Dynamic Game-Theoretic Models to Determine the Value of Intrusion Detection Systems in the Face of Uncertainty

David Paul Moured
Nova Southeastern University, dmoured@gmail.com

This document is a product of extensive research conducted at the Nova Southeastern University College of Engineering and Computing. For more information on research and degree programs at the NSU College of Engineering and Computing, please click here.

Follow this and additional works at: http://nsuworks.nova.edu/gscis_etd

Part of the Information Security Commons, and the Theory and Algorithms Commons

Share Feedback About This Item

NSUWorks Citation

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.
Dynamic Game-Theoretic Models to Determine the Value of Intrusion Detection Systems in the Face of Uncertainty

by

David Paul Moured

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University
2015
We hereby certify that this dissertation, submitted by David Moured, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Sumitra Mukherjee, Ph.D.  
Chairperson of Dissertation Committee  

Michael J. Laszlo, Ph.D.  
Dissertation Committee Member  

Peixiang Liu, Ph.D.  
Dissertation Committee Member  

Approved:

Eric S. Ackerman, Ph.D.  
Dean, Graduate School of Computer and Information Sciences  

Graduate School of Computer and Information Sciences  
Nova Southeastern University  

2015
Firms lose millions of dollars every year to cyber-attacks and the risk to these companies is growing exponentially. The threat to monetary and intellectual property has made Information Technology (IT) security management a critical challenge to firms. Security devices, including Intrusion Detections Systems (IDS), are commonly used to help protect these firms from malicious users by identifying the presence of malicious network traffic. However, the actual value of these devices remains uncertain among the IT security community because of the costs associated with the implementation of different monitoring strategies that determine when to inspect potentially malicious traffic and the costs associated with false positive and negative errors. Game theoretic models have proven effective for determining the value of these devices under several conditions where firms and users are modeled as players. However, these models assume that both the firm and attacker have complete information about their opponent and lack the ability to account for more realistic situations where players have incomplete information regarding their opponent’s payoffs. The proposed research develops an enhanced model that can be used for strategic decision making in IT security management where the firm is uncertain about the user’s utility of intrusion. By using Harsanyi Transformation Analysis, the model provides the IT security research community with valuable insight into the value of IDS when the firm is uncertain of the incentives and payoffs available to users choosing to hack. Specifically, this dissertation considers two possible types of users with different utility for intrusion to gain further insights about the players’ strategies. The firm’s optimal strategy is to start the game with the expected value of the user’s utility as an estimate. Under this strategy, the firm can determine the user’s utility with certainty within one iteration of the game. After the first iteration, the game may be analyzed as a game of perfect information.
Acknowledgements

I would like to express my deepest appreciation and gratitude to my advisor, Dr. Sumitra Mukherjee, for his patient guidance and mentorship as I pursued my final degree. I am truly fortunate to have had the opportunity to work with him. I would also like to thank my committee members, Dr. Michael Laszlo and Peixiang Liu, for their guidance and thought provoking suggestions. I must thank my mentor, Joshua Combs, for the many hours he spent working with me on the topics of Game Theory and Bayesian analysis. And finally, I would like to thank all of my family and friends for their support throughout this journey.
# Table of Contents

**Abstract** iii  
**List of Tables** vii  
**List of Figures** vii  

**Chapters**

1. **Introduction** 1  
   Background 1  
   Problem Statement 6  
   Dissertation Goal 8  
   Research Questions 10  
   Relevance and Significance 12  
   Barriers and Issues 15  
   Assumptions, Limitations, and Delimitations 17  
   Definition of Terms 17  
   Summary 19  

2. **Review of the Literature** 21  
   Inspiring Literature 21  
   Inspection Games 24  
   Security Investing 25  
   Network Security Games 26  
   Bayesian Games 27  
   Comparative Static Analysis 31  

3. **Methodology** 33  
   Overview of Research Methodology 33  
   Specific Research Methodology 34  
     *Step 1. Define the game’s parameters* 35  
     *Step 2. Harsanyi transformation analysis* 40  
     *Step 3. Compute the Bayesian Nash equilibrium for the proposed models* 46  
     *Step 4. Mixed strategy profile under Nash equilibrium for the No-IDS case* 46  
     *Step 5. Mixed strategy profile under Nash equilibrium for the IDS case* 47  
     *Step 6. Comparison of the IDS and No-IDS cases* 48  
     *Step 7. The default configuration case* 48  
     *Step 8. Optimal configuration* 49  
     *Step 9. Validate previous findings* 50  
   Format for Presenting Results 50  
   Resources 51  
   Summary 51  

4. **Results** 53
Model Analysis 53
Nash Equilibrium, No-IDS Case 54
Nash Equilibrium, IDS Case 59
Comparison of IDS and No-IDS Cases 69
Value of Default Configuration 72
Value of Optimal Configuration 74
Achieving Nash Equilibrium 77
Summary 80

5. Conclusions, Implications, Recommendations, and Summary 83
   Conclusions 83
   Implications 88
   Recommendations 90
   Summary 93

References 99
List of Tables

Tables

1. IDS Case Game in Normal Form with Complete Information 3
2. Model Parameters and Strategic Variables 4
3. Definition of Terms 18
4. Propositions, Cavusoglu et al. (2005) 23
5. Bayesian Model Parameters 36
6. Utility Functions for the Proposed Bayesian Game, No-IDS Case 42
7. Utility Functions for the Proposed Bayesian Game, IDS Case 45
8. Comparison of Mixed Strategy Profiles for the No-IDS Case 57
9. Comparison of Mixed Strategy Profiles for the IDS Case 63
10. Comparing Operating Regions 64
11. Effects of Implementing IDS 71
12. The Default Configuration Case 73
13. Value of Optimal Configuration 76
14. Conditions Having the Most Effect on the Value of IDS 85
List of Figures

Figures

1. IDS case in extensive form  6
2. Normal form games, No-IDS Case  37
3. Normal form games, IDS Case 39
4. Harsanyi Transformation of the No-IDS Case  41
5. Harsanyi Transformation of the IDS Case  43
Chapter 1

Introduction

Background

Companies lose millions of dollars every year to cyber-attacks and the risk to these companies is growing exponentially. This loss of funds, and intellectual property, has made Information Technology (IT) security management a huge challenge for companies looking to defend against hackers. Therefore, methods of effectively increasing a firm’s level of network security and minimizing the damage from cyber-attacks has become a popular area of research. Firewalls have been the traditional method of protection, focusing on stopping malicious traffic as it enters or leaves the network. However, emerging security issues cannot be fully addressed by classical approaches like policing. This results in a perpetual struggle between attackers who aim to intrude the deployed systems, and the security administrators trying to protect them (Alpcan & Basar, 2003).

Many companies are increasing their security budget to cope with the recent trend of security breaches; and equally, managers are approaching investments in security measures using decision-theoretic risk management techniques (Cavusoglu, Raghunathan, & Yue, 2008). Intrusion Detection Systems (IDS) have been adopted as an additional layer of security because of their ability to monitor the internal network for
malicious traffic that has already bypassed firewall security or originates from legitimate network users. The actual value of these devices remains uncertain because they often produce a high volume of security alarms requiring manual investigation by security administrators, which can become very costly. Corporations make IT security investment decisions based on the perceived value of their security devices in an attempt to mitigate risks so that the marginal cost of implementing controls is equal to or less than the value of savings from security incidents (Cavusoglu, Mishra, & Raghunathan, 2004). No IDS is perfect in the sense that even when an IDS is implemented, alarms can be triggered for both malicious and normal network traffic, and intrusions can go undetected without triggering an alarm.

Game theory has been an integral part of artificial intelligence (AI), e-commerce, networking, and other areas of computer science and is routinely featured in the field’s leading journals and conferences because of its application in the analysis and design of systems that span multiple entities with their own information and interests (Shoham, 2008). Cavusoglu, Mishra, and Raghunathan (2005) conducted research utilizing game theory as a tool for better understanding the value of an IDS by modeling the firm and hacker as players in an Inspection game and deriving optimal strategies under Nash equilibrium. They also demonstrated that the user’s utility of intrusion ($\mu$), hacking penalty for detection ($\beta$), and the probability of detection ($P_D$) play the most significant role in determining the optimal configuration of the IDS. Their research is the motivation behind this research proposal.
Table 1 presents the game-theoretic model presented by Cavusoglu et al., (2005) in its strategic (normal) form. The payoffs available to the firm and user correspond to the left and right element of each payoff cell respectively and are separated by a comma. The user chooses the strategy that maximizes their payoff which is calculated using the \( \mu \), \( \beta \), and \( P_D \) parameters. The firm chooses the strategy that minimizes its cost which is calculated using the probability of a false alarm \( (P_F) \), the cost of manual investigation \( (c) \), the damage from an undetected intrusion \( (d) \), the fraction of damage recovered from detecting an intrusion \( (\phi) \), and the probability of detection \( (P_D) \).

### Table 1

**IDS Case in Normal Form with Complete Information**

<table>
<thead>
<tr>
<th>Firm</th>
<th>User (H)</th>
<th>User (NH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I,I</td>
<td>((c + (1 - \phi)d, \mu - \beta))</td>
<td>((c, 0))</td>
</tr>
<tr>
<td>I,NI</td>
<td>((c + (1 - \phi)d)P_D + d(1 - P_D), \mu - P_D\beta)</td>
<td>((cP_F, 0))</td>
</tr>
<tr>
<td>NI,I</td>
<td>((dP_D + (c + (1 - \phi)d)(1 - P_D), \mu - (1 - P_D)\beta)</td>
<td>((c(1 - P_F), 0))</td>
</tr>
<tr>
<td>NI,NI</td>
<td>((d, \mu))</td>
<td>((0, 0))</td>
</tr>
</tbody>
</table>

The user’s hacking strategies are to hack (H) or not hack (NH) and the firm’s monitoring strategy is to either inspect (I) a user’s traffic or not inspect (NI) network traffic based on whether the IDS raises an alarm. The firm’s strategy space is the
Cartesian Product of the actions available at each of the information sets expressed $S_F \in \{(I,I), (I,NI), (NI,I), (NI,NI)\}$. The first element in each pair is the firm’s action (inspect or not inspect a user’s network traffic) when the IDS produces an alarm. The second element corresponds to their actions when no alarm is produced. The model’s most relevant parameters are listed in Table 2.

Table 2

*Model Parameters and Strategic Variables*

<table>
<thead>
<tr>
<th>Parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$d$</td>
<td>Damage caused by an undetected intrusion</td>
</tr>
<tr>
<td>$c$</td>
<td>Cost of manual investigation</td>
</tr>
<tr>
<td>$\mu$</td>
<td>Utility of intrusion for users</td>
</tr>
<tr>
<td>$P_d$</td>
<td>Probability of getting an alarm from IDS for an intrusion</td>
</tr>
<tr>
<td>$P_f$</td>
<td>Probability of getting an alarm from IDS for no intrusion</td>
</tr>
<tr>
<td>$\phi$</td>
<td>Fraction of damage prevented or recovered by the firm when an intrusion is detected</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Hacker Penalty for Detection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strategic variables</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$\psi$</td>
<td>Probability of intrusion by a user</td>
</tr>
<tr>
<td>$\rho$</td>
<td>Probability of manual investigation when there is no IDS</td>
</tr>
<tr>
<td>$\rho_1$</td>
<td>Probability of manual investigation when the IDS generates an alarm</td>
</tr>
<tr>
<td>$\rho_2$</td>
<td>Probability of manual investigation when the IDS does not generate</td>
</tr>
</tbody>
</table>

The interactive behavior between a hacker and defender is similar to information warfare, and the process of attack and defense can be abstracted as a tree diagram (Lin,
An extensive-form game is a game specification in tree format giving insight into several of the game’s aspects. Extensive-form games are often used to model games of incomplete information, which is a game where at least one participant cannot determine the payoffs of another opponent (Qingkui & Xianxin, 2008). The game tree details the sequencing of the player’s possible moves, their choices at every decision point, the information (or lack of information) each player has about their opponent, and the payoffs for all outcomes. An extensive-form game models a finite set of rational players, a rooted tree (game tree), and terminal leaf nodes defining one payoff for each player at the end of every possible play.

The game’s structure and its parameters mentioned above are common knowledge to all of the game’s players. Game play begins at the root node and players navigate through the game tree deciding which action to take at each non-terminal node along the way until a terminal node is reached. Figure 1 depicts the game presented in Table 1 in its extensive-form. The terminal nodes on the far right give the payoffs for each of the game’s potential outcomes. For example, if the firm chooses to inspect all traffic (I, I) and the user chooses to hack (H), the firm would incur a cost of \( c + (1 - \phi)d \) and the user would receive \( \mu - \beta \) as their payoff.
Problem Statement

Analyzing security investment and implementing a cost effective security plan requires modeling the tradeoff between attack and defense and determining the value of an IDS. This is extremely difficult because of the numerous costs associated with the different configuration and inspection strategies available for deployment (Lin et al., 2009; Cavusoglu et al., 2005; Zonouz, Joshi, & Sanders, 2010). According to Zonouz et al., 2010, there are two important problems that have practical implications on a firm’s ability to implement a cost effective security policy: balancing the coverage benefits of

Figure 1. IDS case in extensive form

\[
\begin{align*}
F_1 & \quad \rightarrow \quad (c + (1 - \phi) d, \mu - \beta) \\
I, I & \quad \rightarrow \quad ((c + (1 - \phi)d)P_D + d(1 - P_D), \mu - P_D \beta) \\
I, NI & \quad \rightarrow \quad (d, \mu) \\
NI, I & \quad \rightarrow \quad (c, 0) \\
NI, NI & \quad \rightarrow \quad (c P_D, 0) \\
\quad \rightarrow \quad (c(1 - P_D), 0) \\
\quad \rightarrow \quad (0, 0)
\end{align*}
\]
an IDS against the performance costs associated with the resources they consume, and the
cross-validation burden associated with investigating false alarms. The problem is
further complicated because firms are often unsure about the user’s utility of intrusion
and lack the capability to determine the type of hacker they are actually defending
against. Cavusoglu et al., (2005) show that hacking incentives, such as the user’s utility
of intrusion, play a more significant role than the firm’s cost parameters in determining
whether implementing an IDS is beneficial.

Researchers in the IT security community have called for improved methods to better
determine the value of the security devices used to defend against hacker activity. The
interactive behaviors between attack and defense are very complicated because both sides
have several strategies available with different payoffs, making them hard to analyze
effectively (Lin et al., 2009). Also, accounting for the manual inspection costs associated
with the different inspection strategies is a crucial part of determining the value of an IDS
allocation often results in security administrators being overwhelmed because they lack
the resources needed to respond to the high volume of alarms the IDS produces. Game-
theoretic analysis has become a popular tool among the IT Security research community
for analyzing resource allocation, cost analysis, and attack and defense strategies in
information warfare scenarios between attackers and defenders (Bloem et al., 2006;
Cavusoglu et al., 2005; Lin et al., 2009; Alpcan & Basar, 2003). However, game theory
typically assumes that all components of a game such as an opponent’s payoffs are
commonly known, which is arguably the exception rather than the rule in real-world applications (Drouvelis, Müller, & Possajennikov, 2012).

Dissertation Goal

The proposed dissertation aims to contribute to the current body of knowledge by presenting a game-theoretic model that can be used to derive the value of a firm’s IDS, and determine the optimal monitoring strategies when faced with uncertainty as a way to supplement IT security planning. Cavusoglu et al. (2005) call for future research using Harsanyi transformation analysis to extend their model to account for incomplete information where the firm is uncertain of the user’s utility of intrusion but believes the user’s hacking utility to be either high or low. Harsanyi transformation analysis incorporates a third player, Nature, who makes the game’s first move by choosing the type of opponent (high or low utility) the firm faces using a common knowledge prior probability distribution. We use $P_H$ to represent the firm’s belief that the user has high utility, and $P_L = 1 - P_H$ to represent the firm’s belief that the user has low utility.

The proposed model is a Bayesian game that provides several contributions to the IT Security research community by demonstrating the benefits of accounting for uncertainty, and by further validating the use of game-theoretical analysis for IT security management. Harsanyi (1967) introduced the use of the Bayesian approach for achieving equilibrium by assigning a joint probability distribution to all unknown variables and utilizing the expected payoff values. This assumption is called the Bayesian Hypothesis.
and allows incomplete information to be interpreted as a lack of full information about the normal form of the game. The initial probability distributions $P_H$ and $P_L$ are used to represent the firm’s beliefs about each of its opponent’s strategy spaces; and, posterior probabilities are calculated after every observation using Bayes rule to determine if the proposed strategies achieve Bayesian equilibrium.

The proposed research provides a more realistic method for assessing the value of IDS in the face of uncertainty and potentially for the evaluation of other security devices as well. The value of the IDS is calculated as the difference between the firm’s expected costs with and without the IDS under uncertainty regarding the user’s utility for intrusion. The IDS is configured (or tuned) to find the best operating point within its quality profile, which is measured by its false positive ($P_F$) and false negative ($1 - P_D$) rates. The model is used to determine whether, and under what conditions, the IDS offers a positive value. The value of an IDS with its default configuration is also calculated to demonstrate the value added due to optimal configuration. The proposed research also aims to validate previous findings that firms may realize either a positive or negative value of IDS when using the default configuration and that an optimally configured IDS always provides a nonnegative value to their adopters.

An additional goal of the proposed research is to verify previous findings that suggest that the user’s hacking incentives and the game’s external environment play a more significant role than the firm’s cost parameters in determining whether or not deploying an IDS is beneficial. The proposed research shows the significance of understanding the
hacker’s behavior and motivation when employing an IDS by showing that the firm realizes a positive value from an IDS only when the detection rate is higher than a critical value determined by the hacker’s utility and cost parameters. Comparing the results of the proposed model with those of the inspiring literature further validates the use of game theory as a viable tool for valuing security devices as a supplement to IT security management.

