AFRL-RI-RS-TR-2017-074

SURVIVABILITY THROUGH OPTIMIZING RESILIENT MECHANISMS (STORM)

APRIL 2017

INTERIM TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2017-074 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
JAMES S. PERRETTA
Chief, Cyber Assurance Branch

/ S /
WARREN H. DEBANY, JR.
Technical Advisor, Information
Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
APRIL 2017	INTERIM TECHNICAL REPORT	OCT 2013 – SEP 2016

4. TITLE AND SUBTITLE

SURVIVABILITY THROUGH OPTIMIZING RESILIENT MECHANISMS (STORM)

5a. CONTRACT NUMBER
IN-HOUSE

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)

Charles A. Kamhoua

5d. PROJECT NUMBER
G1SS

5e. TASK NUMBER
IH

5f. WORK UNIT NUMBER
01 (R1BX)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/RIGA
525 Brooks Road
Rome NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2017-074

12. DISTRIBUTION AVAILABILITY STATEMENT

Approved for Public Release; Distribution Unlimited. PA# 88ABW-2017-0894
Date Cleared: 07 Mar 2017

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Game theory provides a rich mathematical tool to analyze conflict within strategic interactions and thereby gain a deeper understanding of cyber security issues. Theoretical constructs or mathematical abstractions provide a rigorous scientific basis for cyber security because they allow for reasoning quantitatively about cyber-attacks. Game theory is the branch of applied mathematics that formalizes strategic interaction among intelligent rational agents. The level of sophistication of recent cyber-attacks justifies our assumption of attacker rationality and thus the need of an intelligent defence mechanism based on game theory. This work has applied game theory to numerous cyber security problems: cloud security, cyber threat information sharing, survivability, hardware Trojans, critical infrastructure protection, Online Social Network (OSN), and cyber security monitoring. When appropriate, we have expanded game theoretic frameworks to apply contract theory, prospect theory and evolutionary game theory (to account for limited rationality), and machine learning when there is little information about attackers' strategies and payoffs.

15. SUBJECT TERMS
cloud security, cyber threat information sharing, survivability, hardware Trojans, Online Social Network (OSN), contract theory, prospect theory, evolutionary game theory, machine learning

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**CHARLES A. KAMHOUA**
U	U	U	SAR	31	19b. TELEPHONE NUMBER (*Include area code*) **(315) 330-2686**

TABLE OF CONTENTS

Acknowledgements

This research was performed with support from the Air Force Office of Scientific Research under the auspices of the Laboratory Research Independent Research (LRIR) Program.

1.0 Summary

Recent increases in cyber attacks and identity theft make the Internet seem like a daunting place. Cyber attacks can lead to a severe and rising threat to our society as economic and communication infrastructures heavily depend on computer networks and information technology. The target of cyber attacks can be anyone from individuals to firms or government agencies. Growing cyber security concerns require more effective defense mechanisms to counter these threats.

Our premise in this report is that game theory can help answer the question of how a defender should react to an attacker for the goal of providing cyber security. The strategic interaction between them is captured by a two-player game in which each player attempts to maximize their own interest. The attacker's strategy depends heavily on the defender's actions, and vice versa. Thus, the effectiveness of a defense mechanism relies on both the defender's and attacker's strategic behaviors. Using the game theoretic approach, tactical analysis is performed to investigate the attack from a single node or multiple nodes. Hence, game theory is useful to investigate the strategic decision making situations of the defender and/or to analyze the incentives of the attackers. Game theoretical approaches overcome traditional solutions to cyber security in many aspects, as follows:

1) *Proven mathematics*: Most conventional security solutions, which are implemented either in preventive devices (e.g., firewall or in reactive device (e.g., an anti-virus programs), rely only on heuristics. However, game theory can investigate security decisions in a methodical manner with proven mathematics.
2) *Reliable defense*: Relying on an analytical outcome from the game, researchers can design defense mechanisms for robust and reliable cyber systems against selfish behaviors (or attacks) by malicious users/nodes.
3) *Timely action*: While adoption of the traditional security solution is rather slow due to the lack of incentives for participants, game-theoretic approaches advocate for defenders by using underlying incentive mechanisms to allocate limited resources to balance perceived risks.
4) *Distributed solutions*: Most conventional defense mechanisms make decisions in a centralized manner rather than in an individualized (or distributed) manner. In a network

security game, the centralized manner is almost an impossible solution due to the lack of a coordinator in an autonomous system. Using appropriate game models, security solutions will be implemented in distributed manners.

These above reasons make the game theory paradigm of compelling interest in cyber security problems. In this report, we present our contribution to game theory applied to cyber security.

2.0 Introduction

Interest in using the game theoretic approach to address network security challenges has increased in recent years. In general, the attacker focuses on causing maximum corruption to cyberspace while the defender aims to minimize the damage. The attacker's objective is conflicting to the defender's one, which supports the application of the game theoretic approach to study cyber security issues.

We provide the fundamental concept of game theory and provide a few critical considerations when designing and implementing game theoretic approaches for cyber security. Different types of game-theoretic approaches can model the interaction between malicious attackers and defenders (e.g., static/dynamic, noncooperative/cooperative, incomplete/complete information games and perfect/imperfect information). The network security game can be formulated as a Bayesian game, a static game, a repeated game or stochastic game. We present some major aspects that classifies security games in different ways, and some game approaches assigned to the respective classification as follows.

• *Complete versus incomplete information:* In a *complete information* game, all players' payoff function and strategies are known. However, in an *incomplete information* game, at least one of the players cannot observe the others' payoff functions and strategies.

• *Static or dynamic (based on the number of stages)*: In a *static game* (one stage game), the players are assumed to make their decision at the same time. A *dynamic game* can be defined as a game having many stages. *Backward-induction* is a typical approach to achieve a *subgame-perfect-equilibrium*, a common solution of a dynamic game. The players can repeat a static game in a finite or infinite number of stages.

A *stochastic game* is also derived from dynamic games. In stochastic games, the transition from one stage to another stage follows transition probabilities. The stage game can change randomly or deterministically from time-to-time depending on the history of a fixed set of players. In

general, the probability of the current state relies on the previous state and the players' behaviors. When the current state is independent of the previous state and players' actions, the stochastic game becomes a repeated game with random states.

