University of Victoria | Graduate Studies

Notice of the Final Oral Examination
for the Degree of Master of Science

of

ERKAN ERSAN

BSc (University of Kocaeli, 1998)

"On the (In)security of Behavioral-Based Dynamic Anti-Malware Techniques"

Department of Computer Science

Friday, March 10, 2017
10:00 AM
Engineering and Computer Science Building
Room 468

Supervisory Committee:
Dr. Bruce Kapron, Department of Computer Science, University of Victoria (Co-Supervisor)
Dr. Lior Malka, Department of Computer Science, UVic (Co-Supervisor)

External Examiner:
Dr. Issa Traore, Department of Electrical and Computer Engineering, UVic

Chair of Oral Examination:
Dr. David Giles, Department of Economics, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies

Abstract

The Internet has become the primary vector for the delivery of malicious code in cyber attacks, and malware has rapidly become a pervasive critical threat. Antimalware products offer effective protection from malware threats for servers and endpoint devices using a variety of techniques. Advanced enterprise-level anti-malware products rely on state-of-art behavioral-based detection algorithms, in addition to traditional signature-based mechanisms. These dynamic detection techniques have been around for more than a decade and in response hackers have developed methods to evade them. However, currently known bypass methods require intensive manual labor. Moreover, this manual work has to be repeated whenever a parameter of the environment (such as the payload, operating system, Antivirus version, etc) changes, making these methods impractical. This may lead to the belief that dynamic techniques provide a good deterrence, and hence good protection.

In this thesis we evaluate dynamic techniques. Specifically, we build tools to implement generic unhooking and funneling, and using these tools we show how dynamic techniques can be bypassed with considerably less effort than by fully manual methods. We also extend the repertoire of existing bypass methods and introduce a new malicious function call technique which exploits detection techniques that monitor a limited collection of critical system functions, as well as a method for bypassing guard-page protections. We demonstrate the effectiveness of all our techniques by conducting attacks against two enterprise antivirus products. Our results lead us to conclude that that dynamic techniques do not provide sufficient protection.