

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Lukas RADVILAVIČIUS

REAL-TIME ANTIVIRUS SCANNING METHODS CHARACTERISTICS' EFFICIENCY STUDY

SUMMARY OF DOCTORAL DISSERTATION

TECHNOLOGICAL SCIENCES,
INFORMATICS ENGINEERING (07T)



LEIDYKLA
Vilnius TECHNIKA 2012

Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2007–2012.

Scientific Supervisor

Prof Dr Habil Antanas ČENYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).

The dissertation is being defended at the Council of Scientific Field of Informatics Engineering at Vilnius Gediminas Technical University:

Chairman

Prof Dr Dalius NAVAKAUSKAS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).

Members:

Prof Dr Habil Romualdas BAUŠYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T),

Assoc Prof Dr Dalius MAŽEIKIA (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T),

Assoc Prof Dr Olga KURASOVA (Vilnius University Institute of Mathematics and Informatics, Technological Sciences, Informatics Engineering – 07T),

Prof Habil Dr Rimantas ŠEINAUSKAS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).

Opponents:

Assoc Prof Dr Arnas KAČENIAUSKAS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T),

Prof Dr Habil Vincas LAURUTIS (Siauliai University, Technological Sciences, Electrical and Electronics Engineering – 01T).

The dissertation will be defended at the public meeting of the Council of Scientific Field of Informatics Engineering in the Senate Hall of Vilnius Gediminas Technical University at 2 p. m. on 30 January 2013.

Address: Saulėtekio al. 11, LT-10223 Vilnius, Lithuania.

Tel.: +370 5 274 4952, +370 5 274 4956; fax +370 5 270 0112;

e-mail: doktor@vgtu.lt

The summary of the doctoral dissertation was distributed on 28 December, 2012.

A copy of the doctoral dissertation is available for review at the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, LT-10223 Vilnius, Lithuania) and at the Library of Vilnius University Institute of Mathematics and Informatics (Akademijos g. 4, LT-08663 Vilnius, Lithuania).

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Lukas RADVILAVIČIUS

REALIOJO LAIKO SKENAVIMO ANTIVIRUSINIŲ SISTEMŲ NAŠUMO CHARAKTERISTIKŲ TYRIMAS

DAKTARO DISERTACIJA

TECHNOLOGIJOS MOKSLAI,
INFORMATIKOS INŽINERIJA (07T)



LEIDYKLA
Vilnius TECHNIKA 2012

Disertacija rengta 2008–2012 metais Vilniaus Gedimino technikos universitete.
Mokslinis vadovas:

prof. habil. dr. Antanas ČENYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Disertacija ginama Vilniaus Gedimino technikos universiteto Informatikos inžinerijos mokslo krypties taryboje:

Pirmininkas:

prof. dr. Dalius NAVAKAUSKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

Nariai:

prof. habil. dr. Romualdas BAUŠYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

doc. dr. Dalius MAŽEIKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

doc. dr. Olga KURASOVA, (Vilniaus universitetas, technologijos mokslai, informatikos inžinerija – 07T),

prof. habil. dr. Rimantas ŠEINAUSKAS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Oponentai:

doc. dr. Arnas KAČENIAUSKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

prof. habil. dr. Vincas LAURUTIS (Šiaulių universitetas, technologijos mokslai, elektros ir elektronikos inžinerija – 01T).

Disertacija bus ginama viešame Informatikos inžinerijos mokslo krypties tarybos posėdyje 2013 m. sausio 30 d. 14 val. Vilniaus Gedimino technikos universiteto senato posėdžių salėje.

Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.

Tel.: (8 5) 274 4952, (8 5) 274 4956; faksas (8 5) 270 0112;

el. paštas doktor@vgtu.lt

Disertacijos santrauka išsiuntinėta 2012 m. gruodžio 28 d.

Disertaciją galima peržiūrėti Vilniaus Gedimino technikos universiteto bibliotekoje (Saulėtekio al. 14, LT-10223 Vilnius, Lietuva) ir Vilniaus universiteto Matematikos ir informatikos instituto (Akademijos g. 4, LT-08663 Vilnius, Lietuva) bibliotekose.

VGTU leidyklos „Technika“ 2110-M mokslo literatūros knyga.

Topicality of the problem

Actuality of the problem. The question of information security, e.g. confidentiality, integrity and availability in the personal computer or mobile devices remains important despite the fact it is tried to be solved since the appearance of the personal computer. By solving this task it is important to ensure the consistency between the system productivity, convenience of the users work and data security level. Anti-virus systems are crucially important for protection against malware but also they have an ever growing need for computer resources which cannot be counterbalanced by the increasing speed of computers. Anti-virus, commercial or open source software regularly or by the need tests different settings, processes and data of the user's computer. The resources of the computer (processor and memory) are used during the testing. The growing need for anti-virus systems for the computer resources is determined by the currently dominant malware detection technology based on malware signatures (scanned file analysis lasts longer according to the increase of signatures' base) and more complex functionality of the operating system. This leads that more and more files and system calls must be checked by anti-virus system. Increasing competition between the user's applied software and safety anti-virus software on computer resources when the processor time may be considered as the most crucial. This forces to look for ways to reduce the influence of security system to the users work productivity without reducing the safety level.