A particular kind of stochastic game is the *Markov game*, in which a transition relies upon only the current states of the game and a set of players' strategies. Each player then may receive a different payoff/utility function and aims to increase the expected summation of discounted payoff. The process of states in the Markov game is a Markov process; that is, the probability distribution on the next state is determined only by the previous state and actions. We can obtain Nash equilibria of a Markov game using the solution of a chain of Markov-decision processes.

• *Perfect or imperfect monitoring:* A game is called a *perfect monitoring game* if, each player can find out the strategies chosen by other players at the end of each stage. In a perfect monitoring game, each player precisely observes the past action of all other players without any ambiguity when the player takes its move. On the other hand, in a game of *imperfect monitoring*, the actions of other players cannot be accurately observed at the end of each stage, thus, players have only noisy observation about the past actions of the others.

• *Evolutionary game theory* analyzes the population change over a long period. Similar to biology, selection and mutation are primary processes. While selection promotes some varieties over others, mutation diversifies the population. In game theory, players are assumed to be rational, but the assumption of rationality is relaxed in evolutionary game theory. This means that a small group of mutants can perform some irrational strategies in the evolutionary game. In a large population, players are not assumed to have common knowledge of the game. Players aim to maximize their self-interest or the average number of survival off-spring. The common equilibrium solution in evolutionary game theory is evolutionary stable strategy (ESS) that can resists mutation. Thus, a population can be stable over a long period if players choose to play an ESS.

• *Noncooperative versus Cooperative*. In a noncooperative game-theoretic approach, players choose a strategy to optimize their own interest. On the other hand, cooperative game players have joint strategies to achieve mutual benefits in a cooperative game. Further, players form a coalition to maximize a common objective of the coalition. To ensure that no players incentivize to change their coalition, an equilibrium of a coalition game should be resistant to the action of departing from an established solution of the game by any group of players.

Table I: Cyber Security Game Classification

Questions	Ans-wers	Types of Game	Remarks
Are the rules of the game already in place?	Yes	Game theory model	
	No	Mechanism design principle	
Are the players rational?	Yes	Game theory model	
	No	Evolutionary game model	Population of players, replicator dynamic evolutionary stable strategy
Can the contract or agreement between the players be enforced?	Yes	Cooperative game	Solution concepts: Core, Kernel, Nucleolus, Shapley value
	No	Non-cooperative game	Solution concepts: Nash equilibrium
Does the payoff depend only on the strategy and not the identity of players?	Yes	Symmetric game	
	No	Asymmetric game	
Does a player benefit only at the equal expense of others?	Yes	Zero-sum game	Frequent in military application, pure conflict
	No	Non zero-sum game	Frequent in civilian application, opportunity of cooperation for mutual benefit
Are all players moving simultaneously or are later players not aware of earlier player move?	Yes	Simultaneous game	
	No	Sequential game	
Do all players know the moves previously made by all other players?	Yes	Perfect information	Only sequential game can be of perfect information
	No	Imperfect information	
Does every player know the strategies and payoffs available to the other players?	Yes	Complete information	
	No	Incomplete information	
Does the game have finite number of players, moves, events, outcomes?	Yes	Discrete game	
	No	Continuous game	Differential game
Is the game static or one-shot?	Yes	Static game	
	No	Dynamic game (see A)	
(A) Is the same stage game repeated?	Yes	Repeated game (see B)	
	No	Stochastic game	
(B) Do the players have perfect observability of others' past action?	Yes	Perfect monitoring game	
	No	Imperfect monitoring game (see C)	
(C) Is the signal of past plays, however imprecise and noisy, invariably observed by all players?	Yes	Imperfect public monitoring	Players' signal perfectly correlated
	No	Imperfect private monitoring (see D)	Players' observe different signal of past plays. In the extreme case, players' signals are conditionally independent
(D) Do players, in their selfish optimization, need to infer the private history of other players based on their own imperfect observation?	Yes	Belief based equilibrium	
	No	Belief-free equilibrium	Easily tractable

We created Table I to summarize the different classifications of cyber security games. We contend that game theory is a mature theoretical framework that enables the modeling of several realistic scenarios. More details can be found in our survey [28] and the AFRL Inspire talk [29].
The goal of this research is to advance game theory as a scientific foundation to cyber security and survivability. We model the behavior of an intelligent adversary in cyberspace while finding the best responses to their malicious actions.

3.0 Methods, Assumptions, and Procedures

Game theory provides a rich mathematical tool to analyze conflict within strategic interactions and thereby gain a deeper understanding of cyber security issues. Theoretical constructs or mathematical abstractions provide a rigorous scientific basis for cyber security because they allow for reasoning quantitatively about cyber-attacks. Game theory is the branch of applied mathematics that formalizes strategic interaction among intelligent rational agents. The level of sophistication of recent cyber-attacks justifies our assumption of attacker rationality and thus the need of an intelligent defence mechanism based on game theory. This work has applied game theory to numerous cyber security problems: cloud security, cyber threat information sharing, survivability, hardware Trojans, critical infrastructure protection, Online Social Network (OSN), and cyber security monitoring. When appropriate, we have expanded game theoretic frameworks to apply contract theory, evolutionary game theory (to account for limited rationality), and machine learning when there is little information about attackers' strategies and payoffs.
This research summary presents our 28 most relevant papers organized around 10 subsections. The results from each paper have been peer-reviewed and published in international journals or at international conferences during the three years of this project. There are more than 60 papers published as the result of this effort.

3.1 Game theory applied to cloud security

This subsection focuses on game theory applied to cloud security including Trusted Cloud [1], security interdependency [2], security-aware virtual machine allocation [3-4], and cyber-threats information sharing in cloud computing [5]. The work in [3] also resulted in a patent application [4] and the development of a security-aware virtual machine allocation simulator.

3.1.1 On the Feasibility of an Open-Implementation Cloud Infrastructure: A Game Theoretic Analysis [1].

Trusting a cloud infrastructure is a hard problem, which urgently needs effective solutions. There are increasing demands for switching to the cloud in the sectors of financial, healthcare, or government etc., where data security protections are among the highest priorities. But most of them are left unsatisfied, due to the current cloud infrastructures' lack of provable trustworthiness. Trusted Computing (TC) technologies implement effective mechanisms for attesting to the genuine behaviors of a software platform. Integrating TC with cloud infrastructure shows a promising method for verifying the cloud's behaviors, which may in turn facilitate provable trustworthiness. However, the side effect of TC also brings concerns: exhibiting genuine behaviors might attract targeted attacks. Consequently, current Trusted Cloud proposals only integrate limited TC capabilities, which hampers the effective and practical trust establishment.