The proposed research also provides further insight for security engineers implementing IDS when the firm is uncertain of the user’s utility of intrusion. Evaluation of the firm’s optimal monitoring strategies as the user’s utility of intrusion decreases provides insight into the optimal configuration changes that should be employed when the firm must account for different opponent types. Evaluating scenarios where the probability of detection is greater than the firm’s optimal investigation rate for low utility hackers but lower than their optimal investigation rate for high utility hackers also sheds light on concerns regarding the value of implementing IDS. Further analysis of the changes in equilibrium and the number of game iterations required to achieve equilibrium is used to determine if the proposed model can be used to identify whether the firm faces a high or low utility opponent. The firm’s ability to make this determination while facing uncertainty also provides the IT security research community with further insights into the benefits and consequences associated with the different methods of operating these devices.

**Research Questions**
Completion of the proposed research aims to answer the following questions:

1. Under what conditions are Bayesian equilibrium achieved? What effects do the initial probabilities chosen to represent the likelihood of the firm facing each opponent type have on the model’s ability to achieve equilibrium?

2. Does analysis of the proposed model support the previous findings of Cavusoglu et al. (2005) that hacker incentives and the game’s external parameters have more of an effect on the value of IDS than the firm’s cost parameters? If not, what parameters in the proposed model are the most influential?

3. Under what conditions does the firm benefit from implementing an IDS using its default configuration? How do the optimal monitoring and hacking strategies compare to those defined by Cavusoglu et al. (2005)?

4. What implications exist when the probability of detection falls between the firms optimal detection rates for low and high utility users? How many game iterations are necessary under these conditions to achieve equilibrium and can the firm use this information to determine which type of opponent it faces?

5. What is the value of optimal configuration and do the model’s results validate previous findings that the firm will always receive a positive value when deploying an optimally configured IDS? Can these findings be used to provide further insight to security personnel on the best methods for configuring and deploying these systems?
Relevance and Significance

An IDS plays a major role in detecting attacks and identifying network users with malicious intentions. “The distributed nature and complexity of computing and communication networks leads to an ongoing confrontation between firms and malicious hackers which naturally leads to a game theoretical analysis” (Bloem et al., 2006). The proposed research is most significant in that it better represents the real world game played between hackers and firms where the firm is uncertain of its opponent’s hacking incentives and can adopt more effective strategies that increase their expected payoffs. The benefit of an IDS can be overestimated by current intrusion detection models because they unreasonably assume that an information security officer responds to all alarms without any delay and avoids damages from hostile activities (Ryu & Rhee, 2008).

Furthermore, IT security personnel are faced with choosing between deploying an IDS with its default configuration and fine tuning its configuration through its quality profile, which is measured by its false positive and false negative rates. Alpcan and Basar (2003) discuss the need to satisfy some upper and lower bounds on these rates because lowering one rate inherently raises the other. The ultimate result is higher false alarms, manual inspection of legitimate traffic, and intrusions that go undetected. Cavusoglu, Cavusoglu, & Raghunathan (2009) show, during their research on the effects of configuration in
networks with multilayered security models, that deploying an IDS can hurt a firm if the configuration is not optimized for the firm’s operating environment.

The decision to employ an IDS plays a key role in a firm’s IT security planning and can have several implications on its overall security posture if the system is deployed. Maintaining a detection system can be very costly, even for organizations with a simple security environment, making it necessary to perform the analysis needed to determine whether and how hackers are trying to break in (Moorkerjee, Moorkerjee, & Bensoussan, 2011). The expected cost of ongoing manual inspections must be analyzed to avoid exceeding the value added from intrusion detection. Failure to identify the costs associated with maintaining an IDS results in a lack of resources allocated towards responding to attacks and overwhelmed security personnel tasked with manually investigating the alarms (Bloem et al., 2006). The proposed research provides insight into the cost ramifications of deploying an IDS with its default configuration. Analyzing the value of configuration and the manual inspection costs is even more crucial because the increasing losses associated with cyber-attacks indicate that firms are not spending enough money to adequately protect themselves from hackers (Gordon & Loeb, 2002).

Deriving a firm’s optimal monitoring strategy and the value of its IDS using a game-theoretic model is appropriate for several reasons. Jiang, Fang, Zhang, Tian, and Song, (2009) note that a current challenge is to invent and study appropriate theoretical models of cost-effective security management in security attacks and defenses, because these information security breaches pose a significant threat to national security and economic wellbeing. Previous attempts to model this environment fail to develop a framework that
accurately depicts the cost of preventative security measures because they are often incapable of modeling real world scenarios where attackers and defenders are unsure of their opponent’s utility. In the view of Harsanyi (1967) it is a major analytical deficiency that existing game theory has been almost completely restricted to games of complete information, in spite of the fact that in many real life economic, political, military, and social situations the participants often lack full information about important aspects of the game they are playing. The proposed research is significant because it extends previous complete information game models to account for uncertainty.

Cavusoglu et al. (2005) show that the user’s hacking incentives, $\mu$, have the most substantial effects on the cost of a firm’s IDS. They also call for future research on extending their model to account for a more realistic implementation where the firm is unsure of its opponent’s utility and believes it faces two types of opponents with different payoffs. The proposed research models the firm’s uncertainty of the hacking utility available to users, which better mimics real world security environments. Modeling both of the firm’s high and low utility opponents allows the firm to adjust its inspection strategies accordingly, which is even more critical considering present day hackers are being increasingly motivated by financial gains (utility) rather than curiosity, as demonstrated by (Sophos Labs, 2008).

Because the expansion of the internet has attracted individuals and groups with destructive motivations looking to improve on their perceived utility (Grossklags, Christin, & Chuang, 2008), it is critical, when assessing vulnerability, to account for incomplete information (uncertainty) where players are uncertain of their opponent’s
payoffs to better mimic a real world environment. As the call for improved methods of estimating the value of security devices continues, researchers are finding that firms do not have the necessary information about potential hackers needed to devise an appropriate monitoring strategy. The proposed research addresses the notion that “stronger refinements have to be defined for games with imperfect information in order to achieve equilibrium because, currently, players are ignorant to the characteristics of other players” (Montet & Serra, 2003).

**Barriers and Issues**

Accurately modeling the cost of security devices, particularly detective devices, is inherently difficult because of the manual inspection costs associated with the different investigation strategies and the incomplete information players experience regarding their opponent’s payoffs. As a result, the interactive behaviors between attack and defense are very complicated and the tradeoff between attack and defense cannot be analyzed by means of the traditional experience rule (Lin et al., 2009). The problem is further complicated in that a firm can choose to implement different inspection strategies by choosing to only inspect traffic producing an alarm, all traffic regardless of alarm, or a combination of the two. Each of these monitoring strategies comes at a different cost because of the manual inspection resources needed to respond to alarms and the damages of undetected intrusions. Inspecting too many alarms can potentially cost more than the losses prevented, while inspecting less traffic can result in costly intrusions. Collectively, this makes it very difficult to model the value of IDS.
“Given the current overview of the information security and intrusion detection, there is definitely a need for a decision and control framework to address issues like attack modeling, analysis of detected threats, and decision on response actions” (Alpcan & Basar, 2003). The model proposed by Cavusoglu et al. (2005) addressed a major shortcoming in prior research but fails to account for incomplete information regarding user payoffs. Firms are typically unaware of the payoffs available to the hackers they defend against, making it crucial to account for incomplete information when modeling their configuration and modeling strategies. The value of previous models diminishes as the firms are forced to choose monitoring strategies that do not account for the different hacking incentives, which can lead to poor security planning.

Accounting for incomplete information involves determining the subjective probabilities that will be assigned to represent the firm’s belief about each type of player it faces. This common prior assumption plays an important role in game theory and it would be difficult, if not impossible, to solve without it (Drouvelis et al., 2012). The model’s ability to achieve equilibrium, the resulting value of the firm’s IDS, and the cost of each monitoring strategy, could be skewed if the subjective probabilities are not tailored to accurately represent each opponent type. Drouvelis et al., (2012) discuss the importance of inducing a correct common prior while researching its value and whether the game’s players can learn it over time. Choosing the appropriate variations of the $\mu$ parameter is also necessary to accurately represent each opponent type because of further implications on the model’s ability to achieve equilibrium.


**Assumptions, Limitations, and Delimitations**

The proposed work makes several assumptions. The firm and users are assumed to be risk neutral and utility is consequently assumed to be a linear function of benefits. The risk neutrality assumption eliminates scenarios where the firm is risk averse regarding critical assets or the potential hacker is a risk seeker. It is also assumed that a user receives a benefit of $\mu$ if the intrusion is not detected and incurs a penalty of $\beta$ giving a net benefit of $(\mu - \beta) < 0$ when detected. The user population is assumed to be homogenous consisting of honest and dishonest users and honest users do not choose to hack. Manual investigations are assumed to confirm or rule out intrusions with certainty. The firm incurs a damage of $d$ and that the cost of manual investigation is less than the benefit it receives from detecting an intrusion. A limitation of the proposed research is that it models a onetime game and is not played over several iterations. Modeling a multi-period game would allow the game’s players to adjust their strategies based off of the strategies they observe during previous iterations of the game.

**Definition of Terms**

The terms used in this work are presented in table 3 defined further in within the narrative of this proposal.
Table 3
Definition of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Game Theory</td>
<td>The study of mathematical models of conflict and cooperation between intelligent rational decision makers for strategic decision making.</td>
</tr>
<tr>
<td>Simultaneous Game</td>
<td>A game-theoretic model where both players make a decision at the same time without prior knowledge of the opponent's decision.</td>
</tr>
<tr>
<td>Non-Cooperative Game</td>
<td>A non-cooperative game is one in which players make decisions independently.</td>
</tr>
<tr>
<td>Bayesian Game</td>
<td>In game theory, a Bayesian game is one in which information about characteristics of the other players (i.e. payoffs) is incomplete.</td>
</tr>
<tr>
<td>Bayes Rule</td>
<td>Bayes' rule relates the odds of event $A_1$ to event $A_2$, before (prior to) and after (posterior to) conditioning on another event B.</td>
</tr>
<tr>
<td>Harsanyi Transformation</td>
<td>Harsanyi's approach to modeling a Bayesian game in such a way that allows games of incomplete information to become games of imperfect information. The type of a player determines that player's payoff function and the probability associated with the type is the probability that the player for whom the type is specified is that type.</td>
</tr>
<tr>
<td>Normal Form Game</td>
<td>A normal form game is a description of a game whose representations are not graphical and are represented as a matrix.</td>
</tr>
</tbody>
</table>
### Extensive-Form Game

An extensive-form game allows representation of incomplete information in the form of chance events encoded as moves by Nature in tree format showing explicit representation of the sequencing of player's possible moves, their choices at every decision point, the information each player has about the other player's moves when he makes a decision, and the payoffs for all possible game outcomes.

### Intrusion Detection System (IDS)

A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

### Inspection Policy

An inspection policy determines what network traffic a security administrator will investigate with respect to whether or not the traffic causes an IDS to produce an alert.

### Information Technology (IT)

The application of computer networks and telecommunications equipment to store, retrieve, transmit, and manipulate data often in the context of a business or other enterprise.

### Summary

Firms lose millions of dollars every year from damage attributed to network intrusions by malicious users. Accordingly, firms invest heavily in IT security, choosing from a plethora of both preventative and detective security devices. Intrusion Detection Systems (IDS) are adopted as an additional layer of security by many firms because of their ability to monitor the internal network for malicious traffic that has bypassed their firewall or originated from internal users. The actual value of these devices remains uncertain because they often produce a high volume of false alarms requiring manual investigation by security administrators, which can become very costly. By modeling the tradeoff
between false positives and false negatives, and determining the value of an IDS, firms can better analyze their security investment and cost effective security plans. But modeling these tradeoffs can be extremely difficult because of the numerous costs associated with the different configuration and inspection strategies available for deployment (Lin et al., 2009; Cavusoglu et al., 2005; Zonouz, Joshi, & Sanders, 2010).

Prior research models the firm and network user in an Inspection game of complete information, and derives the mixed strategy equilibria to determine the firm’s optimal monitoring strategy and the associated cost. However, a game where the value of every parameter is common knowledge to the firm is not practical because the firm is often unaware of the true hacking utility available to the user. The proposed dissertation contributes to the current body of knowledge by presenting a game-theoretic model that derives the value of a firm’s IDS and determines optimal monitoring strategies to supplement IT security planning when faced with uncertainty. The proposed Bayesian games of incomplete information provide several contributions to the IT Security research community by presenting a model that demonstrates the benefits of accounting for uncertainty, allows the firm to determine the type of opponent it faces, optimally configure its IDS to defend against these opponents, and by further validating the use of game-theoretical analysis for IT security management.
Chapter 2

Review of the Literature

Inspiring Literature

Cavusoglu et al. (2005) conducted research focused on assessing the value of intrusion detection by utilizing Game Theory. According to their study, the value of IDS is derived using a parsimonious model to determine the optimal strategies for both the firm and user components, strategically choosing the appropriate inspection strategies based on the results. The model consists of components representing every user of the system as well as the firm responsible for performing manual investigations, and then analyzes audit trails to identify intrusions. The model determines the following probabilities:

- Optimal strategy of a user, probability of intrusion
- Optimal strategy for a firm with no IDS, probability of manual inspection
- Optimal strategy (probability of manual inspection) for a firm with an IDS

Analysis was performed on cases with and without the firm choosing to implement an IDS. The Nash equilibriums were computed for each case and Backward Induction was used to determine the best strategies. The mixed strategy profiles representing the Nash equilibrium for the IDS case are computed:
If $\frac{\mu}{\beta} > P_D$, then $(\rho_1 = 1, \rho_2 = \frac{\mu - P_D \phi}{1 - P_D \phi}, \psi = \frac{c(1-P_F)}{c(P_D-P_F)+(1-P_D)d \phi})$

If $\frac{\mu}{\beta} \leq P_D$, then $(\rho_1 = \frac{\mu}{P_D \phi}, \rho_2 = 0), \psi = \frac{cP_F}{P_D \phi - c(P_D-P_F)}$

The decision to implement an IDS was then made based on the cost of each case. The cost of manual investigation indicates that a firm may actually be hurt by implementing an IDS with its default configuration, unless its value comes from its potential as a deterrent. The firm’s cost for implementing an IDS was computed:

$\frac{c}{\phi} \frac{1 - (\phi \left(1 - \frac{c}{\phi_d}\right)P_D + (1 - \phi \left(1 - \frac{c}{\phi_d}\right)P_F)}{1 - (\phi \left(1 - \frac{c}{\phi_d}\right)P_F + (1 - \phi \left(1 - \frac{c}{\phi_d}\right)P_D)}$ when $\frac{\mu}{\beta} > P_D$

$\frac{c}{\phi} \frac{1}{\phi_d + (1 - \frac{c}{\phi_d})P_D/P_F}$ when $\frac{\mu}{\beta} \leq P_D$

Cavusoglu et al. (2005) conclude that implementing an optimally configured IDS is the best strategy. They suggest that the firm actually receives a positive value from an optimally configured IDS because of increased deterrence as opposed to its improved detection. The expected value of an optimally configured IDS was computed:

$\frac{c}{\phi} \left(1 - \frac{d \phi}{(\mu/\beta)^{1-\frac{1}{r}}} d \phi + (1 - (\mu/\beta)^{1-\frac{1}{r}})c\right)$

Results show that a firm only realizes a positive value if the detection rate is higher than a critical value determined by the user’s (hacker’s) utility and cost parameters.
Their research presents a static game-theoretic model where all model parameters are common knowledge and assumes that each player knows exactly what its opponent’s payoffs are. Table 4 summarizes the author’s most significant conclusions.

Table 4

*Propositions, Cavusoglu et al. (2005)*

| Proposition 1: The Nash Equilibrium for the no-IDS Case | The firm’s optimal investigation probability, \( \rho = \frac{\mu}{\beta} \)  
The user’s optimal hacking probability, \( \psi = \frac{c}{d\phi} \) |
| --- | --- |
| Proposition 2: The Mixed Strategy Nash Equilibrium for the IDS case | If \( \frac{\mu}{\beta} > P_D \) then \((\rho_1 = 1, \rho_2 = \frac{\mu-P_D\beta}{(1-P_D)\beta}), \psi = \frac{c(1-P_F)}{c(P_D-P_F)+(1-P_D)d\phi}\)  
If \( \frac{\mu}{\beta} \leq P_D \) then \((\rho_1 = \frac{\mu}{P_D\beta}, \rho_2 = 0), \psi = \frac{cP_F}{P_Dd\phi-c(P_D-P_F)}\) |
| Proposition 3: The IDS Case Compared to the no-IDS Case | The hacking probability is higher if \( P_D < \frac{\mu}{\beta} \)  
The hacking probability is lower if \( P_D \geq \frac{\mu}{\beta} \) |
| Proposition 4: The Default Configuration Case | The value of the IDS is negative when \( P_D < \frac{\mu}{\beta} \)  
The value of the IDS is nonnegative when \( P_D \geq \frac{\mu}{\beta} \) |
| Proposition 5: Optimally Configured IDS | The value of the optimally configured IDS is nonnegative  
The optimally configured IDS deters hackers  
The optimally configured IDS yields the same investigation strategy as a perfect \((P_D = 1 \text{ and } P_F = 0)\) IDS |

Proposition 1 gives the mixed strategy profile under Nash equilibrium for the no-IDS case where firm and user’s optimal strategies make their opponent indifferent between
hacking and investigating respectively. Proposition 2 gives the mixed strategy profile under Nash Equilibria for the IDS case by dividing the parameter space into two distinct regions where different investigation strategies are played by the firm. Proposition 3 compares the no-IDS and IDS cases demonstrating that the user’s hacking probability is higher when \( P_D < \frac{\mu}{\beta} \) and lower when \( P_D \geq \frac{\mu}{\beta} \), even though the probability of detecting a hacker is the same regardless of whether or not the firm chooses to implement an IDS. Proposition 4 analyzes the value of IDS when the configuration is assumed to be exogenous deriving the negative and nonnegative operating regions of an IDS using its default configuration. Proposition 5 demonstrates that the value of an optimally configured IDS is nonnegative, deters hackers, and yields the same investigation strategy as a perfect IDS (\( P_D = 1 \) and \( P_F = 0 \)).

