A BEHAVIORAL GAME-THEORETIC ANALYSIS OF CYBER-SECURITY SCENARIOS INVOLVING DECEPTION AND INTRUSION DETECTION SYSTEMS

a Thesis submitted by

PALVI AGGARWAL

(D14028)

for the award of the degree of Doctor of Philosophy

SCHOOL OF COMPUTING & ELECTRICAL ENGINEERING

INDIAN INSTITUTE OF TECHNOLOGY MANDI

November 14, 2018

THESIS CERTIFICATE

This is to certify that the work contained in the thesis entitled "A behavioral game-theoretic analysis of cyber-security scenarios involving deception and intrusion detection systems." being submitted by Ms. Palvi Aggarwal (Enroll. No: D14028) has been carried out under my supervision. In my opinion, the thesis has reached the standard fulfilling the requirement of regulation of the Ph.D. degree. The results embodied in this thesis have not been submitted elsewhere for the award of any degree or diploma.

November 14, 2018

Dr. Varun Dutt (Supervisor)
Assistant Professor
School of Computing and Electrical Engineering
School of Humanities and Social Sciences
Indian Institute of Technology Mandi
Kamand, Himachal Pradesh, India
Email: varun@iitmandi.ac.in

Declaration by the Research Scholar

I hereby declare that the entire work embodied in this Thesis is the result of investigations carried out by me in the ***School of Computing and Electrical Engineering***, Indian Institute of Technology Mandi, under the supervision of ***Dr. Varun Dutt***, and that it has not been submitted elsewhere for any degree or diploma. In keeping with the general practice, due acknowledgments have been made wherever the work described is based on findings of other investigators.

Place: IIT Mandi, Kamand

Date: November 14, 2018

Signature:

Name: Palvi Aggarwal

Declaration by the Research Advisor

I hereby certify that the entire work in this Thesis has been carried out by ***Palvi Aggarwal***, under my supervision in the ***School of Computing and Electrical Engineering***, Indian Institute of Technology Mandi, and that no part of it has been submitted elsewhere for any Degree or Diploma.

Signature:

Name of the Guide: Dr. Varun Dutt

Date: November 14, 2018

ABSTRACT

Cyber-attacks, i.e., the disruption of normal functioning of computers and loss of private information through malicious network events, are becoming widespread. Deception and Intrusion Detection System (IDS) could be two promising interventions to secure the network from cyber-attacks. However, little is known on how these interventions would interact with human decision-makers in the role of hackers (people who wage cyber-attacks) and analysts (people who defend networks against cyber-attacks). This thesis aims to understand the decisions of people performing as hackers and analysts in cyber-security games using both lab-based experiments and computational cognitive models. First, we experimentally investigated the role of amount and timing of deception on hacker's decisions using a deception game. Results revealed that the average proportion of cyber-attacks were lower and not-attack actions were higher when deception occurred late and its amount was high. Next, we developed and used a real-world simulation tool called HackIt to replicate our lab-based findings in the deception game. Furthermore, we conducted another experiment to investigate the role of the availability of IDS alerts and the availability of information about actions of opponents in games involving participants performing as hackers and analysts. Results revealed that the IDS availability influenced the proportion of defend actions and the information availability about opponent's actions influenced the proportion of attack actions. To understand the cognitive mechanisms that drive hackers' and analysts' decisions in the presence of deception and IDSs, we developed computational cognitive models based upon Instance-based Learning (IBL) theory, a theory of decisions made by relying upon recency and frequency of experienced information. Results from IBL model calibrated to human data in deception game revealed that hackers relied heavily upon recent information when deception occurred late and its amount was high. Furthermore, we

calibrated IBL models to human data collected in games involving IDS alerts. Results revealed that an IBL model that specifically accounted for IDS alert information in its memory structure explained the human data accurately where IDS alerts were available, and IDS was accurate or inaccurate. IBL models were also compared with the ACT-R default parameters and Nash solutions to evaluate their ability to account for hacker's and analyst's decisions across conditions that differed in the availability and accuracy of IDSs. We found that the IBL model with calibrated parameters performed more accurately compared to both ACT-R default models and Nash solutions in capturing human decisions. We highlight the implications of our results for cyber decision-making in the presence of interventions like deception and IDSs.

Keywords: *Cyber security, Cognitive modeling, Analysts, Hackers, Cyber-attacks, Intrusion Detection Systems, Honeypots, Deception, Behavioral game theory, Instance-Based Learning Theory.*

Acknowledgments

First of all, I praise and thank our Lord Almighty, merciful and ever-loving, for bestowing upon me with this research opportunity. It was His strength that manifested in me to endure hardships and succeed in this path to dissertation. There are several other important people without whom, this thesis would have been but just, mere study and I would like to dedicate my heartfelt appreciation to them all.

I am tremendously indebted to Dr. Varun Dutt, my Ph.D. advisor who instilled in me the passion for research. His dedication to work and drive to achieve goals has motivated me greatly. I would like to express my sincere gratitude for your perennial support, your expertise, invaluable guidance, constant encouragement, understanding, patience and healthy criticism.

In addition to my advisor, I would like to express my deepest appreciation for Prof. Cleotilde Gonzalez whose constant advice and guidance in my research has helped shape my thesis as it is today. I would also like to extend my gratitude to the rest of my doctoral committee: Dr. Bharat Singh Rajpurohit, Dr. Dileep A.D., Dr. Padamnabhan, and Dr. Rajendra Ray for their insightful feedback and encouragement, but also for the hard questions which incanted me to explore my research from various perspectives.

My sincere thanks to Prof. Timothy Gonsalves, Director of IIT Mandi and other faculty members of IIT Mandi who helped me gain thorough knowledge of different courses. These courses have helped me immensely in widening my horizon not only in my area of expertise but others as well. My brain is proactively inquisitive now.

I thank my fellow lab members from ACS Lab, Indian Institute of Technology Mandi (Debarati Bandyopadhyay, Neha Sharma, Medha Kumar, Zahid Maqbool, Shruti Kaushik, Abhinav Chaudhry, Akash Rao, Pratik Chaturvedi), for keeping me engaged in challenging

research debates and also for making lab time lively in the last three years. You guys made work interesting.

Nothing is complete without friends, and so was my research here in IIT Mandi. Thank you - Akansha, Merlin, Shaifu, Shilpa, Jyoti Nigam, Indu, Shivani, Krati, Krishan and Pavin Samuel for making my life so easy and at home. A special mention to Dr. Chandan, Dr. Neha and the other medical unit staff for helping in my bad times.

I am grateful to my grandmother, my parents Mrs. Renu Gupta and Mr. Mohan Lal, and my siblings (Anu and Tushar) for providing me moral and emotional support throughout my life. I am grateful to my backbone and my husband Mr. Kuldeep Singh for showing faith in me and believing in me when I needed it the most. I am also grateful to my other family members who have supported me all along.

Lastly, a very special gratitude goes out to everyone at Ministry of Electronics and Information Technology, India and IIT Mandi for providing me with the funding for my research work.

PALVI AGGARWAL

TABLE OF CONTENTS