Survey on Economics of Information Security

Asou Aminnezhad[1], [*] **Ramlan Mahmod**[2], **Mohd Taufik Abdullah**[3]
Faculty of Computer Science and Information Technology, University Putra Malaysia

Abstract
Economics of information security has recently become a rapidly growing field of research that is vitally important for managing the decisions and behaviors in cyberspace security. This field provides valuable insights not only for security experts, but also for policy makers, business managers, economists and psychologists. In this paper, we are going to discuss the emergence and evolution of economics of information security; where it came from, where it is today and its future directions. Research conducted for this survey explores the literature on economic issues in information security and review the advantages, drawbacks, and future research directions to set the scene that the assessment and analysis of the economics of information security publications followed it. Furthermore, we provide a structured discussion and overview of selected sets of works and highlight the models and theories in this field by organizing the presented works into six main categories namely information security investment, trust and privacy, network security, malicious program and malware economics, penetration testing and digital forensics and software security. Additionally, this survey aims to familiarize readers with major areas of this field already in hand to indicate the gaps and overlooked issues in the economics of security.

Keywords:
Economics of Security, Information security, Privacy, Digital Forensic, Game Theory.

1. Introduction

The rapid increase of using new technologies and digital devices are causing obstacles and risks of cyber-attacks more than ever. These security obstacles and challenges mainly stemmed from online threats that shift the attackers' goal from web vandalism and showing off their skills to financial achievement.

In this economic recession, providing security in cyberspace and keeping the attackers out of systems imposes lots of budgets on users. Meanwhile, many organizations are buckling down and tightening their budgets, often lead them to reduce their proactive security expenditures, which are putting organizations and their customers in risk. The importance of these issues has drawn a high public attention and caused the emergence of economics of security field as a springboard for enterprise security and economics.

Economics and security diverged after World War II (WW2) and started coming back together since 2000 that has become a controversial field of interdisciplinary study. Starting 2002, a group of security experts developed and expanded a series of flagship events under the name of [1] which combines expertise from various fields of computer science, economics, business, law and policy and social science. WEIS mainly aims to explore the role of incentives between attackers and defenders, identifies market failures in the Internet security and assesses investments in cyber-defense. Economics of security leads to enhance the financial outcomes while faced with the risks and attacks by combating against them. This field throws light on everyday security issues on one hand and provides new insights for computer scientists and economists on the other hand. This field also applies economic rules not only to generate breakthroughs in theoretical economics but also to understand the problems of security. Economics of security established with the aim to develop an economic models of security that caused to enhance the security for systems and users by means of economic behaviors, models and security decisions. Moreover, in this field game theory and microeconomics theory are becoming as important as the mathematics of cryptography for security engineers.

For a long time, most associations and firms did not assume the economics of security as a significant knowledge. Whereas, the research on economics of security blames the lack of user's familiarity with the risk and defense strategies issues that mainly originated from accelerating the pace of technology versus the low-speed progress in economics of technology and security [2]. Enhancing the users' knowledge with economics of security and its perspective caused to yield invaluable insights of the analysis and design of information security mechanisms. In this area [3] considered those insights and explained why security is hard by exploring the security problems. He also narrowed down the problems by using the microeconomics theory and stated that microeconomics analysis illustrates many gaps and problems that security experts had discovered earlier. Anderson highlighted issues about why security management as a tool for achieving benefit in the market is hard and arose a question about cyber war that why the government should focus on the attack than defense for information warfare. Many consider "Why information security is hard" [3]as a birth of economics of security field. Before Anderson, [4] proposed a lemon theory for a safe marketing in 1970. Lemon theory indicates a situation in marketing when vendors know about goods

Manuscript received July 5, 2016
Manuscript revised July 20, 2016

rather than a customer and bad products caused to eliminate the best ones. He reported the results of research on the economics of security and recommended some policies for dealing with practical problems in economics of security.

For using information security in response to competitor analysis systems[5, 6] published a framework by examining the strategic use of security information from a classic business perspective. They developed an investment model for maximizing the protection of security level in the system. The result illustrated that security hole by criminal activities caused possible vulnerabilities and system failure for the users.

In WEIS 2002, [7]and [8] addressed issues about behavioral economics of privacy regarding the vulnerabilities and externalities in the cyberspace that helped to broaden the economics of privacy issues. Regarding the economics of privacy, a business model by [9] argued that privacy deteriorates rapidly because it charges users by different prices for a same performance that was called price discrimination. In cyberspace, the incentives towards price discrimination and the ability to discriminate the price will be growing. Sellers will be increasingly tempted to engage in differential pricing; however, such practices are fraught with a danger since the public is likely to resent them intensely. From an economic viewpoint, price discrimination may seem profitable and desirable, since it often increases the efficiency of the economy. While, from the user viewpoint it may be offended the users privacy and often arouses strong opposition from the public. A model proposed by [10] for addressing this issue that focuses mainly on the market situation under price discrimination. They considered conditions when consumer is autonomous to choose a strategy for protecting the privacy with the aim to mitigate the side effects of price discrimination.

Apropos of this matter, [9] tackled a striking problem regarding price discrimination in the market that enhances the privacy failure. The problem mainly arose by the question that why privacy being deteriorated and confusing despite the person's effort for improving it. He asserted that a variable pricing by the firms affected the privacy and threaten it that creates the price discrimination problems. It seems to be impossible to solve privacy and security problems completely, so the users and firms need to reinforce their capability to deal with such problems [11].

Some researchers [12] explored the effects of security fears on the share prices and reported results of investigating the impact of economics of security breaches on a non-private business organization. They also provided evidences of considerable drawbacks and flaws in the information security market performance. On reflection, economics of security is not about observing at the past in anger of an economical loss by attack once faced; neither is it about observing at the present in fear of being attacked and economical loss; nor about observing at the future with ambiguity about what may happen for us. The experts in economics of security field should be observant at all times. The aim is not to worry people, but to alert them that how economics of security has progressed over the past decade. The future of economics of security can be recognized only if its past and current positions are well comprehended. Hence, Section 2 discusses the past events and Section 3 focuses on the current status of economics of information security and section 4 concludes the paper.

2. Economics of Security: Then

In this section, we provide an overview of economic issues surrounding cyber security by reviewing the published papers between 2004 and 2008. Regarding the emergence of economics of security field several authors have contended that economics and security should be merged due to the necessity of a security nature for being optimized economically. The researchers tend to correlate economics and security and strengthen the theoretical link between them by the means of game theory and microeconomics.

In this regard, Wölfl published an extensive survey on OECD [13] that considers the economics of malware issues by misaligned incentives and features of economics of security by analyzing the effects of externalities on users in the cyberspace.

Similarly, [14] presented another survey regarding the malware in the field of economics of information security that argued about the organizations necessity to protect their database and their own information at a middle level of vulnerability. The authors claimed that to avoid completely from the vulnerabilities the irrelevant expenditure just charges the users a lot and don't eliminate all the existing vulnerabilities.

Following the economics of privacy, studying digital right management (DRM), security investment, economics of security policies and related metrics have become interesting fields of study for researchers. On this matter, some analysts [15] considered digital right management and related cost model to achieve a novel result in DRM and economics of security policy. They investigated the role of DRM and its economic effects to develop the DRM systems as a trading standard.

Regarding the risk management issues, [16] measured information security risks, since the security risk cannot completely managed without employing appropriate measurement. Furthermore, they asserted that to create, destruct and contort other markets the information security mechanisms are indispensable.

One of the most striking problems around the economics of privacy and security is a market failure that followed by [17]. They argued about the factors are influencing market insurance whether global or local that used for epidemic risks and vulnerabilities in cyberspace. There is not any solvable way to get rid of such vulnerabilities, so for mitigating the possible damages using the strategic decision is the better solution than spending lot of budgets on preventing the malware infection and propagation to enhance the defenders' security. Markets and business are very interested to enhance security investment due to their risk aversion entities. On this matter, [18] started to work on the legislation ways for markets and businesses. They stated that compulsory expenditure on security may cause undesirable results like deforming the security markets and having drawback effects in business contest. They also mentioned Sarbanes-Oxley laws [19] for covert and overt the weaknesses and strength issues surrounding security investment that is a collection of legislation that deal with investment protection and risk management.

3. Economics of Security: Now

Economics of security is becoming a thriving field of study and has drawn great attention of security experts and econometrists recently. This field has been started spilling over into the interface between security, management, dependability, conventional security and privacy. It has also been started by interacting with psychology and sociology, because of undeniable effects of psychology and user behavior on users decisions about economics of security. These effects have caused that researchers think about another aspect of the economics of security that deals with psychology of human behavior.
Economic of security addresses a critical issues about choosing the technical risks by agents in the case of existing technical solutions to mitigate security and privacy risks. Also, the future of economics of security is clouded with various kinds of ambiguities due to the rapid development of technology in cyberspace. These uncertainties affected the users' awareness in cyberspace and make the familiarity with a novel knowledge of the economics of security too difficult.