In this research, we aim to justify the benefits of a fully *Open-Implementation* cloud infrastructure, which means that the cloud's implementation and configuration details can be inspected by both the legitimate and malicious cloud users. We applied game theoretic analysis to discover the new dynamics formed between the Cloud Service Provider (CSP) and cloud users, when the *Open-Implementation* strategy is introduced. We conclude that, even though *Open-Implementation* cloud may facilitate attacks, vulnerabilities or misconfiguration are easier to discover, which in turn reduces the total security threats. Also, cyber threat monitoring and sharing are made easier in an *Open-Implementation* cloud. More importantly, the cloud's provable trustworthiness will attract more legitimate users, which increases CSP's revenue and helps lowering the price. This eventually creates a virtuous cycle, which will benefit both the CSP and legitimate users.

3.1.2 Game Theoretic Modeling of Security and Interdependency in a Public Cloud [2].

As cloud computing thrives, many small organizations are joining a public cloud to take advantage of its multiple benefits. Cloud computing is cost efficient (*i.e.*, cloud user can reduce spending on technology infrastructure and have easy access to their information without up-front

or long-term commitment of resources). Moreover, a cloud user can dynamically grow and shrink the resources provisioned to an application on demand. Despite those benefits, cyber security concern is the main reason many large organizations with sensitive information such as the Department of Defense have been reluctant to join a public cloud. This is because different public cloud users share a common platform such as the hypervisor. A common platform intensifies the well-known problem of cyber security interdependency [2-4]. In fact, an attacker can compromise a virtual machine (VM) to launch an attack on the hypervisor which if compromised can instantly yield the compromising of all the VMs running on top of that hypervisor. Therefore, a user that does not invest in cyber security imposes a negative externality on others. This research uses the mathematical framework of game theory to analyze the cause and effect of interdependency in a public cloud platform. This work shows that there are multiple possible Nash equilibria of the public cloud security game. However, the players use a specific Nash equilibrium profile depending on the probability that the hypervisor is compromised given a successful attack on a user and the total expense required to invest in security. Finally, there is no Nash equilibrium in which all the users in a public cloud will fully invest in security.

3.1.3 Security-aware Virtual Machine Allocation in the Cloud: A Game Theoretic Approach [3].

This work forms the basis of the patent application in [4].

With the growth of cloud computing, many businesses, both small and large, are opting to use cloud services compelled by a great cost savings potential. This is especially true of public cloud computing which allows for quick, dynamic scalability without many overhead or long-term commitments. However, one of the largest dissuasions from using cloud services comes from the inherent and unknown danger of a shared platform such as the hypervisor. An attacker can attack a virtual machine (VM) and then go on to compromise the hypervisor. If successful, then all virtual machines on that hypervisor can become compromised. This is the problem of negative externalities, where the security of one player affects the security of another. This work shows that there are multiple Nash equilibria for the public cloud security game. It also demonstrates that we can allow the players' Nash equilibrium profile to not be dependent on the

probability that the hypervisor is compromised, reducing the factor externality plays in calculating the equilibrium. Finally, by using our allocation method, the negative externality imposed onto other players can be brought to a minimum compared to other common VM allocation methods.

3.1.4 Cyber-threats Information Sharing in Cloud Computing: A game Theoretic Approach [5].

Cyber security is among the highest priorities in industries, academia and governments. Cyber-threats information sharing among different organizations has the potential to maximize discovery of vulnerabilities at a minimum cost. Cyber-threats information sharing has several advantages. First, it diminishes the chance that an attacker exploits the same vulnerability to launch multiple attacks in different organizations. Second, it reduces the likelihood that an attacker can compromise an organization and collect data that will help him launch an attack on other organizations. Cyberspace has numerous interconnections and critical infrastructure owners are dependent on each others' service. This well-known problem of cyber interdependency is aggravated in a public cloud computing platform. The collaborative effort of organizations in developing a countermeasure for a cyber-breach reduces each firm's cost of investment in cyber defense.

Despite its multiple advantages, there are costs and risks associated with cyber-threats information sharing. When a firm shares its vulnerabilities with others there is a risk that these vulnerabilities are leaked to the public (or to attackers) resulting in loss of reputation, market share and revenue. Therefore, in this strategic environment the firms committed to share cyber-threats information might not truthfully share information due to their own self-interests. Moreover, some firms acting selfishly may rationally limit their cyber security investment and rely on information shared by others to protect themselves. This can result in under investment in cyber security if all participants adopt the same strategy.

This research uses game theory to investigate when multiple self-interested firms can invest in vulnerability discovery and share their cyber-threat information. We apply our algorithm to a public cloud computing platform as one of the fastest growing segments of the cyberspace.

3.2 Game theory applied to cyber threat information sharing

This subsection applies game theory to cyber threat information sharing [5-9]. Cyber threat information sharing is a timely research topic. The US Senate passed the Cybersecurity Information Sharing Act (CISA) on October 2015. The law would allow the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies. The actual means of implementing this sharing is a timely research topic that we are applying game theory to.

3.2.1 Establishing evolutionary game models for CYBer security information EXchange (CYBEX) [6].

The initiative to protect critical resources against cyber-attacks requires security investments complemented with a collaborative sharing effort from every organization. A CYBersecurity information EXchange (CYBEX) framework is required to facilitate cyber-threat intelligence (CTI) sharing among the organizations to abate the impact of cyber-attacks. In this research, we present an evolutionary game theoretic framework to investigate the economic benefits of cybersecurity information sharing and analyze the impacts and consequences of not participating in the game. By using micro-economic theory as a substrate, we model this framework as a human-society inspired evolutionary game among the organizations and investigate the implications of information sharing. Using our proposed dynamic cost adaptation scheme and distributed learning heuristic, organizations are induced toward adopting the evolutionary stable strategy of participating in the sharing framework. We also extend the evolutionary analysis to understand sharing nature of participants in a heterogeneous information exchange environment. The preliminary version of this work was published in [7].

