Tomáš Pevný

Komořanská 2066/7•Prague, Czech Republic, 14300• Phone: +420 607 237 527
E-Mail: pevnak@gmail.com

Date: 26.06.2014

Evaluation of diploma thesis
Author: Bc. Peter Hrosso
Title: Black-Box Attack on Network Intrusion Detection Systems
Supervisor: Ing. Tomáš Pevný Ph.D.

The goal of the thesis was the study of practical methods to generate an attack invisible to a chosen detector in the sense that detector will not raise an alarm despite the attack is happening. The study has been performed in the network intrusion detection domain, where such scenarios are common. The developed tool is important for the community as it can identify potential holes in new or already deployed Intrusion Detection Systems.

The first chapter of the thesis introduces the general problem of adversarial machine learning, into which the investigated problem falls. The following chapter describes the domain of network intrusion detection in netflow data and it presents state of the art detector used for the evaluation. The chapter also introduces basic properties a practically usable detector should poses and discusses, how these properties can be utilized to implement an efficient strategy to evade detection. The third chapter shows that by using adopted assumptions the optimal invisible attack can be find by using a gradient descend method. The idea comes from the cited work published in the field of watermarking. The chapter discuses problems caused by the discrete nature of the domain and how they were circumvented. The next chapter experimentally demonstrates that the presented algorithm finds the optimal attack (reaches global maximum) and is more efficient that the brute-force search trying all combinations. Thus, the solution to the stated problem has been found. The last chapter summarizes the work and lays out a possible future work.

Overall the thesis is well written, notation is consistent, all terms were properly introduced, and all prior art cited. It can be used as a seed for a contribution to a workshop or conference, because the presented solution is novel in the domain, it is not trivial due to the aforementioned problems with discreetness, and it is an important contribution. Yet to make it a paper, some of the future work would need to be finished. I remark that some of the future work needs substantial computation resources to be done. The student has worked on the problem independently, diligently, and has demonstrated abilities to think about the problem and to find novel approaches.

With respect to the above, I recommend the grade A.

Sincerely,

Tomáš Pevný