Real-Time System for Assessing the Information Security of Computer Networks

Dimitrina Polimirova and Eugene Nickolov

National Laboratory of Computer Virology - Bulgarian Academy of Sciences,
1113 Sofia, Bulgaria, "Acad. Georgi Bonchev" Str., Block 8, Office 104
{polimira,eugene}@nlcv.bas.bg

Abstract. The report examines the possibility of establishing of real-time system for analysis and assessment of information security of computers, systems and networks in Internet/Intranet/Extranet environment, using TCP/IP protocols. In the paper are presented known information attacks. Separate classes of malicious software investigations are considered concerning different work platforms (produced by different Computing Systems), work environments (produced by different Browser Systems) and work places (produced by different Antimalware Systems). Methods that can be used to implement the systems are suggested. The capabilities of real-time systems are commented at the end of the paper.

Keywords: Data Security, Computer Security, Communication Security, Operating System Security, Web Security, Application Security.

1 The Problem

The modern information society requires the use of various types and configuration computers, systems and networks in TCP/IP environment. These computers, systems and networks are subject to permanent attacks with respect to their information security, which determines the need of investigation on methods and means for their protection.

A common strategy for protecting computers, systems and networks includes using of antivirus and security software. In addition the development of suitable for those computers, systems and networks security policy could be included.

Within the above research opportunities may apprise that it is appropriate to examine this problems of individual stages.

For the purpose of this paper can say that it is necessary to analyze the benefit of building of real-time system for assessment of information security of various types computers, systems and networks, exposed to one or more attacks, taking into account the impact of the protection methods in the face of various antivirus and security software.

Since the 70-th of century the problem for security and protection of computers, systems and networks has drawn developers' and constructors' attention in the area of information technology [1]. With the first malattack in the 60th of last century [2], a progress in the area of information security of computers,

J. Camenisch, V. Kisimov, and M. Dubovitskaya (Eds.): iNetSec 2010, LNCS 6555, pp. 123–133, 2011.

systems and networks is observed and requirements for their information security are increased. As a result for short time ideas significantly reducing the risk in the management of computers, systems and networks are realized.

2 Actuality

The main open problem, which can be placed within this paper, is related with the investigation of public known information attacks on one hand and most popular computing, browsers and antimalware *systems* on the other hand.

The main hypothesis will be linked with the ability to analyze and evaluate the effectiveness of a real-time system for assessing information security used as a means of determining the security policy with the lowest risk for individual computers, systems and networks.

Further analyses and investigations can be made towards precise planning of the economic costs of conducting a security policy for different configurations computers, systems and networks.

3 Goal and Tasks of the Investigation

The studies, which may be planned, should be linked with an analysis of the current state and development prospects of known information attacks, computing systems, browser systems and antimalware systems. Their scientific generalization in the form of real-time systems for assessing of information security is necessary because only in their mutual relations can be achieved the best analysis and therefore the best solutions for information security of computers, systems and networks.

3.1 The Main Goal

As a result of mentioned above the *main goal* of the paper can be specified: to analyze the effectiveness of the integration of the separate classes of malicious software investigations concerning different experimental work platforms, experimental work environments and experimental work places.

The integration is represented by a real-time system for presenting the obtained results with the help of which analysis and assessment of information security of computer systems and networks in the TCP/IP environment can be made.

3.2 Main Tasks

The following *main tasks* are set in reaching the goal:

1. To identify and systematize information attacks known until the moment of investigation;
2. To identify and systematize investigated:
   2.1 Operating Systems (OS), used by the Computing Systems;
   2.2 Browsers, used by the Browser Systems;
   2.3 Antivirus and security software, used by the Antimalware Systems.