3.1 The Current Economics of Security Trends

Despite of several studies that aimed at providing much needed statistical economics of security trends and issues, there is still an urgent need to find one that is complete and reliable. This paper outlines the following two phases of research as conducted for this survey to gain a good understanding of the current economics of security landscape.
Phase 1 monitor, assess and analyze articles covered in the following journals: Decision Support Systems, Telecommunications Policy and IEEE Transactions on Information Forensics and Security. The survey based on the journals published during the period of January 2008 to January 2015, but just has assessed journals that published more than 3 relevant papers during the mentioned period. After refining phase, among all of the related journals just three journals remained on the list that has been explained in the data collection part. We intend to identify the critical issues and get the complete picture of today's posture of economics of security. The question that rose from this refinement is why these journals are selected? There are many journals and publications available today that concentrate on security or economics separately, but this research should involve both concepts of security and economics together to covert and overt the economics issues surrounding security. Furthermore, the authors wanted to focus on identifying trends that it was important to include publications that are well published and are available for a long enough time that have focused on economics of security.
Phase 2 made analyzing of the reports and papers that were issued by GameSec conference, WEIS workshop, and SANS institute. The significant reason for including WEIS and SANS is that they have delivered to the security community in a large for many years. In addition, they have extensive research archives; also, their publications cover both aspects of security and economics. Furthermore, GameSec conference and WEIS present a lot of models and theories that to brighten the economics of security issues for interested parties.

3.1.1 Limitation of Study

3.1.1.1 Phase 1. On reflection, when we limited the work on the main journals and conferences find out that they are not responsive completely to all security trends and issues as our point of view. However, the publications publish several times in a year and have a long-term trend to broad economics of security as knowledge, but to a certain extent reflect the latest development in economics of security field. Although, these journals may not represent the whole spectrum of economics of security's publications. But to overcome this issue we review all breakthroughs in this area in section 3.2. The Authors believe that assessing them may provide valuable insight into the current trends of economics of security. In the discussion part, we analyze and consider all publications and reports to reflect the holistic trend in economics of security for achieving a comprehensive insight. Further, in economics of security field a lot of papers can be found that propose an economical model to mitigate the cost of security. Economic of security includes a lot of cost functions to forecast the expenses associated with production to determine what pricing strategies should be

used for achieving desired profit margins. The profit can be a difference between revenue and costs that both of them can be monetary and psychological. Since, it is hard to measure or quantify psychological benefits and costs, we just focus on the monetary aspect of the analysis that caused to limit the obtained articles.

3.1.1.2. Phase 2. The SANS, WEIS and GameSec conferences reflected the current economics of security trend, but the difference between these three publications and three journals in the list is the number of published papers. According to our findings, these three publications especially WEIS and GameSec conference publish lots of papers at each workshop and present novel models and theories in economics of security. This short-term trend caused to highlight them as a good and reliable source of research in economics of security field.
An existing problem surrounding economics of security is the lack of complete information and news in this field. Also, security researchers do not report all of their findings and breakthrough about security breaches in fear of the consequences of legal liability, and users misuse that is one of the most striking features of this problem. In addition, the hackers do not reveal their successful attack methods because they are afraid to be sued. Another complication is that someone sets out to debunk the scaremongering around an online crime that governments and defense contractors are using to enhance the security in cyberspace. Therefore, finding a real and comprehensive picture of security for launching a new area of research about economics of security is hard and complicated. Hence, it would be very difficult to get a comprehensive view of the current state of economics issues surrounding the security based on the results of such publications.

3.1.2 Data Collection

This section investigates the economics of security issues and models found in the Decision Support Systems Conference Series, IEEE Transactions on Information Forensics and Security, Telecommunications Policy, GameSec conference series, Workshop on the Economics of Information Security (WEIS), and SANS for the period of January 2008 till January 2015. The found resources are searched in well-known and reliable indexing services like IEEE, ACM, Springer, Scopus, Science Direct, DOAJ and some workshops and institutes like WEIS, SANS and GameSec conference to find the most reliable and credible publications in economics of security.
At first, we searched the papers based on the keywords containing both concepts of economics and digital security from 2008 to 2015, and then we broaden it by searching other related keywords to find related results in the field of economics of security. For example, instead of economics we searched with keywords like business, investment, and price and cost separately. Also, we did this method with the substituted keywords instead of security like privacy, risk management, trust, hack, cyber-attacks, digital forensic and penetration testing. We obtained set of papers from our searching by merging all of these keywords and gathering all of them that reached to more than 1200 papers.
Afterwards, we refined and separated related papers. In this phase, after a quick review of the papers to identify whether they are related we obtained the list of related papers that prepares the link between economics and cyber security. Among all of the found papers on economics of security, just 300 of them remained as most related papers for the next phase of our study. Afterward, we applied a new refinement by separating the journals and publications that have been repeated more than three times for the assessment and analysis phase. Applying this refinement and threshold helped us to find the latest reliable publications that focus strongly on economics of security.

3.1.2.1Topics covered in journals (phase 1). The data collection process began with a brainstorming session where all sorts of economics of security topics identified and subsequently merged the related topics together in appropriate groups. For example, every topic that related to economics of malicious programs and all types of malwares like virus, worm and adware, botnet and DDoS attacks categorized as malicious program and malware. The topics that cover economics of network security like wired, wireless, Ad-Hoc, mobile networks were grouped in network security. The topics that dealt with economics of security investment, risk management, security policies and metrics, assurance, and anything pertains to investment of security were categorized as of information security investment. Concerning the articles related to economic issues surrounding the penetration testing, digital forensics and security vulnerabilities merged into one group called penetration testing and digital forensics. Furthermore, we categorized the papers regarding the economic issues in software security and economic models for developing software in the field of software security. Finally, issues associated with economic aspects of trust and privacy is categorized as trust and privacy field as depicted in Table 1.

3.1.2.2. Results obtained from journals
This subsection outlines the profile of articles published in all obtained journals during the January 2008 till January 2015. During the investigation of each publication source, it is interesting to note that in some cases, special topics and fields emphasized by some journals. We can figure out that these publications have concentrated more on specific topics and issues than others. Table 1 lists the six

topics in each publication in economics of security. These topics involved the economics of security field that identified after reading the related papers and deciding about the scope and category that each paper may belong to it.
Outstanding in the results of IEEE Transactions on Information Forensics and Security is that this journal focused mainly on network security field by 3 published papers in this field.
Telecommunications policy journal contains 3 papers, by 2 papers in network security and one at policies, assurance, and investment among our obtained list.
Lastly, in the decision support systems by 2 published paper in security investment that followed by malicious program and malware that are tied to software and application development at one.

3.1.3 Surveys of SANS Institute, WEIS and GameSec Conferences (Phase 2)

In this subsection, we considered three well-established publications that give the best shot to the current trend in economics of security. WEIS and GameSec conferences contain mathematical models, theories and games for economics of security that Table 1 summarizes the amount of coverage given to each topic by all publications included in this survey. As shown in Table 1, most of published papers in economics of security are belonging to WEIS conference. The significant results in WEIS papers indicates to the field of information security investment that took the lead at 35, followed by trust and privacy at 26, malicious program and malware at 12 to constitute the top three fields. The published papers in SANS tend to security investment that shows giving a top priority in this field by 3 papers in this field.
Also, in the GameSec conference researchers concentrate on network security among other fields with 7 articles followed by trust and privacy field and penetration testing and digital forensics that are tied at four. Obtained information shows the significance of each field and primary focus of each publication on them.

3.2 Discussions and Analysis of Results

In this section, we compare and contrast obtained results from SANS, WEIS and GameSec conferences. In addition, we review the obtained journals and some of the other important works in this field.
The significance in this survey is that most papers published in WEIS and GameSec conference aim to develop an economical model for security. The striking issue that has been addressed is finding the most preferable and recommended tool for developing the model in this field. It is widely believed by researchers in economics of security field that one of the best-presented methods for developing a model is a game theory. The game theory prepares a mathematical framework for users to make a security investment decisions that has become a vital and undeniable suggested tool over the past decade. Studying game theory leads security researchers to be more familiar with the behavior of rational agents in a multi-player game. Game theory used for modeling interactions among users, risk recognition and risk prediction that significantly affected economics of security.
On reflection, according to our study the results of the survey show a strong emphasis on the six main fields in the economic issues surrounding security as follows:

- Information Security Investment
- Trust and Privacy
- Network Security
- Malicious Program and Malware
- Penetration Testing and Digital Forensics
- Software Security

In consonance with the results, we can figure out the major shift from pure technical aspect of security towards a more reactive strategic approach based on decision system and mathematical analysis and security. The results also indicate that security responsibility is broadening to get involved the risk managers, econometrists, forensic specialists and psychologists.
Furthermore, the study reveals that the WEIS conferences and SANS focused mainly on information security investment issues in comparison with the GameSec conferences that paid attention to network security issues which is ranked first in this conference.
In this section, we review and discuss all these six fields as follow:

A. Information Security Investment

Decision about information security investment has recently attracted the attention of researchers from computer science, economics and management science. Investment of security was considered as an essential component of risk management among security experts and decision makers in the IT based organizations [20].
Analyzing the Return on Security Investment (ROSI) has always been a sticking point for technology investments due to the immense growth of e-business. On this matter, [21] proposed a comprehensive analytical model to investigate and analyze some security investment decisions that leads to find an appropriate model and framework for ROSI.
In previous works in economics of security using the microeconomics and economical model for information security has been very prevailing. Researchers in this field put their efforts mostly on proposing an economic model for security investment or enhancing the fringe benefits of information security. To narrow down the concept of economics of IT security [22] tried to get a holistic picture

of this topic. They got involved in recognizing the obstacles that users are facing during the quantifying the cost of security.

