MANIPULATIVE CYBER INSURANCE PROCEDURES: THE ROLE OF PRE-COMMUNICATION AND SAFETY MUTUALITY

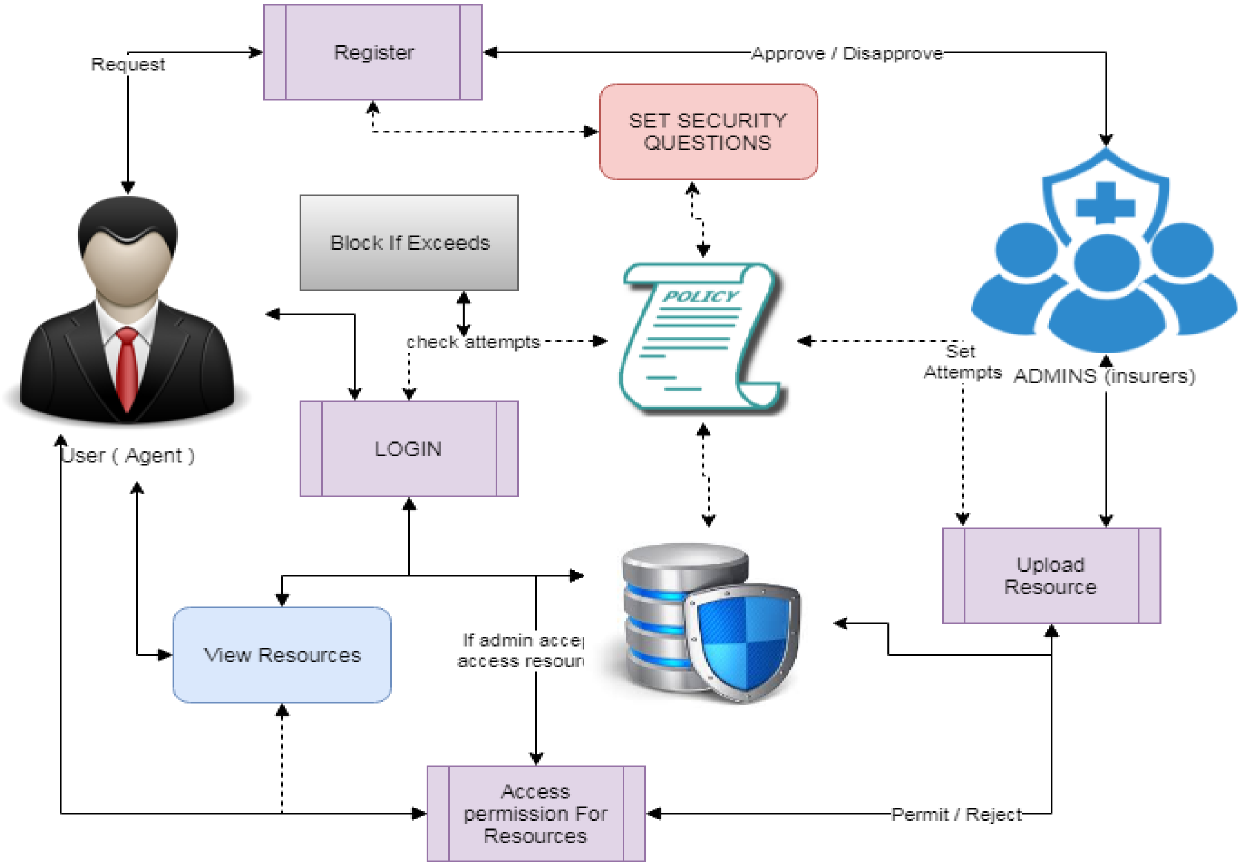
[1] MADDIRALA JAGADISH ASSISTANT PROFESSOR [2] NALLANUKALA JHANSI RANI M.TECH
[1,2] COMPUTER SCIENCE AND ENGINEERING LINGAYAS INSTITUTE OF M ANAGEMENT AND TECHNOLOGY

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.

ARCHITECTURE:



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.