4 Work Definitions

For the goal of this paper the following *work definitions* are proposed [3]:

1. As *information security* we will note the protection of the information in computers, systems and networks from a random or purposeful access of their resources aimed at reading, transferring (coping), modifying or destroying the information;
2. As *information attack* we will note any attempt to break the integrity of information objects that can be bit, byte, sector, file, directory system, browser systems, antimalware systems, operating systems, network systems, etc.;
3. As *computing system* we will note combination of hardware and software tools for solving specific application problems using preliminary prepared algorithmic solutions;
4. As *browser system* we will note software tools (programming tool), which is designed to perform requests for serving in client–server architecture and web functionality;
5. As *antimalware systems* we will note combination of different types of protecting system's components, which includes the following: anti-virus, anti-adware, anti-spyware, anti-trojan horse, anti-downloader, etc.

5 Analysis of Information Attacks

The information attacks can be divided into two main categories: malware and malattacks (Fig. 1). The main difference between them lies in the fact that in case of malware the direct participation of a user at the moment of the attack is missing, while in case of malattack the user's presence is required [4], [5].

Fig. 1. Main categories information attacks

The following attacks can be collected from the current information base of National Laboratory of Computer Virology of Bulgarian Academy of Sciences [6]. It collects information for the information attacks, which were carried out to a separate personal and/or corporate computers, and/or networks, and/or systems for the 2009. This is a generalization of the attacks, implemented in Bulgaria, Balkan Peninsula and south-east Europe.

5.1 Malware

In the category *MALWARE* are included 64 different information attacks, divided into 20 groups (Table 1.).

Table 1. Description of information attacks and their corresponding groups for the *MALWARE* category

Malware Groups	**Single Information Attacks**
I. Ads	(1) AdServer; (2) Adware; (3) Anarchie; (4) Banner; (5) Square news; (6) Investitial; (7) Superstitial; (8) Spam;
II. Browsers	(9) ActiveX; (10) BHO ; (11) Cookie; (12) Prefix of URL; (13) Related Info; (14) Scumware; (15) Ticker;
III. Metadata	(16) ADS (Alternate Data Streams); (17) Binder; (18) Downloader (Trojan Downloader); (19) Dropper;
IV. Joke	(20) Annoyance; (21) Joke;
V. Chat	(22) AOL Attack (America On Line Attack);
VI. Criminal Investigations	(23) Carnivore (DCS1000);
VII. Cracking	(24) Cracking; (25) Password Cracker;
VIII. Spying	(26) Spyware; (27) GUID; (28) IRC Bots; (29) Phishing; (30) Error Reporting Tool; (31) Smart Links; (32) Sniffing; (33) Toolbar; (34) nPnP; (35) WebBug; (36) GSM Pointer; (37) WAP Access Link;
IX. DoS, DDoS	(38) Flooder; (39) Mail Bomber; (40) Nuker; (41) Spoofing; (42) Bacterium;
X. Exploits	(43) Exploit;
XI. Hoaxes	(44) Hoax;
XII. Pop-Ups	(45) Pop-Over; (46) Pop-Under; (47) Pop-Up; (48) Pop-Roll; (49) Pop-Slider;
XIII. Scanners	(50) Port Scanner (IP Scanner); (51) Probe Tools; (52) RAT (Remote Administration Tool); (53) Riskware;
XIV. Keyboard modifiers	(54) Ansi Bomb; (55) Keylogger; (56) Mouselogger; (57) Screenlogger;
XV. Card Fishing	(58) Carding malware;
XVI. Dialer	(58) Dialer;
XVII. Computer Trojan Horses	(60) Computer Trojan Horses;
XVIII. Computer Backdoors	(61) Computer Backdoors;
XIX. Computer Worms	(62) Computer Worms;

5.2 Malattacks

In the category *MALATTACKS* are included 24 different information attacks, divided into 13 groups (Table 2.).