In this regard, [23] proposed a non-cooperative game based on the game theory that tries to analyze individual user's security in the network. They investigated the correlation among network members and their security investment to analyze the equilibrium attitude of members. In this model, the monotonic symmetric Bayesian Nash equilibrium of efforts are existed that help to deal with information uncertainty in the proposing the model. This model prepares an applicable and beneficial perspective of the Internet members on investing in security to enhance financial and security aspects of the system. The authors clarified how they can apply the model to combine risk management issues and security. Simultaneously, [24] addressed the issues regarding risk management decision by means of utility theory and concentrated mainly on the decision to defer costly deterministic investments. They considered the investment function with irreversible fixed costs that introduce rigidity into the investment decision-making profile. They solved the problem of optimal timing of security investments in possible risks of attackers. The significant possible application of this result can be cloud computing for being useful in order to mitigate the amount of capital (fixed) investment. They also described the usefulness and applicable approaches for managing the security of users and modifying the investment and business approaches in the environment [25].

Apropos of the information security investment, Gordon et al. presented an economic model of Gordon-Loeb[5] that defines the optimal amount of investment to protect a given set of information that mitigates the information technology risks. [5] tried to find out the procedure for decreasing the risk. They addressed the issue of rational investment in the security of information technology. The model has a general perspective and does not consider specific aspects of IT risks and the way to avoid such risks. This model assumes that the properties in IT risks might be controlled, because such properties are essential to develop the investment model for security risk. Gordon and Loeb formulate a basic economic model and argued that the best investment strategy for a defender can be protecting the mid-range of vulnerabilities by both the risk profiles of vulnerabilities and the cost to protect them. This model attracted significant attention of both IT practitioners and economists. The original research claims that the optimal investment level never exceeds 1=e-th fraction of the value at risk. The model considers the vulnerability of the information to a security breach and the potential loss occur. Gordon-Loeb model illustrates that for a given possible loss, a firm should not essentially concentrate on its investments on information sets with the highest vulnerability. Since, extremely vulnerable information sets may be inordinately expensive to protect, a firm may be better off focus its efforts on information sets with midrange vulnerabilities. The analysis further suggests that to maximize the expected profit from investment the firm should expend only a small fraction of the probable loss because of a security breach to protect information.

Gordon-Loeb model offers two parameters for a single agent as follows:

Potential monetary loss (l) and probability of security breach without additional security (v): Agent can invest x to reduce the probability of loss to: $(x, v) \leq v$. The optimal investment also can be figured by this formula: $\emptyset(v, l) = \arg\min\{lp(x, v) + x, x \geq 0\}$. In addition, the security breach probability functions can be found as follows: $(x, v) = v^{\alpha x+1}$ for $\alpha > 0$, that α measure of the productivity of security.

In the case of monotone investment if $\frac{\partial_p}{\partial_x}(\mathrm{x}, \mathrm{v}) \leq 0$ and $\frac{\partial^2 p}{\partial_x \partial_v}(\mathrm{x}, \mathrm{v}) \leq 0$, then $\emptyset$ (v, l) is non-decreasing and is augmenting return of investment with vulnerability as follows:

$v^H > v^L \mid \frac{\partial_p}{\partial_x}(\mathrm{x}, v^H)| \geq |\frac{\partial_p}{\partial_x}(\mathrm{x}, v^L)|$.

Gordon and Loeb proposed 1/e rule that claims if the function $p(x, v)$ is log-convex in x then the optimal security investment is bounded by:

$\frac{lv}{e}$, i.e. $\frac{1}{e} \approx 37\%$ of the expected loss.

In this regard, Willemson [26] disputed that the result is false in the full generality of GL model. He studied the information security investment model. He argued that the original model is missing at least one important restriction concerning a monotonicity of the remaining vulnerability viewed as a function of original vulnerability level, and proposed adding the respective condition. Willemson presented a new family of remaining vulnerability functions satisfying all the conditions and generalizing all the currently known example function families.

In this regard,[27] have found the idea that insurance is a powerful incentive mechanism which pushes agents to invest in self-protection. Therefore, insurance increases the level of self-protection, and the level of security, in the Internet in the real hazard situation. Then, they considered the economic agent concepts for spreading of the risks and developed a model for spreading of risks without insurance for agents. In this model agents use the classical expected utility model by supposing the rationality and risk aversion of users. This may motivate the decision maker to bear the risk for maximizing some preferences function for evaluating the level of his satisfaction.

Regarding the indicated risks posed to the information in cyberspace [28] proposed an ontological account of information security architectures. That originated from an economic model of trade-offs between confidentiality,

integrity and availability of security issues by using mathematical models. The proposed model has the capability to prepare a methodology for determining investment of security. This model also focused on illustrating the security architecture and separates its components and found out that the way for modifying the structure and framework of information system. Beautement and Pym considered the main issues regarding using the security policies and management tools to manage and provide a better security investment decision like tools that guide the organizations to mitigate the risk and enhance the trust and privacy. They also found out that the economic viability of the metric and configuration management tools were used just like a sample.

The main concentration of IT security and risk management is based on developing models and solvable ways to enhance the security and mitigate the economic loss in marketing and cyberspace. The security implementation and model development deal with a lot of obstacles and different conditions in marketing to develop an efficient business model. One of the best business models in the scope of risk management is BORIS that introduced by [29] and includes four layers to manage and control the information security. The defined methods follow systematically the chain from business goals including compliance requirements to information security measures. They asserted that as the first requirement for developing the framework, it should be implemented to activate the linkage between security and business. Another requirement indicates that it should be responsible to manage the challenges and problems that information security management deal with it for providing a better performance of IT management and privacy. The framework also should contain a method for evaluation for being used for the task of optimizing the economic and strategic performance of the overall information security infrastructure. Then they tried to recognize the gaps in information security to fill up them by using microeconomics model and claimed that BORIS model can defeat the problems and obstacle that faced with the security management. This argument guides to get a new picture of business goals and financial balance of security.

According to an [30], the world nowadays is faced with a dramatic increase of demand and using internet that cause users posed to a lot of risks by attackers on the internet. This issue inclined researchers to focus on the control and mitigate the security risks in cyberspace to reduce the vulnerabilities. Notwithstanding the research efforts in this field, the proposed methods (such as antivirus, IDS, firewall, honey pot, etc.) just mitigate the real hazard and do not eliminate the risks completely.

With respect to this matter, [31] raised the question that how to manage the risk in cyberspace? They consider the effects of externalities on security investment of users by using a model that merges novel approaches of risk theory and network modeling. They figured out that using insurance would enhance the IT security. Moreover, security insurance is an essential component of risk management to be risk averse for the users. One of the significant results of their model is providing a convenient way to formulate the problem of deploying insurance on the Internet. They provided a methodology to evaluate the impact of insurance and design appropriate insurance policies and algorithms. The network algorithms and network architecture might be designed or re-evaluated according to their ability to implement desirable economic policies (such as the deployment of insurance) for achieving desirable economic goals.

Afterward, Rainer presented an Iterated Weakest Link (IWL) model [32] that is one of the best economic models about dynamic security investment. IWL describes the reason and situation of being rational in a decision based security systems under investment. Also, it shows the correlation between attacker and defender, but was not affected by other market members like a market failure theory. It rather complements the picture of market failure; however, it illustrations that market failure theory is sufficient, but not necessary model for security under investment. Thus, putting more effort on developing another models and theories by analyzing security investment can be efficient.

About analyzing the effects of insurance on network security and security investment, [33] proposed a new economic model based on analyzing phase for cyber security users. This model shows that the probability and risk of damages originated by the external or internal vulnerabilities and depends on both the user security and the network security. The model focuses on the reasons for combining the network externalities and information asymmetry that caused to miss a market for cyber insurance. Hence, the authors decided to consider the effects of information asymmetries in the network externalities and investigated the obtained results. They develop a model by using different market equilibrium like a model of [34] who pioneered examination of equilibria with information asymmetries in the insurance markets area.

Another model in investment of security belonging to [35] that it was a little different from the previous model in security investment. They proposed a model by using a one-shot game with a market insurance to find a Nash Equilibrium and explained the equilibria procedures. The essential part of security games is participating the players to propose a best multi player game. Johnson et al. proposed a game that defenders customize the game conditions to defend against damages of attacks by effectual strategic decisions. They presented some variations of the price of uncertainty metric to develop

their model, also differentiated between a payoff-ratio and cost-ratio metric. Their work fills up some gaps in the scope of security investment and security measurement that are commonly based on technology, finance [36] and marketing [37].