The task of minimizing the need of anti-virus systems for computer resources is trying to be solved by reducing the number of calls to anti-virus system. These algorithms are implemented in many commercial anti-virus systems („Kaspersky“, „Symantec“ etc.) but the operating principles of the decision-making mechanisms (what has to be scanned and what hasn't) are patented and not public. This blocks the application of non-commercial anti-virus systems and causes a need to conduct independent researches in this area.

By preparing this research it was sought for methods and techniques with the result of innovative detection technology based on a small need of device resources and perfectly adapted for mobile phones and tablet computers. After the analysis and experimental study of real malicious software, the results of research of real-time anti-virus system productivity performance were obtained.

Object of research

The problem of the research – the keep of a user's computer labor productivity when the computer is running an anti-virus program.

Aim and tasks of the work

The main goal of the research is the creation of a method that increase efficiency and bandwidth of a real-time scanning process.

These tasks are to be solved to achieve the goal:

1. To explore the scanning mechanisms of a real-time file arrangement system scanning and application capabilities: detection methods, application problems, patents, monitoring methods of the file arrangement system. To perform a technical analysis of malware.
2. To select a design method of information security systems to create a real-time scanning system architecture.
3. To create functional expert system requirements of a real-time scanning system and the Project of the system.
4. To experimentally identify and describe a typical action sequence for the work of operational system with the file system for the specified time interval.
5. To create an experimental system based on a project.
6. To experimentally evaluate the efficiency of the offered method.

Methodology of research

These methods of the research are applied to reach the goal of the work:

- The methods of comparative and literature analysis have been applied to the analysis of the principles of anti-virus systems real-time mechanisms and the operation methods of the existing malware.
- The summary method has been used to systematize the results of analysis and researches and to evaluate the significance.
- The methods of experimental research have been used for examining the performance of malware in the users' personal computers by performing the researchers of method efficiency.

Scientific novelty

The following new results of the computer science engineering were get when preparing this thesis:

The new expert system for the improvement of open-source anti-virus systems performance was proposed.

Practical value

Researches in this field help to adapt to the increasing amounts of data and their verification by the means of real-time scanning. The data about the actions

of the users during the work and the sequences of the action with the file management system were collected during the research. An expert system improving the work of real-time scanning system was composed. Experimental test results of the method suggest that the method application can significantly reduce the need of computer resources for anti-virus systems, increase the work productivity and quality of the computer users and the quality of the open-source anti-virus systems.

The obtained results can be used to develop more efficient anti-virus program for each modern computer, including the tablet and integrated devices with limited resources.

Defended propositions

The following hypotheses are formulated according to the research results:

1. Expert systems that conduct preliminary analysis of the scanned files allow increasing the productivity without the impact for the reliability of the anti-virus system.
2. An application of file arrangement system drivers is more effective than hooking of operational system functions for real time monitoring of the actions carried out with the system of the file arrangement.
3. Relational database can be used to protect and interpret the rules of expert systems.

The scope of the scientific work

The thesis consists of 3 sections, including general conclusions and recommendations, bibliography and list of publications

The volume of the thesis is 110 pages including annexes. There are used 40 pictures and 9 tables in the text. There were used 74 literature references by writing a thesis.

1. Analysis of the real-time scanning mechanisms of the existing antivirus systems

When analyzing literature sources it was found that one of the biggest threats is malware. One of the most effective means is anti-virus programs having a function of real-time scanning. These programs are divided into several main types according to the malware detection methods:

1. Based on signatures.
2. Heuristic.
3. Anomaly analysis.
4. „Sandbox“.
5. „White list“.

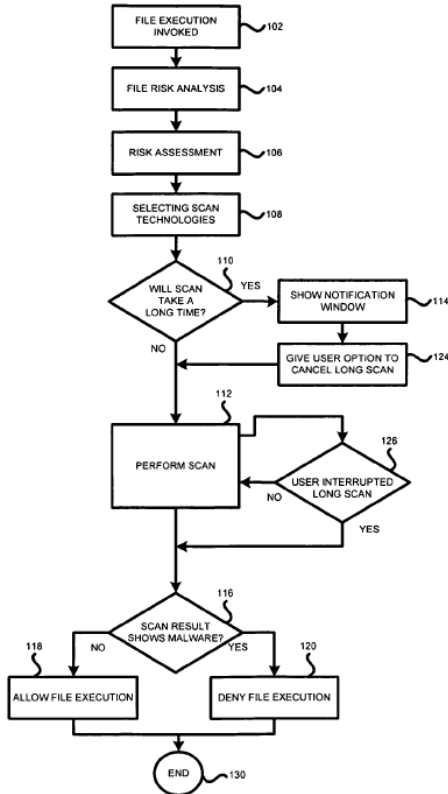


Fig. 1. Patent diagram

The vast majority of anti-virus systems with real-time scanning function are commercial. The technology of their performance is usually private and patented. The performed patent analysis provides a limited understanding about the performance of processes in commercial products. Analysis shows that many commercial products share similar problems but they do not reveal the technical details so not all of the used processes are available for the science.

Kaspersky Lab patented a method and system to scan anti-malware software in US patent. The invention registered in 2010 provides a solution to scan executable files and search for the malware. The block diagram of the invention is showed in Fig. 1. The authors argue that this invention allows reducing the scan time in balancing the fast checks (usually less detailed) with comprehensive but

slower checks. Scan query has to go through a number of processes and only then the system receives an Access authorization. Large files are evaluated separately.