Table 2. Description of information attacks and their corresponding groups for the *MALATTACK* category

Malattacks Groups	Single Attacks
XXI. Using accessible information	(65) Audit Trail; (66) Traffic Analysis;
XXII. Overflow	(67) Buffer Overflow;
XXIII. Vulnerabilities	(68) CGI (Common Gateway Interface) Vulnerabilities; (69) Hijacking; (70) Packet Attacks;
XXIV. Content	(71) Content Attacks;
XXV. Data Encapsulation	(72) Data Driven;
XXVI. Denial of Service	(73) DDoS (Distributed Denial of Service); (74) Flooding;
XXVII. Spoofing	(75) DNS Spoofing; (76) EFT Spoofing; (77) Ethernet Spoofing; (78) IP Spoofing; (79) Screen Spoofing; (80) SET Spoofing; (81) TCP Dump Spoofing; (82) Trace Route Spoofing; (83) Tunnel Spoofing;
XXVIII. CrackPasswd	(84) HTCrackPasswd;
XXIX. Wire/Wireless Phones	(85) Phreaking;
XXX. Physical Analyze Devices	(86) Physical Perimeter Penetration;
XXXI. Social Engineering	(87) Social Engineering;
XXXII. EMI/RFI Intercepts	(88) Wireless Intercepts;
XXXIII. Zombie Computers	(89) Zombies;

Note: Roman numbers in are used later as identifiers of the names of the information attacks groups.

6 Work Platforms, Environments and Places

6.1 Work Platforms

Different experimental work platforms can be investigated for experimental study and analysis of malware for computing systems. The most popular currently using computing systems are based on the operating systems Windows, Linux and Mac. Therefore, for the purposes of this paper, they can be described as basic. On this basis, a reasonable mix of investigations into each one of them may seek and along with it to seek a reasonable summary of their mutual influence.

Fig. 2 shows a percentage distribution of accomplished attacks to Windows OS, Linux OS and Mac OS.

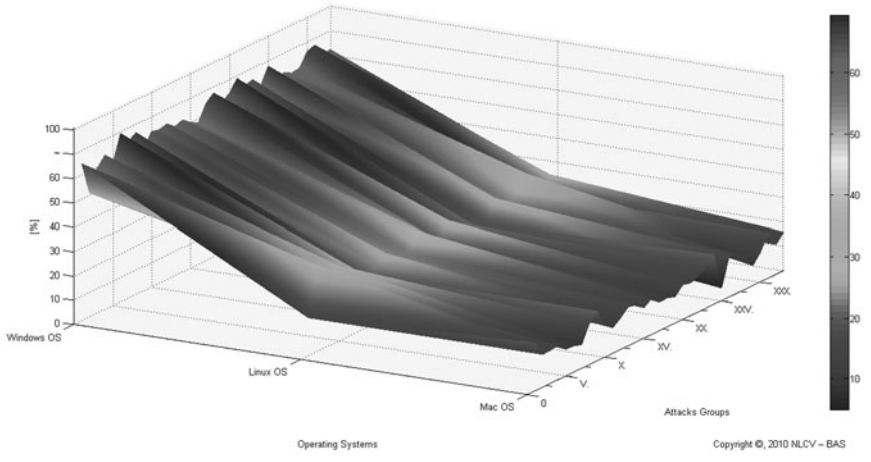

Fig. 2. Percentage distribution of accomplished attacks to Windows, Linux, and Mac

6.2 Experimental Work Places

With respect to the work environments for investigating and analyzing malware for Browser Systems may say that at the current state of information threats can be assessed that the main problem for the security of home, corporate, government networks is the type of the installed browser. Achievements in this area of the various developers are measured not by days, but by hours. With regard to this is sensibly to analyze some chosen from the top 10 classification browsers for the different operating systems.

Fig. 3 shows chosen top 10 the most popular browsers for Bulgaria, Balkan Peninsula and south-east Europe for the main operating systems.

Fig. 4, Fig. 5, and Fig. 6 show percentage distribution of information attacks, accomplished to the separate operating systems with respect to the separate Browser Systems.