B. Economics of Trust, Privacy

The economics of trust and privacy is an elusive and value-laden with a complex issue and has attracted researchers' attention recently. The advent of low-cost technology for manipulating and communicating information has raised significant concerns about personal privacy [38, 39].

Economics of privacy issues has faced with various kinds of flaws associated the policy that raised the question of how privacy can be compatible with economic prosperity in the network. Establishing the trust and privacy in the network affected the private information of users. Networks without privacy imposed negative effects on users and causes a tension between security and trust in computer networks for users. The users should consider their tradeoff and evaluate their privacy for investigating the different strategies to set their privacy preferences at a fix level in their network. Using a game theoretic and economic model also leads to finding the best user's tradeoff and help users to decide whether they want to participate in privacy-preserving mechanisms.

Regarding the economics of privacy, [40] explained the empirical evidence based on the common economic theory in the market. They discerned that verifying the model help to achieve a prediction for improving economics of privacy in the marketing. They figured out that the variety of data collection depends on the price and market structures (in line with the predictions that economic theory makes) and the co-occurrence of more privacy and lower prices. The economics of privacy comes as a surprise and mandates further study that leads to propose an implication for privacy in e-commerce. This implication applied on the browser standards and regulations to increase the privacy of commercial web site operators based on empirical research in the economics of trust and privacy [41].

One of the controversial issues in economics of privacy is control of user's authorization that helps users to enhance their privacy and mitigate related cost to establish privacy. However, some obstacle in the users' authorization and their accessibilities area may occur that affected the privacy and need to be solved. In this regard, [42] worked on the authorization in cyberspace to link this matter to users privacy. They said that users and costumers would like to interact with websites and surfing on the Internet without hindrance; whereas, they are expecting to keep controlling on their private information and security. These issues bring forth a situation which one party in a transaction has more or superior information compared to another that called asymmetric information. Nevertheless, the existence of asymmetric information in a cyber space causes a harmful situation because one party may take advantage of the other party's lack of knowledge. They analyzed the situation by checking privacy of websites to find whether web sites will sell private information based on asymmetric information. They followed the "lemons market" theory by [4] for developing their model.

Akerlof introduced the lemons market theory as a good example for comparing the cyber space to a lemon market. In this model, sellers present "peach or lemon" car to buyers who cannot tell which one is which. The consumer pays only what they would pay for a lemon that no peach cars are sold.

According to [42] assertion the privacy in web sites is similar to the lemons market in the cyber world and costumer chooses among web sites like choosing lemon among the market. But this expectation that all web sites should be safe and respect to their privacy rules are inconceivable. Accordingly, Pitofsky et al. made this more formal for developing a model in the context of websites as follows: Suppose websites fall into two groups: Respecting (R) sites that do not sell private information and Defecting (D) sites that do sell such information as shown in Table 2. A customer may choose to buy or not buy with a site. If the customer buys from a Respecting site, it gains B. If it buys from a Defecting site, it obtains $B - V$, where V is the cost to the customer of a privacy violation. The resulting payoff matrix is shown in Table 2.

The privacy declined largely in order to facilitate differential pricing, which offers greater social and economic gains than auctions or shopping agents that enhances the risk of privacy breach. The significant drawbacks of privacy breach and trust is imposing an economic constraints on e-commerce [43].

A variety of strategies to enhance the trust in e-commerce have been developed that [44] discussed some of these strategies and frameworks in e-commerce and other online transactions. They also pointed out that the economic consequences of information sharing for all parties involved (the data subject and the actual or potential data holders) could be welfare enhancing or diminishing. Their examination concentrated on the economic trade-offs related to consumer's data sharing and protection to solve the privacy problems in cyberspace.

Similarly, model by [45] reveals that the rational economic agents may end up inefficiently over-investing in assembling personal information; for example, he increased the private revenues from sales based on knowledge of the buyer's willingness to pay. The technology that helps in this situation is Privacy Enhancing Technologies (PTEs). PET is any technology

like computer tools, applications and mechanisms which allow online users to protect and enhance the privacy that recently has become a fad among researchers in economics of security field [46].
PTE enhances the possibility to reach equilibria while subjects' individual information is protected and data owners have the ability to analyze collected data. In addition, the probability that privacy enhancing technologies may lead to non-zero sum market outcomes recently has started being addressed in economic research: the usage of PET may permit certain personal information to be shared while other is protected, with common satisfaction of both data subject and data holder [47].

C. Economics of Network Security

Economics of network security has aroused a recent interest in economics game to approach the security investment, security insurance and security asset protection in the network.
An authoritative report by [48]about the current research on the network security shows that most significant reality that should be considered by organizations are the threats faced by computer systems and networks. This kind of threats is increasing and need too much attention to avoid economic losses that caused by these threats. Network security problems are often challenging because of growing complexity and interconnected nature of IT systems [49]. For enhancing the network security and develop economic models users should overcome the risk in cyberspace to present an economic model. In this regard, game theoretical models can be proposed to enhance the security and extend a scientific basis for decision-based strategies of game theory that deals with the network security obstacles. In such security models, the agents or decision makers play the role of either the attacker or the defender when the network faced with obstacles.
Regarding the economics of network [50] presented an economic model for avoiding vulnerabilities and the cost of loss in the Supply-Demand (S-D) network. They described the decision making process by users for developing a model when sophisticated attackers target the network for creating undesirable situation. They convinced that using Nash Equilibrium caused to mitigate the risk and vulnerabilities and make decision for avoiding these kinds of vulnerabilities in the network. They analyzed vulnerabilities in the network by the game theory framework based on Supply-Demand model. After vulnerability analyzing, they developed a conceptual game between a network manager/operator (defender) and a strategic attacker. Network managers are supposed to provide a guarantee against possible damage or loss in the network. This is possible by choosing a feasible flow and the adversary attempt to disrupt the flow by attacking a link. They customized game for 2 players by means of Nash payoff to estimate the vulnerabilities.
Subsequently, they proposed a novel model to mitigate and estimate the possible risk of vulnerability by putting efforts on a game theoretic framework for network. This model developed by using an assessment of the price of security to get a grip solution for the game between attacker and defender. This is done by using the metric of obtained assessment that originated from vulnerability/cost of security tradeoff. In the Supply-Demand network, they use a result of blocking games to develop a framework for analyzing security vulnerability/cost tradeoff. They used the game theoretic approach to find the attack metric in the S-D network that it becomes a means to calculate and compromise the price of vulnerability. This model highlights the importance of strategic decisions for defenders in order to manage and control their interaction in cyberspace.
Regarding the strategies that applied to control and manage the interaction among network nodes, [51] developed a model by using zero-sum game Nash equilibria. They claimed that in the case of attackers target and under each circumstance has always existed Nash Equilibrium in the set of link. Thus, they started to customize the design of network subsets to resist against attackers.
The network chooses its own data protection for the users among existing security solutions that are provided with a different performance and price levels. Some analysts [52] developed a model about relation among users that used a non-cooperative game based on increasing the expected gain by attack. They proved that the model has a unique equilibrium for a user that can estimate the cost of anarchy. Their investigation on network nodes has shown that security providers caused to remain the cost of anarchy at a low level. Moreover, the security providers believe that a long-term interaction of contest might be affected by the price war condition, that need to enhance a control of security issues.
It is commonly accepted that using collaboration for optimal performance and control of security issues can be performed better than a contest in the network. On this matter, [53] has developed a game theoretic model based on cooperation to avoid the network vulnerability and risk. He claimed that the success of cooperative security attempts is affected by nature of risk, identifying and scrutinizing the attacks and defenders reaction. He proposed the model by using the previous models of security attacks [54, 55] that reflects the economic perspectives of network users. This model is using for achieving the security by customizing a weakest-link game, total effort game and best-shot game according to players' behavior. The model shows that cooperation in the security is essential, but it is so difficult when the network size would be larger. However, the existence of

incentive-based schemes in large peer-to-peer networks shows that large-scale cooperative investments are possible if suitable incentives are provided to users.

Afterward, regarding cooperative investment in network security, [56] put their efforts on this issue. They planned to investigate the overheads that could arise in coalition formation when network users attempt to invest cooperatively in security. In order to get a better understanding of the cooperative behavior of network users, they applied a solution concept of recursive core to security games.

One of the commonly proposed ways to protect location privacy and solve some of existing problems is implies that the mobile nodes in the network need to modify the current pseudonyms in the place that called mix zones [57, 58]. As displayed in Figure 1 the nodes in the network can modify their identifiers at the mix zone the situation with 2-node mix zone. The adversary becomes confused about whether the green existing node was blue or red before entering the mix zone. The authors by using game theory identified the non-cooperative characteristic of mobile nodes and lead them to maximize their location privacy at a minimum cost.