The developers of anti-virus software use two basic methods of viewing: on demand and real-time (on Access). In the case of the view on demand the users voluntarily activate the program of virus scan each time when they want to check the computer.

In the case of real-time view the virus protection is activated automatically when the changes in file arrangement system and/or computer memory are recorded. Real-time file arrangement monitoring system usually analyzes the files each time the program calls the function to open or close a file.

Real-time monitoring system can detect changes in file arrangement by these main methods:

1. Acts as a program and take over the functions of file arrangement API interface.
2. Acts as a filtering driver of devices/file arrangement, which attaches to the file arrangement (FAT, NTFS etc.).

The main methods of API monitoring:

- by using SetWindowsHookEx() function;
- by using Proxy library (dll);
- by changing IAT;
- by changing the code of the program;
- by monitoring the file system.

Expert system is a program which is specially designed for modeling the application of human accumulated expert knowledge. Expert system keeps the facts and rules in such form if they are used together they can indicate new facts. Also expert system must be able to explain how these findings were obtained. The expert system uses a repository of human knowledge to solve the problem that traditionally requires the knowledge of an expert. The covered knowledge is called a knowledge domain. Knowledge representation requires more sophisticated information structure than it is available in typical databases. This happens because the information is extracted by analyzing raw data, by adding additional heuristic information.

As expert systems are designed for decision-making under the sets of rules concluded by the experts, their use is available in many information systems including the creation of anti-virus systems. Although the basic task of anti-virus system is to determine whether a particular file is infected or not, an expert system cannot answer to this in many cases. However expert system can be very useful in optimizing system performance.

Following the literature review it can be said that there is a strong basis for the coming of the new method based on efficiency increase of real-time anti-virus systems dedicated of export systems.

2. Architecture of the offered real-time scanning system

In the second chapter of the thesis the requirements and the project of proposed real-time scanning anti-virus system prototype is particularly presented. The following functional requirements are formulated and identified as necessary:

- Requirements of system architecture.
- Limits of resource usage.
- Support of real-time scanning mechanism.
- RAM scanning function.
- Specified directory or drive scanning function.

The following non-functional requirements are formulated:

- Bandwidth.
- Convenience for the user.
- Safety.
- The work of the system should not affect the normal functionality of the operating system.
- The work of the system should not affect the normal functionality of applications.

Delay time of user actions.

The Project of the proposed prototype was implemented in UMLSec language. Thesis contains diagrams of states, composite structure and activity. The figure 2 shows state diagram implemented in UMLSec language and there is status changes coupled with additional UMLSec information – stereotypes shown.

As stereotypes allow proposing much more unambiguous information about the state and its development the Project becomes much clearer and stricter. This obliges the participants of further system development to comply with the set rules.

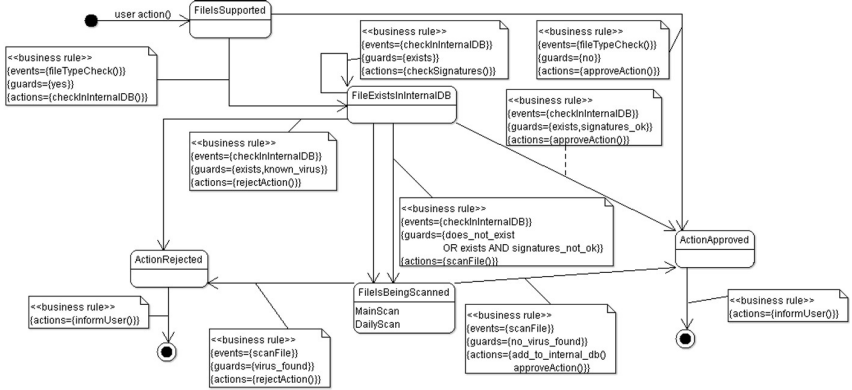


Fig. 2. System state diagram implemented in UMLSec

3. Implementation and performance analysis of the real time scanning system

The third section describes the expert system which is the basis of the created real-time scanning anti-virus program allowing optimization of real-time scanning. It also discusses laboratory conditions under which the tests with malware were carried out and users' actions were analyzed while working with computer appliances.

An expert system is one of the main and most important parts of our proposed system. It will optimize the number of user initiated queries in real-time scanning. Our proposed expert system is assigned to the category of expert systems based on rules which basis and essence is composed of the set of rules constituted by an expert. Also some of the database is required for the storage of internal data and signatures used in ClamAV engine.

Main signature DB – a database provided by ClamAV anti-virus – the biggest malware database from ClamAV. It is being updated few times per year when all signatures from daily.cvd is moved to main.cvd database.

Daily signature DB – this ClamAV database contains newest malware signatures and is updated many times per day. Every few months all content of daily.cvd is moved to main.cvd.

File extension DB – it is the presented method's internal database which keeps extensions of files which should be scanned or not.

Standard file DB – database keeps standard operating system's files' checksums that are marked as trusted and should be never scanned.

Internal hash DB – for antivirus not to do the same job twice, the checksum of all scanned files is kept.

Most used files DB – as users' behavior is analyzed and most used files are stored, there must exist a database to store it.

A rule based method consists of a number of rules. They allow obtaining the required result – to decide what to scan. Each file has to go through all the rules as shown in figure 3 to allow access to a file or check it with the signature databases.

