Collaborative Analysis of Cybersecurity Information Sharing

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science and Engineering

by
Iman Vakilinia

Shamik Sengupta/Dissertation Advisor

May 2019
UNIVERSITY OF NEVADA RENO
THE GRADUATE SCHOOL

We recommend that the dissertation
prepared under our supervision by

Iman Vakilinia

entitled

Collaborative Analysis in Cybersecurity Information Sharing

be accepted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY

Shamik Sengupta, Ph.D., Advisor
Sushil Louis, Ph.D., Committee Member
Mehmet H. Gunes, Ph.D., Committee Member
Engin Arslan, Ph.D., Committee Member
Sankar Mukhopadhyay, Ph.D., Graduate School Representative
David W. Zeh, Ph. D., Dean, Graduate School

May, 2019
Abstract

As the complexity and number of cybersecurity incidents are growing, the traditional security measures are not enough to defend against attackers. In this situation, cyber threat intelligence substantially improves the detection and prevention of sophisticated attacks by providing a comprehensive knowledge about a threat which includes indicators, implications, and actionable advice. One of the key factors of threat intelligence is cybersecurity information sharing, allowing organizations to detect and prevent malicious behaviors proactively.

Due to the importance of cybersecurity information sharing, governmental laws/initiatives have been legislated to mandate/encourage the governmental and private organizations to share their cybersecurity information. However, stimulating organizations to participate and deterring free-riding in such sharing is a big challenge. To this end, the cybersecurity information sharing framework should be equipped with a sound and fair rewarding and participation-fee allocation mechanisms to encourage sharing behavior. Furthermore, as the cybersecurity information conveys sensitive and private data, the sharing platform should protect the underlying sensitive information. In this research, we propose mechanisms and protocols to improve the cybersecurity information sharing platform. Although many research studies have been done to model the development of cybersecurity information sharing frameworks as a non-cooperative game, this problem has not been studied with the cooperative game theoretic approach. We analyze the cybersecurity information sharing with the cooperative game theoretic approach. Moreover, we apply cyber-insurance to motivate organizations toward cybersecurity collaboration.

First, we review prior efforts in the domain of cybersecurity information sharing and cyber-insurance. Then we study the privacy challenges for cybersecurity information sharing platform and we propose a set of protocols to protect the underlying sensitive information. Afterward, we study the design of mechanisms to motivate organizations toward cybersecurity collaboration. We propose a set of new mechanisms to leverage cyber-insurance to strengthen the cybersecurity collaboration to reach the socially optimal point while satisfying mechanism design requirements.
Acknowledgment

I would like to express my deep and sincere gratitude to my advisor Professor Shamik Sengupta for his patience and his continuous support of my PhD study.

I am grateful to Dr. Deepak Tosh, and Dr. Shahriar Badsha for their help and support during our collaboration works.

I would like to thank my parents, and my brother Dr. Shahin Vakilinia for supporting me spiritually throughout my life in general. They were always ready to help me when I needed them. Their endless encouragement, and guidance supported me throughout my life.

Thank you.
Contents

Abstract i
Acknowledgment ii
Contents iii
List of Tables v
List of Figures vi

1 Introduction 1
   1.1 Cybersecurity Information Sharing ............................... 1
   1.2 Cyber-Insurance .................................................. 5
   1.3 Thesis Organization .............................................. 8

2 Background Studies 9
   2.1 Development of Cybersecurity Information Sharing ............... 9
   2.2 Game Theoretic Analysis of Cybersecurity Information Sharing ... 12
       2.2.1 Privacy-preservation in cybersecurity information sharing ... 14
   2.3 Modeling the Cyber-insurance .................................... 17

3 A Coalitional Game Theory Approach for Cybersecurity Information Sharing 19
   3.1 Overview and Problem Statement .................................. 21
   3.2 Rewarding in Coalitional Game with Transferable Utility .......... 26
       3.2.1 Coalitional Game ............................................ 26
       3.2.2 Profit Sharing ................................................ 28
       3.2.3 Coalition Formation ......................................... 30
   3.3 Differentially Private Rewarding .................................. 34
       3.3.1 Differential Privacy .......................................... 35
       3.3.2 Private Rewarding Mechanism ................................ 36
   3.4 Simulation Results .................................................. 43
       3.4.1 Fair Rewarding ................................................ 44
       3.4.2 Differentially Private Rewarding ......................... 46

4 Privacy-Preserving Cybersecurity Information Exchange Mechanism 48
   4.1 System Model ....................................................... 49
4.1.1 Entities and Architecture ........................................ 49
4.1.2 Threat Model ..................................................... 51
4.2 Preliminaries .......................................................... 51
  4.2.1 Building Blocks ............................................... 52
  4.2.2 Cryptographic Assumptions .................................. 54
4.3 Privacy-Preserving Cybersecurity Information Exchange .......... 54
  4.3.1 Initialization .................................................. 55
  4.3.2 Sharing ....................................................... 55
  4.3.3 Dispute ....................................................... 57
  4.3.4 Rewarding ................................................... 57
4.4 Privacy and Security Analysis .................................... 60
4.5 Performance Evaluation ........................................... 61
  4.5.1 Computation Complexity .................................... 62
  4.5.2 Communication Cost ......................................... 63

5 A Coalitional Cyber-Insurance Framework for a Common Platform 64
  5.1 System Model .................................................... 66
    5.1.1 Cyber-Insurance ........................................... 67
    5.1.2 Cybersecurity Information Sharing ........................ 68
    5.1.3 Design Objective ........................................... 69
  5.2 Insuring a Common Platform .................................... 72
    5.2.1 Coalitional Self-Insurance Framework ........................ 72
    5.2.2 Crowdfunding the Coalitional Insurance Framework with
          Different Level of Indemnity and Commitment ............ 83
    5.2.3 Outsourcing the insurance of a common platform .......... 90
  5.3 Numerical Analysis .............................................. 95

6 Conclusion ............................................................ 98

Bibliography .......................................................... 100
List of Tables

3.1 Feature Set of Vulnerability CVE-2016-10012 . . . . . . . . . . . . . 22
5.1 Notations used for a coalitional cyber-insurance framework . . . . . . 70
List of Figures

1.1 STIX 2.0 architecture ........................................... 4
3.1 The cybersecurity information sharing platform ................. 25
3.2 The calculation of reward and participation-fee .................. 25
3.3 Comparing (A) the non-game-theoretic approach and (B) game-
theoretic approach ................................................. 43
3.4 Comparing sampling distributions (A) $\delta = 7$, (B) $\delta = 10$ .... 44
3.5 Privacy leakage with the increasing of (A) $\epsilon$ and (B) $\delta$ ......... 44
3.6 Fairness distance with the increasing of (A) $\epsilon$ and (B) $\delta$ .......... 45
4.1 Architecture of privacy-preserving cybersecurity Information Sharing 52
4.2 Illustration of communications in privacy-preserving cybersecurity
information sharing scheme. ....................................... 54
4.3 Computation time under different number of messages .......... 62
4.4 Communication cost under different number of messages ......... 63
5.1 Organizations coalition for cyber-insurance ....................... 71
5.2 The changes of expected benefit when $p$, $\hat{\psi}$, and $n$ vary .......... 94
5.3 Outsider commitment value ....................................... 97
5.4 The expected benefit of a risk-averse organization by cooperatively
outsourcing the insurance of a common platform .................. 97
Chapter 1

Introduction

1.1 Cybersecurity Information Sharing

The revolution of Information and Communication Technologies (ICT) has brought economic prosperity in recent years. However, securing the cyberspace from malicious attackers has been a critical concern. Due to the increasing rate of cyber crimes and the complexity of cyber-threats, the organizations face difficulty in effectively tackling cybersecurity issues alone. Though an organization’s sole security investigation may lead to developing potential cyber-defense solutions, this reactive approach may not help in better understanding the cybersecurity landscape and take proactive measures to reduce future exploits. The recently proposed “cyber-threat information (CTI) sharing” [1] scheme is envisioned to help the organizations in enhancing their security standpoints. In addition to organizations’ own internal efforts, such sharing could complement their cybersecurity handling tactics and benefit in various means such as (1) fostering cyber situational awareness, (2) developing proactive defense mechanisms, (3) clarity in understanding the threat landscape, malicious actors, security loopholes etc. Thus, organizations’ collaborations could decrease the time of threat detection, while increasing
the accuracy of detection [2, 3] at the same time. Considering the benefits of such sharing, U.S. Congress has passed a bill to promote threat-information sharing among the private entities as well as the federal agencies [4].

Let us first define a set of common security terms [5] which are asset, vulnerability, incident, and threat. An asset is an entity that we are trying to protect. It can be people, property, or information. A vulnerability is a weakness in our system. A vulnerability may exist in different models such as software vulnerability (due to wrong practice and design), Misconfiguration of IT infrastructure, operational or business process vulnerabilities, staffs mistakes intentionally or unintentionally. A threat is what we are trying to protect against. Anything which deliberately or unintentionally can exploit a vulnerability and cause damage to an asset. Finally, a security incident is caused by the exploitation of vulnerability from a threat.

Having these definitions, we now describe the concept of threat intelligence. Gartner [6] explains threat intelligence as “evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard”.

The most well-known applications of threat intelligence are web classification, IP reputation, web reputation, anti-phishing, file reputation, and app reputation [7].

Cybersecurity information sharing is a crucial part of cyber threat intelligence, allowing different entities to share their threat information. To provide a common platform for sharing such information, various protocols and specifications for cybersecurity information sharing such as TAXII, STIX, CybOX, VERIS, MAEC, SCAP, IODEF [8–11] have been developed. Various information can be shared among entities such as raw network logs, attackers techniques, the signature of attacks, and the vulnerabilities’ details. To develop a common platform for threat information exchange, Structured Threat Information Expression (STIX) has been
introduced to facilitate the exchange of cyber threat intelligence. STIX is a lan-
guage to represent the complex cyber threat intelligence, this is done by cate-
gorizing each piece of cyber threat information and then chaining these objects
together. STIX objects are [12]:

- Attack Pattern: The description of threat actors’ methods to compromise
targets. Known as Tactics, Techniques, and Procedures (TTP).

- Campaign: A grouping of adversarial behaviors that describes a set of mali-
cious activities or attacks that occur over a period of time against a specific
set of targets.

- The course of Action: A proper action to prevent or respond to an attack.

- Identity: Individuals, organizations, groups, or the classes of such entities.

- Indicator: A pattern to identify suspicious or malicious cyber activity.

- Intrusion Set: A grouped set of adversarial behaviors and resources with
common properties believed to be orchestrated by a single threat actor.

- Malware: A type of TTP, also known as malicious code and malicious soft-
ware, used to compromise the confidentiality, integrity, or availability of a
victim’s data or system.

- Observed Data: Conveys information observed on a system or network (e.g.,
an IP address).

- Report: Collections of threat intelligence focused on one or more topics, such
as a description of a threat actor, malware, or attack technique, including
contextual details.

- Threat Actor: Individuals, groups, or organizations believed to be operating
with malicious intent.
Figure 1.1: STIX 2.0 architecture

- **Tool**: Legitimate software that can be used by threat actors to perform attacks.

- **Vulnerability**: A mistake in software that can be directly used by a hacker to gain access to a system or network.

These objects are chained to each other by relationship objects to describe how STIX objects are connected to each other. Figure 1.1 displays the architecture of STIX 2.0 [13].

On the other side, to provide a community for cybersecurity information sharing in specific industries, Information Sharing and Analysis Centers (ISACs) [14] are
established. ISACs facilitate sharing threat data based on the business model. ISACs have a member-driven design, aiming to deliver cyber threat intelligence to asset owners. Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

Despite the benefits of cybersecurity information sharing, several challenges still exist, such as the risk of privacy violation, reputation/financial loss, lack of trust among participants, etc. due to sensitive information exposure while sharing the information. In this research, we study the problem of sharing sensitive information. We analyze the players’ decision considering the cost of sharing in a dynamic game. Moreover, we propose a framework to protect and hide the private data in the process of sharing cybersecurity information.

On the other hand, we need a mechanism to motivate organizations toward sharing cybersecurity information. Such a mechanism should be equipped with a rewarding process to encourage sharing behavior. To achieve this goal, we apply cyber-insurance as a measure to share the cost of cyber-attacks among organizations.

### 1.2 Cyber-Insurance

In spite of the necessity of having security measures, they are not sufficient to detect/prevent zero-day and sophisticated cyber-attacks. As a result, organizations are enduring massive damages caused by attackers. Since organizations cannot completely mitigate cyber-threats, they adopt cyber-insurance to transfer such
risks to another party known as the insurer. It is estimated that annual gross written premium will be increased from around $2.5 billion today to reach $7.5 billion by 2020 [15].

However, several challenges are circumventing the growth of the cyber-insurance market. For instance, the lack of reliable data to compute insurance premium, and legal and procedural hurdles for assessing the organizations’ security posture are two of them [16]. In addition, setting a proper insurance policy and premium is sophisticated. If the insurance policy is loose, the insurer might fail or even may go bankrupt, and if the policy is strict, the insured might withdraw from the contract and accept the risks. Moreover, asymmetric information between the insurer and insured exacerbates the situation causing moral hazard and adverse selection problems [17, 18]. Moral hazard refers to the case where insureds can increase the probability of the risks after signing the contract. For instance, the insured reduces its security investment after signing the insurance contract. On the other hand, users with high risk are more likely to take insurance, and an insurer cannot distinguish between insureds before signing the contract. This problem is known as adverse selection.

As the organizations are using the same software libraries, operating systems, firmware, applications, and hardware, they are susceptible to a common set of vulnerabilities. For instance, consider the Heartbleed vulnerability (CVE-2014-0160) in the OpenSSL library which was disclosed on April 2014 [19]. Heartbleed is a severe memory handling bug that results from improper input validation, which allows an attacker to steal the servers’ data that includes private keys, users’ session cookies, and passwords. It is estimated that around half a million of the secure web servers on the Internet certified by trusted authorities were vulnerable to the Heartbleed at the time of disclosure. This vulnerability affected other network services such as email servers, VPNs, and network appliances which were applying the OpenSSL library in their implementation [20].
Since organizations using the common platforms are suffering from the same set of vulnerabilities, their security is interdependent. In this situation, as one party’s investment on security and detection of a common platform’s vulnerabilities brings the positive externalities to other parties using the same platform, organizations tend to under-invest on security, expecting other organizations’ investment [21, 22].

Besides that, organizations using the same platform can reduce the damages of attacks by sharing their cybersecurity information. However, sharing such information is costly for organizations. For instance, reporting a successful cyber-attack may affect the organizations’ reputation negatively while such information can help other organizations to patch their systems to be safe from the same type of attack. Therefore, organizations tend to free-ride by taking advantage of the shared information while not reciprocating. In other words, if we model the cybersecurity information sharing as a non-cooperative game, although the sharing strategy is the socially optimal point, the not-sharing behavior is the Nash-Equilibrium point [23].

Therefore, it is important to motivate organizations to cybersecurity investment and sharing cybersecurity information. Such motivation can be done by assigning punishment/reward to the organizations. However, designing such mechanisms is a big challenge mainly because the provisioning of the cybersecurity investment and sharing is difficult.

Considering the organizations’ security interdependency and their demand for cyber-insurance, we study the design of coalitional insurance mechanisms with the goal of covering the adverse selection, moral hazard, and cybersecurity investment and sharing problems. To this end, we propose a synergistic insurance framework where organizations collaboratively insure a common platform instead of themselves. We present three models for insuring a common platform. In the first model, organizations act as both insurer and insured to distribute the risk in
the coalition. In the second model, the system provides rewards to crowdfund the insurance. Finally, in the third model, we investigate the outsourcing of a common platform insurance. Moreover, we study how such frameworks can improve social welfare by motivating organizations to collaborate on the cybersecurity investment and sharing.

1.3 Thesis Organization

The rest of this report is organized as follows. Next chapter reviews the related researches in cybersecurity information sharing. In chapter 3, we analyze the coalitional game theory approach for calculation of organizations’ rewarding and participation-fee in a cybersecurity information sharing system, then we study the application of differential privacy for private profit sharing calculation. In chapter 4, we propose a privacy-preserving cybersecurity information sharing framework to protect the organizations’ sensitive information. Chapter 5 investigates an application of cyber-insurance to motivate organizations toward cybersecurity collaboration. To this end, a new cyber-insurance framework for a common platform has been introduced. Finally, in chapter 6, we conclude the research.
Chapter 2

Background Studies

2.1 Development of Cybersecurity Information Sharing

The frequency and complexity of cyber attacks have increased with the substantial growth of our daily life dependency to the cyberspace. To get ahead of the security threats, it is crucial to have a proactive security approach to prevent any dangers before they occur. Cybersecurity information sharing is a key factor of proactively defending against sophisticated cyber attacks [24]. Moreover, such sharing decreases the time and enhances the accuracy of the detection and prevention of malicious behaviors in the system. Authors in [10] investigate the existing information exchange formats and protocols and compare them with respect to use-case scenario, sensitivity, interoperability, and scalability. Due to the importance of cybersecurity information sharing, governmental laws/initiatives have been legislated to mandate/encourage the governmental and private organizations to share their cybersecurity information [25]. Several information sharing programs, such as CISSP, NCCIC, ISAC, ISAO [26] are implemented by the Department of Homeland Security (DHS) to provide a collaborative platform
for understanding cybersecurity risks and defenses. For instance, the US Senate has passed the Cybersecurity Information Sharing Act (CISA) [27] federal law designed to improve cybersecurity through enhanced sharing of information about cybersecurity threats. The law allows the sharing of Internet traffic information between the US government and private companies. In the UK, Cybersecurity Information Sharing Partnership (CiSP) [28] is an initiative for industry and government that has been set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment to increase situational awareness and reduce the impact on UK business. EU has also launched several cross-sector and intra-sector initiatives to enhance the EU Member States capability for preparedness, cooperation, information exchange, coordination, and response to cyber threats. The bill “S.754-Cybersecurity Information Sharing Act (CISA) of 2015” [27] has been passed by the U.S. Senate. The bill encourages private companies, businesses, and federal organizations to share cyber-threat information with one another. To facilitate such sharing framework, ITU-T (International Telecommunication Union-Telecommunication) took the initiative to adopt the Cybersecurity Information Exchange (CYBEX) [29] to tighten cybersecurity and infrastructure protection. Dandurand et al [30] describe and investigate the high-level requirements for cybersecurity data exchange and collaboration infrastructure. To provide a common platform for sharing such information, various protocols and specifications for cybersecurity information sharing such as TAXII, STIX, CybOX, VERIS, MAEC, SCAP, IODEF, MISP [8–11, 31] have also developed. Malware Information Sharing Platform (MISP) [31] presents a trusted platform allowing the collection and sharing of important indicators of compromise (IoC) of targeted attacks. This platform also provides the capability to share fraud related information such as indicators of compromises in financial sectors. This helps to proactively defend against targeted attacks. Trusted Automated Exchange of Indicator Information (TAXII) is a protocol for exchanging cyber threat intelligence (CTI). TAXII is specifically designed to support the exchange of CTI
represented in STIX format. Structured Threat Information Expression (STIX) is a language and serialization format to exchange CTI. Using STIX, organizations can share CTI with one another in a consistent and machine-readable manner, this provides a better understanding of cyber-threats to security communities with the goal of faster and more effective responses to cyber-attacks\[12\]. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection, and response. STIX is an expressive, flexible, and extensible XML-based language that conveys potential cyber threat information. Both STIX and TAXII are developed in an open source and collaborative forum. STIX defines twelve STIX Domain Objects includes attack pattern, campaign, course of action, identity, indicator, intrusion set, malware, observed data, report, threat actor, tool, and vulnerability. Cyber Observable Expression (CybOX) is a standardized language for encoding and communicating high-fidelity information about cyber observables, whether dynamic events or stateful measures that are observable in the operational cyber domain. CybOX is not targeted at a single cyber security use case but rather is intended to be flexible enough to offer a common solution for all cyber security use cases requiring the ability to deal with cyber observables. It is also intended to be flexible enough to allow both the high-fidelity description of instances of cyber observables that have been measured in an operational context as well as more abstract patterns for potential observables that may be targeted for observation and analysis apriori. By specifying a common structured schematic mechanism for these cyber observables, the intent is to enable the potential for detailed automatable sharing, mapping, detection and analysis heuristics. CybOX is targeted to support a wide range of relevant cyber security domains including, threat assessment and characterization (detailed attack patterns), malware characterization, operational event management, logging, cyber situational awareness, incident response, indicator sharing, digital forensics and more. Relevant observable events or properties can be captured and shared,
defined in indicators and rules or used to adorn the appropriate portions of attack patterns and malware profiles in order to tie the logical pattern constructs to real-world evidence of their occurrence or presence for attack detection and characterization. Incident response and management can then take advantage of all of these capabilities to investigate occurring incidents, improve overall situational awareness and improve future attack detection, prevention and response[32]. A new method for sharing susceptible passwords as threat intelligence feed has been introduced in [33]. The authors in [34] discussed the automation of STIX document generation using honeypot.