3.2.2 Cyber-Investment and Cyber-Information Exchange Decision Modeling [8].

Inefficiency of addressing cybersecurity problems can be settled by the corporations if they work in a collaborative manner exchanging security information with each other. However, without any incentive and also due to the possibility of information exploitation, the firms may not be

willing to cooperate to share their breach/vulnerability information with the external agencies. Hence it is crucial to investigate how the firms can be incentivized and encouraged, so that they become self-enforced towards participating and sharing their vulnerability information to increase not only their own payoff but also to increase their peers' payoff. This yields a win-win situation. In this work, we study the incentives and costs behind such crucial information sharing and security investments made by the firms. Specifically, a non-cooperative game between N firms is formulated to analyze the participating firms' decisions about the information sharing and security investments, which are the important parameters that affect the possibility of future cyber-attacks. We analyze the probability of successful cyber-attack using the famous dose-response immunity model. Using the negative definite Hessian condition, we find the conditions under which the optimal values of coupled constraint tuple (security investment and sharing quantity) can be found that will maximize the net payoff of the firms. The numerical results also verify the existence of a Nash equilibrium for the optimization problem.

3.2.3 Game Theoretic Modeling to Enforce Security Information Sharing among Firms [9].

Robust cybersecurity information sharing infrastructure is needed to protect the confidential information of the firms from future cyber-attacks which can be difficult to achieve via sole effort. The executive orders from the U.S. federal government clearly encourage the firms to share their cybersecurity breach and patch related information among other federal and private firms for strengthening the nation's security infrastructure. In this work, we present a game theoretic framework to investigate the economic benefits of breach-related information sharing and analyze the impacts and consequences of not participating in the game of information exchange. Considering the security investment and breach sharing intention of a firm are the critical decision parameters for future cyber defence. We model the information exchange framework as a distributed non-cooperative game among the firms and investigate the implications of information sharing and security investments. The proposed incentive model ensures and self-enforces the firms to share their breach information truthfully for maximization of its gross utility with an initial security investment. Theoretical analysis of the incentive framework has been conducted to find the conditions of self-enforcement for sharing more security information with each other. Simulation results depict that the proposed mechanism

promotes information exchange among the firms which also helps to relieve their total security technology investment in the long run.

3.3 Game theory applied to cyber survivability

This subsection applies game theory to cyber survivability [10-15]. Our main motivation for applying game theory is explained in *Bridging Fault Tolerance and Game Theory for Assuring Cyberspace* [10]. Our survivability mechanism is based on replication of mission essential functions and diversity [11-14]. Diversity diminishes the likelihood of a single malware to infect all the system. We have built a Cyber Survive and Recover Simulator to illustrate cyber diversity in a game theoretic framework.

3.3.1 Survivability in Cyberspace using Diverse Replicas: A Game Theoretic Approach [11].

Presented to the Air Force Scientific Advisory Board, December 2013, Rome NY

Today, most system and network operators in an organization (academic institute, industry lab, government facility) deploy fairly homogenous systems primarily because of it makes the following activities easier: maintenance, monitoring and upgrades. Homogeneity could also provide advantages to the software systems, configuration files, security protection mechanisms, hardware or device level, and network interfaces. However, such a homogenous environment also facilitates attackers in concentrating their efforts on just a few types of systems. If the attackers are successful in finding any vulnerability, then they can exploit that to launch an attack that can potentially affect a large number of systems. Thus homogeneity acts as a catalyst that enhances the asymmetric advantages that attackers enjoy today. For example, in May 2012, the Flame virus was declared the most complex malware ever written by researchers at Kaspersky Labs after infecting approximately 1000 machines primarily located in Middle Eastern countries. Flame exploited a flaw in the Microsoft certificate licensing service to propagate and used several novel schemes to avoid detection and gather usage data illicitly. The success of the Flame virus was accelerated by the fact that most computers run identical software to Microsoft.

One of the ways to impede attackers is to make the expected payoff much lower than the cost of launching attacks. It is to be noted that attackers would like to use the best possible and most efficient strategies to inflict the maximum damage. Thus, attackers can be discouraged by diversifying the technologies that the systems use. This is because a typical attack exploits a specific vulnerability and different systems are not likely to be affected. For example, if systems were different, the attackers would have to explore additional vulnerabilities as a vulnerability in one system might not exist in other systems. This diversity would cause impediments for the attackers in two ways: 1.) by increasing their effort required to infect systems, and 2.) by reducing the number of systems that could be infected because of the additional efforts required. In summary, the more diversity is introduced in a system, the less will be the attacker's payoff from exploiting a system's vulnerability. In either case, the return on investment is reduced, making it less profitable to attack.

The main contribution of this work is to provide an analytical modelling of replicas diversity for critical mission survival using game theory. This research shows that the more dangerous vulnerabilities (that affect more replicas) in a system are sometimes less likely to be exploited. The attacker may be better off exploiting small vulnerabilities because they will be less protected by the defender.

In the future, we will consider incomplete-information games in which the attacker skill level is not common knowledge but private information. Future work will also look into the case that the attacker can simultaneously exploit multiple vulnerabilities while the defender can also simultaneously protect against several vulnerabilities.

3.3.2 Replication and Diversity for Survivability in Cyberspace: A Game Theoretic Approach [12].

An effective defense-in-depth avoids a large percentage of threats and defeats those threats that turn into attacks. When an attack evades detection, is not defeated, and disrupts systems and networks, the defensive priority turns to survival and mission assurance. In this context, mission assurance seeks to ensure that critical mission essential functions (MEFs) survive and fight through the attacks against the underlying cyber infrastructure. Survivability represents the quantified ability of a system, subsystem, equipment, process, or procedure to function

continually during and after a disturbance. US Air Force systems carry varying survivability requirements depending on MEF's criticality and protection conditions. Almost invariably, however, replication of a subsystem, equipment, process, or procedure is necessary to meet a system's survivability requirements. Therefore, the degree of replication within a system can be paramount for MEF's survival. Moreover, diversity will prevent the same fault or attack from damaging all the replicas so that they can continue the mission. This research shows that the more dangerous vulnerabilities (that affect more replicas) in a system are sometimes less likely to be exploited. In fact, diversity always gives extra challenges to attackers. This work uses the mathematical framework of game theory to show the significance of replica diversity for mission survival in cyberspace.

3.3.3 Diversity and System Security: A Game Theoretic Perspective [13].

It has been argued that systems that are comprised of similar components (i.e., a monoculture) are more prone to attacks than a system that exhibits diversity. But it is not currently clear how much diversity is needed and how to leverage the underlying diversity in the design space. Here we attempt to study these issues using a game theoretic model comprised of networked systems and an attacker. The model illustrates how the concept of the Nash Equilibrium provides a theoretical framework for designing strategic security solutions and how the mixed strategy solution space provides a conceptual basis for defining optimal randomization techniques that can exploit the underlying diversity. This work also studies how strategic behavior influences the diversity and vulnerability of an overall system. Simulation results provide further insights into the effectiveness of our solution approach and the dynamics of strategic interaction in the context of system security.