File extension in extensions DB?” – this rule is one of the most important – once it decides the file should be scanned according to its extension.

“File size good for scan?” – rule is based on file size. Method decides to allow access to file according to files' size. “File located in standard file DB” – as all operating systems, as well as applications (like Microsoft Office) and services (e.g. database servers) has standard files that are compiled and linked by their producers, they can be marked as trusted and not scanned every time.

“File located in internal DB” – rule checks if the file was scanned before and with which signature database version “File scanned with newest Signature Dbs?” – as it is clear by now, that file has to be scanned, now it is very important to find out was it scanned with current version of virus signatures databases. In case it was – we can simply allow access to file without wasting expensive time to scan it again.

“File scanned with newest Main signature DB?” – If file was not scanned with newest virus signatures databases, it is even more important to determine if it was scanned with Main signature database. Principled scheme of the method is shown in figure 3. There are few features that were the most important in the design and creation of the system. One of them is the reduction of the resources exploitation. The other is a real-time scanning options correction which prevents the computer from malicious code infection.

This section also describes the creation of real-time scanning anti-virus system prototype. It consists of a software service which is implemented as the part of expert system decision-making. There is also a prototype with the user interface and operating systems module sequences takeover created

Information relevant to the user is shown in the main window. Primarily the virus database information is presented (in the group *DCAntiVirus Database info*). The window shows the numbers of the main and daily database, the dates and the available number of signatures. There is a button at the bottom of a group for the updating the databases.

The group *DCAntiVirus Scan info* shows the scanning information: service status, number of good files in the internal database, the last file scanned and the scan result. If the file has been infected the result field displays the name of the virus.

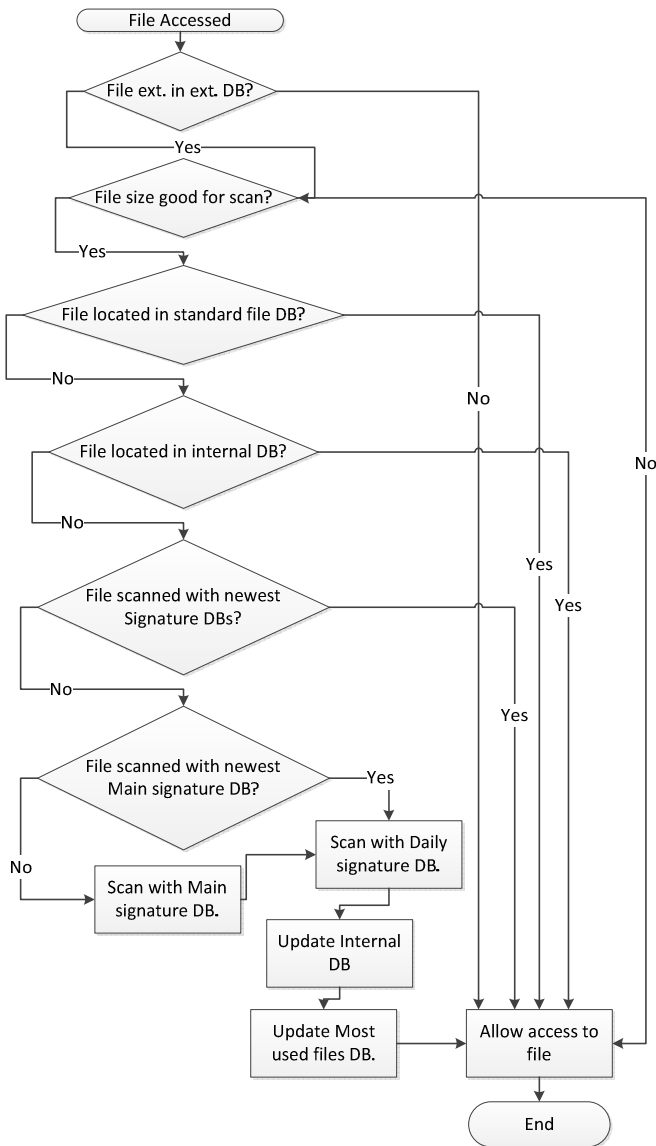


Fig. 3. Scheme of expert system

A virtual security laboratory Tele-Lab has been applied for the experiments with the malware and created prototype. It allowed safely and effectively carry out the tests without any danger to the real users and systems. The basis of a laboratory is consisted of a virtual machines and the platform of their management. Virtual machines are run via remote access. Virtual machine is a software system that provides action environment for the operating systems. Such computer systems emulated by the software are easily restored or transferred if there is an error or the failure.

For a future increase of scalability of this solution, the introduction of security tokens for the access to the middleware services is considered.

After implementing Tele-Lab in Vilnius Gediminas technical university, extended testing of virtual servers and working methods were applied. One of the most important tasks were to try and adapt Tele-Lab platform not only for learning tasks, but also for expanded usage.

One of the most important issues for the real-time scanner is to protect the user from the current data stream from the network. Preliminary scheme of 3 virtual machines is visualised in figure 7. Victim computer with windows XP operating system and implemented real-time rule-based antivirus system is marked number 1. It is monitoring the data stream coming from the local network. In the same team – two attacking computers are placed (marked numbers 2 and 3 accordingly in figure 4).