### 2.2 Game Theoretic Analysis of Cybersecurity Information Sharing

Game theoretic analysis of Cybersecurity information sharing have been studied extensively in [21, 22, 35–37]. The security information sharing in competitive environments with the game theory approach has been studied in [36]. Khouzani et al. [22] has presented a Bayesian game for sharing vulnerabilities in a competitive environment and developed a monetary-free sharing mechanism by considering competitive loss, direct loss, and market shrinkage into account, which encourages the organizations to invest and share at the same time. The research investigates the Perfect Bayesian Equilibria (PBE) of the game between competing firms using the same platform and shares the same vulnerabilities in their systems. They analyze the incentives behind investments in the detection of the security vulnerabilities and sharing of their findings. The proposed game has two stages, first organization decide the investment amount for security researches, second organizations have to decide how much of information they should share with other organizations. Economic analysis of security information sharing and applying incentives for motivation has been studied in [21]. This research studies the optimal
incentive rate to motivate organizations for sharing and to prevent organizations from free-riding in cybersecurity information sharing. The role of a social planner to control free-riding in cybersecurity information sharing game has been investigated in [37]. Liu et al. investigate the socially optimal outcome where organizations are risk-averse. Economic impacts of mandatory security breach reporting through security audits and imposing sanctions in the principal-agent model have been studied in [35].

Using micro-economics models, various cybersecurity information sharing frameworks [38–42, 42–45] are studied in the past which emphasize on enhancing production efficiency. Authors in [38] propose an analytical framework to characterize the effective parameters for security investment and information sharing decision, and analyze the effects of the incentives for information sharing amongst competing firms and their impact on firms’ profits. The paper concludes that security technologies and information sharing act as strategic complements in equilibrium. Cavusoglu et al. [40] provide necessary and sufficient conditions to verify this fact that optimal information security can be attained at a lesser cost provided security information is shared. Since organizations share their threat data, some might take the opportunity to free-ride without exchanging anything back. Thus appropriate incentivization mechanism is required to prohibit the free-riding on other firms’ security information so that no firm can gain more by making under-investment. The research presented in [44] has proposed an evolutionary game-theoretic framework for cyber-threat information sharing where CYBEX dynamically controls the participation cost so as to enhance participation in the sharing framework.

Hausken [39] studies how the social planner can control the information sharing and security investment in a two-period game to achieve the most benefit. The [45] analyzes the benefits and drawbacks of information sharing by proposing a model among organizations with the different level of dependency. The proposed model
applies functional dependency network analysis to investigate the attacks propagation and game theory for information sharing management. Gao et al. [42] examine the role of security breach probability function in the decision of security investment and information sharing, then analyze the effects of social planner regulations in the decision of information sharing.

Tosh et al. [41] present a game-theoretic framework to investigate the economic benefits of cyber-threat information sharing and analyze the impacts and consequences of not participating in the game of information exchange. They model the information exchange framework as distributed non-cooperative game among the firms and investigate the implications of information sharing and security investments. [43] has studied the best-response strategy for cyber-investment as well as the amount of information to share in CYBEX.

The [46] have investigated the cybersecurity information sharing from an evolutionary game theoretic strategy and investigated the conditions under which the players’ self-enforced evolutionary stability can be achieved. Furthermore, the authors have presented a heuristic approach to obtain an evolutionary stable strategy.

2.2.1 Privacy-preservation in cybersecurity information sharing

To preserve the privacy of the organizations while sharing cybersecurity information, authors in [47] presents a privacy-preserving and aggregatable cybersecurity information sharing scheme. To this end, the scheme applies to combine format-preserving and homomorphic encryption cryptographic primitives. An attribute-based access control CYBEX mechanism has been presented in [48]. In [49], the best strategy for sharing information in CYBEX has been investigated.
In order to preserve the privacy in the shared information, anonymization and sanitization techniques have been studied extensively in [50–53]. These techniques eliminate sensitive information from original data such that the sanitized data fulfills the functionality requirements. However, these techniques are not adequate to protect the organizations’ sensitive information in cybersecurity information sharing as we study in this research.

In order to take advantage of sharing cybersecurity information, collaborative intrusion detection systems (CIDS) have been presented in [54–56]. These schemes investigate the requirements of CIDS components in order to detect sophisticated attacks. Besides, collaborative predictive blacklisting has been presented in [57, 58]. Freudriger et al. [59] have presented a controlled data sharing model for collaborative predictive blacklisting. In their model, entities estimate the benefits of collaboration and agree on what to share in a privacy-preserving way. Du et al. [60] discussed the application of secure multiparty computation in collaborative intrusion detection systems to preserve the privacy of the underlying information.

A good overview of privacy-preserving collaborative intrusion detection systems can be found in [61]. However, these schemes do not consider privacy preserving requirements in the cybersecurity information exchange framework.

Privacy risks in sharing cybersecurity information have been studied in [62]. In this work, the authors have studied the trade-off between the need for potentially sensitive data, and the perceived privacy risk of sharing that data.

A framework for privacy preservation of cybersecurity information sharing has been proposed in [63]. This scheme uses group signature to hide the identities of the organizations. However, this scheme does not protect the participants’ information. [23] has modeled the privacy issue in cybersecurity information sharing as a game between organizations and attackers. Although such a model helps the organizations to decide their sharing strategy, it does not provide any practical
solution to protect the underlying information. Badsha et al. [64] used homomorphic encryption to propose a privacy-preserving learning framework to compute an aggregated decision tree from the organizations’ cybersecurity information.

It is also worth to mention that, Goldman et al. [65] have studied the problem of information exchange in the multi-agent systems where the problem is to decide the optimal rate of information exchange among agents considering the cost of sharing information with the risk of revealing it to competing agents in an unreliable connection.

As in the cybersecurity information sharing, rewarding and participation-fee leaks sensitive information about the organizations’ cyber-infrastructure [66], we aim to protect those values. Applying cryptographic techniques, many research studies have been done to protect the private information while allowing the computation of a function. For instance, secure multiparty computation [67] and homomorphic encryption [68] are introduced to compute the result of a function without revealing the sensitive input parameters belonging to the entities. Despite the benefit of such methods, an attacker with side information accessing the output value can still infer private information. In order to overcome this challenge, perturbation techniques have been introduced [69]. In such methods, the output is perturbed to preserve the individual values private in the result while keeping the output utility as much as possible.

Differential privacy [70] is a well-known provable concept in the privacy literature which is independent of adversary and data. Differential privacy was first proposed to protect the statistical database where a trusted curator perturbs responses for the queries. Afterwards, this concept has been more developed in many other studies such as data-mining [71], mechanism design [72, 73], smart metering [74, 75], and distributed stream monitoring [76]. In this research, we
apply differential privacy to present privacy preserving profit sharing model for cybersecurity information sharing reward/participation-fee calculation.

## 2.3 Modeling the Cyber-insurance

The design of a cyber-insurance contract has been studied extensively in the literature [16–18, 77–86]. Johnson *et al.* [16] have formulated a one-shot security game with market insurance assuming homogeneous players, fair insurance premiums, and complete information. The result of this research demonstrates the importance of tuning the stipulations for security investment and the development of a market for cyber-insurance to achieve social welfare. The role of cyber-insurance in improving the overall security has been studied in [81, 83]. Pal *et al.* [81] have shown that in the oligopolistic cyber-insurance market, the network security is not improving. However, a monopoly cyber-insurer can help solve the moral hazard problem partially and improve network security by discriminating the contracts.

Tosh *et al.* [87] have modeled a three-layer game theoretic framework in which the players are organizations, adversaries, and the insurer, where the organization look for the optimal self-defense investment considering sharing cybersecurity information and cyber-insurance, the adversary aims to find the proper attack rate, and the insurer’s goal is to find the best coverage level. Khalili *et al.* [85] have investigated the premium discrimination model based on pre-screening to improve the insurer’s profits and circumvent the moral hazard problem. Moreover, the benefits of pre-screening in increasing the profit for the insurer and improving the network security have been studied in [78]. A differentiated pricing framework for security vendors has been proposed in [79] to improve the cyber-insurance market. In [84], the authors have studied the design of an incentive-compatible and attack-aware insurance policy by formulating a bi-level game framework to model the interaction of users, attackers, and insurers. The effect of risk interdependency
on insurer’s utility has been studied in [80, 88]. The result shows that the risk interdependency provides more profit to an insurer. A new model for insuring the cyber-products using the blockchain technology for crowdfunding has been introduced in [89].

In contrast to these research studies, in this work, we investigate the benefits of coalitional approaches for insuring a common platform. The reliability and security of an organization using a common platform depends on all other organizations’ collective effort in security. As a result, security investments by strategic players is typically modeled as a public-good problem, known as the Interdependent Security game [90]. As selfish players free-ride on positive externalities of others’ contributions, the equilibria for such games are usually inefficient. To solve this problem, we propose several mechanisms where organizations collaboratively participate in the insurance process. Such design push organizations toward cybersecurity cooperation while satisfying the mechanism design requirements as we study in section 5.
Chapter 3

A Coalitional Game Theory Approach for Cybersecurity Information Sharing

Considering the players of cybersecurity information sharing game as self-interested rational players, the sharing cybersecurity information can be costly for the information possessor. For example, attackers might utilize the shared information for reconnaissance, the competitive organization might take advantage of the shared information which indirectly affects the organization’s utility, and sensitive private information (such as names and email addresses) might leak out. On the other hand, the finder of a vulnerability can sell it on the black market. Thus, stimulating the owner of cybersecurity information to choose sharing behavior is a big challenge.

Plenty of research studies have been done in modeling the benefit and cost of the cybersecurity information sharing by applying game theory for instance [21, 22, 36]. Traditionally, the cybersecurity information sharing is modeled as a non-cooperative game where the players are the organizations, and the strategies are
choosing between sharing and not-sharing. In this case, we have the following conditions: if none of the organizations share their information, the organizations’ payoffs are zero, if some of the organizations participate in sharing, but the others refuse to reciprocate, then the organizations who refused, receive better payoff than the rest of them. Finally, if all of the organizations share, then all of them benefit from sharing. This game resembles the well-known Prisoner’s Dilemma game [91]. Although the best payoff is received from mutual sharing, players choose not-sharing as their Nash Equilibrium approach.

To change the equilibrium point to the sharing strategy, we need a mechanism to stimulate the sharing behavior. Here, choosing the proper rewarding value is a big challenge. To stimulate organizations to share applicable information, the reward should be an increasing function of the total benefits of the other organizations applying the information. Furthermore, as we assume the organizations are the only financial sources of the cybersecurity information sharing system, the total rewards are equal to the total amount of organizations’ participation-fee. The participation-fee calculation ought to prevent organizations from free-ride by taking advantage of shared information without participation. Furthermore, this fee should be fair, such that the organizations’ payment should be proportional to their benefits from the information.

On the other hand, organizations’ participation-fees are classified as confidential information since they reveal the organizations’ cyber-infrastructure configuration through the organizations’ cybersecurity investment tendency [66]. Disclosure of organizations’ participation-fee, paves the attackers’ way for reconnaissance to exploit the organizations’ vulnerabilities. Thus, the value of organizations’ participation-fee should be protected. As an example, consider that a vulnerability in a specific database management system has been detected and an organization is interested to pay a big amount of money to access such information. Such an
In this chapter, we investigate the fair and private rewarding and participation-fee calculation by applying the coalitional game theory and differential privacy in the cybersecurity information sharing system. The main objective of our proposed mechanism is to stimulate organizations to share more useful information with the goal of increasing the organizations’ payoff fairly while preserving the participants’ participation-fee private. To achieve this goal, first we investigate the solution concepts of Shapley value and Nucleolus allocations in the cybersecurity information sharing game. Second, we inspect the differential privacy concept in the coalitional cybersecurity information sharing rewarding.

In this chapter, we present a novel coalitional game for rewarding and participation-fee allocation in the cybersecurity information sharing, and then we investigate the Shapley value and Nucleolus distribution solution concepts of utility among organizations in the cybersecurity information sharing. Moreover, we investigate the application of differential privacy in coalitional game theory. For this purpose, we relax the fairness definition by introducing δ-fair concept. Then, we study the rewarding mechanism in the coalitional cybersecurity information sharing environment, such that the organizations’ participation-fees are protected from an adversary with side information.

### 3.1 Overview and Problem Statement

Let $O = \{o_1, ..., o_n\}$ represent the organizations participating in cybersecurity information sharing. Although various information can be shared among organizations such as raw network logs, attackers techniques, the signature of attacks, and
the vulnerabilities’ details, in this work, we particularly focus on sharing discovered security vulnerabilities as in [22]. In each sharing cycle, a set of vulnerabilities \( V = \{v_1, ..., v_m\} \) will be detected by the participant organizations. For example, a cycle can be a time window of a year. Each vulnerability is associated with a unique feature set \( F_{v_k} \in V \), which is the vulnerability specification.

As an example, consider vulnerability CVE-2016-10012\(^1\). The feature set of this vulnerability is shown in Table 3.1. In this table, CVSS (Common Vulnerability Scoring System, https://nvd.nist.gov/vuln-metrics/cvss) is a metric for the calculation of vulnerabilities’ impacts, and CWE (Common Weakness Enumeration, https://cwe.mitre.org/) represents the weakness category.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS</td>
<td>7.2</td>
</tr>
<tr>
<td>Confidentiality Impact</td>
<td>Complete (There is total information disclosure, resulting in all system files being revealed.)</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)</td>
</tr>
<tr>
<td>Authentication</td>
<td>Not required (Authentication is not required to exploit the vulnerability.)</td>
</tr>
<tr>
<td>Gained Access</td>
<td>None</td>
</tr>
<tr>
<td>Vulnerability Type(s)</td>
<td>Overflow Gain privileges</td>
</tr>
<tr>
<td>CWE ID</td>
<td>119</td>
</tr>
<tr>
<td>Vendor, Product, Version</td>
<td>Openbsd, Openssh, 7.3</td>
</tr>
</tbody>
</table>

Having \( F_{v_k} \), organizations can calculate the expected cost of vulnerability exploitation. For example, assume there is a vulnerability allowing the attackers to gain access to the data of a database system. This can be realized from the vulnerability properties CVE. The exposing of underlying data has different costs for

\(^1\)http://www.cvedetails.com/cve/CVE-2016-10012/
the organizations. Therefore, the organizations would value the vulnerability information differently considering the cost and benefit of patching their vulnerable systems. Such valuations are performed considering the risk estimation of the exploitation of the vulnerabilities associated with the affected assets. Let \( \pi_i(F_{v_k}) \) be the expected cost of exploitation of vulnerability \( v_k \) for \( o_i \). Let \( P_i(F_{v_k}) \) and \( E_i(F_{v_k}) \) denote the probability and the cost of successful exploitation of \( v_k \) for \( o_i \), respectively. Thus, we can calculate the expected cost as

\[
\pi_i(F_{v_k}) = P_i(F_{v_k}) \times E_i(F_{v_k})
\]  

(3.1)

In the rest of chapter, we will denote \( \pi_i(F_{v_k}) \) with \( \pi_{i,k} \) for simplicity. If \( o_i \) patches the vulnerability by accessing the shared information before exploitation, then \( \pi_{i,k} \) is the expected benefit of accessing the shared information for \( o_i \) regarding the vulnerability \( v_k \).

We assume there is a trusted third party server \( S \), verifying the vulnerability information and computing the participation-fee and reward for the players.

Once \( o_j \) submits the vulnerability information \( v_k \) to \( S \), \( S \) first verifies it and then calculate the reward \( r_{j,k} \). The reward \( r_{j,k} \) is the total payment of the other participant organizations \( o_i \neq j \) for accessing the vulnerability information \( v_k \). Let \( x_{i,k} \) denote the \( o_i \)'s payment for accessing the shared information of the vulnerability \( v_k \). Hereafter, the term participation-fee represents \( x_{i,k} \). The possessor of vulnerability information decides whether to share the vulnerability information or not, based upon the proposed reward value \( r_{j,k} = \sum_{o_i \in O} x_{i,k} \). Let \( f_i \) denote the membership-fee of \( o_i \) at the end of cybersecurity information sharing, then \( f_i \) is computed as

\[
f_i = \sum_{v_k \in V} (x_{i,k} - r_{i,k})
\]

(3.2)
The steps of information sharing are as follows. At the first step, organizations register into the system by providing the certificates and their platform information to $S$. As the vulnerability information is sensitive and can be used by malicious entities to attack the other systems, in the proposed model, the framework requires to authenticate the organizations to prevent the entrance of malicious entities. When a new vulnerability has been detected by one of the members, $S$ calculates the patching benefit and participation-fee for the organizations getting advantage of such information. Then, based on the total participation-fee, $S$ computes the reward value for the information possessor.

When a cybersecurity information sharing cycle ends, $S$ calculates the membership-fee $f_i$. If $f_i$ is negative, then $S$ pays corresponding amount to $o_i$, and if $f_i$ is positive, then $o_i$ pays corresponding amount to $S$.

Figure 3.1 displays the general architecture of cybersecurity information sharing system, and Figure 3.2 depicts the overall picture of participation-fee and reward calculation.

On the other hand, we assume there is an adversary accessing the reward value $r_{i,k}$, and aiming to estimate the victim organization’s participation-fee. We assume adversary has side information and organizations might collude with an adversary by sharing their participation-fee. Our goal is to present an efficient mechanism for preserving the privacy of an organization’s participation-fee while approximating fair profit sharing in the process of rewarding. More specifically, the fair and private mechanism should satisfy the following requirements.

**Fairness** The rewarding and participation-fee allocation should be fair, such that the reward is calculated based on the organizations’ advantage from the information, and participation-fee is calculated based on the advantage receives from the information. Furthermore, in the privacy preserving model, the cost of augmented noise to the reward value should be distributed fairly among participants.
**Privacy** The mechanism should prevent an adversary with side information to infer an organization’s participation-fee. An adversary might have access to participation-fees of some organizations by colluding with them.
Having this system model, first we study the fair profit sharing among organizations by investigating the Shapley value and Nucleolus solution concepts. Then, we examine the private rewarding method to protect an organization’s participation-fee $x_{j,k}$ from an adversary with the side information. To achieve this goal, we present a differentially private rewarding mechanism.

### 3.2 Rewarding in Coalitional Game with Transferable Utility

In this section, first, we introduce the coalitional games, then we investigate the requirements of participation-fee and reward calculation for cybersecurity information sharing system. Finally, we analyze the solution concepts for the coalitional formation of cybersecurity information sharing game.

#### 3.2.1 Coalitional Game

Coalitional game theory studies the behavior of rational self-interested players in strategic settings where players reach agreements to elevate their payoffs. The main question in a coalitional game is how to share the benefits among agents in a coalition. The most well-known solution concepts for such sharing are the Shapley value [92] and the Nucleolus [93]. Saad et al. [94] classify the coalitional game into three different groups as canonical coalitional games, coalition formation games, and coalitional graph games. In canonical coalitional games, the grand coalition of all users is an optimal structure and is of major importance and the problem is to stabilize the grand coalition. In coalition formation games, the network structure that forms depends on gains and costs from cooperation and the problem is how to form an appropriate coalitional topology. In coalitional graph games, players’ interactions are governed by a communication graph structure and the problem is
to stabilize the grand coalition or form a network structure taking into account
the communication graph.