**Inspection Games**

The proposed game theoretic model between a hacker and firm trying to determine an appropriate inspection strategy most resembles an Inspection Game (Cavusoglu et al., 2005). An Inspection Game models a situation where an inspectee has incentive to violate a legal obligation, and the inspector is responsible for monitoring their adherence to the law. The first Inspection Game in literature was introduced by Dresher (1962) to analyze the treaty of arms reduction in 1962. Much like the proposed dissertation work, the mathematical analysis utilizes a two player, non-cooperative game that seeks to determine an optimal inspection scheme that induces legal behavior, working under the assumption that illegal actions are carried out strategically. Inspection Games were
eventually branched out to the so called Smugglers Game by Thomas and Nisgav (1976) who extended the model to a multistage recursive game between customs and a smuggler, where customs patrols are looking for the illegal actions of the smuggler.

Hohzaki (2013) investigated the value of the game’s information between customs and smugglers by modeling the Inspection Game with incomplete information. The author presents a model where player B can obtain information about player A, but player A is not afforded that same luxury. Similar to the proposed research, a game is modeled where the inspector has to make a decision based off of his belief on the characteristics of his opponent and the state of the game. The game is analyzed using its Bayesian equilibrium to solve for its Nash equilibrium equivalent because it takes into account the player’s beliefs.

**Security Investing**

Bohme and Moore (2010) model security investing and place an emphasis on the importance of making security management decisions over time as they analyze the effects of over and under investing. Under investing in security measures can result in tragic losses, while over investing can also become costly if a firm spends more money on protective measures than the value of the assets they are protecting. The cost metrics associated with these security devices, and the utility available to users, realistically changes over time as the manual investigation costs and value of the protected information changes. The authors also validate previous findings that prove that
understanding the hacker’s motivation and behavior also plays a crucial role in determining the best monitoring strategies.

Young, Wei, and Metin (2009) analyze security investing by analyzing intrusion detection decisions in the presence of multiple alarm types. The alarm types differ in occurrence probabilities, damage, and investigation costs. They use multi-period optimization models to study the allocation of the investigation budget, optimal false alarm rates, and allocation of the investment budget in the presence of alternate investment options. The authors find it optimal to ignore non-critical alarms in order to save a portion of the investigation budget to be allocated for critical alarms that may arise in the future. They also determine that under a tight security budget an IDS is most effective when it is configured at a low false alarm rate. Further analysis shows that the cost of ignoring alarms is a prominent decision factor for management in the intrusion detection problem.

**Network Security Games**

Bloem et al., (2006) presented a game theoretical model of the interaction between an IDS and attacker to investigate the optimal allocation of a system administrator’s time. The authors build on previous game-theoretic models by identifying the time administrators spend manually investigating alarms and accounting for its importance; they also introduce an algorithm for allocating the time they have available for investigating attacks. Their Automatic or Administrator Response (AOAR) algorithm reformulates the resource allocation problem as a formal optimal control problem with
more sophisticated cost structures, treating the administrator’s time as a scarce resource. The AOAR algorithm utilizes classification of successful attacks with Linear Programming optimization as a tool for deciding how to respond to each attack.

Lin et al., 2009 show that the interactive behavior between the hacker and the defender is similar to information warfare, and utilize game theory to extract the process of attack and defense and present it as a tree diagram. They model this process as a zero-sum game and present solutions based on the Minmax theorem. In zero-sum games, the Minmax solution is equivalent to the Nash Equilibrium. Thus those strategies listed in the probability spread can satisfy both involvers. The Minmax theorem was chosen because the tradeoff between attack and defense is hard to accurately keep by means of the traditional experience rule.

**Bayesian Games**

In an interaction, it is possible that one player has features it is aware of but that the opponent is not (e.g. cost, payoff, valuation or fighting ability); these information asymmetries can be referred to as the player’s type (Amann & Possajennikov, 2009). Previous literature shows that games with incomplete information may be modeled as Bayesian games to account for player’s beliefs. The natural way to achieve the equivalent of Nash equilibrium is by calculating the Bayesian Nash equilibrium (also referred to as Bayesian equilibrium). Ceppi, Gatti, and Basilico (2009) analyze algorithms for computing the Bayesian Nash equilibrium in two player strategic form games, noting that the computation of equilibria in games is a challenging task and that these types of games
are typically reduced to complete information games of imperfect information before they are solved.

Harsanyi (1967) proposed an alternative Bayesian approach for the analysis of incomplete information allowing uncertainty to be made explicit and be quantified. Harsanyi Transformation dictates that there is a probability distribution over the set of every type of player in the game. Player’s beliefs about their opponents are derivable from a common prior distribution. Thus the game is transformed into one of complete, but imperfect information, which is equivalent to the original game of incomplete information.

Harsanyi (1995) demonstrates that with suitable modeling, all forms of incomplete information can be reduced to a game where players have less than full information about their opponent’s payoff functions. The game begins with a chance move made by a third player, Nature, that informs each player of their type and the players choose their actions accordingly. The probability distribution assigned to Nature is known by the game’s players and is typically assigned based the player’s beliefs and prior experience. Using the Bayesian approach, a subjective joint probability distribution is assigned to all unknown variables and the players maximize the mathematical expectation of their own payoff. Harsanyi’s modeling and analysis has become a standard tool of the trade and may be viewed as the foundation for nearly all economic analysis involving differential information including economic theory (Van Damme, & Weibull, 1995).
Chuin and Xinmin (2009) expanded on previous game-theoretical work based on rent-seeking theory that modeled the relationship between proprietors of a coal mine enterprise and the local government officials. Previous work modeled this problem as a complete information dynamic game under the assumption that the exact values of payoffs were known. The authors established three incomplete information dynamic game models utilizing Harsanyi Transformation analysis in a Signaling game between local government supervision departments and coal mine owners. A Signaling game is a Bayesian game where one of the players is of a certain type which is assigned by Nature. That player’s opponent is unaware which type of player it faces and must account for this uncertainty through Bayesian analysis. Their model was used to extend previous research by accounting for incomplete information and giving their sub game refined Bayesian equilibriums to make suggestions on improving safety in coal mine production.

Carroll and Grosu (2009) performed a game theoretic investigation of the effects of deception in the interactions between an attacker and a defender of a computer network by modeling their interactions as a Signaling game of incomplete information. The authors model uncertainty in a scenario where the defender deploys honeypots in their network and chooses whether to disguise the normal system. The attacker must determine whether or not to proceed with compromising the system in the face of incomplete information on the type of system being attacked. The authors calculate the Bayesian equilibrium of the game and show how the defender can use this analysis to better protect their network.
Bayesian games have also been used to analyze the process of Research and Development (R&D) investment. The development of an enterprise and the economic growth of a country rely heavily on R&D investment. Liu, He, and Wang (2008) analyzed the R&D investment decision making process between computing firms by modeling a game of incomplete information. Optimal investment strategies were computed using the Bayesian equilibrium to account for the incomplete patent information experienced by both of the game’s players. Incomplete information arises when an enterprise decides whether or not to invest in R&D because they are unaware if their competitor is doing the same. Their analysis shows that enterprises continue to have motivation to invest in R&D when they have complete information. In contrast, when facing incomplete information, the enterprises lose their motivation to invest and the competition between enterprises is generally an order-less competition, centering on the prices of products.

Noam, Leshem, and Mesessr (2010) extend previous research on competitive spectrum sharing by proposing a symmetric Gaussian interference game with incomplete information where players choose between frequency division multiplexing (FDM) and full spread (FS) of their transmit power. They note that the complete information games result in a Nash equilibrium point where players mutually choose FS and interfere with each other, which is not always practical and can lead to large overhead. This outcome is often undesirable from a global network point of view and even for individual users as well. Both players know the square magnitudes of their channel gains and their noise Power Spectrum Density (PSD), but are unaware of their opponent’s channel gains. The
authors show that extending the previous complete information models allows users to agree to use different sub bands and achieve an equilibrium point where players choose FDM for some channel realizations and FS for others. Incorporating uncertainty allows the authors to achieve a Bayesian equilibrium that increases each user’s throughput and overall spectrum utilization.

Yin and Gan (2005) study the use of Signaling dames for analyzing Customer Relationship Management (CRM). They model CRM as a game with both cooperative and non-cooperative aspects. The business’s goal to maximize customer satisfaction requires cooperation; but there are non-cooperative aspects of the game as the business and customers make decisions under the conditions of incomplete information. Yin and Gan (2005) use Backwards Induction to obtain the Bayesian equilibrium for both players. The Bayesian equilibrium is then used to predict the player’s actions during the transaction and reveal the true player types and preferences during the game.

**Comparative Static Analysis**

Cavusoglu et al. (2005) use comparative static analysis to determine the effect of their model’s parameters on the overall value of the IDS. Comparative static analysis is a common technique for analyzing the effects that parameters have on an economic model, as well as the changes to its equilibrium. Tao and Hong (2009) use comparative static analysis to determine the relationships between different elements of the Virtual Money Market that serves as an instrument of small payment in e-commerce. Their analysis verifies the relationships among the virtual money operators, consumer channels, network
players, virtual money circulation, and the government regulations. Doni and Ricchiuti (2013) use comparative static analysis to determine the effects of green customers and environmentally responsible firms on the market equilibrium. They determine that when the degree of environmental consciousness is very high, responsible firms over provide environmentally friendly goods, which can have potentially negative effects on the market. Comparative static analysis will also be used to analyze the results of the proposed research.
Chapter 3

Methodology

Overview of Research Methodology

Cavusoglu et al. (2005) called for future research to address their model’s inability to account for uncertainty when a firm is unsure of the user’s utility of intrusion. This study extended their previous work to present a game-theoretic model with incomplete information capable of determining the value of an IDS to a firm’s IT security infrastructure. Harsanyi transformation analysis was used to model the Bayesian games in their extensive form with the firm facing both high and low utility opponents. The utility of the high and low utility users was taken to be $\mu$ and $\alpha\mu$ ($0 < \alpha < 1$), respectively. The firm’s uncertainty about the user’s utility was modeled by the following prior probability distribution: $P_H = P[\text{utility} = \mu]$ and $P_L = P[\text{utility} = \alpha\mu] = 1 - P_H$. The firm’s optimal monitoring strategies for both the IDS and no-IDS cases were computed using models where the low utility opponent experienced a decreasing utility for intrusion. Each of the model’s results was compared to those obtained under the assumption of complete information by Cavusoglu et al. (2005). Further analysis of the changes to the firm’s optimal monitoring strategies and the number of game iterations required to achieve Bayesian Nash equilibrium was used to determine if the models could be used to determine which user the firm had actually faced.
The remainder of the chapter is organized as follows: the Specific Research Methodology section provides a blueprint for accomplishing the proposed dissertation work. This section contains nine subsections titled Step 1 through Step 9, which detail the process of developing the proposed models utilizing Harsanyi transformation analysis, solving for their Bayesian Nash equilibrium, and analyzing the effects of incorporating uncertainty on the player’s optimal strategies, value of IDS, and optimal configuration. The Format for Presenting Results section defines the format that was used to present the models’ results, and is followed by the Resource Requirements section. The chapter concludes with a Summary section.

**Specific Research Methodology**

This dissertation provided insight into how Harsanyi transformation analysis and Bayesian games can be used to extend previous games of complete information to model more practical scenarios. Previous research provided a blueprint for modeling Bayesian games of incomplete information in their extensive form using Harsanyi transformation analysis. Bayes’ Rule was used to update posterior probabilities, as necessary, to update the firm’s beliefs and aid in calculating the players’ optimal strategies in the Bayesian Nash equilibrium. Backwards Induction was used to derive the equilibrium in the firm’s manual investigation and the users’ hacking strategies for the IDS and no-IDS cases.

Further analysis of the changes in the firm’s optimal configuration and the number of game iterations required to achieve Nash equilibrium was used to determine if the
models’ could be used by the firm to determine which opponent type it had actually faced. Analysis also included comparisons between the modeled results and the propositions set forth in the inspiring literature as seen in Table 4. This research examined propositions 1 through 5, allowing for comparative analysis of the no-IDS, IDS, default configuration, and the optimal configuration cases. Comparative analysis was also used to determine the effects of different model parameters on the value of IDS and its deterrence to potential hackers.

Step 1. Define the game’s parameters

Incomplete information games were modeled for both the IDS and no-IDS cases. The games’ players consisted of a firm and a user playing a two-person non-cooperative game that utilized Harsanyi transformation analysis to account for the firm’s incomplete information regarding the user’s utility of intrusion. Both models used the parameters defined in Table 5.
Table 5

**Bayesian Model Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d$</td>
<td>Damage caused by an undetected intrusion</td>
</tr>
<tr>
<td>$c$</td>
<td>Cost of manual investigation</td>
</tr>
<tr>
<td>$\mu$</td>
<td>Utility of intrusion for users</td>
</tr>
<tr>
<td>$P_D$</td>
<td>Probability of getting an alarm from IDS for an intrusion</td>
</tr>
<tr>
<td>$P_F$</td>
<td>Probability of getting an alarm from IDS for no intrusion</td>
</tr>
<tr>
<td>$\phi$</td>
<td>Fraction of damage prevented by the firm when an intrusion is detected</td>
</tr>
<tr>
<td>$\beta$</td>
<td>Hacker penalty for detection</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>Percentage of utility available to the low utility user</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strategic variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\psi$</td>
<td>Probability of intrusion by a user</td>
</tr>
<tr>
<td>$\psi_{Low}$</td>
<td>Probability of intrusion by a low utility user</td>
</tr>
<tr>
<td>$\psi_{High}$</td>
<td>Probability of intrusion by a high utility user</td>
</tr>
<tr>
<td>$\rho$</td>
<td>Probability of manual investigation when there is no IDS</td>
</tr>
<tr>
<td>$\rho_1$</td>
<td>Probability of manual investigation when the IDS generates an alarm</td>
</tr>
<tr>
<td>$\rho_2$</td>
<td>Probability of manual investigation when the IDS does not generate an alarm</td>
</tr>
<tr>
<td>$P_H$</td>
<td>Probability the firm faces a high utility opponent</td>
</tr>
<tr>
<td>$P_L$</td>
<td>Probability the firm faces a low utility opponent ($1 - P_H$)</td>
</tr>
</tbody>
</table>

A complete information game between the firm and user type was first modeled in normal form in both the IDS and no-IDS cases. In both cases, when $\alpha = 1$, the results were identical to those with complete information, as presented by Cavusoglu et al.
Modelling the a low utility user with a utility of \( \alpha \mu \) provided insight into the firm’s appropriate strategies when the firm lacks complete information regarding the user’s utility of intrusion. The no-IDS case is modeled in Figure 2, with the high utility user corresponding to the complete information game presented in the inspiring literature and the low utility opponent experiencing a utility of \( \alpha \mu \), where \( 0 < \alpha < 1 \).

\[\begin{array}{c|cc}
\text{Firm} & \text{High Utility User} & \\
 & H & NH \\
\hline
I & (c + (1 - \phi)d, \mu - \beta) & (c, 0) \\
NI & (d, \mu) & (0, 0) \\
\end{array}\]

\[\begin{array}{c|cc}
\text{Firm} & \text{Low Utility User} & \\
 & H & NH \\
\hline
I & (c + (1 - \phi)d, \alpha \mu - \beta) & (c, 0) \\
NI & (d, \alpha \mu) & (0, 0) \\
\end{array}\]

*Figure 2. Normal form games, No-IDS case*
Each of the games in Figure 2 became sub games presented in their extensive form when modeling the no-IDS case. The user’s hacking strategy was to hack (H) or not hack (NH), and the firm’s monitoring strategy was to either inspect (I) or not inspect (NI) user traffic. Figure 3 models the IDS case with the high utility user corresponding to the complete information game presented in the inspiring literature and the low utility opponent experiencing a utility of $\alpha \mu$, where $0 < \alpha < 1$. 
<table>
<thead>
<tr>
<th>Firm</th>
<th>High Utility User</th>
<th>Low Utility User</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td></td>
<td>NH</td>
<td>NH</td>
</tr>
<tr>
<td>I,I</td>
<td>( (c + (1 - \phi)d, \mu - \beta) )</td>
<td>( c, 0 )</td>
</tr>
<tr>
<td>I,NI</td>
<td>( ((c + (1 - \phi)d)P_D + d(1 - P_D), \mu - P_D\beta) )</td>
<td>( cP_F, 0 )</td>
</tr>
<tr>
<td>NI,I</td>
<td>( (dP_D + (c + (1 - \phi)d)(1 - P_D), \mu - (1 - P_D\beta) )</td>
<td>( c(1 - P_F), 0 )</td>
</tr>
<tr>
<td>NI,NI</td>
<td>( (d, \mu) )</td>
<td>( (0, 0) )</td>
</tr>
</tbody>
</table>

*Figure 3. Normal form games, IDS case*
Each of the games in Figure 3 became sub games presented in their extensive form when modeling the IDS case. The user’s hacking strategy was to hack (H) or not hack (NH), and the firm’s monitoring strategy was to either inspect (I) or not inspect (NI) network traffic based on whether the IDS raised an alarm. The firm’s strategy space was the Cartesian product of the actions available at each of the information sets expressed $S_F \in \{(I,I), (I,NI), (NI,I), (NI,NI)\}$. The first element in each pair represented the firm’s action (inspect or not inspect a user’s traffic) when the IDS produced an alarm. The second element corresponded to their action when no alarm was produced.