3.3.4 CSRS: Cyber Survive and Recover Simulator [14].

We present a game theoretic model to analyze strategic attack-defense scenarios as well as present our research and development effort to develop a software tool that facilitates analysis of strategic use of redundancy and diversity techniques for cyber survivability and recoverability by leveraging the developed game theoretic model. The simulator shows the potential of using game

theoretic approaches for exploiting diversity for cyber survivability. The game theoretic model illustrates how the concept of the Nash Equilibrium provides a theoretical framework for designing strategic security solutions and how the mixed strategy solution space provides a conceptual basis for defining optimal randomization techniques that can exploit the underlying diversity. The simulator provides capabilities to simulate various attack-defense scenarios, analyze defense tactics, and provide feasible security solutions to help adopt appropriate defense strategies.

3.3.5 Improving System Reliability Against Rational Attacks Under Given Resources [15].

System reliability has always been a challenging issue for many systems. In order to achieve high reliability, redundancy and voting schemes are often used to tolerate unintentional component failures. For unintentional failures caused by, for instance, normal wear-outs, hardware failures, or software bugs, etc., adding more redundancies often improves a system's reliability. However, when attack-caused failures exist, the number of redundant components and the number of participating voting entities may not be positively proportional to system reliability. In this work, we study system reliability and system defense strategies when the system is under rational attacks. In particular, we analyze how defense and attack strategies may impact system reliability when both the defender and attacker are given a fixed amount of resources that can only be used for adding camouflaging components or enhancing existing components' cyber protection by defenders, or selecting a subset of components to attack by attackers, respectively. We use a game theoretic framework to present an algorithm to decide the optimal defense strategy in fighting against rational attacks.

The main contributions of this work are: 1) formal analysis of the relationship between attack and defense strategy, and how they affect system reliability; 2) development of an algorithm to determine the optimal defense strategy against rational attacks; and 3) an experimental study of how the defense and attack resources impact the defender’s strategy.

In this work, we only considered that components can be compromised while the communication channel for the voting protocol is reliable. However, in reality, communication channels played an important role when it comes to the system reliability, often times they are the target of attacks. When network reliability was taken into consideration, less communication in reaching a

consensus could imply higher reliability of the consensus; on the other hand, fewer voting participants (less communication) could result in lower reliability. It becomes more complicated when intentional attacks existed. Hence, our next step is to include the communication channel into the system model and investigate how the communication channel affects system reliability and defense strategy.

3.4 A Game-Theoretic Approach for Testing for Hardware Trojans [16]

Won the AFRL's Information Directorate Fred I. Diamond Award "for the best technical paper published … in a refereed journal"

The microcircuit industry is witnessing a massive outsourcing of the fabrication of ICs (Integrated Circuit), as well as the use of third party IP (Intellectual Property) and COTS (Commercial Off-The-Shelf) tools during IC design. These issues raise new security challenges and threats. In particular, it brings up multiple opportunities for the insertion of malicious logic, commonly referred to as a hardware Trojan, in the IC. Testing is typically used along the IC development lifecycle to verify the functional correctness of a given chip. However, the complexity of modern ICs, together with resource and time limitations, makes exhaustive testing commonly unfeasible. In this work, we propose a game-theoretic approach for testing digital circuits that takes into account the decision-making process of intelligent attackers responsible for the infection of ICs with hardware Trojans. Testing for hardware Trojans is modeled as a zero-sum game between malicious manufacturers or designers (i.e., the attacker) who want to insert Trojans, and testers (i.e., the defender) whose goal is to detect the Trojans. The game results in multiple possible mixed strategy Nash equilibria that allow identification of optimum test sets that increase the probability of detecting and defeating hardware Trojans in digital logic. Results also show that the minimum number of Trojan classes tested by the defender and the fines imposed to the attacker can deter rational as well as irrational attackers from infecting circuits with Trojans.

The preliminary version of this work was published in [17]. This game model is expanded in [27] based on the robust behavioral framework of prospect theory (PT) which allows to capture potential uncertainty, risk, and irrational behavior in the decision making of both attacker and

defender. We used the results from this work to design a Hardware Trojans Detection simulator based on game theoretic principles. Further, this line of research was expanded to submit an AFOSR in-house basic research proposal *Design Engineering That Overcomes Unwanted Replacements (DETOUR)* which is recommended for funding (pending funding availability) at $600K for the next 3 years. DETOUR combats the deceptive digital logic (DDL) that undermine the most software-enhance legacy systems. DETOUR proactively reprogram a single structured Application Specific Integrated Circuit (ASIC) to mimic the need-to-replace legacy IC as well as neighboring ICs that are likely nearing EOL. DETOUR also apply state-of-the-art ASICs that integrate fixed logic circuitry with reconfigurable fabric. Also, DETOUR allows us to mimic, both physically and virtually, multiple ICs on a board. DETOUR introduce replication and design diversity within the ASIC to ensure faithful capturing of the legacy ICs' functionality and to enhance system fault-tolerance.

From this project insights were gained into hardware security and trust - in particular, combating hardware Trojans. These activities have reached a level that warranted consolidation of the knowledge into an offering for the Advanced Course in Engineering (ACE) [18] to consider incorporating into its academic and training curriculum. The PI and co-PI were spurred by the ACE's record of having transitioned its R&D efforts to over 24 different US government customers in the past 6 years alone with some customers have operationalized numerous deliverables within weeks of receipt. Academic instruction in cutting edge concepts and research in combating hardware Trojans is envisioned as a key part of the successful preparation of future cyber leaders and useful R&D deliverables produced by the ACE. The PI and co-PI prepared a course in combating hardware Trojans to the ACE Leadership directly meet the requirement to incorporate a security focused hardware module into the larger cyber-security academic and training curriculum.

3.5 Game theory applied to secure Online Social Network (OSN)

3.5.1 Social network attack simulation with honeytokens [19].

In the social media era, the ever-increasing utility of Online Social Networks (OSN) services provides a variety of benefits to users, organizations, and service providers. However, OSN services also introduce new threats and privacy issues regarding the data they are dealing with.

