

جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences



INTELLIGENT INTRUSION DETECTION SYSTEM AGAINST MIRAI ATTACK

A thesis submitted in partial fulfilment of the requirements for the degree of
Master of Science in (Information/Network) Security

By:

Aziza Gherman A Al- amri

Bachelor in Information Technology

Under Supervision of:

Dr.Meryem Ammi

Submitted to:

Department of Information Security, Computer and Information Security College
Naif Arab University for Security Sciences

May 2019

Table of Contents

Abstract.....	ii
Acknowledgements.....	iii
Statement of Original Authorship.....	iv
Table of Contents.....	v
List of Abbreviations	vii
List of Figures.....	viii
List of Tables	ix
Chapter 1: Introduction	1
1.1 Overview	1
1.2 objectives.....	2
1.3 Problem statement	2
1.4 contribution.....	2
1.5 Thesis organization.....	3
Chapter 2: Background and Literature Review	5
2.1 Intrusion detection systems.....	5
2.2 Statistics of countries that adopt E-healthcare.....	6
2.3 Security Risks	9
2.4 Reaper (IoTroop) and Mirai botnet IOTAttacks.....	18
2.5 Study of recent defenses and countermeasures.....	30
2.6 Model Training	36
Chapter 3: Methodology.....	41
3.1 Methodology.....	41
3.2 Data Acquisition	42
3.3 Pre-processing	43
3.4 Model Processing.....	43
3.5 Case study.....	44
Chapter 4: Results and Discussions	47
4.1 Data assessment.....	47
4.2 Results discussion.....	47
Chapter 5: Conclusion and Future Work.....	51
5.1 Conclusion	51
5.2 Future work.....	51

References	53
Arabic Summary	57
Arabic Title	58

List of Abbreviations

Access Control Lists	ACLs
Alberta Health Services	AHS
Command-and-Control	CNC
Computed Tomography	CT
Distributed Denial-of-Service	DDoS
Electronic Health Record	HER
Electronic Medical Record	EMR
Health Information Exchange	HIE
Health information technology	HIT
Internet Data Centre	IDC
Internet of Things	IOT
Magnetic Resonance Imaging	MRI
Medical Imaging Devices	MID
Medical Practice Management	MPM
National Health Service	NHS
Personal Health Record	PHR
Practice Management System	PMS
World Health Organization	WHO

List of Figures

Figure 1: Number of countries with UHC	7
Figure 2: Timeline of country adoption of eHealth policies or strategies.....	8
Figure 3: Countries that reported employing an mHealth program, by type	8
Figure 4: Countries that reported at least one type of mHealth programmed	9
Figure 5: Information stealing	13
Figure 6: tampering man in the middle attack	15
Figure 7: A botnet attack against the virtual medical cloud environment	16
Figure 8: The cloud healthcare system responds to a botnet attack	16
Figure 9: Mirai logical infrastructure.....	19
Figure 10: Diagram of Malware Propagation Infrastructure.....	24
Figure 11: The code that generates the IP address to Mirai's code	27
Figure 12: IoTroop transfers its data to the report server.....	28
Figure 13: The security infrastructure of the virtual community	32
Figure 14: : Ixia Application.....	33
Figure 15: Exploit flowchart from radware	35
Figure 16: Random Forest Concept	35
Figure 17: Support Vector Machine Concept	38
Figure 18: Mitigation of Mirai Botnet by Data mining method	42
Figure 19: Mirai botnet simulation architecture.....	44
Figure 20: Recruiter log while searching for bots.....	45
Figure 21: Listed bots database showing records of 2 devices information	45
Figure 22: Attacker log after commands are sent to bots.....	46
Figure 23: Received packets from Bot 1 and Bot 2 on victim machine	46
Figure 24: Learning Curve of SVM.....	49
Figure 25: Learning Curve of Random Forest	49
Figure 26: Learning Curve of Gaussian Naive Bayes.....	49
Figure 27: Learning Curve of Logistic Regression.....	50

List of Tables

Table 1: The located vulnerabilities based on devices and infrastructure	27
Table 2: The arguments used as part of the HTTP GET request	28
Table 3: The key-value tuples retrieved data.....	28
Table 4: IPS Protection.....	29
Table 5: Snapshot of normal csv files showing time, source, destination, protocol, length and info.....	43
Table 6: Random Forest Confusion Matrix	48
Table 7: Logistic Regression Confusion Matrix	48
Table 8: Gaussian Naive Bayes Confusion Matrix	48
Table 9: Support Vector Machine Confusion Matrix	48