ALGORITHM:

REINFORCEMENT LEARNING ALGORITHM

Reinforcement learning (RL) is an area of machine learning inspired by behaviorist psychology [citation needed], concerned with how software agents ought to take actions in an environment so as to maximize some notion of cumulative reward. The problem, due to its generality, is studied in many other disciplines, such as game theory, control theory, operations research, information theory, simulation-based optimization, multi-agent systems, swarm intelligence, statistics and genetic algorithms. In the operations research and control literature, reinforcement learning is called approximate dynamic programming, or neuron-dynamic programming. The problems of interest in reinforcement learning have also been studied in the theory of optimal control, which is concerned mostly with the existence and characterization of optimal solutions, and algorithms for their exact computation, and less with learning or approximation, particularly in the absence of a mathematical model of the environment. In economics and game theory, reinforcement learning may be used to explain how equilibrium may arise under bounded rationality. In machine learning, the environment is typically formulated as a Markov decision process (MDP), as many reinforcement learning algorithms for this context utilize dynamic programming techniques. The main difference between the classical dynamic programming methods and reinforcement learning algorithms is that the latter do not assume knowledge of an exact mathematical model of the MDP and they target large MDPs where exact methods become infeasible.

MODULES:

1. PRESCREENING

Normally the screening process of the system can be done by login system but with this system username and password alone not enough to authenticate the system. The security questions will be set to each user separately in order to make sure the correct user logged in or not. It sets the limit the access of users from threats. The class can be limited by admin while registering and admin alone approve the user’s entry to system.

2. THREAT DETECTION

The threat can be detected with the help of prescreening technique. Threats can be illegal access to system with more than five times trying to access the particular account with different act. The Insurance policies can be set to different users. According to policies users can be access. Within certain number of attempts goes wrong the user can be blocked and need to request admin to unblock again.

3. LIMIT RESOURCES

Admin is the authorized person to control polices and rules breaches. The wrong access of particular document more than certain number of time that is described in the policy can be blocked by admin and gets the intimation of breaches to admin. Then according to request by admin to user can be block or unblock the resources which are uploaded by admin/user.

4. ANALYSIS

The analysis of the system is done in this module. The proposed algorithm’s efficiency is calculated here. The comparison of various factors can be handy to calculate and visualize in the graphs such as pie chart, bar chart, line chart. The data to plot the graph is taken from the system which is done.

FUTURE WORKS:

There are a number of directions to pursue to extend the above results. As mentioned earlier, all our results are derived under the assumption of perfect information. Studying the problem with pre-screening under partial information assumptions would be an important direction of future research; this would include imperfect knowledge of the agents’ type by the principal as well as imperfect knowledge of the interdependence relationship by the agents and the principal. Other modeling choices such as alternative use of pre-screening assessment (as opposed to linear discounts on premiums), and more general ways of capturing correlated risks (e.g., joint distribution of losses as opposed to average loss being a function of joint effort), would also be of great interest. Finally, a competitive market setting and its effects on network security is also worth studying.

REQUIREMENT ANALYSIS

The project involved analyzing the design of few applications so as to make the application more users friendly. To do so, it was really important to keep the navigations from one screen to the other well-ordered and at the same time reducing the amount of typing the user needs to do. In order to make the application more accessible, the browser version had to be chosen so that it is compatible with most of the Browsers.

REQUIREMENT SPECIFICATION

Functional Requirements

- Graphical User interface with the User.

Software Requirements

For developing the application the following are the Software Requirements:

1. Python
2. Django
3. Mysql
4. Wampserver

Operating Systems supported

1. Windows 7
2. Windows XP
3. Windows 8

Technologies and Languages used to Develop

1. Python

Debugger and Emulator

- Any Browser (Particularly Chrome)

Hardware Requirements

For developing the application the following are the Hardware Requirements:

- Processor: Pentium IV or higher
- RAM: 256 MB
- Space on Hard Disk: minimum 512MB

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.

[1] Online Appendix. Available at hps://www.dropbox.com/sh/ek4p20ornmcio56/

AADjDafFU1CbbHtMB4tX7qDea?dl=0.