Since in cybersecurity information sharing system, the goal is to have the grand
coalition of the entities to maximize the benefits of sharing information, the prob-
lem of proper rewarding and participation-fee allocation falls into canonical coaliti-
tional games category. Canonical coalitional games have been studied in the wire-
less network area. For instance, Singh et al. [95] discuss the profit sharing in
coalition base resource allocation in wireless networks, and fair payoff allocation
for cooperation in wireless ad-hoc networks using Shapley value is studied in [96].
Muto et al. [97] categorize a set of coalitional games as big-boss games. In such
games, the coalition value is dependent on the existence of a specific player (namely
big-boss) in the coalition. The coalition of subsets not containing the big-boss re-
ceives zero value. In this work, we model the cybersecurity information sharing
as a coalitional game such that if the information possessor does not locate in the
coalition then there is no benefit for any member of the coalition. Hence, this game
is a subset of big-boss games. Afterward, we investigate the solution concepts of
profit sharing in the cybersecurity information sharing game.

As pointed out earlier, typically organizations are not willing to share their cy-
bersecurity information because of the sharing cost. Let $\tau_{i,k}$ denote the sharing
cost of $v_k$ for $o_i$, then $o_i$ would share $v_k$ if and only if $\tau_{i,k} < r_{i,k}$. Besides that, the
impacts of vulnerabilities are not equal and other organizations $o_j \neq i$, would pay
$x_{j,k}$ to access $v_k$ to patch their systems as long as the patching benefit outweighs
the participation-fee, in other words we have $x_{j,k} < \pi_{j,k}$. If $x_{j,k}$ is small, then
the reward may not be motivative for $o_i$, and as a result, $o_i$ will not share the
information, resulting in risk of vulnerability exploitation for $o_j$. On the other
hand, if $x_{j,k}$ is large, then the margin of profit for $o_j$ is small. Thus, in this setting,
we are interested in the fair distribution of the utilities among organizations to
satisfy all of them. To achieve this goal, first, we define the following features for the rewarding mechanism in cybersecurity information sharing.

**Definition 4.1.** The rewarding mechanism of the cybersecurity information sharing is *dynamic* if it calculates the reward based on the overall benefits to the system. In the dynamic rewarding mechanism, the participants are motivated to share more useful information since the reward is an increasing function of the benefits achieved by the other organizations exploiting the shared information.

**Definition 4.2.** The rewarding mechanism of the cybersecurity information sharing is *fair* if the participation-fee for beneficiary organizations calculated based on their advantages from accessing the information. If the rewarding mechanism is not fair, organizations may not contribute to the reward value (since their benefits may not outweigh the payment cost). In this case, the reward may not be motive for the information possessor and as a result, the information will not be shared in the system.

**Definition 4.3.** The rewarding mechanism of the cybersecurity information sharing is *stable*, if it is dynamic and fair.

As we are interested in finding the *stable* rewarding mechanism, we investigate the profit sharing in the coalition formation of cybersecurity information sharing.

### 3.2.2 Profit Sharing

In coalitional game with transferable utility, an n-person game is given by the pair $G(N,v)$, where $N = \{1, 2, ..., n\}$ is the set of players and $v$ is a real-valued payoff that the coalition’s members can distribute among themselves. $v$ is also called the characteristic function of the game, which returns a value for each subset of $N$. In other words $v : 2^N \rightarrow \mathbb{R}$. *Superadditivity* and *Convexity* of the game are defined as follows.
Definition 4.4. (Superadditivity) A game $G(N,v)$ is superadditive, if for all $S, T \subset N$ and $(S \cap T = \emptyset)$, then $v(S) + v(T) \leq v(S \cup T)$.

Definition 4.5. (Convexity) A game $G(N,v)$ is convex if for all $S, T \subset N$, then $v(S \cup T) \geq v(S) + v(T) - v(S \cap T)$.

While the characteristic function describes the payoff available to coalitions, it does not prescribe a way of distributing these payoffs. An allocation is a vector $\bar{x} = (x_1, ..., x_n)$ assigning payoff to each player. In the cybersecurity information sharing game, we are looking for an allocation which stimulates organizations to make the largest coalition. In other words, we are looking for an allocation which is located in the Core.

Definition 4.6. (Core) An allocation $x$ is in the core of $G(N,v)$ iff $x(N) = v(N)$ and for any $S \subseteq N$ we have $x(S) \geq v(S)$. In words, core is the set of $x$ payoff allocations with the property that no coalition of agents can guarantee all of its members a payoff higher than to what they currently receive under $x$.

As the Core allocation is a set of allocations that are feasible and cannot be improved upon by any coalition, the Core allocation is Pareto efficient. Therefore, there is no pareto improvement from Core allocation. We investigate two most widely used fair allocation methods in this chapter which are Shapley Value [92] and Nucleolus [93].

Definition 4.7. (Shapley Value) The Shapley value deals with dividing the surplus among players in a coalition. Given the coalition $(v, N)$, the Shapley value for each player $i$ is calculated as:

$$\phi_i(v) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(n-|S|-1)!}{n!} [v(S \cup \{i\}) - v(S)]$$ (3.3)
Definition 4.8. (*Nucleolus*) *Nucleolus* searches for the allocation which minimizes the worst inequity. As an inequity measure of an allocation $x$, it uses *excess* value as

$$e(x, S) = v(S) - \sum_{j \in S} x_j$$  \hspace{1cm} (3.4)

Both *Shapley value* and *Nucleolus* prescribe a unique solution in all cases.

### 3.2.3 Coalition Formation

Here, we model the cybersecurity information sharing as a multi-stage coalitional game. The game players are the organizations. The information possessor $o_i$ strategy is to decide whether to share or not to share the information taking into account the reward value $r_{i,k}$. If $o_i$ decides to share the vulnerability information $v_k$, then its utility is $u_{i,k} = r_{i,k} - \tau_{i,k}$. On the other side, when the vulnerability gets shared then the utility of $o_{j \neq i}$ players are $u_{j,k} = \pi_{j,k} - x_{j,k}$. This game has $m$ stages where $m$ represent the number of vulnerabilities which are being detected in the cybersecurity information sharing cycle. Thus, the characteristic function of this game for each stage is

$$v(S) = \begin{cases} 
0 & |S| = 1 \text{ or } i \notin S \\
\sum_{j \in S} \pi_{j,k} & i \in S 
\end{cases}$$  \hspace{1cm} (3.5)

Here, the value of a single coalition is equal to 0, this is due to the fact that no information is getting shared between entities. If the information possessor belongs to the coalition, then the value of coalition is equal to the total benefit of organizations existing in the coalition. In this case, the organizations receiving profits from the shared information should pay to the information possessor.
As an example, consider we have \( O = \{o_1, o_2, o_3\} \). \( o_1 \) detects a vulnerability \( v_k \) and shares its feature set \( F_{v_k} \) to \( o_2 \) and \( o_3 \). Then, \( S \) computes the patching benefit of this vulnerability over \( o_2 \) and \( o_3 \) as \( \pi_{2,k} = 5, \pi_{3,k} = 12 \). In this case, for \( |S| = 1 \) or \( o_1 \notin S \), no information is getting shared and as a result, the value of coalition is zero. For, \( S = \{o_1, o_2\} \), \( S = \{o_1, o_3\} \), and \( S = \{o_1, o_2, o_3\} \), the coalition values are \( v(S) = 5 \), \( v(S) = 12 \), and \( v(S) = 17 \) respectively.

In this setting, it is trivial that there is no incentive for any subset of the members to separate and form smaller cooperation. In other words, this game is Superadditive. In the following, we investigate the Shapley value and Nucleolus allocations for the cybersecurity information sharing game.

**Theorem 4.1.** The Shapley Value allocation for the cybersecurity information sharing coalitional game is located in the Core.

**Proof:** The Shapley Value solution of a convex game is in the core [98]. Thus we investigate the convexity of the game. As in this game \( v(S \cup T) = v(S) + v(T) \) and the value of \( v(S \cap T) \geq 0 \), thus the game is convex and the Shapley Value solution is in the core. 

**Theorem 4.2.** The Shapley value of the \( o_i \) (information possessor) is half of the total patching benefits of other organizations accessing the information, and the Shapley value for \( o_{j \neq i} \) is half of its patching benefit from accessing the information in cybersecurity information sharing game.

**Proof:** First we start from the Shapley Value of the \( o_i \). Let \( (S \subseteq N \setminus \{i\}, |S| = p) \), to simplify the proof we use an auxiliary variable \( V_p \) as

\[
V_p = \frac{p!(n-p-1)!}{n!} 
\]  

(3.6)
Then based on equations (3.3) and (3.6) we have

\[ \phi_i(v) = \sum_{p=1}^{n-1} \mathcal{V}_p \cdot \sum_{S \subseteq N \setminus \{i\}} [v(S \cup \{i\}) - v(S)] \]

Note that, when \( p = n \), then the coalition contains \( o_i \), and thus we do not count this subset. Based on equation (3.5), \( v(S) = 0 \) and the value of \( v(S \cup \{i\}) \) is a coefficient of \( \sum_j \pi_{j,k} \), in other words \( v(S \cup \{i\}) = \alpha_p \cdot \sum_j \pi_{j,k} \). Hence, we can rewrite \( \phi_i(v) \) as

\[ \phi_i(v) = \sum_{p=1}^{n-1} \frac{p!(n - p - 1)!}{n!} \cdot \alpha_p \cdot \sum_j \pi_{j,k} \]

As the number of subsets \( (S \subseteq N \setminus \{i\}, |S| = p) \) is \( \binom{n-1}{p} \) and for each subset \( S \), we have \( \frac{p}{n-1} \) benefit values, thus we can calculate \( \alpha_p \) as

\[ \alpha_p = \binom{n-1}{p} \cdot \frac{p}{n-1} \]

Thus \( \phi_i(v) \) is

\[
\phi_i(v) = \sum_{p=1}^{n-1} \frac{p!(n - p - 1)!}{n!} \cdot \binom{n-1}{p} \cdot \frac{p}{n-1} \cdot \sum_j \pi_{j,k} \\
= \sum_{p=1}^{n-1} \frac{p!(n - p - 1)!(n-1)! \cdot p}{n!p!(n-p-1)! \cdot (n-1)!} \cdot \sum_j \pi_{j,k} \\
= \sum_{p=1}^{n-1} \frac{p}{n(n-1)} \cdot \sum_j \pi_{j,k} \\
= \frac{1}{n(n-1)} \sum_{p=1}^{n-1} p \cdot \sum_j \pi_{j,k} \\
= \frac{1}{n(n-1)} \cdot \frac{n(n-1)}{2} \cdot \sum_j \pi_{j,k} \\
= \frac{1}{2} \cdot \sum_j \pi_{j,k}
\]

Now we compute \( o_j \)'s Shapley Value. For \( o_j \), we need to count the subsets \( S \) containing \( o_i \), since the coalition values for other subsets are zero. In this case, we
have \([v(S \cup \{j\}) - v(S)] = \pi_{j,k}\). Thus, we have \(\sum_{S \subseteq N \setminus \{j\}} [v(S \cup \{j\}) - v(S)] = \beta_p \cdot \pi_{j,k}\), where \(\beta_p\) is the number of subsets \(\{S \subseteq N \setminus \{j\}, \{i\} \in S, |S| = p\}\) which is

\[
\beta_p = \binom{n - 2}{p - 1}
\]

Thus we have

\[
\phi_j(v) = \sum_{p=1}^{n-1} \frac{p!(n-p-1)!}{n!} \cdot \binom{n-2}{p-1} \cdot \pi_{j,k}
\]

\[
= \sum_{p=1}^{n-1} \frac{p!(n-p-1)!(n-2)!}{n!(p-1)!(n-p-1)!} \cdot \pi_{j,k}
\]

\[
= \sum_{p=1}^{n-1} \frac{p}{n(n-1)} \cdot \pi_{j,k}
\]

\[
= \frac{1}{n(n-1)} \sum_{p=1}^{n-1} p \cdot \pi_{j,k}
\]

\[
= \frac{1}{n(n-1)} \cdot \frac{n(n-1)}{2} \cdot \pi_{j,k}
\]

\[
= \frac{1}{2} \cdot \pi_{j,k}
\]

**Theorem 4.3.** The Shapley value and Nucleolus solution concepts, coincide in the cybersecurity information sharing game.

**Proof:**

In order to proof this theorem, we calculate the excess value in equation (3.4) with the Shapley Value allocation. Let \(o_i\) indicate the information possessor and \(o_{j \neq i}\) represent other organizations. For subsets \(|S| = 1\) and \(i \notin S\), the coalition value is zero \(v(S) = 0\) and we have \(\sum_{j \in S} x_j = 0\), thus we have \(e(x, S) = 0\). For the remain subsets, according to theorem (2) \(o_i\)'s allocation is \(\frac{1}{2} \sum_{j \in S} \pi_{j,k}\) and \(o_j\)' allocation is \(\frac{1}{2} \pi_{j,k}\). By replacing the coalition value according to equation (3.5) characteristic
function, we have

\[ e(x, S) = v(S) - (x_i + \sum_{j \in S} x_j) \]

\[ = \sum_{j \in S} \pi_{j,k} - (\frac{1}{2} \sum_{j \in S} \pi_{j,k} + \sum_{j \in S} \frac{1}{2} \pi_{j,k}) = 0 \]

As the excess value for all of the subsets are equal to zero and since Nucleolus present a unique solution, then we conclude that the solution concepts of the Shapley Value and Nucleolus coincide in the cybersecurity information sharing game.

So far we have analyzed the fair profit sharing in cybersecurity information sharing. However, as the participation-fee reveals sensitive information about the organizations’ cyber-infrastructure, in the next section we propose a method to protect participation-fee.

### 3.3 Differentially Private Rewarding

As the organizations’ participation-fee in the cybersecurity information sharing rewarding system reveals sensitive information about the organizations’ cyber-infrastructure, and such information can be exploited by the attackers to exploit the organizations’ vulnerabilities, it is critical to protecting the organizations’ participation-fee. To this end, in this section, we propose a differentially private mechanism for cybersecurity information sharing coalitional game. First, we describe the differential privacy and the methods for achieving this requirement. Then, we analyze the security requirements for cybersecurity information sharing.
Finally, we propose our algorithm and check if it fulfills the differential privacy requirement.

### 3.3.1 Differential Privacy

The notion of differential privacy [70] was first introduced in the statistical database to hide sensitive private data in aggregate statistical information. Roughly speaking, the goal of differential privacy is to allow learning useful information about a population in the database while protecting an individual’s information. By applying differential privacy, the responses to the queries are independent of the presence or absence of an individual in the database. This method applies a randomized response to prevent an adversary armed with background information to infer the existence of an individual in the database with a probability. Formally we can define the differential privacy as follows.

**Definition 5.1.** *(Differential privacy)* [70] Let \( D \in \mathbb{N}^{|\mathcal{U}|} \) denote a collection of records from a universe \( \mathcal{U} \). A randomized algorithm \( \mathcal{M}(D) \) is \( \epsilon \)-differentially private if for any set of possible output \( O \subseteq \text{Range}(\mathcal{M}) \) and for any adjacent databases \( D, D' \in \mathbb{N}^{|\mathcal{U}|} \) such that \( ||D - D'||_1 \leq 1 \) (\( D, D' \) known as neighbor databases which only differ in one record), we have

\[
\Pr[\mathcal{M}(D) \in O] \leq e^\epsilon \times \Pr[\mathcal{M}(D') \in O]
\] (3.7)

In this definition, \( \epsilon \) is known as the privacy budget. The smaller value of \( \epsilon \) leading stricter indistinguishability and improves privacy. In words, Definition 5.1 indicates that by having access to the differentially private mechanism output, it is unlikely to distinguish which of two neighboring databases are given as input to the mechanism. There are two well-known tools to provide differential privacy as described in the following.
1) **The Laplace Mechanism** [70]

In this technique, a noise value is appended to the output to hide the original value. One way to calculate the noise is to sample it from the Laplace distribution. In this case, first, the global sensitivity rate is measured. Given any function \( f : \mathbb{N}^{[d]} \to \mathcal{O} \), the global sensitivity of \( f \) is defined as

\[
\Delta f = \max_{D, D' \in \mathbb{N}^{[d]}} \frac{||f(D) - f(D')||_1}{||D-D'||_1 = 1}
\]  

(3.8)

Then, the Laplace mechanism calculates the output as follows

\[
\mathcal{M}(D, f(\cdot), \epsilon) = f(D) + \text{Lap}(\Delta f / \epsilon)
\]  

(3.9)

2) **The Exponential Mechanism** [72]

The exponential mechanism chooses output with probability considering the utility of output while preserving the result differentially private. More precisely, let \( u(D, O) : (\mathbb{N}^{[d]} \times \mathcal{O}) \to \mathbb{R} \) represent the utility function receiving the database and mechanism output value as input and returns the utility score. Let’s define \( \Delta u \) as

\[
\Delta u = \max_{D, D' : ||D-D'||_1 \leq 1} \max_{O \in \mathcal{O}} |u(D, O) - u(D', O)|
\]

(3.10)

Then, the mechanism \( \mathcal{M}(D, u) \) is \( \epsilon \)-differentially private if it returns \( O \) with probability proportional to \( \exp\left(\frac{\epsilon u(D, O)}{2\Delta u}\right) \).

### 3.3.2 Private Rewarding Mechanism

In the fair and private rewarding mechanism, as we want to keep the fairness property, we apply the exponential mechanism to preserve the fairness quality.
The Laplace mechanism can not directly be applied in cybersecurity information sharing rewarding, it is because the global sensitivity range can be large causing the noise value increases substantially and as a result, the participation-fee might get larger than the patching benefit. Hence, we apply the exponential mechanism.

In order to apply the exponential mechanism, first, we need to define the utility function. As our mechanism needs to fulfill fairness along with the privacy, we define the utility function considering fairness. To this end, we relax the fairness allocation presented in the profit sharing by defining δ-fairness.

**Definition 5.2.** Let \( \Psi = (\psi_1, ..., \psi_n) \) represent the fair allocation, then the allocation \( \bar{x} = (x_1, ..., x_n) \) is δ-fair if for all \( x_i \), we have \( x_i \in (\psi_i - \delta, \psi_i + \delta) \).

According to δ-fairness definition, and the fair profit sharing discussed in section 3.2, in the cybersecurity information sharing rewarding, for the information possessor \( o_i \), an allocation \( x_i \) is δ-fair if we have \( x_i \in (1/2 \sum_j \pi_j - \delta, 1/2 \sum_j \pi_j + \delta) \), and for \( o_j \) exploiting the patching benefit, an allocation \( x_j \) is δ-fair if we have \( x_j \in (1/2 \pi_j - \delta, 1/2 \pi_j + \delta) \).

Note that, δ value should be chosen in a way to fulfill the differential privacy requirement. More precisely, when the probability of output for a mechanism over a database input is larger than zero, then the probability of output for the mechanism over the adjacent database should also be larger than zero. Formally we have

\[
(\Pr[\mathcal{M}(\mathcal{D}) \in \mathcal{O}] > 0) \Rightarrow (\Pr[\mathcal{M}(\mathcal{D}') \in \mathcal{O}] > 0)
\]  

(3.11)

To meet this requirement, the δ value should be chosen such that if the most effective element in the database is removed then the probability of mechanism
output is still larger than zero. Formally we have

$$
\hat{x} < \sum_{n=2}^{\infty} \delta
$$

s.t. \( \hat{x} \in D, \hat{x} = \arg \max |M(D) - M(D - \hat{x})|_1 \) (3.12)

This requirement indicates that with the increasing of the input values variance and also with the decreasing of the number of input elements, \( \delta \) value should be increased, which results in the increasing of fairness cost.

As the randomized response is changing the fair profit sharing, we are interested in finding the \( \delta \)-fair private profit sharing. Our proposed mechanism has two parts. In the first part, we deal with finding the private and \( \delta \)-fair reward value, and in the second part, we investigate the private and \( \delta \)-fair cost division among participants.

Let \( X = (x_1, \ldots, x_n) \) represent the profit allocation given the allocation of information possessor \( x_i = r_i \). The algorithm (1) takes as input the privacy budget \( \epsilon \) and the fair profit sharing vector \( \Psi = (\psi_1, \ldots, \psi_n) \) (which is \( \psi_j = \pi_j / 2 \) and \( \psi_i = \sum_j \pi_j / 2 \) in cybersecurity information sharing), and obtains the private \( \delta \)-fair reward \( r_i \) as output.

