J. Basic. Appl. Sci. Res., 3(2s)218-221, 2013
© 2013, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied
Scientific Research
www.textroad.com

An Analysis of Cyber Attacks

Hamed Niki[1] and Parvaneh Shahamati[2] and Somayyeh Ravoshi[3]

[1]University Teacher, Department of Computer engineering, Qazvin Payamenoor University
[2,3]University Student, Qazvin Payamenoor University

Received: June 10 2013
Accepted: July 10 2013

ABSTRACT

In this paper, issues related to soft war and its concepts are described. This project aims at familiarizing the readers with the concepts associated with cyber space (cyber) and the risks thereof. The concepts provided here are cyberspace, scale of cyber attacks, factors involved in cyber attacks, victims and measures to prevent these attacks, including Intrusion Detection Systems (IDS). Then, a solution to reducing the number of attacks is proposed. It should be noted that, for this solution to be implemented, one can only rely on efforts made by researchers.

KEYWORDS: cyber, dimensions of cyber attacks, cyber attack victims, cyberspace, IDS

1. INTRODUCTION

By 1945, most wars were *hard* ones. Then, in light of the world's polarization into East and West blocks, a new round of competition between the United States and the Soviet Union began, which was called the Cold War. The Cold War was a mix of *hard* and *soft* ware, in which two superpowers, despite sending each other significant threat signals, avoided direct confrontation. With the collapse of the Soviet Union in 1991 and the end of the Cold War, using the experience from two world wars and the Cold War, war experts in the United States found that political, economic and other goals can be achieved at lower cost and without directly involvement in other countries. This notion was introduced into the political literature under the name Soft War.

2. Definition of Soft War

The notion of Soft War is normally conceived as opposing to Hard War. John Collins, a theorist at US National University of War, describes the soft war as "a planned use of advertising tools to influence the intellectual coordinates of an enemy in ways that will serve the advertiser's national security purposes".

3. Definition of Cyber

Lexically, the word 'cyber' has been defined as virtual and intangible. Cyber is a term taken from the word «kybernetes» meaning steersman or guide, and was first used in the book Neuromancer by William Gibson, an author of science fictions.

4. Cyber Space

Cyber space is a virtual environment in the space of international networks (connected via information highways such as the Internet), where all the information about relations between individuals, cultures, nations, countries and generally anything tangible on the Earth exists in the form of digital text, picture, audio and documents. Through computers connected via the international networks, users can access this information globally.

5. Cyber Attacks

Cyber attacks include a range of actions, including website elimination and stealing valuable information. A cyber attack can be defined as any action by an insider or external factors that endangers national, or organizational, security. Cyber attacks may be motivated by political conflicts, social tensions, religious extremism and, in some cases, retaliation.

6. Dimensions of Cyber Attacks

6.1. Politically Motivated Attacks

Politically motivated cyber criminals may belong to extremist groups using cyberspace to publish and distribute their propaganda. Politically motivated attacks can be divided into three categories:

- political protests against government action
- dissatisfaction with the creation of a public document, policy or law
- rage against acts of physical violence

Corresponding Author: Hamed Niki, Department of Computer engineering Branch of Information technology, University of Qazvin Payamenoor, Country Iran. Email address: Hamed.niki@ikiu.ac.ir

6.2. Attacks Motivated by Sociocultural Factors

Cyber attacks may happen due to individuals and groups competing over resources, power and taking control. Such attacks can be divided into three general categories:

- social and cultural aggression
- land disputes
- historic events and special days

6.3. Economically Motivated Attacks

Economically motivated attacks can be classified into two groups:

- attacks with incentives coming from economic and/or personal conditions and financial cooperation
- political or economic espionage-related attacks

7. Cyber Attack Factors

Cyber attackers are computer systems. Behind any attack, there is a well-motivated human factor, with the most basic member being the invader. This is why human factors are the first point of transition between cyber incidents and physical incidents. Understanding the existence, and close monitoring of the possibility, of certain types of attack based on economic and political events, can be a key to predicting those events. Human factors committing cyber attacks are divided into four groups:

- individuals who seek entertainment and/or skill improvement
- agents
- social protesters
- national governments

Hackers are among agents committing attacks. The term hacker was used for the first time in the mid 60's and means a computer programmer who plows computer codes. Hackers were talented people who could find new ways of using computer programs and create programs most others couldn't even imagine.

