Designing Cyber Insurance Policies: The Role of Pre-Screening and Security Interdependence

B SRINIVASA RAO[1], A KALAVATHI[2]
[1, 2] *Department of Computer Applications, Vasireddy Venkatadri Institute of Technology, Guntur, India*

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 cyber security and their impact on the contract design problem. The first is the interdependent nature of cyber security, 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 pre-screening, 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.***

Indexed Terms- ***System, Python, Django, MySQL, and WampServer.***

I. 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.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.

II. MODULES

- 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.

- THREAT DETECTION

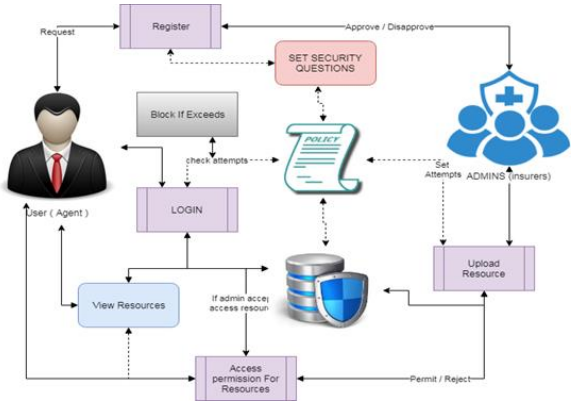
The threat can be detected with the help of prescreening technique. Threats can be illegal access to system with more than five times trying to access the particular account with different act. The Insurance policies can be set to different users. According to policies users can be access. Within certain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

- 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.

- ANALYSIS

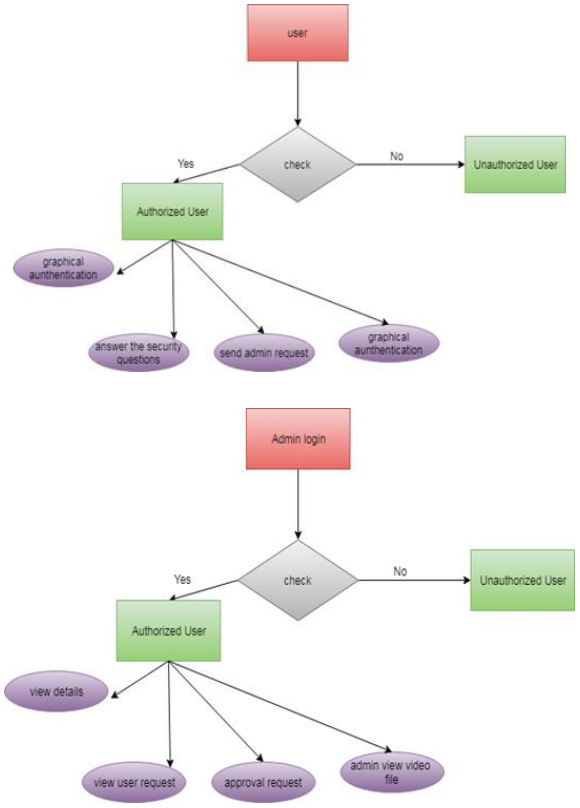
The analysis of the system is done in this module. The proposed algorithm's efficiency is calculated here. The comparison of various factors can be handy to calculate and visualize in the graphs such as pie chart, bar chart, line chart. The data to plot the graph is taken from the system which is done.



III. ER DIAGRAM

- User

This diagram shows the user functionality in this if the user is Check no the user is unauthorized user otherwise authorized User then continue the there function.



- Admin

This diagram shows the admin functionality in this if the admin is Check no the admin is unauthorized user otherwise authorized Admin then continue the there function.

IV. 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.

- FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential. Three key considerations involved in the feasibility analysis are, this study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of

training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

TYPES OF TESTS

- Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

- Integration testing

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

- Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input: identified classes of valid input must be accepted.
Invalid Input: identified classes of invalid input must be rejected.
Functions: identified functions must be exercised.
Output: identified classes of application outputs must be exercised.
Systems/Procedures: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

- System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

- White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

- Black Box Testing

Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot “see” into it. The test provides inputs and responds to outputs without considering how the software works.