For instance, in a reliable OSN service, a user should be able to set up his desired level of information sharing and securely manage sensitive data. Currently, few approaches exist that can model OSNs for the purpose, let alone a model the effects that attackers can have on these networks. In this work a novel OSN modeling approach is presented to fill the gap. This model is based on an innovative game-theoretic approach and it is analyzed both from a theoretical and simulation-oriented view. The game-theoretic model is implemented to analyze several attack scenarios. Honeytokens, which are an information security tool based upon deception, are defined and identified as a security tool that could help in OSN security. As the results show, there are several scenarios where OSN services are very vulnerable and hence more protection mechanisms should be provided to secure the data contained across these networks, including the use of honeytokens. In this work we introduce a novel OSN modeling approach for optimal data sharing based on innovative game theories, considering the states/optimal policies of data sharing on OSNs and possible confrontations between the attacker and the user. After we develop the theoretical framework, we conduct experiments, integrating our ideas with honeytokens in several attack scenarios. Finally, we analyze our experimental results and discuss recommendations based on the results.
The conference paper stemming from this work won an IEEE Best Paper Award at FOSINT-SI 2013 [20].

3.5.2 Trusted Online Social Network (OSN) services with optimal data management [21].

Online Social Network (OSN) services have rapidly grown into a wide network and offer users a variety of benefits. However, they also bring new threats and privacy issues to the community. Unfortunately, there are attackers that attempt to expose OSN users' private information or conceal the information that the user desire to share with other users. Therefore, in this research we develop a framework that can provide trusted data management in OSN services. We first define the data types in OSN services and the states of shared data with respect to Optimal, Under-shared, Over-shared, and Hybrid states. We also identify the facilitating, detracting, and preventive parameters that are responsible for the state transition of the data. In a reliable OSN service, we address that a user should be able to set up his or her desired level of information sharing with a certain group of other users. However, it is not always clear to the ordinary users

how to determine how much information they should reveal to others. In order to support such a decision, we propose an approach for helping OSN users to determine their optimum levels of information sharing, taking into consideration the payoffs (potential Reward or Cost) based on the Markov decision process (MDP). As an extension of the MDP-based approach, we also introduce a game theoretic approach, considering the interactions of OSN users and attackers with conflicting interests whose decisions affect each other's. Finally, after developing the framework for the optimal data sharing on OSNs, we conduct several experiments with attack simulation based on the proposed ideas and discuss the results. Our proposed approach has the capability to allow a large amount of variables to be altered to suit particular setups that an organization might have.

3.6 Contract-Theoretic Resource Allocation for Critical Infrastructure Protection [22]

Critical infrastructure protection (CIP) is envisioned to be one of the most challenging security problems in the coming decade. One key challenge in CIP is the ability to allocate resources, either personnel or cyber, to critical infrastructures with different vulnerability and criticality levels. In this work, a contract-theoretic approach is proposed to solve the problem of resource allocation in critical infrastructure with asymmetric information. A control center (CC) is used to design contracts and offer them to infrastructures' owners. A contract can be seen as an agreement between the CC and infrastructures' owners. When the contract is put into use, the CC allocates resources and gets rewards in return. Contracts are designed in a way to maximize the CC's benefit and motivate each infrastructure owner to accept a contract and obtain proper resources for its protection. Infrastructures are defined by both vulnerability levels and criticality levels which are unknown to the CC. Therefore, each owner of infrastructure can claim that theirs is the most vulnerable or critical to gain more resources. A novel mechanism is developed to handle such an asymmetric information while providing the optimal contract that motivates each infrastructure to reveal its actual type. The necessary and sufficient conditions for such resource allocation contracts under asymmetric information are derived. Simulation results show that the proposed contract-theoretic approach maximizes the CC's utility while ensuring that no infrastructure owner has an incentive to ask for another contract, despite the lack of exact information at the CC.

3.7 Game Theory with Learning for Cyber Security Monitoring [23]

Recent attacks show that threats to cyber infrastructure are not only increasing in volume, but are getting more sophisticated. The attacks may comprise multiple actions that are hard to differentiate from benign activity, and therefore common detection techniques have to deal with high false positive rates. Because of the imperfect performance of automated detection techniques, responses to such attacks are highly dependent on human-driven decision-making processes. While game theory has been applied to many problems that require rational decision making, we find a limitation on applying such a method on security games when there is limited information. In this work, we propose Q-Learning to react automatically to the adversarial behavior of a suspicious user to secure the system. This work compares variations of Q-Learning with a traditional stochastic game. Simulation results show the possibility of Naive Q-Learning, despite restricted information on opponents.

3.8 A game theoretic approach to detect and co-exist with malicious nodes in wireless networks [24]

Identification and isolation of malicious nodes in a distributed system is a challenging problem. This problem is further aggravated in a wireless network because the unreliable channel hides the actions of each node from one another. Therefore, a regular node can only construct a belief about a malicious node through monitoring and observation. In this work, we use game theory to study the interactions between regular and malicious nodes in a wireless network. We model the malicious node detection process as a Bayesian game with imperfect information and show that a mixed strategy perfect Bayesian Nash Equilibrium (also a sequential equilibrium) is attainable. While the equilibrium in the detection game ensures the identification of the malicious nodes, we argue that it might not be profitable to isolate the malicious nodes upon detection. As a matter of fact, malicious nodes can co-exist with regular nodes as long as the destruction they bring is less than the contribution they make. To show how we can utilize the malicious nodes, a post-detection game between the malicious and regular nodes is formalized. Solution to this game shows the existence of a subgame perfect Nash Equilibrium and reveals the conditions that are necessary to achieve the equilibrium. Further, we show how a malicious node can construct a

belief about the belief held by a regular node. By employing the belief about the belief system, a Markov Perfect Bayes–Nash Equilibrium is reached and the equilibrium postpones the detection of the malicious node. Simulation results and their discussions are provided to illustrate the properties of the derived equilibria. The integration of the detection game and the post-detection is also studied and it is shown that the former one can transit into the latter one when the malicious node actively adjusts its strategies.

3.9 Modeling Cooperative, Selfish and Malicious Behaviors for Trajectory Privacy Preservation Using Bayesian Game Theory [25]

As new mobile Wireless Sensor Networks (mWSNs) for location-aware applications are emerging, trajectory privacy invasion is becoming an indispensable issue. Many promising techniques are under development. Considering the decentralized network architecture, most of Trajectory Privacy Preservation (TPP) techniques rely on the cooperation from peer nodes, cluster headers, or a third party. However, only a few works have addressed the issue of selfish behaviors in such cooperation required techniques. Nevertheless, the problem of facing selfish and compromised nodes in the non-cooperative and hostile environment is rarely touched upon. In this work, we apply Bayesian game theory to model cooperative, selfish and malicious behaviors of autonomous mobile nodes in decentralized mWSNs. We formulate and analyze the TPP game among peer nodes in both strategic and dynamic forms. The equilibrium strategies for users to evaluate the degree of trust in participating in in-network TPP activities are provided and analyzed in theoretical and simulation results.