Narasimhan et al. followed a theory by [57] that proposed a model to capture the evolution of location privacy for the mix zone and mobile node. Their model investigates these issues as follows:

- The users opinion about tracking power of the adversaries
- The amount of anonymity that users acquire in the mix-zones
- The price and the time of modifying pseudonyms

This strategic model is mainly used when the players in the network are mobile nodes. The authors also developed an n-player complete information game for finding the Nash equilibria to show that pseudonyms modifying is possible when it would be required. They also asserted that all defection strategy profile equilibrium and equilibrium with cooperation do not always exist as payoffs in the n-player. This is obvious that by enhancing investment in the network security the individual security improves rapidly that can be optimal by using the games with positive externalities.

D. Economics of Penetration Testing and Digital Forensic

Digital forensic investigation involves a series of processes on digital evidence such as identification, preservation, analysis and presentation based on the digital traces that has a discrete nature [59]. The economics of digital forensics and penetration testing can be considered as important issues that concentrate on digital traces in a cost-effective manner [60, 61].

Digital forensics is an essential tool for finding solutions surrounding cybercrimes (e.g. phishing and bank fraud), and likewise leads to find a solution for crimes against people where evidence may exist on the computer (e.g. money laundering and child exploitation). Forensic tools have also become a critical tool for information assurance due to the capability of recovering the evidence left by cyber-attacks. The research based on DF can concurrently make a lower development costs and enhance the quality of research attempts. This can be done with a meticulous planning and attention to cooperation, standardization, and shared implementation. This is probably one of the few techniques at our disposal for surviving the coming crisis in digital forensics.

In 2012 regarding the attackers strategic decision [62] used an agent-based simulation in a simple network security game. In their model hacker tries to use agent-based simulation in a simple network to maximize the amount of consequences of attack and damage that he/she is planning for them. However, a defender attempt is mitigating the possible damage and loss caused by the attacker. During the simulation phase they approached a Nash Equilibrium strategy for the attacker and defender side that contain a variety of cost conditions. They informed network administrators about attacker behaviors to mitigate the possible loss and cost that imposed by criminal attacks.

In the matter of economics ways to avoid the attacks, stone Gross et al. [63] presented an in-depth study of how the fake antivirus software is implemented and handled. Their idea was unique and based on the information contained on a number of key servers that were part of the attacker's infrastructure. They also leveraged to obtain data for developing an economic model about hacker's performance. The model illustrates the attackers performance in a cyberspace that how they should act to refund and charge back. This helps to retain a balanced financial posture that does not directly explicit their criminal entity. However, the economic model outlines the operations procedures for identifying the behaviors that lead to differentiate these criminal attempts from a legitimate economic procedure. In addition, when these attacks posed to the users using the attack-tree model help to be familiar with the attacker's decisions. Attack-trees lead to visualize possible attacks as Boolean combinations of atomic attacks and combat attack-related parameters such as cost, success probability and likelihood.

Concerning the attack-tree model [64] presented some economic algorithms and models about several attacks namely: Iterated AND/OR Rules Algorithm, DNF with Cost-Reduction Algorithm, Exact Utility in the Infinite Repetition Model Algorithm, also developed the Infinite Repetition Model. A first algorithm uses the AND-rule and the OR-rule at every node of the attack-tree. In order to make the OR-rule work in the general case, cost-

reduction is used. The cost of every atomic attack reduces at every OR-node of the attack-tree. The cost-reduction step starts from the root vertex and ends in the root vertices.

F =(X ∧ X 1) ∨ (X ∧ X 2) ∨ (((X ∧ X 3) ∨ (X ∧ X 4)) ∧ X) 5

For example, in case we have an attack-tree with a Boolean formula which is depicted in Figure 2 (left), the cost c of the atomic attack X must be used in two places: (1) in the root node we divide the cost by 3 and (2) in the sub-tree (X ∧ X 3) ∨ (X ∧ X 4).

We should divide the cost again by 2, and hence, the cost c of X reduces to c/6 in this sub-tree while in the sub-trees X ∧ X 1 and X ∧ X2 it reduces to c/3.

After the costs of all atomic attacks are decreased in this way, we apply the AND, OR negativity rules starting from the leaves of the tree (the atomic attacks) and ending with the root vertex.

Regarding the attacks and its consequences, [65] investigated the enormous gap between the potential and actual harm. They presented a solution for the weakest-link analyses may be unable to present an interpretation because it lies in a shortcoming of common threat models. The significant result is that crowd of users present a sum-of-effort rather than a weakest-link defense. Many attacks succeed in particular scenarios but it is not supposed to be responsible and lucrative when applied for the larger population. Thus, the developed model should be able to fill the gap between the potential and actual risk appropriately. They also asserted that the financial entity of attack indicates that attackers prefer to withdraw the attack when the attack seems not be profitable by the attacker's prediction. This shows that hackers prefer using the sum-of-effort rather than a weakest-link defense. They presume that while the costs are the main limitation on attacks, the risk of anticipation for cybercriminal can be disregarded.

Furthermore, in this section we briefly review the economics of penetration testing that it is a relevant tool for information security practitioners and deliberate search for potential vulnerabilities in a system by using the attack techniques [66].

Penetration testing is a method for evaluating computer and network security by simulating an attack on a computer system or network from existing risks that used for information gathering option and reducing the uncertainty in cyberspace. The penetration testing process involves analysis for investigating any possible vulnerability that leads to having a poor or improper system configuration. This analyzes is carried out from the position of a potential attacker and can include active exploitation of security vulnerabilities. Penetration testing is used for determining the possibility of a specific set of attack vectors, recognizing higher-risk vulnerabilities that may be difficult or unmanageable to identify with automated network or application vulnerability scanning software. Additionally, it can help to evaluate the extent of possible business and operational effects of successful attacks and test the ability of network defenders to successfully identify and respond to the attacks.

Penetration testing is comparable with ethical hacking because both of them analyze the target system from an attackers point of view and report the weaknesses instead of exploiting them [66]. The similarity between pentesting and attacks leads to the insight that the information exposed by pentests must be modeled in a same way like the information that exposed by attacks. There are differences on the cost side like a pentests cause calculable up-front costs, however the costs related with successful attacks are typically more unstable and higher.

E. Economics of Software Security

Software security concept has been considered as an arms race between attackers and defenders and become a critical trend of research in security and its economics. In cyberspace users are facing a risk posed by a critical flaw in software infrastructure that exerts negative effects on security. Also, it leads to enhance the attackers' tendency towards compromising information security infrastructure. In [67], authors compared the productivity of three software liability policies: supplier liability for damages, supplier liability for patching costs and imposed security standards by government. They asserted that supplier liability is not profitable for improving the social welfare in the short-run in the case of losses. While, liability for patching costs can be profitable if either patching costs are large or the likelihood of a zero-day attack is low, patching costs are small and zero-day likelihood is high. The zero-day attack possibility is at the highest point when user-patching costs are large. Accordingly, the patch liability is not efficient, but partial patch liability can boost supplier investment and improves welfare when patching costs are not large. In contrary, in environments with low zero-day attack likelihood, supplier's full patch liability can be optimized. These also show that government can help to both patching and loss liability of the supplier by imposing the standards on software security investment if the zero-day attack possibility is significantly low. However, if zero-day attacks are a common occurrence and patching costs are not at the highest point; partial patch liability can be the most efficient policy. They explored three separate liability mechanisms, namely zero-day loss liability, patch liability and security standards to derive policy development for software security liability in different classes of software and market environments.

In this matter the controversial topic in economics of software security that can be indicated is about software

security patching and incentives. In this regard, [68] considered the impact of user incentives on software security. This analyzing had been done in a network of individual users under a costly patching and negative network security externalities. They started with an accurate comparison about some alternative policies for better handling the network security. In the case of proprietary software, when software security faced with a risk and higher cost of patching a dominant strategy for both of the welfare-maximizing social planner and the profit-maximizing vender is applying the rebates for patching customers. For freeware usage tax is most effective policy, except when both patching costs and security risk is low. Optimal patching rebates and taxes tend to increase with an enhanced security attack and cost of patching; however, they have the ability to mitigate the security risk that considered as a high-risk level and affects the security cost.

Afterward, for mitigating a security cost [69] analyzed the economic phenomena that happen within the software market framework and affected a software security platform. He presented some economic solutions for problems that faced to business concerning with security. These phenomena include dilemma that arises from the situation, asymmetrical information and risks that confronted to both insurance company and two-sided markets. One of the suggested solutions about risk management that increased by enhancing the liability level is software insurance infrastructure cost. Another solution supported by software insurance is a technical signaling to deal with an information asymmetry. This signaling can take a form of self-imposed software packaging constraints, self-imposed application sandboxing, and the employment of a reputation system for applications that to some extent manage the existing risk.

Afterward, for managing the indicated risk [70] examined essential issues in real world regarding the software vulnerability disclosure. They contended that using the shared information help the clients to protect themselves against attacks that exploit those specific vulnerabilities. They investigated this obstacle by putting their efforts to identify and classify the behavior of software's users and their characteristics. This investigation involved the malign, benign or identifier users to consider their behavior for achieving economic benefit.