- Unit Testing

Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases. Test strategy and approach Field testing will be performed manually and functional tests will be written in detail. Test objectives all field entries must work properly. Pages must be activated from the identified link. The entry screen, messages and responses must not be delayed. Features to be tested Verify that the entries are of the correct format No duplicate entries should be allowed all links should take the user to the correct page. Integration Testing Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

- Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

TECHNOLOGIES USED

Storage and protection they defined bellow in detail.
Python is a general-purpose interpreted, interactive, Object-oriented, and high-level programming language. An interpreted language, Python has a design philosophy that emphasizes code readability (notably using whitespace indentation to delimit code blocks rather than curly brackets or keywords), and a syntax that allows programmers to express concepts in fewer lines of code than might be used in languages such as C++or Java. It provides constructs that enable clear programming on both small and large scales. Python interpreters areavailable for many operating systems. CPython, the reference implementation of Python, is open source software and has a community-based development model, as do nearly all of its variant implementations. CPython is managed by the non-profit Python Software Foundation. Python features a dynamic type system and automatic memory management. It supports multiple programmingparadigms,including objectorie nted, imperative, functional and procedural, and has a large and comprehensive standard library Django is a high-level Python Web framework that encourages rapid development and clean, pragmatic design. Built by experienced developers, it takes care of much of the hassle of Web development, so you can focus on writing your app without needing to reinvent the wheel. It’s free and open source. Django's primary goal is to ease the creation of complex, database driven websites. Django emphasizes reusability and "pluggability" of components, rapid development, and the principle of don't repeat yourself. Python is used throughout, even for settings files and data models.

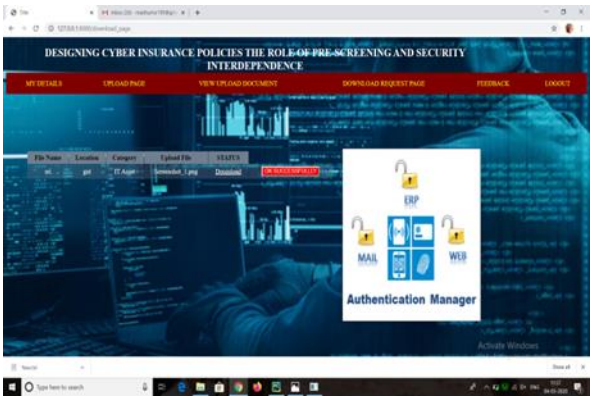
V. RESULTS

- Login Form:

The gadget starts with login page where the registered person can enter user name and password to be in a position to get right of entry to the system.

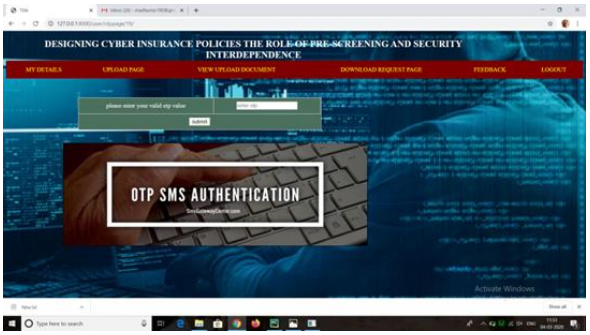
- Authentication Page

This Authentication page contain the authentication of the user by using the security things.



- OTP SMS Authentication Page:

The OTP SMS Authentication Page provides an authentication by using the SMS as a OTP (one time password).



- Details Page:

The Details Page provides the file name, category, upload file and location

- Registration Page:

The Registration Page provides the registration facility to the new user.

- Wordpress File Upload Page:

The Wordpress Upload Page provides the updation of the wordpress file.

- Details Page:

The Details Page provides details of the client first name, last name, userid , mobile number , email and gender.

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.

REFERENCES

[1] M. M. Khalili, P. Naghizadeh and M. Liu, "Designing cyber insurance policies: Mitigating moral hazard through security pre-screening", *Proc. 7th Int. EAI Conf. Game Theory Netw. (Gamenets)*, pp. 63-73, 2017.

[2] M. M. Khalili, P. Naghizadeh and M. Liu, "Designing cyber insurance policies in the presence of security interdependence", *Proc. 12th Workshop Econ. Netw. Syst. Comput. (NetEcon)*, pp. 7, 2017.