3.10 Cyber Security Resource Allocation: A Markov Decision Process Approach [26]

An effective defense-in-depth in cyber security applies multiple layers of defense throughout a system. The goal is to defend a system against cyber-attack using several independent methods. Therefore, a cyber-attack that is able to penetrate one layer of defense may be unsuccessful in other layers. Common layers of cyber defense include: attack avoidance, prevention, detection, survivability and recovery. It follows that in security-conscious organizations, the cyber security investment portfolio is divided into different layers of defense. For instance, a two-way division

is agility and recovery. Cyber agility pursues attack avoidance techniques such that cyber-attacks are rendered as ineffective; whereas cyber recovery seeks to fight-through successful attacks. We show that even when the primary focus is on the agility of a system, recovery should be an essential point during implementation because the frequency of attacks will degrade the system and a quick and fast recovery is necessary. However, there is not yet an optimum mechanism to allocate limited cyber security resources into the different layers. We propose an approach using the Markov Decision Process (MDP) framework for resources allocation between the two end layers: agility and recovery.

4.0 Results and Discussion

The game theoretic approach can capture the interaction between defenders and attackers. When we use game theoretical approaches to design or implementation in cyber systems, we should consider the following issues:

1) *Rationality:* Almost all game theoretic models applied to cyber security mainly focus on equilibrium strategy in the action profiles of defenders and attackers. However, in a real cyber system, due to bounded rationality and limited information, it is difficult for both the attacker and the defender to always perform the best-response actions. Furthermore, in cases where multiple equilibria exist, it is unclear which the players will choose or even if they can agree to choose one at all. Our work addresses limited rationality in [6, 7, 27].
2) *Incomplete information:* In a real cyber system, when the attacker and defender make their decision, they often consider many uncertain but real factors such as how much traffic is generated in a general network, the signal to noise ratio (SNR) and/or power of nodes in a wireless network. However, in a realistic scenario, the defender cannot observe all information perfectly. Therefore, the defenders should be able to analyze and understand the environment. Learning the changing of environment can decrease the convergent speed to the equilibrium and make the implementation be more complex. We propose in [23] that machine learning be applied when there is limited information to formulate a security game.
3) *Multiple layers of protection:* The literature [28] targeted one specific defense mechanism by the defender that tries to maximize its payoff by setting appropriate parameters. However, the existence of multi-layers defenders protecting against attack, which are often implemented in

present cyber systems, is disregarded. Therefore, an appropriate game approach is required to answer how multi-layers defender can protect against attacks when the defending layers are implemented at the same time and how they can enhance the other layers. We are investigating a game theoretic approach with multiple layers of defense in our new AFOSR funded in-house research Cloud ARMS (Allocation, Replication, Monitoring, and Sharing).

Finally, some game theoretic works model a security game as two-player games in which multiple attackers or defenders are considered as one entity. The two-player game is a reasonable model if those multiple attackers or defenders coordinate to have the same strategies and payoffs, but may not be realistic in a practical system due to the potential diversity of the strategies and payoffs of the attackers and defenders. More research is needed to address the different uncertainties we discussed in this section.

5.0 Conclusions

We have demonstrated that game theory provides a rich mathematical tool to analyze conflict within strategic interactions and thereby gain a deeper understanding of cyber security issues. Our work has applied game theory to numerous cyber security problems: cloud security, cyber threat information sharing, survivability, hardware Trojans, critical infrastructure protection, Online Social Network (OSN), and cyber security monitoring. However, there are still several challenges such as limited rationality, incomplete information, and the possibility of multiple layer of cyber defence that need further investigation.

6.0 References

1) Charles A. Kamhoua, Anbang Ruan, Andrew Martin, Kevin A. Kwiat "On the Feasibility of an Open-Implementation Cloud Infrastructure: A Game Theoretic Analysis" *in the proceedings of the 2015 IEEE/ACM International Conference on Utility and Cloud Computing (UCC 2015)*, Limassol, Cyprus, December 2015.
2) Charles A. Kamhoua, Luke Kwiat, Kevin Kwiat, Joon Park, Ming Zhao, Manuel Rodriguez, "Game Theoretic Modeling of Security and Interdependency in a Public Cloud" *in the proceedings of IEEE International Conference on Cloud Computing, (IEEE CLOUD 2014)* Anchorage, Alaska, June 2014.

3) Luke Kwiat, Charles A. Kamhoua, Kevin Kwiat, Jian Tang, Andrew Martin "Security-aware Virtual Machine Allocation in the Cloud: A Game Theoretic Approach" *in proceedings of the IEEE International Conference on Cloud Computing, (IEEE CLOUD 2015),* New York, June 2015.
4) Luke Kwiat, Charles A. Kamhoua, Kevin Kwiat, "Security Method for Allocation of Virtual Machines in a Cloud Computing Network" *US Patent Application Number 14861227*.
5) Charles A. Kamhoua, Andrew Martin, Deepak Tosh, Kevin A. Kwiat, Chad Heitzenrater, Shamik Sengupta "Cyber-threats Information Sharing in Cloud Computing: A game Theoretic Approach" *in the proceedings of the IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2015),* New York, November 2015.
6) Deepak K. Tosh, Shamik Sengupta, Charles A. Kamhoua, Kevin A. Kwiat "Establishing Evolutionary Game Models for CYBer security information EXchange (CYBEX)" *Accepted at the Special Issue on Cyber Security in the Critical Infrastructure: Advances and Future Directions, journal of computer and system sciences, Elsevier*.
7) Deepak K. Tosh, Shamik Sengupta, Charles A. Kamhoua, Kevin A. Kwiat, Andrew Martin "An Evolutionary Game-Theoretic Framework for Cyber-threat Information Sharing" *in the proceedings of the IEEE International Conference on Communications (IEEE ICC 2015),* London, UK, June 2015.
8) Deepak K. Tosh, Shamik Sengupta, Charles A. Kamhoua, Kevin A. Kwiat "Cyber-Investment and Cyber-Information Exchange Decision Modeling" *in proceedings of the IEEE International Symposium on Cyberspace Safety and Security (CSS2015),* New York, August 2015.
9) Deepak K. Tosh, Shamik Sengupta, Charles A. Kamhoua, Kevin A. Kwiat "Game Theoretic Modeling to Enforce Security Information Sharing among Firms" *in the proceedings of the IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2015),* New York, November 2015.
10) Kevin A. Kwiat, Charles A. Kamhoua "Bridging Fault Tolerance and Game Theory for Assuring Cyberspace" *Special Issue of Cyber Security and Information Systems Information Analysis Center (CSIAC) Journal, Focus on Air Force Research Laboratory's Information Directorate*, Volume 4, Number 1, December 2015.