**Step 2. Harsanyi transformation analysis**

A game of incomplete information can be transformed into a game of complete but imperfect information through Harsanyi transformation by adding a third player, Nature, and conditioning the payoffs on Nature’s unknown moves (Carroll & Grosu, 2009). The no-IDS case modeled in Figure 4 is an extensive-form game tree where the root node, Nature, moves first by randomly choosing the firm’s opponent from a prior probability distribution over the high and low utility user types. The probability distribution was known by all of the game’s players. The tree’s sub games correspond to the games modeled in Figure 2, depicting both user types and their associated payoffs. Each sub game consisted of its own game tree components, and the terminal nodes (right most nodes) represent the payoffs for a game played against that particular user type.
Figure 4. Harsanyi Transformation of the No-IDS case
Table 6 shows the utility functions of the no-IDS case modeled in Figure 4 and depicts every strategy that was available to the game’s players and the associated payoffs.

Table 6

*Utility Functions for the Proposed Bayesian Game, No-IDS Case*

<table>
<thead>
<tr>
<th>$S_U$</th>
<th>$S_F$</th>
<th>$U$</th>
<th>$P_F$</th>
<th>$P_U$</th>
</tr>
</thead>
<tbody>
<tr>
<td>NH</td>
<td>I</td>
<td>$U_1$</td>
<td>$c$</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>I</td>
<td>$U_2$</td>
<td>$c$</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>NI</td>
<td>$U_1$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>NI</td>
<td>$U_2$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>H</td>
<td>I</td>
<td>$U_1$</td>
<td>$c + (1 - \phi)d$</td>
<td>$\mu - \beta$</td>
</tr>
<tr>
<td>H</td>
<td>I</td>
<td>$U_2$</td>
<td>$c + (1 - \phi)d$</td>
<td>$\alpha\mu - \beta$</td>
</tr>
<tr>
<td>H</td>
<td>NI</td>
<td>$U_1$</td>
<td>$d$</td>
<td>$\mu$</td>
</tr>
<tr>
<td>H</td>
<td>NI</td>
<td>$U_2$</td>
<td>$d$</td>
<td>$\alpha\mu$</td>
</tr>
</tbody>
</table>

$S_U$ = User’s Strategy  
$S_F$ = Firm’s Strategy  
$U$ = Opponent Type  
- $U_1$ = High Utility Opponent  
- $U_2$ = Low Utility Opponent  
$P_F$ = Cost of Manual investigation  
$P_U$ = User’s Utility for Intrusion

Each row in Table 6 corresponds to a potential set of strategies that could be played by each player and the associated payoffs. The first column denotes the user’s strategy ($S_U$); the second column denotes the firm’s strategy ($S_F$); and the third column denotes whether the user ($U$) is a high or low utility opponent ($U_1$, $U_2$). Columns four and five provide the payoffs for the firm ($P_F$) and user ($P_U$), respectively, given the player’s strategies and opponent type depicted in that row. Figure 5 utilizes Harsanyi Transformation analysis to
model the IDS case in its extensive form. The tree’s sub games correspond to the games modeled in Figure 3.
Figure 5. Harsanyi Transformation of the IDS case
Table 7 shows the utility functions of the IDS case modeled in Figure 5 and depicts every strategy that was available to the game’s players and the associated payoffs.

**Table 7**

*Utility Functions for the Proposed Bayesian Game, IDS Case*

<table>
<thead>
<tr>
<th>$S_u$</th>
<th>$S_f$</th>
<th>$U$</th>
<th>$P_f$</th>
<th>$P_u$</th>
</tr>
</thead>
<tbody>
<tr>
<td>NH</td>
<td>NI, NI</td>
<td>$U_1$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>NI, NI</td>
<td>$U_2$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>NI, I</td>
<td>$U_1$</td>
<td>$c(1 - P_f)$</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>NI, I</td>
<td>$U_2$</td>
<td>$c(1 - P_f)$</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>I, NI</td>
<td>$U_1$</td>
<td>$cP_f$</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>I, NI</td>
<td>$U_2$</td>
<td>$cP_f$</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>I, I</td>
<td>$U_1$</td>
<td>$c$</td>
<td>0</td>
</tr>
<tr>
<td>NH</td>
<td>I, I</td>
<td>$U_2$</td>
<td>$c$</td>
<td>0</td>
</tr>
<tr>
<td>H</td>
<td>NI, NI</td>
<td>$U_1$</td>
<td>$d$</td>
<td>$\mu$</td>
</tr>
<tr>
<td>H</td>
<td>NI, NI</td>
<td>$U_2$</td>
<td>$d$</td>
<td>$\alpha \mu$</td>
</tr>
<tr>
<td>H</td>
<td>NI, I</td>
<td>$U_1$</td>
<td>$(dP_D + (c + (1 - \phi)d)(1 - P_D))$</td>
<td>$\mu - (1 - P_D)\beta$</td>
</tr>
<tr>
<td>H</td>
<td>NI, I</td>
<td>$U_2$</td>
<td>$(dP_D + (c + (1 - \phi)d)(1 - P_D))$</td>
<td>$\alpha \mu - (1 - P_D)\beta$</td>
</tr>
<tr>
<td>H</td>
<td>I, NI</td>
<td>$U_1$</td>
<td>$(c + (1 - \phi)d)P_B + d(1 - P_D)$</td>
<td>$\mu - P_D\beta$</td>
</tr>
<tr>
<td>H</td>
<td>I, NI</td>
<td>$U_2$</td>
<td>$(c + (1 - \phi)d)P_B + d(1 - P_D)$</td>
<td>$\alpha \mu - P_D\beta$</td>
</tr>
<tr>
<td>H</td>
<td>I, I</td>
<td>$U_1$</td>
<td>$c + (1 - \phi)d$</td>
<td>$\mu - \beta$</td>
</tr>
<tr>
<td>H</td>
<td>I, I</td>
<td>$U_2$</td>
<td>$c + (1 - \phi)d$</td>
<td>$\alpha \mu - \beta$</td>
</tr>
</tbody>
</table>

$S_u$ = User’s Strategy  
$S_f$ = Firm’s Strategy  
$U$ = Opponent Type  
- $U_1$ = High Utility Opponent  
- $U_2$ = Low Utility Opponent  
$P_f$ = Cost of Manual investigation  
$P_u$ = User’s Utility for Intrusion
Each row in Table 7 corresponds to a potential set of strategies that could be played by each player and the associated payoffs. The first column denotes the user’s strategy ($S_U$); the second column denotes the firm’s strategy ($S_F$); and the third column denotes whether the user ($U$) is a high or low utility opponent ($U_1$, $U_2$). Columns four and five provide the payoffs for the firm ($P_F$) and user ($P_U$), respectively, given the player’s strategies and opponent type depicted in that row.

**Step 3. Compute the Bayesian Nash equilibrium for the proposed models**

Figures 4 and 5 model Bayesian games because of the incomplete information experienced by the firm and the probabilistic analysis inherent in games where a player’s prior and posterior beliefs must be modeled to represent uncertainty. Backwards Induction was used to derive the Bayesian Nash equilibrium in the firm’s manual investigation and the user’s hacking strategies for both the IDS and no-IDS cases. Their equilibria were then used to further analyze the effects of modeling incomplete information. Further analysis of the conditions needed to achieve equilibrium and the effects of the $\alpha$, $P_H$, and $P_L$ parameters was then used to answer Research Question 1.

**Step 4. Mixed strategy profile under Nash equilibrium for the no-IDS case**

Proposition 1 of the inspiring literature derived the mixed strategy equilibria for the no-IDS complete information game modeled by Cavusoglu et al. (2005) as $\rho = \frac{\mu}{\beta}$ and $\psi = \frac{c}{d\phi}$. The user’s optimal strategy was to hack with a probability of $\frac{c}{d\phi}$, which made the firm indifferent to investigating/not investigating user traffic and the firm’s optimal
strategy of investigating with a probability of $\frac{\mu}{\beta}$ made the user indifferent to hacking/not hacking. Comparative analysis between Proposition 1 of this study and Proposition 1 of the inspiring literature was used to analyze the impact of incorporating the firm’s uncertainty in the no-IDS case. Because the firm’s optimal strategy in this study was to choose a probability of manual inspection $\rho = \frac{\bar{\mu}}{\beta}$, the firm’s strategy was contingent upon the expected value of the user’s utility $\bar{\mu} = P_H(\mu) + P_L(\alpha \mu) = (P_H + (1 - P_H)\alpha)\mu$. Consequently, the probability of manual inspection changed as the $P_L$, $P_H$, and $\alpha$ parameters were updated based on new information.

Step 5. Mixed strategy profile under Nash equilibrium for the IDS case

Proposition 2 of the inspiring literature derived the mixed strategy equilibria for the IDS complete information game modeled by Cavusoglu et al. (2005) as follows:

If $\frac{\bar{\mu}}{\beta} > P_D$, then $\rho_1 = 1, \rho_2 = \frac{\mu - P_D \beta}{(1 - P_D) \beta}, \psi = \frac{c(1 - P_F)}{c(P_D - P_F) + (1 - P_D)d\phi}$

If $\frac{\bar{\mu}}{\beta} \leq P_D$, then $\rho_1 = \frac{\bar{\mu}}{P_D \beta}, \rho_2 = 0, \psi = \frac{cP_F}{P_D d\phi - c(P_D - P_F)}$

The IDS divided the parameter space into two distinct regions where different strategies were played. This study computed the mixed strategy equilibria for the IDS case accounting for the firm’s incomplete information and compared the results to those of the inspiring literature. Also, given that $\frac{\bar{\mu}}{\beta} > P_D$ implies $\frac{\mu}{\beta} > P_D$ and that $\frac{\bar{\mu}}{\beta} \leq P_D$ implies $\frac{\bar{\mu}}{\beta} \leq P_D$, the firm’s strategies remained the same when the updated values of $\bar{\mu}$ resulted in $P_D$ falling into one of these operating regions. Research Question 4 was answered by analyzing the effects of incorporating uncertainty in the interesting case.
where the firm’s probability of detection lay in the region where $\frac{a \mu}{\beta} < P_D < \frac{\mu}{\beta}$. The number of game iterations needed to achieve equilibrium and the player’s optimal monitoring strategies were also analyzed when $P_D$ fell in this range to determine if the firm could use the model’s results to identify whether it had faced a high or low utility opponent.

**Step 6. Comparison of the IDS and No-IDS cases**

Proposition 3 of the inspiring literature compared the IDS and no-IDS cases. Cavusoglu et al. (2005) demonstrated that the hacking probability was higher when $P_D < \frac{\mu}{\beta}$ and lower when $P_D \geq \frac{\mu}{\beta}$. They also showed that the effective detection rates were identical in the IDS and no-IDS cases. In the IDS case, the investigation of users was so efficient in reducing the firm’s cost when $P_D \geq \frac{\mu}{\beta}$ that the user had to reduce the hacking probability from that of the no-IDS case to make the firm indifferent to investigating/not investigating traffic. However, the firm had to extend its investigation to the no-alarm state in the IDS case when $P_D < \frac{\mu}{\beta}$, which was so inefficient in reducing the firm’s cost that the user increased his or her hacking probability from that of the no-IDS case to make the firm indifferent to investigating/not investigating traffic. This study analyzed the effects of modeling incomplete information on the effective detection and hacking rates to determine whether these results held true.

**Step 7. The default configuration case**

In Proposition 4 of the inspiring literature, Cavusoglu et al. (2005) demonstrated that the value of IDS was negative when $P_D < \frac{\mu}{\beta}$ and nonnegative when $P_D \geq \frac{\mu}{\beta}$ in the default
configuration case. This study answered Research Question 3 by analyzing the effects of incorporating the firm’s uncertainty on these negative and positive operating regions to determine if the value of the IDS continued to be negative when $P_D < \frac{\mu}{\beta}$ and nonnegative when $P_D \geq \frac{\mu}{\beta}$. This study also analyzed whether or not accounting for incomplete information changed the bounds that define the positive and negative operating regions defined by the IDS and comparative analysis was used to determine the contributing factors.

**Step 8. Optimal configuration**

In Proposition 5 of the inspiring literature, Cavusoglu et al. (2005) demonstrated that an optimally configured IDS deterred hackers and yielded the same inspection strategy as a perfect IDS ($P_D = 1, P_F = 0$). They also demonstrated that the value of optimally configured IDS was strictly nonnegative. In the IDS case, the firm must decide what value to assign $P_D$ during configuration. The optimal configuration of the IDS in the complete information game was achieved by setting the detection rate to $P_D = \frac{\mu}{\beta}$. This study answered Research Question 5 by analyzing the effects of modeling incomplete information on the value of optimal configuration. Comparative analysis between the results of the inspiring literature and the newly derived value of optimal configuration (and its associated $P_D$) provided further insight into the effects of modeling incomplete information.
Step 9. Validate previous findings

This study also validated previous findings that the firm’s external parameters and hacking incentives played more of a role than the firm’s cost parameters in determining if the firm benefits from implementing IDS. Previous research demonstrated that a large portion of the IDS value came from its deterrence to hackers. Research Question 2 was answered by confirming that, when modeling incomplete information, increases in $\frac{\mu}{\beta}$ and $\frac{c}{d_\phi}$ offered more incentive for users to hack, which in turn caused the firm to investigate more frequently. Further analysis was performed to determine which parameters played the biggest role in determining the value of IDS. Potential management implications and areas of future research were also identified.

Format for Presenting Results

The results of this study included the modeling of the IDS and no-IDS incomplete information games, their associated Nash equilibria, the derived value of IDS, and analysis of the models’ parameters. The firm’s optimal investigation and user’s hacking strategies, along with the calculations for achieving Nash equilibrium, were also presented for each of the games modeled. Propositions 1 and 2 of this Dissertation Report present the mixed strategy equilibria of the no-IDS and IDS cases when modeling incomplete information. Proposition 3 compares the IDS and no-IDS cases, Proposition 4 presents the value of IDS using its default configuration, and Proposition 5 derives the value of optimal configuration when modeling incomplete information. Proposition 6
presents the findings for the interesting cases where the firm’s detection rate falls into the-ranges where \( \frac{\alpha \mu}{\beta} < P_D < \frac{\mu}{\beta} \) (IDS case) and \( \frac{\alpha \mu}{\beta} < \rho < \frac{\mu}{\beta} \) (no-IDS case). Tables were used to present a comparative analysis between Propositions 1-5 of this Dissertation Report and Propositions 1-5 set forth in the inspiring literature.

**Resources**

Hardware, software, peer-reviewed journals, industry standards, and industry experts were used to complete this research. A laptop was dedicated for performing research and running the computational software used to complete this study. Maple 18.01 mathematical and analytical software by Maplesoft was used to verify all of the computations that supplement the models’ design and implementation. Access to numerous academic journals was provided by Nova Southeastern University, along with independent subscriptions to IEEE, ACM, and INFORMS professional societies. Current industry standards were researched and mentoring in the fields of game theory and Bayesian analysis was sought out to further validate the modeling of the IDS and no-IDS cases.

**Summary**

This study modeled two player non-cooperative Bayesian games between a firm whose goal was to implement the least costly manual inspection strategy for its IDS and a
network user looking to maximize his or her payoff by deciding whether or not to hack. Unlike previous research, these game-theoretic models allowed the firm to calculate its optimal inspection strategy in the face of uncertainty when it was unsure of the user’s utility of intrusion. Harsanyi transformation analysis was used to model the Bayesian games in their extensive form, allowing the firm to account for its incomplete information. Backwards induction was used to derive the Nash equilibrium of each game for further analysis.

Variations to the user’s utility of intrusion allowed for the analysis of different games where the firm’s uncertainty was modeled against the potential of facing both high and low utility opponents. The players’ optimal strategies and the value of IDS were compared to those presented in Propositions 1-5 of the inspiring literature. Each of the model’s ability to achieve Nash equilibrium, the number of game iterations required to achieve equilibrium and the firm’s optimal monitoring strategies were also evaluated to determine if the proposed models could be used by the firm to determine whether it had faced a low or high utility opponent. Previous findings that the firm’s external environment and hacking incentives played more of a role in determining the value of IDS were examined and management implications were derived.
Chapter 4

Results

Model Analysis

The incomplete information games for the no-IDS and IDS cases were modeled in their normal form in Figures 2 and 3. Harsanyi transformation analysis was used to convert the games of incomplete information into games of complete, but imperfect, information to account for the firm’s uncertainty of the user’s expected utility of intrusion. Harsanyi transformation added a third player, Nature, which induces the firm’s uncertainty regarding its opponent, allowing the firm to adjust its strategy accordingly. Figures 4 and 5 model the no-IDS and IDS cases in extensive-form game trees where the root node, Nature, moves first by randomly choosing the firm’s opponent from a prior probability distribution over the high and low utility opponent types. The mixed strategy Bayesian Nash equilibrium for both games was derived using backwards induction.

A mixed strategy is the assignment of a probability to each pure strategy available to the game’s players. Mixed strategies allow players to randomly choose one of their pure strategies. The low and high utility users have two pure strategies, H and NH, in the no-IDS and IDS cases. The firm has two pure strategies in the no-IDS case, I and NI, and four pure strategies in the IDS case, (I,I), (I,NI), (NI,I), and (NI,NI). In the no-IDS case, the firm investigates a portion of user traffic with a probability of ρ, the low utility user
hacks with a probability of $\psi_{low}$, and the high utility user hacks with a probability of $\psi_{High}$. In the IDS case, the firm investigates a portion of user traffic when the IDS generates an alarm with a probability of $\rho_1$ and investigates a portion of user traffic when no alarm is generated with a probability of $\rho_2$. The low and high utility users hack with a probability of $\psi_{low}$ and $\psi_{High}$ in both the alarm and no-alarm states.