[3] C. Hemenwa, ABI Research: Cyber Insurance Market to Reach 10B by 2020, 2015, [online] Available: http://www.advisenltd.com/2015/07/30/abi-research-cyber-insurance-market-to-reach-10b-by-2020/.

[4] *U.S. Cyber Insurance Market Demonstrates Growth Innovation in Wake of High Profile Data Breaches*, 2015, [online] Available: http://www.iii.org/pressrelease/us-cyber-insurance-market-demonstrates-growthinnovation-in-wake-of-high-profile-data-breaches-102015.

[5] 5. N. Shetty, G. Schwartz and J. Walrand, "Can competitive insurers improve network security?", *Proc. 3rd Int. Conf. Trust Trustworthy Comput. (TRUST)*, pp. 308-322, 2010.

[6] 6. N. Shetty, G. Schwartz, M. Felegyhazi and J. Walrand, "Competitive cyber-insurance and Internet security", *Proc. Econ. Inf. Secur. Privacy*, pp. 229-247, 2010.

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

[8] 8. G. A. Schwartz and S. S. Sastry, "Cyber-insurance framework for large scale interdependent networks", *Proc. 3rd Int. Conf. High Confidence Netw. Syst.*, pp. 145-154, 2014.

[9] 9. H. Ogut, N. Menon and S. Raghunathan, "Cyber insurance and IT security investment: Impact of interdependence Risk", *Proc. Workshop Econ. Inf. Secur.*, pp. 1-30, 2005.

[10] 10. Z. Yang and J. C. S. Lui, "Security adoption and influence of cyber-insurance markets in heterogeneous networks", *Perform. Eval.*, vol. 74, pp. 1-17, Apr. 2014.

[11] 11. J. Kesan, R. Majuca and W. Yurcik, "The economic case for cyberinsurance", Jan. 2004.

[12] 12. J. P. Kesan, R. P. Majuca and W. Yurcik, "Cyber-insurance as a market-based solution to the problem of cybersecurity", *Proc. Workshop Econ. Inf. Secur.*, pp. 1-46, 2005.

[13] 13. A. Hofmann, "Internalizing externalities of loss prevention through insurance monopoly: An analysis of interdependent risks", *Geneva Risk Insurance Rev.*, vol. 32, no. 1, pp. 91-111, 2007.

[14] 14. M. Lelarge and J. Bolot, "Economic incentives to increase security in the Internet: The case for insurance", *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, pp. 1494-1502, Apr. 2009.

[15] 15. S. Romanosky, L. Ablon, A. Kuehn and T. Jones, "Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?", 2017, [online] Available: https://www.rand.org/pubs/working_papers/WR1208.html.

[16] 16. Y. Liu et al., "Cloudy with a chance of breach: Forecasting cyber security incidents", *Proc. USENIX Secur. Symp.*, pp. 1009-1024, 2015.

[17] 17. R. A. Miura-Ko, B. Yolken, N. Bambos and J. Mitchell, "Security investment games of interdependent organizations", *Proc. 46th Annu. Allerton Conf. Commun. Control Comput.*, pp. 252-260, Sep. 2008.

[18] 18. B. Johnson, J. Grossklags, N. Christin and J. Chuang, "Are security experts useful? Bayesian

nash equilibria for network security games with limited information", *Proc. 15th Eur. Symp. Res. Comput. Secur. (ESORICS)*, pp. 588-606, 2010.

[19] 19. B. Johnson, J. Grossklags, N. Christin and J. Chuang, "Uncertainty in interdependent security games", *Proc. 1st Conf. Decision Game Theory Secur. (GameSec)*, pp. 234-244, 2010.

[20] 20. M. Lelarge, "Coordination in network security games: A monotone comparative statics approach", *IEEE J. Sel. Areas Commun.*, vol. 30, no. 11, pp. 2210-2219, Dec. 2012.

[21] 21. R. Böhme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework", *Proc. Workshop Econ. Inf. Secur.*, pp. 1-36, 2010.

[22] 22. A. Mas-Colell, M. D. Whinston and J. R. Green, Microeconomics Theory, New York, NY, USA:Oxford Univ. Press, 1995.