6.3 Work Places

With respect to the work places for investigating and analyzing malware based on Antimalware Systems may say that when assessing the information security of the endpoints in the information structure is necessary to report the presence/absent of specialized antivirus and security tools. Depending on the type and nature of the activity and depending on the available funds, different antivirus and security solutions with respect to their functionality and with respect to the end user competent can be chosen. Therefore it is extremely difficult to find a widely applicable antivirus and security solution. This necessitates creating of top 10 antivirus and security solutions classifications which can be used for different investigations.

Fig. 3. Top 10 most popular browsers for Windows, Linux and Mac

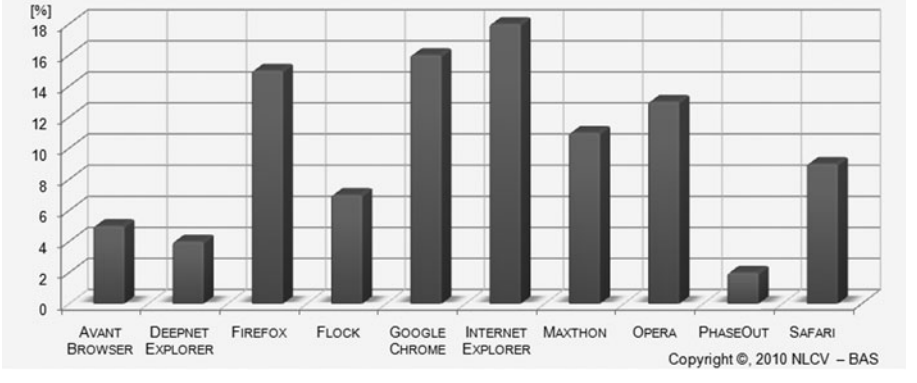

Fig. 4. Percentage distribution of accomplished attacks to Windows OS with respect to the separate Browser Systems

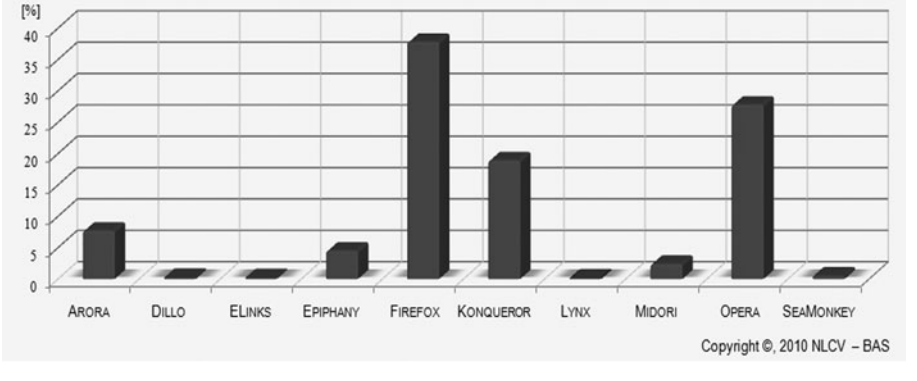

Fig. 5. Percent distribution of accomplished attacks to Linux OS with respect to the separate Browser Systems

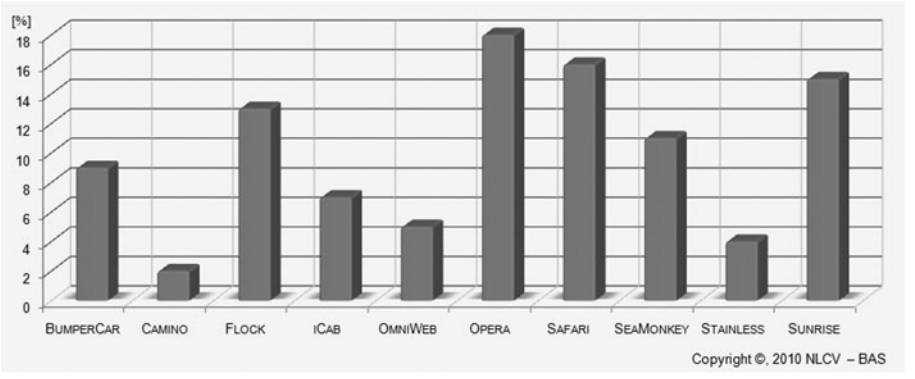

Fig. 6. Percent distribution of accomplished attacks to Mac OS with respect to the separate Browser Systems