Backwards induction was used to derive the mixed strategies for both players that constitute the Bayesian Nash equilibrium of the proposed incomplete information games. Bayesian Nash equilibrium is a term used to reference the Nash equilibrium of a Bayesian game. To avoid confusion, the term Nash equilibrium will be used exclusively throughout the remainder of the dissertation. The Nash equilibrium is a solution concept in which each player knows the equilibrium strategies of the other players, and neither player can improve his or her payoff by changing strategy. In game theory, backwards induction is the process of reasoning backwards by first solving for the game’s equilibrium before further analysis occurs. In equilibrium, the user chooses a hacking strategy that allows the firm to achieve its optimal cost, and the firm chooses a manual investigation strategy that ensures that the user maximizes his or her expected benefit of intrusion. Playing these strategies achieves equilibrium by ensuring that the firm remains indifferent to investigating/not investigating user traffic and that the user remains indifferent to hacking/not hacking.

**Nash Equilibrium, No-IDS Case**
The firm’s uncertainty in the no-IDS case was modeled as a game of incomplete information where the firm is uncertain of the utility of intrusion available to the user, believing it will face either a low or high utility opponent. The user, however, knows the true utility and chooses his or her hacking strategy as if he or she were playing a game of complete information. The firm’s expected costs when playing each user type are the following:

$$F_{Low}(\rho, \psi_{Low}) = (1 - P_H)(\rho c + \rho \psi_{Low}(1 - \phi)d + \psi_{Low}(1 - \rho)d)$$  \hspace{1cm} (1)$$

$$F_{High}(\rho, \psi_{High}) = (P_H)(\rho c + \rho \psi_{High}(1 - \phi)d + \psi_{High}(1 - \rho)d)$$ \hspace{1cm} (2)$$

The firm’s total expected cost is as follows:

$$F_{Cost}(\rho, \psi_{Low}, \psi_{High}) = (1 - P_H)(\rho c + \rho \psi_{Low}(1 - \phi)d + \psi_{Low}(1 - \rho)d) + (P_H)(\rho c + \rho \psi_{High}(1 - \phi)d + \psi_{High}(1 - \rho)d)$$ \hspace{1cm} (3)$$

The low and high utility users’ expected benefits of intrusion are as follows:

$$H_{Low}(\rho, \psi_{Low}) = \psi_{Low} \mu - \psi_{Low} \rho \beta$$ \hspace{1cm} (4)$$

$$H_{High}(\rho, \psi_{High}) = \psi_{High} \mu - \psi_{High} \rho \beta$$ \hspace{1cm} (5)$$

Both the low and high utility users know his or her type and choose a strategy that maximizes $H_{Low}(\rho, \psi_{Low})$ and $H_{High}(\rho, \psi_{High})$ respectively. The firm, however, has to account for the possibility of facing either the low or high utility user while minimizing
\( F_{\text{Cost}}(\rho, \psi_{\text{Low}}, \psi_{\text{High}}). \) The solution to the game of incomplete information is stated in the following proposition.

**Proposition 1.** *The following mixed strategy profiles constitute the Nash equilibria for the no-IDS case \( (\rho = \frac{\mu}{\beta}, \psi_{\text{Low}} = \frac{c}{\phi}, \psi_{\text{High}} = \frac{c}{\phi}). \)

The mixed strategy equilibrium given in Proposition 1 shows that the firm’s optimal strategy is to randomly investigate user traffic with a frequency proportional to \( \frac{\mu}{\beta} \), making the user indifferent to hacking/not hacking. The firm accounted for its uncertainty regarding the type of opponent it faced by utilizing the probability of facing a high utility user \( (P_H) \) and the probability of facing a low utility user \( (1 - P_H) \), as modeled in Figure 4. Both the low and high utility users’ optimal strategy is to hack with a probability of \( \frac{c}{\phi} \). The reduced utility experienced by the low utility user did not change the calculation of the firm’s optimal expected cost \( \left( \frac{c}{\phi} \right) \). Although the firm’s overall cost function is weighted to represent the probability of facing each user type, the firm’s actual cost calculations are identical once the game is played, regardless of the user’s type. As a result, both users play the same hacking strategy to ensure the firm remains indifferent to investigating/not investigating traffic.

Modeling the game as one of incomplete information resulted in identical hacking strategies in the equilibrium as those of the complete information game modeled in the inspiring literature. However, Proposition 1 shows that the firm will randomly investigate user traffic at a lower rate when the firm accounts for its incomplete
information than it did under the assumption of complete information. When the game was modeled with incomplete information, the probability of manual investigation was lowered by \((P_H + (1 - P_H)\alpha)\), which is a weighted coefficient reliant on the probability of facing either the low or high utility user. Table 8 compares the mixed strategy equilibria of the complete information game modeled by Cavusoglu et al. (2005), a complete information game against the low utility user, and the incomplete information game modeled in Figure 4.

Table 8

**Comparison of Mixed Strategy Profiles for the No-IDS Case**

<table>
<thead>
<tr>
<th>Utility</th>
<th>Mixed Strategy Profiles</th>
</tr>
</thead>
</table>
| \( Utility = \alpha\mu \) Low Utility User | The firm’s optimal investigation probability, \( \rho = \frac{\alpha\mu}{\beta} \)  
The user’s optimal hacking probability, \( \psi = \frac{c}{a\phi} \) |
| \( Utility = \mu \) Cavusoglu et al. (2005)     | The firm’s optimal investigation probability, \( \rho = \frac{\mu}{\beta} \)  
The user’s optimal hacking probability, \( \psi = \frac{c}{a\phi} \) |
| \( Utility = \bar{\mu} \) Where \( \bar{\mu} = (P_H + ((1-P_H)\alpha)\mu \) | The firm’s optimal investigation probability, \( \rho = \frac{\bar{\mu}}{\beta} \)  
The low utility user’s optimal hacking probability, \( \psi_{Low} = \frac{c}{a\phi} \)  
The high utility user’s optimal hacking probability, \( \psi_{High} = \frac{c}{a\phi} \) |
Figure 4 models the transformation of the incomplete information game into one of imperfect information by assigning probabilities to represent the likelihood of the firm’s opponent being either the low or high utility user. The firm’s strategy is to investigate I, or not investigate NI, (i.e., \( S^F \in [I, NI] \)). The low and high utility users’ strategies are either to hack, H, or not hack, NH, (i.e., \( S^U_{Low} \in [H, NH] \) and \( S^U_{High} \in [H, NH] \)). The game is then solved as if the strategy spaces for the low and high utility users are \( I_J^{U_Low} \in [0,1] \) and \( I_J^{U_High} \in [0,1] \), respectively, and the strategy space for the firm is \( \rho \in [0,1] \).

Backwards induction was used to calculate the players’ optimal strategies in the Nash equilibrium. The low utility user’s hacking strategy \( \psi_{Low} = \frac{c}{\partial\phi} \) was derived by calculating the derivative of the firm’s expected cost against a low utility user (Equation 1) with respect to \( \rho \), setting it equal to 0 and solving for \( \psi_{Low} \).

\[
\frac{\partial F_{Low}(\rho, \psi_{Low})}{\partial \rho} = c + \psi_{Low}(1 - \phi)d + \psi_{Low}d = 0
\] (6)

Likewise, the high utility user’s hacking strategy \( \psi_{High} = \frac{c}{\partial\phi} \) was derived by calculating the derivative of the firm’s expected cost against a high utility user (Equation 2), setting it equal to 0 and solving for \( \psi_{High} \).

\[
\frac{\partial F_{High}(\rho, \psi_{High})}{\partial \rho} = c + \psi_{High}(1 - \phi)d + \psi_{High}d = 0
\] (7)

Deriving the firm’s optimal investigation strategy \( \rho = \frac{\psi}{\beta} \) was more complex because it must reflect the firm’s uncertainty regarding whether it will face the low or high utility user. The firm accounted for its incomplete information by calculating its optimal
investigation strategy against the low utility user ($\rho^{\text{Low}}$) and the high utility user ($\rho^{\text{High}}$) separately while utilizing the probabilities of facing each user type to determine the strategy it will play. The firm’s optimal strategy against the low utility user was derived by calculating the derivative of the user’s expected benefit of intrusion (Equation 4) with respect to $H_{\text{Low}}(\rho, \psi_{\text{Low}})$, setting it equal to 0,

$$\frac{\partial H_{\text{Low}}(\rho, \psi_{\text{Low}})}{\partial \psi} = \alpha \mu - \rho \beta = 0$$

(8)

and solving for $\rho$ where $\rho = \frac{\alpha \mu}{\beta}$. Similarly, the firm’s optimal strategy against the high utility user was derived by calculating the derivative of the user’s expected benefit of intrusion (Equation 5) with respect to $H_{\text{Low}}(\rho, \psi_{\text{High}})$, setting it equal to 0,

$$\frac{\partial H_{\text{High}}(\rho, \psi_{\text{High}})}{\partial \psi} = \mu - \rho \beta = 0$$

(9)

and solving for $\rho$ where $\rho = \frac{\mu}{\beta}$. The firm’s overall optimal strategy in light of experiencing incomplete information was then calculated as follows:

$$\rho = (1 - P_H)(\rho^{\text{Low}}) + P_H(\rho^{\text{High}}) = (1 - P_H) \left( \frac{\alpha \mu}{\beta} \right) + P_H \left( \frac{\mu}{\beta} \right) = \frac{\bar{\mu}}{\beta}, \text{ (where } \bar{\mu} \text{ equals } P_H + (1 - P_H)\alpha \mu)$$

(10)

Nash Equilibrium, IDS Case

The firm’s uncertainty regarding its opponent in the IDS case was also modeled as a game of incomplete information. Again, the user knows his or her true utility as they did
in the no-IDS case and chooses the hacking strategy as if he or she were playing a game of complete information. The low and high utility users’ expected benefits of intrusion are the following:

\[ H_{\text{Low}}(\rho_1, \rho_2, \psi_{\text{Low}}) = \psi_{\text{Low}} \alpha - \psi_{\text{Low}} \beta (\rho_1 P_D + \rho_2 (1 - P_D)) \]  
(11)

\[ H_{\text{High}}(\rho_1, \rho_2, \psi_{\text{High}}) = \psi_{\text{High}} \mu - \psi_{\text{High}} \beta (\rho_1 P_D + \rho_2 (1 - P_D)) \]  
(12)

In the IDS case, the IDS divided the parameter space into two distinct regions (alarm state and no-alarm state) where the user and firm played different strategies. The firm’s expected costs against the low and high utility users in the alarm state are as follows:

\[ F_{\text{Alarm}}^\text{Low}(\rho_1, \psi_{\text{Low}}) = (1 - P_H)(\rho_1 c + \eta_1 (1 - \rho_1)d + \eta_1 \rho_1 (1 - \phi)d) \]  
(13)

\[ F_{\text{Alarm}}^\text{High}(\rho_1, \psi_{\text{High}}) = (P_H)(\rho_1 c + \eta_1 (1 - \rho_1)d + \eta_1 \rho_1 (1 - \phi)d) \]  
(14)

The firm’s expected costs against the low and high utility users in the no-alarm state are as follows:

\[ F_{\text{NoAlarm}}^\text{Low}(\rho_2, \psi_{\text{Low}}) = (1 - P_H)(\rho_2 c + \eta_2 (1 - \rho_2)d + \eta_2 \rho_2 (1 - \phi)d) \]  
(15)

\[ F_{\text{NoAlarm}}^\text{High}(\rho_2, \psi_{\text{High}}) = P_H(\rho_2 c + \eta_2 (1 - \rho_2)d + \eta_2 \rho_2 (1 - \phi)d) \]  
(16)

The firm’s overall costs in the alarm and no-alarm states are as follows:

\[ F_{\text{Alarm}}(\rho_1, \psi_{\text{Low}}, \psi_{\text{High}}) = F_{\text{Alarm}}^\text{Low}(\rho_2, \psi_{\text{High}}) + F_{\text{Alarm}}^\text{High}(\rho_2, \psi_{\text{High}}) \]  
(17)

\[ F_{\text{NoAlarm}}(\rho_2, \psi_{\text{Low}}, \psi_{\text{High}}) = F_{\text{NoAlarm}}^\text{Low}(\rho_2, \psi_{\text{Low}}) + F_{\text{NoAlarm}}^\text{High}(\rho_2, \psi_{\text{High}}) \]  
(18)
The firm minimizes $F_{\text{Alarm}}(\rho_1, \psi_{\text{Low}}, \psi_{\text{High}})$ when the IDS generates an alarm and $F_{\text{NoAlarm}}(\rho_2, \psi_{\text{Low}}, \psi_{\text{High}})$ when the IDS does not generate an alarm. The low and high utility users’ maximize $H_{\text{Low}}$ and $H_{\text{High}}$, respectively. Similar to the no-IDS case, the firm has to choose a manual investigation strategy that accounts for its uncertainty regarding which opponent it faces. Proposition 2 gives the mixed strategy profiles in the Nash equilibrium for the IDS case.

Proposition 2. The following mixed strategy profiles constitute the Nash Equilibria for the incomplete information game in the IDS case.

When $P_D < \frac{\mu}{\beta}$,

$$\rho_1 = 1, \quad \rho_2 = \frac{\mu - P_D \beta}{(1 - P_D) \beta}, \quad \psi_{\text{Low}} = \frac{c(1 - P_F)}{c(P_D - P_F) + (1 - P_D)d\phi},$$

$$\psi_{\text{High}} = \frac{c(1 - P_F)}{c(P_D - P_F) + (1 - P_D)d\phi}$$

When $P_D \geq \frac{\mu}{\beta}$,

$$\rho_1 = \frac{\mu}{P_D \beta}, \quad \rho_2 = 0, \quad \psi_{\text{Low}} = \frac{cP_F}{P_D d\phi - c(P_D - P_F)},$$

$$\psi_{\text{High}} = \frac{cP_F}{P_D d\phi - c(P_D - P_F)}$$

The IDS divides the parameter space into two distinct operating regions where the firm and users play different strategies in the equilibrium. Proposition 2 shows that both the low and high utility user types played the same hacking strategy. Just as in the no-IDS case, the reduced utility experienced by the low utility user does not change the calculation of the firm’s optimal expected cost $\left(\frac{c}{\phi}\right)$, and the users play the strategy that
allows the firm to achieve this cost. The low and high utility users will hack with a
frequency proportional to \( \frac{c(1-P_F)}{c(P_D - P_F) + (1-P_D)d\Phi} \) in the no-alarm state \( (P_D < \frac{\mu}{\beta}) \) and
\( \frac{cP_F}{P_Dd\Phi - c(P_D - P_F)} \) in the alarm state \( (P_D \geq \frac{\mu}{\beta}) \). Manual investigation by the firm will occur
in the alarm state with a frequency proportional to \( \frac{P_D}{P_D\beta} \) when the IDS generates an alarm,
with no investigations taking place in the absence of an alarm. In the no-alarm state, all
users who generate an alarm are investigated, and users are randomly investigated with a
frequency proportional to \( \frac{P_D \beta}{(1-P_D)\beta} \) when the IDS does not generate an alarm.

When compared to the inspiring literature, modeling the game as one of incomplete
information results in identical hacking strategies by the low and high utility users. The
probability of manual investigation by the firm is again lowered by \( (P_H + (1 - P_H)\alpha) \) in
both the alarm and no-alarm states. Table 9 compares the mixed strategy equilibria of the
complete information game set forth by Cavusoglu et al. (2005), a complete information
game against the low utility user, and the incomplete information game modeled in
Figure 5.
### Table 9

**Comparison of Mixed Strategy Profiles for the IDS Case**

<table>
<thead>
<tr>
<th>Utility</th>
<th>Nash Equilibria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utility = $\mu$</td>
<td>When $P_D &lt; \frac{\mu}{\beta}$, $\delta_1 = 1, \delta_2 = \frac{\mu - P_D \delta}{(1 - P_D)\beta}$, $\psi = \frac{c(1 - P_F)}{c(P_D - P_F) + (1 - P_D)d\phi}$</td>
</tr>
<tr>
<td>Cavusoglu et al. (2005)</td>
<td>When $P_D \geq \frac{\mu}{\beta}$, $\delta_1 = \frac{\mu}{P_D \delta}, \delta_2 = 0$, $\psi = \frac{cP_F}{P_D d\phi - c(P_D - P_F)}$</td>
</tr>
<tr>
<td>Utility = $\alpha \mu$</td>
<td>When $P_D &lt; \frac{\mu}{\beta}$, $\delta_1 = 1, \delta_2 = \frac{a\mu - P_D \delta}{(1 - P_D)\beta}$, $\psi = \frac{c(1 - P_F)}{c(P_D - P_F) + (1 - P_D)d\phi}$</td>
</tr>
<tr>
<td>Low Utility User</td>
<td>When $P_D \geq \frac{\mu}{\beta}$, $\delta_1 = \frac{a\mu}{P_D \delta}, \delta_2 = 0$, $\psi = \frac{cP_F}{P_D d\phi - c(P_D - P_F)}$</td>
</tr>
<tr>
<td>Utility = $\tilde{\mu}$</td>
<td>When $P_D &lt; \frac{\tilde{\mu}}{\beta}$, $\delta_1 = 1, \delta_2 = \frac{\tilde{\mu} - P_D \delta}{(1 - P_D)\beta}$, $\psi_{Low} = \frac{c(1 - P_F)}{c(P_D - P_F) + (1 - P_D)d\phi}$</td>
</tr>
<tr>
<td>Where $\tilde{\mu} = (P_H + ((1 - P_H)\alpha)\mu$</td>
<td>$\psi_{High} = \frac{c(1 - P_F)}{c(P_D - P_F) + (1 - P_D)d\phi}$</td>
</tr>
<tr>
<td></td>
<td>When $P_D \geq \frac{\tilde{\mu}}{\beta}$, $\delta_1 = \frac{\tilde{\mu}}{P_D \delta}, \delta_2 = 0$</td>
</tr>
<tr>
<td></td>
<td>$\psi_{Low} = \frac{cP_F}{P_D d\phi - c(P_D - P_F)}$</td>
</tr>
<tr>
<td></td>
<td>$\psi_{High} = \frac{cP_F}{P_D d\phi - c(P_D - P_F)}$</td>
</tr>
</tbody>
</table>

Accounting for incomplete information causes the IDS to define a larger operating region for the alarm state ($P_D \geq \frac{\mu}{\beta}$) and a lower operating region for the no-alarm state ($P_D < \frac{\mu}{\beta}$) than in the complete information game modeled in the inspiring literature. Table 10 compares the newly defined operating regions to those of the complete information game.
set forth by Cavusoglu et al. (2005) and those of a complete information game against a low utility user.