F. Economics of Malicious Program and Malware

Nowadays, Botnet herders and attackers have become an increasing security concern in cyber space. The organized cybercrime, state-sponsored hackers, and cyber espionage can pose security risks to users while the risks mostly stems from online threats and malicious attack. Malicious attacks and its incentives become a controversial concern in economics of security field that allocates a new line of thinking for observant users to avoid or mitigate the risk of malware.

In the last few years, the cyber space encountered with a dramatic growth in the number and variety of malware. Moreover, the shift of malware motivation from showing off their skills, web vandalism and defacement and DDoS attack to economical gaining is remarkable. These issues caused to shift the research nature of malware towards study of the previous economic models of security to propose a novel model in economics of malware.

As remarked by [71] many factors exist that are affecting the characteristics of the attackers in cyberspace that lead researchers to study more on it and propose a lot of models and theories on malicious behavior. They proposed a formula for familiarity of users with malicious attacks and behavior. Familiarity with following factors of formula leads to be familiar with a proposed model. Value V ($), Number N, Interconnection I (number of nodes directly reachable), Difficulty D (# of people who know how to do it), Expense E ($), Time T (time to hack), Likelihood L (Chance of getting caught), Penalty P (fine and/or jail). Factors help economist, government and users to conceive the models and implications better. About malware probability they remarked that as the combined attractiveness of computers and networks increases the likelihood of an exploit rise, also enhancing the cost and risk caused to reduce the likelihood of an exploit that can be shown as follows:

$$M\ \mu = \frac{Vm * Nm * Im}{(Dm + Em + Tm) * (Lm * Pm)}$$

According to this risk model, governments and firms will be informed about risk management in the case of facing with attacks by investigating the effects of malicious attacks and economic loss of it.

In this regard, [72] tried to develop an economical model for investigating effects of malicious attack and analyzing the cost of such threats that take place by malware attacks. The proposed model helps users to make a better decision about all required components for recovery of lost data, estimate the cost of threats and the likelihood of attack propagation.

Most of the users overlook possible damage that caused by stealth malware like email-attachments, freeware/shareware, spyware, sniffer, rootkit, popups, and peer-to-peer fileshares. For solving this issue, Kondakci started to work on malwares and their effects on the economic lost by discussing two sets of functions. These functions used to explain the spread of attacks and potential damage may happen due to the existence of malware. Check the evolutionary functions of infection procedure and the loss functions provide a risk-impact analysis of failed systems. Thus, users need to be cautious about this malware attack and analysis its risks and consequences.

The application and software variety caused that such analyses drawn the attention of many network users. Epidemic of malware investigation is related to analysis of system performance, economic loss, and threats. Also, this investigation indicated that for mitigating a risk of malware attack the users should become more familiar with the attackers and defenders strategies to countermeasure against malwares damage.

Regarding the strategies that can be applied to counter and offset against the malwares damage, [73] presented some strategies and implications for anti-phishing and claimed that their game is applicable to web security problems in the most cases by default. Their theoretical proposed model lead researchers and policy makers to analyze and learn different ways of defense against phishing. The model also used for an anti-phishing industry and implemented based on CBP game [74]that one of the well-known models to countermeasure against phishing. Colonel Blotto game (CBP) is an old but interesting game, which has mainly overlooked because of its complication. Blotto games constitute a class of two-person zero-sum games which players are tasked to distribute simultaneously limited resources over several objects (or battlefields). In the classic version of the game, the player devoting the most resources to a battlefield wins that battlefield, and the gain (or payoff) is then equal to the total number of battlefields won. The Colonel Blotto game is an example of a game in which the psychology of the players' matters and leads to better comprehension about the dynamics of the two-step detect-and-takedown defense against phishing threats. Colonel Blotto game helps to give a complete characterization of two-player asymmetric to unique equilibrium payoffs and used for mapping the phishing obstacles. The game is mainly applicable for capturing resource allocation obstacle among a phisher and defender with asymmetrical resources.

Surrounding the malware and malicious attacks, a lot of strategies exist that help to develop an economic theory for avoiding the drawbacks of botnet in a cyberspace. In addition, these strategies lead security researchers to prepare a holistic game theoretical model that show and predict the interaction among botnet herder and defender group (network/computer users). In this regard,[75] proposed a framework and stated that the botnet herder's goal is intensifying his intrusion in a network of computers for pursuing economic profits; whereas, the defender group' goal is defending the botnet herder's intrusion. The percentage of infected computers in the network changes according to a modified SIS (susceptible-infectious-susceptible) epidemic model. In addition, Bensoussan et al. found out two possible closed-loops Nash Equilibrium to solve the differential game concerning using the differential game model. They asserted that these Nash equilibria solutions are related to the productivity of defense strategies and the control strategy switching, specified as rates of infection. The two Nash equilibria are either (1) the defender group defends at the maximum level while the botnet herder exerts an intermediate constant intensity attack effort or (2) the defender group applies an intermediate constant intensity defense effort while the botnet herder attacks at a full power to mitigate the effects of externalities and avoid from extra expending on security.

In this regard, [76] proposed a model based on investment of security to measure the effects of network externalities like malware in a cyberspace. They investigated network agent's behaviors that are the main reason for originating the risk of malware and its propagation. Each agent is permitted to be autonomous about choosing the situation between being protected or not protected. Agent achieves to this permission by investing on security and offering some security solutions that mitigates the likelihood of damage in the case of infection. They used random graph theory idea to solve the micro model and compute the fulfilled expectations equilibria explicitly. In this game, the situation is similar to free-rider problem [77] that agents follow the rule of security for achieving high level of protection that lead them to offset and countermeasure against attackers decision. While, in the case of weaker protection network can exhibit critical mass that caused significant drawbacks for agents in the lack of strong protection status.

They have also developed a model for epidemic risks as introduced in [78, 79] where agents are strategic players and have a capability to choose whether to be protected or not. On their model: if they are determined about investing in self-protection, the agents stay in S (as in Safe or Secure); otherwise, they stay in state N (Not safe). If the agents do not invest, their probability of loss is pN. If they do not invest, for an amount which we assume is a fixed amount c, then their loss probability is mitigating and equal to pS<pN.

In state N, the expected last wealth of the agents is pN (w − ℓ) + (1 − pN) w, where w is their initial wealth and ℓ is the size of the possible loss; in state S, the expected last wealth is pS (w − ℓ − c) + (1 − pS) (w − c). Hence, the optimal strategy is for the agents to invest in self-protection only if the cost for self-protection is less than the threshold:

$$C < (pN - pS)\ell$$

In order to make a decision, the agents should evaluate pN and pS. Making a decision about staying in the self-protection status or not changes the infection risk possibility and consecutively changes the dynamic of propagation on the graph. The model analyzes the network externalities function that is found in the macro model. Lelarge et al. also proposed a model according to finding that has been optimized in [27, 31, 80] to incorporate feasible cyber insurance. In a situation where

the protection is strong and ensures that the agent with self-protection does not face with the risk of attackers the authors try to compare this situation with a free-rider problem in cyberspace.

In security game, the players make their decisions independently and each one seeks unilaterally the maximum possible gain by possible rational choices of the other players. A special case, called Max-Min (or Min-Max) in game theory, is when each player unilaterally maximizes his gain when the other players minimize simultaneously their losses (or maximize their own specific gains). Another equilibrium type is Nash, where no player unilaterally can win by moving away from the equilibrium if it exists. In [81], it is assumed that the attacks are on one target at the time; a certain amount of effort is put progressively, with increasing and convex costs, but attacker only achieves a probability of success in yielding a reward. The attacker will seek to maximize the actual reward, but has to decide as a strategy on an optimal stopping rule by computing the expected gain of carrying on with the attack and carrying the costs. Also, the models that pertain to economics of security [81] gives some results assuming an explicit form $(1-\exp(-t/\alpha))$ for the probability of success with time t, and an explicit linearly increasing cost with time. It also considers the case of switching costs in changing target, if the expected benefit of going on with the current target gets below the expected benefit from the new target. Assuming the attacker realizes the security level of target after switching to it, he will pay both switching cost and higher penetration cost. This implies that the target should apply in cycles increasing security levels to deter the attackers. The target may also claim that the used system is highly secure, thus the attacker does not know whether the target has a high or low security level. The attacker is forced to apply Bayesian inference, and it is shown that low security targets are better off hiding the fact that they are low- security, and high security targets should advertise that they are highly secure.

In contrary with the defense game, [82] developed a game for malicious attack based on a non-detection "cat-and-mouse" case as a Nash Equilibrium game, with malicious packets hiding within the normal flow. These packets are sent by an attacker that is trying not to be detected when the defender is active. The attacker must select a path, such as a highly loaded link to send his malicious packet for minimizing the detection probability. The defender must select the links to scan for maximizing the detection. In [83] the reverse is studied in a similar way, in that way the defender wants to send some flow through a network with vulnerable links subject to attacks. In addition,

3.3 Critical Overlooked Security Issues

On reflection, as survey results point out some overlooked issues surrounding economics of security field. In this regard, we have conceived that a little research has been done in the field of economics of software security; likewise, in the field of penetration testing and digital forensic. Also, most of the articles surrounding the economics of forensic are related to physical forensic that does not cover the digital forensics appropriately.