Fig. 7 shows chosen top 10 most popular Antimalware Systems for Bulgaria, Balkan Peninsula and south-east Europe for the main operating systems.

Fig. 7. Top 10 most popular Antimalware Systems for Windows, Linux and Mac

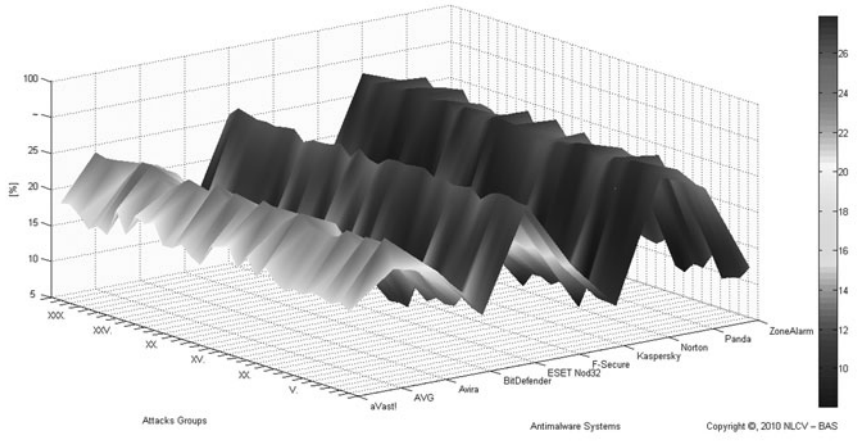

Fig. 8. Percentage distribution of successful accomplished attacks groups to the Windows OS with respect to the separate Antimalware Systems

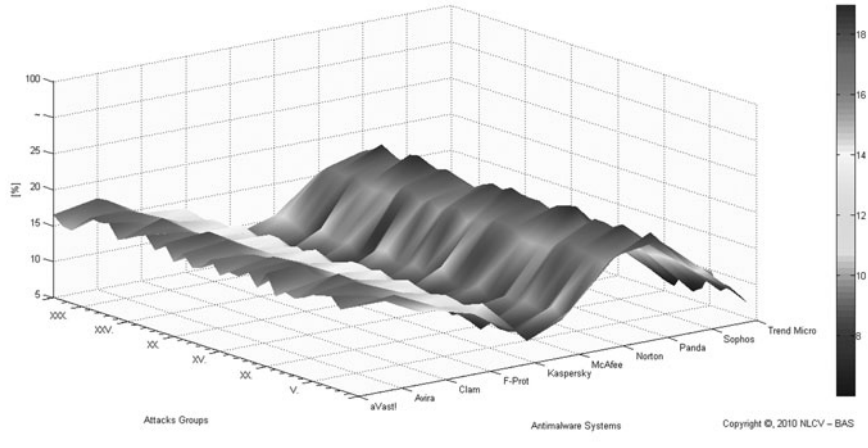

Fig. 9. Percentage distribution of successful accomplished attacks groups to the Linux OS with respect to the separate Antimalware Systems

Fig. 8, Fig. 9, Fig. 10 show the percentage distribution of successful accomplished attacks groups to the separate operating systems with respect to the separate Antimalware Systems.