Attacker computers are prepared with dynamic IP addresses, thus everytime they tries to talk with the victim machine, their IP address differs and in such way the bigger network model is simulated. This is done because of the limitations in Tele-Lab where teams can be formed from only limited number of computers. Attacker initiate the connection with the victim machine and tries to send malicious code to the victim. Malicious code that is being sent to the victim system is taken from the 0 day clamAV antivirus database (at the testing day).

After every initiated connection, attacker's system changes the IP address, removes the attempted malicious code from the list and waits for 30 seconds for the next attempt to connect to the victim machine.

In the simplified log view of rule-based real-time antivirus system, it is possible to check the efficiency and speed of the antivirus system and the workload of the victim machine. The workload and antivirus system efficiency is very similar to the real-world numbers on almost identical systems (as shown in figure 5) thus allowing to use Tele-Lab platform to be used for various automated software checks and expanding its capabilities as a virtualized working platform.

As the bandwidth is very important to the real-time system it was necessary to select all of its parts that may cause as low as possible delays. A series of tests were conducted with the possible components of the system.

Detours library intercepts functions overwriting calling tables of processes. For every function, library rewrites two functions. Detours library can take over any function of any library.

Easyhook library supports interception of unmanaged source code while using managed code. It assures that no garbage of resources or memory are left in intercepted program. It is also able to use handlers to take over uncontrolled API functions.

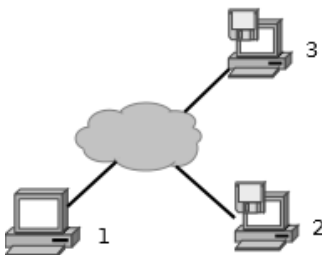


Fig. 4. Scheme of the testing environment architecture

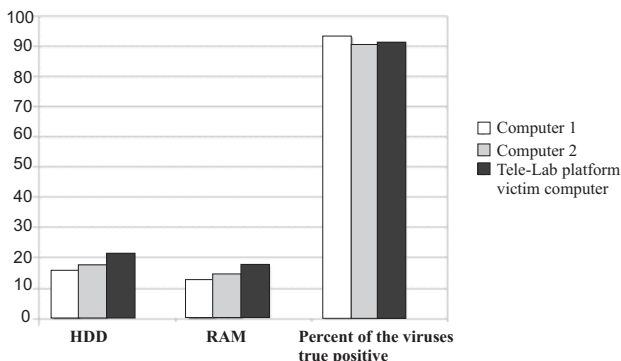


Fig. 5. Comparison of system load and efficiency (HDD, RAM checked with HWMonitor)

One of the prioritized qualities of our proposed method is speed thus these tests are very important when deciding which library to choose. The correct choice of library influences the overall speed of the system.

For each of the libraries, programs-servers were coded. They support command line format. Programs does not perform any tasks so that time of tasks wouldn't influence the time. *Run* – application is loaded and waiting while

new process will be finished. *Hook* – one of the libraries are inserted and takes over call of function *CreateFile*.

From figure 2 it is clearly seen that when the program is started with EasyHook, it does it slower (142.27%). Next figure shows library work test. It can be seen that Detours library didn't have any effect on running time while EasyHook shows once again worse results. It was slower 305%.

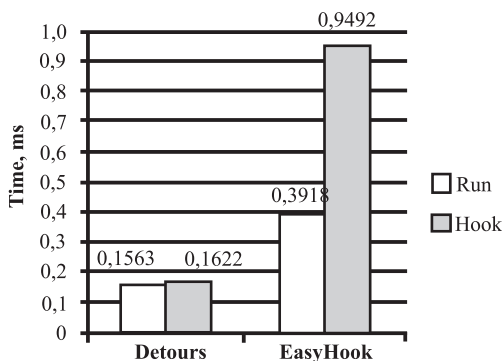


Fig. 6. Time of library loading

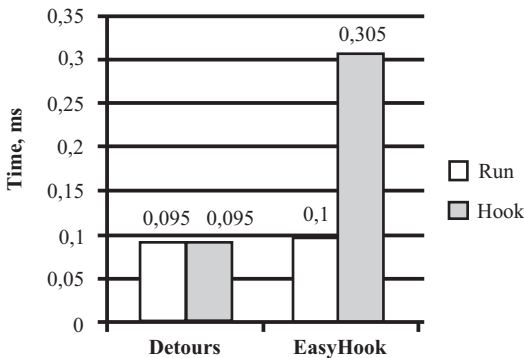


Fig. 7. Libraries work test

It was decided to use the freely available Clam AntiVirus (ClamAV) scanner as the foundation for our real-time rule based anti-virus engine for desktop users. ClamAV consists of a core scanner library as well as various command line programs, but it does not have any real-time scanning method. So, we modified the ClamAV scanner library for use with our service and real-time protection.

ClamAV Virus Database as of February 2011 consisted of 879 500 signatures. The ClamAV virus definition database contains two types of virus patterns: (1) basic patterns formed of simple sequence of characters that identify a virus, and (2) multi-part patterns that consist of more than one basic sub-pattern. To match a virus, all sub-patterns of a multi-part pattern must match in order. ClamAV virus patterns can also contain wildcard (*) characters. The combination of multi-part patterns and wildcard characters allows ClamAV to detect polymorphic viruses. Polymorphic viruses are more difficult to detect than non-polymorphic viruses, because each instance of a virus has a different footprint from other instances.