7.1. The Purpose of Hacking

In their plowing of computer codes, hackers may pursue one or more of these purposes:

1. to make known their mastery of computer and information technology
2. notification of security weaknesses in computer networks
3. personal or group revenge
4. acquiring virtual property of individuals or companies
5. without a reason

8. Attack Victims

8.1. Ministry of Petroleum

There was an attack by a virus known as "Viper", which left behind very damaging effects on Iran. Viper had been designed and transferred to the computer systems of Ministry of Petroleum to reduce oil production, and was able to irreversibly delete all the data from the servers making information retrieval impossible under any circumstances. After removal of information, Viper would burn the motherboard, and the server would go out of service. From the perspective of IT professionals, three factors, namely poor management, disruption or penetration of foreign software and hardware failure, make it possible to hack computer networks through virus attacks or any other method. Since advanced software demands advanced hardware platform, we need to determine the factor(s) which paved the way for the cyber attack targeted at the Ministry of Petroleum.

8.2. Ministry of Science

Ministry of Science, Research and Technology was the second ministry targeted by cyber attackers. Joint projects of the Ministry of Science with the Ministry of Defense might have motivated the hackers to penetrate the department's servers and gain access to the main server to create interference and obtain information.

8.3. Nuclear Facilities

There has been cyber war against Iran's nuclear facilities by the West since 2005. Research by Symantec shows that the West started a project of cyber attack on Iran's nuclear facilities in 2005 and implemented it in 2007. July 24, 2010 was the day cyber attacks on Iran (e.g. Stuxnet) were launched.

Iran's computers were severely attacked by the computer worm Stuxnet, which attempted to steal information from industrial controlling systems, exposing them on the Internet. Stuxnet was able to destroy the gas pipes, cause damages in nuclear facilities and even make factory boilers explode. The spy worm managed to penetrate control systems built by Germany's Siemens used in the industrial facilities for providing drinking water, oil wells, power plants and other industrial facilities.

9. Measures to Prevent Cyber Attacks

9.1. Intrusion Detection System (IDS)

The task of an intrusion detection system is to detect and identify any unauthorized or malicious use of, or damage to, the systems by both internal and external users. Today, intrusion detection and prevention is one of the main mechanisms for securing computer networks and systems. It is also used along with firewalls and as a security supplement to them. There are various methods of attack detection capable of detecting malicious actions within the network. Systems are composed of many different components which can be put together in different ways to provide different functions.

9.2. Types of Network Attacks Based on Attack Mode

A network intrusion is generally considered an attack. Network attacks can be divided into two main groups, depending on how it's done. A network attack can be described in terms of the objectives pursued by attacker. The objective is usually a Denial of Service (DOS) or unauthorized access to network resources.

Denial of Service: In this type of attack, the attacker disrupts services provided by a server to its users.

Network Access Attacks: In this type of attack, the attacker can gain unauthorized access to network resources and use the possibility to carry out unauthorized, and even illegal, activities.

9.2.1. Types of Network Attacks in Terms of the Attacker

- *Attacks by trusted users (internal):* This is one of the most dangerous types of attacks because, on the one hand, the user has access to various network resources and, on the other hand, security policies do not often set sufficient limitations on them;
- *Attacks by non-trusted users (external):* This is the most common type. An outsider, who is, normally, not trusted attacks a network;
- *Attacks by inexperienced attackers:* many intrusion and attack tools are available on the internet. In fact, many people, without any specific experience, can simply use the tools available to create network problems.
- *Attacks by experienced users:* professional, experienced strikers are conversant in writing various types of malicious code.

10. Supplements to IDS Security

Intrusion Detection Systems are solutions (or to put it another way, a type of technology) used for security purposes in computer networks. Traditionally, different supplementary systems are used along with IDS's, each with its own stand in establishing security. Here, firewalls, encryption and authentication mechanisms, and access control lists are introduced.