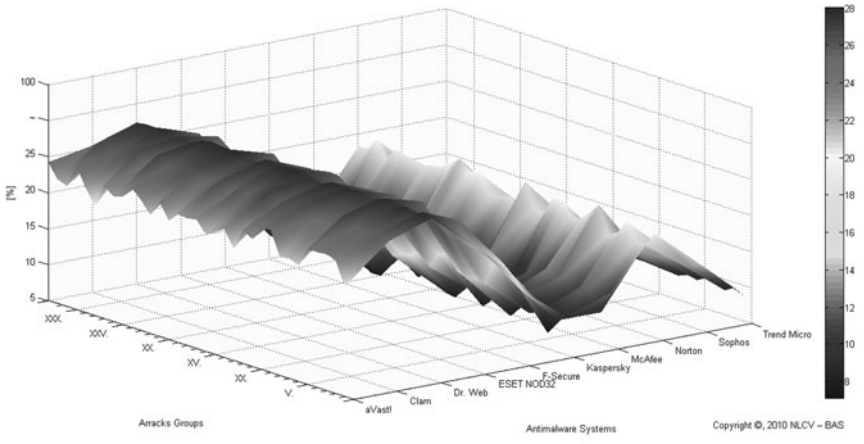

Fig. 10. Percentage distribution of successful accomplished attacks groups to the Mac OS with respect to the separate Antimalware Systems

7 Used Methods

Methods which can be used for the realization of real-time system for assessment of information security of computer networks can include:

1. Creating a reference *binary sequences* describing the behavior of malware through which planned actions in different platforms, environments and locations are carried out;
2. Creating a *data containers* for cyclic accumulation, processing and archiving;
3. Creating a *graphical environment* for online visualization of the obtained results with respect to the selected parameters as a function of other selected parameters.

8 Possibilities of the Real-Time System

The real-time system for assessing the information security will be able to provide a possibility for:

1. Assessing the *velocity propagation* of malware, the *kind* of attacked objects and the *methods* for reducing the impact of malware over TCP/IP environment.

   The methods for reducing the impact include:

   1.1 detection and real-time protection;
   2.2 detection and real-time cleaning;
   2.3 detection and real-time immunization;
   2.4 detection and real-time quarantine.

2. *Assessing the sustainability* of the impact of different malware on various types of information objects in different platforms, environments and locations;
3. *Assessing the applicability and approbation* of different types and kinds of commercial antivirus and security solutions.

   For each triple relation *platform–environment–place*, the assessment for applicability gives:

   3.1 the most security solution (with the lowest risk);

   3.2 the most economical solution (at acceptable risk).

The assessment for approbation gives an opportunity for each selected place, which claimes a certain volume functionality applicable to a certain combination *platform–environment*, to be officially confirmed, that it has the announced functionality.

9 Conclusions and Recommendations

The chosen formulation for investigations of malware for different computing systems (presented by operating systems), browser systems (presented by the top 10 most popular browsers) and antimalware systems (presented by the top 10 most popular antivirus and security software) contains the necessary potential for extensive research in this and other neighboring areas.

The results obtained by the real-time system for assessing the information security, give an opportunity for concrete planning of security policy of different configurations computers, systems and networks.

Conditions for precise planning of economic expenses, related to the performing of security policy for determinate configuration computer, system and networks, are created.

References

1. Denning, D.E.: A lattice model of secure information flow. Communications of the ACM 19(5), 236–243 (1976)
2. The St. Petersburg Times, `http://www.sptimes.com/Hackers/history.hacking.html`
3. Brotby, W.K.: Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement, pp. 7–8. CRC Press, Boca Raton (2009)
4. Parsons, J.J., Oja, D.: New Perspectives Computer Concepts 2010: Introductory. Cengage Learning, p. 162 (2009)
5. Radhamani, G., Rao, R.: Web Services Security and E-business, p. 115, p. 25, Global (2007)
6. National Laboratory of Computer Virology – BAS, National Cybersecurity Portal, `http://ncs.nlcv.bas.bg/`