Internal database ensures that once tested and clean file will not be tested for the second time. At first it is necessary to calculate the checksum of the file. There are a lot of methods to do that. However it should be chosen the fastest one, otherwise the opening of the file may linger not only because of the reading but also because of the calculating of the checksum. The test showed that MD5 algorithm counted the checksum the fastest. Of course the speed of all algorithms reduced when working with large files. But in all cases MD5 was three times faster than RIPEMD160 algorithm. This has led to its use for file scanning model.

Table 1. Test results of hash function usage. Time is presented in seconds

The checksum method	File size, MB		
	76.607	8.068	0.754
MD5	0.30	0.03	0.0025
SHA256	1.67	0.17	0.017
RIPEMD160	0.87	0.09	0.009

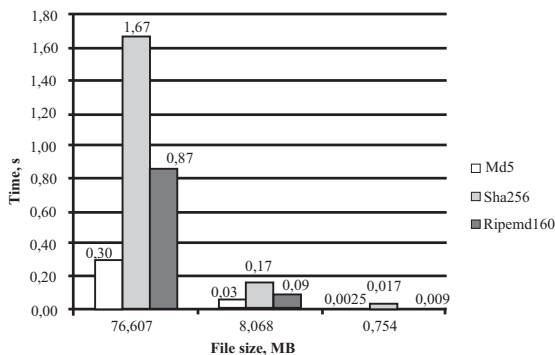


Fig. 8. Test results of hash function usage

The chapter ends with the created prototype results verification in experimental way. The tests showed the efficiency of the tasks of each expert system in percentage.

Table 2. Experimental results of rule based expert system

No.	Name of the rule	Total number of events	Number of events for checking	Decrease of events in percentage
1	Standard file database	1 020 411	524 381	48.61
2	File extension database	1 020 411	562 912	44.83
3	Internal file database	1 020 411	139 580	86.32
4	According to the file size	1 020 411	896 858	12.11
	All tasks together	1 020 411	35 788	96.49

After applying all the rules one by one (order is not important), remaining number of operations is 35 788. It is a decrease of 96.49%.

Table 2 shows that the largest impact on reducing the number of scanned actions had the rule no. 3 „Internal file database“, that reduced the scanned number in 86.32 percent. This means that repetitive scans of the same file are the most affective for the efficiency of the anti-virus system. Also the results indicate that repetitive scanning does not make sense, because application of expert system did not reduce the efficiency of anti-virus system. The worst results in reducing the number of scanned files were shown by the task no. 4 “According to the file size“. It essentially represents extremely large number of the files in the system faced by the users. The rules of application optimization are limited. However if the sum of filtered file size by the rule is compared to the sum of all the other file size (about 70 percent) we can say that despite the low number of filtered files this rule is necessary and crucially important in terms of anti-virus system resource consumption. An efficiency of rules No.1 and No.2 application can still be increased by expanding the number of database records. Given the fact that two of the four rules still have optimization opportunities it can be said that by improving the rules final efficiency of system application can approach to the percentage indicators enabling an application of the system in practice.

General conclusions

According to the test results it was shown the principal correctness of proposed expert system for the open-source real-time anti-virus systems performance improvement. The system may be recommended to integrate with the open-source anti-virus systems. The testes showed that after the use of these

type systems, open-source signature based anti-virus systems can be used to protect the computer from malware in real time.

The principal opportunity to preserve and interpret the rules of the expert system on the basis of relational database management system was confirmed. The proposed solution can find applications in internet technologies due to broad scale application of RDBMS and low level of online technology integration with specialized systems of expert rules storage and treatment.

An application of expert system helped to reduce the load in 96.49% and despite that any single virus from malicious software code base was noticed. A further optimization of expert system rules is possible and it would increase the system performance to an acceptable level for practical application.

It is approved that virtualized environment can fully emulate all the situations related to the spread of malware code. This environment was adapted to model the attacks of network malware code.

List of published works on the topic of the dissertation in the reviewed scientific periodical publications

Čenys, A.; Normantas, A.; Radvilavičius, L. 2009. Designing role-based access control policies with UML, *Journal of Engineering Science and Technology Review* 2(1): 48–50. ISSN 1791-2377.

Radvilavičius, L.; Čeponis, D. 2011. Window API funkcijų sekų perėmimo bibliotekų tyrimas, *Mokslas – Lietuvos ateitis* 3(1): 15–19. ISSN 2029-2341.

Radvilavičius, L.; Marozas, L.; Čenys, A. 2012. Overview of real-time antivirus scanning engines, *Journal of Engineering Science and Technology Review* 5(1): 63–71. ISSN 1791-2377.

In the other editions

Willems, Ch.; Klingbeil, Th.; Radvilavičius, L.; Čenys, A. 2011. A distributed virtual laboratory architecture for cybersecurity training, in *Proceedings 6th International Conference on Internet Technology and Secured Transactions (ICITST-2011)*, 11–14 December 2011, Abu Dhabi, United Arab Emirates. Abu Dhabi: IEEE, p. 408–415. ISBN 9781908320001. Prieiga per internetą:
<<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6148474>>.

Radvilavičius, L.; Talmontienė, J. 2012. Antivirusinių programų failinės sistemos stebėjimo realiu laiku metodų tyrimas, *Jaunųjų mokslininkų darbai* 3(36): 116–122.

