A Self Organized Threat Intelligence Architecture for Intrusion Detection Systems

by

DGCP Piyasena (168255E)

A thesis submitted to University of Moratuwa in partial fulfilment of the requirements for the
Master of Computer Science, *Specialized in Security Engineering*

Department of Computer Science & Engineering
University of Moratuwa, Sri Lanka

February 2020

A Self Organized Threat Intelligence Architecture for Intrusion Detection Systems

by

DGCP Piyasena (168255E)

A thesis submitted to University of Moratuwa in partial fulfilment of the requirements for the
Master of Computer Science, *Specialized in Security Engineering*

Department of Computer Science & Engineering
University of Moratuwa, Sri Lanka

February 2020

Declaration

I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text. Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

_____ _____

DGCP Piyasena: Date

Approved by:

_____ _____

Lt Col Dr Chandana D. Gamage Date
Department of Computer Science and Engineering
University of Moratuwa

Copyright Statement

Abstract

An Intrusion Detection System (IDS) is a software application that monitor a corporate network or a computer system and flag activities which it construes to be malicious operations. The rapid and expansive growth of Internet has heightened concerns on how to protect both stored and transmitted digital information in an effective manner.

The reactive IDS will primarily detect intrusions and send out alerts. Defending the system is a secondary task, and its success depends on how early detection can occur when an intrusion is ongoing so that warnings can be sent in time. IPS, which is mainly proactive, will primarily detect vulnerabilities and take preventive measures in addition to providing the second stage functionality for an IDS but with limited knowledge and countermeasure capabilities.

As a solution to this problem, research has been conducted on an area called Automated Defense. The design of Automated Defense systems needs to be radically different from the IDS/IPS schemes as properties such as online real-time availability of all participants, use of threat intelligence schemes, availability of high computation power, etc have to be considered. Taking into consideration the context in which Threat Intelligence Architecture operates, where transaction value is very low, IDS/IPS systems need to be designed with a careful trade-off between reliability and cost of implementation.

The research presented in this thesis aims to develop a solution to the problem of providing the functionality of an IDS with an IPS capability that is highly responsive, adaptive and able to leverage the most up-to-date knowledge on dealing with threats. The main objective of the research is to combine an IDS with Threat Intelligence in a manner that can detect file creations and copying anomalies and provide the mechanisms to alert and initiate actions to take defensive measures to decrease the potential for damage from attackers.

The main objective of the research is to combine with Threat Intelligence to provide a mechanism to alert and initiate actions to take defensive measures to decrease the potential for damage.

Acknowledgements

First of all I would like to thank my supervisor Dr. Chandana Gamage whose encouragement, guidance, support, and criticism from start to the very end, allowed me to understand the objectives and challenges of a master degree thesis. I would also like to thank Dr. Shehan Perera (Project Cordinator) for extensive advice, helpful feedback, and constant support.

Furthermore, my special thanks go to Dr. Shantha Fernando who provided an excellent, supporting, innovative, and inspiring environment in which it was a pleasure to create this thesis. Last but not its a pleasure to thank all my CiTes colleagues those who helped to make my thesis in a motion. I would also like to express my sincere gratitude to Mr Tim Crothers from Vice President Security Solutions at Target Minneapolis, Minnesota for the technical expertise provided.

Finally, words alone cannot express the thanks I owe Mr. DG Piyasena my father, Mrs. Pathma Swarnalatha my mother for all the encouragement extended.

Abbreviations

IDS - Intrusion Detection Systems
IPS - Intrusion Prevention Systems
TI - Threat Intelligence
CTI - Cyber Threat Intelligence
SOC - Security Operation Center
SIEM -Security information and event management
openIOC - Open Indicators of Compromise
STIX - Structured Threat Information Expression
CybOX - Cyber Observable
CybOX - Cyber Observable
TAXII - Trusted Automated Exchange of Indicator Information
IODEF - The Incident Object Description and Exchange Format
TIE - Threat Intelligence Exchange
TISP - Threat Intelligence Sharing Platform
HTTP - Hypertext Transfer Protocol
TPM - Trusted Platform Module
VM - Virtual Machine
VME - Virual Machine Environment
VMM - Virtual Machine Monitor
NIDS - Network Based Intruder Detection Systems
HIDS - Host Based Intruder Detection Systems
PIDS - Physical Intruder Detection Systems
OSSIM - Open Source Security Information Management

Table of Contents

List of Tables

List of Figures