11) Charles A. Kamhoua, Kevin Kwiat, Joon Park, Patrick Hurley, Mainak Chatterjee, "Survivability in Cyberspace using diverse replicas: A Game Theoretic Approach" *in the Journal of Information Warfare,* Vol. 12, Issue 2, page 27. September 2013.

12) Charles A. Kamhoua, Kevin Kwiat, Mainak Chatterjee, Joon Park, Patrick Hurley, "Replication and Diversity for Survivability in Cyberspace: A Game Theoretic Approach" *Leading Issues in Information Warfare and Security Research,* volume 2, pp173-190, Published by Academic Conferences and Publishing International Limited, ISBN: 978-1-910810-64-4, October 2015.

13) Swastik Brahma, Kevin Kwiat, Pramod K. Varshney, Charles A. Kamhoua, "Diversity and System Security: A Game Theoretic Perspective" *in the proceedings of Military Communications Conference, (IEEE MILCOM 2014)* Washington, DC, October 2014.

14) Swastik Brahma, Kevin Kwiat, Pramod K. Varshney, and Charles A. Kamhoua, "CSRS: Cyber Survive and Recover Simulator" *in the proceedings of the 2016 IEEE High Assurance Systems Engineering Symposium (HASE),* Orlando, Florida, January 2016.

15) Li Wang; Shangping Ren; Bogdan Korel, Kevin Kwiat, Eric Salerno, "Improving System Reliability Against Rational Attacks Under Given Resources" *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol.44, no.4, pp.446,456, April 2014.

16) Charles A. Kamhoua, Hong Zhao, Manuel Rodriguez, and Kevin A. Kwiat, "A Game-Theoretic Approach to Testing for Hardware Trojans" *IEEE Transactions on Multi-Scale Computing Systems, Special Issue/Section on Hardware/Software Cross-Layer Technologies for Trustworthy and Secure Computing,* vol. 2, no. 3, pp. 199-210, July-Sept. 1 2016.

17) Charles A. Kamhoua, Manuel Rodriguez, and Kevin A. Kwiat, "Testing for Hardware Trojans: A Game-Theoretic Approach" *in the proceedings of the Conference on Decision and Game Theory for Security (GameSecc 2014),* Los Angeles, CA, USA, November 2014.

18) Kamal Jabbour and Susan Older, "The Advanced Course in Engineering on Cyber Security: A Learning Community for Developing Cyber-Security Leaders" http://www.cis.syr.edu/~sueo/papers/ace-wecs.pdf

19) Jonathan White, Joon Park, Charles A. Kamhoua, Kevin A. Kwiat, "Social Network Attack Simulation with Honeytokens", *Journal of Social Network Analysis and Mining, (SNAM),* Springer, July 2014.

20) Jonathan White, Joon Park, Charles A. Kamhoua, Kevin A. Kwiat, "Game Theoretic Attack Analysis in Online Social Network (OSN) Services" *in the proceedings of the International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI), in conjunction with the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM),* Niagara Falls, Canada, August 2013. **BEST PAPER AWARD**

21) Joon S. Park, Kevin A. Kwiat, Charles A. Kamhoua, Jonathan White, Sookyung Kim "Trusted online social network (OSN) services with optimal data management" *Computers & Security* 42, pp116-136, published by Elsevier, March 2014.

22) AbdelRahman Eldosouky, Walid Saad, Charles A. Kamhoua, and Kevin Kwiat "Contract-Theoretic Resource Allocation for Critical Infrastructure Protection" *in the proceedings of IEEE Global Communication Conference (Globecom),* San Diego, California, December 2015.

23) Keywhan Chung, Charles A. Kamhoua, Kevin A. Kwiat, Zbigniew Kalbarczyk, Ravishankar K. Iyer, "Game Theory with Learning for Cyber Security Monitoring" *in the proceedings of the 2016 IEEE High Assurance Systems Engineering Symposium (HASE)*, Orlando, Florida, January 2016.

24) Wenjing Wanga, Mainak Chatterjee, Kevin Kwiat, Qing Li, "A game theoretic approach to detect and co-exist with malicious nodes in wireless networks" *Computer Networks* 71 (2014) 63–83.

25) Xinyu Jin, Niki Pissinou, Sitthapon Pumpichet, Charles A. Kamhoua, Kevin A. Kwiat "Modeling Cooperative, Selfish and Malicious Behaviors for Trajectory Privacy Preservation using Bayesian Game Theory" *in the proceedings of the 38th IEEE Conference on Local Computer Networks (LCN)*, Sydney, Australia, October 2013.

26) Laurent Njilla, Charles A. Kamhoua, Kevin A. Kwiat, Patrick Hurley, Niki Pissinou, "Cyber Security Resource Allocation: A Markov Decision Process Approach" *in the proceedings of the 2017 IEEE High Assurance Systems Engineering Symposium (HASE),* Singapore, January 2017.

27) Walid Saad, Anibal Sanjab, Yunpeng Wang, Charles A. Kamhoua, and Kevin Kwiat "Hardware Trojan Detection Game: A Prospect-Theoretic Approach" *Accepted at the IEEE Transactions on Vehicular Technology,* 2017.

28) Cuong T. Do, Nguyen H. Tran, Choongseon Hong, Charles A. Kamhoua, Kevin A. Kwiat, Erik Blasch, Shaolei Ren, Niki Pissinou, Sundaraja Sitharama Iyengar "Game Theory for Cyber Security and Privacy" *Accepted at ACM Computing Surveys*.
29) Charles A. Kamhoua "Cyber Security Game" AFRL Inspire (similar to TED Talk), Available Online [https://www.youtube.com/watch?v=gG8P6bYByIM] December 13, 2016.