About the author

Lukas Radvilavicius was born in Vilnius, on 3 of January 1982.

First degree in Informatics Engineering, from Faculty of Fundamental Sciences, Vilnius Gediminas Technical University (VGTU), 2004.

Master of Science in Informatics Engineering, from Faculty of Fundamental Sciences, VGTU, 2006. Has a job experience as a CEO of IT company, teacher of informatics, FP6 and EU structural funds project coordinator.

In 2007–2011 – PhD student of VGTU. At present – researcher

At Research Laboratory of Security of Information Technologies of VGTU.

REALIOJO LAIKO SKENAVIMO ANTIVIRUSINIŲ SISTEMŲ NAŠUMO CHARAKTERISTIKŲ TYRIMAS

Problemos formulavimas ir darbo aktualumas. Informacijos saugos, t. y. konfidencialumo, vientisumo ir prieinamumo, užtikrinimo klausimas asmeniniame kompiuteryje ar mobiliuosiuose įrenginiuose išlieka aktualus nepaisant to, kad jį bandoma išspręsti nuo pat asmeninio kompiuterio atsiradimo. Sprendžiant šį uždavinį svarbu užtikrinti darną tarp sistemos našumo ir naudotojų darbo patogumo bei duomenų saugos lygio. Antivirusinės sistemos yra kritiškai svarbios apsaugai nuo kenksmingo programinio kodo (KPK), bet kartu pasižymi vis didėjančiu poreikiu kompiuterio resursams, kuris negali būti kompensuotas didėjančia kompiuterių sparta. Antivirusinė, komercinė ar atvirojo kodo programa reguliariai arba pagal poreikį tikrina skirtingus naudotojo kompiuterio nustatymus, procesus ir duomenis. Tikrinant naudojami kompiuterio resursai – procesorius, operatyvioji atmintis. Didėjančių antivirusių sistemų poreikį kompiuterio resursams lemia šiuo metu dominuojanti KPK aptikimo technologija, paremta KPK parašais (didėjant parašų bazei ilgiau trunka skenuojamų bylų analizė), taip pat sudėtingėjantis operacinių sistemų funkcionalumas.

Rengiant disertaciją buvo ieškoma metodų ir būdų, kurių rezultatas – naujoji aptikimo technologija, grindžiama mažų įrenginio resursų poreikiu, būtų puikiai pritaikoma mobiliesiems telefonams ir planšetiniams kompiuteriams. Atlikus analizę ir eksperimentinius tyrimus su realia kenksminga programine įranga, gauti realiojo laiko antivirusinių sistemų našumo charakteristikų tyrimų rezultatai.

Tiriamoji problema – naudotojo kompiuterio darbo našumo išlaikymas tuo metu, kai kompiuteryje veikia antivirusinė programa.

Tyrimų šioje srityje aktualumą taip pat pagrindžia daugelis publikacijų moksliniuose žurnaluose, kurių autoriai akcentuoja šiame darbe nagrinėjamos temos aktualumą.

Tyrimo objektas. Disertacijos tyrimo objektas – realiojo laiko antivirusinių programų darbo efektyvumo tyrimas.

Darbo tikslas ir uždaviniai. Darbo tikslas yra metodo, padidinančio realiojo laiko skenavimo proceso efektyvumą ir greitaveiką, sukūrimas.

Darbo tikslui pasiekti reikia išspręsti šiuos uždavinius:

1. Ištirti esamus realiojo laiko failų išdėstymo sistemos skenavimo mechanizmus ir jų taikymo galimybes: aptikimo metodus, taikymo problemas, patentus, failų išdėstymo sistemos stebėjimų metodus. Atlikti techninę KPK analizę.
2. Pasirinkti informacijos saugos sistemų projektavimo metodą realiojo laiko skenavimo sistemos architektūrai kurti.
3. Sukurti realiojo laiko skenavimo sistemos funkcinius eksperimentinės sistemos reikalavimus ir sistemos projektą.
4. Eksperimentiškai nustatyti ir aprašyti tipinę operacinės sistemos darbo su failų sistema veiksmų seką nustatytam laiko intervalui.
5. Remiantis projektu sukurti eksperimentinę sistemą.
6. Eksperimentiškai įvertinti pasiūlyto metodo efektyvumą.

Tyrimo metodika. Darbo tikslui pasiekti taikomi šie tyrimo metodai:

- Lyginamosios analizės ir literatūros analizės metodai buvo taikomi analizuojant antivirusinių sistemų realiojo laiko mechanizmų principus, esamų kenkėjiškų programų veikimo metodus.
- Apibendrinimas – analizės ir tyrimų rezultatų susisteminimas bei reikšmingumo nustatymas.
- Eksperimentinio tyrimo metodai buvo taikomi nagrinėjant KPK veikimą vartotojų asmeniniuose kompiuteriuose, vykdant metodo efektyvumo bandymus.

Mokslinis naujumas. Rengiant disertaciją, gauti šie informatikos inžinerijos mokslui nauji rezultatai:

1. Pasiūlyta nauja eksperimentinė sistema, skirta atvirojo kodo antivirusinių sistemų našumo charakteristikų didinimui.
2. KPK tyrimams pritaikyta virtualizuota saugumo laboratorija su galimybėmis testuoti KPK lokaliuose ir nutolusiose tarnybinėse stotyse.