In addition, security inefficiencies pose some critical risks to privacy that enhances the financial burden of security. However, by occurring security break the significant downtime of systems or the loss of data enhanced, but paying more attention to this issue helps to mitigate the security and privacy risks.

Another significant dismiss is the lack of enough economic models to enhance the security of mobile devices that need more attention for filling up the gaps in this area. Furthermore, it is widely believed that lack of the information security expertise among the IT workforce has posed a hindrance to fight against cybercrime because there are a lot of opportunities for hackers to compromise information security infrastructure. We can also highlight another flaw in this field by denoting that just some publications like WEIS and GameSec conferences focus mainly on the economics of security issues, and it is vitally important to impress other well-known and reliable publications and journals for getting them more involved in this area. In addition, organizations and firms must understand this matter that the best security technologies in the world cannot stop a social engineer impersonating legal user to access the systems. Hence, they should not invest further to avoid the risks and vulnerabilities. They should learn how should adapt themselves with a real risk environment; also, they should try to be risk averse for mitigating the risk of attack instead of the ineffective attempts for avoiding the risk by spending exorbitant costs on security.

To wrap up all findings, the significance of this study is dramatically shifting the current economics of security landscape towards more strategic approaches like metrics, policies, risk management and investment of security. As remarked by [84], information security has emerged as a new paradigm that requires a multi-decision approach that has arisen the microeconomics of security issues due to the decision based nature of this field.

4. Conclusion

Economics of security has shifted from theoretical issues to implement the mathematical and economical models. This survey provides an overview of development in the economics of security and categorizes the presented

works into six main sub-field based on obtained results as follows: information security investment, trust, privacy and access control, network security, malicious program and malware economics, penetration testing and digital forensics and software security.

This overview aims to familiarize readers with major areas in this field and to indicate the overlooked issues as much as possible. The results of the survey have also illustrated that as we entered the twenty-first century the field of economics of security has widened and its focus is dramatically moving towards develop a mathematical model for optimizing the cost of security. It is no coincidence that the study shows a shift towards the legal and security investment, economics of risk management and economics of malware. The survey's findings have also disclosed that most of the security challenges mainly related to the decision are based on strategies in security for financial gaining. The researchers in this field are widely believed that decision-making strategy will approach in the future evolutions of the economics of security discipline. New research efforts are demanded to fading out the gap between economic and security issues to reinforce the economics tendency surrounding the security by proposing efficient implementations and models.

References:

[1] Workshop on the Economics of Information Security (WEIS). Available from: http://weis2012.econinfosec.org/.

[2] Science, N.R.C.C. and T.B.S.S.S. Committee, Computers at Risk: Safe Computing in the Information Age1991: Washington, DC: National Academy Press.

[3] Anderson, R. Why information security is hard-an economic perspective. 2001.

[4] Akerlof, G.A., The market for" lemons": Quality uncertainty and the market mechanism. The quarterly journal of economics, 1970: p. 488-500.

[5] Gordon, L.A. and M.P. Loeb, The economics of information security investment. ACM Trans. Inf. Syst. Secur., 2002. 5(4): p. 438-457.

[6] Gordon, L.A. and M.P. Loeb, Using information security as a response to competitor analysis systems. Communications of the ACM, 2001. 44(9): p. 70-75.

[7] Acquisti, A. Security of Personal Information and Privacy: Economic Incentives and Technological Solutions. 2002.

[8] Camp, J. Marketplace Incentives to Prevent Piracy: An Incentive for Security? in WEIS 2002. 2002.

[9] Odlyzko, A. Privacy, economics, and price discrimination on the Internet. in Proceedings of the 5th international conference on Electronic commerce. 2003. ACM.

[10] Acquisti, A. and J. Grossklags. Privacy and rationality: preliminary evidence from pilot data. in Third Workshop on the Economics of Information Security (2004, Minneapolis, Mn). 2004.

[11] Odlyzko, A. The unsolvable privacy problem and its implications for security technologies. in Information Security and Privacy. 2003. Springer.

[12] Campbell, K., et al., The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security, 2003. 11(3): p. 431-448.

[13] Wölfl, A., The service economy in OECD countries. 2005.

[14] Ozment, A. and S.E. Schechter. Bootstrapping the adoption of internet security protocols. in Proc. Fifth Workshop on the Economics of Information Security. 2006.

[15] Park, Y. and S. Scotchmer, Digital rights management and the pricing of digital products, 2005, National Bureau of Economic Research Cambridge, Mass., USA.

[16] Anderson, R. and T. Moore, The economics of information security. Science, 2006. 314(5799): p. 610-613.

[17] Böhme, R. and G. Kataria. Models and measures for correlation in cyber-insurance. in Workshop on the Economics of Information Security (WEIS), University of Cambridge, UK. 2006.

[18] Ghose, A. and U. Rajan. The economic impact of regulatory information disclosure on information security investments, competition, and social welfare. 2006.

[19] Megnien, C., Quels sont les resultats des forages du programme craie 700? Bulletin d'Information des Geologues du Bassin de Paris, 2000. 37(2): p. 142-147.

[20] Su, X., An overview of economic approaches to information security management. 2006.

[21] Cavusoglu, H., B. Mishra, and S. Raghunathan, A model for evaluating IT security investments. Communications of the ACM, 2004. 47(7): p. 87-92.

[22] Brecht, M., T. Nowey, and A. Krones. A Closer Look at Information Security Costs. in Workshop on the economics of information security, WEIS conference. 2012.

[23] Pal, R. and P. Hui, Modeling internet security investments: Tackling topological information uncertainty. Decision and Game Theory for Security, 2011: p. 239-257.

[24] Ioannidis, C., D. Pym, and J. Williams, Fixed costs, investment rigidities, and risk aversion in information security: A utility-theoretic approach. Economics of Information Security and Privacy III, 2011: p. 171-191.

[25] Aminnezhad, A., et al., Cloud forensics issues and opportunities. International Journal of Information Processing and Management, 2013. 4(4): p. 76-85.

[26] Willemson, J. On the Gordon & Loeb model for information security investment. 2006.

[27] Lelarge, M. and J. Bolot. Economic incentives to increase security in the internet: The case for insurance. in INFOCOM 2009, IEEE. 2009. IEEE.

[28] Beautement, A. and D. Pym. Structured systems economics for security management. 2010.

[29] Sowa, S., L. Tsinas, and R. Gabriel, BORIS–Business ORiented management of Information Security. Managing Information Risk and the Economics of Security, 2009: p. 81-97.

[30] Internet Growth Statistics - the Global Village Online. 2013; Available from: http://www.internetworldstats.com/emarketing.htm.

[31] Bolot, J. and M. Lelarge, Cyber insurance as an incentive for Internet security. Managing information risk and the economics of security, 2008: p. 269-290.

[32] Rainer, B., The Iterated Weakest Link A Model of Adaptive Security Investment. 2009(June): p. 24-25.