In the beginning, \( \delta \) value is selected in such a way to fulfill the requirement (3.12). As the goal of the privacy preserving algorithm is to retain fairness as much as possible, we define the utility function as follows

$$
u(\Psi, X) = \frac{1}{||X - \Psi||_1 + 1} \quad (3.13)$$

In this definition, we consider the increasing of distance between profit allocation and fair profit sharing decrease the utility. As the maximum value of utility is
obtained in Ψ allocation, then according to equation (3.10) we have

$$\Delta u(\Psi, \mathbf{X}) = \frac{1}{||\Psi - \Psi||_1 + 1} - \frac{1}{\max(\psi_j) + 1}$$

$$= 1 - \frac{1}{\max(\psi_j) + 1} = \frac{\max(\psi_j)}{\max(\psi_j) + 1}$$

(3.14)

To meet the δ-fair requirement, the candidate reward values are taken from ($\psi_i - \delta, \psi_i + \delta$) range. Then, the probability distribution of different values for reward is calculated and the output is sampled from the following distribution.

$$Pr[r_i = x_i] = \frac{\exp\left(\frac{\epsilon.(\max(\psi_j) + 1)}{2.(||\mathbf{X} - \Psi||_1 + 1).\max(\psi_j)}\right)}{\sum_{x_i \in (\psi_i - \delta, \psi_i + \delta)} \exp\left(\frac{\epsilon.(\max(\psi_j) + 1)}{2.(||\mathbf{X} - \Psi||_1 + 1).\max(\psi_j)}\right)}$$

(3.15)

This distribution is chosen to fulfill the differential privacy requirement as discussed in theorem 5.1. Note that, with the decrease of the distance to fair allocation, the probability increases exponentially. This makes the distribution to be biased toward fair profit sharing while fulfilling the differential privacy requirement.

**Theorem 5.1** Algorithm (1) is δ-fair and ε-differentially private.  

*Proof:* It is trivial that Algorithm (1) is δ-fair as the range of samples is ($\psi_i - \delta, \psi_i + \delta$). In order to prove ε-differential privacy, we investigate the probability of having the same output for two neighbor profiles $\mathbf{X}, \mathbf{X'}$. We sketch the proof from [99]. Thus we have

(Note that, $||\mathbf{X} - \Psi||_1 - ||\mathbf{X'} - \Psi||_1 \leq \max(\psi_j)$.)
Hence we can rewrite the probabilities as follows

$$Pr[Alg1(X) = r] \leq \exp(\epsilon).Pr[Alg1(X') = r]$$

Algorithm 1: Randomized algorithm for finding the differentially private reward value

\[\text{Input : Privacy budget } \epsilon, \text{ fairness threshold } \delta, \text{ and fair profit sharing vector } \Psi\]

\[\text{Output: The randomized private } \delta\text{-fair reward value } r_i\]

1. \(S \leftarrow 0;\)
2. \textbf{foreach } \(x_i \in (\psi_i - \delta, \psi_i + \delta) \textbf{ do}\)
3. \quad \(S \leftarrow S + \exp\left(\frac{\epsilon.\max(\psi_i) + 1}{2(||X - \Psi||_1 + 1).\max(\psi_i)}\right);\)
4. \textbf{end}\)
5. Sample \(r_i\) from the following distribution \(Pr[r_i = x_i] = \frac{\exp\left(\frac{\epsilon.\max(\psi_i) + 1}{2(||X - \Psi||_1 + 1).\max(\psi_i)}\right)}{S}\)
6. \textbf{return } r_i;\)

In the next algorithm, we apply differential privacy to privately divide the cost of reward into the organizations considering their patching benefits. Note that, if we divide the cost fairly, this problem is a particular instance of the airport
cost allocation game [100]. In this case, the adversary with side information and the collusion of organizations reveals the victim’s patching benefit. Thus, in algorithm (3) we randomize the cost to preserve the differential privacy. In this case, we model the utility function as follows

$$u(X, Y) = \frac{1}{||Y - X||_1 + 1}$$ \hspace{1cm} (3.16)

Having this definition, with the increase of distance of allocation and As the maximum utility is obtained in $Y = X$, then $\Delta u$ is

$$\Delta u(X, Y) = \frac{1}{||Y - X||_1 + 1} - \frac{1}{||X - (X - \max(x_j))||_1 + 1}$$

$$= 1 - \frac{1}{\max(x_j) + 1} = \frac{\max(x_j)}{\max(x_j) + 1}$$ \hspace{1cm} (3.17)

Algorithm (2) takes the profit sharing vector $X$ with $x_i = r_i$, the fairness threshold value $\delta$, and the original fair profit sharing vector $\Psi$ as input, and generates the private $\delta$-fair profit sharing allocation vector $Y = (y_1, \ldots, y_n)$ as output such that $y_i = r_i$.

In algorithm (2), every possible combination of participation-fees leading to the reward value $r_i$, as it can be seen in line 3. The combinations of participation-fees make the samples of the distribution. Afterward, the probability distribution is calculated and the participation-fee vector is sampled from the following distribution to fulfill the differential privacy requirement as discussed in theorem 5.2.

$$Pr(Y = m) = \frac{\exp\left(\frac{c.(\max(x_j)+1)}{2.(||m - X||_1 + 1).\max(x_j)}\right)}{\sum_{m \in M} \exp\left(\frac{c.(\max(x_j)+1)}{2.(||m - X||_1 + 1).\max(x_j)}\right)}$$ \hspace{1cm} (3.18)

**Theorem 5.2** Algorithm (2) is $\delta$-fair and $\epsilon$-differentially private. \hspace{1cm} **Proof:**

The proof is almost the same as that of Theorem 5.1. As the elements of the
matrix $M$ is chosen from the range of $(\psi_j - \delta, \psi_j + \delta)$, algorithm (2) is $\delta$-fair. Let $X$ and $X'$ be neighbor payment profiles, then we have

(Note that, $||m - X||_1 - ||m - X'||_1 \leq \max(x_j)$.)

$$\frac{Pr[Alg2(X) = Y]}{Pr[Alg2(X') = Y]} = \frac{\exp(\frac{\epsilon.(\max(x_j)+1)}{2(||m - X||_1 + 1).\max(x_j)})}{\exp(\frac{\epsilon.(\max(x_j)+1)}{2(||m - X'||_1 + 1).\max(x_j)})} \times \frac{\sum m \in M \exp(\frac{\epsilon.(\max(\psi_j)+1)}{2(||m-X||_1^1 + 1).\max(\psi_j))}}{\sum m \in M \exp(\frac{\epsilon.(\max(\psi_j)+1)}{2(||m-X'||_1^1 + 1).\max(\psi_j))}}$$

$$= \exp(\frac{\epsilon.(\frac{1}{||m - X||_1^1} - \frac{1}{||m - X'||_1^1})}{2.\max(\psi_j+1)} \times \frac{\sum m \in M \exp(\frac{\epsilon.(\max(\psi_j)+1)}{2(||m-X||_1^1 + 1).\max(\psi_j))}}{\sum m \in M \exp(\frac{\epsilon.(\max(\psi_j)+1)}{2(||m-X'||_1^1 + 1).\max(\psi_j))}}$$

$$\leq \exp(\frac{\epsilon}{2}).\exp(\frac{\epsilon}{2}). \frac{\sum m \in M \exp(\frac{\epsilon.(\max(\psi_j)+1)}{2(||m-X||_1^1 + 1).\max(\psi_j))}}{\sum m \in M \exp(\frac{\epsilon.(\max(\psi_j)+1)}{2(||m-X'||_1^1 + 1).\max(\psi_j))}}$$

$$= \exp(\epsilon)$$

Hence we can rewrite the probabilities as follows

$$Pr[Alg2(X) = Y] \leq \exp(\epsilon).Pr[Alg2(X') = Y]$$
Algorithm 2: Randomized algorithm for finding the differentially private reward value

**Input**: The fair cost allocation vector $\mathbf{X}$ with $x_i = r_i$, the fairness threshold value $\delta$, and the original fair profit sharing vector $\Psi$

**Output**: The randomized private $\delta$-fair patching benefit vector $\mathbf{Y}$

1. $S \leftarrow 0$
2. Initialize matrix $\mathbf{M}$’s rows to all of possible combinations of the cost allocations such that for each row vector $\mathbf{m}$ we have $a_{i,m} = r_i$, $a_{j,m} \in (\psi_j - \delta, \psi_j + \delta)$, and $\sum_j a_{j,m} = r_i$.
3. **foreach** row vector $\mathbf{m} \in \mathbf{M}$ **do**
   4. $S \leftarrow S + \exp(\epsilon (\max(x_j) + 1) / 2(||\mathbf{m} - \mathbf{X}||_1 + 1) \cdot \max(x_j))$;
5. **end**
6. Sample $\mathbf{Y}$ from the following distribution $\Pr[\mathbf{Y} = \mathbf{m}] = \exp(\epsilon (\max(x_j) + 1) / 2(||\mathbf{m} - \mathbf{X}||_1 + 1) \cdot \max(x_j)) / S$
7. return $\mathbf{Y}$;

---

**Figure 3.3**: Comparing (A) the non-game-theoretic approach and (B) game-theoretic approach

### 3.4 Simulation Results

In this section, we investigate the performance of our proposed mechanisms. First, we evaluate the effect of applying coalitional game theory model introduced in section 3.2 for reward/participation-fee allocation on cybersecurity information sharing system. Afterward, we analyze the private reward/participation-fee allocation as presented in section 3.3.
Figure 3.4: Comparing sampling distributions (A) $\delta = 7$, (B) $\delta = 10$

Figure 3.5: Privacy leakage with the increasing of (A) $\epsilon$ and (B) $\delta$

### 3.4.1 Fair Rewarding

Here, we compare our proposed game-theoretic mechanism discussed in section 3.2 with the static allocation where participation-fee and reward are constant values for all of the organizations and every vulnerability information sharing. The goal of this experiment is to study the benefits of applying the game theoretic approach comparing to a static reward/participation-fee allocation scheme. We set the number of organizations to $n = 10$ and the number of vulnerabilities to $m = 100$. We assume each vulnerability randomly detected by an organization and the rest of organizations are vulnerable with probability 0.5. Organizations are sorted in the list based on their size in terms of their patching benefit $\pi_{j,k}$ (e.g. $o_{10}$ is the largest...
organization and \( o_1 \) is the smallest organization). We assume the patching benefit is proportional to the organization’s size and we calculate it as \( \pi_{j,k} \sim \mathcal{N}(j \times 10, 5) \).

In the static model, we consider \( r_{i,k} = 100, x_{j,k} = 20 \). Figure 3.3b shows the improvement achieved by game-theoretic formation as compared to the non-game-theoretic approach as depicted in Figure 3.3a. We calculate net-benefit value as the summation of patching benefit and sharing reward deducted by the participation-fee. As it can be seen, using the game-theoretic approach results in better distribution of the payoff among organizations while in the non-game-theoretic model the larger organizations benefit more from the system. It is due to the fact that in the non-game-theoretic setting, participation-fee is same for all of the organizations without consideration of their benefit from the system, while in the game-theoretic approach, the participation-fee is dynamically calculated based on the patching benefit. Besides that, as the reward value in the game-theoretic method is dynamically calculated based on the patching benefit, organizations are stimulated to share more useful information to the system. In our simulation, the game-theoretic approach results in higher rewards comparing to the non-game-theoretic approach. We have used MatTuGames [101] to implement the proposed profit-sharing model.

![Figure 3.6: Fairness distance with the increasing of (A) \( \epsilon \) and (B) \( \delta \)](image-url)
3.4.2 Differentially Private Rewarding

Here, we analyze the performance of differentially private profit sharing algorithms introduced in section 3.3. For this purpose, we measure the changes of privacy-leakage and fairness-distance when other parameters vary. We calculate privacy-leakage through Kullback-Leibler (KL) divergence [102]. KL divergence computes the difference between two distributions. Let $D, D'$ represent two neighbor databases differ in only one organization participating in the rewarding process, and $Q, Q'$ indicate the probability of patching benefit distribution, correspondingly. Since by increasing the difference of these distributions, the databases are more distinguishable, we define the privacy-leakage to be calculated as KL divergence as follows

$$D(Q||Q') = \sum_{y\in \mathcal{Y}} Q(y) \ln\left(\frac{Q(y)}{Q'(y)}\right)$$  \hspace{1cm} (3.19)

Figure 3.4 illustrates the sampling distributions where $n = 10$ and $x = 50$ for $\delta = 7$ and $\delta = 10$. Note that, in this case, the $\delta$ value should be larger than seven according to requirement (3.12). It can be seen that the increase of $\delta$ value provides more privacy by distributing sample space and decreasing the probability of sample selection as a result. Also, with the decrease of the distance to fair allocation, the probability increases exponentially. This makes the distribution to be biased toward fair profit sharing while fulfilling the differential privacy requirement. On the other hand, figure 3.5 displays the impacts of $\delta$, $\epsilon$, and $n$ on privacy leakage. As it can be observed, by increasing the privacy budget $\epsilon$, the privacy leakage increase but at the decreasing rate. Moreover, with the growth of the number of organizations in the coalition, the privacy leakage decreases. This is in light of the fact that with the growth of organizations coalition the sample space is also growing as indicated in equations (15), and (18).

In order to calculate the fairness, we calculate the distance between the fair profit sharing vector $\Psi$ and the expected profit allocation vector $\bar{Y}$ from our algorithms.
output, and then we divide the result by the number of participating organizations to calculate the average distance. Figure 3.6 shows the impacts of $\delta$, $\epsilon$, and $n$ on fairness distance. The distance from fair allocation is decreasing with an increase of organizations number and an increase of $\epsilon$. On the other hand, increasing the $\delta$ value, increase the fairness distance linearly. As a result, it can be concluded that the increase of the number of organizations participating in the cybersecurity information sharing coalition, the value of patching benefit, and $\delta$ yield better performance of our algorithm. Moreover, the algorithm provides a better result when the patching benefits variance is small.
Chapter 4

Privacy-Preserving Cybersecurity
Information Exchange Mechanism

Collaboration through information sharing has certain implications, for which, the organizations feel reluctant to participate. The demotivating factors can be: (1) the possibility of information exploitation through such exchange as the sharing organizations may not trust on the other participants, (2) concerns on privacy which may get exposed to attackers or other competitors from the shared information, (3) organizations’ market reputation might get negatively affected, (4) lack of incentivization with respect to a organization’s sharing contribution. In order to address the trust issue in Defense Security Information Exchange (DSIE), it enforces the members to sign a Non-Disclosure Agreement (NDA) [103], which states that all information is non-attributional and that only DSIE members can view the information. However, this approach cannot be applicable in scenarios when the trust levels of organizations are not known \textit{a priori}. In addition, the issue of privacy preservation has not been investigated in the context of CTI exchange, which is an important building-block in the sharing frameworks. With such schemes, the organizations can be ensured that their identities are not revealed to the information receiving parties and therefore reduces the chances of cyber-exploitation.
from the malicious entities. Furthermore, incentivization schemes for enhancing information sharing is of high requirement in order to prevent free-ridings in the sharing system, where participants may take advantage of the shared information without reciprocating.

In this chapter, we model a privacy-preserving cybersecurity information sharing framework using cryptographic primitives. The proposed scheme consists of four components, *Registration, Sharing, Dispute, Rewarding*. In the proposed model, first the participant organizations register themselves to the system in the Registration phase. After which, the organizations share their data with the server anonymously in the Sharing phase. At the same time, in order to implement the incentive mechanism, the organization receives an anonymous tickets from the server for their collaboration in the system. Organizations receive rewards for their tickets at the Rewarding phase. For this purpose, we apply a new aggregatable blind signature based on BBS+ signature scheme [104]. The aggregatable blind signature makes the tickets unlinkable while allowing the server to verify the number of issued tickets. At the Dispute phase, the system will detect and potentially eliminate the malicious organization.

In this chapter, we propose a privacy-preserving cybersecurity information sharing framework. To achieve this goal, a new aggregatable blind signature scheme is presented to reward participation anonymously.

### 4.1 System Model

#### 4.1.1 Entities and Architecture

In this section, we give an overview of our scheme. We consider that each CY-BEX cycle includes the following four components: (i) Registration, (ii) Sharing,
(iii) Dispute, (iv) Rewarding. Without loss of generality, we consider the system consists of three entities, a trusted Group Manager $\mathcal{GM}$, a set of participating organizations $O_1, \ldots, O_N$, and Server $S$. $\mathcal{GM}$ is a regulator where organizations participate in. $S$ provides the hosting service for sharing cybersecurity information. We consider $S$ as an honest-but-curious entity, i.e. $S$ strictly follows the protocol but it is curious about the identity of the organizations. In the case that the $S$ colludes with some of the organizations, they should learn nothing about the identity of other organizations from the information contributed by the organizations. The components and entities of the proposed architecture are shown in Fig. 4.1. A typical workflow of the entire system can be described as follows. First the participant organizations register themselves to the $\mathcal{GM}$. After registration, each organization receives a group private key from $\mathcal{GM}$. For sharing cybersecurity information, $O$ at the beginning sanitize the message and then sign it with group’s private key. Afterward $O$ anonymously sends the message and its corresponding signature to $S$. After receiving messages, $S$ first verifies the signature and the validity of the message, if they are correct then it publishes the message. If the message is corrupt (i.e. invalid or malicious), $S$ dispatches a dispute to $\mathcal{GM}$. The dispute contains the message, the corresponding signature, and the evidence of false message. By investigating the dispute report from $S$, in the case of an invalid or malicious report, $\mathcal{GM}$ traces the signature to reveal the identity of malevolent organization and subsequently revokes its private key. $S$ rewards organizations after their participation to the system. This rewarding is anonymous such that $S$ is not able to detect the organization’s identity. At the end of sharing cycle, organizations request their aggregated rewards, without revealing any information about their shared messages. To achieve anonymous rewarding, we propose a new aggregatable blind signature based on BBS+ signature [104].
4.1.2 Threat Model

Here we highlight the design objective. Our goal is to present a sound and complete mechanism for preserving privacy of organizations in the process of sharing cybersecurity information. Specifically we aim to achieve the following requirements.

Privacy. $S$ should not be able to identify the organization contributing cybersecurity information to the system. In addition, cybersecurity information should not reveal the organizations’ identity.

Authenticity. $S$ should be able to authenticate organizations when they want to share cybersecurity information. This step should be done anonymously. In addition, a malicious organization will be caught if it tries to share corrupt information.

Rewarding. To prevent organizations from free-riding in the system, there should be an incentive mechanism to reward organizations based on their contribution to the cybersecurity sharing program. The rewarding process should preserve the privacy of organizations as well.

Identification. System should be able to identify and expel the malevolent organization. The malevolent organization sends invalid or malicious message to the system.

4.2 Preliminaries

Here we describe preliminaries building blocks and cryptographic assumptions of our scheme.
4.2.1 Building Blocks

**Pairing.**[105] Let $G_1$, $G_2$ and $G_T$ be cyclic multiplicative groups of prime order $p$, where each group has unique binary representation. $g_1$ is a generator of $G_1$ and $g_2$ is a generator of $G_2$. $\psi$ is a computable isomorphism from $G_2$ to $G_1$ with $\psi(g_2) = g_1$. A pairing function or a bilinear map $e : G_1 \times G_2 \rightarrow G_T$ has the following properties:

1. Bilinearity: $\forall x \in G_1$, $y \in G_2$ and $a, b \in \mathbb{Z}_p^*$, $e(x^a, y^b) = e(x, y)^{ab}$.

2. $e(g, h) \neq 1$ where $g, h$ are generators of $G_1$ and $G_2$ respectively.

$G_1$ and $G_2$ can be the same or different groups. We say that two groups $(G_1, G_2)$ are a bilinear group pair if the group actions in $G_1$, $G_2$, $G_T$, and the bilinear mapping $e$ are all efficiently computable.

**Zero-Knowledge Proof.** The notion of zero-knowledge proof (ZKP) is introduced by Goldwasser et al. [106] in which the prover takes an interactive input
From the verifier and responds based on this input. We follow the notion introduced by Camenisch and Stadler [107] for various proofs of knowledge of discrete logarithms, and proofs of the validity of statement about discrete logarithms. For instance, \( ZKP\{(\alpha) : y = g^\alpha\} \) denotes a "zero-knowledge proof of knowledge of integer \( \alpha \) such that \( y = g^\alpha \) holds". With Fiat-Shamir heuristic [108], we are able to turn such a protocol into the non-interactive zero-knowledge proof, denoted by \( SPK\{(\alpha) : y = g^\alpha\} \).