Darbo rezultatų praktinė reikšmė. Šios srities tyrimai padeda prisitaikyti prie didėjančių duomenų kiekių ir jų tikrinimo realiojo laiko skenavimo priemonėmis. Tyrimų metu buvo surinkti duomenys apie vartotojų darbo metu atliekamus veiksmus ir jų sekas su bylų valdymo sistema, sudaryta eksperimentinė sistema, leidžianti optimizuoti realiojo laiko skenavimo sistemų darbą. Ekspe-

rimentiniai metodo bandymų rezultatai leidžia teigti, kad metodo taikymas gali labai sumažinti antivirusinių sistemų poreikį kompiuteriniams resursams, padidinti kompiuterių naudotojų darbo našumą ir kokybę, pagerinti nekomercinių, taip pat atvirojo kodo antivirusinių sistemų kokybę.

Gauti tyrimų rezultatai gali būti naudojami kuriant optimizuotas antivirusines programas kiekvienam šiuolaikiniam kompiuteriui, įskaitant ribotus resursus turinčius planšetinius ir integruotus įrenginius.

Ginamieji teiginiai. Remiantis tyrimų rezultatais suformuluoti šie ginamieji teiginiai:

1. Ekspertinės sistemos, atliekančios išankstinę skenuojamų failų analizę, leidžia padidinti AV našumą be poveikio antivirusinės sistemos patikimumui.
2. Failų išdėstymo sistemos tvarkyklių taikymas yra efektyvesnis už operacinės sistemos funkcijų perėmimą (angl. hooking), norint realiuoju laiku stebėti veiksmus, atliekamus su failų išdėstymo sistema.
3. Reliacinė duomenų bazė gali būti naudojama ekspertinių sistemų taisyklės saugoti ir interpretuoti.

Disertaciją sudaro įvadas, 3 skyriai, bendrosios išvados ir rekomendacijos, literatūros sąrašas ir publikacijų sąrašas.

Darbo apimtis – 110 puslapių, įskaitant priedus, tekste panaudoti 40 paveikslų ir 9 lentelės. Rašant disertaciją buvo panaudoti 74 literatūros šaltiniai.

Bendrosios išvados

Remiantis eksperimentų rezultatais, buvo parodytas principinis siūlomos ekspertinės sistemos, skirtos atvirojo kodo realiojo laiko antivirusinių sistemų charakteristikoms gerinti, principinis korektiškumas. Sistema gali būti rekomenduota integruoti su atvirojo kodo antivirusinėmis sistemomis. Atlikti bandymai parodė, kad, panaudojus tokio tipo sistemas, atvirojo kodo, parašais pagrįstas antivirusines skenavimo sistemas galima naudoti kompiuterio apsaugai nuo kenksmingo programinio kodo realiuoju laiku.

Patvirtinta principinė galimybė saugoti ir interpretuoti ekspertinės sistemos taisyklės reliacinės duomenų bazių valdymo sistemos pagrindu. Pasiūlytas sprendimas gali rasti pritaikymą interneto technologijose dėl plataus RDBVS taikymo masto ir žemo internetinių technologijų integracijos lygio su specializuotomis ekspertinių taisyklių saugojimo ir apdorojimo sistemomis.

Ekspertinės sistemos pritaikymas leido sumažinti apkrovą 96,49 % ir nepaisant to nepastebėtas nei vienas virusas iš kenksmingo programinio kodo bazės. Ekspertinės sistemos taisyklių tolimesnis optimizavimas yra įmanomas ir leistų padidinti sistemos efektyvumą iki praktiniam taikymui priimtino lygio.

Patvirtinta, kad virtualizuota aplinka gali visiškai emuliuoti visas situacijas susijusias su kenksmingo programinio kodo plitimu. Ši aplinka buvo adaptuota tinklinio kenksmingo programinio kodo atakoms modeliuoti.

Trumpos žinios apie autorių

Lukas Radvilavičius gimė 1982 m. sausio 3 d. Vilniuje. 2004 m. įgijo informatikos inžinerijos bakalauro laipsnį Vilniaus Gedimino technikos universiteto (VGTU) Fundamentinių mokslų fakultete. 2006 m. įgijo informatikos inžinerijos mokslo magistro laipsnį VGTU. Turį darbo patirties kaip IT įmonės vadovas, informatikos mokytojas, ES FP6 ir struktūrinių fondų projektų koordinatorius.

2007–2012 m. – VGTU doktorantas. Šiuo metu dirba VGTU Informacinių technologijų saugos mokslo laboratorijoje.

Lukas RADVILAVIČIUS

REAL-TIME ANTIVIRUS SCANNING METHODS
CHARACTERISTICS' EFFICIENCY STUDY

Summary of Doctoral Dissertation
Technological Sciences, Informatics Engineering (07T)

REALIOJO LAIKO SKENAVIMO ANTIVIRUSINIŲ
SISTEMŲ NAŠUMO CHARAKTERISTIKŲ TYRIMAS

Daktaro disertacijos santrauka
Technologijos mokslai, Informatikos inžinerija (07T)

2012 12 28. 1,5 sp. I. Tiražas 70 egz.
Vilniaus Gedimino technikos universiteto
leidykla „Technika“, Saulėtekio al. 11, LT-10223 Vilnius
Spausdino UAB „Ciklonas“
J. Jasinskio g. 15, 01111 Vilnius