[33] Shetty, N., et al., Competitive cyber-insurance and internet security. Economics of Information Security and Privacy, 2010: p. 229-247.
[34] Rothschild, M. and J. Stiglitz, Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. The quarterly journal of economics, 1976: p. 629-649.
[35] Johnson, B., R. Böhme, and J. Grossklags, Security games with market insurance. Decision and Game Theory for Security, 2011: p. 117-130.
[36] Kirstein, R., Risk-neutrality and strategic insurance, 1999, CSLE Discussion Paper.
[37] Böhme, R., Towards insurable network architectures. it-Information Technology, 2010. 52(5): p. 290-293.
[38] Gellman, R. Privacy, consumers, and costs: How the lack of privacy costs consumers and why business studies of privacy costs are biased and incomplete. in Digital Media Forum, Ford Foundation. 2002.
[39] Varian, H.R., Economic aspects of personal privacy. Topics in Regulatory Economics and Policy, 1996: p. 127-138.
[40] Preibusch, S. and J. Bonneau, The privacy landscape: product differentiation on data collection. Economics of Information Security and Privacy III, 2011: p. 263-283.
[41] Preibusch, S., K. Krol, and A.R. Beresford. The privacy economics of voluntary over-disclosure in Web forms. 2012.
[42] Pitofsky, R., et al., Privacy online: Fair information practices in the electronic marketplace. Statement of the Federal Trade Commission before the Committee on Commerce, Science and Transportation, United States Senate, Washington, DC, 2000.
[43] Ben-Ner, A. and L. Putterman, Trust in the New Economy1. 2002.
[44] Guerra, G., et al., Economics of trust in the information economy: Issues of identity, privacy and security. OECD Information Security and Privacy Working Paper No. JT00142557, OII Research Report No. 1, 2003.
[45] Hirshleifer, J., The private and social value of information and the reward to inventive activity. The American economic review, 1971. 61(4): p. 561-574.
[46] Shen, Y. and S. Pearson, Privacy Enhancing Technologies: A Review. 2013.
[47] Acquisti, A., Identity management, privacy, and price discrimination. Security & Privacy, IEEE, 2008. 6(2): p. 46-50.
[48] Cisco, economic impact of network security threats. 2002.
[49] Cybenko, G., A. Giani, and P. Thompson. Cognitive hacking and the value of information. in Workshop on Economics and Information Security. 2002.
[50] Gueye, A. and V. Marbukh, A Game-Theoretic Framework for Network Security Vulnerability Assessment and Mitigation, in Decision and Game Theory for Security2012, Springer. p. 186-200.
[51] Gueye, A., J. Walrand, and V. Anantharam, Design of network topology in an adversarial environment. Decision and Game Theory for Security, 2010: p. 1-20.
[52] Maillé, P., P. Reichl, and B. Tuffin, Interplay between security providers, consumers, and attackers: a weighted congestion game approach. Decision and Game Theory for Security, 2011: p. 67-86.
[53] Rahman, M.R., A survey of incentive mechanisms in peer-to-peer systems, 2009, Citeseer.
[54] Grossklags, J., N. Christin, and J. Chuang. Security and insurance management in networks with heterogeneous agents. in Proceedings of the 9th ACM conference on Electronic commerce. 2008. ACM.
[55] Grossklags, J., N. Christin, and J. Chuang. Secure or insure?: a game-theoretic analysis of information security games. 2008.
[56] Narasimhan, H., V. Varadarajan, and C.P. Rangan, Towards a Cooperative Defense Model Against Network Security Attacks. 2010.
[57] Freudiger, J., et al. On non-cooperative location privacy: a game-theoretic analysis. in Proceedings of the 16th ACM conference on Computer and communications security. 2009. ACM.
[58] Manshaei, M., et al., Game theory meets network security and privacy. ACM transaction on Computational Logic, 2011. 5.
[59] Aminnezhad, A., A. Dehghantanha, and M.T. Abdullah, A survey on privacy issues in digital forensics. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2012. 1(4): p. 311-323.
[60] Overill, R., et al., A cost-effective model for digital forensic investigations, in Advances in Digital Forensics V2009, Springer. p. 231-240.
[61] Casey, E., Digital evidence and computer crime: Forensic science, computers, and the internet2011: Academic press.
[62] Nochenson, A. and C.L. Heimann, Simulation and Game-Theoretic Analysis of an Attacker-Defender Game, in Decision and Game Theory for Security2012, Springer. p. 138-151.
[63] Stone-Gross, B., et al., The underground economy of fake antivirus software, in Economics of Information Security and Privacy III2013, Springer. p. 55-78.
[64] Buldas, A. and R. Stepanenko, Upper Bounds for Adversaries' Utility in Attack Trees, in Decision and Game Theory for Security2012, Springer. p. 98-117.
[65] Florêncio, D. and C. Herley, Where Do All the Attacks Go?, in Economics of Information Security and Privacy III2013, Springer. p. 13-33.
[66] Böhme, R. and M. Félegyházi, Optimal information security investment with penetration testing, in Decision and Game Theory for Security2010, Springer. p. 21-37.
[67] August, T. and T.I. Tunca, Who should be responsible for software security? A comparative analysis of liability policies in network environments. Management Science, 2011. 57(5): p. 934-959.
[68] August, T. and T.I. Tunca, Network software security and user incentives. Management Science, 2006. 52(11): p. 1703-1720.
[69] Anderson, J., J. Bonneau, and F. Stajano. Inglorious installers: security in the application marketplace. in Workshop on the Economics of Information Security (WEIS). 2010.
[70] Kannan, K., R. Telang, and H. Xu. Economic analysis of the market for software vulnerability disclosure. in System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on. 2004. IEEE.
[71] The Economics of Cybercrime and the Law of Malware Probability, 2010.

[72] Kondakci, S., A concise cost analysis of Internet malware. Computers & Security, 2009. 28(7): p. 648-659.
[73] Chia, P.H. and J. Chuang, Colonel blotto in the phishing war, in Decision and Game Theory for Security2011, Springer. p. 201-218.
[74] Borel, E., The Theory of Play and Integral Equations with Skew Symmetric Kernels. Econometrica, 1953: p. 97-100.
[75] Bensoussan, A., M. Kantarcioglu, and S.C. Hoe, A game-theoretical approach for finding optimal strategies in a botnet defense model, in Decision and Game Theory for Security2010, Springer. p. 135-148.
[76] Lelarge, M. Economics of malware: Epidemic risks model, network externalities and incentives. in Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on. 2009. IEEE.
[77] Varian, H., System reliability and free riding. Economics of Information Security, 2004: p. 1-15.
[78] Lelarge, M. and J. Bolot. A local mean field analysis of security investments in networks. in Proceedings of the 3rd international workshop on Economics of networked systems. 2008. ACM.
[79] Lelarge, M. and J. Bolot. Network externalities and the deployment of security features and protocols in the internet. in ACM SIGMETRICS Performance Evaluation Review. 2008. ACM.
[80] Bolot, J.C. and M. Lelarge. A new perspective on internet security using insurance. in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. 2008. IEEE.
[81] Cremonini, M. and D. Nizovtsev, Understanding and influencing attackers' decisions: Implications for security investment strategies. 2006.
[82] 82. Kodialam, M. and T. Lakshman. Detecting network intrusions via sampling: a game theoretic approach. in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. 2003. IEEE.
[83] Bohacek, S., et al., Game theoretic stochastic routing for fault tolerance and security in computer networks. Parallel and Distributed Systems, IEEE Transactions on, 2007. 18(9): p. 1227-1240.
[84] Theoharidou, M., et al., The insider threat to information systems and the effectiveness of ISO17799. Computers & Security, 2005. 24(6): p. 472-484.

Table 1- -Obtained Fields from Selected publications

	Decision Support Systems	GameSec Conference	IEEE Transactions on Information Forensics and Security	SANS	Telecommunications Policy	WEIS	TOTAL
Penetration Testing and Digital Forensics	-	**4**	-	-	-	**12**	**16**
Malicious Program and Malware	**1**	**2**	-	-	-	**12**	**15**
Network Security	-	7	**3**	-	**2**	**9**	**21**
Information Security Investment	**2**	**2**	-	**3**	**1**	**35**	**43**
Software Security	**1**	-	-	-	-	**10**	**11**
Trust and Privacy	-	**4**	-	-	-	**26**	**30**
TOTAL	4	19	3	3	3	104	136

Table 1- Payoff matrix

	Respect	Defect
Buys	B	B-V
Doesn't	0	0

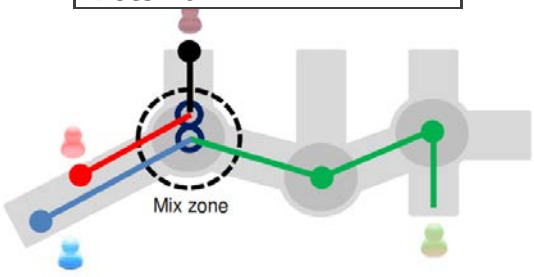

Figure 1- An example of a 2-node mix zone, where mobile nodes change their identifiers at the mix zone

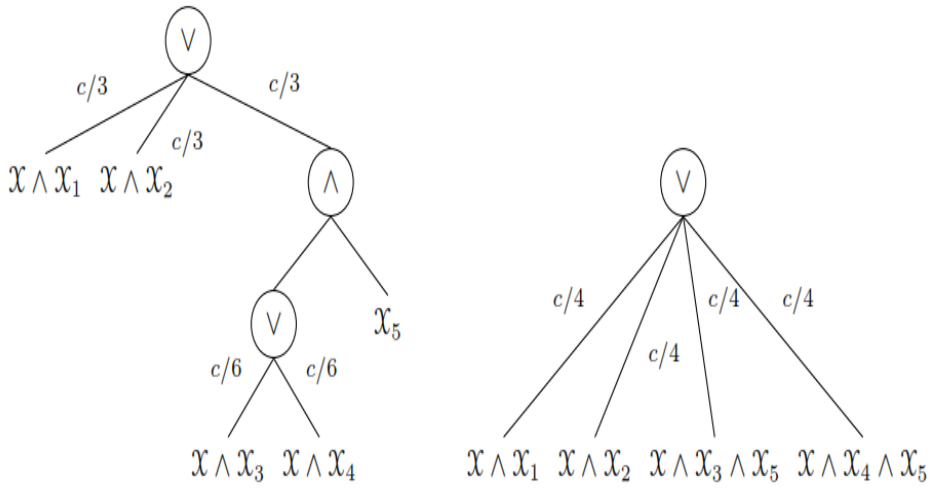

Figure 2 - Iterated cost reduction based on the tree structure (left) and cost reduction based on the DNF (right)