**Group Signature.** A group signature scheme allows members of a group to sign messages on behalf of the group. Signatures can be verified with respect to a single group public key, but they do not reveal the identity of the signer. Furthermore, it is not possible to decide whether two signatures have been issued by the same group member. However, in case of a later dispute, there exists a designated group manager who can open signatures, i.e., reveal the identity of the signer. We use BBS group signature[105] in our scheme because of its efficiency. BBS group signature is comprised of four algorithms: key generation (\texttt{KeyGen}), signing algorithm (\texttt{Sign}), verification algorithm (\texttt{Verify}), and opening algorithm (\texttt{Open}). We elaborate these components inside the scheme.

**Blind Signature.** In a blind signature, the content of a message is hidden, before it is signed. Thus the signer is not aware of the message’s content. To achieve this goal, we apply BBS+ signature[104]. In BBS+ signature, the signer can sign messages in a commitment without knowing their values. The construction of the BBS+ signature is as follows. Let \( \langle g \rangle, \langle h \rangle, \langle h_0 \rangle, \langle h_1 \rangle, ..., \langle h_l \rangle \in \mathbb{G} \). The signer chooses \( \gamma \in \mathbb{Z}_p^* \) as his secret key and computes \( \omega = g^\gamma \) as the public key. To sign messages \( m_1, ..., m_t \), the signer randomly picks \( e, s \in \mathbb{Z}_p \) and computes \( A = (hh_0^e h_1^{m_1} ... h_t^{m_t})^{1/e+\gamma} \). The signature can be verified by checking if \( e(A, \omega g^e) = e(hh_0^e h_1^{m_1} ... h_t^{m_t}, g) \). For the blind signature, the user sends the Pedersen Commitment [109] of the message to the signer.
Figure 4.2: Illustration of communications in privacy-preserving cybersecurity information sharing scheme.

### 4.2.2 Cryptographic Assumptions

The cryptographic assumptions are as follows:

**q-Strong Diffie-Helman Problem.** Let $G_1, G_2$ be cyclic groups of prime order $p$. Consider $g_1$ and $g_2$ be generators of $G_1$ and $G_2$ respectively. Given a $(q + 2)$-tuple $(g_1, g_2, g_2^\gamma, g_2^{\gamma^2}, ..., g_2^{\gamma^q})$ as input, then output a pair $(g_1^{1/(\gamma + x)}, x)$ where $x \in \mathbb{Z}_p^*$.

**Decision Linear Problem in $G_1$.** Given $u, v, h, u^a, v^b, h^c \in G_1$ as input, then decide if $c = a + b$.

### 4.3 Privacy-Preserving Cybersecurity Information Exchange

In this section, we elaborate the construction details for each component of the proposed mechanism. The messages flow between entities is depicted in Fig.4.2.
4.3.1 Initialization

In the beginning, all of the participants organizations register themselves to the cybersecurity exchange program. For registration, each organization presents the required credentials to the trusted group manager \( \mathcal{GM} \). Subscribers accept the predefined policy of the model. This policy includes the systems’s rules and penalties. An entrance fee can be assigned in the joining process. After accreditation of organizations, \( \mathcal{GM} \) executes KeyGen(\( N \)) algorithm of BBS group signature with \( N \) as the number of the participant organizations. KeyGen(\( N \)) takes as input the number of members of the group \( N \) and proceeds as follows. \( \mathcal{GM} \) selects randomly a generator \( g_2 \in \mathbb{G}_2 \) and sets \( g_1 \leftarrow \psi(g_2) \). \( \mathcal{GM} \) selects \( h \leftarrow \mathbb{G}_1 \backslash \{1_{\mathbb{G}_1}\} \), and \( \xi_1, \xi_2 \leftarrow \mathbb{Z}_p^* \) and sets \( u, v \in \mathbb{G}_1 \) such that \( u^{\xi_1} = v^{\xi_2} = h \). \( \mathcal{GM} \) selects \( \gamma \leftarrow \mathbb{Z}_p^* \) and sets \( w = g_2^\gamma \). Using \( \gamma \), \( \mathcal{GM} \) generates for each user \( 1 \leq i \leq N \), an SDH tuple \( A_i, x_i \): where \( x_i \leftarrow \mathbb{Z}_p^* \) and \( A_i \leftarrow g_1^{1/(\gamma+x_i)} \in \mathbb{G}_1 \). The group public key is \( gpk = (g_1, g_2, h, u, v, w) \). The private key of \( \mathcal{GM} \) is \( gmsk = (\xi_1, \xi_2) \) and each \( O_i \)'s private key is the tuple \( gsk[i] = (A_i, x_i) \). The output of KeyGen(\( N \)) algorithm is the keys \( gmsk, gpk \), and the set of \( gsk[i] \) (\( 1 \leq i \leq N \)). Here, \( gmsk \) is \( \mathcal{GM} \) private key, \( gpk \) is the public key which is shared with all of the entities in the scheme, and \( gsk[i] \) is \( O_i \) private key. \( \mathcal{GM} \) securely sends back \( gsk[i] \) to \( O_i \). In the rest of paper, we indicate the participant organization by \( O \) for convenience. At the same time, \( S \) randomly chooses \( \gamma, e \in \mathbb{Z}_p^* \) and computes \( \omega = h_0^\gamma \). The secret key is \( \gamma, e \) and the public key is \( \omega \).

4.3.2 Sharing

At the time of sharing cybersecurity information, \( O \) first uses anonymization and sanitization techniques [50–53] to remove all of the identifier information from its message. As an example, consider postal address, personal name, email address,
phone number, etc. These identifiers are removed from the message. Furthermore, quasi-identifier values, whose combinations can uniquely identify the organization should be generalized or removed. It is out of our scope to consider this problem. Then $O$ anonymously connects to $S$. This anonymous network can be based on Tor [110]. $O$ signs the sanitized message $M$ by executing the algorithm $\text{Sign}(gpk, gsk, M_j)$ of BBS group signature. This algorithm takes as input the group public key $gpk$, user’s private key $gsk$, and the message $M_j \in \{0, 1\}^*$. $O$ selects exponents $\alpha, \beta \leftarrow \mathbb{Z}_p^*$ and computes a linear encryption of $A$: $T_1 \leftarrow u^\alpha$, $T_2 \leftarrow v^\beta$, $T_3 \leftarrow Ah^{(\alpha+\beta)}$. Then, it computes two helper values $\delta_1 \leftarrow x\alpha$, and $\delta_2 \leftarrow x\beta \in \mathbb{Z}_p$. Afterward $O$ computes the following proof of knowledge:

$$
\text{PoK}_{\sigma_j}\{\alpha, \beta, x, \delta_1, \delta_2\}:
\begin{align*}
&u^\alpha = T_1, v^\beta = T_2, \\
e(T_3, g_2)^x.e(h, w)^{-\alpha-\beta}.e(h, g_2)^{-\delta_1-\delta_2} = \\
e(g_1, g_2)/e(T_3, w), \\
&T_1^xu^{-\delta_1} = 1, T_2^xv^{-\delta_2} = 1\} \text{(m)}.
\end{align*}
$$

The signature is $\sigma_j \leftarrow (T_1, T_2, T_3, \text{PoK}_\sigma)$. $O$ anonymously sends $(M_j, \sigma_j, C_j)$ to $S$. Here $C_j = h_0^{s_j} h_1^{ID}$ is a commitment over the organization’s ID, and $s_j'$ is chosen randomly for each commitment such that $s_j' \neq s_i'$ ($1 \leq i \neq j \leq m$). By receiving $M_j$ and $\sigma_j$, $S$ verifies the correctness of the signature through executing $\text{Verify}(gpk, M_j, \sigma_j)$ algorithm. This algorithm takes as input the group public key $gpk$, the message $M_j$, and the group signature $\sigma_j$, verifies that $\sigma_j$ is a valid signature by checking validity of proof of knowledge $\text{PoK}_{\sigma_j}$. $S$ performs the initial checks for the validity of the message and its signature, then it shares $M_j$ and $\sigma_j$ if they are correct. The subscribers check the validity of the signatures as well before applying the message. This checking step prevents malicious $S$ to share invalid messages. The instantiation of $\text{PoK}_{\sigma_j}$ can be found in [105].
4.3.3 Dispute

Due to the anonymous nature of sharing data, a malevolent organization might share incorrect or malicious information. Therefore we need a mechanism to detect the malicious subscriber. In the case that $S$ or the subscribers detect a malicious message, they initiate the Dispute process with $G.M$. In the dispute process, $S$ or the subscribers send evidence of incorrect information $\zeta_j$ along with $M_j$ and its corresponding signature $\sigma_j$. The group policy contains the rules to detect $M_j$ as incorrect, and it is described the requirements of $\zeta_j$. After verifying $\zeta_j$, $G.M$ finds the malicious organization through executing $\text{Open}(gpk, gmsk, M_j, \sigma_j)$ algorithm. This algorithm is used for tracing a signature to the signer. It takes as input the group public key $gpk$, the corresponding group manager’s private key $gmsk$ together with the message $M_j$ and the signature $\sigma_j$ to trace. It recovers the user’s $A$ as $A \leftarrow T_3/(T_1^{\xi_1} T_2^{\rho_2})$, then looks up the user index corresponding to the identity $A$ recovered from the signature. $G.M$ reveals the malicious organization’s identity and revokes the group signature. The punishment for the malicious entity should be specified in the registration phase policy. After each dispute process, the registration step should be repeated to generate the new group signature.

4.3.4 Rewarding

To prevent free-riding, the system has an incentive mechanism for sharing data. In the rewarding phase, $S$ anonymously rewards organizations based on their contribution to the system. However, the rewarding process is challenging when the identity of the players are concealed. In this process organizations receive a ticket $\tau_j$ for each message they are contributing to the system. We assume $S$ is able to identify $O$’s identity through analyzing the shared messages in the system. Therefore, our rewarding process should prevent $S$ to distinguish the issued tickets for $O$. To hide the tickets, we present a new aggregatable blind signature.
After sharing data, $S$ gives a ticket to $O$ which is a signature over the $O$’s commitment $C_j$. Because of the hiding feature of commitment, $S$ does not know the identity of $O$. The contributor organizations can redeem their rewards after each CYBEX cycle. $O$ aggregates all of its tickets received from $S$, and proof that the received tickets are correctly made, without revealing any information about underlying tickets. In this case $S$ is unable to infer $O$’s identity by linking the provided tickets to the shared messages. To achieve this goal, we propose a new aggregatable blind signature which is based on BBS+ signature. At the beginning of each CYBEX cycle, $S$ randomly chooses secret values $e, \gamma \in Z_p^*$ and computes $\omega = g^\gamma$ as the public key. For each message contribution, After verification of the message and its signature, $S$ randomly chooses $s_j \in Z_p^*$ and signs $O_i$’s commitment $C_j$ as $A_j = (h h_0^s h_1^{s_1} \ldots h_m^{s_m})^{1/e+\gamma}$. Then $S$ sends back a ticket $\tau_j = (A_j, s_j)$ to $O$. At the end of CYBEX cycle, $S$ publishes $e$ to the public, and organizations can redeem their rewards. Let $m$ indicate the number of $O$’s tickets in a CYBEX cycle. $O$ first calculates $\hat{s} = \sum_{j=1}^{m} s_j$, and then aggregates all of the received tickets as $\hat{A} = \prod_{j=1}^{m} A_j$. Then $O$ chooses the secret value $k \in Z_p^*$ and computes the new commitment for each $C_j$ as $\hat{C}_j = h^k C_j$. Afterward $O$ computes the following signature proof of knowledge

$$SPK_+\{ (\hat{A}, \hat{s}, ID, s'_1, \ldots, s'_m, k) : e(\hat{A}, \omega g^{e}) = e(h h_0^\hat{s} h_1^{s'_1} \ldots h_m^{s'_m}, g)$$

$$\hat{C}_1 = h^k h_0^{s'_1} h_1^{ID}$$

$$\vdots$$

$$\hat{C}_m = h^k h_0^{s'_m} h_1^{ID}$$

$$}\{ (M) \}.$$}

After verification of $SPK_+$, $S$ accepts $O$’s assertion and transfer credits based on the anonymous e-cash protocols [111].
Details of SPK. The instantiation of $SPK_\tau$ is as follows. The prover randomly selects $r \in Z_p^*$ and computes the helper commitment $T_A = \hat{A}^r$.

(Commitment.) The prover picks random values $\rho r, \rho s, \rho_{ID}, \rho_{s'_1}, ..., \rho_{s'_m}, \rho_k \in Z_p^*$, and computes the following values

$$R_0 = e(h, \omega g^e)^{-\rho r} \cdot e(h_1, g^m)^{\rho_{ID}} \cdot e(h_0, g)^{\rho s},$$

$$R_1 = h^{\rho r} h_0^{\rho s} h_1^{\rho_{ID}},$$

$$\ldots$$

$$R_m = h^{\rho r} h_0^{\rho s} h_1^{\rho_{ID}}$$

(Challenge.) The prover computes the challenge $c$ using a hash function $H(.)$ as

$$c = H(M, R_0, R_1, ..., R_m)$$

(Response.) Using $c$, the prover computes

$$z_r = \rho r - cr$$

$$z_s = \rho s - c\hat{s}$$

$$z_{ID} = \rho_{ID} - cID$$

$$z_{s'_1} = \rho_{s'_1} - cs'_1$$

$$\ldots$$

$$z_{s'_m} = \rho_{s'_m} - cs'_m$$

$$z_k = \rho_k - ck$$

Then the prover sends $(c, R_0, ..., R_m, z_r, z_s, z_{ID}, z_{s'_1}, ..., z_{s'_m}, z_k)$ to the verifier.
(Verify.) The verifier checks the following equalities

\[ R_0 \overset{?}{=} (e(T_A, \omega g^e)/e(h, g))^c \cdot e(h, \omega g^e)^{-z_r} \cdot e(h_1, g^m)^z_{ID}. \]

\[ e(h_0, g)^z_i \cdot e(h_0, g)^{z_i'} \cdots e(h_0, g)^{z_m} \]

\[ R_1 \overset{?}{=} \hat{C}_1 c h \bar{z}_1 h_0^{-1} h_{1}^{z_{ID}} \]

\[ \ldots \]

\[ R_m \overset{?}{=} \hat{C}_m c h \bar{z}_m h_0^{-1} h_{1}^{z_{ID}} \]

### 4.4 Privacy and Security Analysis

In this section, we analyze the privacy and security of the proposed framework. Particularly we are interested in analyzing our proposed aggregate blind signature in the rewarding phase since the security and privacy of the other sections of the mechanism are directly come from the ability to sign anonymously through the group signature scheme.

**Theorem 1.** In the rewarding phase, \( S \) is not able to identify the identity of the message originator.

**Proof:** There are two types of attack \( S \) can perform to identify \( O \). First, in the sharing phase \( S \) keeps the record of tickets and their corresponding messages, and in the rewarding phase discovers the issued tickets and finding the associated shared messages in its database. Then by correlating the shared messages, \( S \) infers \( O \)'s identity. In the second attack, \( S \) examining the available parameters to identify \( ID \) value. Due to the blindness feature of BBS+ signature, \( O \) can prove the correctness of the signature without revealing the message and signature. In our scheme, the \( e \) value is the same for all of the tickets and \((A, s, ID, s'_1, \ldots, s'_m, k)\) values are hidden in the proof of knowledge step. For the first attack, \( S \) is not able to link the aggregated ticket to the issued tickets. This is due to the fact
that, \( O \) applies the zero-knowledge-proof for \((\hat{A}, \hat{s}, ID, s'_1, ..., s'_m, k)\) values. Also, \( O \) hides the provided commitment \( C_j \) to the new commitment \( \hat{C}_j \), and because of the commitment’s hiding feature, \( S \) can not deduce the initial corresponding commitment. For the second attack, the ID value is hidden in the commitments and zero-knowledge-proof. Hence with CDH assumption, \( S \) can not compute ID value.

**Theorem 2.** \( O \) cannot forge or double-spend the ticket.

**Proof:** For forging a ticket \( \tau_j \), \( O \) has to compute \( A_j \), since \( O \) does not have access to \( S \) secret key \( \gamma \) and with consideration of the q-SDH and CDH assumptions, then \( O \) is incapable to forge a ticket. If \( O \) randomly chooses a value for the ticket then \( O \) can not generate the \( SPK_{\hat{\tau}} \). On the other hand, \( O \) can not provide a correct \( SPK_{\hat{\tau}} \) with double-spending. Since \( s'_j \) should be different for each commitment \( C_j \) then \( O \) can not provide the correct \( SPK_{\hat{\tau}} \). On the other hand, If \( O \) attempts to double spend a ticket, then it can not generate the correct proof of equality for \( s'_j \) in the \( e(\hat{A}, \omega g^\epsilon) = e(h h_{0}^{s'_j} h_{1}^{m.ID}, g) e(h_{0}^{s'_1} + ... + s'_m, g) \) equation and the corresponding commitment \( \hat{C}_j = h^k h_{0}^{s'_j} h_{1}^{ID} \) which can not be performed if \( \tau_j \) is forged or double-spent.

### 4.5 Performance Evaluation

In this section, we evaluate the computation and communication performances of the proposed framework. The testbed is built on Linux Ubuntu 15.04 with 2.5GHz CPU and 12GB RAM. We use the Pairing Based Cryptography Library [112] for the implementation of pairing functions. The parameters of 160-bit long group order and 512-bit long base field are applied in “Type A” elliptic curve generator. In our prototype, \( \mathbb{G}_1 \) and \( \mathbb{G}_2 \) are the same group.
Since the computation complexity mainly comes from the operations of pairing (Pairing), exponentiation (Exp), multiplication (Mul), and Inversion (Inv) in the pairing groups, the computation performance is relying on them. The sharing stage involves $\mathcal{O}$ and $\mathcal{S}$. $\mathcal{O}$ generates the signature $\sigma_i$ over the message $M$, thus its computation complexity contains: $3 \times \text{mul}_1$, $9 \times \text{exp}_1$, $2 \times \text{inv}_1$, $3 \times \text{pairing}$, $2 \times \text{mul}_T$, $3 \times \text{exp}_T$, $2 \times \text{inv}_T$, and $1 \times \text{hash}$. Meanwhile, $\mathcal{S}$ verifies $\sigma_i$, thus its computation complexity contains: $4 \times \text{mul}_1$, $8 \times \text{exp}_1$, $4 \times \text{inv}_1$, $3 \times \text{pairing}$, $2 \times \text{mul}_T$, $3 \times \text{exp}_T$, $2 \times \text{inv}_T$, and $1 \times \text{hash}$. In the rewarding phase, $\mathcal{O}$ provides the signature proof of knowledge $SPK_K$, hence its computation complexity contains: $(3 + m) \times \text{pairing}$, $(1 + 2m) \times \text{mul}_1$, $(1 + m) \times \text{mul}_T$, $(3m) \times \text{exp}_1$, $(3 + m) \times \text{exp}_T$, $1 \times \text{inv}_T$, and $1 \times \text{hash}$. On the other hand, $\mathcal{S}$ verifies $SPK_K$, thus its computation complexity contains: $(5 + m) \times \text{pairing}$, $(2 + 3m) \times \text{mul}_1$, $(2 + m) \times \text{mul}_T$, $(4m) \times \text{exp}_1$, $(5 + m) \times \text{exp}_T$, and $2 \times \text{inv}_T$.