Table 10

Comparing Operating Regions

<table>
<thead>
<tr>
<th>Operating Region</th>
<th>Utility = $\alpha \mu$ (Low Utility User)</th>
<th>Utility = $\bar{\mu}$ (Where $\bar{\mu} = (P_{H} + ((1-P_{H}) \alpha)\mu$)</th>
<th>Utility = $\mu$ (Cavusoglu et al. (2005))</th>
</tr>
</thead>
<tbody>
<tr>
<td>No-Alarm State</td>
<td>$P_D &lt; \frac{\alpha \mu}{\beta}$</td>
<td>$P_D &lt; \frac{\bar{\mu}}{\beta}$</td>
<td>$P_D &lt; \frac{\mu}{\beta}$</td>
</tr>
<tr>
<td>Alarm State</td>
<td>$P_D \geq \frac{\alpha \mu}{\beta}$</td>
<td>$P_D \geq \frac{\bar{\mu}}{\beta}$</td>
<td>$P_D \geq \frac{\mu}{\beta}$</td>
</tr>
</tbody>
</table>

Figure 5 models the transformation of the incomplete information game into one of imperfect information by assigning probabilities to represent the likelihood of the firm’s opponent being either the low or high utility user. The low and high utility users’ strategy space remains the same as in the no IDS case. The firm’s strategy space in the IDS case is more complex because the IDS separates the firm’s information into two sets: alarm and no-alarm. The firm has two actions, to investigate or not investigate, available in both the alarm and no-alarm states. The firm’s strategy space is the Cartesian product of the actions available at each of these sets: $S^F = \{(I, I), (I, NI), (NI, I), (NI, NI)\}$, where the first element in each pair specifies the firm’s action when the firm observes an alarm from the IDS, and the second element is the firm’s action when it does not observe an
alarm. The game is solved as if the strategy space for the low and high utility user are
\( \psi_{\text{Low}} \in [0,1] \) and \( \psi_{\text{High}} \in [0,1] \) with a strategy space for the firm
of \( (\rho_1, \rho_2) \in [0,1] \times [0,1] \). Lemma 1 from the inspiring literature holds true in the analysis
of the incomplete information game.

Lemma 1. Assuming that the IDS performs better than random guessing, that is \( P_D > P_F \), the frequency of manual investigation is always higher in the alarm state than in the
no-alarm state (i.e., \( \rho_1 \geq \rho_2 \)). Additionally, the firm may conduct manual investigation
in the no-alarm state only when it completely investigates all alarm states.

Lemma 1 shows that the firm will investigate a larger percentage of users who
generate alarms from the IDS than those who do not generate alarms. Manual
investigations are more efficient in the alarm state. The firm may only begin
investigating users who do not generate an alarm when the probability of manual
investigation in the alarm state is equal to one. As a result, the firm does not investigate
any user in the no-alarm state when the probability of manual investigation in the alarm
state is less than one. Accordingly, after the firm has exhausted its resources to
investigate all users in the alarm state, it can begin to investigate a portion of users in the
no-alarm state. The firm’s overall expected cost is calculated as follows:

\[
F_{\text{Cost}}(\rho_1, \rho_2, \psi) = (P_F + \psi (P_D - P_F))F_{\text{Alarm}}(\rho_1, \psi) + (1 - P_F - \psi (P_D - P_F))F_{\text{NoAlarm}}(\rho_2, \psi)
\]

The following probabilities were also used in calculating the mixed strategy Nash
equilibrium of the incomplete information game.
\[ \eta_1 = \text{Prob}(\text{Intrusion} \mid \text{Alarm}) = \frac{P_D \psi}{P_D \psi + P_F (1-\psi)} \]  
(20)

\[ \eta_2 = \text{Prob}(\text{Intrusion} \mid \text{No-Alarm}) = \frac{(1-P_D)\psi}{(1-P_D)\psi+(1-P_F)(1-\psi)} \]  
(21)

\[ \text{Prob}(\text{Alarm}) = P_F + \psi (P_D - P_F) \]  
(22)

\[ \text{Prob}(\text{Alarm}) = P_F + \psi (P_D - P_F) \]  
(23)

The low and high utility users continue to play a strategy that allows the firm to achieve its optimal cost, making the firm indifferent to investigating/not investigating user traffic. Backwards induction was used to calculate the low and high utility users’ optimal strategies in the alarm and no-alarm states. The low utility user’s hacking strategy in the alarm state \( \psi_{Low} = \frac{cP_F}{P_D d\phi - c(P_D-P_F)} \) was derived by calculating the derivative of the firm’s expected cost against a low utility user (Equation 13) with respect to \( \rho_1 \), setting it equal to 0 and solving for \( \psi_{Low} \).

\[ \frac{P_{Low}^{\text{Alarm}}(\rho_1, \rho_2, \psi_{Low})}{\partial \rho_1} = (c ((P_D - P_F) - d\phi P_D) \psi_{Low} + cP_F = 0 \]  
(24)

The high utility user’s hacking strategy in the alarm state \( \psi_{High} = \frac{cP_F}{P_D d\phi - c(P_D-P_F)} \) was derived by calculating the derivative of the firm’s expected cost against a high utility user (Equation 14) with respect to \( \rho_1 \), setting it equal to 0 and solving for \( \psi_{High} \).

\[ \frac{P_{High}^{\text{Alarm}}(\rho_1, \rho_2, \psi_{High})}{\partial \rho_1} = (c ((P_D - P_F) - d\phi P_D) \psi_{High} + cP_F = 0 \]  
(25)

Playing these strategies ensures that the firm has no incentive to change its investigation strategy, which is required to for the game to achieve Nash equilibrium.
The firm must derive an investigation strategy that accounts for the low and high utility users in both the alarm and no-alarm states \((\rho_1, \rho_2)\). The firm calculates its investigation strategy in the alarm state \((\rho_1)\) as the sum of \(\rho_1^{Low}\) played against the low utility user and \(\rho_1^{High}\) played against the high utility user. Likewise, the firm calculates its investigation strategy in the no-alarm state \((\rho_2)\) as the sum of \(\rho_2^{Low}\) played against the low utility user and \(\rho_2^{High}\) played against the high utility user. The firm then plays the game as if it is playing against one user who will experience the low utility user’s expected benefit of intrusion with a probability of \((1 - P_H)\) and the high utility user’s expected benefit of intrusion with a probability of \(P_H\).

\[
\rho_1 = (1 - P_H)(\rho_1^{Low}) + P_H(\rho_1^{High})
\]

\[
\rho_2 = (1 - P_H)(\rho_2^{Low}) + P_H(\rho_2^{High})
\]

The firm’s optimal investigation strategy against the low utility user in the alarm state \(\rho_1^{Low}\left(\frac{\alpha u}{\beta P_D}\right)\) was found the best strategy to maximize the user’s expected benefit of intrusion. The firm derives the low utility user’s optimal benefit of intrusion by calculating the derivative of the low utility user’s expected benefit of intrusion (Equation 11) with respect to \(\psi_{Low}\), setting it equal to 0, setting \(\rho_2\) equal to 0 (per Lemma 1), and solving for \(\rho_1^{Low}\).

\[
\frac{F_{Alarm}(\rho_L, \psi_{Low})}{\partial \psi} = \alpha \mu - \beta (\rho_1 P_D + \rho_2 (1 - P_D)) = 0
\]

The firm derives its optimal investigation strategy against the low utility user in the no-alarm state \(\rho_2^{Low}\left(\frac{\alpha u - \beta P_D}{\beta (1 - P_D)}\right)\) as the best strategy to maximize the user’s expected benefit of intrusion.
intrusion. The firm calculates the low utility user’s optimal benefit in the no-alarm state by calculating the derivative of the low utility user’s expected benefit of intrusion (Equation 11) with respect to $\psi_{\text{Low}}$, setting it equal to 0, setting $\rho_1$ equal to 1 (per Lemma 1), and solving for $\rho_2^{\text{Low}}$.

$$\frac{\partial}{\partial \psi} I^{\text{Low}}_{\text{No Alarm}}(\rho_2, \psi_{\text{Low}}) = \alpha \mu - \beta \left( \rho_1 P_D + \rho_2 (1 - P_D) \right) = 0 \quad (29)$$

The firm derives its optimal investigation strategy against the high utility user in the alarm state $\rho_1^{\text{High}} \left( \frac{u}{\beta P_D} \right)$ as the best strategy to maximize the user’s expected benefit of intrusion. The firm derives the high utility user’s optimal benefit of intrusion by calculating the derivative of the high utility user’s expected benefit of intrusion (Equation 12) with respect to $\psi_{\text{High}}$, setting it equal to 0,

$$\frac{\partial}{\partial \psi} H^{\text{High}}(\rho_1, \rho_2, \psi_{\text{High}}) = \mu - \beta \left( \rho_1 P_D + \rho_2 (1 - P_D) \right) = 0 \quad (30)$$

setting $\rho_2$ equal to 0 (per Lemma 1), and solving for $\rho_1^{\text{High}}$. The firm derives its optimal investigation strategy against the high utility user in the no-alarm state $\rho_2^{\text{High}} \left( \frac{u - \beta P_D}{\beta (1 - P_D)} \right)$ as the best strategy to maximize the user’s expected benefit of intrusion. The firm derives the high utility user’s optimal benefit of intrusion by calculating the derivative of the high utility user’s expected benefit of intrusion (Equation 12) with respect to $\psi_{\text{High}}$, setting it equal to 0, setting $\rho_1$ equal to 1 (per Lemma 1), and solving for $\rho_2^{\text{High}}$.

$$\frac{\partial}{\partial \psi} H^{\text{High}}(\rho_1, \rho_2, \psi_{\text{High}}) = \mu - \beta \left( \rho_1 P_D + \rho_2 (1 - P_D) \right) = 0 \quad (31)$$
Because the firm plays the game as if it were playing against one user who will experience the low utility user’s expected benefit with a probability of \((1 - P_H)\) and the high utility user’s expected benefit with a probability of \(P_H\), the firm calculates its optimal investigation strategies \(\rho_1\) and \(\rho_2\) given the probability of facing each opponent as follows where \(\bar{\mu} = (P_H + (1 - P_H)\alpha)\mu): \[
\rho_1 = (1 - P_H) \left( \frac{\alpha u}{\beta P_D} \right) + P_H \left( \frac{u}{\beta P_D} \right) = \frac{\bar{\mu}}{\beta P_D} \tag{32}
\]
\[
\rho_2 = (1 - P_H) \left( \frac{\alpha u - \beta P_D}{\beta(1 - P_D)} \right) + P_H \left( \frac{u - \beta P_D}{\beta(1 - P_D)} \right) = \frac{\bar{\mu} - \beta P_D}{\beta(1 - P_D)} \tag{33}
\]

**Comparison of IDS and No-IDS Cases**

The detection and hacking rates were analyzed to further understand the effects of implementing an IDS when the firm faces incomplete information and to determine whether these effects differ from those of the inspiring literature. Proposition 3 compares the IDS and no-IDS incomplete information games.

**Proposition 3.** *The IDS and No-IDS cases compared.*

- i. \(\rho_2 \leq \rho \leq \rho_1\)
- ii. The probability of detecting a hacker is the same in the IDS case
- iii. The hacking probability is higher in the IDS case when \(P_D < \frac{\bar{\mu}}{\beta}\) and lower when \(P_D \geq \frac{\bar{\mu}}{\beta}\)

The effective detection rate is identical in the IDS and no-IDS cases when the firm models incomplete information because the firm’s optimal strategy remains to make the user indifferent to hacking/not hacking. Although the probability of detecting a hacker is
the same regardless of whether or not the firm implements an IDS, the hacking probability is higher in the IDS case when \( P_D < \frac{\mu}{\beta} \) and lower when \( P_D \geq \frac{\mu}{\beta} \). The effects of implementing an IDS when the firm is faced with incomplete information are identical to those in the complete information game set forth by Cavusoglu et al. (2005). However, the results differ in that new operating regions are derived for the alarm and no-alarm states.

Proposition 3 reveals that when accounting for incomplete information, the IDS defines a smaller operating region where the hacking rate is higher in the IDS case \( (P_D < \frac{\mu}{\beta}) \) and a larger operating region where the hacking rate is lower than in the no-IDS case \( (P_D \geq \frac{\mu}{\beta}) \). Table 11 compares the detection and hacking rates between the IDS and no-IDS cases when accounting for incomplete information with those of the inspiring literature.
Table 11

**Effects of Implementing IDS**

| Detection Rate | Utility = \( \mu \)  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[Detection Rate(<em>{NO-IDS})] = [Detection Rate(</em>{IDS})]</td>
<td>Cavasoglu et al. (2005)</td>
</tr>
</tbody>
</table>
| Hacking Rate | Utility = \( \bar{\mu} \)  
| The hacking probability is higher if \( P_D < \frac{\mu}{\beta} \) | Where \( \bar{\mu} = (P_H + (1-P_H)\alpha)\mu \)  
| The hacking probability is lower if \( P_D \geq \frac{\mu}{\beta} \) |  
| [Detection Rate\(_{NO-IDS}\)] = [Detection Rate\(_{IDS}\)] |  

The detection rate remains the same between the IDS and no-IDS cases. The user is only affected by the firm’s strategy through the detection rate, which determines the probability that a hacker will be detected. As a result, the firm adjusts its strategy in the incomplete information game to keep the same level of detection in the IDS case as the no-IDS case just as it did when modeling complete information. The firms sets \( \bar{\mu} - \beta \rho = \bar{\mu} - \beta [Detection \ Rate\(_{NO-IDS}\)] = 0 \) in the no-IDS case and \( \bar{\mu} - \beta (\rho_1 P_D + \rho_2 (1 - P_D)) \) \( = \bar{\mu} - \beta [Detection \ Rate\(_{IDS}\)] = 0 \) in the IDS case.

The firm, however, plays a different investigation strategy in the IDS case to ensure the same level of detection is achieved by first allocating investigative resources to the alarm state before they are allocated to the less efficient no-alarm state. Compared to the no-IDS case, the hacking probability continues to be higher when \( P_D < \frac{\bar{\mu}}{\beta} \) and lower when
$P_D \geq \frac{\mu}{\beta}$. This result occurs because the users’ strategies in the equilibrium make the firm indifferent to investigating/not investigating user traffic. As a result, the users adjust their hacking rate accordingly in the different operating regions to ensure the firm remains indifferent.

**Value of Default Configuration**

Choosing to implement an IDS without configuring the detection rate or in cases where the IDS is not configurable benefits the firm only if it realizes added value when compared to the no-IDS case presented in Proposition 1. Proposition 4 summarizes the value of an IDS when the configuration is assumed to be exogenous.

**Proposition 4.** *The default configuration case.*

1. *The value of IDS is nonnegative when $P_D \geq \frac{\mu}{\beta}$*
2. *The value of IDS is negative when $P_D < \frac{\mu}{\beta}$*

Proposition 4 demonstrates that implementing an IDS without configuring the IDS to complement the operating environment is detrimental to the firm when $P_D < \frac{\mu}{\beta}$ even though the IDS performs better than random guessing because the investigation cost increases with the investigation rate and the damage cost increases with the hacking probability. Implementing an IDS when $P_D \geq \frac{\mu}{\beta}$ results in the firm experiencing a lower
cost than in the no-IDS case because the investigation rate and hacking probability are lower.

The results are identical to those of the complete information game set forth by Cavusoglu et al. (2005) aside from the newly defined operating regions that represent the alarm and no-alarm states. Proposition 4 shows that modeling incomplete information results in a larger operating region that returns a positive value to the firm when \( P_D \geq \frac{\bar{u}}{\bar{p}} \), and a smaller operating region that is detrimental to the firm when \( P_D < \frac{\bar{u}}{\bar{p}} \) when compared to the inspiring literature. Table 12 compares the value of IDS using its default configuration when accounting for incomplete information with the value of IDS under the assumption of complete information.

