A proposal of software project

ZeTIs - Zero Time Security

Supervisor: Mgr. Pavel Jeģek, Ph.D.

Team members:

Martin Dráb, Miroslav Chomut, Tomáģ Martinec, Zuzana Vytisková

Deadline: September 2013

Introduction

Host Intrusion Prevention Systems (HIPS) are an important part of computer security. Unlike antivirus programs, that mostly use static methods (database of signatures, static heuristic analysis) to detect dangerous applications, HIPSes take advantage of behavioural analysis performed during the execution of the application in question. Thus, they are able to detect malicious programs, currently unknown to the antiviruses, and block their activity.

There are many HIPS implementations that provide sufficient level of security on 32-bit versions of Windows. However, changes introduced in 64-bit Windows (built-in protection of kernel code and important data structures) caused that many approaches used before do not work now. Even many commercial products haven't reached sufficient level of security yet.

The goal of this project is to design and implement a rule-based HIPS.

Proactive Security Challenge 64 (PS C64) test suite (http://www.matousec.com/projects/proactive-security-challenge-64/) is planned to be used as a basic platform for inspiration of kinds of threats the system should be able to deal with and for measurement of the results. This set of tests focused on HIPSes will be analysed and the ZeTiS software should be able to pass a subset of the tests described there. The project does not aim for real coverage of the PSC 64 test, the goal is to design the system, especially the structure of the rules, strong enough to support implementation of a complete set of rules and modules to pass all the PSC 64 tests. Thus only an example rule set and modules will be developed as part of the ZeTiS project as prove of a concept.

The ZeTiS will only be a HIPS which means it should offer the behavioural analysis and basic firewall capabilities. An optional sub-goal of the project is to prepare ZeTiS for cooperation with some wide-spread antivirus available for free (e.g. Avira Free Antivirus) which can block already-known dangerous software before it is started.

The project will be divided into the following parts:

A set of kernel drivers will be provided to filter operations performed by running processes. The project will cover areas where documented interfaces are provided by the Windows kernel (file system, registry, network communication and process and thread access). However, there are other areas where no documented filtering interface is provided. One of them, the Windows graphics subsystem (implemented in win32k.sys driver), will be researched and covered in the ZeTiS project.

The kernel drivers are the most critical part of the ZeTiS project and so appropriate attention should be paid to their testing. Implementation is planned in C.

Rule Management System (RMS) will describe rules - their structure, configuration, execution and some default rules. Given a set of rules, the RMS will be able to decide whether to permit or block majority of operations on its own. The remaining cases will prompt the user for a decision and provide them with relevant information in a human understandable form. Information important for decision is for example the type of operation, which process, file or registry key is involved or arguments the application was started with. The main part of the RMS component is expected to be implemented as a user-space Windows service in a native programming language. The configuration of the rules should be accessible through the graphical interface of the HIPS.

The Graphical User Interface should provide information about the current state of the software to the user and allow them to configure the whole HIPS and view logs. System of messages that helps the user to resolve the events undecided by the rule system will be also an important part of the GUI.
The **target platforms** supported by the ZeTiS software should be at least both 64-bit and 32-bit versions of Windows 7. There are no known problems preventing the support of Windows Vista (SP1 and higher), Windows Server 2008 or Windows 8 environments, but it is not an essential part of the project.

Since thousands of actions monitored and filtered by the ZeTiS occur in the system every second, performance issues are expected and acceptable performance should be reached.