Fig. 4.3 displays the computation time of $\mathcal{O}$ and $\mathcal{S}$ with the increasing number of $M$. As it can be seen, the computation time is small and the proposed mechanism is feasible. For example, to submit, verify and reward 100 messages, $\mathcal{O}$ requires 26 seconds time and $\mathcal{S}$ requires 11 seconds time.
4.5.2 Communication Cost

Here we evaluate the communication cost between entities. For sharing each message, \( \mathcal{O} \) transmits the message together with the \( \sigma \) to the \( \mathcal{S} \). Here we do not consider the message size, since the message size is not constant. \( \sigma \) consists of \((T_1, T_2, T_3, \text{PoK}_\sigma)\). Each of the \( T_1, T_2, T_3 \in \mathbb{G}_1 \), is 129 bytes. \( \text{PoK}_\sigma \) includes \((c, s_\alpha, s_\beta, s_x, s_{\delta_1})\). The output of the hash function is \( c \) with the size of 32 bytes. We consider 128 bytes for each element in \( \mathbb{Z}_p^* \). \((s_\alpha, s_\beta, s_x, s_{\delta_1})\) are elements in \( \mathbb{Z}_p^* \), therefore the total size of \( \sigma \) is 1059 bytes. \( \mathcal{S} \) in return, sends back a ticket to the \( \mathcal{O} \). Each ticket \( \mathcal{A}_j \) is an element of \( \mathbb{G}_1 \) with the size of 129 bytes. Finally \( \mathcal{O} \) transmits its aggregated ticket to \( \mathcal{S} \). The signature proof of knowledge contains: \( m \times 129 \) bytes \((R_1, ..., R_m)\), \( m \times 128 \) bytes \((z_{s_\epsilon}, ..., z_{s_m})\), 131 bytes \((R_0)\), \( 4 \times 128 \) bytes \((z_r, z_{ID}, z_s, z_k)\), and 36 bytes \((c)\). Fig. 4.4 displays the communication cost between \( \mathcal{O} \) and \( \mathcal{S} \) with the increasing number of \( M \). We can see that the overall communication cost is small in the present networks.
Chapter 5

A Coalitional Cyber-Insurance Framework for a Common Platform

In this chapter, we study a set of mechanisms to motivate organizations toward cybersecurity collaboration. To this end, we leverage the cyber-insurance as a stimulant. Since organizations cannot completely mitigate cyber-threats, they adopt cyber-insurance to transfer such risks to another party known as the insurer. It is estimated that annual gross written premium will be increased from around $2.5 billion today to reach $7.5 billion by 2020 [15].

However, several challenges are circumventing the growth of the cyber-insurance market. For instance, the lack of reliable data to compute insurance premium, and legal and procedural hurdles for assessing the organizations’ security posture are two of them [16]. In addition, setting a proper insurance policy and premium is sophisticated. If the insurance policy is loose, the insurer might fail or even may go bankrupt, and if the policy is strict, the insured might withdraw from the contract and accept the risks. Moreover, asymmetric information between the
insurer and insured exacerbates the situation causing moral hazard and adverse selection problems [17, 18]. Moral hazard refers to the case where insureds can increase the probability of the risks after signing the contract. For instance, the insured reduces its security investment after signing the insurance contract. On the other hand, users with high risk are more likely to take insurance, and an insurer cannot distinguish between insureds before signing the contract. This problem is known as adverse selection.

Since organizations using the common platforms are suffering from the same set of vulnerabilities, their security is interdependent. In this situation, as one party’s investment on security and detection of a common platform’s vulnerabilities brings the positive externalities to other parties using the same platform, organizations tend to under-invest on security, expecting other organizations’ investment [21, 22].

Besides that, organizations using the same platform can reduce the damages of attacks by sharing their cybersecurity information. However, sharing such information is costly for organizations. For instance, reporting a successful cyber-attack may affect the organizations’ reputation negatively while such information can help other organizations to patch their systems to be safe from the same type of attack. Therefore, organizations tend to free-ride by taking advantage of the shared information while not reciprocating. In other words, if we model the cybersecurity information sharing as a non-cooperative game, although the sharing strategy is the socially optimal point, the not-sharing behavior is the Nash-Equilibrium point [23].

Therefore, it is important to motivate organizations to cybersecurity investment and sharing cybersecurity information. Such motivation can be done by assigning punishment/reward to the organizations. However, designing such mechanisms is a big challenge mainly because the provisioning of the cybersecurity investment and sharing is difficult.
Considering the organizations’ security interdependency and their demand for cyber-insurance, we study the design of coalitional insurance mechanisms with the goal of covering the adverse selection, moral hazard, and cybersecurity investment and sharing problems. To this end, we propose a synergistic insurance framework where organizations collaboratively insure a common platform instead of themselves. We present three models for insuring a common platform. In the first model, organizations act as both insurer and insured to distribute the risk in the coalition. In the second model, the system provides rewards to crowdfund the insurance. Finally, in the third model, we investigate the outsourcing of a common platform insurance. Moreover, we study how such frameworks can improve social welfare by motivating organizations to collaborate on the cybersecurity investment and sharing.

In this chapter, we propose a coalitional insurance framework where organizations act as both insurer and insured of a common platform. Further, we discuss how our proposed mechanisms for such framework satisfy the budget balanced, \textit{ex ante} individual rationality, and incentive compatibility properties. Furthermore, we present a model for crowdsourcing the insurance of a common platform taking into account the budget balanced, \textit{ex ante} individual rationality, and incentive compatibility to propel organizations toward social welfare.

\section{System Model}

In this section, we elaborate the system model of a coalitional cyber-insurance framework for a common platform. First, we model the cyber-insurance for a common platform, then we model the cybersecurity information sharing in the coalition, and finally, we discuss the design objectives.
5.1.1 Cyber-Insurance

Let $\mathcal{O} = \{o_1, ..., o_n\}$ represent the strategic organizations participating in a coalition of cybersecurity information sharing for a common platform. For simplicity and without loss of generality, we let $p$ represent the probability that the attackers $\mathcal{A}$ (irrespective of their type) discover a new vulnerability for the common platform and exploit it. Note that $p$ can be modeled differently based on the common platform’s type, however analyzing and studying the modeling of $p$ is outside the scope of this chapter.

Each organization $o_i$ decides on the amount of risk to be transferred to an insurer. This decision is based on the organization’s risk aversion and insurance-fee. Organizations can be risk-averse, risk-neutral, or risk-seeker. In a setting with multiple options with same expected gain, a risk-averse organization chooses an option with less risk, the risk-seeker chooses an option with the most risk, and the risk-neutral does not have any priority. A utility function mapping wealth into utility $u(w)$ can describe risk attitude where $\frac{\partial u(w)}{\partial w^2} > 0$. For instance, $u(w)$ is concave for a risk-averse organization $\frac{\partial^2 u(w)}{\partial w^2} < 0$. On the other hand, the insurer is a risk-seeker entity accepting risks of another party in return for a premium. In this chapter, the insurance covers the cost of exploitation of the new vulnerabilities associated with a common platform.

Let $l_i$ represent the loss of cyber-attack on $o_i$, the insurance indemnity is $\pi_i = \alpha_i \times l_i$ where $\alpha_i \in [0, 1]$; $\alpha_i = 1$ indicating the full coverage, and $0 < \alpha_i < 1$ representing the partial coverage. Let $\beta_i$ denote the premium the insured has to pay for the insurance. The insurance is called actuarially fair if the net-payoff is zero. In other words, in the actuarially fair insurance, the premium is equal to the expected value of compensation $\bar{\beta}_i = \pi_i \times p$. The risk-averse agent strictly prefers full coverage in the actuarially fair setting [17]. However, in reality, the premium is higher than the actuarially fair $\hat{\beta}_i = \pi_i \times p + \tau$, where, $\tau$ represents the administrative
cost which is the insurer’s profit and cost of safety capital. When the insurance premium is at least actuarially fair, only risk-averse agents insure themselves [17].

5.1.2 Cybersecurity Information Sharing

After the establishment of a coalition for cybersecurity information sharing, the probability of successful exploitation of a vulnerability decreases once $A$ exploits a vulnerability over one of the organizations in the coalition. This is because the exploited organization shares the vulnerability information to the other organizations in the coalition and they patch their systems accordingly. We use $\mu(n) \in [0, 1]$ to describe the epidemic model of the expansion of vulnerability exploitation. $\mu(n) = 0$ indicates that the coalition does not have any benefit as the vulnerability information does not get shared before all of the organizations get exploited. As the value of $\mu(n)$ approaches one, the efficiency of the cybersecurity information sharing coalition increases. The value of $\mu(n)$ depends on the nature of the vulnerability, type of attacker, and the agility of cybersecurity information sharing framework.

There is another set of vulnerabilities where $\mu(n)$ approaches zero. For instance, consider a vulnerability where the time gap between the detection of exploitation and patching the system is large enough (for instance advanced persistent threats) allowing $A$ to exploit other organizations as well. As another example assume an equipped $A$ capable to attack more than one organization at the same time. Thus, $\mu(n)$ can be interpreted as an index of cybersecurity information sharing impact in a coalition of $n$ organizations. It is expected that with the growth of $n$, the value of $\mu(n)$ increases as well.

Now let us study the model formally. Let $K, \bar{K} \subseteq O$ represent the set of exploited organizations from a new vulnerability and the set of other organizations in the
coalition (complement of $\mathcal{K}$), respectively. Having $k = |\mathcal{K}|$ and $\bar{k} = |\bar{\mathcal{K}}|$, we have $\mathcal{K} \cup \bar{\mathcal{K}} = \mathcal{O}, \mathcal{K} \cap \bar{\mathcal{K}} = \emptyset, k + \bar{k} = |\mathcal{O}|$.

Let $q_{i,k}$ denote the probability that $o_i \in \mathcal{K}$, and $\bar{q}_{i,\bar{k}}$ denote the probability that $o_i \in \bar{\mathcal{K}}$. Note that the matrix $\mathbf{Q} = \{q_{i,k}\}$ is modeling the epidemic model of the expansion of vulnerability exploitation. In other words, we use $\mathbf{Q}$ to model the efficiency of the cybersecurity information sharing for the common platform. If organizations efficiently share the vulnerability information then the vulnerability is getting patched and as a result the number of exploited organizations $k$ decreases. On the other hand, if the vulnerability information has not been shared efficiently (e.g. the time gap between sharing the vulnerability information and patching it is large enough allowing attackers to exploit other organizations as well), the number of exploited organizations $k$ increases.

We summarize the notations used in this chapter in Table 5.1.

### 5.1.3 Design Objective

The main objective of our insurance policy design is to improve the security state of organizations by motivating organizations to participate in cybersecurity information sharing and invest in security to find new vulnerabilities in a common platform. To this end, there are several challenges that should be addressed in our design as follows:

- **Adverse selection.** Users with high risk are more likely to take insurance, and an insurer cannot distinguish between insureds before signing the contract. Also, it is not easy to assess the risk of a vulnerability exploitation, and the estimation of the probability of successful attack from insurer and insureds are different. The insurer tends to estimate this value greater than
Table 5.1: Notations used for a coalitional cyber-insurance framework

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$</td>
<td>The probability that an attacker finds a new vulnerability of the common platform</td>
</tr>
<tr>
<td>$n$</td>
<td>The number of the organizations in the coalition</td>
</tr>
<tr>
<td>$l_i$</td>
<td>$o_i$’s loss from a cyber-attack over the common platform</td>
</tr>
<tr>
<td>$\mathcal{K}$</td>
<td>The set of exploited organizations in the coalition</td>
</tr>
<tr>
<td>$\bar{\mathcal{K}}$</td>
<td>The set of organizations in the coalition which have not been exploited</td>
</tr>
<tr>
<td>$q_{i,k}$</td>
<td>The probability that $o_i \in \mathcal{K}$</td>
</tr>
<tr>
<td>$\bar{q}_{i,k}$</td>
<td>The probability that $o_i \in \bar{\mathcal{K}}$</td>
</tr>
<tr>
<td>$\pi_i$</td>
<td>The insurance indemnity to $o_i$</td>
</tr>
<tr>
<td>$\beta_i$</td>
<td>The insurance premium for $o_i$</td>
</tr>
<tr>
<td>$\bar{\beta}_i$</td>
<td>The actuarially fair premium</td>
</tr>
<tr>
<td>$c_i$</td>
<td>The $o_i$ commitment for the indemnity</td>
</tr>
<tr>
<td>$\hat{c}_{i,k}$</td>
<td>The payment of $o_i$ to community when $k$ organizations exploited</td>
</tr>
<tr>
<td>$\hat{\pi}_{i,b}$</td>
<td>The indemnity that $o_i$ receives when $k$ organizations exploited</td>
</tr>
<tr>
<td>$\hat{\tau}$</td>
<td>The expected available budget for reimbursement from the coalition</td>
</tr>
<tr>
<td>$\hat{\psi}$</td>
<td>The expected indemnity</td>
</tr>
<tr>
<td>${-i}$</td>
<td>The set of organizations in the coalition except $o_i$</td>
</tr>
<tr>
<td>$c_{\text{ext}}$</td>
<td>The outsider commitment to the coalition</td>
</tr>
<tr>
<td>$\tau$</td>
<td>Insurer administrative cost</td>
</tr>
<tr>
<td>$\psi_i$</td>
<td>$o_i$’s bid for the commitment</td>
</tr>
<tr>
<td>$\hat{\psi}$</td>
<td>Minimum of the commitment bids submitted by the organizations.</td>
</tr>
<tr>
<td>$c$</td>
<td>The vector of the organizations’ commitments.</td>
</tr>
<tr>
<td>$\beta$</td>
<td>The vector of the organizations’ premiums.</td>
</tr>
<tr>
<td>$\bar{\beta}$</td>
<td>The total premium collected from the coalition</td>
</tr>
<tr>
<td>$R_i(c, \beta)$</td>
<td>$o_i$’s reward for its commitment.</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>The degree of risk aversion</td>
</tr>
<tr>
<td>$v_c$</td>
<td>The value of vulnerability information for the coalition</td>
</tr>
<tr>
<td>$v_I$</td>
<td>The value of vulnerability information for the insurer</td>
</tr>
<tr>
<td>$v_b$</td>
<td>The black market value of the vulnerability information</td>
</tr>
<tr>
<td>$\mathcal{V}$</td>
<td>The sum of value of the vulnerability information for the coalition and insurer</td>
</tr>
<tr>
<td>$\theta$</td>
<td>The system’s offer to the vulnerability finder</td>
</tr>
</tbody>
</table>

The insureds’ estimation. Such information asymmetry causes a discrepancy in the insurance agreement.

- **Moral hazard.** After signing an insurance contract, the insurer might decrease its security investment exceeding the chance of a new vulnerability detection by an attacker.
• **Incentive compatibility.** A mechanism is incentive compatible if players can achieve their best outcome by playing based on their true preferences. In interdependent security settings, organizations tend to free-ride such that they do not invest in security or share their cybersecurity information, but getting benefit from the security information shared by the other organizations. We are interested in designing mechanisms where security investment and sharing of cybersecurity information is the organizations’ dominant strategy. In this case, the mechanism should be equipped with a rewarding/punishment tool to stipulate organizations for security investment and also sharing cybersecurity information.

• **Fairness.** The costs and benefits should be fairly divided between insurers and insureds based on their efforts and commitments following the insurance policy.
5.2 Insuring a Common Platform

In this section, we study three models for insuring a common platform. In the first model, organizations act as both insurer and insured to distribute the risk in the coalition. In the second model, the system provides rewards to crowdfund the insurance. Finally, in the third model, we study the outsourcing of a common platform insurance.

5.2.1 Coalitional Self-Insurance Framework

As organizations use a common platform, they are sharing the same set of vulnerabilities. In order to decrease the cost of cyber-attack over a common platform, we propose a model where organizations distribute the risks among themselves. In our proposed coalitional self-insurance model, every organization \( o_i \) in the community commits to an indemnity value \( c_i \). This commitment can be done through payment guarantee contracts. These commitment values will be the source of indemnity when a new vulnerability exploits in the system.

Then, once a new vulnerability of the common platform is exploited, the exploited organizations will be reimbursed based on the organizations’ commitments pool.

Having such a model, we have the following benefits:

- Organizations are stipulated to invest in security and share their cybersecurity information in a more efficient way. This is due to the fact that the loss of a vulnerability exploitation for every organization in the coalition is costly for other organizations as well.

- As the exploited organizations need to prove the exploitation of the vulnerability to get reimbursed by the system, they should share the vulnerability
information to other organizations in the coalition. Therefore, other organizations are able to patch their systems afterward.

- Organizations share the cost of cyber-attack and transfer the risks to the system without paying the administrative cost of an insurance.

Let $\hat{c}_{i,k}$ represent the payment of $o_i$ to community when $k$ organizations are exploited, and let $\hat{\pi}_{i,k}$ represent the indemnity that $o_i$ receives when $k$ organizations are exploited by a new vulnerability of the common platform.

Then, following this model, we can represent the expected utility of an organization $o_i$ in the coalition as

$$
\mathbb{E}[u_i] = p(\sum_{k=1}^{n} q_{i,k} \cdot (-l_i + \hat{\pi}_{i,k}) + \bar{q}_{i,n-k} \cdot (-\hat{c}_{i,n-k}))
$$

(1)

s.t. \quad \sum_{k=1}^{n} q_{i,k} + \sum_{k=1}^{n} \bar{q}_{i,k} = 1, \quad \hat{\pi}_{i,n} = 0, \hat{c}_{i,0} = 0

Note that in this model, when all of the organizations get exploited, we have $\hat{\pi}_{i,n} = 0, \hat{c}_{i,0} = 0$.

Then the problem is how to calculate the proper value for $\hat{c}_{i,k}$ and $\hat{\pi}_{i,k}$ to satisfy the requirements mentioned in section 5.1.3 in addition to the \textit{ex ante} individual rationality and the budget balanced properties defined as follows:

\textbf{Ex \textit{ante} individual rationality}. This requires that an agent’s expected utility in the framework should be greater than its expected utility outside the framework. \textit{Ex \textit{ante}} individual rationality attracts agents to participate in the framework. Also, we define the \textit{ex ante} weak individual rationality when the expected utility of an organization does not change whether it is in the framework or not.
**Budget balanced.** As the resource of indemnity is the commitment values, we need to satisfy the budget balanced property as follows

\[
\sum_{i \in K} \hat{\pi}_{i,k} = \sum_{i \in \bar{K}} \hat{c}_{i,k}
\]

Specifying our requirements, now let’s study the design of mechanisms which satisfies these properties. A mechanism can be specified by a game \( g : \mathcal{M} \to \mathcal{U} \) where \( \mathcal{M} = \{m_1, ..., m_n\} \) is a set of input messages and \( \mathcal{U} = \{u_1, ..., u_n\} \) is the output of the mechanism. A player chooses its message \( m_i \) to increase its utility \( u_i \). In what follows, we present the first mechanism to fulfill the system requirements.

**Mechanism 1.** Organizations submit their proposed values \( \bar{\psi} = \{\psi_1, ..., \psi_n\} \) for the commitment. Let \( \hat{\psi} = \min \bar{\psi} \), then the commitment and the indemnity of each organization are calculated as

\[
\hat{c}_{i,k} = \hat{\psi} \\
\hat{\pi}_{i,k} = \frac{\bar{k} \cdot \hat{\psi}}{\bar{k}}
\]

(Note that, here \( \mathcal{M} = \bar{\psi} \) and \( u_i \) obtains from (1)).

**Proposition 1.** The budget balanced property is held in mechanism 1.

**Proof:** We need to show that the total of the committed values is equal to the total indemnity value, which is given to the exploited organizations.

\[
\sum_{o_i \in \bar{K}} \hat{c}_{i,k} = \sum_{o_i \in \bar{K}} \hat{\psi} = \bar{k} \cdot \hat{\psi} \\
\sum_{o_i \in K} \hat{\pi}_{i,k} = \sum_{o_i \in K} \frac{\bar{k} \cdot \hat{\psi}}{\bar{k}} = \bar{k} \cdot \hat{\psi}
\]
Proposition 2. Assume the number of exploited organizations in the coalition is identically distributed $k \sim U[0, n]$, and the probability of exploitation/not-exploitation of an organization is a fair coin, then mechanism 1 satisfies the ex ante individual rationality and the expected benefit for each organization is:

$$E[u_i] - E[u^0_i] = p\left(\frac{\hat{\psi}}{2n} \left(\frac{n-2}{2} + \ldots + \frac{1}{n-1}\right)\right) \quad (2)$$

Proof: For ex ante individual rationality, we need to show that, the expected utility of an organization in the coalition is higher than the expected utility of an organization outside of the coalition $E[u_i] \geq E[u^0_i]$. The expected utility of $o_i$ outside of coalition can be calculated as

$$E[u^0_i] = p\left(\sum_{k=1}^{n} q_{i,k} \cdot (-l)\right)$$

In the case of applying the model, the expected utility of $o_i$ is

$$E[u_i] = p(q_{i,1} \cdot (-l_i + \frac{(n-1) \cdot \hat{\psi}}{1}) + \bar{q}_{i,n-1} \cdot (\hat{\psi}) + q_{i,2} \cdot (-l_i + \frac{(n-2) \cdot \hat{\psi}}{2}) + \bar{q}_{i,n-2} \cdot (\hat{\psi}) + \ldots +$$

$$q_{i,n-1} \cdot (-l_i + \frac{\hat{\psi}}{n-1}) + \bar{q}_{i,1} \cdot (\hat{\psi}) + q_{i,n} \cdot (-l_i))$$

As the number of exploited organizations in the coalition is identically distributed and the probability of exploitation/not-exploitation of an organization is a fair coin, we have $\sum_{k=1}^{n} q_{i,k} = \sum_{k=1}^{n} \bar{q}_{i,k} = \frac{1}{2}$ and $q_{i,1} = q_{i,2} = \ldots = q_{i,n} = \bar{q}_{i,1} = \bar{q}_{i,2} = \ldots = \bar{q}_{i,n} = \frac{1}{2n}$, therefore we can write the $o_i$’s expected utility as

$$E[u_i] = p\left(\sum_{k=1}^{n} q_{i,k} \cdot (-l)\right) +$$

$$p\left(\frac{\hat{\psi}}{2n} \left((n-1) + \frac{(n-2)}{2} + \ldots + \frac{1}{n-1} - (n-1)\right)\right)$$
As $n \geq 2$, we have $\mathbb{E}[u_i] \geq \mathbb{E}[u_i^0]$.