Table 12

<table>
<thead>
<tr>
<th>The Default Configuration Case</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Utility = ( \mu )</strong></td>
</tr>
<tr>
<td><em>Cavusoglu et al. (2005)</em></td>
</tr>
<tr>
<td>The value of the IDS is negative when ( P_D &lt; \frac{\mu}{\bar{p}} )</td>
</tr>
<tr>
<td>The value of the IDS is nonnegative when ( P_D \geq \frac{\mu}{\bar{p}} )</td>
</tr>
</tbody>
</table>
The value of an IDS is calculated as the expected cost without the IDS minus the expected cost with the IDS. Plugging the results of Proposition 2 into equation 19 gives the firm’s expected cost of
\[
\left(\frac{c}{\phi}\right) \left(\frac{1-(\phi(1-c\phi d)P_D)^* (1-\phi (1-c\phi d)P_F)}{1-(\phi d)P_F+(1-c\phi d)P_D}\right)
\]
when \( P_D < \frac{\bar{\mu}}{\beta} \) and
\[
\left(\frac{1}{\phi\phi d} \frac{1}{1-c\phi d} P_D P_F \right)
\]
when \( P_D \geq \frac{\bar{\mu}}{\beta} \). These costs hold true regardless of which opponent type the firm faces in the alarm and no-alarm states. Subtracting these costs from the firm’s cost in the no-IDS case results in a negative value of
\[
-\left(\frac{c}{\phi}\right) \left(\frac{(P_D-P_F)(1-\phi)(d\phi-c)}{d\phi-(d\phi-c)P_D+cP_F}\right)
\]
when \( P_D < \frac{\bar{\mu}}{\beta} \) and a positive value of \( \left(\frac{c}{\phi}\right) \left(\frac{(P_D-P_F)(d\phi-c)}{P_D d\phi-c(P_D-P_F)}\right) \) when \( P_D \geq \frac{\bar{\mu}}{\beta} \).

**Value of Optimal Configuration**

Assuming that the IDS is configurable, the firm can choose to configure the IDS by setting the value of \( P_D \) and subsequently \( P_F \). Proposition 2 shows that the firm can be in one of two regions using the default configuration where \( P_D \geq \frac{\bar{\mu}}{\beta} \) or \( P_D < \frac{\bar{\mu}}{\beta} \). The firm incurs a lower cost when \( P_D \geq \frac{\bar{\mu}}{\beta} \) and should consequently choose a value that falls in this operating region. The firm must also decide where in this operating region \( P_D \) should fall to maximize the value of optimal configuration. Proposition 5 highlights the importance of optimally configuring an IDS and its benefit to a firm.

**Proposition 5.** The value of optimal configuration.
i. The value of the optimally configured IDS is strictly nonnegative.

ii. The firm configures the IDS to investigate all users who generate alarms from the IDS ($\rho_1 = 1$) and none of the users who do not generate alarms ($\rho_2 = 0$).

iii. The firm sets the detection rate equal to $P_D = \frac{\mu}{\beta}$ in the optimal configuration case.

Proposition 5 provides strong support for the claim that firms should configure their IDS whenever possible to ensure they receive a positive return on investment. Proposition 4 demonstrates that implementing an IDS using its default configuration can be detrimental to the firm if $P_D < \frac{\mu}{\beta}$, whereas the value of an optimally configured IDS is strictly nonnegative. An optimally configured (imperfect) IDS also yields the same manual investigation strategy as the perfect IDS ($P_D = 1, P_F = 0$) by configuring the IDS to investigate all users who generate an alarm and none of the users who do not (Cavusoglu et al., 2005). The optimal configuration for the incomplete information game yields an identical manual investigation strategy ($\rho_1 = 1, \rho_2 = 0$) as the inspiring literature.

The value of optimal configuration when accounting for incomplete information is higher than the value demonstrated in the complete information game set forth by Cavusoglu et al. (2005). The increase in value can be attributed to the results of Proposition 4, which define a larger operating region that returns a positive value to the firm when $P_D \geq \frac{\mu}{\beta}$. As a result, when the firm has to account for the potential of facing a lower utility opponent, the optimal detection rate ($P_D = \frac{\mu}{\beta}$) is configured at a value that is unobtainable in the model set forth by Cavusoglu et al. (2005) because it takes advantage
of the newly defined (larger) operating region that returns a positive value of IDS. Table 13 compares the value of optimal configuration between the two games.

Table 13

<table>
<thead>
<tr>
<th></th>
<th>Utility = $\mu$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cavusoglu et al. (2005)</td>
<td>$\frac{c}{\phi} \left( 1 - \frac{d\phi}{(\frac{\mu}{\beta})^{1-\frac{1}{r}}} + \left( 1 - \left( \frac{\mu}{\beta} \right)^{1-\frac{1}{r}} - c \right) \right)$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Utility = $\bar{\mu}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where $\bar{\mu} = (P_H + (1-P_H)\alpha)\mu$</td>
<td>$\frac{c}{\phi} \left( 1 - \frac{d\phi}{(\frac{\mu}{\beta})^{1-\frac{1}{r}}} + \left( 1 - \left( \frac{\mu}{\beta} \right)^{1-\frac{1}{r}} - c \right) \right)$</td>
</tr>
</tbody>
</table>

Proposition 3 shows that the IDS returns a positive return to the firm when $P_D \geq \frac{\bar{\mu}}{\beta}$ with the firm experiencing a cost of $\frac{c}{\phi} \frac{d\phi}{\phi} + \left( 1 - \frac{c}{\phi} \right) P_D$, which simplifies to $\frac{cdP_F}{P_D(d\phi-c)+cP_D^{1/r}}$. Given that $P_D = P_F^r$ and $P_D = P_D^{1/r}$, writing the cost as a function of $P_D$ returns a cost of $\frac{cdP_D^{1/r}}{P_D(d\phi-c)+cP_D^{1/r}}$. The firm has to decide where in this region $P_D$ should lie. To determine what value to assign to $P_D$, the firm takes the derivative of the cost function and sets it greater than or equal to 0.

$$\frac{d}{P_D} F_{\text{Cost}} = -\frac{cd(d\phi-c)P_D^{1/r}}{(d\phi-c)P_D+cP_D^{1/r}} \geq 0$$  (34)
The derivate implies that the firm should set $P_D$ as small as possible. To set the value of $P_D$ as small as possible and remain in the operating region where $P_D \geq \frac{\mu}{\beta}$, the firm optimally configures the IDS by setting $P_D = \frac{\mu}{\beta}$ and subsequently $P_E = \left(\frac{\mu}{\beta}\right)^{1/r}$.

**Achieving Nash Equilibrium**

The most interesting circumstance the firm faces is that where the firm’s probability of detection lies between its optimal detection rates for the low and high utility users. In this scenario the probability of detection lies in the range where $\frac{\alpha u}{\beta} < P_D < \frac{\mu}{\beta}$ for the IDS case and $\frac{\alpha u}{\beta} < \rho < \frac{\mu}{\beta}$ for the no-IDS case. Proposition 1 defines a detection rate of $\rho = \frac{\mu}{\beta}$ in the equilibrium for the no-IDS case and Proposition 5 defines the optimal configuration in the IDS case as $P_D = \frac{\mu}{\beta}$. However, the equilibria defined in Proposition 1 and Proposition 2 are not achievable over multiple iterations of the game because the firm does not face a combination of the low and high utility users as the game progresses. Instead, the firm faces the same user of low or high utility as the game advances over time. This scenario is analyzed to determine how many game iterations are needed to achieve equilibrium and whether it is possible for the firm to determine which type of opponent it faces.

In the no-IDS case, $\frac{\alpha u}{\beta} \leq \rho$ implies that $P_H$ could potentially equal 0, and $\rho \leq \frac{\mu}{\beta}$ implies that $P_H$ could potentially equal 1. In the IDS case, $\frac{\alpha u}{\beta} \leq P_D$ implies that $P_H$ could
potentially equal 0, and \( P_D \leq \frac{\mu}{\beta} \) implies \( P_H \) could potentially equal 1. These extreme situations were ignored, and the interesting regions where \( \frac{\alpha \mu}{\beta} < P_D < \frac{\mu}{\beta} \) in the IDS case and \( \frac{\alpha \mu}{\beta} < \rho < \frac{\mu}{\beta} \) in the no-IDS case were analyzed. The firm must determine if equilibrium is achievable for the duration of the game and devise a method for doing so. Proposition 6 summarizes the findings when the firm’s detection rate falls into the aforementioned ranges.

**Proposition 6.** Achieving equilibrium when the firm’s probability of detection lies between its optimal detection rates for the low and high utility users.

i. The firm is able to measure either its cost (no-IDS case) or the value of IDS (IDS case) after the game’s first iteration and determine whether it faces a high or low utility opponent.

ii. Within one game iteration, the firm is able to adjust \( P_H \) to ensure it plays a manual investigation strategy that achieves Nash equilibrium for the remainder of the game’s duration.

iii. After the first iteration of the incomplete information game is played, the game returns to one of complete information.

Proposition 6 shows that the firm is able to sacrifice the first iteration of the game to determine whether its opponent is a low or high utility user. The firm then adjusts the probability of facing a high utility user \( P_H \) to 1 if it determines that the opponent was a high utility user or to 0 to reflect the low utility user. Identifying the firm’s true opponent type, and adjusting \( P_H \) accordingly, transforms the game back into a complete information game, and equilibrium will be achieved throughout future game iterations. These results hold true in both the no-IDS and IDS cases.

In the no-IDS case, ignoring the extreme cases where \( P_H \) is equal to 1 or 0, the firm’s detection rate falls in the range \( \frac{\alpha \mu}{\beta} < \rho < \frac{\mu}{\beta} \). The firm plays the first iteration of the game
and analyzes its cost to determine the type of opponent it faced. Proposition 1 demonstrates that the high utility user becomes indifferent to hacking/not hacking when the firm investigates users with a probability of $\rho = \frac{\mu}{\beta}$, whereas the low utility user becomes indifferent when $\rho = \frac{\alpha\mu}{\beta}$. It is easy to see that the high utility opponent will be given incentive to hack when $\rho < \frac{\mu}{\beta}$. Similarly, the low utility opponent will no longer remain indifferent when $\rho > \frac{\alpha\mu}{\beta}$ and will be discouraged from hacking. The firm’s cost after the game’s first iteration will reflect its opponent’s strategy to hack or not hack, which can then be used to determine whether it faced a high or low utility opponent. The firm can then adjust $P_H$ accordingly to ensure it plays its optimal strategy against its true opponent. The game is then transformed into one of complete information, and equilibrium is achieved throughout future iterations.

In the IDS case, ignoring the extreme cases where $P_H$ is equal to 1 or 0, the firm’s detection rate falls in the range $\frac{\alpha\mu}{\beta} < P_D < \frac{\mu}{\beta}$. Proposition 4 shows that $P_D$ can be in one of two operating regions when it plays against the low utility user. The value of IDS is positive when $P_D \geq \frac{\alpha\mu}{\beta}$ and negative when $P_D < \frac{\alpha\mu}{\beta}$. Proposition 4 also shows that the value returned from the IDS will be positive when $P_D \geq \frac{\mu}{\beta}$ and negative when $P_D < \frac{\mu}{\beta}$ when the firm faces the high utility user. Given that $\frac{\alpha\mu}{\beta} < P_D < \frac{\mu}{\beta}$, the IDS will return a positive value when it faces a low utility opponent ($P_D \geq \frac{\alpha\mu}{\beta}$) and a negative value when it faces a high utility opponent ($P_D < \frac{\mu}{\beta}$). As a result, the firm can measure the value
returned from its IDS after the game’s first iteration and determine which type of user it faced. The firm can then adjust $P_H$ accordingly to ensure it plays its optimal investigation strategy against its true opponent. The game is then transformed into one of complete information, and equilibrium is achieved throughout future game iterations.

**Summary**

Propositions 1 through 6 demonstrate the value of IDS when the firm is uncertain of the utility of intrusion available to the user by utilizing Harsanyi transformation analysis to model games of incomplete information and perform backwards induction to derive the players’ mixed strategy profiles in the Nash equilibrium. The firm’s opponent is modeled as either a high utility user experiencing a utility of $\mu$ or a low utility user receiving a lower utility of $\alpha\mu$ where $0 < \alpha < 1$. Utilizing the Harsanyi method, the firm assigns probabilities to the likelihood of playing the game against a low or high utility user. Although the firm is uncertain which opponent it will face, the user is aware of his or her type (low or high utility) when the game begins and chooses a strategy accordingly. The resulting hacking strategies for both the low and high utility users mimic those of the complete information game modeled in the inspiring literature. The firm, however, is forced to adjust its manual investigation strategies in both the IDS and no-IDS cases for the games to achieve Nash equilibrium.

The probability of manual investigation in the IDS and no-IDS cases is lowered by a weighted coefficient $(P_H + (1 - P_H)\alpha)$ reliant upon the initial probability assigned to the
The likelihood of facing a high utility user. Accounting for the firm’s uncertainty also forces the IDS to define new operating regions for the alarm state \( P_D \geq \frac{\bar{\mu}}{\beta} \) and no-alarm state \( P_D < \frac{\bar{\mu}}{\beta} \), whose bounds are also lowered by \( (P_H + (1 - P_H)\alpha) \). When comparing the IDS and no-IDS cases, the detection rates are identical. The value of an IDS using its default configuration is calculated as the firm’s cost in the IDS case subtracted from the firm’s cost in the no-IDS case, showing that the value of IDS is negative when \( P_D < \frac{\bar{\mu}}{\beta} \) and nonnegative when \( P_D \geq \frac{\bar{\mu}}{\beta} \). The optimal configuration of the IDS when the firm accounts for its incomplete information is achieved by setting the detection rate equal to \( P_D = \frac{\bar{\mu}}{\beta} \). An optimally configured IDS investigates all user traffic that generates an alarm and none of the user traffic that does not. The value of optimal configuration is strictly nonnegative, with the firm realizing a higher value than that modelled in the inspiring literature.

The firm’s optimal configuration in the Nash equilibrium for the incomplete information game sets the detection rate equal to \( P_D = \frac{\bar{\mu}}{\beta} \), which lies between the firm’s optimal detection rates when playing complete information games against the low utility user \( \left( \frac{a\mu}{\beta} \right) \) and the high utility user \( \left( \frac{\mu}{\beta} \right) \). When \( \frac{a\mu}{\beta} < P_D < \frac{\mu}{\beta} \), the firm is faced with the challenge of determining what type of opponent it faces and devising a method for adjusting its strategy to ensure equilibrium is achieved in future game iterations. The firm solves this dilemma by playing the first iteration of the game, evaluating its cost (no-IDS case) and the value received from the IDS (IDS case), and adjusting the value of \( P_H \)
accordingly to ensure that the firm plays its optimal strategy throughout the rest of the game. These results hold true in both the IDS and no-IDS cases.
Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

The mixed strategy Nash equilibria presented in Propositions 1 and 2 answered Research Question 1 by defining the conditions under which Nash equilibrium was achieved for the no-IDS and IDS games of incomplete information. An interesting result is that although the firm’s investigation strategies changed when modeling incomplete information, both the low and high utility users played the same hacking strategy as the user in the complete information game modeled in the inspiring literature. The result can be explained by the fact that when the firm uses the expected utility of the user as its estimate of the user’s utility, the firm’s optimal expected cost \( \frac{\mu}{\phi} \) under Nash equilibrium is independent of the user’s utility. Although the firm’s overall expected cost function is weighted to represent the probability of facing each user type, the firm’s actual cost calculations were identical to those under the assumption of complete information once the game was played (and a user was chosen), regardless of the user’s type. As a result, both the high and low utility users played the same hacking strategy to ensure the firm remained indifferent to investigating/not investigating traffic.

Modeling the firm’s uncertainty using Harsanyi transformation analysis enabled the firm to transform its game of incomplete information into one of complete, but imperfect,
information so that the game’s Nash equilibrium could be analyzed. To account for its uncertainty, the firm adjusted its investigation probabilities in both the IDS and no-IDS cases by a value of \((P_H + (1 - P_H)\alpha)\), assuming a game of perfect information against a user with a utility of \(\bar{\mu}\).

This study confirmed previous claims that the hacking rate and investigation rate continue to increase in \(\frac{\bar{\mu}}{\beta}\) and \(\frac{c}{d\phi}\) when modeling incomplete information. An increase in \(\frac{c}{d\phi}\) implies a less efficient manual investigation while an increase in \(\frac{\bar{\mu}}{\beta}\) implies a higher expected benefit of intrusion to the user. Propositions 1 through 6 combined to answer Research Question 2 by validating previous findings that the user’s hacking incentives and the firm’s external parameters continue to have more of an effect on the value of IDS than the firm’s cost parameters. The most influential parameters are presented in Table 14.
Table 14

*Conditions Having the Most Effect on the Value of IDS*

<table>
<thead>
<tr>
<th>Hacking Incentives</th>
<th>External Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>• $\mu$ - Utility of intrusion for high utility users</td>
<td>• $P_H$ - Probability the firm faces a high utility user</td>
</tr>
<tr>
<td>• $\beta$ - Hacker penalty for detection</td>
<td>• $P_L$ - Probability the firm faces a low utility user ($1 - P_H$)</td>
</tr>
<tr>
<td>• $\alpha$ - The low utility user experiences a benefit of $\alpha \mu$ where $0 &lt; \alpha &lt; 1$</td>
<td></td>
</tr>
</tbody>
</table>

Proposition 3 compared the IDS and no-IDS cases, demonstrating that improper configuration encouraged hacking with the hacking probability being higher when $P_D < \frac{\mu}{\beta}$ and lower when $P_D \geq \frac{\mu}{\beta}$. The firm’s optimal configuration, calculated in Proposition 5, was achieved by setting the detection rate equal to $P_D = \frac{\mu}{\beta}$. Given that $\bar{\mu} = (P_H + (1 - P_H)\alpha)\mu$, the value of optimal configuration and its configuration settings were also dictated by the parameters presented in Table 14.