10.1. Firewalls

Firewall is one of the oldest and best known security solutions. It can apply various security policies based on administrator settings, including the flow permit, the ability to communicate outside the network and assigning which out-of-network services authorized users are allowed to use. In general, two types of policies can be used in firewalls:

- To allow any connections that are not explicitly prohibited, and
- To avoid all communication flows except in cases where there is explicit permission;

One difference between IDS's and firewalls is that firewalls are normally located at access points of a network to allow certain inbound or outbound flows, while IDS's are passive components whose responsibility is to respond to potential attacks. IDS's use their sensors to scan network traffic, and there are limited types used at network access points, such as routers. In one of the possible settings where IDS and firewall can be used together, sensors are located outside the network and before the firewall, in the so-called 'demilitarized zone', to scan all inbound connections. This way, they can assign security policies for the firewall.

10.2. Encryption and Authentication Mechanisms

Encryption is one of the most common and most effective ways to protect information security. This mechanism is capable of providing secure point-to-point data transfer between clients, servers and routers. However, encryption cannot be used as the only path to safety.

10.3. Access Control Lists

Access control lists are a set of rules used by firewalls and routers to apply restrictions on traffic and access. These are not by themselves sufficient for responding to attacks. However, based on the security policy at work, these lists can be applied to firewalls and routers to restrict a range of IP's[1] to certain services.

[1] Internet Protocol

11. Types of IDS

IDS functionality can be host-based, network-based, or distributed.

11.1. Host-based Systems

These systems, briefly called HIDS, protect a host against intrusions. HIDS is run on the system to control all activities and processes. It uses the resources of the system, including memory and processor(s), and is responsible for access control (e.g. what processor uses what resources, etc.).

11.2. Network-based Systems

These systems, briefly called NIDS, function in the context of networks, scanning and analyzing the traffic at all levels in search of symptoms signaling infiltrations or attacks. Possible types of network-level attacks include DOS and, port scanning. These systems usually scan incoming or outgoing access points to the network. They often have several sensors at different locations to get traffic. The characteristics of the traffic are sent to a central database of intrusion detection where, based on different approaches, intrusive actions are detected.

11.3. Distributed Systems

Nowadays, with the increasing network bandwidths and the need for continuous scanning data, network intrusion detection systems should also develop at a similar rate. Network-based centralized architecture methods cannot meet the needs of today's networks. In these methods, to detect multi-step attacks, holding the status of communication and protocol-based interactions, the system throughput undergoes compaction and loss due to having only one service point. Intrusion detection algorithms are based on a set of rules and are growing rapidly. Implementation of distributed IDS imposes necessities on network architecture, software for proper distribution and splitting of traffic between the parallel segments. The performance of distributed IDS can be based on two types of techniques: traffic division and load balancing.

12. Solutions Proposed to Mitigate Attacks

To reduce cyber attacks, an agency called ‘National Center for Cyber Coordination’ can be established. The agency would then scan the traffic of all the websites using services provided by the domestic ISP’s. This way, suspicious behavior by clients can be monitored in a defined time period. In case of violation, legal action will be undertaken, otherwise, the client is identified as a regular user and the monitoring can be stopped.

Here’s an example of how this can be implemented: a set of keywords is specified; if any of these keywords are used in the client’s emails, their activity will be monitored for a defined time period to make sure if there is a threat.

Noteworthy here is that this is only a small example of the idea can be implemented. It can be extended to bring many parts of cyberspace under control and, consequently, reduce risks.

REFERENCES

[1] Ziai Parvar, H. (2007 A), The Soft War - On Computer Wars, Qom, Bagheri, Second Print

[2] Ziai Parvar, H. (2007 B), The Soft War - On Computer Wars, Qom, Bagheri, Second Print

[3] Hazeq Nikroo, H. (2008), A Review of the Zionist PSYOP at the 33-day War, PSYOPS Site (http://www.arnet.ir/?lang=fa&state=showbody_news&row_id=10863)

[4] Taghanaki, H. (2004), Virtual Jihad, Virtual Jihad Weblog (http://mhta.persianblog.ir/post/36)