When the number of exploited organizations in the coalition is identically distributed $\mathcal{K} \sim U[0, n]$, by extending Proposition 2, we have the following observations:

- When the probability of exploitation is higher than the probability of not-exploitation ($q_{i,x} > \bar{q}_{i,y}, \forall i, x, y$), then mechanism 1 is \textit{ex ante} individually rational. In this case, with the increase in the number of organizations in the coalition, the expected utility is also increasing.

- When the probability of exploitation is less than the probability of not-exploitation ($q_{i,x} < \bar{q}_{i,y}, \forall i, x, y$), then mechanism 1 is \textit{ex ante} individually rational if the following inequality holds:

  \[
  \left( \frac{(n-2)^2}{2} + \frac{(n-3)^3}{3} + \ldots + \frac{1}{n-1} \right) \geq (\bar{q}_{i,y} - q_{i,x})
  \]

  In this case, with the increase in the number of organizations in the coalition, the expected utility is decreasing.

- In an \textit{ex ante} individually rational setting, organizations’ utilities increase with the increase in $\hat{\psi}$. Also, with the increase in the number of organizations in the coalition, the expected utility is increasing as well.

\textbf{Proposition 3.} \textit{When the probability of exploitation/not-exploitation of an organization is a fair coin and $n > 2$, the mechanism is ex ante individual rational if $q_{i,k} = 0, \forall k > 1$.}

\textit{Proof:} When the probability of exploitation/not-exploitation of an organization is a fair coin, we have $q_{i,k} = \bar{q}_{i,k} = \binom{n}{k} \cdot \left( \frac{1}{2} \right)^n$, thus the expected benefit of the mechanism is
\[ E[u_i] - E[u_i^0] = p(\hat{\psi} \cdot \left(\frac{1}{2}\right)^n \cdot \left(\binom{n}{1}\right) ((n - 1) - 1) + \binom{n}{2} \left(\frac{n - 2}{2} - 1\right) + \ldots + \binom{n}{n-1} \left(\frac{1}{n-1} - 1\right)) \]

The above equation is negative for \( n > 2 \). However, when \( k = 1 \) the expected benefit is

\[ E[u_i] - E[u_i^0] = p(\hat{\psi} \cdot \left(\frac{1}{2}\right)^n \cdot \left(\binom{n}{1}\right) ((n - 1) - 1)) \]

Which is always positive.

In order to satisfy the \textit{ex ante} individual rationality when the probability of exploitation/not-exploitation of an organization is a fair coin, we can modify mechanism 1 such that only the first organization which reports the exploitation will be reimbursed. This also accelerates the flow of cybersecurity information sharing, and organizations are stipulated to investigate the security breaches in the early stages to report damages. By applying this method and following proposition 3, we can see that when \( q_{i,1} \geq \bar{q}_{i,1} \) the mechanism is \textit{ex ante} individual rational, and when \( q_{i,1} < \bar{q}_{i,1} \), the mechanism is \textit{ex ante} individual rational if \((q_{i,1}(n - 1) - \bar{q}_{i,1}) \geq 0\). In other words, this observation indicates that as the probability of not-exploitation is increasing, the organizations’ utilities are decreasing in mechanism 1.

\textbf{Improvement}

Note that in mechanism 1, as all of the organizations in the coalition should be able to afford \( c_i = \hat{\psi} \), the value of \( \hat{\psi} \) has been set to the least amount between all of the proposed values from the organizations. However, this limits the benefits organizations can receive from the coalition especially when the variance of the proposed values \( \tilde{\psi} \) is high. For instance, assume a coalition of three organizations, where a small organization \( o_1 \) would set \( \psi_1 = \$1000 \), while the other two big
organizations \( o_2 \) and \( o_3 \) would set \( \psi_2 = \psi_3 = $100,000 \), in this case, \( \hat{\psi} = $1000 \) will be selected. However, the coalition of two big companies will bring more values for them since in that case \( \hat{\psi} \) will be $100,000. On the other hand, a malicious organization \( o_i \) would bid a small value for \( \psi_i \) to decrease the performance of other organizations in the coalition. To solve this problem, we present the extension of mechanism 1 to make a set of coalitions as follows.

**Mechanism 1 extension.** Following mechanism 1, after making the first coalition, the organization with the least proposed value is removed from the coalition and the process is repeated by setting the new proposed values as \( \psi_i = \psi_i - \hat{\psi} \). The iteration continues until two organizations remain in the coalition.

We explain the mechanism 1 extension with an example. Consider the previous example with three organizations and proposed values as \( \bar{\psi} = \{1000, 100000, 100000\} \). In this case, in the first iteration, \( \hat{\psi} \) will be set to 1000. After the first iteration, \( o_1 \) will be removed, and the new coalition is \( \{o_2, o_3\} \), with \( \bar{\psi} = \{99000, 99000\} \), thus the new \( \hat{\psi} \) will be set to 99,000. Assume that an attacker exploits a new vulnerability of a common platform over \( o_1, o_2 \). Then, \( o_3 \) pays $1000 for the first coalition of the three organizations, and \( o_1, o_2 \) each receives $500 as indemnity. On the other hand, \( o_3 \) pays $99,000 to \( o_2 \) for the second coalition.

**Claim 1.** Mechanism 1 alleviates the moral hazard and adverse selection problems, and it is incentive compatible.

It is easy to see that, as in mechanism 1, the organizations act as both insurer and insured, the moral hazard and adverse selection requirements are alleviated. On the other hand, since growing the number of exploited organizations decrease all of the organizations’ utilities, then organizations are stipulated to invest in security and share their vulnerability information in the system which makes the system incentive compatible.
**Fairness Issue**

When the probability of exploitation of each organization is equal, as the exploited organizations receive the same amount while other organizations are paying the same amount to the system, the fairness property is satisfied in mechanism 1. However, when the probability of exploitation is not equal, mechanism 1 is not fair. As the risk of exploitation of organizations is different, their payment and indemnity should be set accordingly to satisfy the fairness property.

For example, consider that there are two organizations using the same platform, and they have made a coalition. An attacker finds a new vulnerability but as he is resource bounded, it is not possible to attack both organizations at the same time. In addition, the attacker knows that the exploited organization is going to share the vulnerability information with the other organization and the other organization will patch its system afterward. In this case, the attacker chooses an organization with the highest benefit to attack. Hence, we have $q_{1,1} \neq q_{2,1}$.

Therefore, if we set the $\hat{c}_{i,k}$ and $\hat{\pi}_{i,k}$ following mechanism 1, then the *ex ante* individual rationality and fairness property will not be satisfied. In this case, we can apply the following mechanism.

**Mechanism 2.** Once the system receives the organizations’ proposed values for the commitment $\bar{\psi} = \{\psi_1, ..., \psi_n\}$, the commitment and indemnity for all of the organizations are calculated as

\[
\hat{c}_{i,k} = \hat{\psi} \cdot q_{i,k} \\
\hat{\pi}_{i,k} = \frac{\sum_{i \in K} q_{i,k} \cdot \hat{\psi}}{k}
\]
Note that in mechanism 2, the commitment and indemnity values are tuned based on the probability of an attack to meet the fairness property.

**Proposition 4.** *The mechanism 2 satisfies the budget balanced property.*

*Proof:* We need to show that the total commitment values are equal to the total reimbursements.

\[
\sum_{i \in \bar{K}} \hat{c}_i = \sum_{i \in \bar{K}} \hat{\psi} \cdot q_{i,k} \\
\sum_{i \in \bar{K}} \hat{\pi}_{i,k} = \sum_{i \in \bar{K}} \frac{\sum_{j \in \bar{K}} q_{j,k} \cdot \hat{\psi}}{k} = \sum_{j \in \bar{K}} \hat{\psi} \cdot q_{j,k}
\]

\[\blacksquare\]

**Proposition 5.** *The mechanism 2 satisfies the ex ante individual rationality property if the following inequality holds*

\[
\sum_{j \in \{-i\}} \frac{q_{j,k}}{k} \geq \bar{q}_{i,n-k}, \quad \forall i, k
\]

*Proof:* For *ex ante* individual rationality, we need to show that, the expected utility of an organization in the coalition is higher than the expected utility of an organization outside of the coalition \(E[u_i] \geq E[u_i^0]\). Using the mechanism 2, we can expand the \(o_i\)'s expected utility as
\[ E[u_i] = \bar{q}_{i,n-1} \cdot (-\hat{\psi} \cdot q_{i,1}) + \frac{\sum_{j \in \{i+1\}} q_{j,1} \cdot \hat{\psi}}{1} + \frac{\sum_{j \in \{i+1\}} q_{j,2} \cdot \hat{\psi}}{2} + \frac{\sum_{j \in \{i+1\}} q_{j,n-1} \cdot \hat{\psi}}{n-1} \]

As \( E[u_0] = p(\sum_{k=1}^{n} q_{i,k} \cdot (-l)) \), then \( E[u_i] \) can be written as

\[
E[u_i] = E[u_0] + p((q_{i,1} \cdot \hat{\psi})\left(\frac{\sum_{j \in \{i+1\}} q_{j,1}}{1} - \bar{q}_{i,n-1}\right) + (q_{i,2} \cdot \hat{\psi})\left(\frac{\sum_{j \in \{i+1\}} q_{j,2}}{2} - \bar{q}_{i,n-2}\right) + ... + (q_{i,n-1} \cdot \hat{\psi})\left(\frac{\sum_{j \in \{i+1\}} q_{j,n-1}}{n-1} - \bar{q}_{i,1}\right))
\]

From the above equation, it can be seen that when \( \forall i, k \) we have \( \sum_{j \in \{i+1\}} \frac{q_{i,k}}{k} \geq \bar{q}_{i,n-k} \), then \( E[u_i] \geq E[u_0] \).

**Mechanism 2 extension.** As it can be seen from proposition 5, with the growth of the number of exploited organizations, the system moves toward violating the *ex ante* individual rationality property. Thus, in order to satisfy the *ex ante* individual rationality property, we can set the policy to just reimburse the first \( \hat{k} \) organizations which report the damage of exploitation of a new vulnerability.

Here, \( \hat{k} \) is the maximum number satisfying the \( \sum_{j \in \{i+1\}} \frac{q_{i,k}}{k} \geq \bar{q}_{i,n-k}, \forall i \). As the function \( \sum_{j \in \{i+1\}} \frac{q_{i,k}}{k} - \bar{q}_{i,n-k}, \forall i \) is decreasing with increasing of \( \hat{k} \), \( \hat{k} \leq n \), and \( n \) is not large, then \( \hat{k} \) can be found by exhaustive search. This approach also accelerates the flow of cybersecurity information sharing, and organizations are
stipulated to investigate the security breaches at early stages to report damages. Moreover, the same approach introduced in the mechanism 1 extension can be applied to improve the performance of mechanism 2 by making several coalitions based on the proposed commitment values.

**Claim 2.** The mechanisms 2 alleviates the moral hazard and adverse selection problems, and it is fair and incentive compatible.

Same as mechanism 1, as the organizations act as both insurer and insured, the moral hazard and adverse selection requirements are alleviated. On the other hand, since the exploitation of an organization decreases all of the organizations’ utilities, then organizations are stipulated to invest in security and share their vulnerability information in the system which makes the system incentive compatible. Also, as only the first $\hat{k}$ exploited organizations are reimbursed, organizations tend to invest in monitoring security breaches and report them as early as possible. This empowers the cybersecurity information sharing. Moreover, as the organizations’ commitment and reimbursement to the system are based on the probability of their exploitation, the fairness property will be satisfied as well.

**Flexibility Challenge**

Although mechanisms 1 and 2 are beneficial for the organizations, they do not allow organizations to set their indemnity value directly. If a mechanism allows the organizations to choose their own values for indemnity and commitment, then as the system should satisfy the budget balanced property, the organizations who commit to less value achieve more utility. This makes the $c_i = 0$ the best response strategy of the organizations. On the other hand, when the loss value is large, organizations might not be able to cover the cost of loss and as a result, the total commitment value can be far from the required loss coverage. In order to solve this
problem, in the next sections, we study the mechanisms to give the flexibility of choosing commitment and indemnity to the organizations. To this end, we apply the premium and reward in the design to satisfy the budget balanced property and motivate organizations to make the commitment.

5.2.2 Crowdfunding the Coalitional Insurance Framework with Different Level of Indemnity and Commitment

In this section we study a model which is equipped to the premium and reward, to let organizations choose the coverage level and the commitment while satisfying the budget balanced property. Furthermore, this model achieves outsiders participation by providing a reward to them.

As the system should be budget balanced, the total value of the rewards should be equal to the total premium values. Let \( c = \{\hat{c}_{i,j}\}, \forall i, j \) and \( \beta = \{\beta_i\}, \forall i \). The reward value, \( o_i \) receives from the system can be represented as \( R_i(c, \beta) : \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}^+ \). In addition, we have \( \frac{\partial R_i(c, \beta)}{\partial c_i} > 0 \) as the reward value is an increasing function of the commitment value to the system. Then, the \( o_i \)'s expected utility is

\[
E[u_i] = p \left( \sum_{k=1}^{n} q_{i,k} \cdot (-l_i + \hat{\pi}_{i,k}) + \bar{q}_{i,n-k} \cdot (-\hat{c}_{i,n-k}) \right) + (1 - p) \cdot R_i(c, \beta) - \beta_i
\]

s.t. \( \sum_{k=1}^{n} q_{i,k} + \sum_{k=1}^{n} \bar{q}_{i,k} = 1, \hat{\pi}_{i,n} = 0, \hat{c}_{i,0} = 0 \)

We set reward as \( R_i(c, \beta) = \frac{\sum_{i=1}^{n} \beta_i}{\sum_{i=1}^{n} c_{i,j}} \times \sum_{j=1}^{n} c_{i,j} \) to meet the fairness requirement. Because of the reward value, this model motivates the risk-seeker entities out of the coalition to participate in the insurance process as well.
In this model, the reward and premium values are controller variables to stabilize the system. To increase the total commitment value, the system can increase the reward, which causes the increase of premium. In contrast, the system can decrease the premium, by decreasing the reward that causes the decrease of the total commitment value.

It can be seen that in the worst case scenario, $o_i$ commits to $c_i$ and does not insure itself, thus it endures the full cost of commitment payment and the loss of attack, and its utility will be $u_i = -l_i - c_i$. Conversely, in the best case scenario, $o_i$ does not insure itself and no organization is getting exploited, thus its utility will be $u_i = R_i(c_i, \beta)$. The worst case scenario and the best case scenario happen to the risk-seeker organizations, while the risk-averse organizations enroll in the insurance.

Note that in this model as the organizations are charged based on their coverage level, they should be reimbursed in the case of a cyber-attack. However, it is not always possible to satisfy the budget balanced property since as the number of exploited organizations grows, the available budget in the pool decreases. To solve this problem, we present two approaches as follows.

**Approach 1.** In order to satisfy the budget balanced property and motivate organizations to share their cybersecurity information, the system can set its policy such that only the first organization, which reports the exploitation of a new vulnerability, receives the reimbursement. This mechanism works as follows; At the beginning, organizations submit their desired commitment values $\{c_i\}$ to the system. Then organizations choose their coverage level $\pi_i$ from $0 \leq \pi_i \leq \sum_{j \in \bar{K}} c_j$.

In this case, having the actuarially fair premium, $o_i$’s expected utility is

$$E[u_i] = p(q_{i,1} \cdot (-l_i + \pi_i) + \bar{q}_{i,n-1} \cdot (-\sum_{j \in \bar{K}} c_j)) + (1-p) \cdot (p \cdot \sum_{j=1}^{n} q_{j,1} \cdot \pi_j \sum_{j=1}^{n} c_j \cdot c_i) - (p \cdot q_{i,1} \cdot \pi_i)$$
In this case, organizations are stipulated to investigate the security breaches and accelerate the reporting of such information; this improves the flow of cybersecurity information in the coalition.

**Proposition 6.** Approach 1 satisfies the budget balanced property.

*Proof:* For the budget balanced property, we need to show that the total commitment received from the organizations is equal to the indemnity which the exploited organization will be reimbursed, and the total rewards are equal to the total premiums.

\[
\sum_{i \in \mathcal{K}} \frac{\pi_{\kappa \in \mathcal{K}}}{\sum_{j \in \mathcal{K}} c_j} \cdot c_i = \frac{\pi_{\kappa \in \mathcal{K}}}{\sum_{j \in \mathcal{K}} c_j} \cdot \sum_{i \in \mathcal{K}} c_i = \pi_{\kappa}
\]

And

\[
\sum_{i=1}^{n} \mathcal{R}_i(c, \beta) = \sum_{i=1}^{n} \left( p \cdot \sum_{j=1}^{n} \frac{q_{j,1} \cdot \pi_j}{c_j} \cdot c_i \right) = \\
\sum_{i=1}^{n} p \cdot q_{i,1} \cdot \pi_i = \sum_{i=1}^{n} \beta_i
\]

**Discussion**

This model does not satisfy *ex ante* individual rationality and as a result a risk-neutral organization’s best response strategy is to bid \( \hat{c}_i = 0, \hat{\pi}_i = 0 \). However, the risk-averse organization’s best response strategy is to bid \( \hat{\pi}_i = l_i, \hat{c}_i = 0 \) as the premium is actuarially fair. On the other hand, the risk-seeker entities would set \( \hat{\pi}_i = 0, \hat{c}_i > 0 \) and selects \( \hat{c}_i \) based on its budget and risk function. Thus, this model will be advantageous if and only if we have risk-seeker organizations in the model. In order to achieve this, the platform can allow other entities outside of the coalition to participate in the insurance process as well. In this case, the risk-seeker entities make a commitment with the goal of receiving a reward from the premiums.
organizations pay to the coalition. This crowd-funding model allows organizations to have more power on the price of cyber-insurance to avoid a monopoly market.