The results of Proposition 4 answered Research Question 3 by defining the conditions in which the firm benefited from implementing unconfigured IDS when modeling incomplete information. Model analysis demonstrated that the value of IDS is negative when $P_D < \frac{\mu}{\beta}$ and nonnegative when $P_D \geq \frac{\mu}{\beta}$. These results are similar to the findings of Cavusoglu et al. (2005) with one major difference. Given that $\frac{\bar{\mu}}{\beta} < \frac{\mu}{\beta}$, accounting for the
firm’s uncertainty resulted in a larger operating region where the firm benefited from implementing an IDS. Although Proposition 5 validated previous findings that firms should always choose to implement optimally configured IDS, an interesting conclusion is that the firms that accurately model their incomplete information are less likely to suffer from implementing out-of-the-box IDS solutions.

Proposition 6 answered Research Question 4 by analyzing the scenario where the firm’s probability of detection lies between its optimal detection rates for the high and low utility users. Although the Nash equilibrium was calculated for the no-IDS and IDS cases in Propositions 1 and 2, the firm is not playing its optimal investigation strategies once the game begins because the firm does not face a combination of high and low utility users as the game progresses. Instead, the firm faces one user of either high or low utility and continues to face that same user type as the game continues. Utilizing the results of Propositions 1 and 2 along with the optimal configuration derived in Proposition 5, further analysis demonstrated that the models set forth in this dissertation can be used by a firm to identify its opponent’s true type and ensure that equilibrium is achieved throughout future game iterations.

By optimally configuring the IDS where \( P_D = \frac{\bar{\mu}}{\bar{\beta}} \) with \( P_D \) falling in the range where \( \frac{\alpha \mu}{\beta} < P_D < \frac{\mu}{\beta} \), the firm is able to measure the value returned by the IDS after the game’s first iteration and determine whether it faces a high or low utility user. Proposition 4 demonstrated that the IDS returns a negative value when \( P_D < \frac{\mu}{\beta} \), indicating that the firm is facing a high utility user, and a positive value when \( P_D > \frac{\alpha \mu}{\beta} \), indicating that the firm
facing a low utility user. Remembering that $\bar{\mu} = (P_H + (1 - P_H)\alpha)\mu$, the firm can then set the value of $P_H$ to either 1 or 0 to transform the game back into one of complete information and play its optimal investigation strategy against the high or low utility user accordingly. The firm is then able to play its optimal investigation strategy throughout the remainder of the game, and equilibrium is achieved.

Proposition 5 answered Research Question 5 by calculating the firm’s optimal detection rate to be $P_D = \frac{\bar{\mu}}{\beta}$ and analyzing the value of optimal configuration. The results of Proposition 5 validated previous findings that the value of optimal configuration is strictly nonnegative, allowing the firm to minimize its cost and deter hackers, which also reduces the need for manual investigation. Proposition 5 also demonstrated that accurately accounting for the firm’s incomplete information yields a lower cost and a higher value of optimal configuration than the results set forth in previous literature. The increase in value can be attributed to the newly defined operating regions in Proposition 4, where the firm benefits if $P_D > \frac{\mu}{\beta}$. Given that $\frac{\mu}{\beta} < \frac{\bar{\mu}}{\beta}$, the beneficial operating region is larger than previously defined under the assumption of complete information ($P_D > \frac{\mu}{\beta}$).

As a result, the firm’s optimal configuration, $P_D = \frac{\bar{\mu}}{\beta}$, utilized a value that was impractical in the inspiring literature because it lay in the region that was detrimental to the firm.

The strengths of this study are in its ability to utilize game-theoretic models to derive the value of IDS, determine the players’ optimal strategies, and provide a framework for achieving equilibrium in information security games of incomplete information. Unlike previous research, the game-theoretic models of this study allow the firm to calculate its
optimal investigation strategies when faced with uncertainty, helping to further validate the use of game-theoretical analysis for IT security management. Propositions 1-6 provided a methodology for firm’s implementing IDS to analyze the value returned, achieve optimal configuration, and identify the conditions needed to account for the firm’s uncertainty. Other strengths of the study include the framework provided for transforming incomplete information into imperfect information, analyzing the game’s initial results, and transforming the game back into one of complete information where equilibrium is achieved throughout the remainder of the game.

This study also contained several limitations and assumptions. The firm and users were assumed to be risk neutral, and utility was consequently assumed to be a linear function of benefits, which eliminated scenarios in which the firm was risk averse regarding critical assets or the potential hacker was a risk seeker. The study also assumed that all of the game’s parameters besides the user’s utility of intrusion were common knowledge, which is often not the case in real-world scenarios. Manual investigations were assumed to confirm or rule out intrusions with certainty, which may also not be the case in practice.

Implications

This study provides several contributions to the IT security research community by demonstrating the benefits of accounting for uncertainty and validating the use of game-theoretical analysis for IT security management. Analysis of the changes in equilibrium and the number of game iterations required to achieve equilibrium demonstrate the
proposed models’ ability to be used as a tool for identifying the firm’s true opponent type, configuring IDS accordingly, and ensuring that equilibrium is achieved. The firm’s ability to make this determination while facing uncertainty also provides further insight into the benefits and consequences associated with the different methods of operating these devices.

This study’s results also provide several contributions to professional practice. One of the biggest contributions of the study is the presentation of game-theoretic models that provide a more realistic methodology for assessing the value of IDS and potentially for the evaluation of other security devices. In professional practice, firms are charged with protecting their assets from malicious users whose benefit of intrusion varies based on their different motivations and skill levels. The Bayesian games of incomplete information modeled in this dissertation contribute to the current body of knowledge and professional practice by presenting a methodology for deriving the value of a firm’s IDS and determining its optimal monitoring strategies to supplement IT security planning in light of the firm’s uncertainty.

Further insight is afforded for security engineers tasked with implementing IDS in these environments by highlighting the significance of understanding hacker behavior and motivation. The results of this study show that when accounting for incomplete information, the firm realizes a positive value from IDS only when the detection rate is higher than a critical value determined by the probability of defending against different hacker types and their individual utility and penalty parameters. Accounting for uncertainty ultimately results in the firm’s configuration lying in a range where it under-
investigates some users and over-investigates other users. Demonstrating that the firm’s uncertainty regarding its opponent can be virtually eliminated after one game iteration allows the firm to adjust to its optimal configuration and investigation strategies accordingly, shedding light on concerns regarding the value of implementing IDS in more practical scenarios where all of the game’s parameters are not common knowledge.

This study also provides valuable insight for future research. Analysis of the incomplete information games modeled in this dissertation validate previous findings that suggest that the user’s hacking incentives and the game’s external environment play the most significant roles in determining whether IDS should be deployed and how it should be configured. As a result, emphasis should be placed on analyzing hacking incentives and the operating environments in question when utilizing game theory as a tool for deriving the value of other security devices. This declaration holds true regardless of the level of uncertainty (if any) experienced by the game’s players. The successful modeling of incomplete information games, where the firm potentially faces several opponent types, also further validates game theory as a viable tool for modeling security games.

The framework provided can easily be used as a baseline for future modeling of security games experiencing incomplete information with numerous opponent types.

**Recommendations**

The conclusions of this study lend themselves to several recommendations for professional practice. Perhaps the most important recommendation for firms choosing to implement IDS is that they dedicate sufficient resources to analyzing the hacking
incentives and incorporate these findings into their optimal configuration settings.

Proposition 5 shows that the optimal configuration, $P_D = \frac{\mu}{\beta}$, is dependent upon the user’s hacking incentives. Although the firm’s cost parameters affect the value of IDS, they do not affect the optimal configuration. Furthermore, Proposition 4 demonstrates that the IDS can be detrimental to the firm when the detection rate is lower than a critical value defined by the IDS ($P_D < \frac{\mu}{\beta}$), placing even more emphasis on the importance of optimal configuration. Moorkerjee et al. (2011) demonstrated that choosing the correct configuration (detection and false positive rates) depends on the characteristics of the user populations in their analysis of the interactions between a firm and the hackers attempting to compromise the firm’s information assets.

Special attention should be paid to operating environments with higher hacking incentive. Ponemon Institute (2013) noted in their 2013 Cost of Cyber Crime Study that the average annualized cost of cybercrime appears to vary by industry, with organizations in financial services, defense, and energy experiencing substantially higher cybercrime costs than organizations in the retail, hospitality, and consumer products segments. They also reported that based on enterprise seats, smaller organizations incur a significantly higher per capita cost than larger organizations, further highlighting the importance of analyzing the firm’s external operating environment.

This dissertation provides the framework for modeling security games of incomplete information where the firm believes it faces one opponent type of either low or high utility throughout the duration of the game. An interesting extension to the study would be modeling the firm’s uncertainty in a setting where the user population consists of both
low and high utility users, requiring the firm to account for facing either the high or low utility user type in each of the game’s iterations as the game progresses. Demonstrating the conditions needed for the game to achieve and maintain equilibrium would be of great value to the IT research community as would the approach taken to adjust the probabilities of facing each user type over time.

Another valuable extension would be extending the models presented in this study to analyze the value of Intrusion Detection and Prevention Systems (IDPS). These systems extend the abilities of traditional IDS to include the capability of blocking or containing intrusions whenever possible. IDPS represent an important line of defense against attacks that can compromise the security of an enterprise but configuring them for effective detection and prevention can be very difficult (Alsubhi, Aib, Francois, & Boutaba, 2009). Modeling the damage recovered from the successful prevention of attacks would be a valuable extension to this study, shedding light on the value added (if any) from the implementation of IDPS. Successfully extending the study to incorporate incomplete information experienced by the user regarding the firm’s cost parameters would also further validate game theory as a tool for modeling security games of incomplete information. Modeling the user’s uncertainty would also provide further insight into the hacker’s behavior in a more realistic scenario.

Proposition 6 demonstrates that firms can model their uncertainty and utilize the value returned from IDS to discover the hackers true utility and to configure their IDS accordingly. Firms that must account for incomplete information should follow the road map presented in this dissertation to ultimately convert their uncertainty into complete
information so that they can implement optimal investigation strategies from that point forward. It remains critical that current hacking incentives and recent trends are continuously evaluated by firms and that they periodically adjust their IDS configurations accordingly. One computing trend that security engineers should continue to monitor is cloud computing. The Sophos 2014 Security Threat Report concludes that the current business trend of organizations migrating to cloud services for managing their customer data, internal project plans, and financial assets will lead to an emergence of attacks aimed at gaining access to corporate clouds (Sophos Labs, 2008).

Summary

The frequency of network intrusions steadily increases every year, costing firms millions of dollars. As a result, firms invest heavily in IT security devices, adopting IDS as an additional layer of security because of their ability to monitor the network for malicious traffic. The actual value of these devices remains uncertain because they often produce a high volume of false alarms requiring manual investigation by security administrators, which can become very costly. Determining the value of IDS is extremely difficult because of the costs associated with the implementation strategies available for deployment and their resulting false positives and negatives. Over inspecting user traffic can potentially cost more than the losses prevented, while under inspecting user traffic can result in costly intrusions.
Modeling security games where the value of every parameter is common knowledge is not practical because organizations often lack knowledge regarding the actual payoff available to users choosing to hack their networks. The ability to accurately model the value of these security devices is vital to implementing cost effective network security. Furthermore, firms are faced with the challenge of implementing IT security strategies that are capable of determining the true value of IDS when the firm faces incomplete information regarding the utility of intrusion available to potential hackers. Unlike previous research, the game-theoretic models displayed in Figures 4 and 5 allow the firm to calculate its optimal investigation strategies and analyze the value of IDS in the face of this uncertainty.

The inspiring research focused on utilizing game theory to assess the value of IDS. Cavusoglu et al. (2005) utilized the players’ optimal mixed strategies in the Nash equilibrium in conjunction with the firm’s cost parameters to derive the value of IDS under the assumption of complete information. It was assumed that the user receives a benefit of $\mu$ if the intrusion is not detected and incurred a penalty of $\beta$, giving a net benefit of $(\mu - \beta) < 0$ when detected. The user population was assumed to be homogenous, consisting of honest users and dishonest users (potential hackers). Manual investigations were assumed to confirm or rule out intrusions with certainty, and that the cost of manual investigation was less than the benefit received from the detection of an intrusion. Their model showed the importance of optimal configuration and presented the conditions necessary for the firm to benefit from the implementation of an unconfigured IDS. They also demonstrated that the user’s utility of intrusion ($\mu$),
hacking penalty for detection ($\beta$), and the probability of detection ($P_d$) played the most significant roles in determining the optimal configuration of IDS.

Two-player non-cooperative Bayesian games between a firm and a network user were modeled in this study to derive the value of IDS when the firm is uncertain of the utility of intrusion available to the user. To model incomplete information, the firm had to account for the possibility of facing either a high utility user experiencing a utility of intrusion of $\mu$, or a low utility user experiencing a utility of $\alpha\mu$ where $0 < \alpha < 1$. Previous research provided a blueprint for modeling Bayesian games of incomplete information in their extensive form using Harsanyi Transformation analysis. Harsanyi (1967) proposed an alternative Bayesian approach for the analysis of incomplete information, allowing uncertainty to be quantified by utilizing a probability distribution over the set of potential player types. The games of incomplete information were then transformed into games of complete, but imperfect, information. Backwards induction was then used to derive the Nash equilibria in the IDS and no-IDS incomplete information games.

The effects of accounting for uncertainty in the players’ mixed strategies, value of IDS, value of optimal configuration, and the models’ ability to determine its true opponent type and the ability to achieve Nash equilibrium throughout future game iterations were analyzed. The models’ ability to determine the value of IDS under the assumption of incomplete information was analyzed with Propositions 1–5 being compared to Propositions 1-5 of the inspiring literature for further analysis.

The mixed strategy equilibria for the no-IDS case presented in Proposition 1 showed that the firm’s optimal strategy was to randomly investigate user traffic with a frequency
proportional to \( \frac{\bar{\mu}}{\beta} \), making the user indifferent to hacking and/not hacking. Accounting for the firm’s uncertainty resulted in its manual investigation rate being lowered by a value of \( (P_H + (1 - P_H) \alpha) \) when compared to the complete information game set forth in the inspiring literature. Both the low and high utility users’ optimal strategy were to hack with a probability of \( \frac{c}{d\phi} \), which was identical to the results modeled under the assumption of complete information.

Proposition 2 derived the mixed strategy equilibria for the IDS case with the IDS dividing the parameter space into two distinct operating regions where the firm and users played different strategies in the equilibrium. Once again, when compared to the inspiring literature, modeling the game as one of incomplete information resulted in identical hacking strategies where the low and high utility users hacked with a frequency proportional to \( \frac{c(1-P_F)}{c(P_D - P_F) + (1-P_D)d\phi} \) in the no-alarm state \( (P_D < \frac{\bar{\mu}}{\beta}) \) and \( \frac{cP_F}{P_Dd\phi - c(P_D - P_F)} \) in the alarm state \( (P_D \geq \frac{\bar{\mu}}{\beta}) \). Manual investigation by the firm occurred with a frequency proportional to \( \frac{\bar{\mu}}{P_D\beta} \) when the IDS generated an alarm, and a frequency proportional to \( \frac{\bar{\mu} - P_D\beta}{(1-P_D)\beta} \) when there was no alarm. When compared to previous literature, the probability of manual investigation by the firm was again lowered by \( (P_H + (1 - P_H)\alpha) \) in both the alarm and no-alarm states.

Proposition 3 compared the IDS and no-IDS cases, demonstrating that the effective detection rate was identical in both cases and that the hacking probability was higher in
the IDS case when $P_D < \frac{\mu}{\beta}$ and lower when $P_D \geq \frac{\mu}{\beta}$. These results were identical to those presented in Proposition 3 of the inspiring literature. Proposition 4 demonstrated that implementing an IDS with its default configuration was detrimental to the firm when $P_D < \frac{\mu}{\beta}$ and beneficial when $P_D \geq \frac{\mu}{\beta}$. The results were identical to those of the complete information game set forth by Cavusoglu et al. (2005), aside from the newly defined operating regions that presented a larger operating region that returned a positive value to the firm when $P_D \geq \frac{\mu}{\beta}$ and a smaller operating region that was detrimental to the firm when $P_D < \frac{\mu}{\beta}$. Proposition 5 provided strong supports for previous claims that firms should configure their IDS whenever possible to ensure they receive a positive return on investment. Optimal configuration when the firm was faced with incomplete information regarding the utility of intrusion available the user was achieved by setting the detection rate at $P_D = \frac{\mu}{\beta}$. Optimal configuration in the incomplete information game returned a lower cost to the firm and a higher value of optimal configuration than those presented under the assumption of complete information.

Proposition 6 analyzed the interesting case in which the firm’s probability of detection lies between its optimal detection rates for the low and high utility users. In this scenario, the mixed strategy equilibria defined in Proposition 1 and Proposition 2 were not achievable throughout the game’s duration because the firm’s opponent was either a high or low utility user and not a combination of both as accounted for in the mixed strategy equilibria. Proposition 6 defined a methodology for utilizing the firm’s cost (no-IDS case) or the value of IDS (IDS case) after the game’s first iteration to determine the user’s
true utility of intrusion and adjusting the probability of facing that user accordingly to ensure the firm played its optimal investigation strategies throughout the remainder of the game.

The results of this dissertation study provided valuable contributions to the current body of knowledge and the IT research community by demonstrating the models’ ability to derive the value of security devices while accounting for incomplete information. This study also validated previous findings that hacking incentives and the firm’s external environment play more of a role in determining the value of IDS than the firm’s cost parameters, further validating game theory as a viable tool for valuing security devices as a supplement to IT security management. Propositions 1-6 resulted in recommendations that firms should only choose to implement configurable IDS to ensure they receive a positive return on investment. Those firms must also pay special attention to the hacking incentives and external environment when deriving their optimal investigation strategies and configuring IDS.
References


Secure Software Integration and Reliability Improvement (pp. 75-81). Shanghai, China: IEEE.


