DESIGNING CYBER INSURANCE POLICIES: THE ROLE OF PRE-SCREENING AND SECURITY INTERDEPENDENCE

A.VijayKumar[1], Dr.S.Leela Krishna[2], G.Tejeshwene[3], S.Rajendhar[4], E.Anvesh Reddy[5], V.Sai Pavan[6]

[1]Assistant Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[2]Associate Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[3,4,5,6] IVth Btech Student, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

ABSTRACT:

Cyber insurance is a viable method for cyber risk transfer. However, it has been shown that depending on the features of the underlying environment, it may or may not improve the state of network security. In this paper, we consider a single profit-maximizing insurer (principal) with voluntarily participating insureds/clients (agents). We are particularly interested in two distinct features of cybersecurity and their impact on the contract design problem. The first is the interdependent nature of cybersecurity, whereby one entity's state of security depends not only on its own investment and effort, but also the efforts of others' in the same eco-system (i.e. externalities). The second is the fact that recent advances in Internet measurement combined with machine learning techniques now allow us to perform accurate quantitative assessments of security posture at a firm level. This can be used as a tool to perform an initial security audit, or prescreening, of a prospective client to better enable premium discrimination and the design of customized policies. We show that security interdependency leads to a "profit opportunity" for the insurer, created by the inefficient effort levels exerted by interdependent agents who do not account for the risk externalities when insurance is not available; this is in addition to risk transfer that an insurer typically profits from. Security pre-screening then allows the insurer to take advantage of this additional profit opportunity by designing the appropriate contracts which incentivize agents to increase their effort levels, allowing the insurer to "sell commitment" to interdependent agents, in addition to insuring their risks. We identify conditions under which this type of contracts leads to not only increased profit for the principal, but also an improved state of network security.

KEY WORDS : cybersecurity , prescreening , insurance , moral hazard.

INTRODUCTION:

The Existing works consider competitive insurance markets under compulsory insurance, and analyze the effect of insurance on agents' security expenditures. The authors of consider a competitive market with homogeneous agents, and show that insurance often deteriorates the state of network security as compared to the no-insurance scenario. The existing studies a network of heterogeneous agents and show that the introduction of insurance cannot improve the state of network security. Study the impact of the degree of agents' interdependence, and show that agents' investments decreases as the degree of interdependence increases. Study a competitive market under the assumption of voluntary participation by agents, with and without moral hazard. In the absence of moral hazard, the insurer can observe agents' investments in security, and hence premium discriminates based on the observed investments. They show that such a market can provide incentives for agents to increase their investments in self-protection. However, they show that under moral hazard, the market will not provide an incentive for improving agents' investments. The impact of insurance on the state of network security in the presence of a monopolistic welfare maximizing insurer has been studied in existing system. In these models, as the insurer's goal is to maximize social welfare, assuming compulsory insurance, agents are incentivized through premium discrimination, i.e., agents with higher investments in security pay lower premiums. As a result, these studies show that insurance can lead to improvement of network security. An insurance market with a monopolistic profit maximizing insurer, under the assumption of voluntary participation, has been studied in existing work, which shows that in the presence of moral hazard, insurance cannot improve network security as compared to the no-insurance scenario.

LITERATURE SURVEY:

Organizations and businesses,big and small are facing increasingly more complex, costly and frequent cyber threats. Many technology based protection methods such as novel cryptography schemes and protection software's have been developed to reduce the risk of cyber threats. In addition to a myriad of technology based protection methods, cyber-insurance has emerged as an accepted risk mitigation mechanism, that allows purchasers of insurance policies/contracts to transfer their residual risks to the insurer. The impact of cyber insurance on firms' security investment has been quite extensively studied in the past few years. These studies include cyber-insurance as a method for risk transfer, as well as a possible incentive mechanism for risk reduction, . Many papers on cyber insurance markets have studied the impact of cyber-insurance on the state of network security. Existing literature has arrived at two seemingly contradictory conclusions about the potential of cyber-insurance as an incentive mechanism for risk reduction. The difference is mainly due to the underlying model of the insurer/insurance market. In particular, when the cyber-insurance market is modeled as a competitive market, the insurance contracts are designed with the intention of attracting clients, and are hence not optimized to induce better security behavior. As a result, the introduction of cyber-insurance deteriorates network security. Furthermore, as a consequence of the assumption of competitive markets, the insurers make no profit. On the other hand, by considering a monopolist (profit-neutral) cyberinsurer, whose goal is to increase social welfare, it is possible to design cyber-insurance contracts that lead users to improve their efforts toward securing their systems, and consequently, improve the state of security. The works in propose premium discrimination; the idea is to assign less favorable contracts (i.e., higher premiums) to agents with worse types or lower efforts. These contracts can lead to an increase in social welfare and network security, as well as non-negative profit for the insurer. However, the underlying models assume that the insurer acts to increase social welfare (due to e.g., government regulation), and is therefore not profit-maximizing. In addition, participation by agents is assumed compulsory. In this paper, we are similarly interested in the possibility of using cyberinsurance as an incentive mechanism for improved network security. We modify two of the key existing assumptions, in order to better capture the current state of cyber-insurance markets, by considering a profit-maximizing cyber-insurer, and ensuring that participation is voluntary, i.e., agents may opt out of purchasing a contract. We propose the use of pre-screening (initial audit) by the insurer; prescreening allows the insurer to evaluate the potential client's security posture, prior to offering the contract.

This essentially allows the insurer to premiumdiscriminate the agents, based on their perceived/measured state of security. We provide sufficient conditions under which the introduction of pre-screening can lead to higher profits for the insurer, and that it also positively impacts the state of security. In other words, this type of pre-screening is a potential option for making cyber-insurance contracts better drivers for improved cyber-security.

EXISTING SYSTEM:

The Existing works consider competitive insurance markets under compulsory insurance, and analyze the effect of insurance on agents' security expenditures. The authors of consider a competitive market with homogeneous agents, and show that insurance often deteriorates the state of network security as compared to the no-insurance scenario. The existing studies a network of heterogeneous agents and show that the introduction of insurance cannot improve the state of network security. Study the impact of the degree of agents' interdependence, and show that agents' investments decreases as the degree of interdependence increases. Study a competitive market under the assumption of voluntary participation by agents, with and without moral hazard. In the absence of moral hazard, the insurer can observe agents' investments in security, and hence premium discriminates based on the observed investments. They show that such a market can provide incentives for agents to increase their investments in self-protection. However, they show that under moral hazard, the market will not provide an incentive for improving agents' investments. The impact of insurance on the state of network security in the presence of a monopolistic welfare maximizing insurer has been studied in existing system. In these models, as the insurer's goal is to maximize social welfare, assuming compulsory insurance, agents are incentivized through premium discrimination, i.e., agents with higher investments in security pay lower premiums. As a result, these studies show that insurance can lead to improvement of network security. An insurance market with a monopolistic profit maximizing insurer, under the assumption of voluntary participation, has been studied in existing work, which shows that in the presence of moral hazard, insurance cannot improve network security as compared to the no-insurance scenario.

PROPOSED SYSTEM:

In this paper, we are interested in analyzing the possibility of using cyber-insurance as an incentive for improving network security. We adopt two model assumptions which we believe better capture the current state of cyber insurance markets but differ from the majority of the existing literature; we shall assume a profit maximizing cyber insurer, and voluntary participation, i.e., agents may opt out of purchasing a contract. Under this model, we focus on two features of cyber-insurance: (i) availability of risk assessment for mitigating moral hazard, and (ii) the interdependent nature of security. The first feature is due to the fact that recent advances in Internet measurements combined with machine learning techniques now allow us to perform accurate, quantitative security posture assessments at a firm level. This can be used as a tool to perform an initial security audit, or pre-screening, of a prospective client to mitigate moral hazard by premium discrimination and the design of customized policies. The second distinct feature, the interdependent nature of security, refers to the observation that the security standing of an entity often depends not only on its own effort towards implementing security metrics, but also on the efforts of other entities interacting with it within the eco-system. Such interdependency is crucial for the insurer’s contract design problem, as the insurer will need to offer coverage to each insured for both its losses due to direct breaches, as well as indirect losses caused by breaches of other entities.