**Approach 2.** As another approach, the system can reimburse the organizations based on the total exploited organizations and the available budget in the pool. In this case, the available budget will be distributed fairly among the exploited organizations. The system charges organizations based on their expected coverage level. Let us define $\Gamma(\pi_i)$ as follows

$$\Gamma(\pi_i) = \begin{cases} 
\pi_i & \sum_{j \in K} \pi_j \leq \sum_{j \in \bar{K}} c_j \\
\frac{\sum_{j \in \bar{K}} c_j}{\sum_{j \in K} \pi_j} \cdot \pi_i & \text{Otherwise}
\end{cases}$$

As the organizations should pay their premium based on the expected coverage that they will be reimbursed in the case of exploitation, then assuming that the organizations are exploited with the same probability, the fair premium is

$$\hat{\beta}_i = p(q_{i,1} \cdot (\Gamma(\pi_i)) + q_{i,2} \cdot (\Gamma(\pi_i + \bar{\pi}_{-i})) + q_{i,3} \cdot (\Gamma(\pi_i + 2 \times \bar{\pi}_{-i})) + ... + q_{i,n-1} \cdot (\Gamma(\pi_i + (n - 2) \cdot \bar{\pi}_{-i}))$$

Where $\bar{\pi}_{-i}$ represents the average indemnity of the organizations in the coalition excluding $o_i$. In addition, the commitment value is

$$\hat{c}_i = \begin{cases} 
c_i & \sum_{j \in K} c_j \leq \sum_{j \in \bar{K}} \pi_j \\
\frac{\sum_{j \in \bar{K}} \pi_j}{\sum_{j \in K} c_j} \cdot c_i & \text{Otherwise}
\end{cases}$$

**Proposition 7.** Approach 2 satisfies the budget balanced property.
Proof: We need to show that the total commitment value is equal to the total reimbursement value. When \( \sum_{j \in K} c_j \leq \sum_{j \in K} \pi_j \) we have

\[
\sum_{i \in K} \hat{c}_i = \sum_{i \in K} c_i \\
\sum_{i \in K} \Gamma(\pi_i) = \sum_{i \in K} \left( \frac{\sum_{j \in K} c_j}{\sum_{j \in K} \pi_j} \right) \cdot \pi_i = \sum_{j \in K} c_j
\]

And when \( \sum_{j \in K} \pi_j \leq \sum_{j \in K} c_j \) we have:

\[
\sum_{i \in K} \hat{c}_i = \sum_{i \in K} \frac{\sum_{j \in K} \pi_j}{\sum_{j \in K} c_j} \cdot c_i = \sum_{j \in K} \pi_j \\
\sum_{i \in K} \Gamma(\pi_i) = \sum_{i \in K} \pi_i
\]

Outsider Participation

As we have discussed earlier, in this model, the risk-seeker entities outside the coalition is also able to invest in the insurance with the goal of receiving a reward. In this case, the premium and reward should be set in such a way to attract outsiders to invest in the system. In other words, the \textit{ex ante} individual rationality property for the outsiders should be satisfied. Therefore, the expected utility of an entity outside of the coalition should be larger than zero \( \mathbb{E}[u_{\text{ext}}(c_{\text{ext}})] > 0 \). Let \( \hat{\beta} = ||\beta||_1 \) represent the total premium collected from the coalition. Algorithm 1 can be used to achieve this goal. In this algorithm, the premium has been set to satisfy the \textit{ex ante} individual rationality for the external entities. First, the expected indemnity cost and the expected available budget are calculated in lines 1-6. Then, in lines 7 and 12, the algorithm compares the expected indemnity cost and expected available budget to check the corresponding requirement. In case
\( \tilde{c} \leq \tilde{\pi} \), the following should be held

\[
E[u_{ext}(c_{ext} | \tilde{c} \leq \tilde{\pi})] = p(-c_{ext}) + \left(1 - p\right) \left(\frac{\tilde{\beta}}{\sum_{j=1}^{n} c_j + c_{ext}} \cdot c_{ext}\right) > 0 \Rightarrow 
\]

\[
\tilde{\beta} > p \cdot \left(\frac{\sum_{i=1}^{n} c_i + c_{ext}}{1 - p}\right) 
\]

And in case \( \tilde{\pi} < \tilde{c} \) the following requirement should be satisfied

\[
E[u_{out}(c_{ext} | \tilde{\pi} < \tilde{c})] = p\left(-\frac{\tilde{\pi}}{(\tilde{c} + c_{ext})} \cdot c_{ext}\right) + \left(1 - p\right) \left(\frac{\tilde{\beta}}{\sum_{i=1}^{n} c_i + c_{ext}} \cdot c_{ext}\right) > 0 \Rightarrow 
\]

\[
\tilde{\beta} > p \cdot \tilde{\pi} \cdot \left(\frac{\sum_{i=1}^{n} c_i + c_{ext}}{(1 - p) \cdot (\tilde{c} + c_{ext})}\right) 
\]

If the requirement satisfies, then the algorithm exits, otherwise the premium value increases in lines 9 and 14. Note that this increase can be done based on the fairness definition. For example following the proportional fairness, the organizations will be charged based on their required indemnities. Once the premium has been increased, organizations might lower their coverage level accordingly, thus the algorithm jumps to line 2 to calculate \( \tilde{c} \) again.

The complexity of algorithm 1 is \( O(2^n \cdot \tilde{\pi}) \). This is because the line 4 iterates \( (2^n - 1) \) times to calculate the \( \tilde{c} \) value, and in the worst case the total requested indemnity decreases to zero in \( \tilde{\pi} \) iterations.

**Proposition 8.** *In the case of \( \tilde{c} \leq \tilde{\pi} \), outsider’s best response strategy is to commit c_{ext} as*

\[
c_{ext}^* = \sqrt{\frac{(1 - p) \cdot \tilde{\beta} \cdot \sum_{i=1}^{n} c_i}{p} - \sum_{i=1}^{n} c_i} 
\]
Algorithm 3: Tuning premium to acquire external commitment resource

Input: The vector of indemnities $\pi$, The vector of commitments $c$, The matrix of exploitation probability $Q$. The probability that an attacker finds a vulnerability for the common platform $p$, The desired commitment from an external resource $c_{\text{ext}}$, The total premium $\beta$

Output: The tuned total premium value $\tilde{\beta}$

1. $\tilde{c} \leftarrow 0$, $\tilde{\pi} \leftarrow 0$
2. $\tilde{\pi} \leftarrow \pi \cdot Q$
3. $\tilde{\pi} \leftarrow ||\tilde{\pi}||_1$
4. foreach possible set of $K \in O$ do
5. \hspace{1em} $\tilde{c} \leftarrow \tilde{c} + \prod_{i \in K} q_{i,|k|} \cdot \sum_{j \in K} c_j$
6. end
7. if $\tilde{c} \leq \tilde{\pi}$ then
8. \hspace{1em} if $\tilde{\beta} < \frac{p \cdot \sum_{i=1}^{n} c_i + c_{\text{ext}}}{1-p}$ then
9. \hspace{2em} Increase $\beta$, update $\pi$, and Goto line 2
10. end
11. end
12. if $\tilde{\pi} < \tilde{c}$ then
13. \hspace{1em} if $\tilde{\beta} < \frac{p \cdot \sum_{i=1}^{n} c_i + c_{\text{ext}}}{(1-p) \cdot \tilde{c} + c_{\text{ext}}}$ then
14. \hspace{2em} Increase $\beta$, update $\pi$, and Goto line 2
15. end
16. end
17. return $\tilde{\beta}$

Proof: As the second derivative of $E[u_{\text{out}}(c_{\text{ext}}|\tilde{c} \leq \tilde{\pi})]$ is negative, thus we calculate the first order condition as

$$\frac{\partial E[u_{\text{out}}(c_{\text{ext}}|\tilde{c} \leq \tilde{\pi})]}{\partial c_{\text{ext}}} = 0$$

$$-p + (1-p)\left(\tilde{\beta} \cdot \sum_{j=1}^{n} c_j \right) = 0$$

$$c_{\text{ext}}^* = \sqrt{(1-p) \cdot \tilde{\beta} \cdot \sum_{i=1}^{n} c_i - \sum_{i=1}^{n} c_i}$$

On the other hand, in the case of $\tilde{\pi} < \tilde{c}$ as the second derivative of the outsider’s expected utility is positive, it can be seen that the increase of commitment value, increases the expected utility.
5.2.3 Outsourcing the insurance of a common platform

Although the crowdfunding is beneficial, outsiders might not participate in the insurance process when it cannot estimate the $p$ value. This incapability of estimation might be because of the inaccessibility of a common platform (e.g. hardware) or the lack of expertise. In this case, we study a model of outsourcing the insurance of a common platform to cover the demanded coverage level. In this model, the organizations insure the cost of exploitation of the common platform’s vulnerabilities. In the case of exploitation of the vulnerabilities related to the common platform, the insurer reimburses the organizations that have been damaged.

The benefits of this model are as follows:

- The insurer has a better estimation of the probability of the exploitation $p$. Since in the traditional cyber-insurance model it is not easy to estimate $p$ as this parameter usually depends on multiple systems working together. On the other hand, there are some limitations to the security evaluation of the entire system. While in this model, the coverage is limited to only the common platform. This comforts the evaluation process and as a result, the adverse selection problem will be addressed partially.

- Monitoring the current security state is easier for the insurer, as the attack vectors are limited to the common platform. This alleviates the moral hazard problem.

- Organizations collaboratively insure a common platform taking advantage of sharing the price of the administrative cost. In contrast, having an incentive compatible mechanism, the insurer profits as the organizations invest more on their security and share their cybersecurity information and as a result, fewer organizations will be exploited and the cost of indemnity would decrease.
Let $\pi_K$ represent the indemnity that the insurer should pay to the coalition considering the set of exploited organizations $K$. Then, the total premium that the coalition should pay $\hat{\beta}_O$ is

$$\hat{\beta}_O = p\left(\sum_{i=1}^{n} \sum_{j=1}^{n} q_{i,j} \cdot \pi_i\right) + \tau$$

And the expected utility of the coalition is

$$\mathbb{E}[u_O] = p\left(-\sum_{i\in K} l_i + \pi_K\right) - \hat{\beta}_O$$

Then to satisfy the fairness property, $o_i$’s premium can be calculated as

$$\hat{\beta}_i = p\left(\sum_{j=1}^{n} q_{i,j} \cdot \pi_i\right) + \left(\sum_{j=1}^{n} q_{i,j} \cdot \tau\right)$$

Note that, this model is beneficial for the organizations as the administrative cost of the insurer is divided between them. However, as the organizations have outsourced the risk of exploitation, they might decrease their investment in the security of the common platform and they are not motivated to share their cybersecurity information. In order to satisfy the incentive compatibility, the following approaches can be applied.

**Approach 1.** The insurer does not provide the full coverage. In this case, as the organizations also endure the cost of exploitation, they would invest in the security of the common platform. However, in this case, the incentive compatibility problem is still existing as organizations are not motivated to share their cybersecurity information.

**Approach 2.** In order to stipulate organizations and free-market security testers to invest in the security of the common platform to find a new vulnerability, the system can provide a bug bounty rewarding system [113–115]. In this case, the
system pays the vulnerability finder. However, it is important to set a reward value properly, since if the value is small, then there is no motivation for investment in finding a new vulnerability. Worse than that, a free market tester who finds a new vulnerability might sell the vulnerability information on the black market. On the other hand, if the value is high, the organizations and insurance company might lose. The value of a vulnerability for the coalition of organizations \( v_c \) is

\[
v_c = \sum_{i=1}^{n} \sum_{j=1}^{n} q_{i,j} (l_i - \pi_i)
\]

On the other hand, the value of the vulnerability for the insurer \( v_I \) is

\[
v_I = \sum_{i=1}^{n} \sum_{j=1}^{n} q_{i,j} (\pi_i)
\]

Thus, the total benefit of accessing the vulnerability information to patch the system is \( \mathcal{V} = v_c + v_I = \sum_{i=1}^{n} \sum_{j=1}^{n} q_{i,j} \cdot l_i \) which is equal to the case of no insurance being applied. As studied in [116, 117], the fair payment to the vulnerability finder is half of the benefit of the information beneficiaries.

**Proposition 9.** Assume there is a black market value \( v_b \) for the new vulnerability and this value is an independent draw from a uniform distribution with support \([0, N]\), then the best response strategy of the system is to offer \( \frac{\mathcal{V}}{2} \) to the vulnerability finder.

**Proof:** Let \( \theta \) represent the offer to the vulnerability finder. The expected payoff of the system is

\[
\mathbb{E}[u_s] = Pr(v_b < \theta) \cdot (\mathcal{V} - \theta)
\]

\[
= \left( \frac{\theta}{N} \right) \cdot (\mathcal{V} - \theta)
\]
The first order condition is

\[
\frac{\partial}{\partial \theta} \left( \frac{\theta}{N} \cdot (V - \theta) \right) = 0
\]

\[
\frac{V - \theta^*}{N} - \frac{\theta^*}{N} = 0
\]

\[
\theta^* = \frac{1}{2} \cdot V
\]

As the second derivative of the expected gain is negative, \( \theta^* \) provides the maximum expected gain.

Proposition 9 shows that, when the market value is not biased, the fair payment and the best response strategy are equal.

**Approach 3.** In order to motivate organizations to share their cybersecurity information and decrease the probability of exploitation of a large number of organizations from the same vulnerability, the insurer sets one part of the indemnity as the reward value. In this case, there is a fixed amount that is given to the exploited organizations, if the number of exploited organizations is small, the share of reward is large and as the number of organizations grows, this share shrinks. In this way, as with the growth of the exploited organizations the reward value decreases, the organizations tend to share their data in the coalition to receive a larger share of the reward. Let \( R \) represent the reward value, then the premiums of the coalition and each organization can be calculated as follows

\[
\hat{\beta}_\text{C} = p \left( \sum_{i=1}^{n} \sum_{j=1}^{n} q_{i,j} \cdot \pi_i \right) + R + \tau
\]

\[
\hat{\beta}_i = p \left( \sum_{j=1}^{n} q_{i,j} \cdot (\pi_i + R) \right) + \left( \sum_{j=1}^{n} q_{i,j} \cdot \tau \right)
\]
And the expected utilities of the coalition and each organization are

\[ \mathbb{E}[u_C] = p(\sum_{i \in K} -l_i + \pi_K + R) - \hat{\beta}_O \]

\[ \mathbb{E}[u_i] = p\left(\sum_{j=1}^{n} q_{i,j} \cdot (-l_i + \pi_i + \frac{R}{j})\right) - \hat{\beta}_i \]

It is easy to see that the above model is budget balanced and incentive compatible to motivate organizations for security investment and sharing behavior.

The combination of the three approaches mentioned above can be used to achieve the best result.

Figure 5.2: The changes of expected benefit when \( p \), \( \hat{\psi} \), and \( n \) vary
5.3 Numerical Analysis

In this section, we analyze the expected utility of the proposed models. In the first case study, we consider a set of organizations using a common platform. For simplicity, we assume the number of exploited organizations in the coalition is identically distributed \( k \sim U[0, n] \), and the probability of exploitation/not-exploitation of an organization is a fair coin. In order to check the benefit of the coalitional self-insurance framework, we calculate the expected benefit of applying this model. Then, applying the mechanism 1, the profit of an organization in the coalition is

\[
p(\frac{\hat{\psi}}{2n}(\frac{n-2}{2} + \ldots + \frac{1}{n-1}))
\]

as discussed in proposition 2. Figure 5.2 depicts the expected benefits of an organization in the coalition when \( p \), \( \hat{\psi} \), and \( n \) vary. In figures 5.2 (a) and (b), we have set \( p = 0.1 \).

As it can be seen with the increase of \( n \) (figure 2. (a)), \( \hat{\psi} \) (figure 2. (b)), and \( p \) (figure 2. (c)), an organization’s expected benefit increases with increasing rates. This implies that when the probability of an attack to organizations over the common platform is not biased, organizations’ expected benefit is increasing with the growth of the probability of finding a vulnerability by an attacker, the organizations’ commitment value, and the number of organizations in the coalition.

In the next case study, we consider a set of risk-averse organizations that aim to cover a specific amount of the indemnity in the case of a cyber-attack. Note that although mechanism 1 or 2 can be applied, as organizations are resource-bounded, they might not be able to commit to large values to cover all of the requested indemnities. For example, consider that a loss of an attack for an organization is $1,000,000 yet the expected coverage level applying mechanism 1 or 2 is $10,000. Thus, in this case, organizations outsource the insurance. The benefit of applying the crowdfunding is that organizations can achieve a cheaper premium for their insurance service by saving the insurance administrative cost. Furthermore, this helps to change a monopolistic insurance market into a competitive market. To
analyze the crowdfunding model, we check how the outsiders’ commitment value changes with the variation of other parameters. As in this model, the expected coverage level is higher than the expected commitment coverage of organizations in the coalition, we study the case of $\bar{c} \geq \bar{x}$. In this case, following proposition 8, the outsider chooses $c^*_{ext} = \sqrt{(1-p)\tilde{\beta} \sum_{i=1}^{n} c_i - \sum_{i=1}^{n} c_i}$ to maximize its benefit. Figure 5.3 depicts an outsider’s best response commitment strategy, when the total internal commitment $\sum_{i=1}^{n} c_i$, the probability of finding a new vulnerability $p$, and the total premium value $\tilde{\beta}$ vary. As it can be seen, with the growth of $p$ and $\sum_{i=1}^{n} c_i$, the outsider commitment decreases with an increasing rate; and with the increase of $\tilde{\beta}$, the outsider commitment increases with a decreasing rate.

Finally, consider the case of outsourcing the insurance of a common platform to an insurer. We follow the model introduced in section 4.3 to collaboratively outsource a common platform to an insurer. In this case, the risk-averse organizations register for the insurance. We apply Constant Absolute Risk Aversion (CARA) to model the organizations’ risk aversion [17, 18]. CARA is one of the most well-known candidate functions to model the utility function considering the risk aversion level. This function maps wealth to utility by $u(w) = -\exp(-\sigma \cdot w)$, where $\sigma$ indicates the degree of risk aversion. The expected benefit is calculated based on the discount of the administrative cost and also the decrease of exploitation probability by assuming that the organizations in the coalition share the probability of attack between themselves. Figure 5.4 depicts how the risk-averse organizations benefit from such a model when the number of organizations in the coalition vary. We have set the $E[u^0_i] = -10$ and we calculated the expected benefit for organizations with different level of risk aversion $\sigma = 0.01, \sigma = 0.05$, and $\sigma = 0.1$. As it can be seen by increasing the number of organizations in the coalition, the organizations’ utilities are increasing.

Note that although in this section we have discussed the direct benefits of applying the model, as discussed in the chapter, the main advantages of the proposed models
Figure 5.3: Outsider commitment value

Figure 5.4: The expected benefit of a risk-averse organization by cooperatively outsourcing the insurance of a common platform are their indirect profits which are the alleviation of the moral hazard, adverse selection, and motivating organizations toward the social welfare by investing in cybersecurity and sharing cybersecurity information.
Chapter 6

Conclusion

Despite the benefits of sharing cybersecurity information, stimulating organizations to share their cybersecurity information is a big challenge. As such sharing is costly, organizations tend to free-ride in the system and as a result, useful information is not getting shared. To motivate sharing behavior, we have proposed a set of mechanisms. We investigated the Shapley Value and Nucleolus solution concepts of cybersecurity information sharing as a coalitional game to reach a fair, dynamic, and stable profit sharing method.

We have also studied the problem of sharing cybersecurity information taking privacy cost into account. Considering the impact of cyber attacks at the organizational level, it is crucial to adopt the sharing of cyber-threat information as a common practice. However, the privacy of participating organization remains a bottleneck in self-motivating toward the exchange of such critical information. Considering the involvement of three categories of players such as organizations, attackers, and CYBEX, we formulated a dynamic game among them to derive the optimal strategy of how much sanitation an organization must choose to keep its net benefit maximum. At the same time, CYBEX figures out the optimal incentive amount to motivate organizations to share and participation cost to impose using
best response analysis. The simulation results depict the efficiency of the proposed models. Furthermore, we proposed a new privacy-preserving framework for cybersecurity information sharing platform using group signature and zero-knowledge proof.

Moreover, we analyzed a set of new mechanisms for cyber-insurance considering the cybersecurity information sharing. Leveraging cyber-insurance and risk inter-dependency for a common platform, we have presented three models for insuring a common platform to alleviate Moral Hazard, Adverse Selection, and Free-Riding problems. In the first model, organizations act as both insurer and insured to distribute the risk in the coalition. In the second model, the system provides rewards to crowdfund the insurance. Finally, in the third model, we have studied the outsourcing of a common platform insurance. We presented mechanisms to motivate organizations for security investment and cybersecurity information sharing while cooperatively transferring risks.
Bibliography


[12] [https://oasis-open.github.io/cti-documentation/](https://oasis-open.github.io/cti-documentation/).

[13] [https://freetaxii.github.io/](https://freetaxii.github.io/).


[27] “S.754 - to improve cybersecurity in the united states through enhanced sharing of information about cybersecurity threats, and for other purposes.’, https://www.congress.gov/bill/114th-congress/senate-bill/754/.”


[32] https://cybox.mitre.org/about/.


[128] I. Damgård and E. Fujisaki, “A statistically-hiding integer commitment scheme based on groups with hidden order,” in *International Conference on*


