical lists of IP addresses that caused computers to be infected multiple times.
- Post attack: Searching for additional weaknesses in Microsoft's IIS servers.

5.6 Estonia Hack Attack

- Target Identification: The relocation of the Bronze Soldier in Tallinn.
- Reconnaissance: Using well-known search engines to identify possible weaknesses in the websites of well-known Estonian organizations.
- Ramp-up: Installation of malware on targeted computer systems.
- Damage: Government and commercial services (such as banks) became unavailable during the attack.

- Residue: Russian-language bulletin boards and one defaced website with the phrase: “Hacked from Russian hackers”.
- Post attack: Scanning of the infected computer networks to determine the effects of the attacks.

5.7 Conficker Worm

- Target Identification: Exploring cloud computing.
- Reconnaissance: Using well-known search engines to identify possible vulnerabilities in a cloud computing system.
- Ramp-up: Writing the code for the Conficker worm.
- Damage: Launching the Conficker worm in the cloud, thus making its target resources available to the attacker.
- Residue: No unintended attacks caused by the worm in this case.
- Post attack: Releasing additional versions of the worm to verify the effects.

5.8 Stuxnet Worm

- Target Identification: Uranium enrichment infrastructure in Iran.
- Reconnaissance: Using well-known search engines to identify possible vulnerabilities in industrial software and equipment developed by Siemens.
- Ramp-up: Writing the code for the Stuxnet worm and installing additional malware on targeted computer networks.
- Damage: It physically damaged the Iranian Nuclear enrichment systems.
- Residue: Infiltration of computer systems other than those in Iran.
- Post attack: Verifying the effects on Iran’s industrial software systems.

6 Protection of Critical Infrastructure

The protection of critical infrastructure involves the readiness to act against serious incidents threatening the critical infrastructure of a nation. Recently there is an increasing need to protect critical infrastructure from terrorist or other physical attacks, including cyber-attacks [20]. The previous sections emphasized this need by reviewing eight of the most significant computer network attacks. Apart from Stuxnet, there have been other instances of infrastructure attacks through computer networks [21]:

- Maroochy Shire Council’s sewage control system in Queensland, Australia was attacked.
- A teenager in Worcester, Massachusetts broke into the Bell Atlantic computer system and disabled part of the public switched telephone network using a dial-up modem connected to the system. This attack disabled phone services at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport.

- In 2000, the Interior Ministry of Russia reported that hackers seized temporary control of the system regulating gas flows in natural gas pipelines.
- In August 2005, Zotob worm crashed thirteen of DaimlerChrysler's U.S. automobile manufacturing plants forcing them to remain offline for almost an hour. Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware, and Michigan were also forced down.
- The Sobig virus was blamed for shutting down train signaling systems throughout the east coast of the U.S. The virus infected the computer system at CSX Corp.'s Jacksonville, Florida headquarters, shutting down signaling, dispatching, and other systems.
- The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as the Slammer worm infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours.

The Attack Model of Section 2.2 is able to map these Infrastructure computer based attacks. The ultimate goal of this research is to prevent such attacks by identifying the initial stages early enough for preventative actions. The model is able to present any type of computer network based attack, since computer based attacks on Infrastructure uses the same techniques and methodologies as traditional computer network attacks. The Reconnaissance and Ramp-up stages for attacking Infrastructure are similar for attacking computer networks.

7 Conclusion and Future Work

The goal of the network attack model was to represent the majority of network based attacks. This temporal model was verified by mapping eight significant computer network attacks. The attacks were chosen to represent the most significant computer attacks (hacks) in the authors view. The mapping of these attacks shows the usability of the temporal model in aiding critical infrastructure protection.

To prevent or protect against computer attacks, the CSIR are investigating methods to detect the Reconnaissance and Ramp-up stages of an attack. If these stages can be detected, mitigating action can be taken against computer attacks. The attack model is under development and will evolve as the research progress. Future work includes adding new dimensions to the classification of attacks, namely origin and motivation of the attack. Reviewing the reasons of why a network was easily penetrated and focusing on the commonalities of learnt lessons will also be explored.

References

1. Heater, B.: Male: A Brief Timeline (2011), http://www.pcmag.com/slideshow/story/261678/malware-a-brief-timeline/
2. Hall, K.: The 7 worstcyberattacks in history (that we know about) (2012), http://dvice.com/archives/2010/09/7-of-the-most-d.php

3. Julian: 10 Most Costly Cyber Attacks in History (2011), http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history/
4. van Heerden, R.P., Irwin B., Burke, I.D.: Classifying Network Attack Scenarios using an Ontology. In: Proceedings of the 7th International Conference on Information Warfare and Security, pp. 331-324 (2012)
5. Desai, P.: Towards an undetectable computer virus, Master's thesis, San Jose State University (2008), http://www.cs.sjsu.edu/faculty/stamp/students/Desai_Priti.pdf
6. Subramanya, S.R., Lakshminarasimhan, N.: Computer viruses. Potential IEEE, 20(4), pp. 16-19 (2001)
7. Blümler, P.: I-LOVE-YOU: Viruses, Trojan Horses and Worms, www.econmr.org/datapool/page/30/virus.pdf
8. Orman, H.: The Morris worm: a fifteen-year perspective. Security & Privacy, IEEE, 1(5), pp. 35-43 (2003)
9. Chen, T.M., Robert J.M.: Worm epidemics in high-speed networks. Computer, 37(6), pp. 48-53 (2004)
10. Cass, S.: Anatomy of malice [computer viruses]. Spectrum, IEEE, 38(11), pp. 56-60 (2004)
11. Bosworth, S., Kabay, M.E.: Computer security handbook. John Wiley & Sons Inc., New York (2002)
12. Bishop, M.: Analysis of the ILOVEYOU Worm (2000), http://nob.cs.ucdavis.edu/classes/ecs155-2005-04/handouts/iloveyou.pdf
13. Moore, D., Shannon, C.: Code-Red: a case study on the spread and victims of an Internet worm. In: Proceedings of the 2nd ACMSIGCOMM Workshop on Internet measurement, ACM, pp. 273-284 (2002)
14. Zou, C.C., Gong, W., Towsley, D.: Code red worm propagation modeling and analysis. In: Proceedings of the 9th ACM conference on Computer and Communications security, ACM, pp. 138-147 (2002)
15. Sarwar, U., Ramadass, S., Budiarto, R.: Dawn Of The Mobile Malware: Reviewing Mobile Worms. In: Proceedings of the 4th International Conference on Sciences of Electronic, Technologies of Information and Telecommunications (SETIT2007), pp. 35- 39 (2007)
16. Czosseck, C., Ottis, R., Taliharm, A.M.: Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. International Journal of Cyber Warfare and Terrorism (IJCWT), 1(1), pp. 24-34 (2011)
17. Davis, J.: Hackers Take Down the Most Wired Country in Europe, Wired Magazine, 9(15) (2007)
18. Sharma, V.: An Analytical Survey of Recent Worm Attacks, In IJCSNS, 11(11), pp. 99 - 103 (2011)
19. Falliere, N., Murchu, L.O., Chien, E.: W32.stuxnet dossier: version 1.4, White paper, Symantec Corp., Security Response (2011), http://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf
20. Bradley, F.: Critical infrastructure protection. Electric Energy T and D, 7(2), pp. 4-6 (2003)
21. Tsang, S.: Cyberthreats, Vulnerabilities and Attacks on SCADA Networks (2009), http://gspp.berkeley.edu/iths/Tsang SCADA%20Attacks.pdf