SYSTEM REQUIREMENTS :

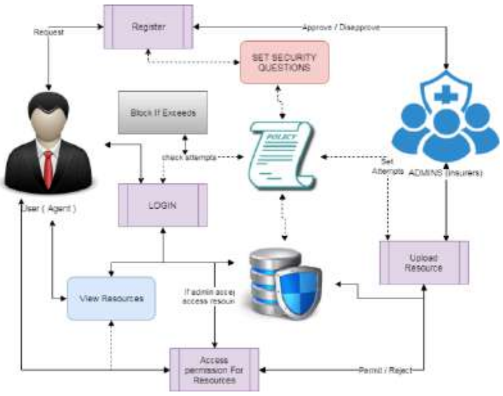
Hardware Requirements:

RAM	: 8 GB
Hard Disk	:512GB
Processor	: Pentium IV or higher

Software Requirements:

Operating Systems	:	Windows 10
Coding Languag	:	Python.
Front-End	:	Django
Back-End	:	My sql server

SYSTEM ARCHITECTURE:



CONCLUSION:

We studied the problem of designing cyber insurance contracts by a single profit-maximizing insurer, for both risk-neutral and risk-averse agents. While the introduction of insurance worsens network security in a network of independent agents, we showed that the result could be different in a network of interdependent agents. Specifically, we showed that security interdependency leads to a profit opportunity for the insurer, created by the inefficient effort levels exerted by free-riding agents when insurance is not available but interdependency is present; this is in addition to risk transfer that an insurer typically profits from. We showed that security prescreening then allows the insurer to take advantage of this additional profit opportunity by designing the right contracts to incentivize the agents to increase their effort levels and essentially selling commitment to interdependent agents. We show under what conditions this type of contracts leads to not only increased profit for the principal and utility for the agents, but also improved state of network security.

BIBLIOGRAPHY:

[1] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies: Mitigating moral hazard through security prescreening," in The 7th International EAI Conference on Game Theory fo Networks (Gamenets), 2017.

[2] M. M. Khalili, P. Naghizadeh, and M. Liu, "Designing cyber insurance policies in the presence of security interdependence," in The 12th Workshop on the Economics of Networks, Systems and Computation (NetEcon), 2017.

[3] C. Hemenwa, "ABI Research: Cyber insurance market to reach $10B by 2020," www.advisenltd.com/2015/07/30/abi-researchcyber-insurance-market-to-reach-10b-by-2020/, 2015.

[4] Insurance Information Institute, "U.S. cyber insurance market demonstrates growth, innovation in wake of high profile data breaches," www.iii.org/pressrelease/us-cyber-insurance-marketdemonstrates-growthinnovation-in-wake-of-high-profile-databreaches-102015, 2015.

[5] N. Shetty, G. Schwartz, and J. Walrand, "Can competitive insurers improve network security?," in The Third International Conference on Trust and Trustworthy Computing (TRUST), 2010.

[6] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand, “Competitive cyber-insurance and internet security,” Economics of Information Security and Privacy, pp. 229–247, 2010.

[7] G. Schwartz, N. Shetty, and J. Walrand, “Cyber-insurance: Missing market driven by user heterogeneity,” 2010.

[8] G. A. Schwartz and S. S. Sastry, “Cyber-insurance framework for large scale interdependent networks,” in The Third International Conference on High Confidence Networked Systems, 2014.

[9] H. Ogut, N. Menon, and S. Raghunathan, “Cyber insurance and it security investment: Impact of interdependence risk,” in The Workshop on the Economics of Information Security, 2005.

[10] Z. Yang and J. C. S. Lui, “Security adoption and influence of cyber-insurance markets in heterogeneous networks,” Performance Evaluation, vol. 74, pp. 1–17, Apr. 2014