[2] Rainer Bohme. 2005. Cyber-insurance revisited. In ¨Proceedings of the Workshop

on the Economics of Information Security (WEIS).

[3] Rainer Bohme. 2012. Security audits revisited. In ¨ International Conference on

Financial Cryptography and Data Security. Springer, 129–147.

[4] Jean Bolot and Marc Lelarge. 2009. Cyber insurance as an incentive for Internet

security. In Managing information risk and the economics of security. Springer.

[5] Annee Hofmann. 2007. Internalizing externalities of loss prevention through

insurance monopoly: an analysis of interdependent risks. e Geneva Risk and

Insurance Review 32, 1 (2007), 91–111.

[6] Benjamin Johnson, Jens Grossklags, Nicolas Christin, and John Chuang. 2010.

Are security experts useful? Bayesian Nash equilibria for network security

games with limited information. In European Symposium on Research in Computer

Security. Springer, 588–606.

[7] Benjamin Johnson, Jens Grossklags, Nicolas Christin, and John Chuang. 2010.

Uncertainty in interdependent security games. In International Conference on

Decision and Game Theory for Security. Springer, 234–244.

[8] Jay P. Kesan, Ruperto P. Majuca, and William Yurcik. 2005. Cyber-insurance as a market-based solution to the problem of cybersecurity-a case study. In Proceedings of the Workshop on the Economics of Information Security (WEIS).

[9] Mohammad Mahdi Khalili, Parinaz Naghizadeh, and Mingyan Liu. 2017. Designing cyber insurance policies: Mitigating moral hazard through security pre-screening. In the 5th International Conference on Game Theory for Networks (GameNets). IEEE.

[10] Marc Lelarge. 2012. Coordination in network security games: a monotone

comparative statics approach. IEEE Journal on Selected Areas in Communications

30, 11 (2012), 2210–2219.

[11] Marc Lelarge and Jean Bolot. 2009. Economic incentives to increase security in

the Internet: e case for insurance. In Proceedings of IEEE INFOCOM. 1494–1502.

[12] Yang Liu, Armin Sarabi, Jing Zhang, Parinaz Naghizadeh, Manish Karir, Michael

Bailey, and Mingyan Liu. 2015. Cloudy with a Chance of Breach: Forecasting

Cyber Security Incidents. In Proceedings of the 24th USENIX Security Symposium.

[13] Andreu Mas-Colell, Michael Dennis Whinston, and Jerry R. Green. 1995. Microe-

conomic theory. Oxford University press, New York.

[14] R. Ann Miura-Ko, Benjamin Yolken, Nicholas Bambos, and John Mitchell. 2008.

Security investment games of interdependent organizations. In Proceedings of

46th Annual Allerton Conference on Communication, Control, and Computing.

252–260.

[15] Hulisi Ogut, Nirup Menon, and Srinivasan Raghunathan. 2005. Cyber insurance

and IT security investment: Impact of interdependence risk. In Proceedings of

the Workshop on the Economics of Information Security (WEIS).

[16] Ranjan Pal, Leana Golubchik, Konstantinos Psounis, and Pan Hui. 2014. Will

cyber-insurance improve network security? A market analysis. In Proceedings of

IEEE INFOCOM. 235–243.

[17] Galina A Schwartz and S Shankar Sastry. 2014. Cyber-insurance framework

for large scale interdependent networks. In Proceedings of the 3rd international

conference on high condence networked systems. ACM, 145–154.

[18] Nikhil Shey, Galina Schwartz, Mark Felegyhazi, and Jean Walrand. 2010. Com-

petitive cyber-insurance and internet security. In Economics of Information

Security and Privacy. Springer, 229–247.

[19] Nikhil Shey, Galina Schwartz, and Jean Walrand. 2010. Can competitive insurers

improve network security?. In International Conference on Trust and Trustworthy

Computing. Springer, 308–322.

[20] Zichao Yang and John CS Lui. 2014. Security adoption and inuence of cyber-insurance markets in heterogeneous networks. Performance Evaluation 74 (2014),1–17.