# Malware detection techniques using modern theoretical computer science

Daniel Daniš
idanis@fit.vutbr.cz

In this paper we will discuss the usability of theoretical computer science in techniques of malware detection. There are many ways and possibilities how to use the knowledge of theoretical computer science in the methods and ways of detecting malware or attacks on computer systems.

The number of malware is growing extraordinarily fast. Therefore, it is important to have efficient malware detectors. Many of these techniques of obfuscation rely on operations on the stack such as inserting dead code by adding useless push and pop instructions, or hiding calls to the operating system. In theoretical informatics, we can for example construct Pushdown System (PDS) detector that takes into account the behavior of the stack [1]. The usage of pushdown automata in various malware detection techniques is a typical example of an application of the theoretical computer science.

Slightly different approach is used in Intrusion Detection Systems (IDS). These systems are very often based on Learning Automata that detect malware using network flow data. Learning automata allow us to do detection over time and developing the threat value based on past experiences from the environment [2].

These examples and other methods and techniques for malware detection that use knowledge of modern theoretical computer science will be discussed and described closely later in this work.

## References

[1] Song, F., Touili, T.: Pushdown Model Checking for Malware Detection, Tools and Algorithms for the Construction and Analysis of Systems: 18th International Conference, Springer, March 24 – April 1, 2012

[2] Jamali, S., Jafarzadeh, P.: An intelligent intrusion detection system by using hierarchically structured learning automata, Neural Computing and Applications, Springer, 2015